

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

Базовое тестирование выполнения команд

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

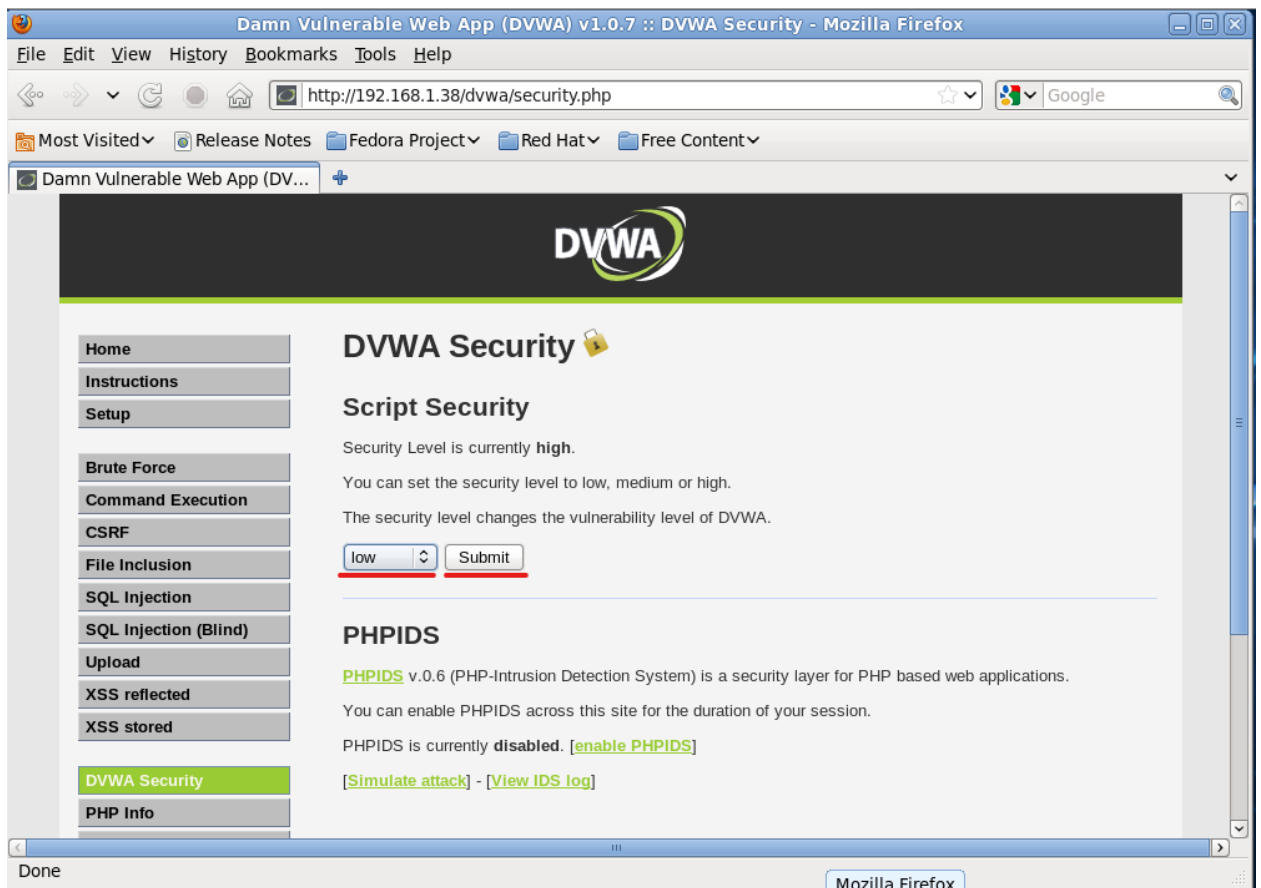
Проверяем настройки сетевого оборудования:

```
student@Fedora14:/var/www/html/dvwa/config
File Edit View Search Terminal Help
[root@Fedora14 config]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:F8:F0:E3
          inet addr:192.168.1.38  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8:f0e3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:52546 errors:0 dropped:0 overruns:0 frame:0
          TX packets:22900 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:71815579 (68.4 MiB)  TX bytes:1661472 (1.5 MiB)

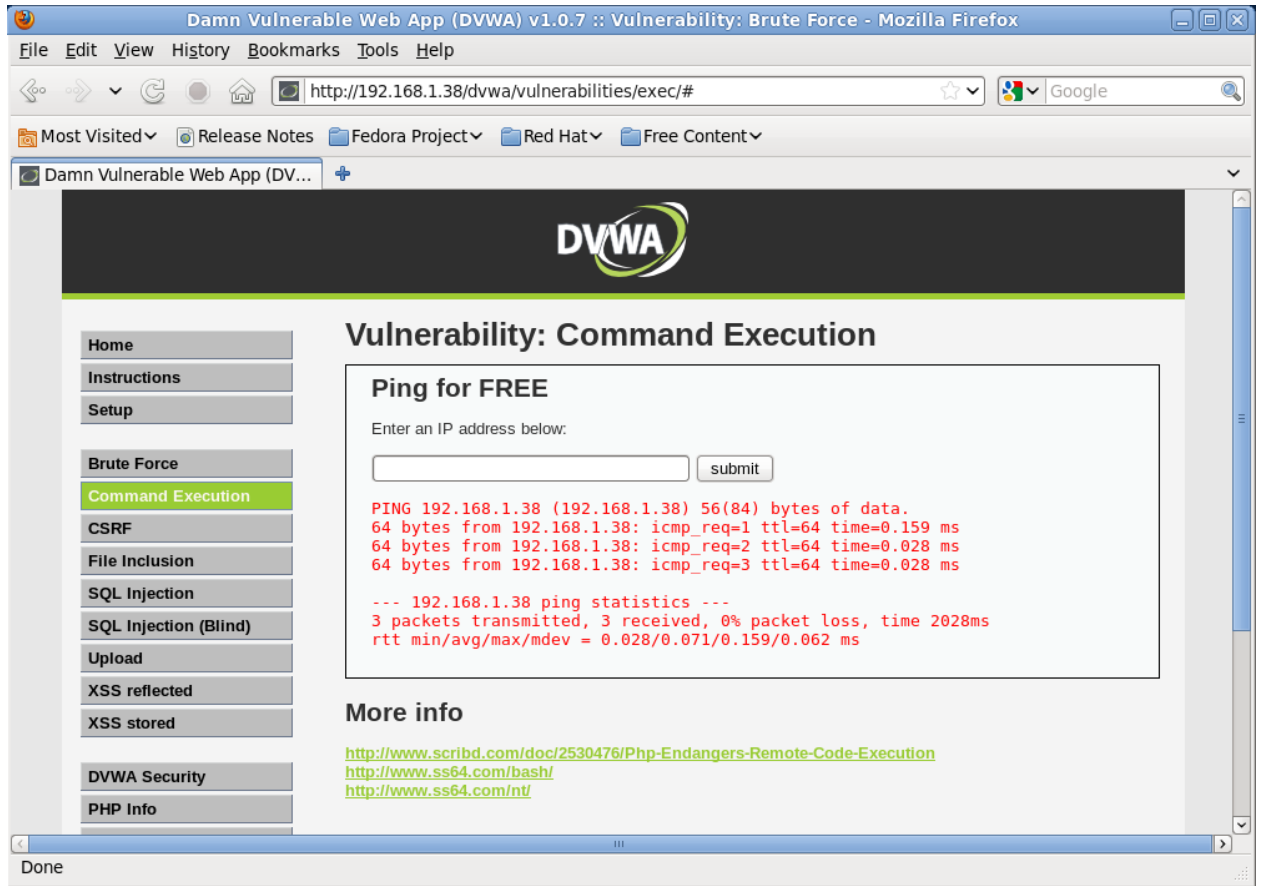
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:188 errors:0 dropped:0 overruns:0 frame:0
          TX packets:188 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:66203 (64.6 KiB)  TX bytes:66203 (64.6 KiB)

[root@Fedora14 config]#
```

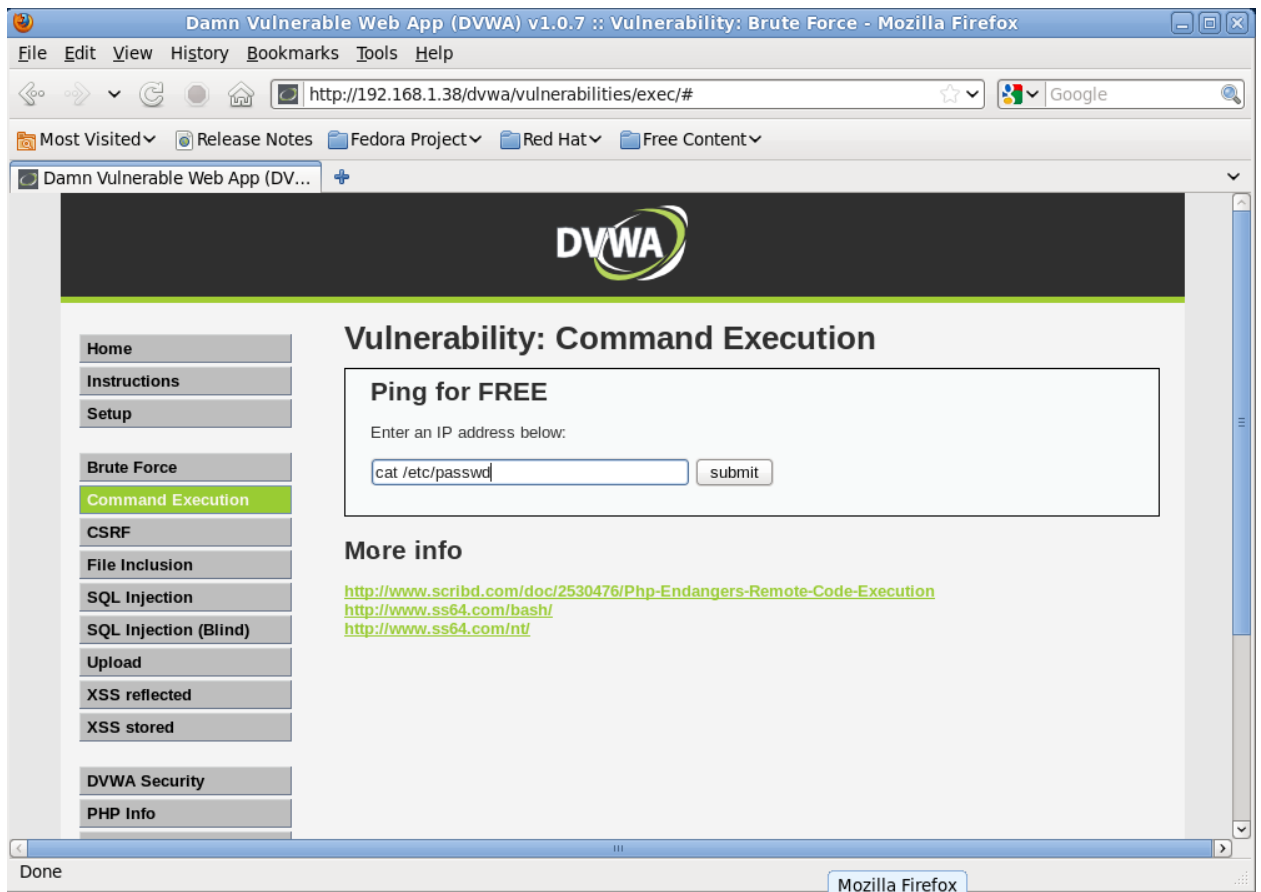
Ставим низкий уровень защиты:



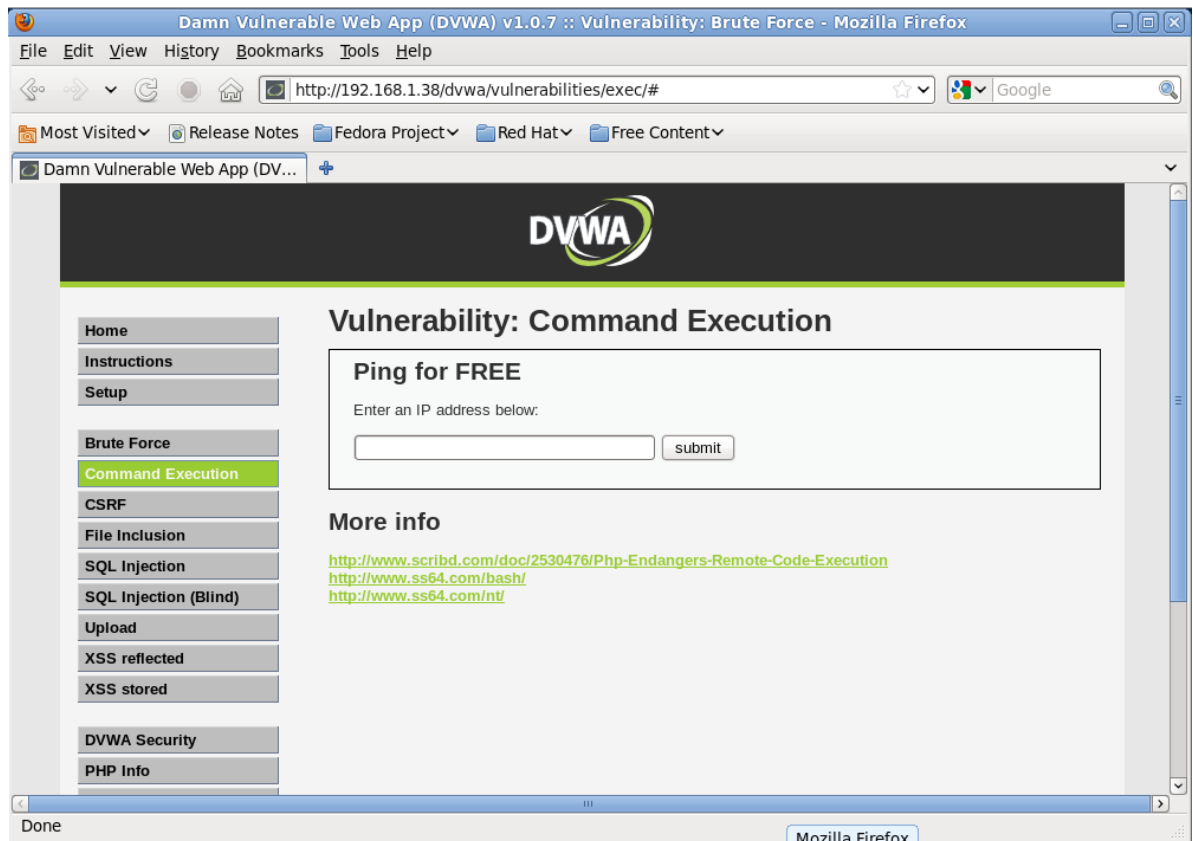
Попробуем просто осуществить ping к какому-то компьютеру:



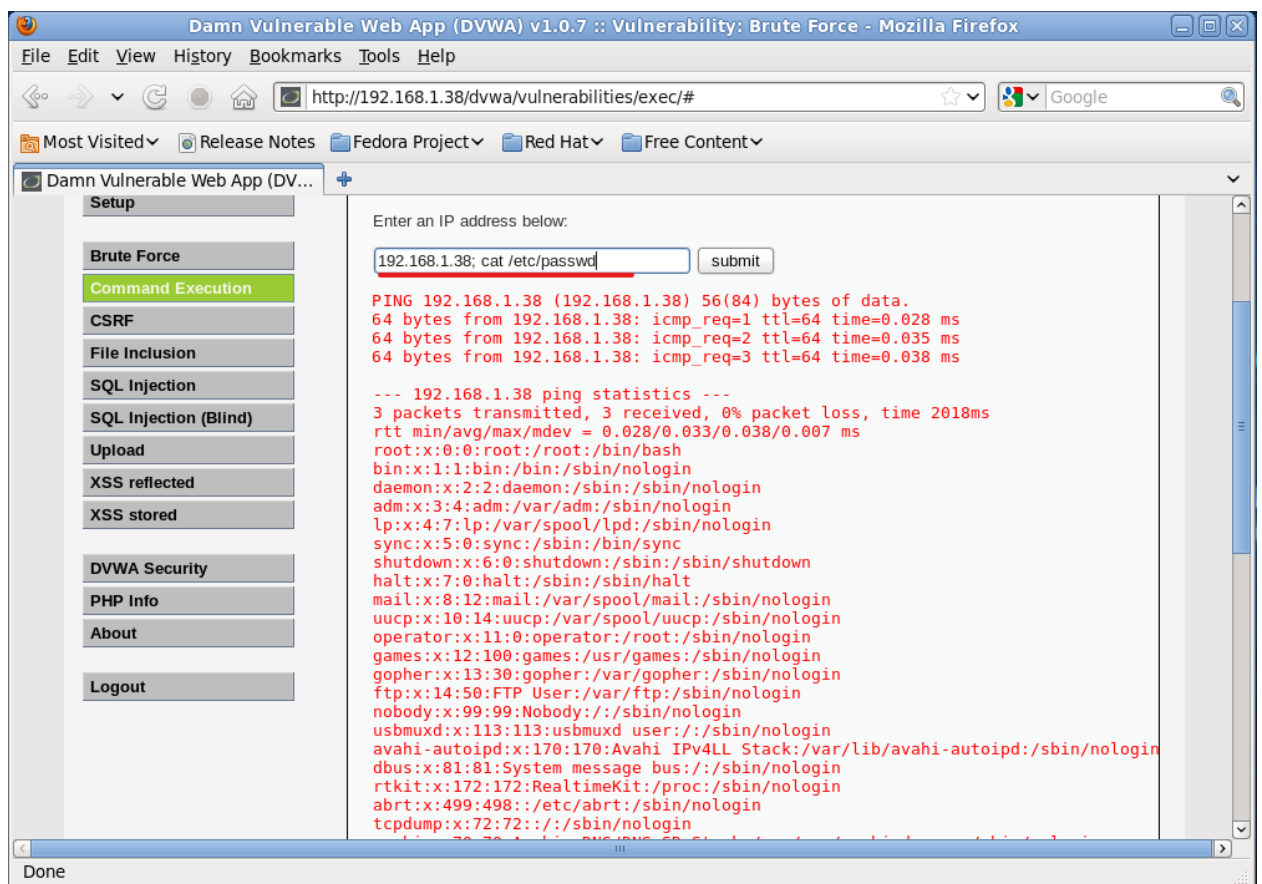
Попробуем просто вставить код:



В результате ничего не вышло:



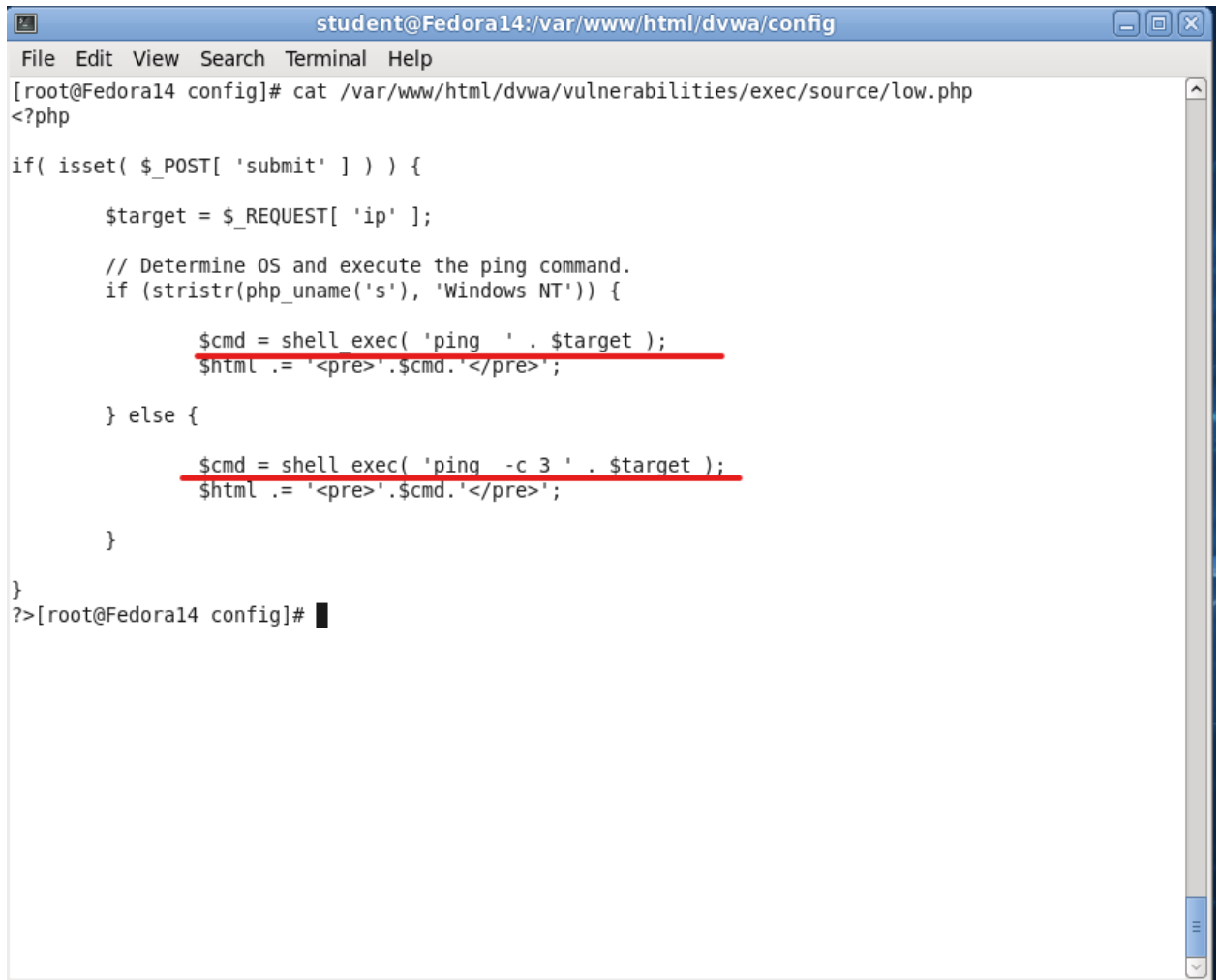
Теперь попробуем вставить вместе с ip адресом, и можно заметить, что
Вывелись данные из файла passwd:



Изучим причину уязвимости:

Найдите две строки с `shell_exec`. Это строки с кодом, запускающим `ping` в зависимости от используемой ОС. В Unix-подобных ОС команды объединяются с помощью оператора «;»

Заметим, что в коде нет проверки на то, что содержимое `$target` подходит под маску `ip`-адреса:



```
student@Fedora14:/var/www/html/dvwa/config
File Edit View Search Terminal Help
[root@Fedora14 config]# cat /var/www/html/dvwa/vulnerabilities/exec/source/low.php
<?php

if( isset( $_POST[ 'submit' ] ) ) {

    $target = $_REQUEST[ 'ip' ];

    // Determine OS and execute the ping command.
    if (stristr(PHP_OS, 'Windows NT')) {

        $cmd = shell_exec( 'ping ' . $target );
        $html .= '<pre>'.$cmd.'</pre>';

    } else {

        $cmd = shell_exec( 'ping -c 3 ' . $target );
        $html .= '<pre>'.$cmd.'</pre>';

    }

}

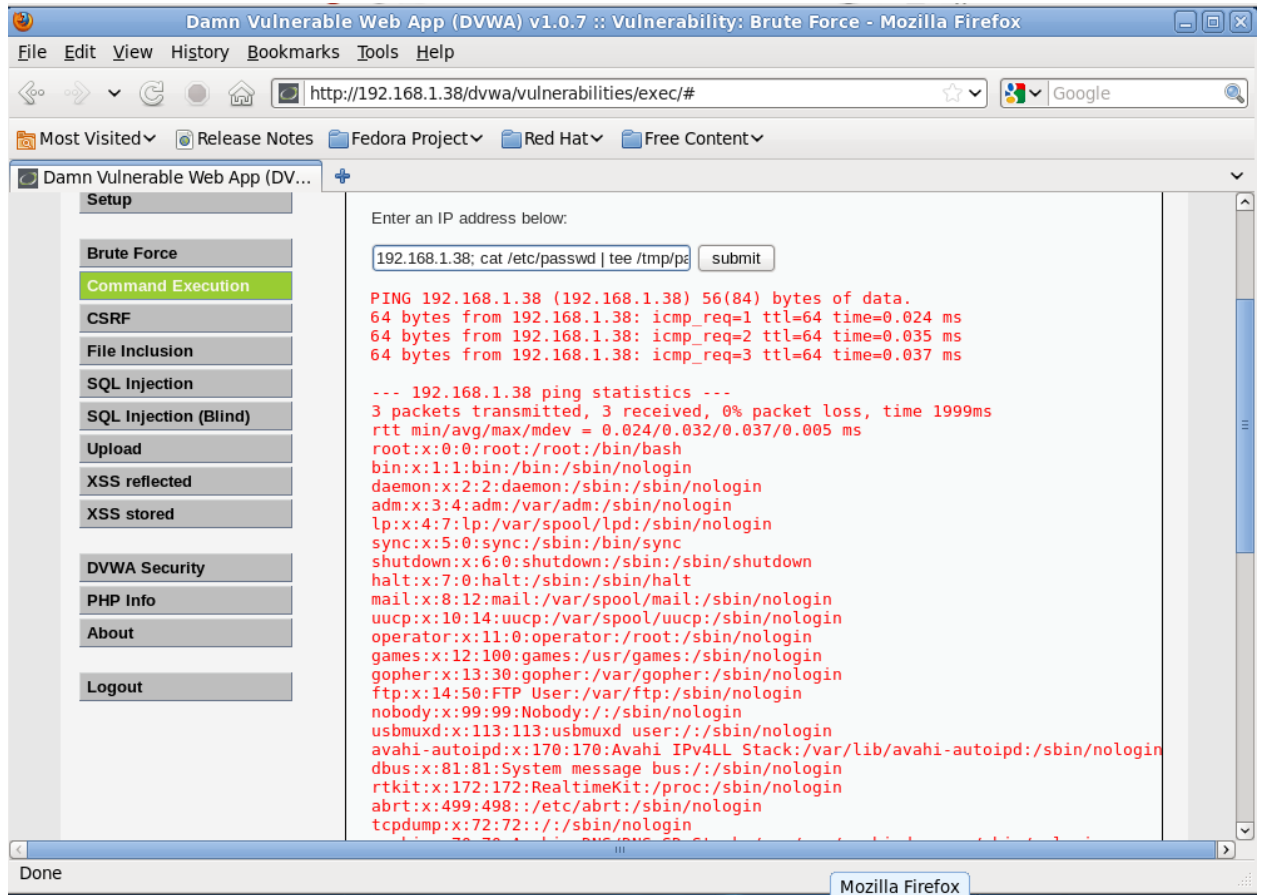
?>[root@Fedora14 config]#
```

Скопировали `passwd` в `tmp`:



```
student@Fedora14:/var/www/html/dvwa/config
File Edit View Search Terminal Help
[root@Fedora14 config]# cp /etc/passwd /tmp
[root@Fedora14 config]# ls /tmp
gedit.root.3997857219  orbit-student  pulse-LqV4KSDUsb0q  virtual-student.X6rBJR
keyring-ItzJao        passwd          pulse-PKdhtXMmr18n
lost+found            pear           virtual-student.bUghvn
orbit-gdm             pulse-2PCj1NAL3SRg  virtual-student.g7vCXU
[root@Fedora14 config]#
```

Введем в поле веб-приложения IPADDRESS; cat /etc/passwd | tee /tmp/passwd:



Отчет о работе:

