PROGETTO S6/L5

SCOPO: usare l'attacco XSS reflected per rubare i cookie di sessione alla macchina DVWA,tramite uno script.Poi dobbiamo :

- **Spiegare come si comprende che un sito è Vulnerabile.**
- **Portare l'attacco XSS .**
- **Fare un report su come avviene l'attacco con qualche screen short.**

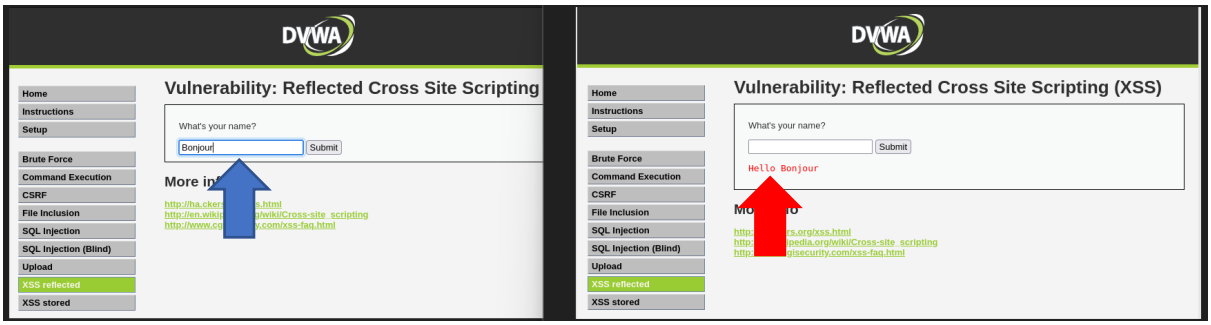
1-) capire che cos'è un attacco xss reflected

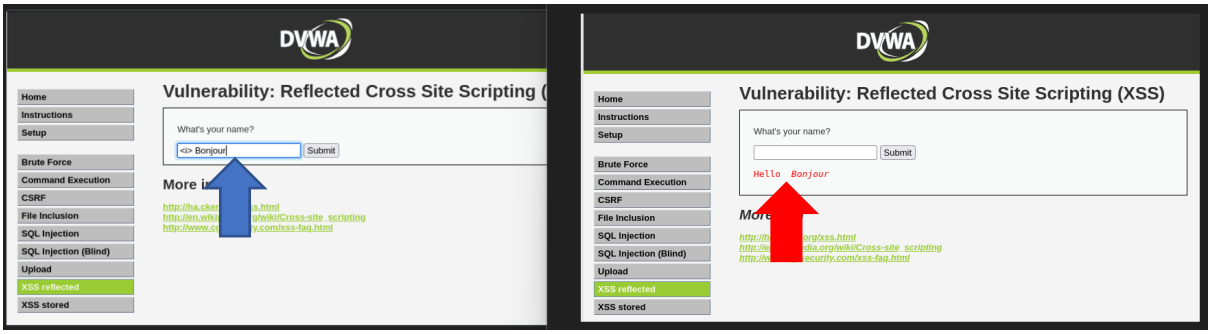
Un attacco XSS(cross site scrypting) reflected: è il fatto di eseguire script dannosi a l'interno di un sito web vulnerabile nello scopo finale di rubare informazione sensibile agli utenti.
Questi tipi di attachi, sfruttanno il fatto che l'input degli utenti mancano adeguata sanitizzazione.
Sfruttanno anche cookie di sessione per eseguire l'attacco.I cookie di sessione sono un tipo di cookie utilizzato nelle applicazione web per memorizzare temporaneamente informazioni durante la durata di una sessione di navigazione.

2-) come capire che un sito web è vulnerabile?

Come detto prima; Il successo di un attacco XSS reflected è dovuto al fatto che il sito web sia vunerabile o non sanitizzato(che esegue il codice).per dimostrare che la nostra macchina DVWA esegue il codice abbiamo usato la stessa parola "Bonjour" l'abbiamo inserito nella barra di ricerca del sito e abbiamo avuto come out put la stessa parola.ma inserendo la stessa parola con la comand: "<i>" abbiamo ottenuto la parola Bonjour in corsivo quindi questo sito esegue il codice e per conseguenza è vulnerabile.

PROGETTO S6/L5





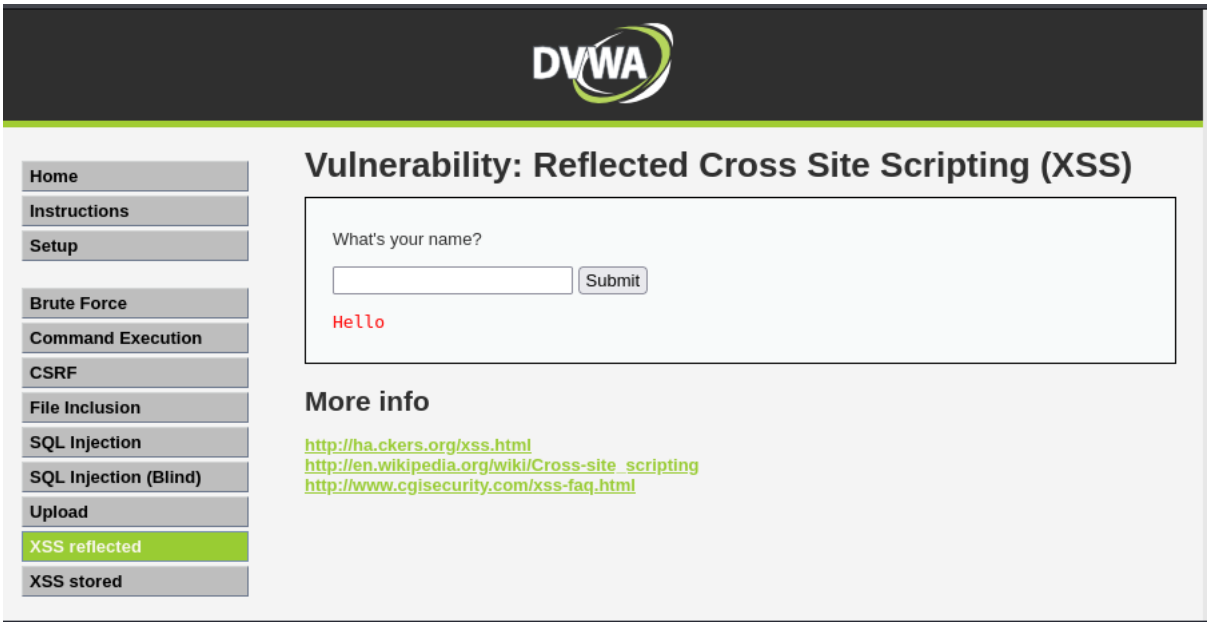
se invece il sito web non era vulnerabile avremmo ottenuto gli stessi risultati in output.

Tuttavia è importante non confondere questo tipo di attacco con l'attacco: CSRF(Cross Site Request Forgery) che entra nalla stessa categoria(XSS). nell'attacco CSRF l'attacante convince un utente autenticato a eseguire determinata azione, come fare click su un link o visualizzare un'immagine.e questa azione invia involontariamente una richiesta HTTP a un sito web al quale l'utente è autenticato.

3-) Portare l'attacco

Per portare l'attacco abbiamo utlizzato la macchina Metasploitable2 su Kali Linux eseguendo il ping. Poi abbiamo aperto la DVWA abbiamo stabilito la DVWA su XSS abbiamo inserito il script malevole e poi abbiamo fatto invio. E abbiamo ottenuto i risultati seguente:

PROGETTO S6/L5



Dopo di che abbiamo usato netcat per rubare il link di sessione utilizzando la comanda: nc -l -p 12345 . con 12345 che indica la porta.