Di Edoardo Castelli

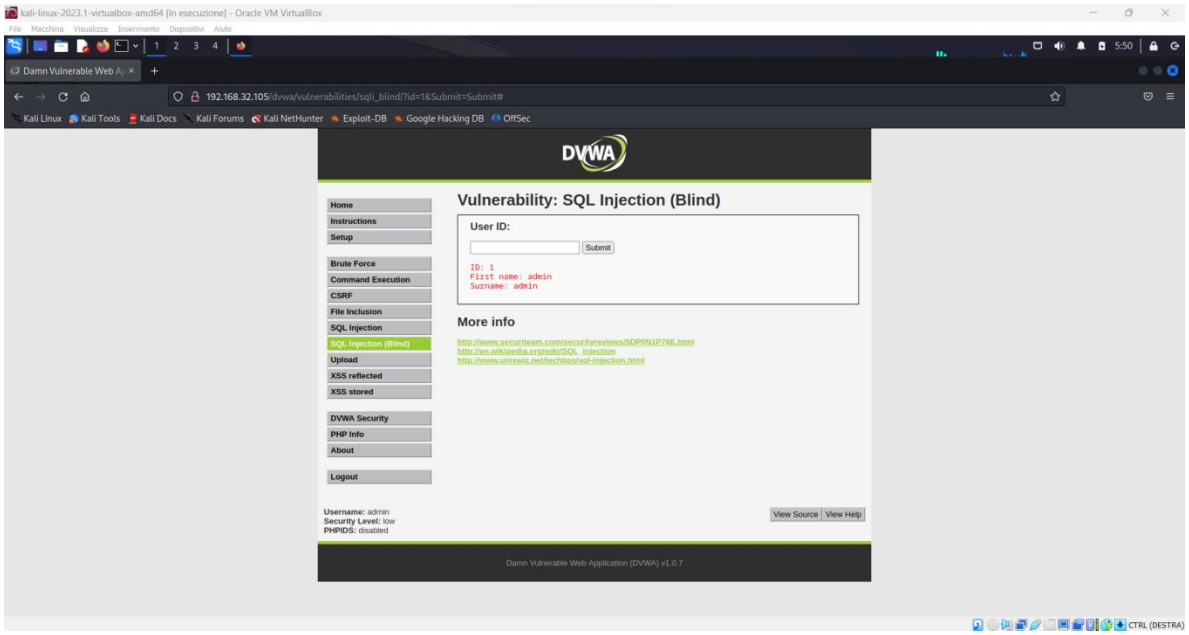
Web Application Hacking

Per il progetto di questa settimana è richiesto allo studente di sfruttare le vulnerabilità di XSS e SQL Injection per effetuare degli attacchi web, con obiettivo la DVWA installata sulla macchina Metasploitable.

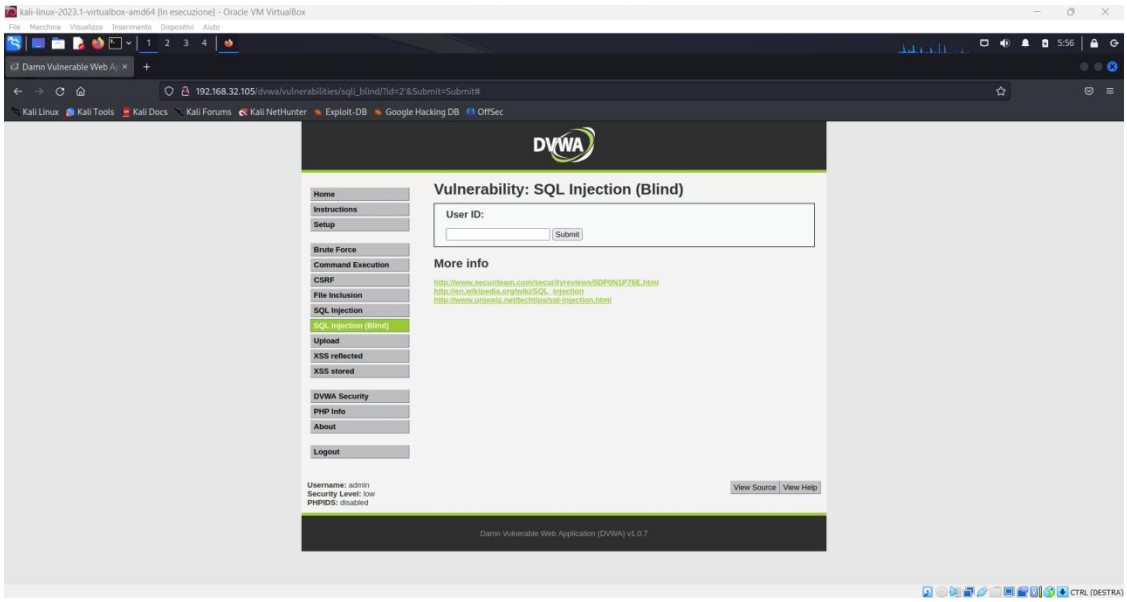
In particolare, la consegna prevede una SQLi di tipo Blind e un attacco XSS persistente, che invii i cookie di sessione degli utenti ad un server a disposizione dell'attaccante.

- SQLi (Blind):

Dopo essermi accertato che le macchine siano correttamente configurate ed aver impostato il livello di sicurezza della DVWA (low), mi sposto nella sezione SQLi (blind) ed inizio a verificare la presenza di un punto di iniezione, prima inserendo un comando correto ("1" nel campo ID):

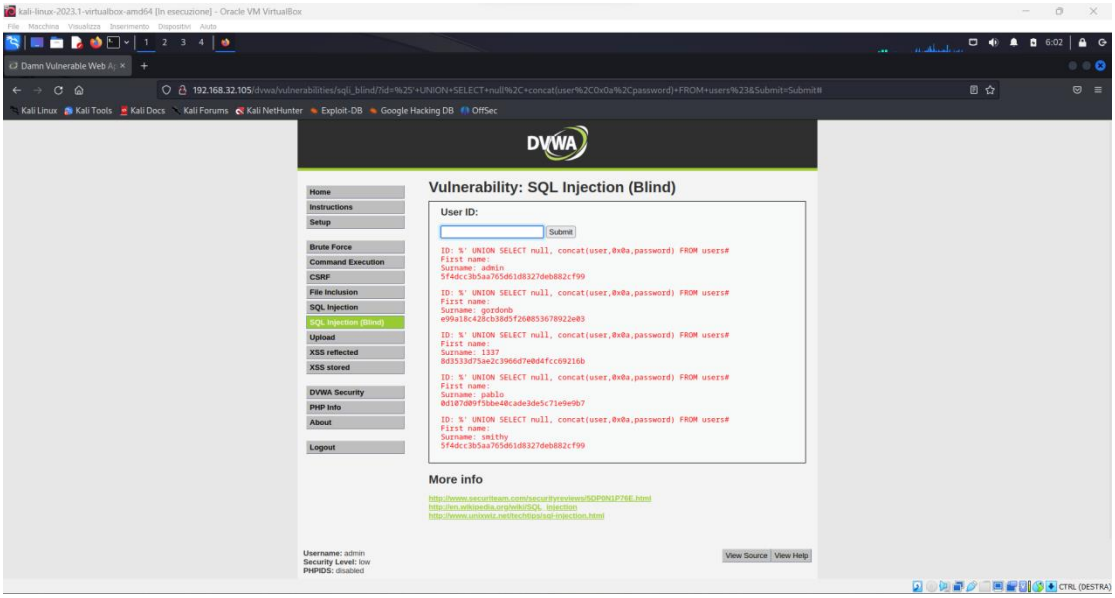


Conseguentemente inserisco un comando errato, per essere sicuro che la DVWA restituisca entrambi i tipi di output (in questo caso " 1' "):

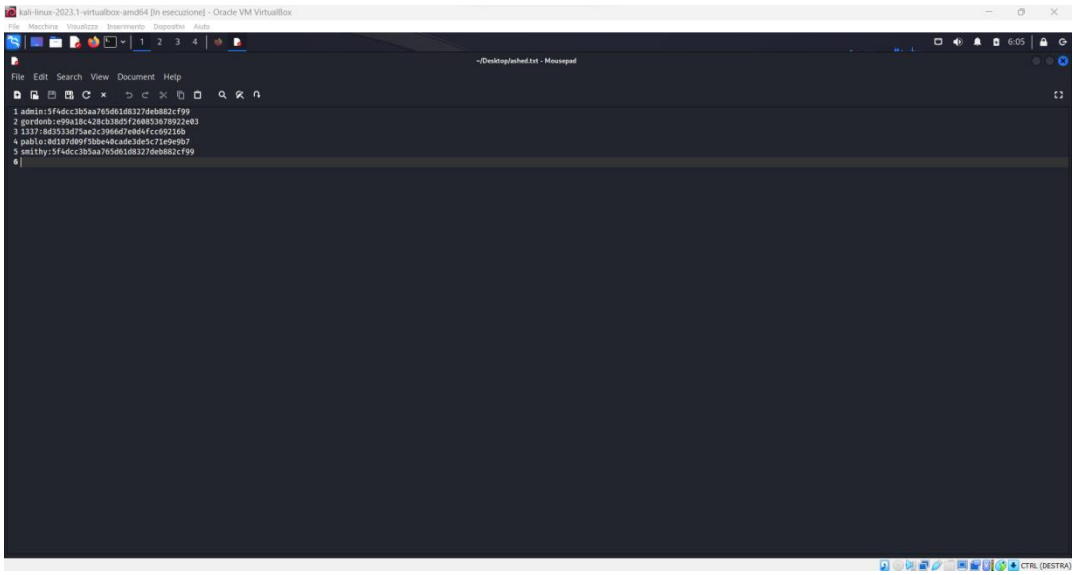


Trattandosi di un'iniezione di tipo "blind", non rimango molto stupito dalla mancanza di messaggi di errore. Provo comunque ad inserire una query più complessa per tentare l'estrapolazione delle credenziali, con il comando " %' UNION SELECT null, concat(user,0x0a,password) FROM users# ".

Considerando l'output del comando, concludo asserendo che la procedura è andata a buon fine.

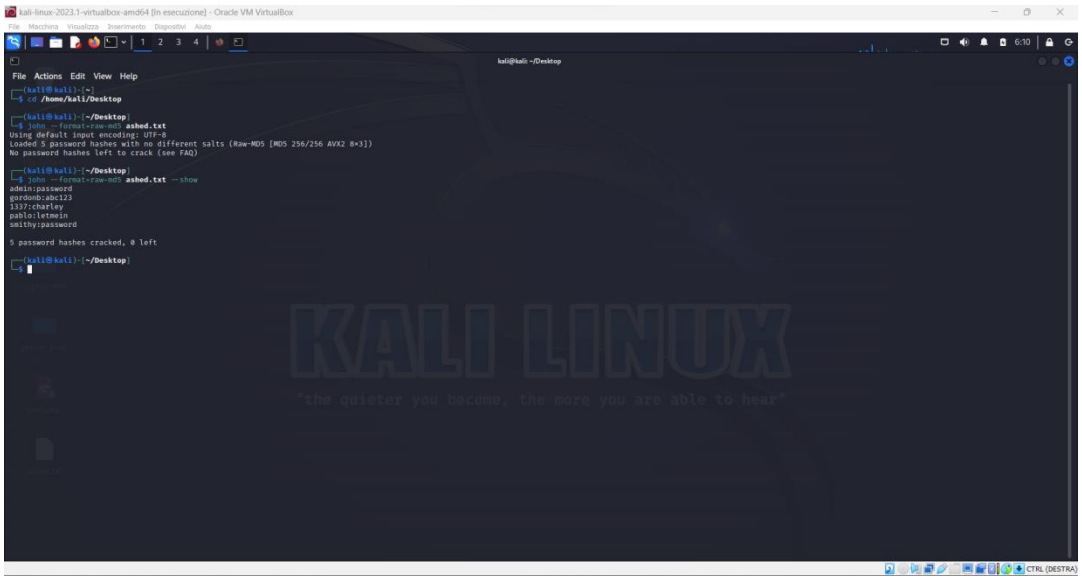


Giunto a questo punto, creo un file di testo sulla macchina Kali di modo da avere la lista dei nomi utenti e le password nello stesso documento, pronto per essere "dato in pasto" a John the Ripper, il tool scelto per il cracking delle stesse password appena estrapolate:

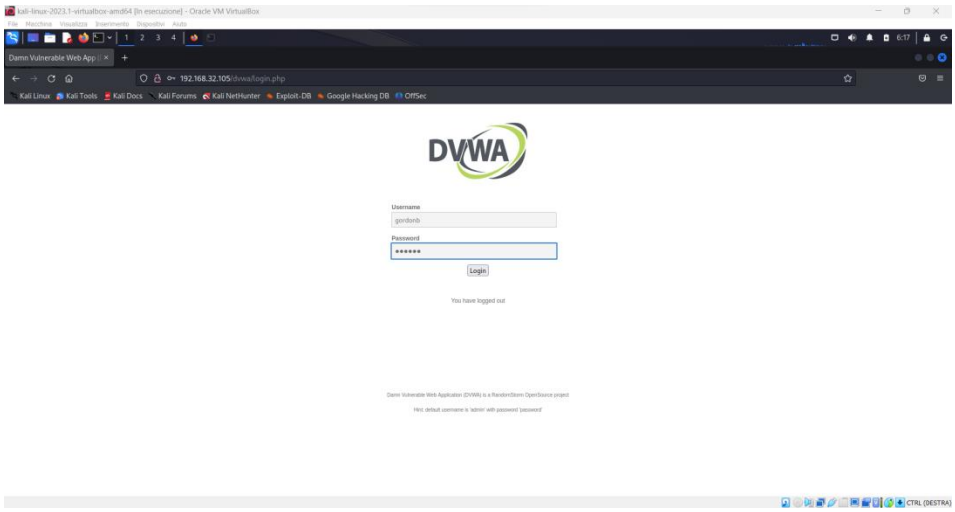


Salvo il file sul Desktop e avvio il tool di cracking, utilizzando il comando

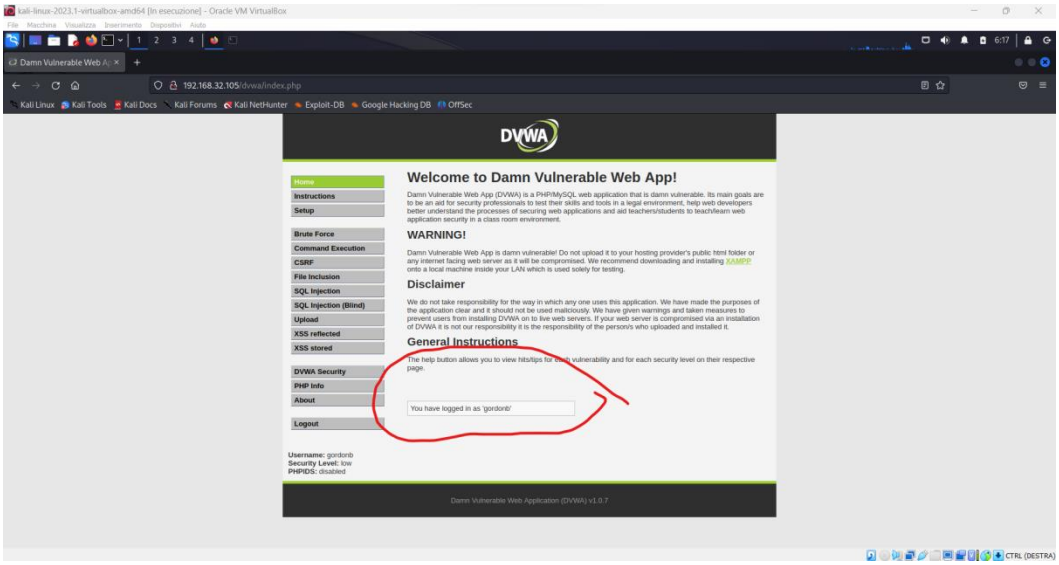
“ john -- format=raw-MD5 ashed.txt” e aggiungendo successivamente “-- show” per verificare l’output del programma:



Arrivato a questo punto, provo una delle combinazioni estrapolate (per l’user “gordonb”, in questo caso) per essere sicuro che l’attacco sia andato a buon fine:



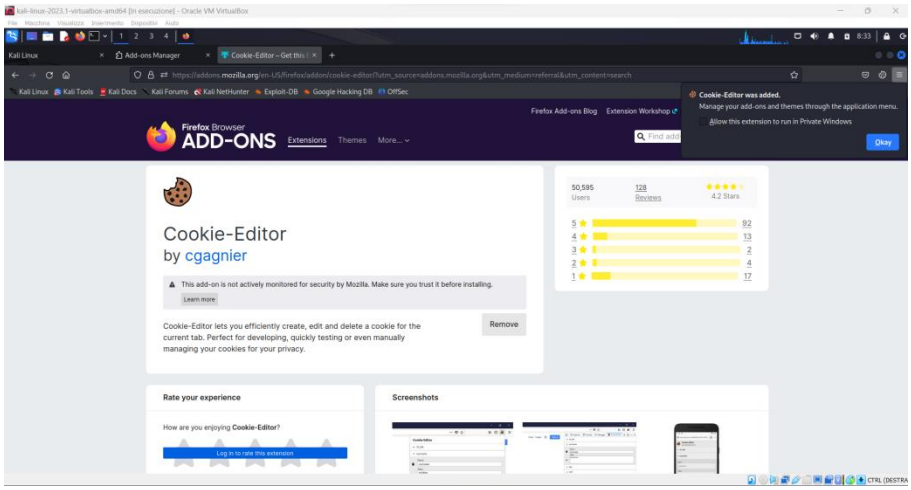
Il login ha avuto successo, come si può notare dalla pagina di benvenuto dello stesso utente "gordonb".



- **XSS (stored):**

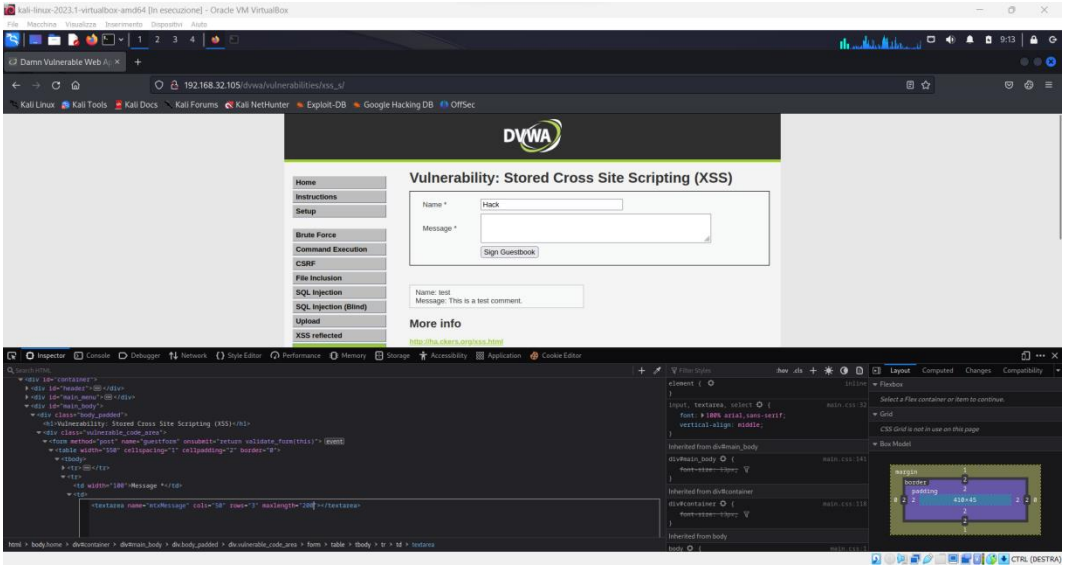
Si procede a questo punto con il tentativo di exploit per la corretta implementazione di un XSS persistente, un tipo di attacco molto pericoloso vista la difficoltà per gli utenti e gli amministratori della macchina target di rintracciare il codice malevolo "nascosto" nel codice sorgente di una delle stesse pagine della web application. Nel caso specifico, verrà utilizzato questo tipo di attacco per recuperare impropriamente i cookie di sessione degli utenti.

Sarà anzitutto necessario, qualora non se ne fosse già provvisti, installare un cookie editor sul browser, spostandosi dunque in NAT se non fatto precedentemente e poi di nuovo in rete interna.

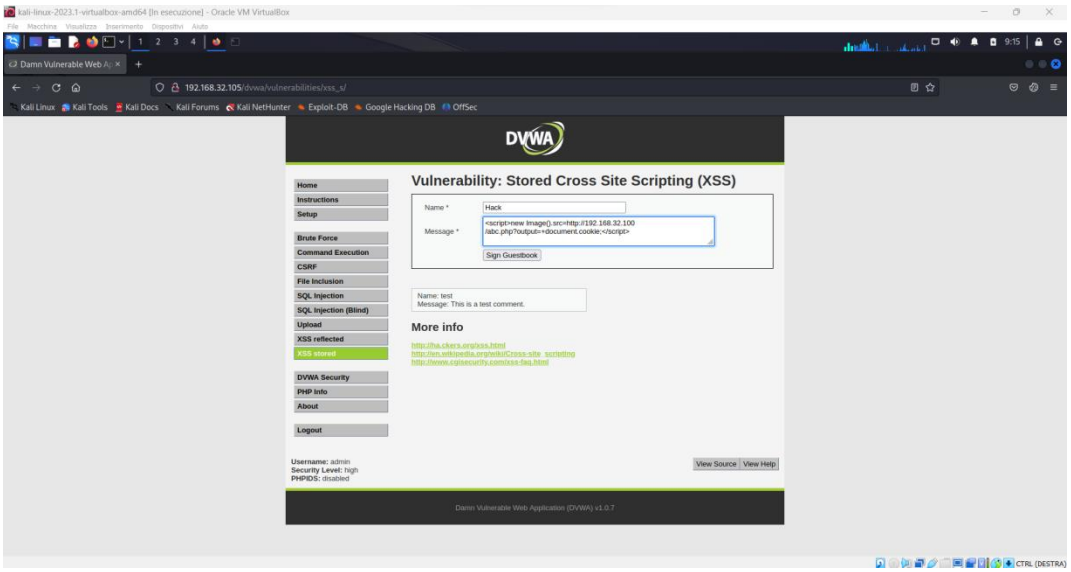


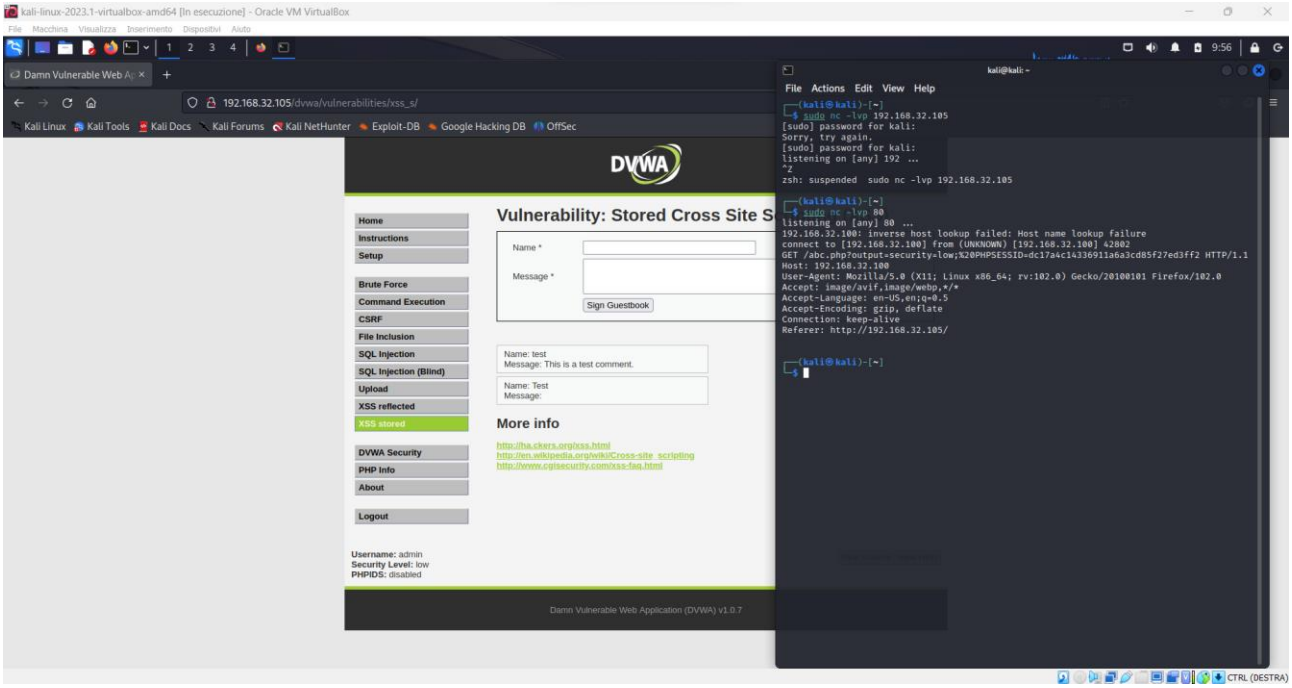
Una volta fatto ciò, sarà possibile modificare od inserire i cookie di sessione a mio piacimento, potendo di fatto appropriarmi della sessione dell'utente malcapitato.

Apro quindi la DVWA e mi sposto nella sezione "XSS stored", dove anzitutto provo a modificare la lunghezza massima della casella "message" da "50" a "200":

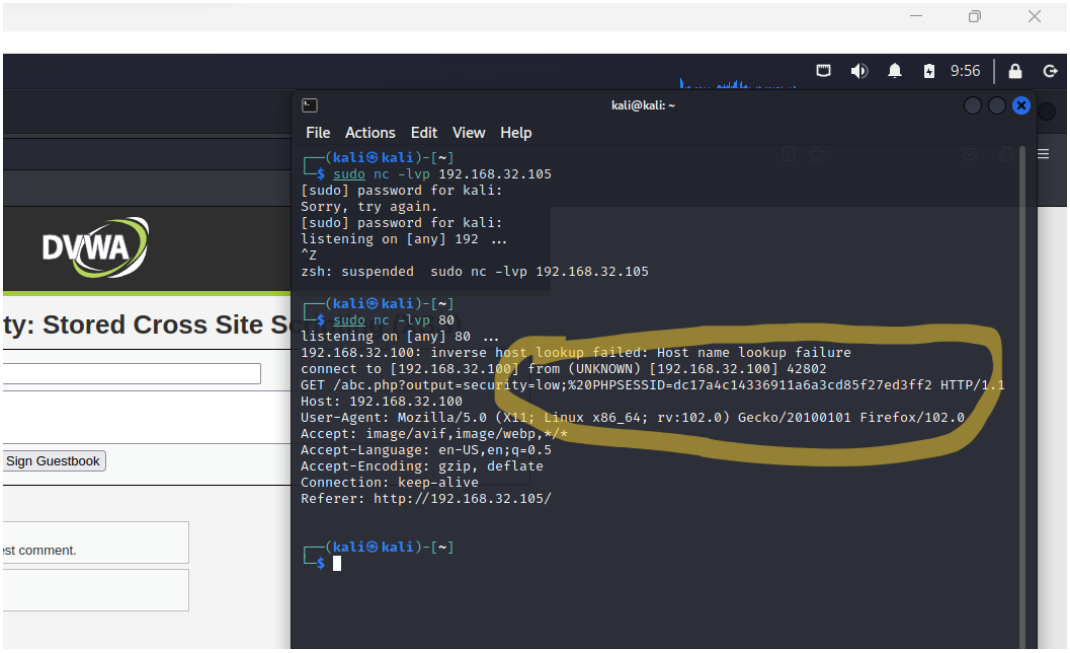


Fatto ciò, sarà possibile caricare sul sito lo script malevolo, che reindirezzerà i cookie di sessione degli utenti a NetCat, in questo caso configurato come server in ascolto sulla porta 80 sulla macchina Kali:

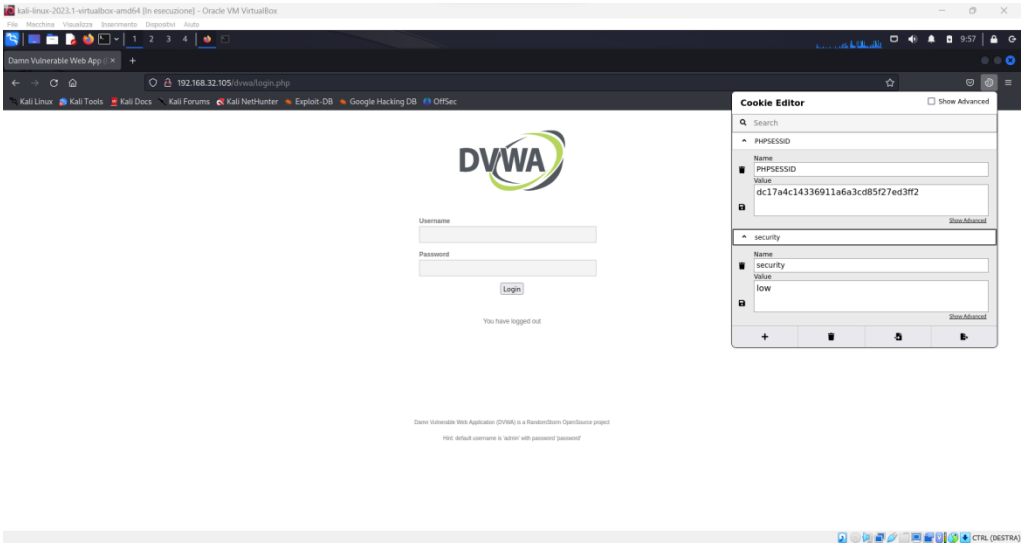




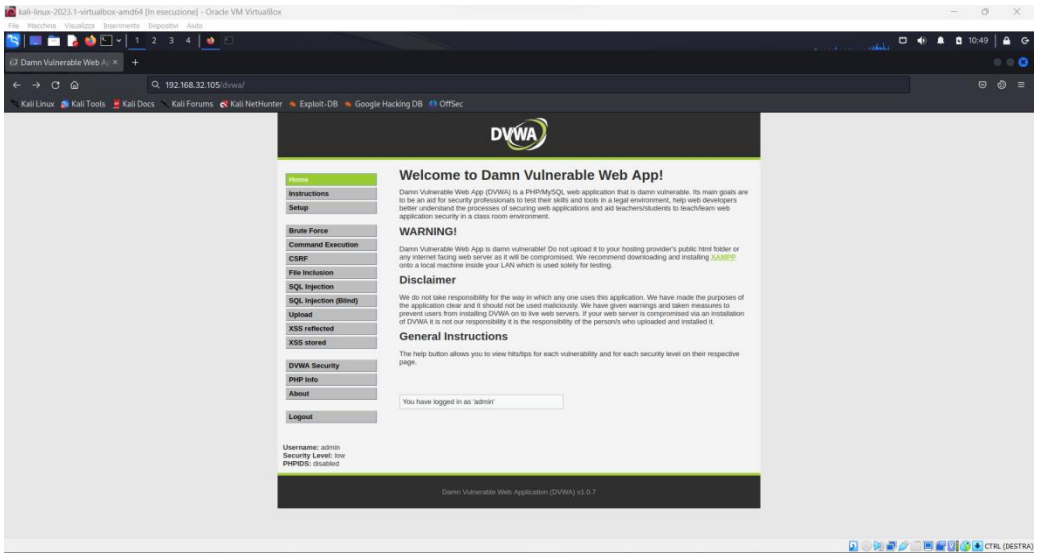
Si può notare come su Netcat sia possibile grazie allo script inserito recuperare il cookie di sessione dell'utente.

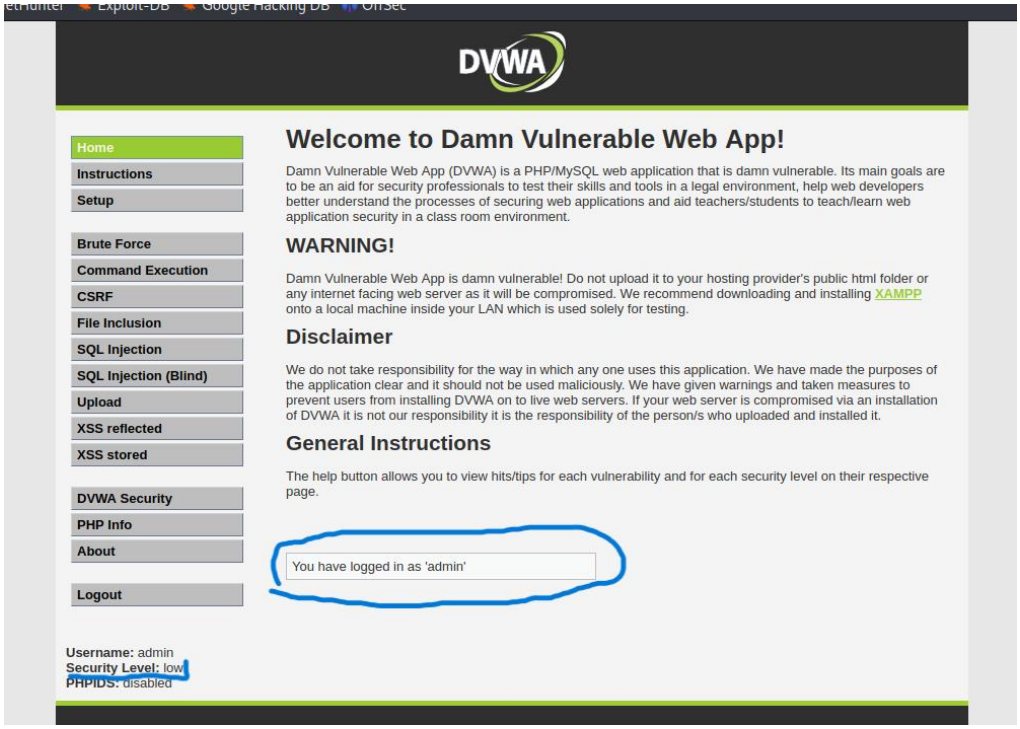


A questo punto, sarà possibile sfruttare il cookie appena sottratto, tramite il cookie-editor precedentemente installato, per accedere alla sessione “rubata”:



Una volta salvate le impostazioni del cookie, sarà sufficiente cancellare nell’URL “login.php” e premere “Invio”. Se il browser ha salvato correttamente il cookie di sessione, si aprirà la pagina di benvenuto della DVWA, come se avessimo regolarmente inserito le credenziali.


kali-linux-2023.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
192.168.32.105/dvwa/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web App!
WARNING!
Disclaimer
General Instructions
You have logged in as 'admin'
Username: admin
Security Level: low
PHPIDS: disabled
Damn Vulnerable Web Application (DVWA) v1.0.7


Exploit-DB
Google Hacking DB
OffSec
DVWA
Home
Instructions
Setup
Brute Force
Command Execution
CSRF
File Inclusion
SQL Injection
SQL Injection (Blind)
Upload
XSS reflected
XSS stored
DVWA Security
PHP Info
About
Logout
Welcome to Damn Vulnerable Web App!
Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.
WARNING!
Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.
Disclaimer
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.
General Instructions
The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.
You have logged in as 'admin'
Username: admin
Security Level: low
PHPIDS: disabled