

Выполнил Мешечкин Д. Инфобез-2345

Задание 1: Это задание выполняется на домене **attacker.com**. Прочитать куки домена **attacker.com** и вывести их. Попробовать прочитать и вывести куки домена **victim.com**.

Загружаю страницу **attacker.com**, через консоль разработчика смотрю куки, которые записал сайт в браузер.

The screenshot shows the Chrome DevTools Network tab. A single cookie entry is selected: `(ed0683a0-b34f-497a-87e3-bbc88fa5c32c)` with value `value`. The cookie details pane on the right shows the following properties:

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
<code>(ed0683a0-b34f-497a-87e3-bbc88fa5c32c)</code>	<code>value</code>	<code>attacker.com</code>	<code>/</code>	<code>Thu, 26 Jan 2023 1...</code>	<code>43</code>	<code>False</code>	<code>false</code>	<code>Lax</code>	<code>Wed, 25 Jan 2023 1...</code>

Properties pane (right side):

- `(ed0683a0-b34f-497a-87e3-bbc88fa5c32c).value`
- `Created: "Wed, 25 Jan 2023 16:48:14 GMT"`
- `Domain: "attacker.com"`
- `Expires / Max-Age: "Thu, 26 Jan 2023 16:48:14 GMT"`
- `HostOnly: true`
- `HttpOnly: false`
- `Last Accessed: "Wed, 25 Jan 2023 16:48:14 GMT"`
- `Path: "/"`
- `SameSite: "Lax"`
- `Secure: false`
- `Size: 43`

На данный момент попытался воскресить php-fpm - не вышло добиться толковой работоспособности и/или загрузки php скриптов с сайта. Этим уже когда-то потом буду заниматься.

После запросом через консоль командой `document.cookie` запрашиваю.

The screenshot shows the Chrome DevTools Console tab. The output of the command `document.cookie` is displayed:

```
>>> document.cookie
<code>"(ed0683a0-b34f-497a-87e3-bbc88fa5c32c)=value"</code>
```

At the bottom of the console, there is a detailed log of network requests:

- `GET http://attacker.com/ [HTTP/1.1 304 Not Modified lms]`
- `Content Security Policy: The page's settings blocked the loading of a resource at inline ("default-src"). [attacker.com:11:1]`
- `Content Security Policy: The page's settings blocked the loading of a resource at inline ("default-src"). [attacker.com:11:1]`
- `GET http://attacker.com/icons/ubuntu-logo.png [HTTP/1.1 404 Not Found 0ms]`
- `GET http://attacker.com/favicon.ico [HTTP/1.1 404 Not Found 0ms]`
- `>>> document.cookie`
- `<code>"(ed0683a0-b34f-497a-87e3-bbc88fa5c32c)=value"</code>`

Проделываю туже операцию с **victim.com**.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
645962aa-ccc6-4382-b8f3-5fd3cf33683b	value	victim.com	/	Thu, 26 Jan 2023 17:10:26 GMT	43	false	false	Lax	Wed, 25 Jan 2023 17:10:26 GMT

[645962aa-ccc6-4382-b8f3-5fd3cf33683b]: "value"
 Created: "Wed, 25 Jan 2023 17:10:26 GMT"
 Domain: "victim.com"
 Expires / Max-Age: "Thu, 26 Jan 2023 17:10:26 GMT"
 HostOnly: true
 HttpOnly: false
 Last Accessed: "Wed, 25 Jan 2023 17:10:26 GMT"
 Path: "/"
 SameSite: "Lax"
 Secure: false
 Size: 43

Запрашиваю куки через консоль.

This page is in Almost Standards Mode. Page layout may be impacted. For Standards Mode use <!DOCTYPE html>. [Learn More]

Content Security Policy: The page's settings blocked the loading of a resource at inline ("default-src").

Content Security Policy: The page's settings blocked the loading of a resource at inline ("default-src").

>> document.cookie
 < "645962aa-ccc6-4382-b8f3-5fd3cf33683b}=value"

Запросы кук с различных доменов имеют различные значения, аналогично различным сайтам.

Честно, я не очень понял смысл задания и требования результата.

Задание 2: Дан сайт, который при нажатии на кнопку меняет цвет фона. Дописать, чтобы при открытии сайта JS обращался в web storage за цветом фона и восстанавливает его.

```

<body>
    <script>
        function changeBodyColor(color) {
            document.body.style.backgroundColor = color;
        }
    </script>
    <button onclick="changeBodyColor('red')">Make it hell!</button>
    <button onclick="changeBodyColor('green')">Make it grass!</button>
</body>
```

Создаётся файл в директории /var/www/html/ht-7-2.html с наполнением из задания.

Для того, чтобы сайт записывал изначально данные в WebStorage необходимо добавить строчку в <script>:

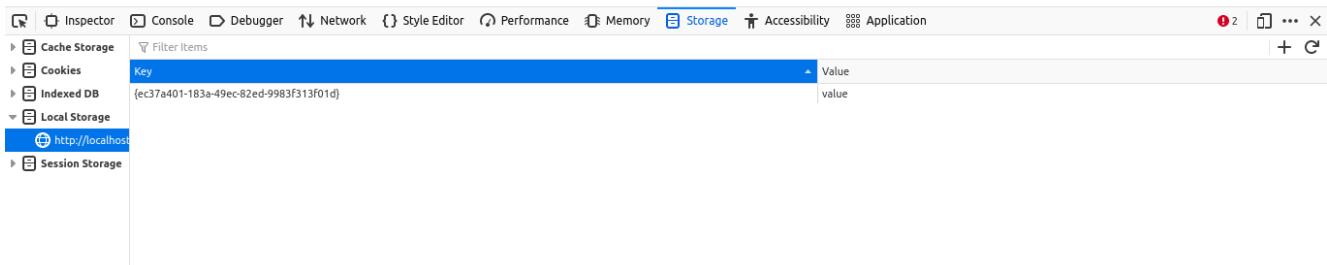
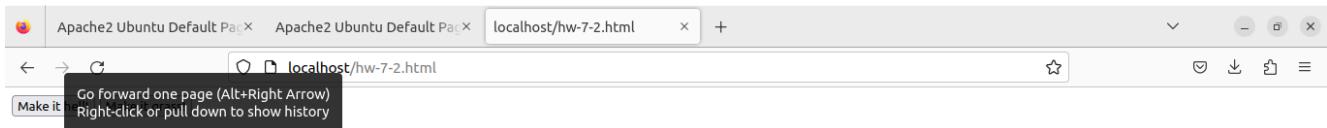
```
localStorage.setItem('bgColor', 'white');
```



```
GNU nano 6.2
body>
<script>
    localStorage.setItem('bgColor', 'white');
    function changeBodyColor(color) {
        document.body.style.backgroundColor = color;
    }
</script>
<button onclick="changeBodyColor('red')">Make it hell!Make it grass!
```

Таким образом, при перезаходе на страницу, фон будет всегда белым, независимо от того, каким был фон до выхода из браузера/перезахода/обновления сессии.

Где-то в браузере подобная информация от localStorage не отображается, кроме информации о куках.



Опять же, возвращаясь к тексту домашних заданий, объяснениям в видео - на данном этапе "реформирования" прошли, на мой взгляд не очень удачно. Начиная с ДЗ№5 смысл заданий не очень понятен, если честно.