Kauno technologijos universitetas

Informatikos fakultetas

T120B181 Kompiuterių tinklų ir interneto sauga

Laboratorinis darbas Nr.5.

Nedas Liaudanskis IFF-1/9

Studentas

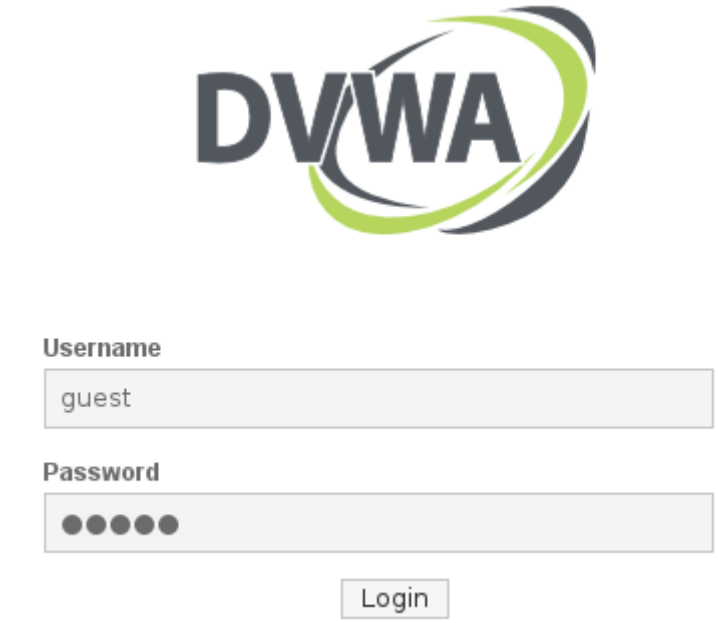
dėst. Donatas Sandonavičius

Dėstytojas

Įvadas

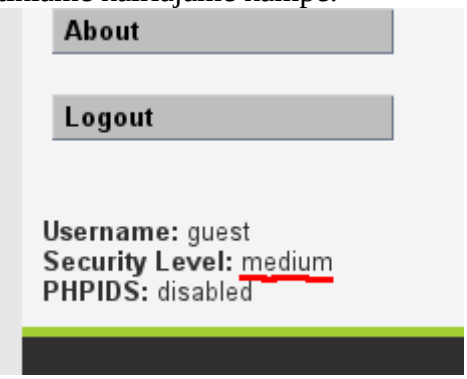
1.1. Prisijungimas

Šiame darbe bus atliekamos praktinės įsilaužimo į nesaugią web aplikaciją užduotys. Tam bus naudojama DVWA mokomoji nesaugi web aplikacija. Aplikaciją galite atsisiųsti adresu: https://github.com/ethicalhack3r/DVWA/ arba VMware virtulią XP OS su veikiančią aplikaciją adresais nurodytais moodle puslapyje. Jeigu sėkmingai įsijungėte šią aplikaciją atidarykite nuoruodą https://localhost/~dummyuser/ prisijungimo vardas **guest**, slaptažodžis **guest**



1.2. Saugumo lygio keitimas

Visos šiame laboratoriniame darbe atlikekamos atakos turi būti aliktos su vidutinio sistemos saugumo lygiu (***medium***). Dabartinis saugumo lygis rodomas visuose web aplikacijos puslapiuose apatiniame kairiajame kampe.



Saugumo lygį galima pakeisti puslapyje '**DVWA Security**'.

Dėmesio! Neniokokite web aplikacijos failų ir duomenų bazės, nedarykite destruktyvių veiksmų, nes nulaužus aplikacija susitrukdysite atliekdami savo užduotį.

2. Atakos

Laboratorinio darbo metu jums reikia atlikti ir aprašyti šias atakas:

1. Failų įkėlimo ataką
2. Failų įterpimo ataką
3. Komandų injekcijos ataką
4. SQL injekcijos ataką

1 Failų įkėlimo ataka

Darbas atliekamas DVWA sistemos ***Upload*** skiltyje.

Jūsų užduotis yra į sistemą įkelti PHP failą, kurį būtų galima įvykdyti serveryje. Kaip įrodymą įkeltas PHP scenarijus turi išspausdinti jūsų vardą ir pavardę. Tam kad jūsų failai nesimaišytų su kitų studentų įkeliamais failais įkeliamą failą vadinkite savo vardu ir pavarde (pvz: jonas.jonaitis.php).

Per šį sistemos puslapį įkeliami failai talpinami kataloge https://localhost/~dummyuser/hackable/uploads/ ten galite pasitikrinti ar jūsų failas įkeltias ir ar jis vykdomas.

Ataskaitoje aprašykite veiksmus kuriuos atlikote, šiai užduočiai pasiekti.

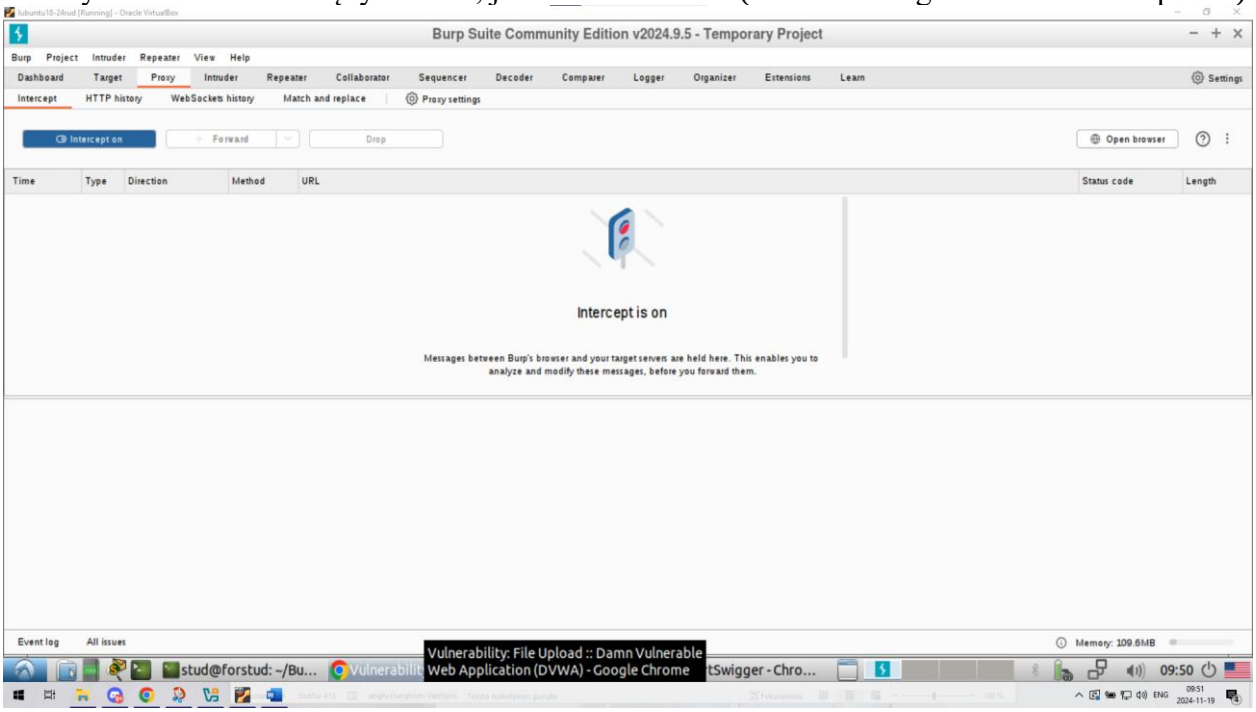
Atlikta ataka:

Norint atlikti failų įkėlimo ataką, pasinaudojau protokolo įrankis įrankiu. kuris leidžia peradresuoti interneto srautą per tarpinį serverį (proxy serverį). Tokie įrankiai naudojami norint stebėti, modifikuoti arba saugiai nukreipti interneto užklausas Šio įrankio dėka mes galime modifikuoti išsiunčiamas užklausas, taip, kad mano išsiunčiamas Nedas.php failas butų laikomas nuotrauka.

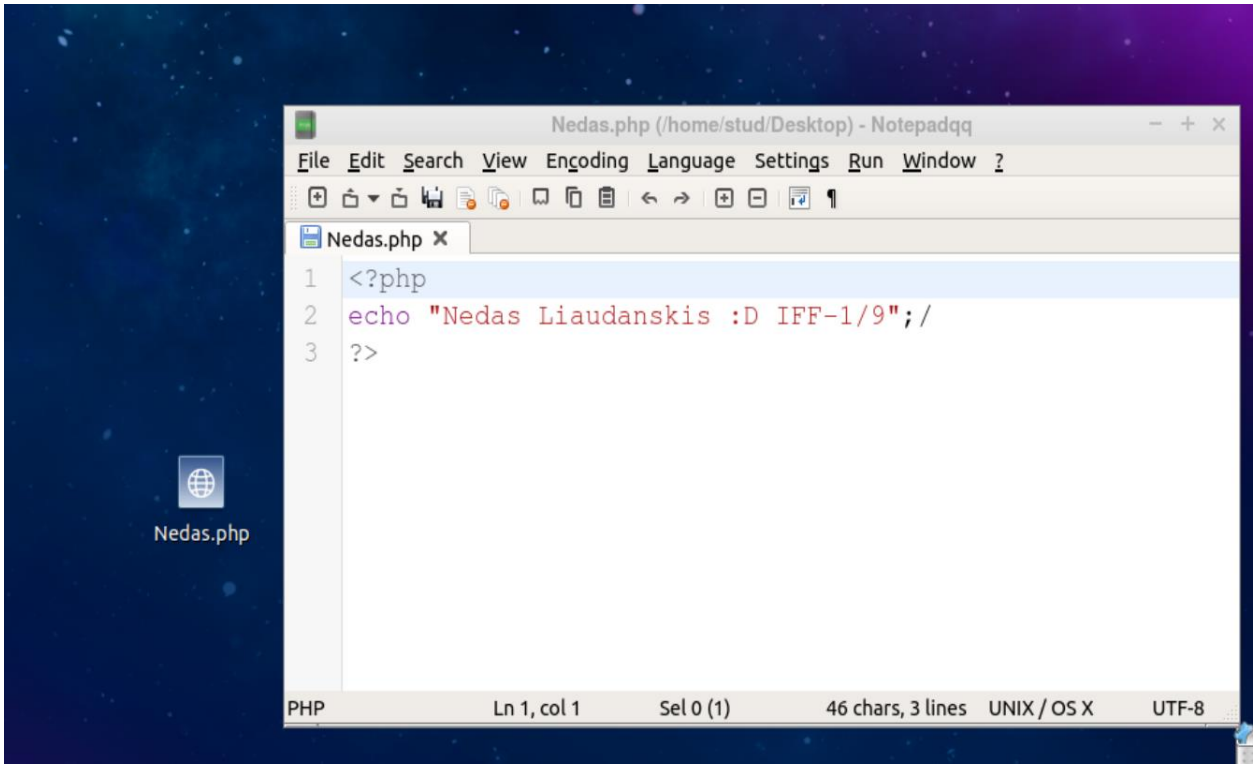
Protokolinis įrankis naudotas šiam laboratoriniame darbe buvo: Burp Suite.

Pirmas žingsnis buvo įjungti protokolinį įrankį, kurs leis mums modifikuoti išsiunčiamas užklausas (Burp Suite pav. 1).
Toliau reikia sukurti mums norimą .php failą (Nedas.php pav. 2). Failą pavadinau Nedas.php ir jame pridėjau paprastą komandą, kuri išrašo mano vardą ir pavardę, kartu su grupe. Sukurtas failas yra bandomas įkelti į sistemą (Įkeliamas Nedas.php failas pav. 3), įkeliant failą protokolinis įrankis sustabdo užklausos siuntimą ir leidžia ją modifikuoti. Norint, jog mano .php failas butų užskaitytas, kaip nuotrauką pakeičiau Content-type lauke esančia informaciją, iš application x-php į image/jpeg (Užklausa po pakeitimų pav. 5). Taip padarius ir išsiuntus užklausą failas buvo priimtas. Priimtas

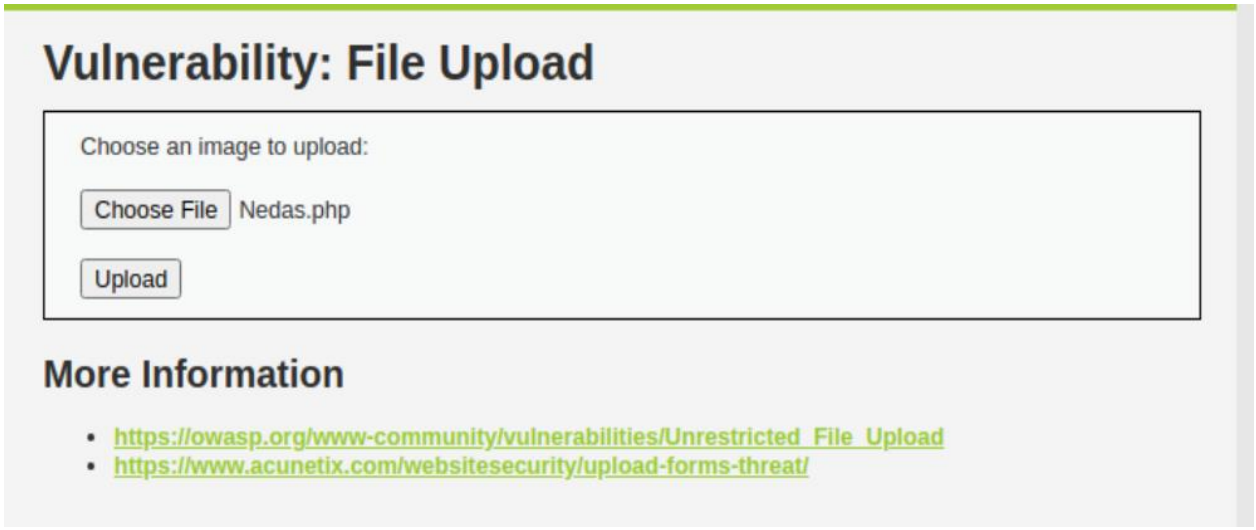
failas yra užkraunamas ir įvykdomas, jame esantis kodas (Failo sėkmingas atvaizdavimas pav. 7).



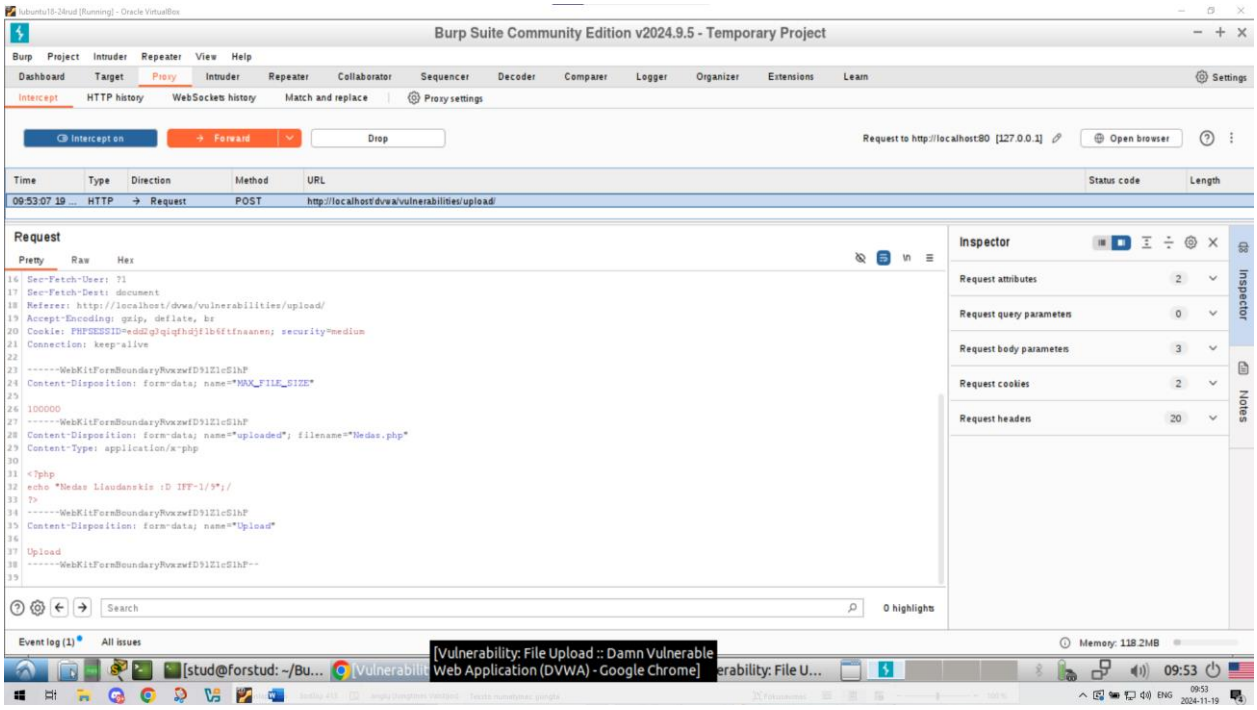
Burp Suite pav. 1



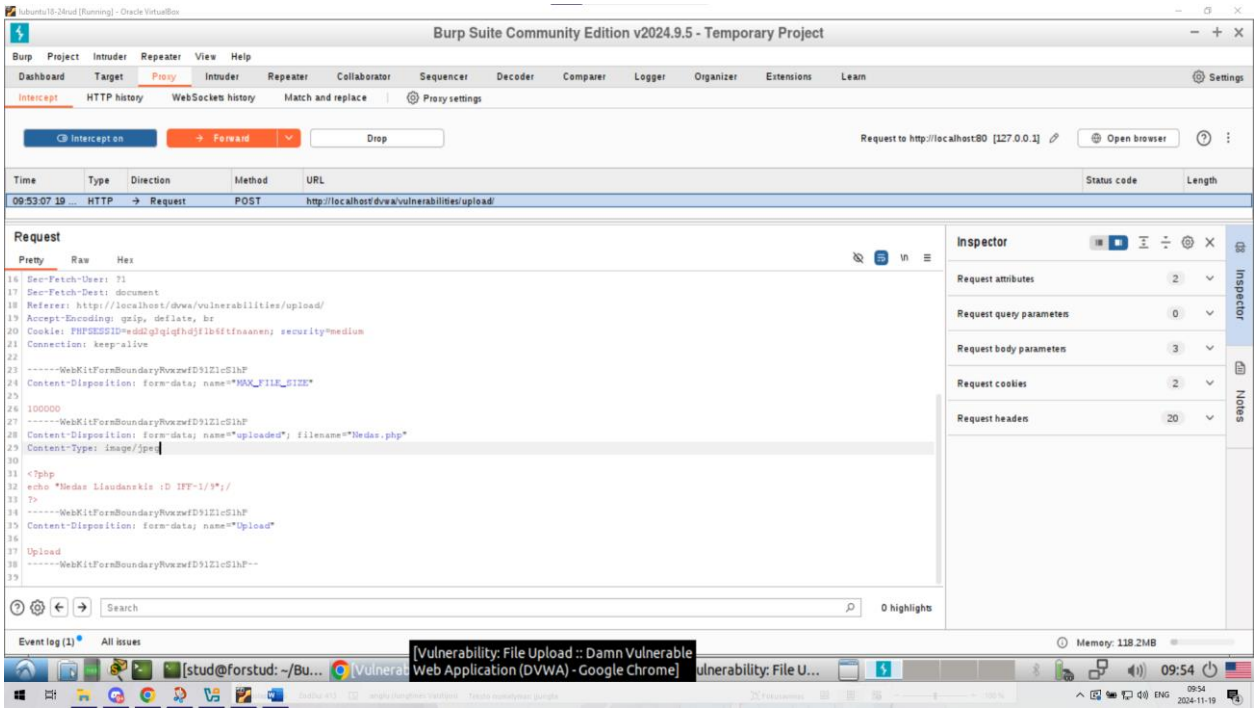
Nedas.php pav. 2



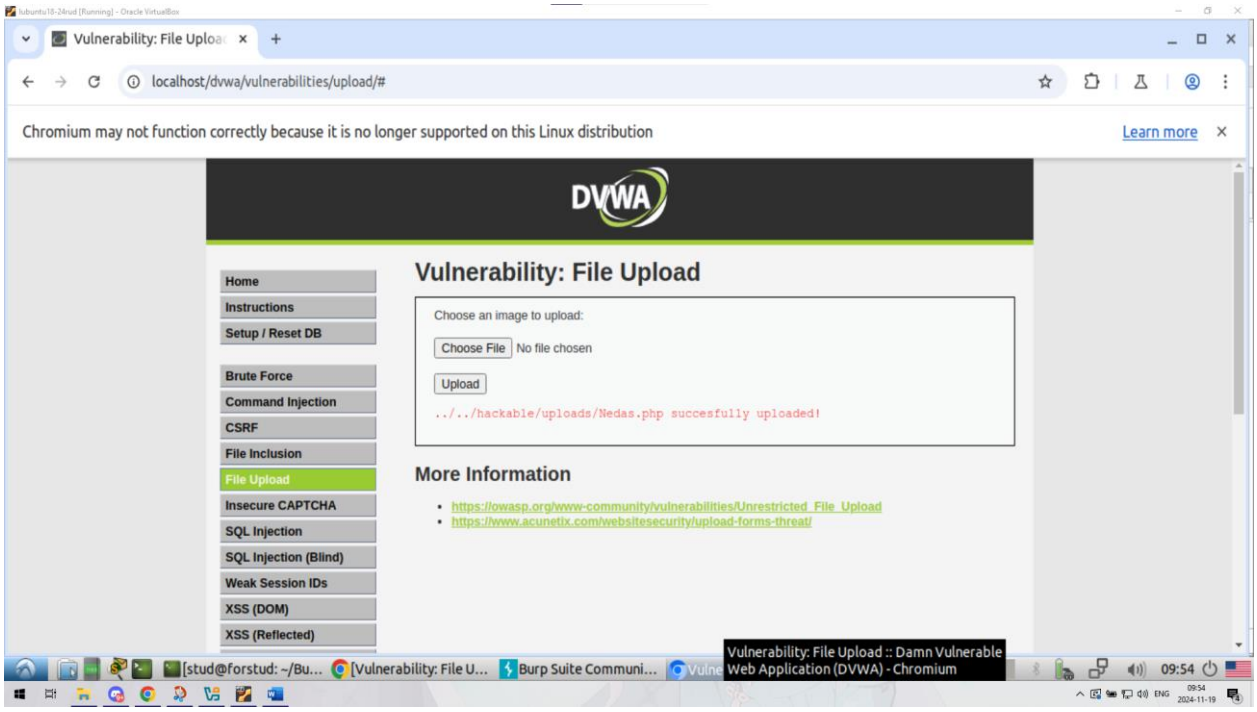
Įkeliamas Nedas.php failas pav. 3



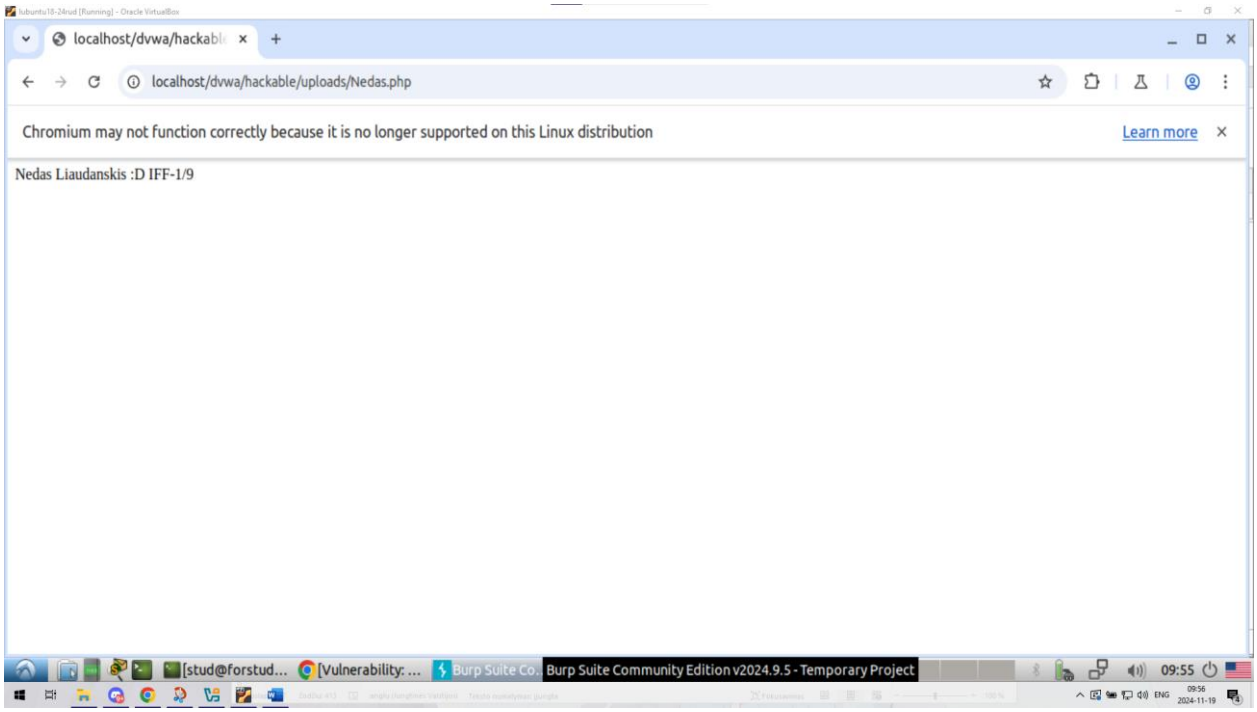
Užklausa, prieš pakeitimus pav. 4



Užklausa po pakeitimų pav. 5



Failas sėkmingai įkeltas pav. 6



Failo sėkmingas atvaizdavimas pav. 7

Failų įterpimo ataka

Darbas atliekamas DVWA sistemos ***File inclusion*** skiltyje.

Šis puslapis suformuojamas įterpiant serveryje esantį include.php failą. Jūsų tikslias priversti serverį įvykdyti jūsų pasirinktą PHP kodą. Kaip įrodymą serveris privalo išspausdinti jūsų vardą ir pavardę. Šiai užduočiai atlikti negalima naudototis 2.2 užduotyje įkeltais failais.

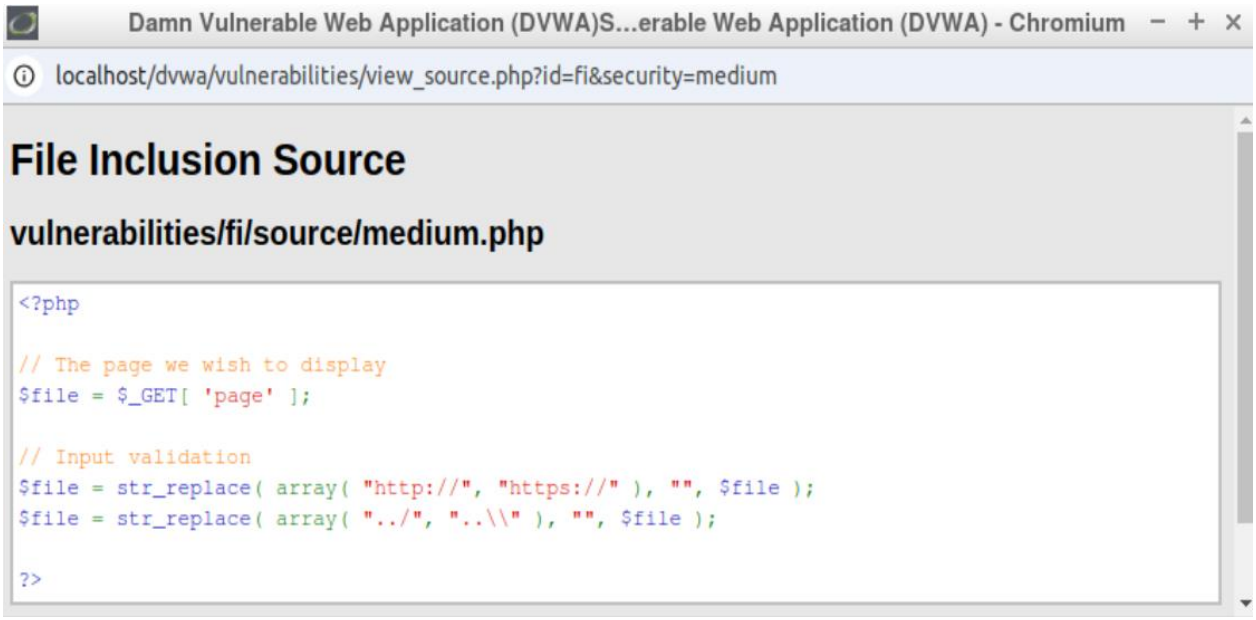
Ataskaitoje aprašykite veiksmus kuriuos atlikote, šiai užduočiai pasiekti.

Atlikta ataka:

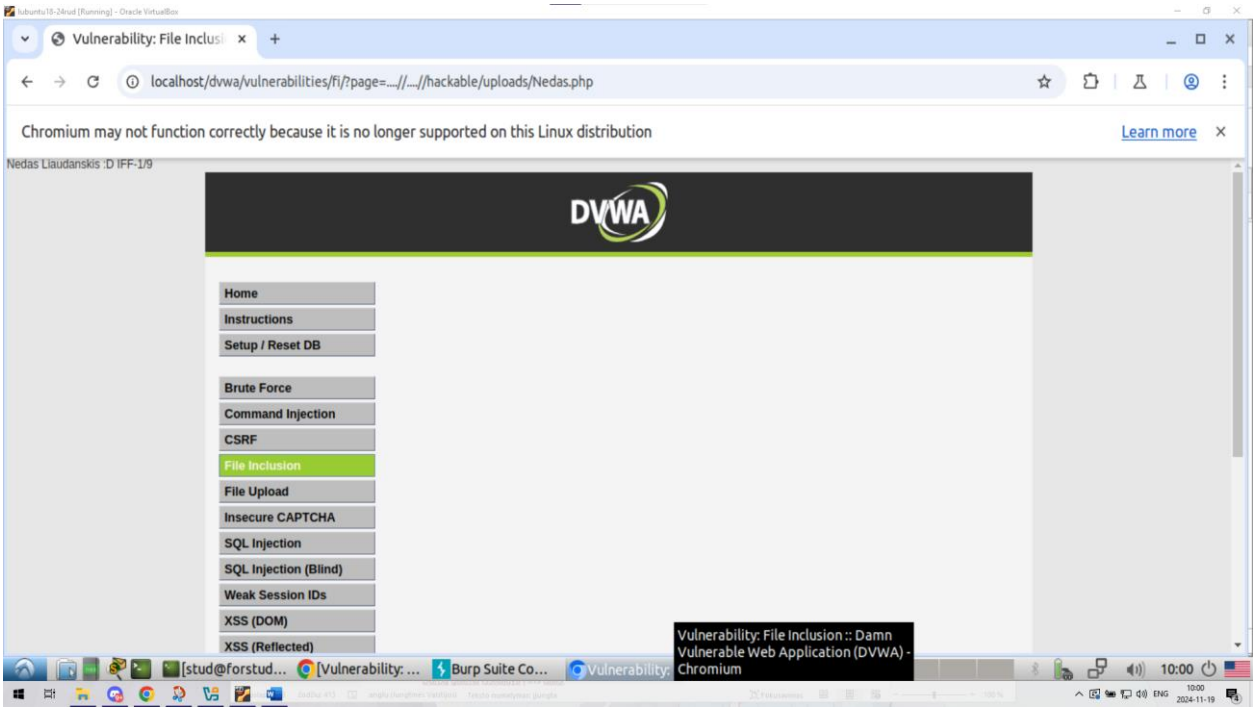
Šioje laboratorinio dalyje, reikia vietoj index.php užkrauti kitokį failą, tačiau navigacijai trukdo tai, jog visi (http://) (https://) ir (../) (..\\) simboliai yra pakeičiami tuščiais (Kodas, neleidžiantis naviguoti po sistemą pav. 8). Taigi reikėjo surasti kitokį būdą naviguoti po sistemą. Būdas, kurį aš naudojau buvo vietoj (../) panaudoti (....//) tokiu būdų vidinė šio simbolio dalis:

(..../)

Būtų panaikinta ir liktu tik (../). Likusi dalis yra komanda, kurios dėka galime naviguoti sistema ir užkrauti norimus failus. Tą ir padariau. Užkroviau savo Nedas.php failą (Užkrautas Nedas.php failas pav. 9).



Kodas, neleidžiantis naviguoti po sistemą pav. 8



Užkrautas Nedas.php failas pav. 9

Komandų injekcijos ataka

Darbas atliekamas DVWA sistemos ***Command execution*** skiltyje.

Darbas susideda iš dviejų etapų. Pirmojo etapo tikslas priversti sistemos interpretatorių vykdyti jūsų komandas. Kaip įrodymą turite suformuoti užklausą kurioje būtų vykdoma sistemos interpretatoriaus komanda ***echo*** ir į puslapį būtų išvedmas jūsų vardas ir pavardė.

Antrojo etapo tikslas panaudojant sistemos interpreatatorių priversti serverį vykdyti jūsų nurodytą PHP kodą. Kaip įrodymą PHP kodas turi išspausdinti jūsų vardą ir pavardę.

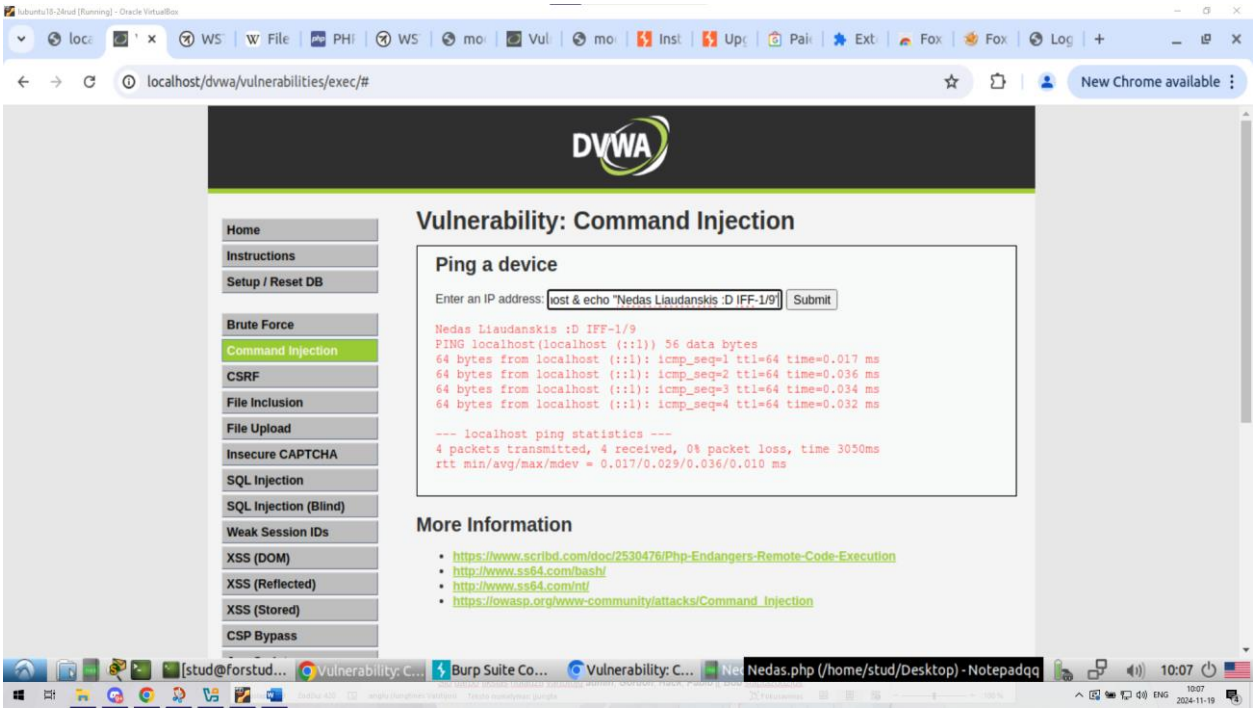
Ataskaitoje aprašykite veiksmus kuriuos atlikote, šiai užduočiai pasiekti.

Atlikta ataka:

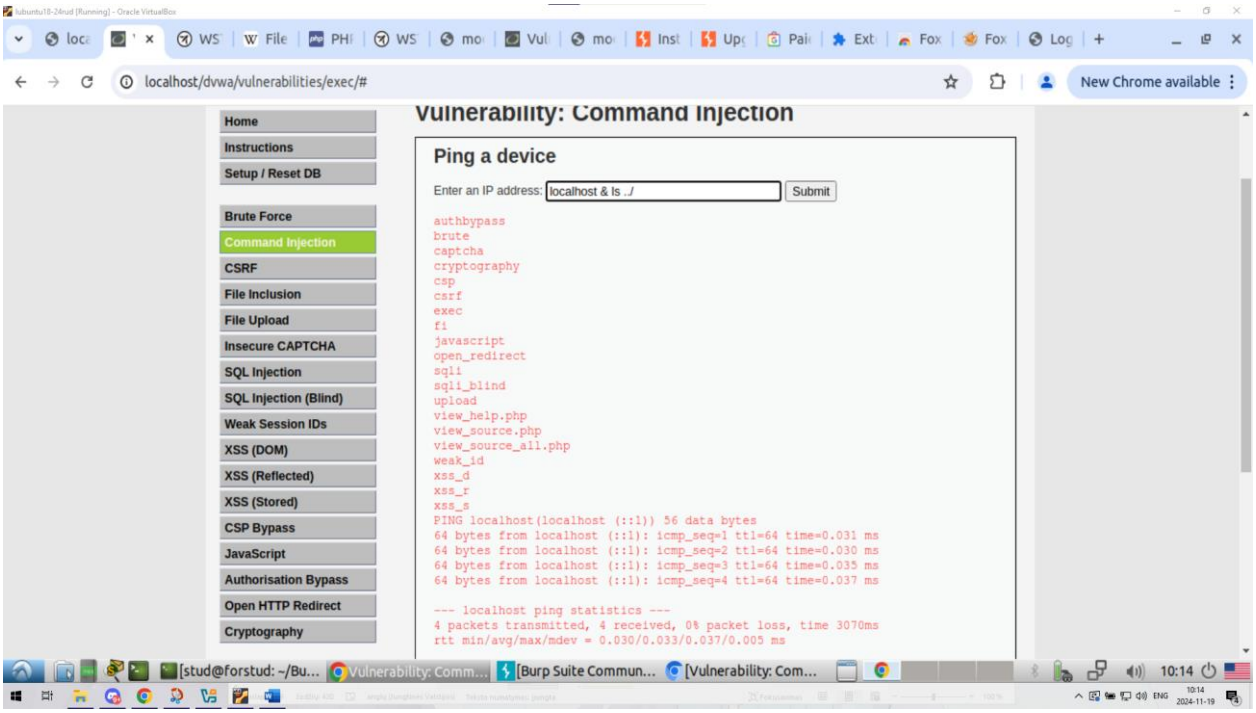
Kaip ir antroje užduotyje ši užduotis, tam tikras rašytas komandas panaikina ((&&) ir (||)). Tačiau tai yra tik dvi komandos. Norint atlikti šią dalį pasinaudojau & ženklu, kuris leidžia atlikti sekančia komandą tuo pačiu metu kaip atliekama pirma komanda. Taigi pridėjus šį ženklą, buvo gan lengva naudojant injekcija atlikti papildomas komandas.

Pirmiausiai išrašiau savo vardą, pavardę ir grupę, naudojant tokią komandą: localhost & echo "Nedas Liaudanskis :D IFF-1/9" (Paprastos komandos injekcija pav. 10).

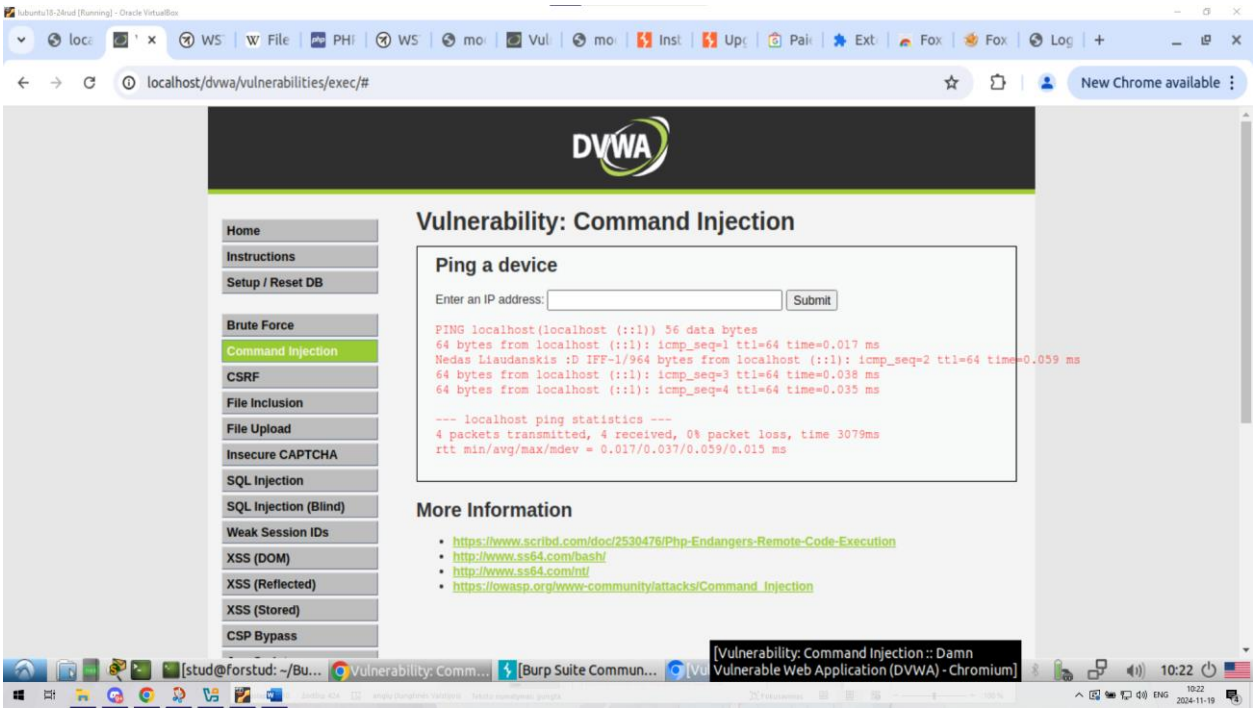
Antrame etape panaudojau localhost & ls ../ komandą, kuri padėjo sužinoti sistemos struktūrą (Sistemos stukrūtos atvaizavimas komadinės injekcijos būdu pav. 11). Žinodamas struktūrą sugebėjau gauto prieigą prie mano įkelto Nedas.php failo, kurį paleidau naudojant paprasčiausią komandą: localhost & php ../../hackable/uploads/Nedas.php. (Nedas.php failo paleidimas, naudojant komandinę injekciją pav. 12)



Paprastos komandos injekcija pav. 10



Sistemos stukrūtos atvaizavimas komadinės injekcijos būdu pav. 11



Nedas.php failo paleidimas, naudojant komandinę injekciją pav. 12

SQL injekcijos ataka

Darbas atliekamas DVWA sistemos ***SQL injection*** skiltyje.

Šio darbo tikslas nulaužti vartotojų ***admin***, ***Gordon***, ***Hack***, ***Pablo*** ir ***Bob*** slaptažodžius. Darbą galima išskaidyti į tris dalis:

1. Priversti serverį atskleisti duomenų bazės lentelių struktūrą
2. Priversti serverį išspausdinti visų vartotojų slaptažodžių hešus
3. Išversti heš funkcijų reikšmes ir gauti slaptažodžius

Ataskaitoje aprašykite veiksmus kuriuos atlikote, šiai užduočiai pasiekti.

Atlikta ataka:

Pirma dalis buvo atskleisti lentelės struktūrą. Norint gauti lentelių struktūra, reikia gauti lentelių pavadinimus. Tam padaryti panaudojau šią komandą: 1 or 1=1 UNION SELECT null, table_name FROM information_schema.tables #
Tokia komanda, atlieka UNION SELECT null, table_name FROM information_schema.tables # komandos dalį visada, nes 1=1 visada tiesa. Atlikus komandą, gavau lentelių pavadinimus.

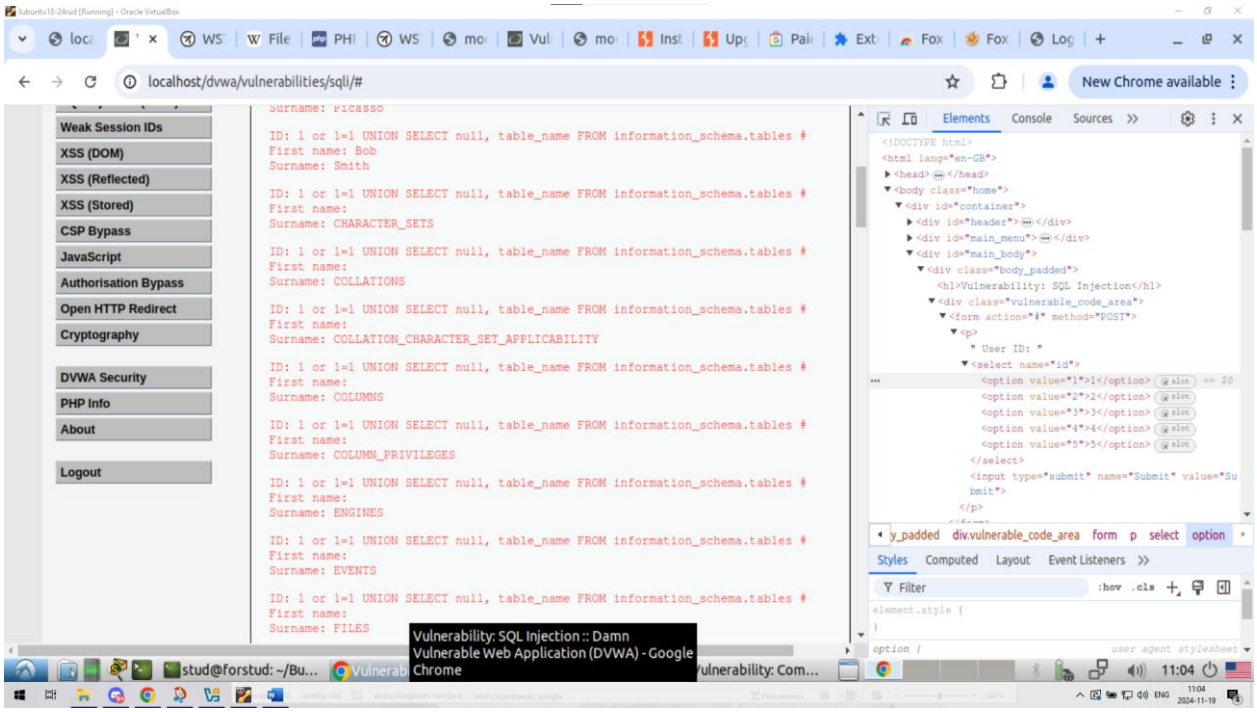
Sekantis žingsnis būtų gauti stulpelių pavadinimus. Šiam žingsniui padaryti naudojau šitą, komandą: ‘ or 1=1 union select null, concat(table_name,0x0a,column_name) from information_schema.columns where table_name = 'users'. (Gauti stulpelių pavadinimai pav. 14)

Antra dalis buvo gauti naudotojų slaptažodžius. Šiai daliai atlikti naudojau tokią komandą: 1 or 1=1 UNION SELECT user, password FROM users#. (Gauti slaptažodžiai pav. 15)

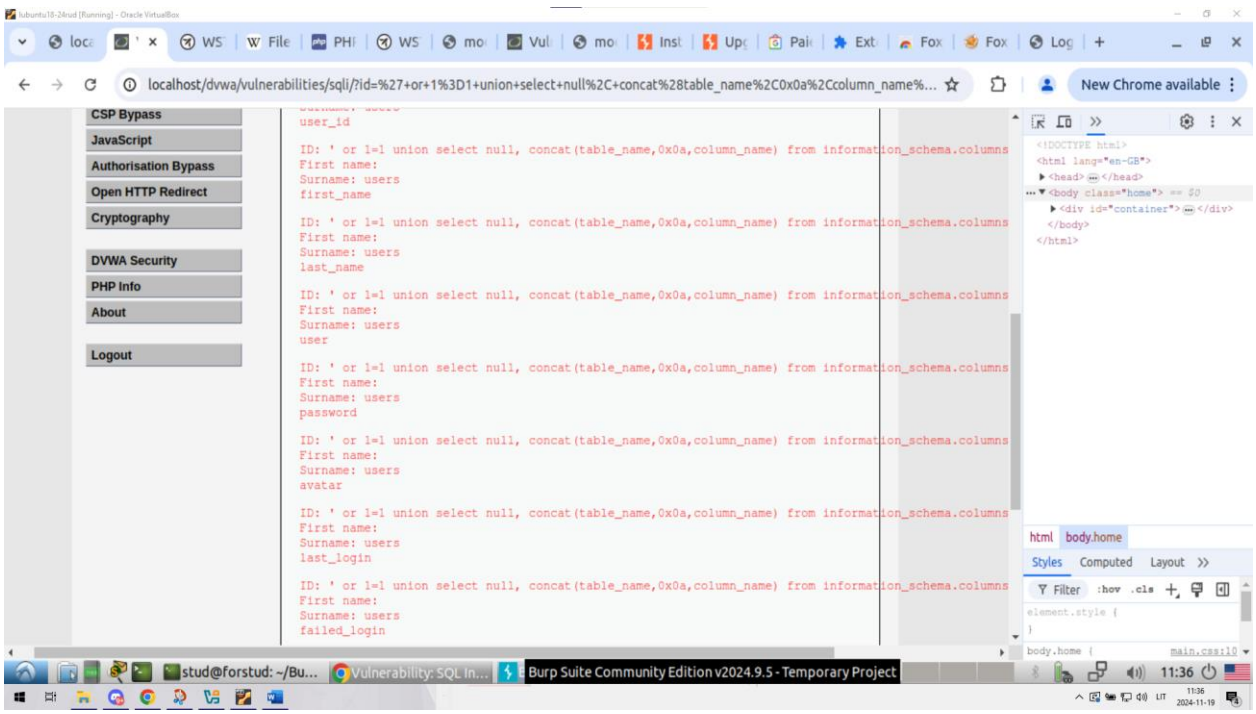
Tečia dalis buvo gautas haš funkcines reikšmes, paversti į tikrus slaptažodžius. Slaptažodžiai naudojo MD5 haš, tai buvo galima naudoti įvairius įrankius slaptažodžiui gauti. Aš panaudojau paprasčiausią internetinę svetainę: https://10015.io/tools/md5-encrypt-decrypt. (Slaptažodžių atkodavimas pav. 16)

Gauti slaptažodžiai:

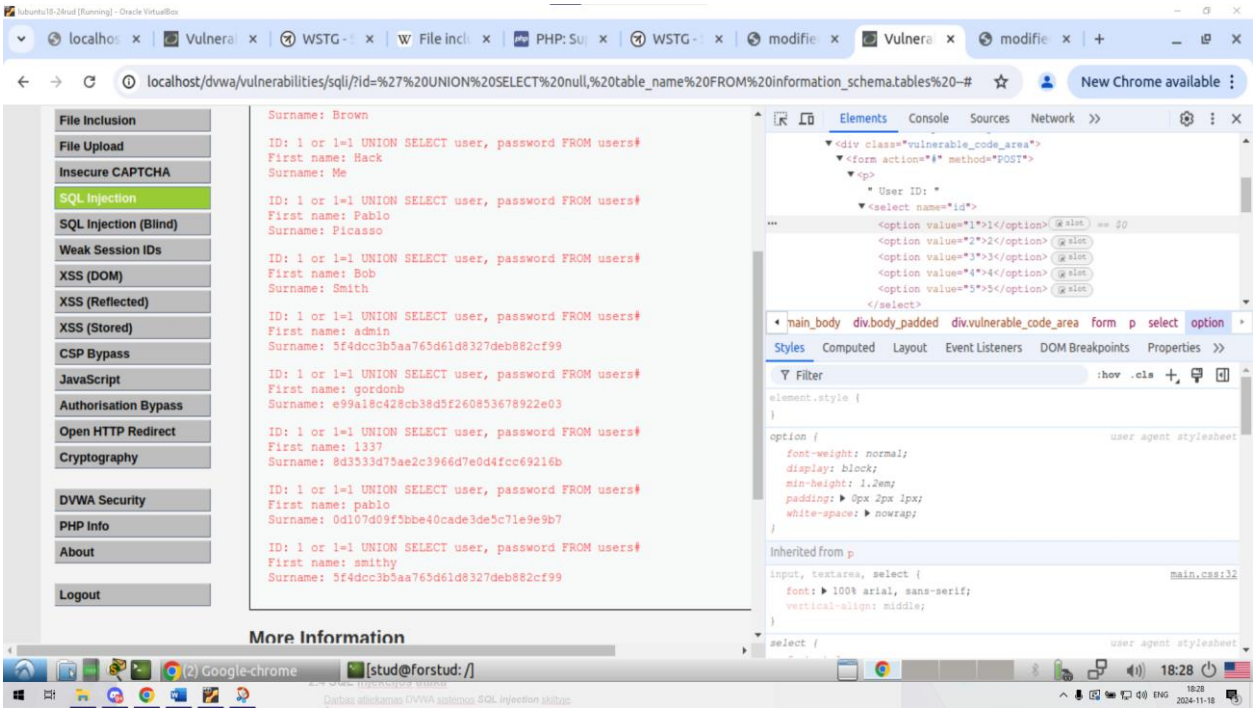
Naudotojas	Užkuoduotas slaptažodis	Slaptažodis
Admin	5f4dcc3b5aa765d61d8327deb882cf99	slaptažodis
Gordon	e99a18c428cb38d5f260853678922e03	abc123
Hack	8d3533d75ae2c3966d7e0d4fcc69216b	charley
Pablo	0d107d09f5bbe40cade3de5c71e9e9b7	letmein
Bob	5f4dcc3b5aa765d61d8327deb882cf99	slaptažodis



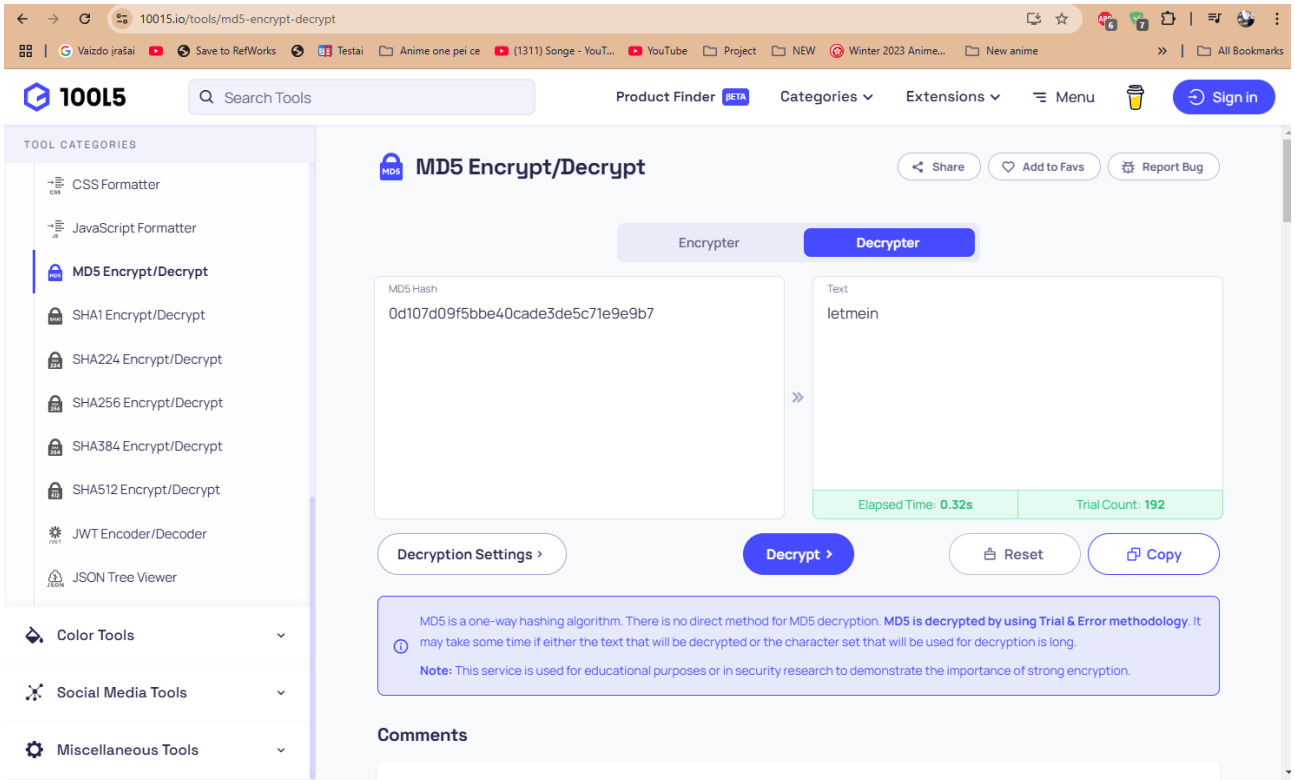
Gauti lentelių pavadinimai pav. 13



Gauti stulpelių pavadinimai pav. 14



Gauti slaptažodžiai pav. 15



Slaptažodžių atkodavimas pav. 16