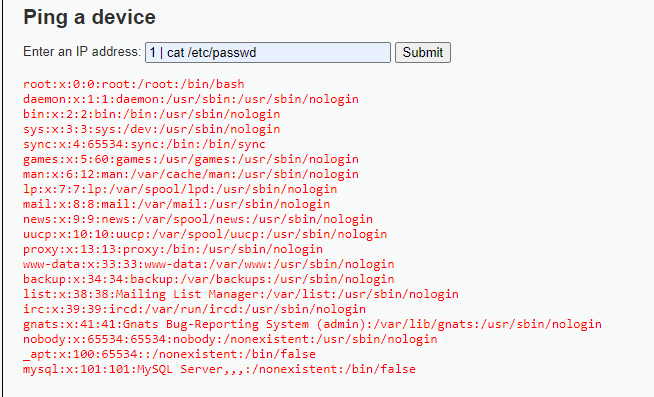
Ernest Šembera, 0036524274

Treća laboratorijska vježba: Ranjivosti web aplikacija

1. Izvođenje naredbi (Command Injection)

Nakon što sam isprobao par naredbi zadanih u zadatku, shvatio sam da se pomoću 1 | “naredba” može izvršiti bilo koja bash naredba, te sam upisao naredbu za ispis podataka cat te putanju do tražene datoteke.

Rezultat je bio sljedeći:

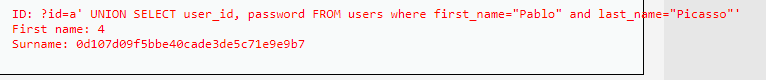


1. Napadi SQL umetanjem (SQL injection)

Nakon što sam ovdje isprobao primjere dane u zadatku, shvatio sam da se manipulacija bazom može raditi pomoću naredbe koja unutar jednostrukih navoda dodaje UNION SELECT naredbu. S obzirom da se tražio password Pabla Picassa, poslao sam sljedeću SQL naredbu:

*?id=a' UNION SELECT user\_id, password FROM users where first\_name="Pablo" and last\_name="Picasso"'*

A ona mi je vratila sljedeće



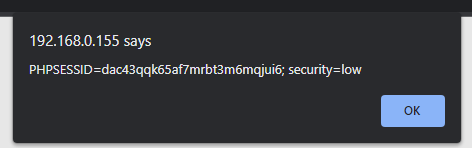
Zatim sam otišao na crackstation.net i dešifrirao password, te sam dobio sljedeće iz čega se može vidjeti da je password letmein:

Graphical user interface, text, application

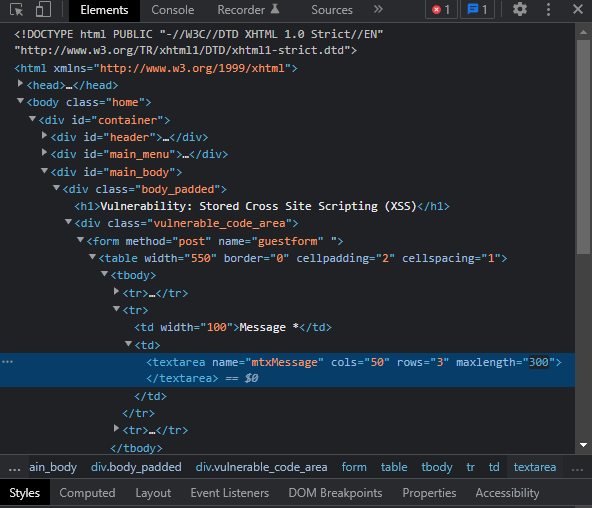
Description automatically generated

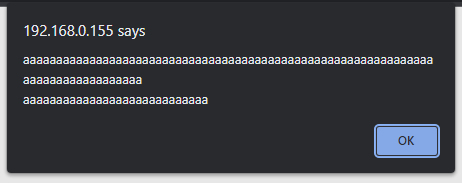
1. XSS (Cross Site Scripting)

Nakon što sam isprobao naredbe zadane u zadatku, shvatio sam da se u ovom primjeru mogu pokretati JS kodovi tako da u neko od dva polja (“Name” ili “Message”) upišem <script>”JS kod”</script>. S obzirom da je trebalo dobiti session cookie, pokrenuo sam naredbu *<script>alert(document.cookie)</script>* te sam u alertu dobio cookie.



Na pitanje kako bih zaobišao ograničenje broja znakova koje je moguće upisati, zaobišao bih to tako da bi u inspect elementsu promijenio vrijednost atributa maxwidth na neki veliki broj (npr. 300), te bih tada mogao poslati naredbu koja sadrži 300 znakova.





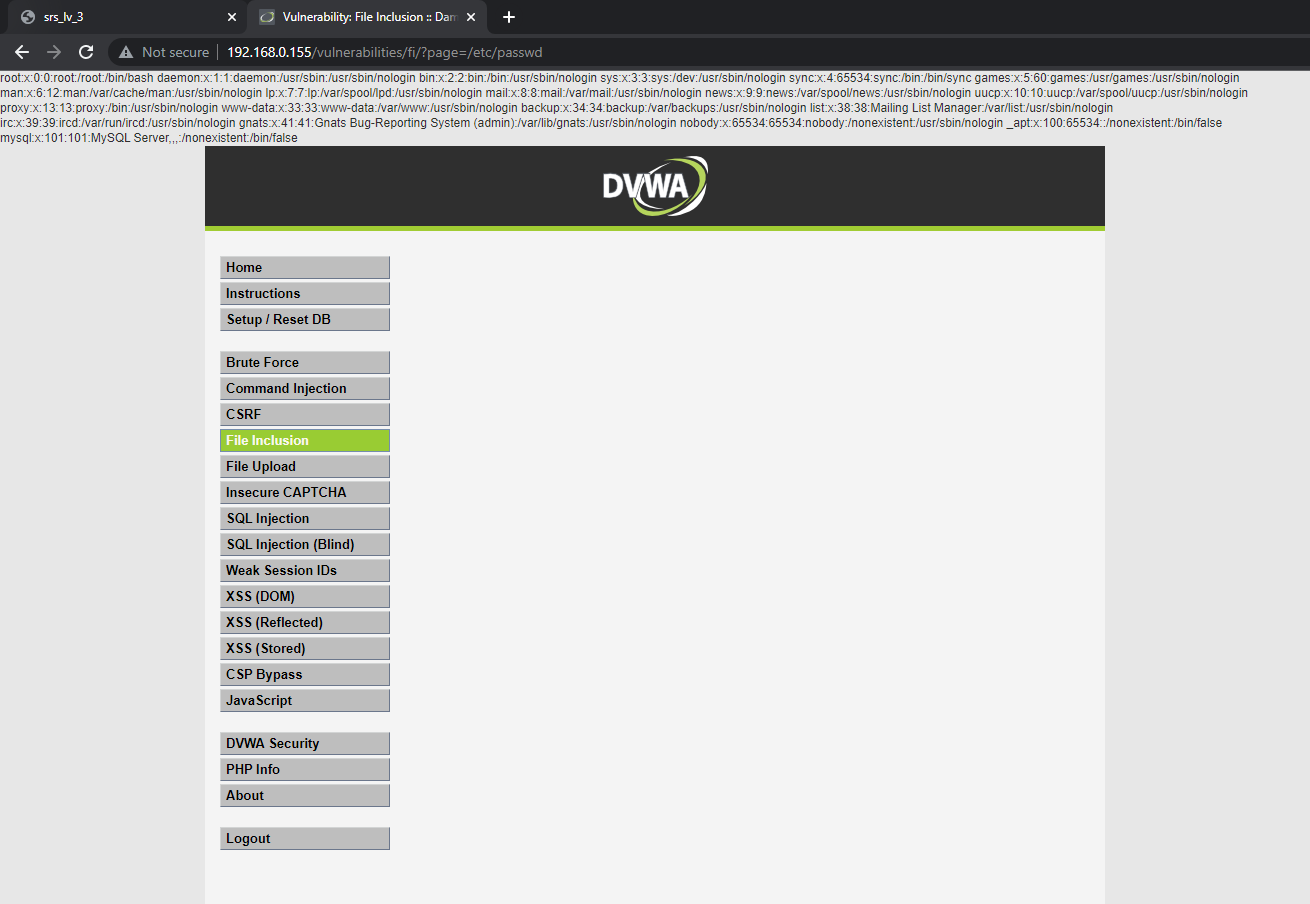
Dokaz da sam pokrenuo naredbu sa više od 50 znakova

U XSS(reflected) napadu, također koristimo JS kod kako bi napravili napad, samo ga ovaj put predajemo umjesto objekta koji bi inače poslali server tako da u polje gdje bismo inače upisali svoje ime upišemo sljedeći kod:

*?name=<script>alert(document.cookie);</script>*

1. Inkluzija datoteka (File inclusion)

U zadnjem zadatku ove laboratorijske vježbe je trebalo napraviti napad inkluziju datoteka, to sam izveo tako što sam umjesto imena neke od ponuđenih datoteka u link stavio /etc/passwd kao što je prikazano na sljedećoj slici:



Ovaj napad bih spriječio tako što bih hardkodirao putanje do file-ova koji bi trebali biti dostupni, a za sve ostale bih poslao 404.