1. Открыть консоль браузера на http://attacker.com и запросить файл с http://victim.com с помощью XHR. Изучить реакцию браузера в консоли.

2. Примечание: домены `attacker.com` и `victim.com` должны резолвиться в `127.0.0.1`, конфиг nginx тоже должен отдавать все так, чтобы на начало задания работало оба алерта.

Добавить данную политику CSP на сайте http://victim.com. Загрузить страницу `victim.com/csp.php?js=<script/src=//attacker.com/evil.js></script>`, посмотреть что произошло. Исправить политику CSP так, чтобы вредоносный код не выполнялся.

Файл csp.php

```
<body>
<h3>Whatever _malicious_ you inserted shouldn’t be executed!</h3>
<?php
  echo $_GET["js"];
?>
<h3>But legitimate code still should execute</h3>
<script src="http://victim.com/some.js"></script>
</body>
```

Политика CSP

```
Content-Security-Policy: default-src 'none'; script-src 'unsafe-inline'

http://localhost;
```

Файл some.js

```
alert("I’m legitimate!")
```

Файл evil.js

```
alert("I’m evil!")
```

3. Не дать вредоносному коду `http://victim.com/hw-6-3.php?name=<script>alert("hacked")</script>` выполниться на странице http://victim.com/hw-6-3.php (представлена ниже) с помощью политики CSP (написать политику CSP). Легитимный код при это должен выполняться.

Страница hw-6-3.php

```
<body>
<h3>Whatever _malicious_ you inserted shouldn’t be executed!</h3>
<?php
  echo $_GET["name"];
?>
<h3>But legitimate code still should execute</h3>
<script src="http://victim.com/some.js"></script>
<script src="http://sub.victim.com/some.js"></script>
</body>
```

4. (*) Обойти политику CSP: `script-src 'unsafe-eval' http://victim.com http://partner.com http://home.victim.com` на странице http://victim.com/hw-6-4.html?text=123. Сделать безопасно, понять почему теперь безопасно.

Файл hw-6-4.html

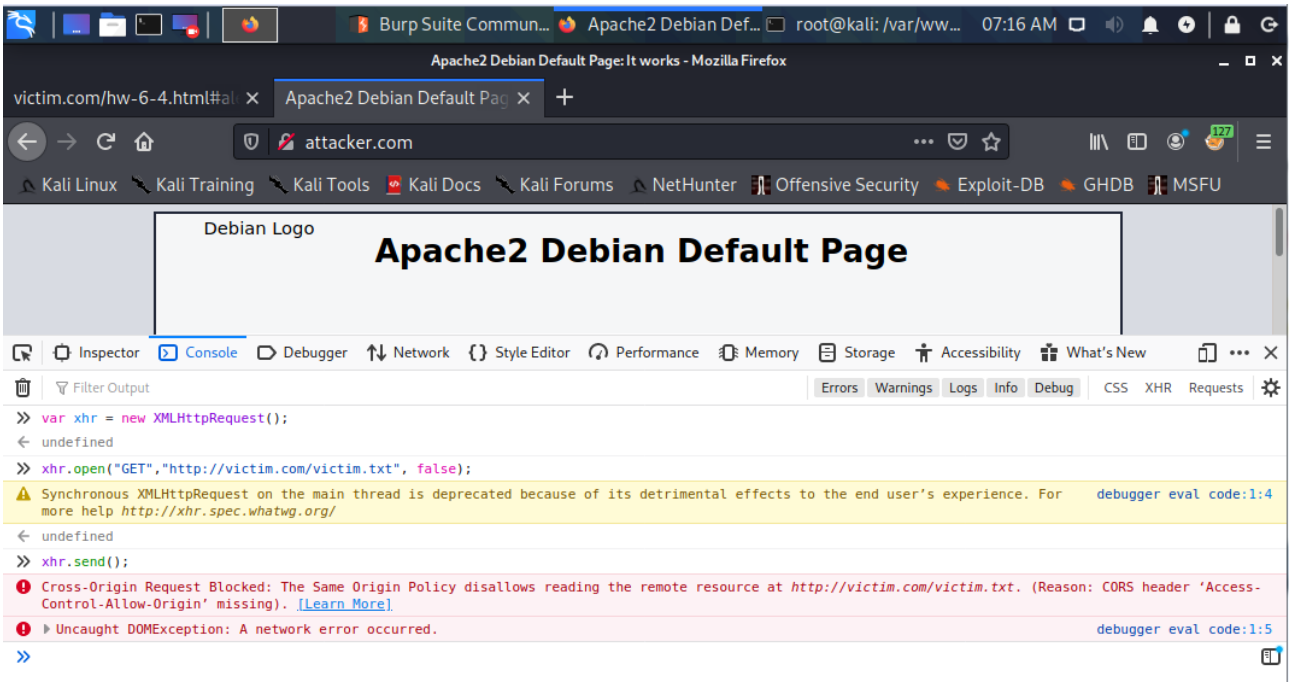
```
<body>
<h3>Legitimate code still should execute</h3>
<script src="/hw-6-4.js"></script>
</body>
```

Файл hw-6-4.js

```
function okFunction () {
  alert("I'm legitimate!");
}
setTimeout(document.URL.split("#")[1], 1000);
setTimeout(okFunction, 1000);
```

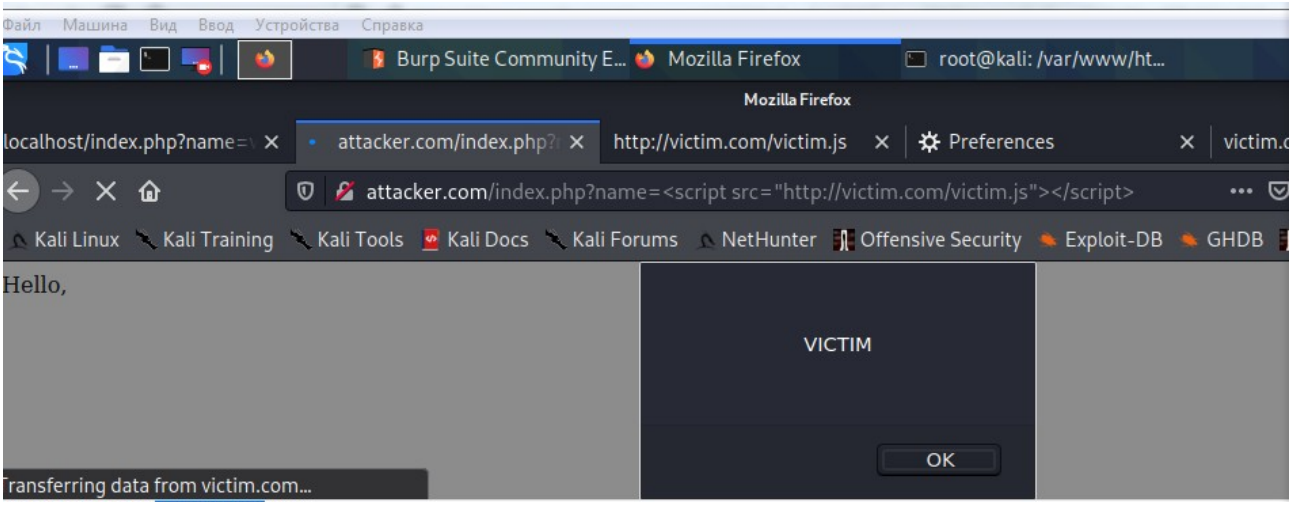
5. (*) Установить bWAPP.

1. Через консоль браузера.



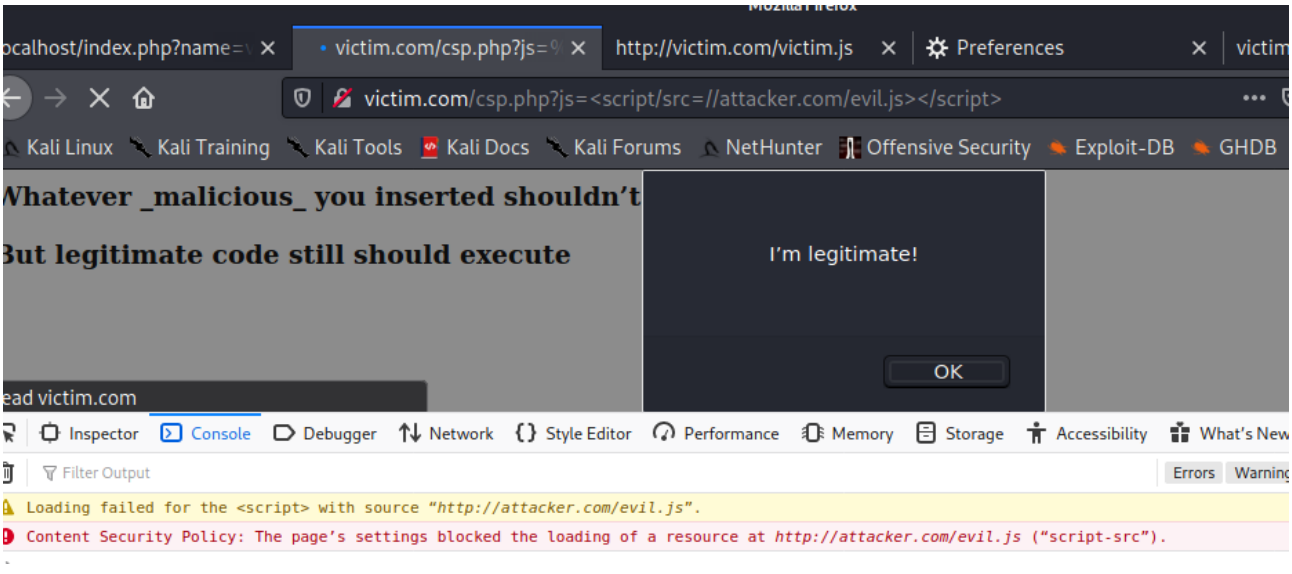
А теперь немного поменяем конфиг и попробуем выполнить скрнипт через командную строку.

```
        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 localhost;

        location / {
                # First attempt to serve request as file, then
                # as directory, then fall back to displaying a 404.

                add_header Content-Security-Policy "script-src unsafe-inline;";

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



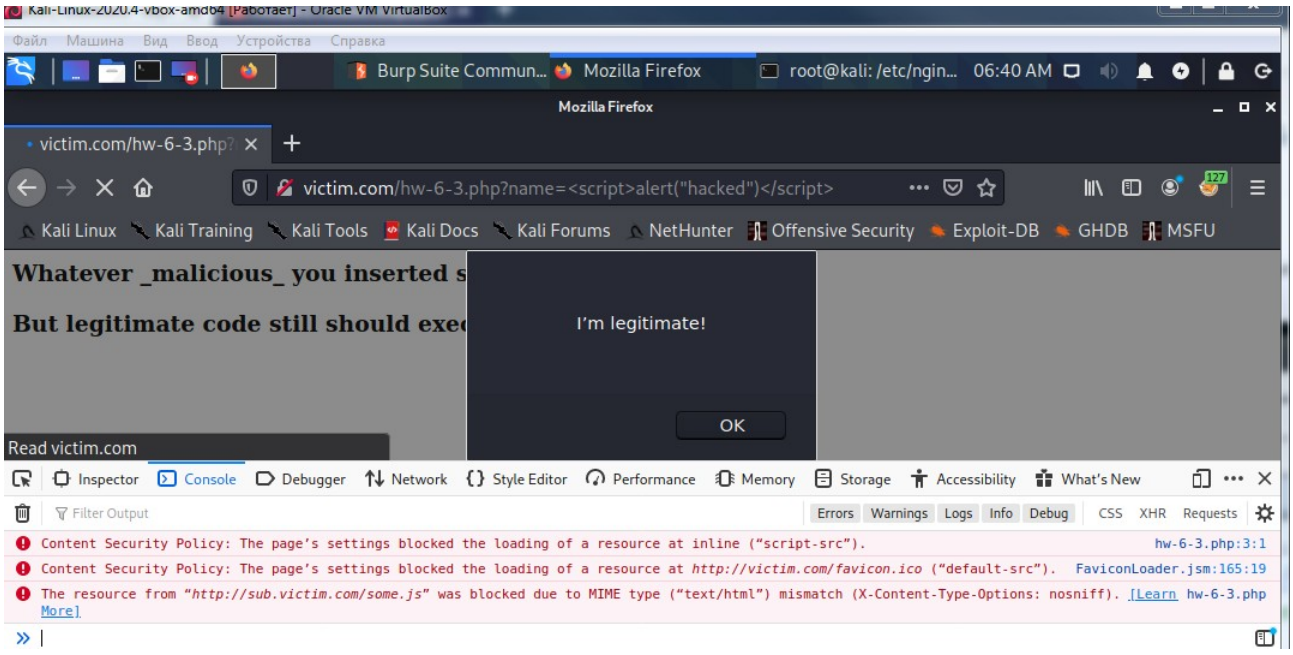
2.

```
        # pass PHP scripts to FastCGI server
        #
        location ~ \.php$ {
                include snippets/fastcgi-php.conf;
        #
        #       # With php-fpm (or other unix sockets):
        add_header Content-Security-Policy "script-src 'unsafe-inline' http://victim.com;";
        fastcgi_pass unix:/run/php/php7.4-fpm.sock;
        #       # With php-cgi (or other tcp sockets):
        #       fastcgi_pass 127.0.0.1:9000;
        }
```



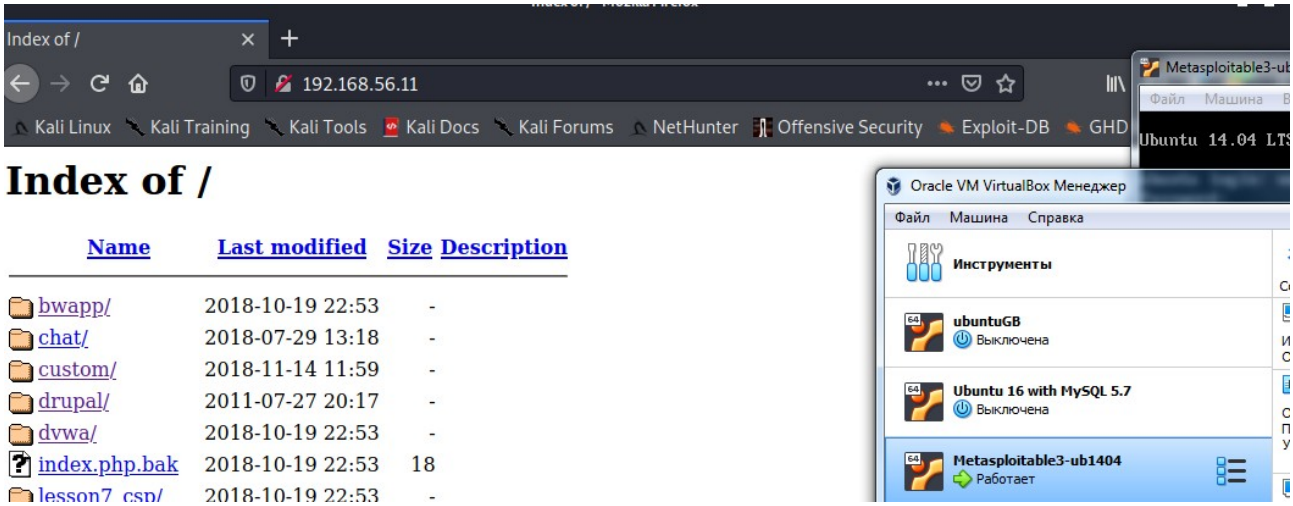
3.

```
location ~ \.php$ {
        include snippets/fastcgi-php.conf;
#
#       # With php-fpm (or other unix sockets):
add_header "Content-Security-Policy" "default-src 'none';script-src  http://victim.com http://sub.victim.com";
fastcgi_pass unix:/run/php/php7.4-fpm.sock;
#       # With php-cgi (or other tcp sockets):
#       fastcgi_pass 127.0.0.1:9000;
}
```



4*. По идее надо убрать unsafe-eval. Я убрал но все равно скрипт отрабатывает.

5*. bwapp на виртуалке Metasploitable. Подлючаюсь по локальной сети через виртуалку kali




Burp Suite Community E...
bWAPP - Login - Mozilla...
06:25 AM
bWAPP - Login - Mozilla Firefox
bWAPP - Login
192.168.56.11/bwapp/login.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
bWAPP
an extremely buggy web app !
Login
New User
Info
Talks & Training
Blog
/ Login /
Enter your credentials (bee/bug).
Login:
Password:
Set the security level:
low
Login
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
MME
Security Audits & Training
Scan your website for XSS and SQL Injection vulnerabilities