

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г.
ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ
компьютерной безопасности и
криптографии

Burp Suite, атака «Человек посередине»

ОТЧЕТ ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЕННЫХ БАЗ ДАННЫХ»

студента 4 курса 431 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Сенокосова Владислава Владимировича

Преподаватель

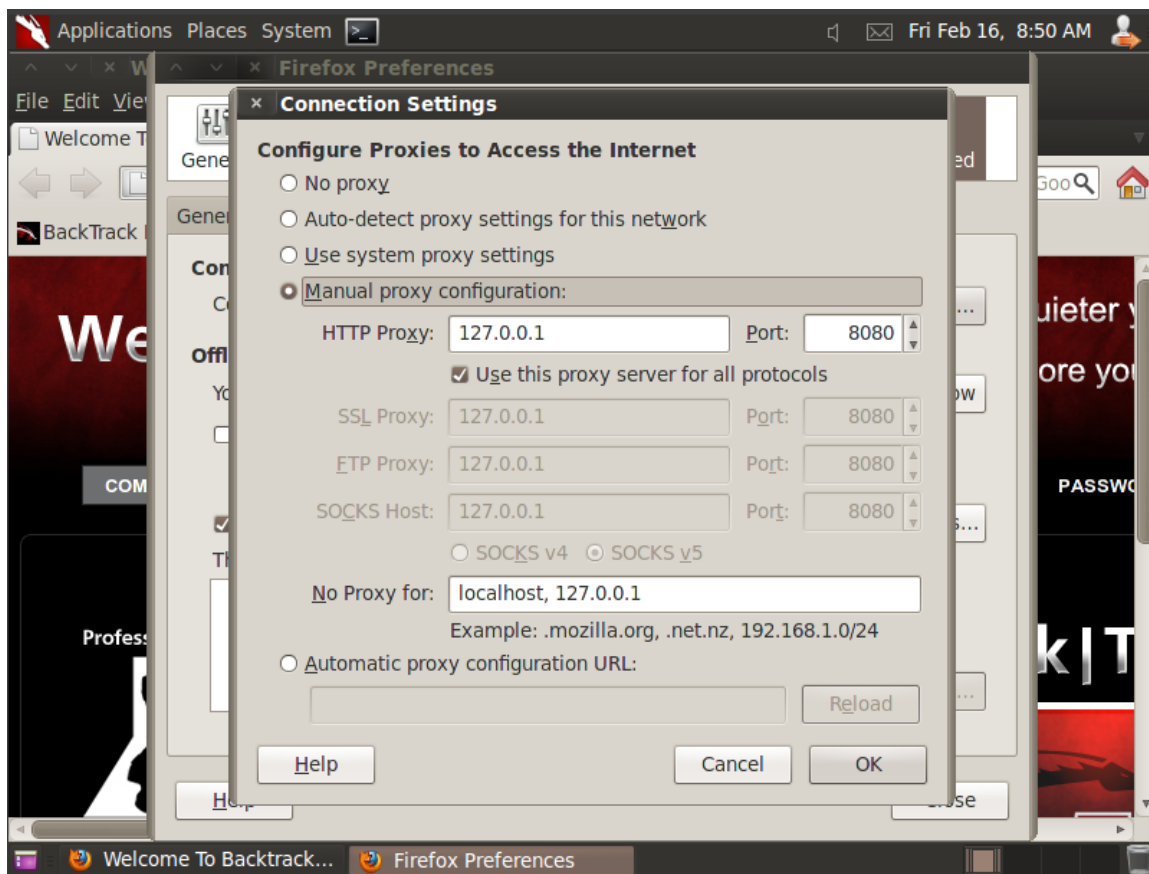
доцент, к.п.н

подпись, дата

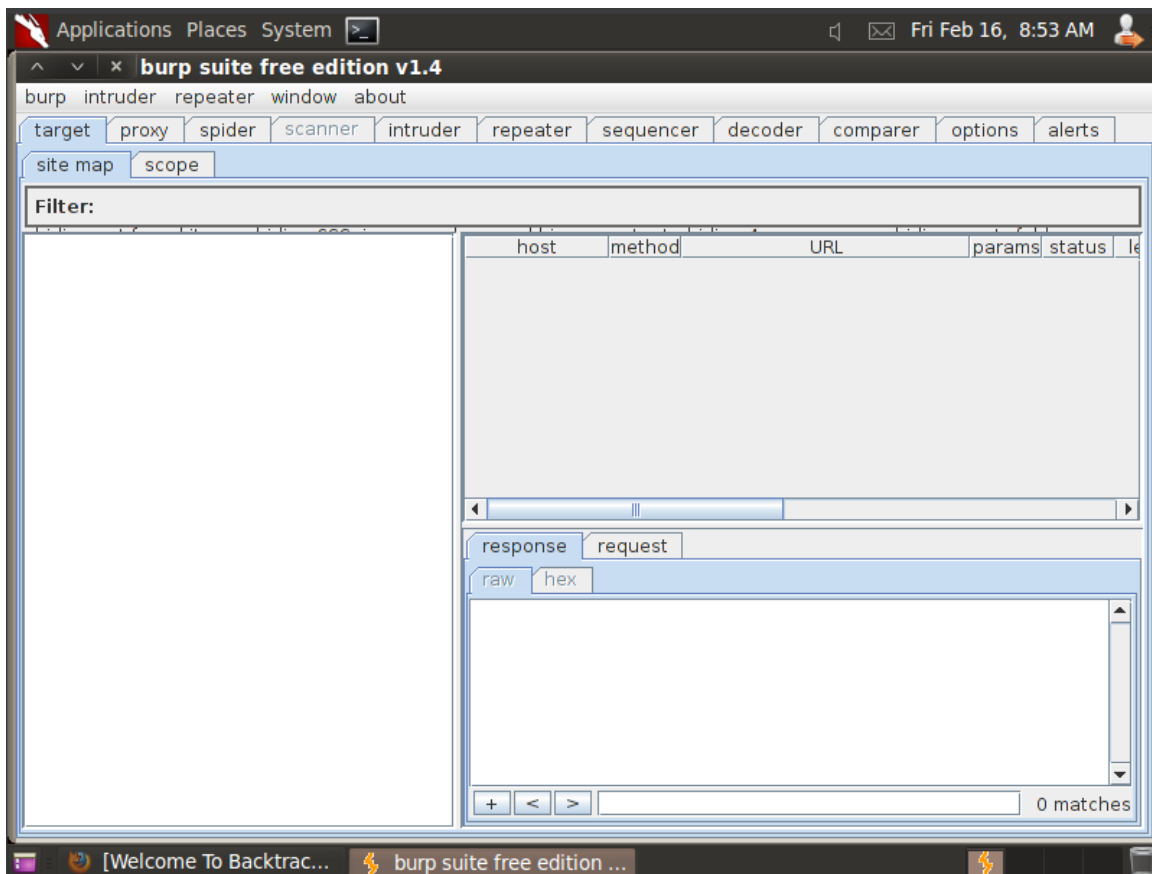
А. С. Гераськин

Саратов 2024

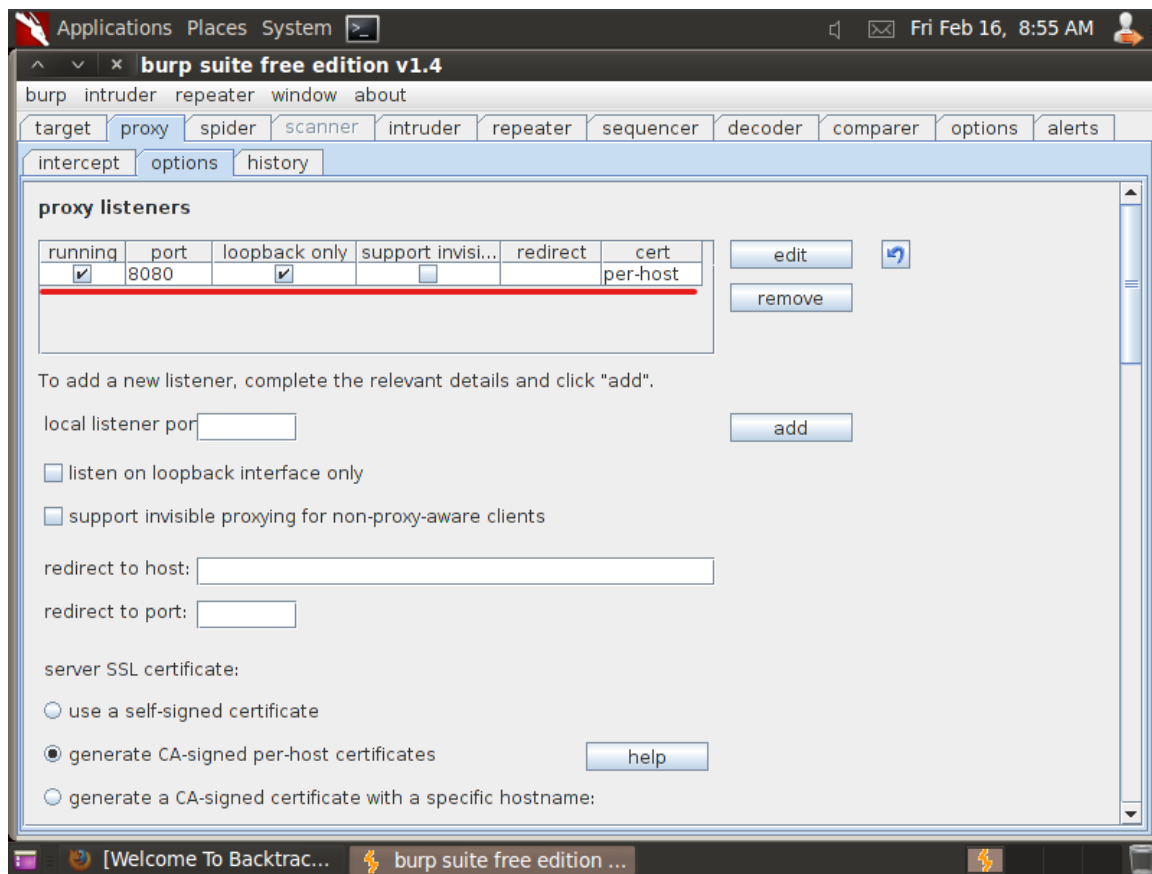
Осуществим настройку Firefox Proxy:



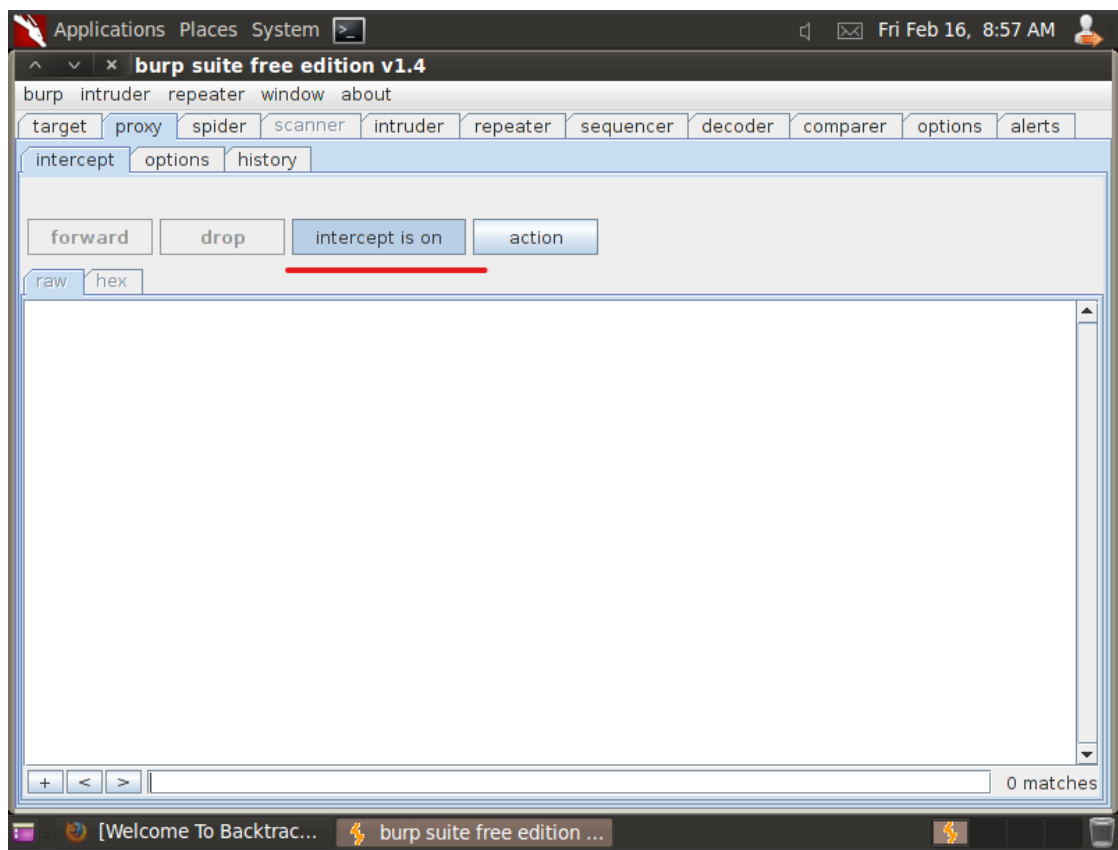
Перейдем к конфигурации Burp Suite:



Настраиваем в нем Проху:



Активируем перехват:

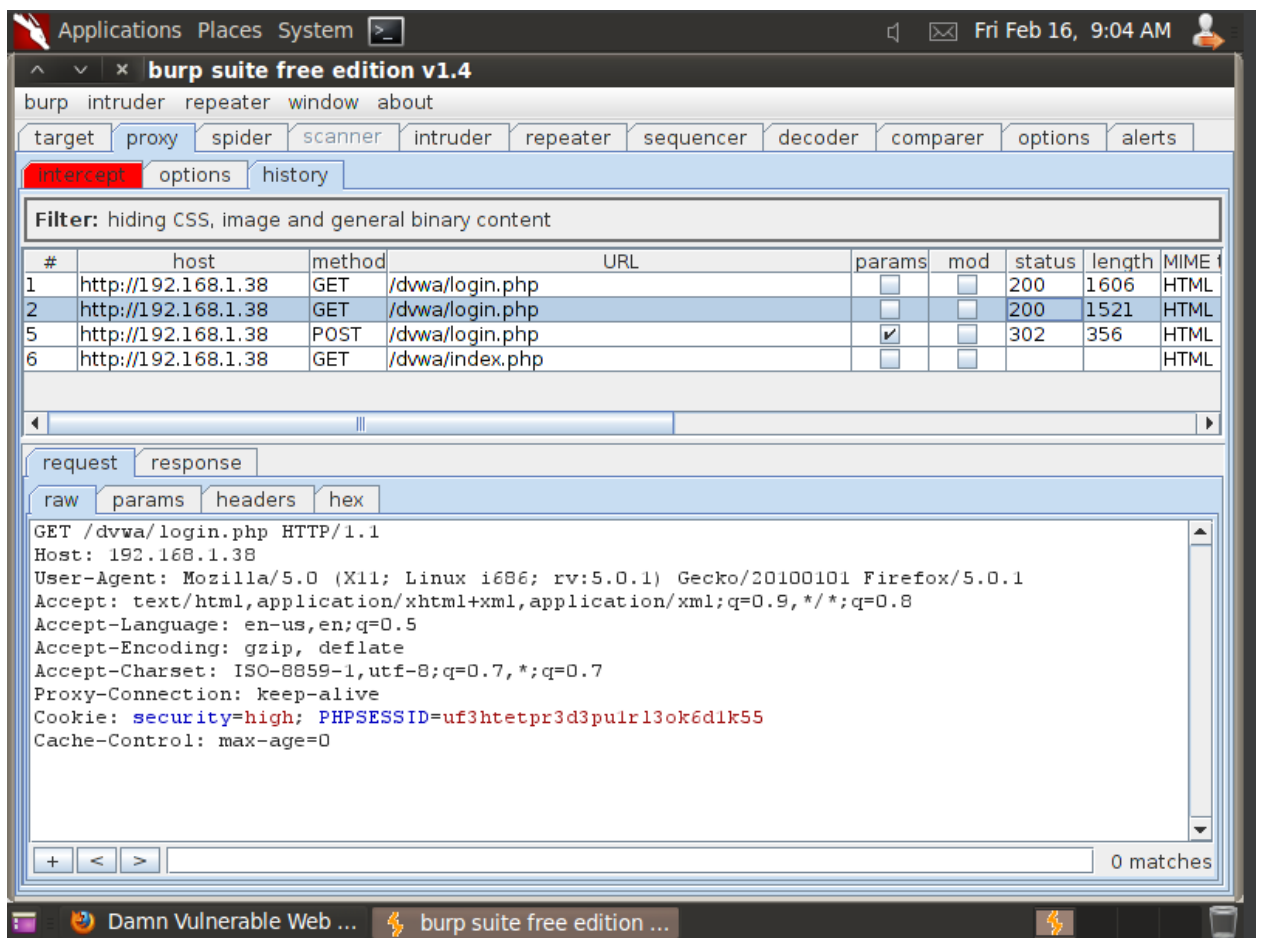
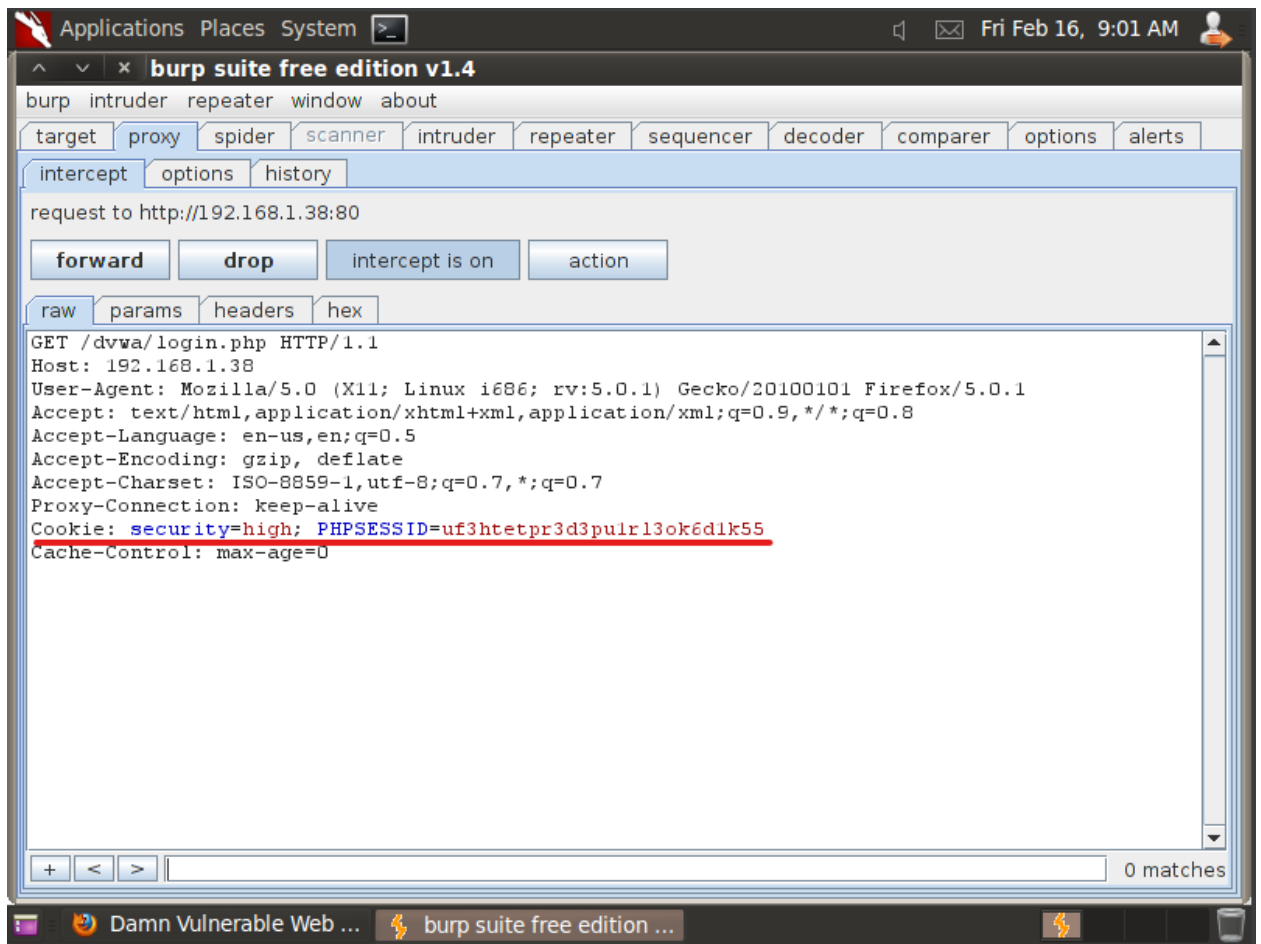


Перехват с помощью Burp Suite:

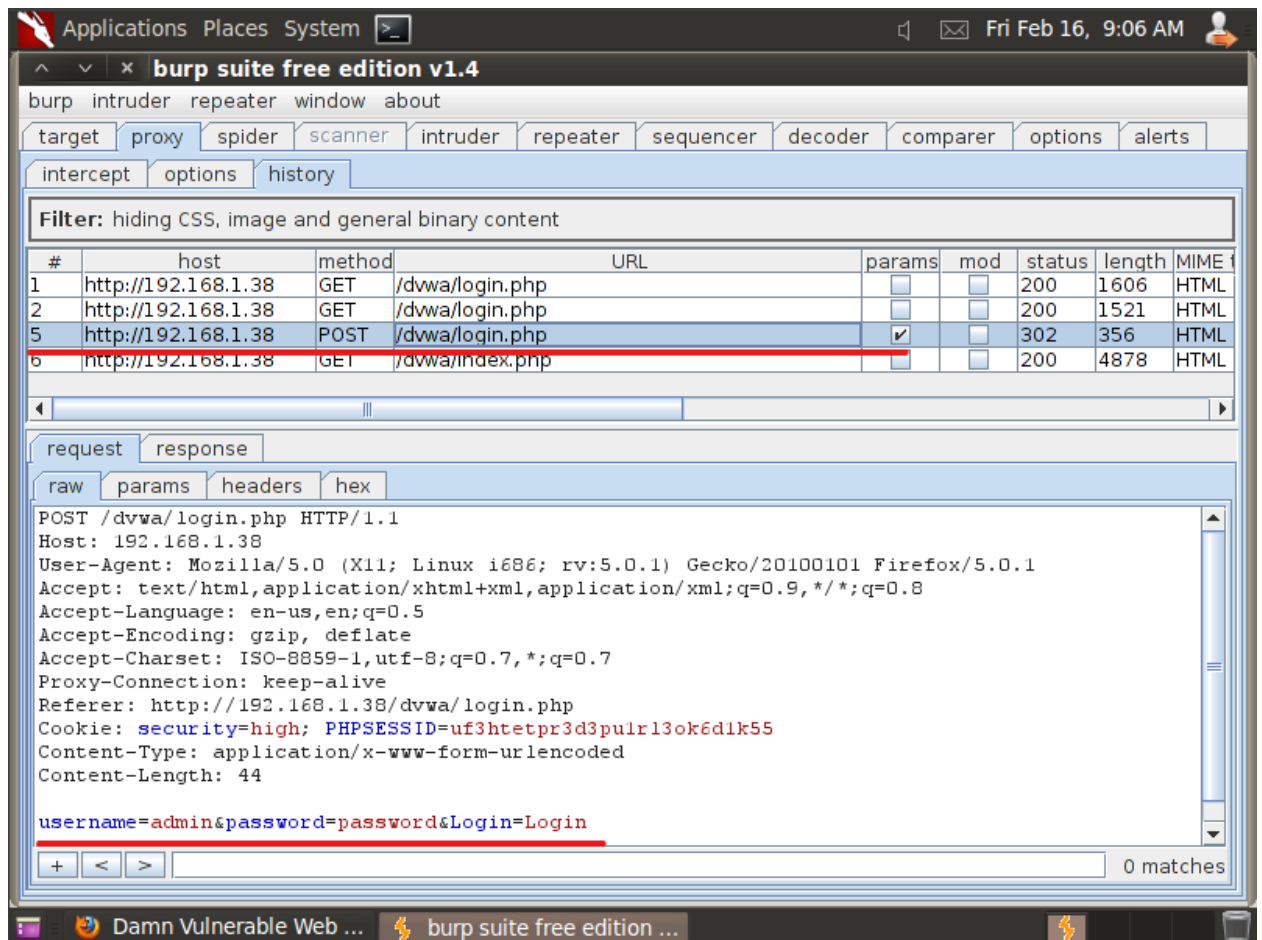
Домашняя страница DVWA не отобразится, но вы увидите сообщение о соединении.



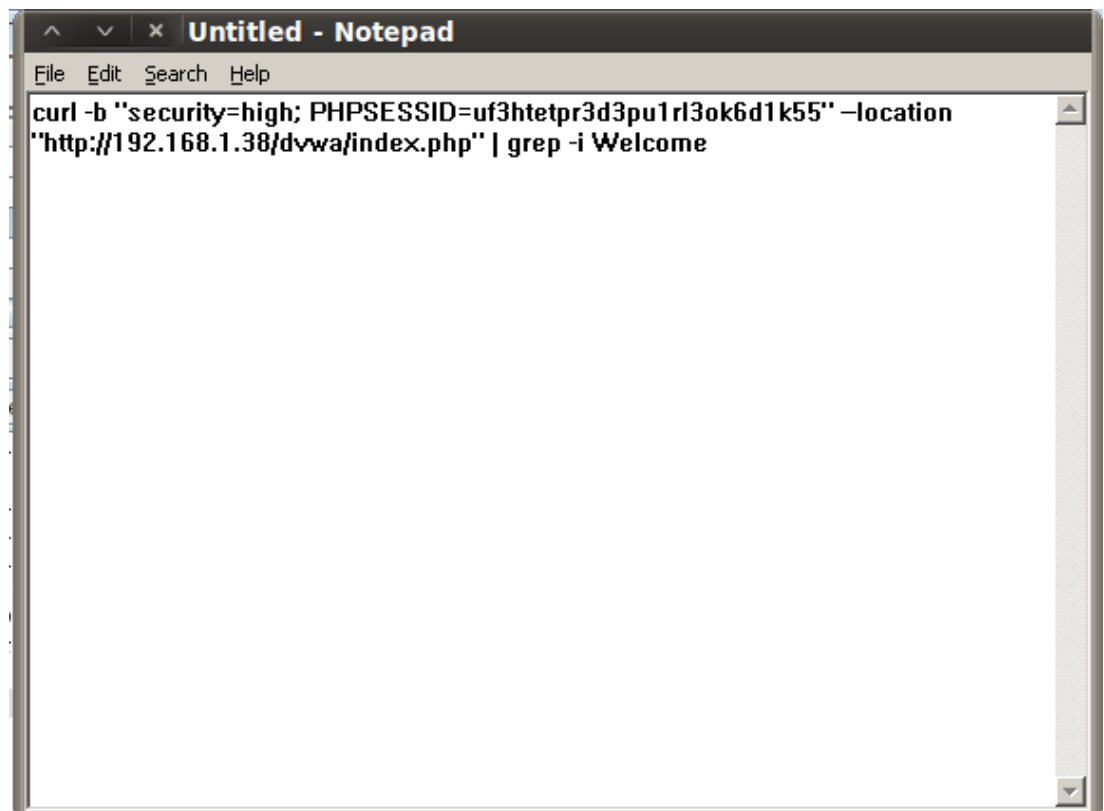
В Burp Suite нажимаем “Forward” 2 раза:



После того как произвели авторизацию:



Сохраним полученные куки и вставим их в curl-команду:

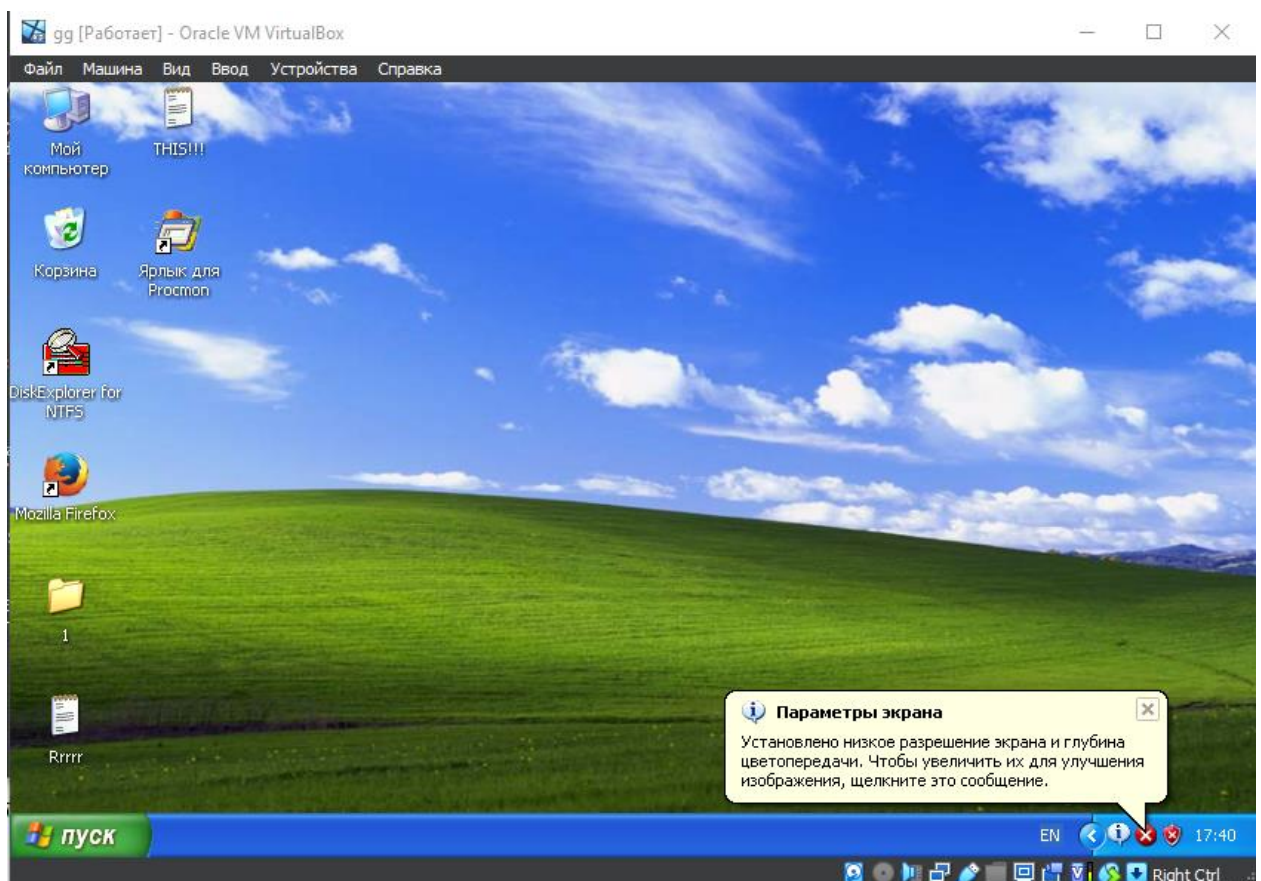


Атака человек по середине через curl:

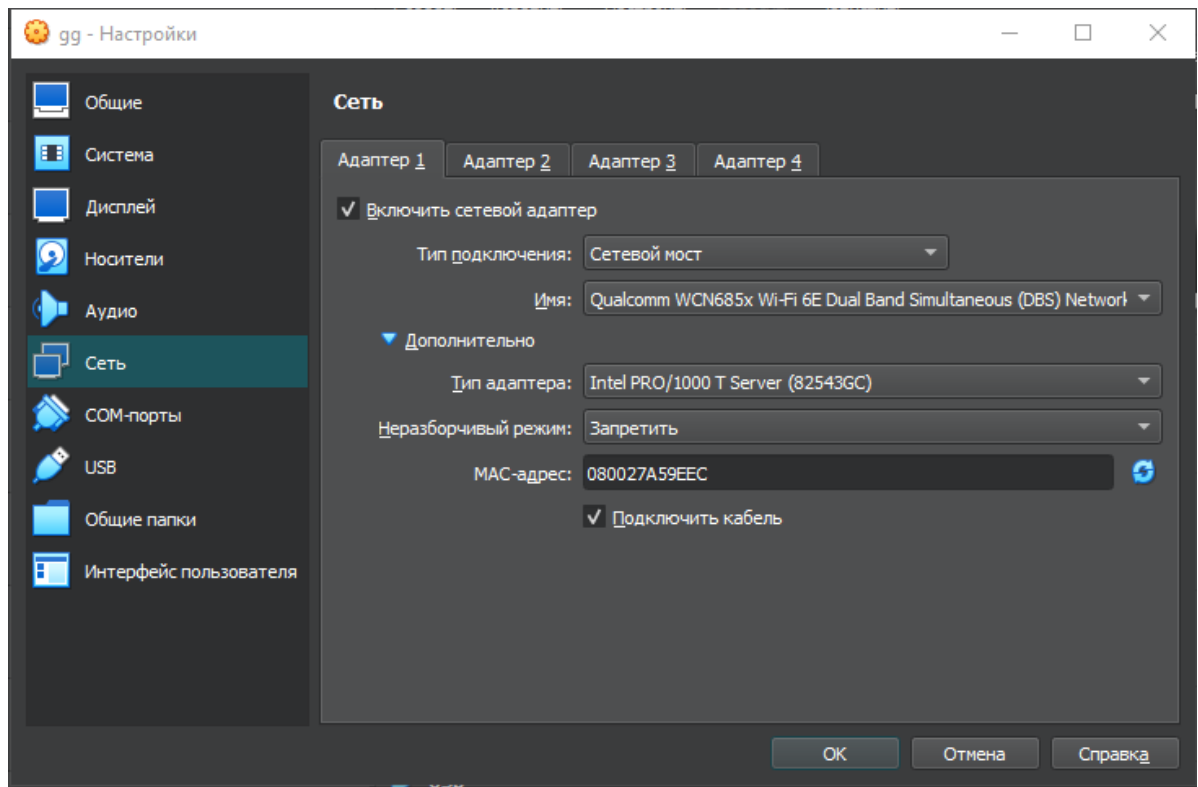
```
root@root: ~
File Edit View Terminal Help
root@root:~# curl -b "security=high; PHPSESSID=uf3htetpr3d3pu1rl3ok6d1k55" --location "http://192.168.1.38/dvwa/index.php" | grep -i Welcome
% Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
           Dload  Upload   Total     Spent    Left  Speed
102  4498  102  4498    0     0    0     0 --<title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Welcome</title>
1576k      0  --:--:--  --:--:--  --:--:-- 2196k
      <h1>Welcome to Damn Vulnerable Web App!</h1>
root@root:~#
```

Атака человек по середине через Firefox

Настроим Windows:



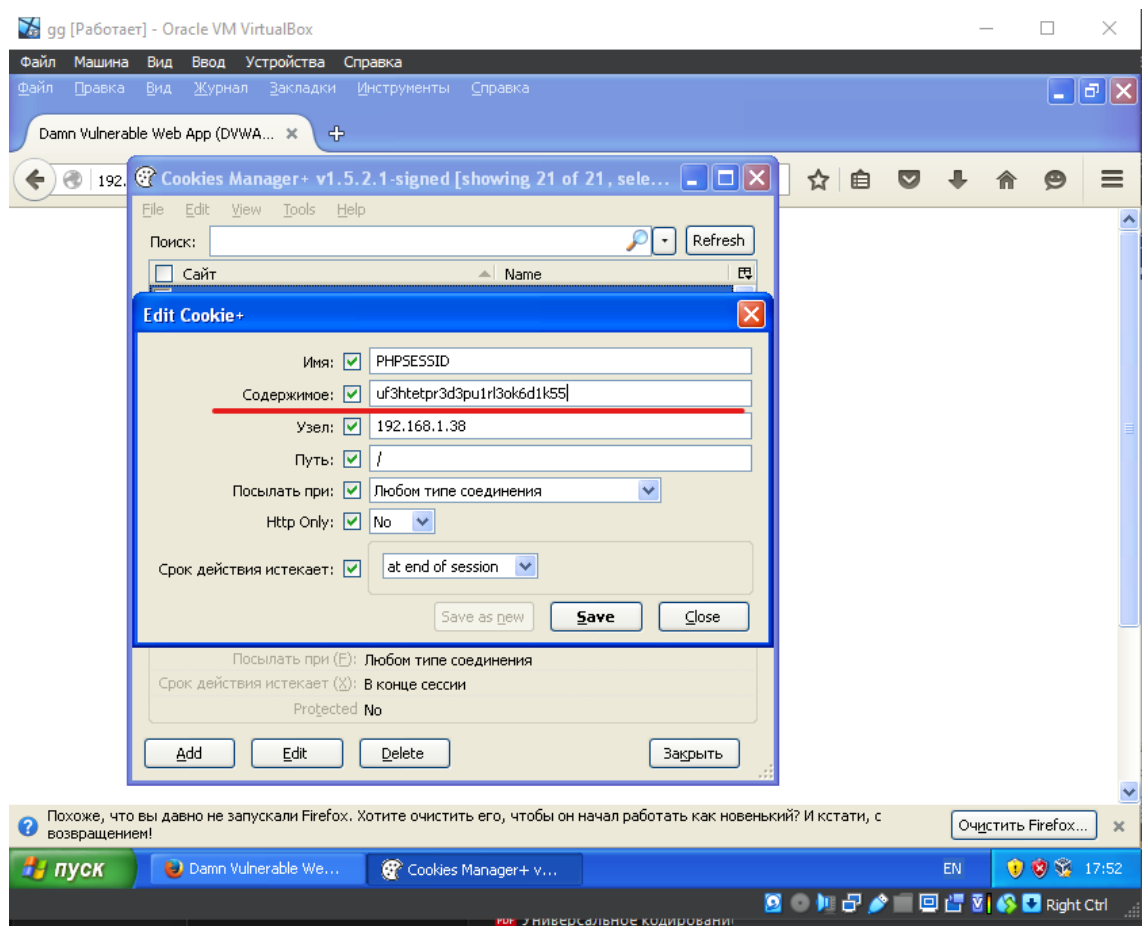
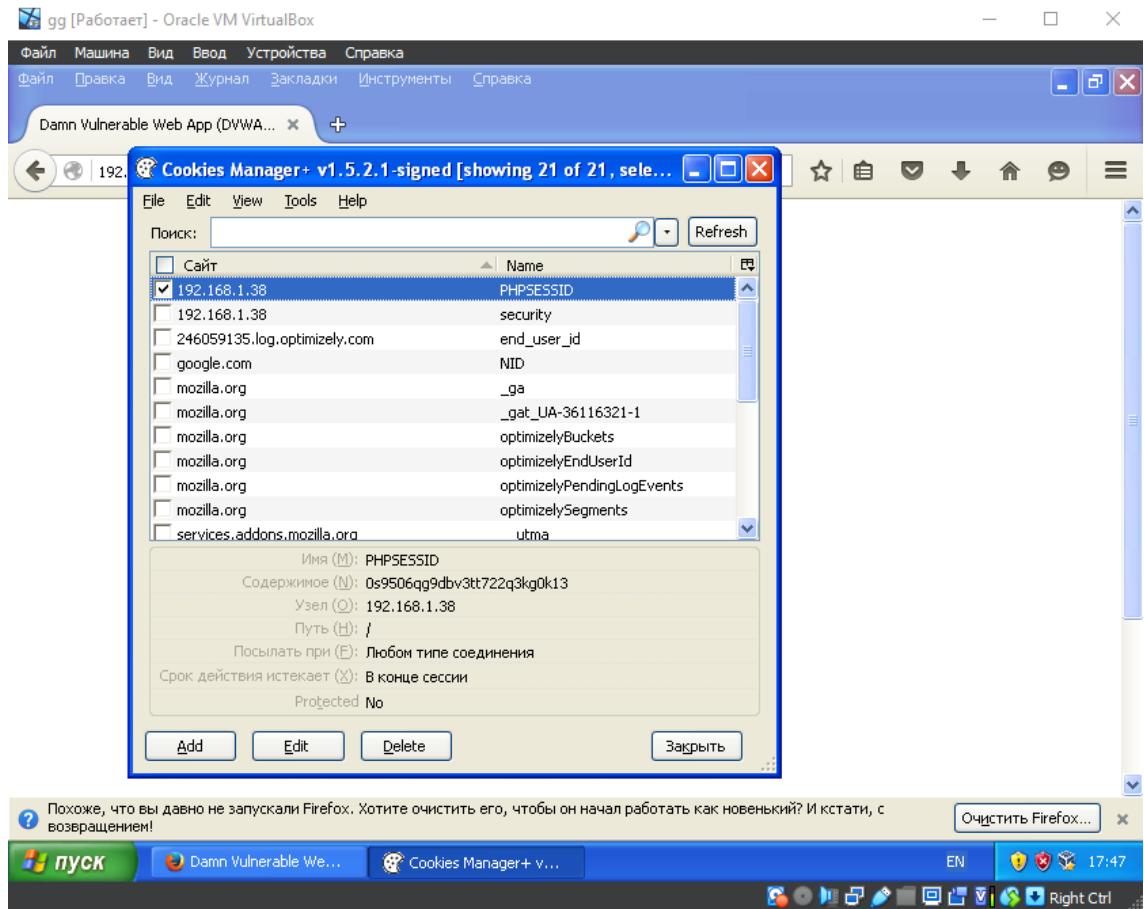
Сетевое подключение:



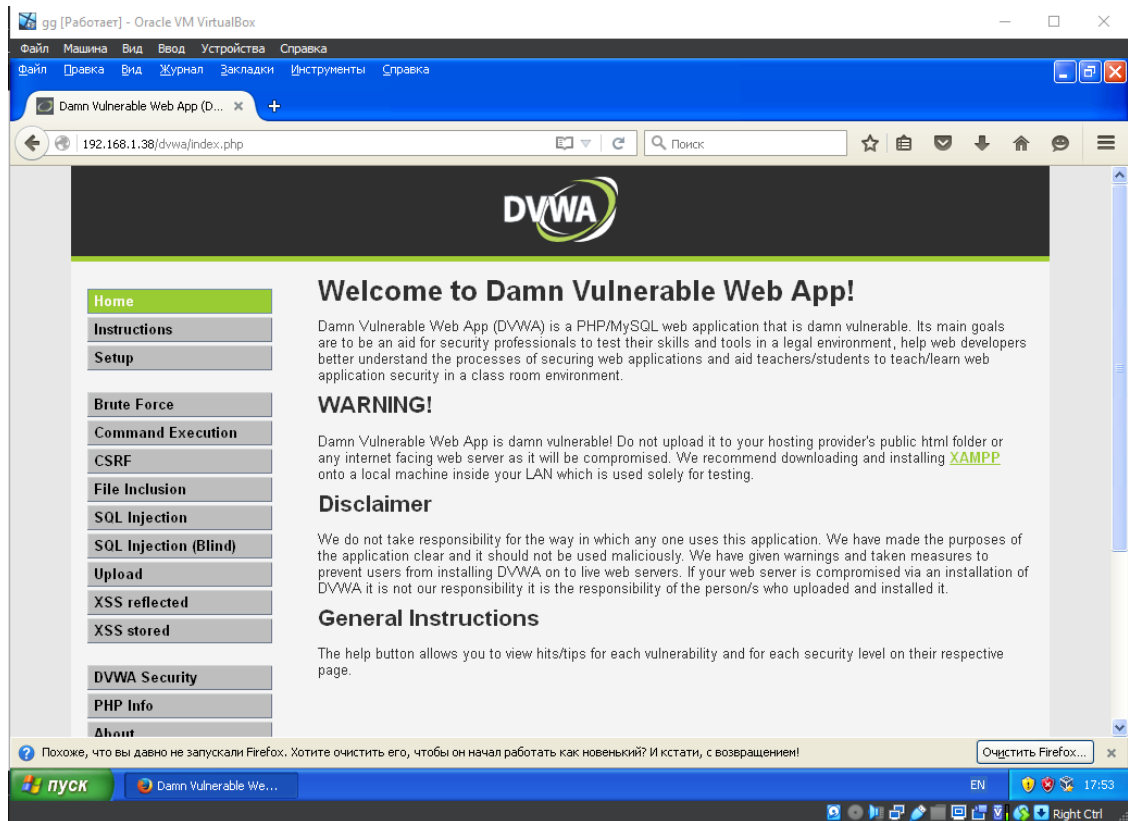
Доступ есть к сети:



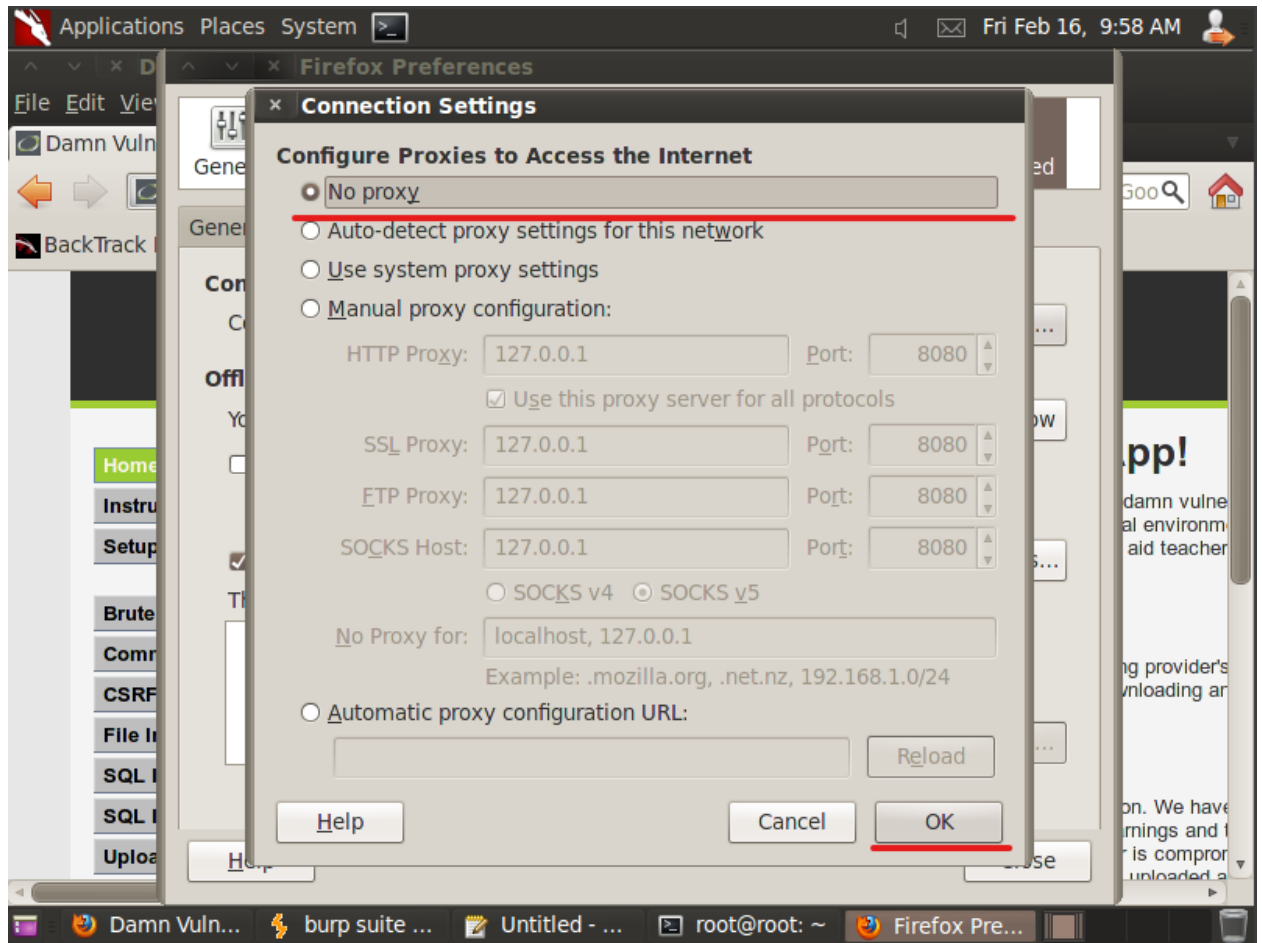
Запускаем Cookies Manager +:



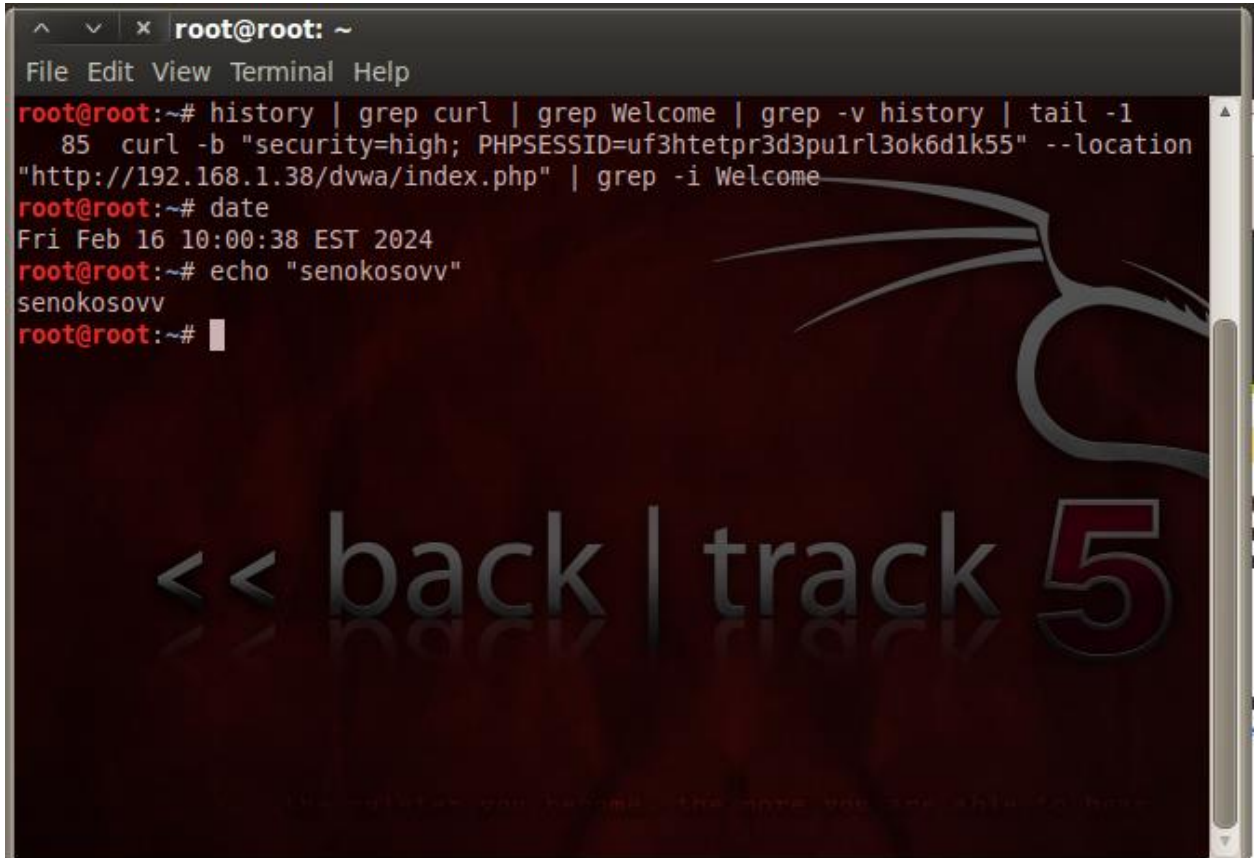
Теперь осуществим вход в систему:



Теперь удаляем проху в BackTrack:



Отчет о проделанной работе:



```
root@root: ~
File Edit View Terminal Help
root@root:~# history | grep curl | grep Welcome | grep -v history | tail -1
 85  curl -b "security=high; PHPSESSID=uf3htetpr3d3pu1rl3ok6d1k55" --location
"http://192.168.1.38/dvwa/index.php" | grep -i Welcome
root@root:~# date
Fri Feb 16 10:00:38 EST 2024
root@root:~# echo "senokosovv"
senokosovv
root@root:~#
```

<< back | track 5

The exploit was successful, the app was able to follow