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

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>
```

Задание 3. (*) Самостоятельно настроить CORS на http://victim.com. Разрешить http://localhost с помощью CORS делать запросы к http://victim.com.

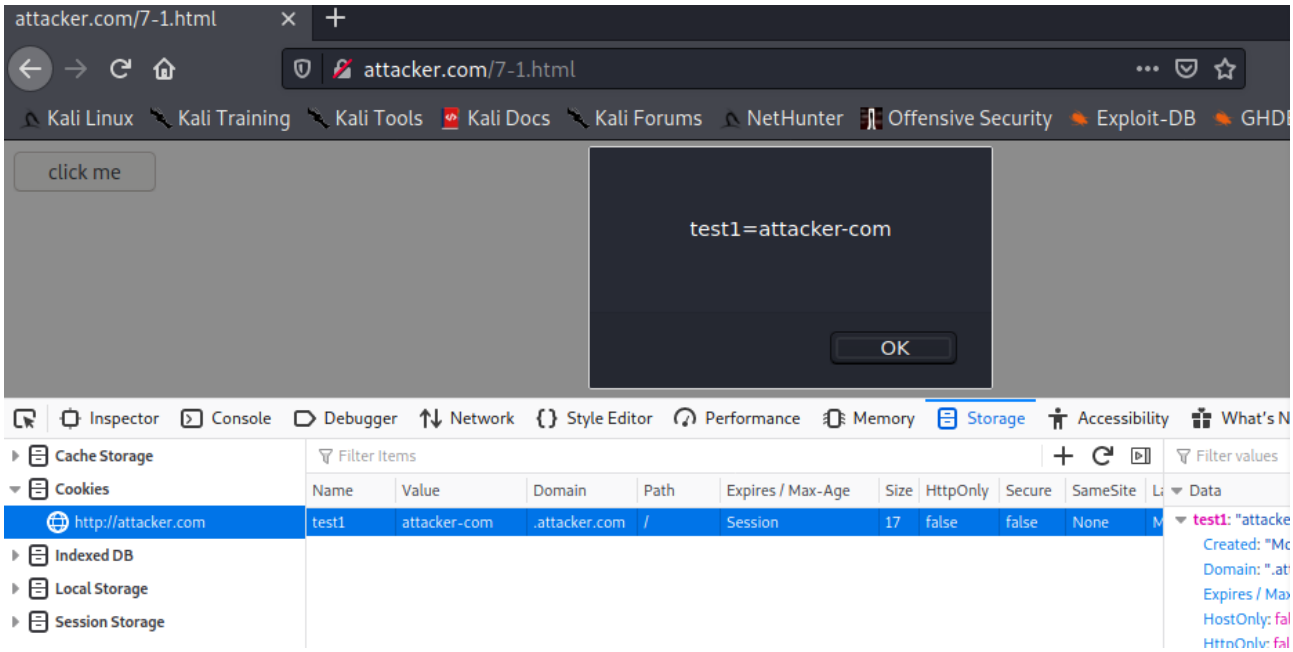
Задание 4. (*) Решить как можно больше XSS на уровне low в bWAPP.

1. Ставим в конфиге nginx cookie и cors для всех сайтов

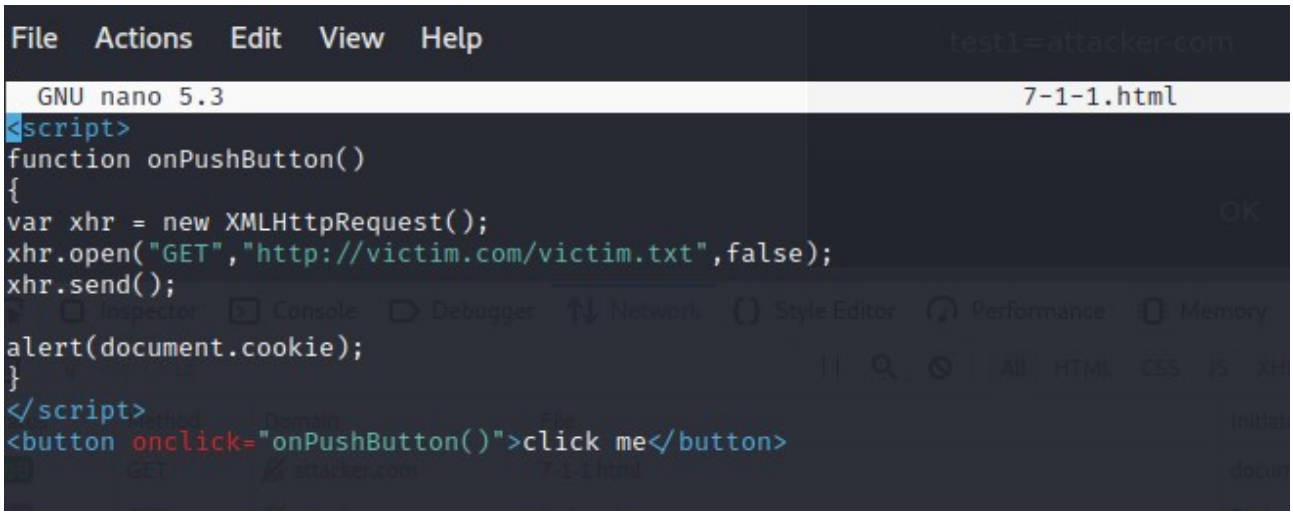
```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        server_name localhost;
        root /var/www/html;

        location / {
         add_header "Set-Cookie" "test1=attacker-com; Domain=attacker.com";
         add_header "Set-Cookie" "test2=attacker-com_victim-com; Domain=victim.com";
         #add_header Access-Control-Allow-Origin "http://victim.com";
         add_header 'Access-Control-Allow-Origin' '*';
        add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
        add_header 'Access-Control-Allow-Headers' 'DNT,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Range';
        add_header 'Access-Control-Expose-Headers' 'Content-Length,Content-Range';
      try_files $uri $uri/ =404;
        }
}
```

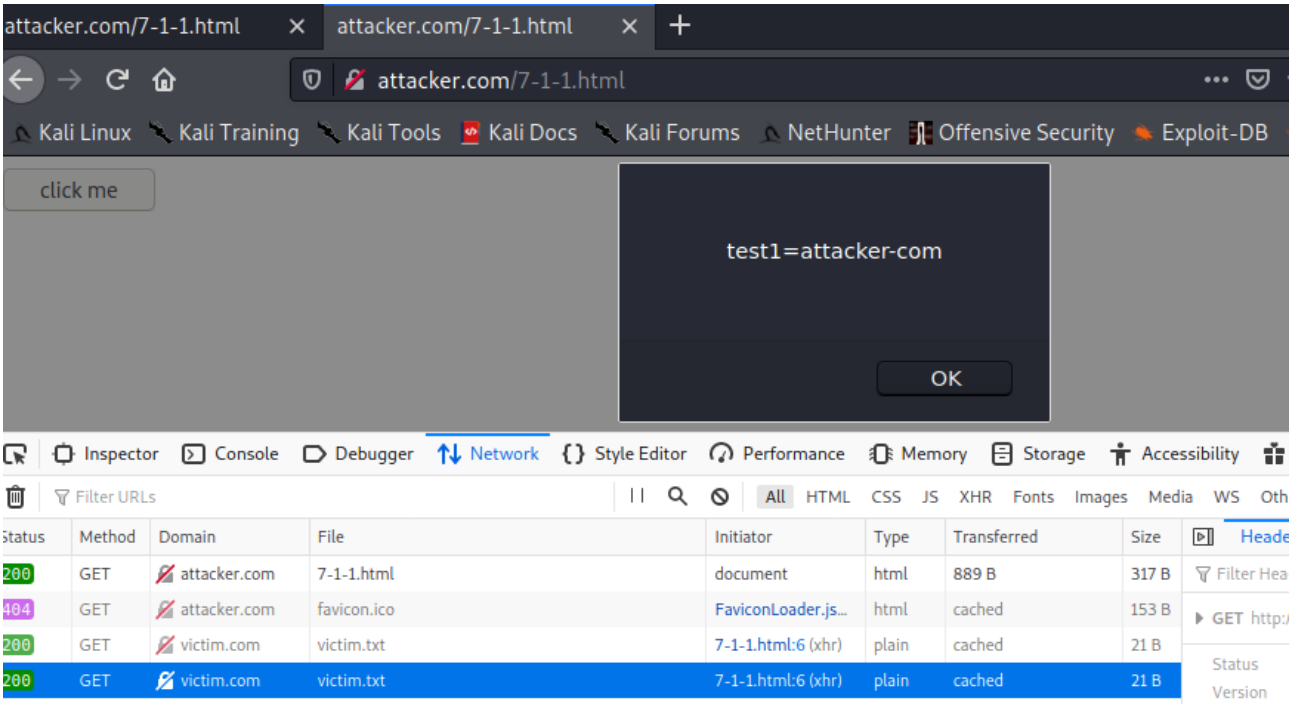
Читаем таким кодом куку с attacker.com

```
File  Actions  Edit  View  Help
  GNU nano 5.3                                    7-1.html
<script>
function onPushButton()
{
alert(document.cookie);
}
</script>
<button onclick="onPushButton()">click me</button>
```



Таким кодом показываем куку на victim.com





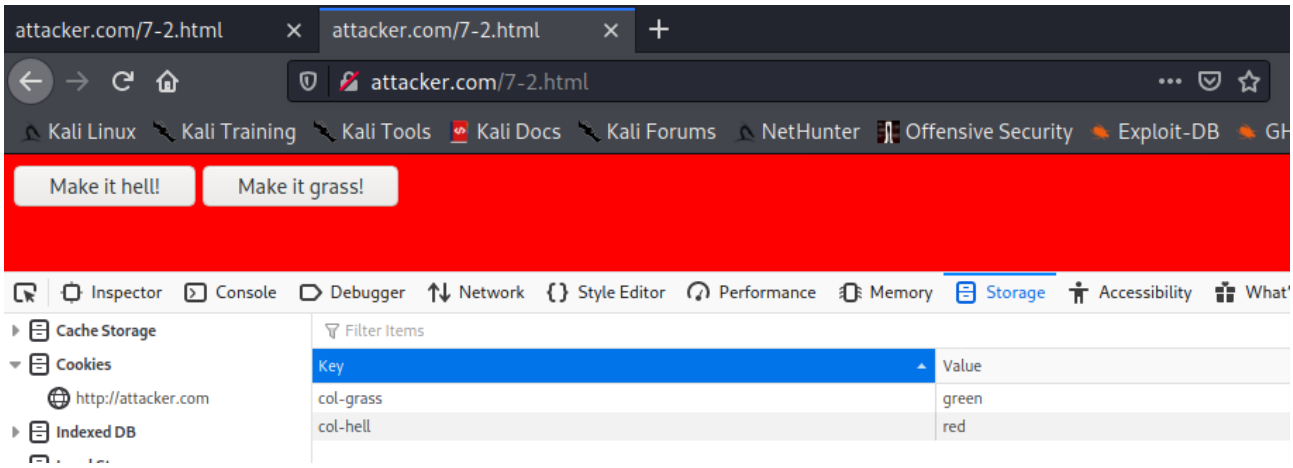
2.

root@kali: /var/www/html

File Actions Edit View Help

GNU nano 5.3 7-2.html *

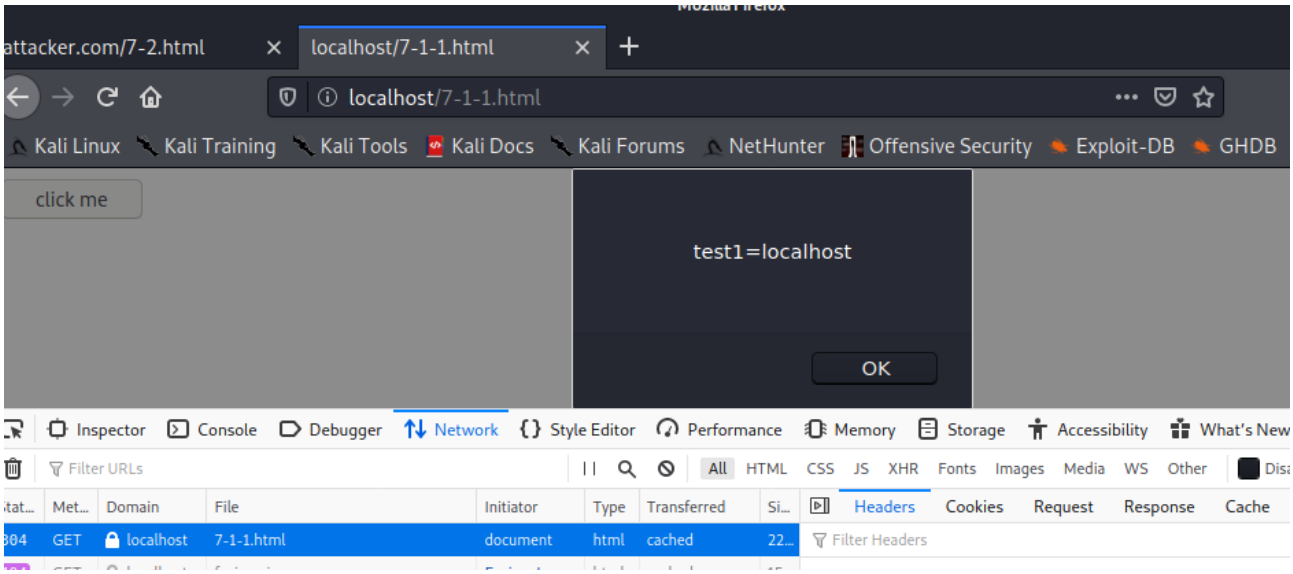
```
<html>
<body>
<script>
localStorage.setItem("col-hell", "red");
localStorage.setItem("col-grass", "green");

  function changeBodyColor(color) {
    var col = localStorage.getItem(color);
    document.body.style.backgroundColor = col;
  }
</script>
<button onclick="changeBodyColor('col-hell')">Make it hell!</button>
<button onclick="changeBodyColor('col-grass')">Make it grass!</button>
</body>
</html>
```



3*. Сделал в задании 1 на примере attacker.com. Для localhost надо просто добавить куку в конфиге

GNU nano 5.3 test.conf

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

        server_name localhost;
        root /var/www/html;

        location / {
         add_header "Set-Cookie" "test1=attacker-com; Domain=attacker.com";
         add_header "Set-Cookie" "test123=localhost; Domain=localhost";
         add_header "Set-Cookie" "test2=attacker-com_victim-com; Domain=victim.com";
         #add_header Access-Control-Allow-Origin "http://victim.com";
         add_header 'Access-Control-Allow-Origin' '*';
        add_header 'Access-Control-Allow-Methods' 'GET, POST, OPTIONS';
        add_header 'Access-Control-Allow-Headers' 'DNT,User-Agent,X-Requested-With,If-Modified-Si
        add_header 'Access-Control-Expose-Headers' 'Content-Length,Content-Range';
      try_files $uri $uri/ =404;
        }
}
```



4*. На GET и POST на low и medium работает вот такая вещь