

## Урок 6: Браузеры: концепции безопасности

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](http://attacker.com) и [victim.com](http://victim.com) должны резолвиться в [127.0.0.1](http://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>](http://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:

### 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>](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://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>
```

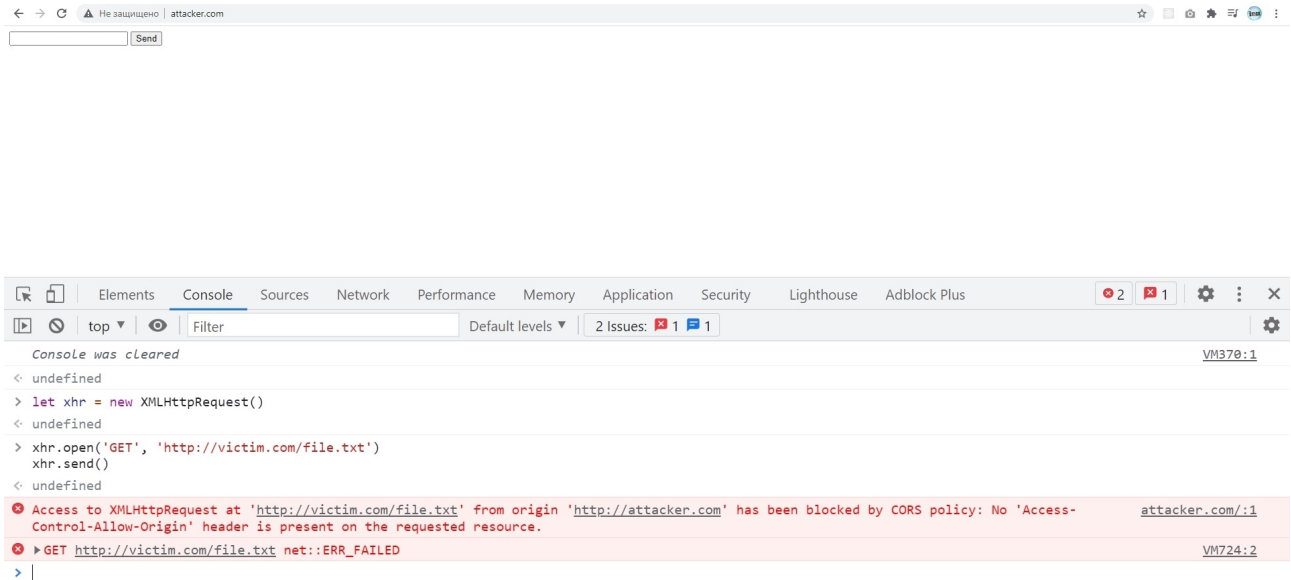
#### Файл hw-6-4.js

```
function okFunction () {
    alert("I'm legitimate!");
}

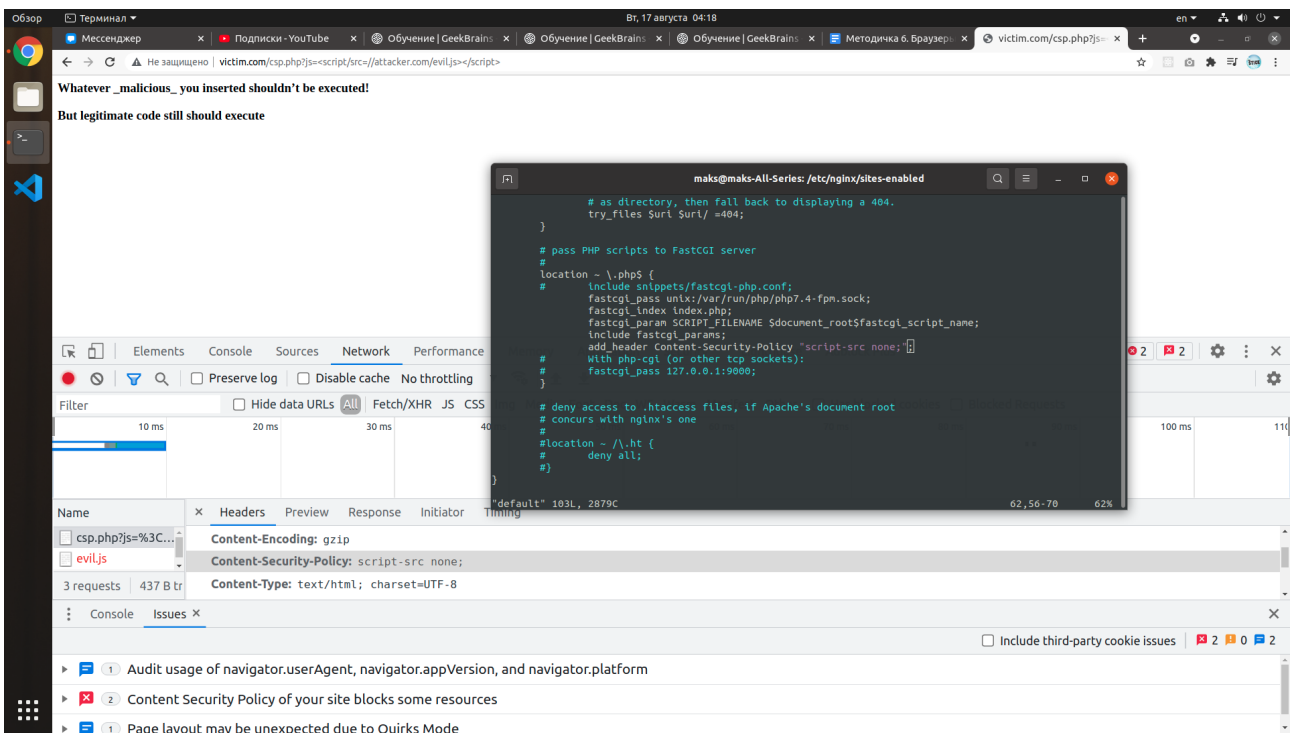
setTimeout(document.URL.split("#")[1], 1000);
setTimeout(okFunction, 1000);
```

## 5. (\*) Установить bWAPP.

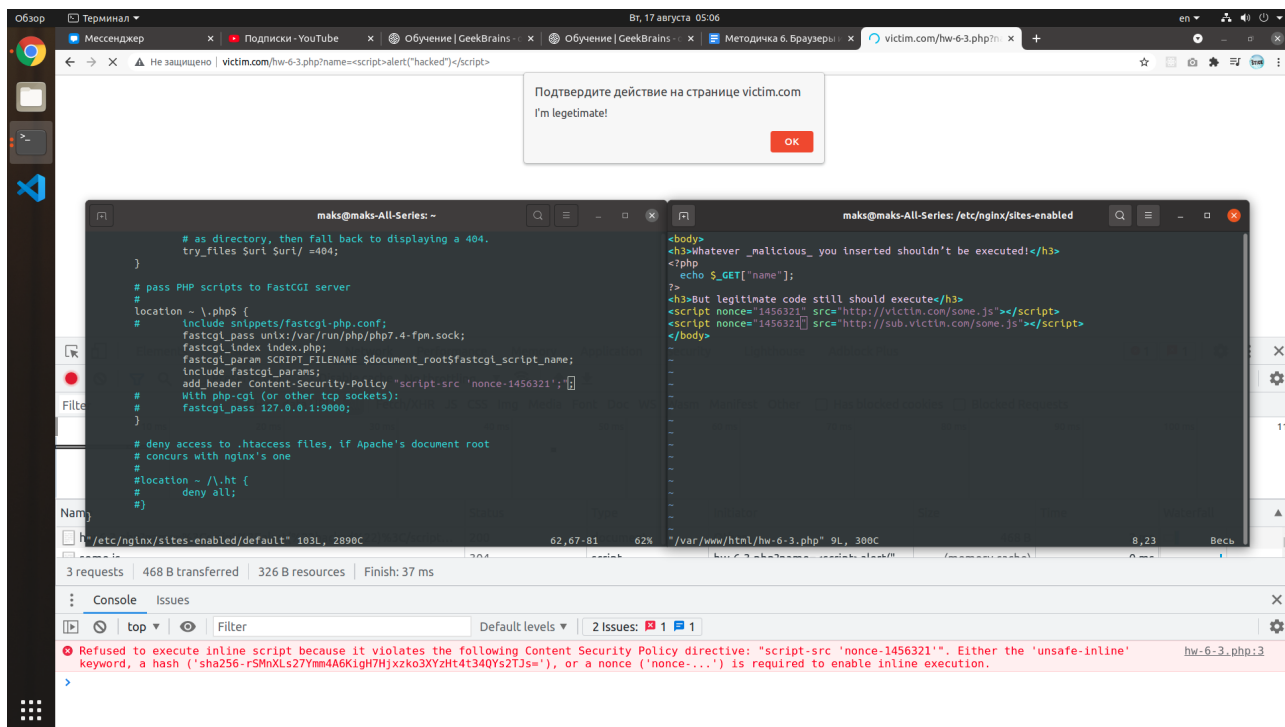
1.



2.



3.



4, 5

Не успел.

