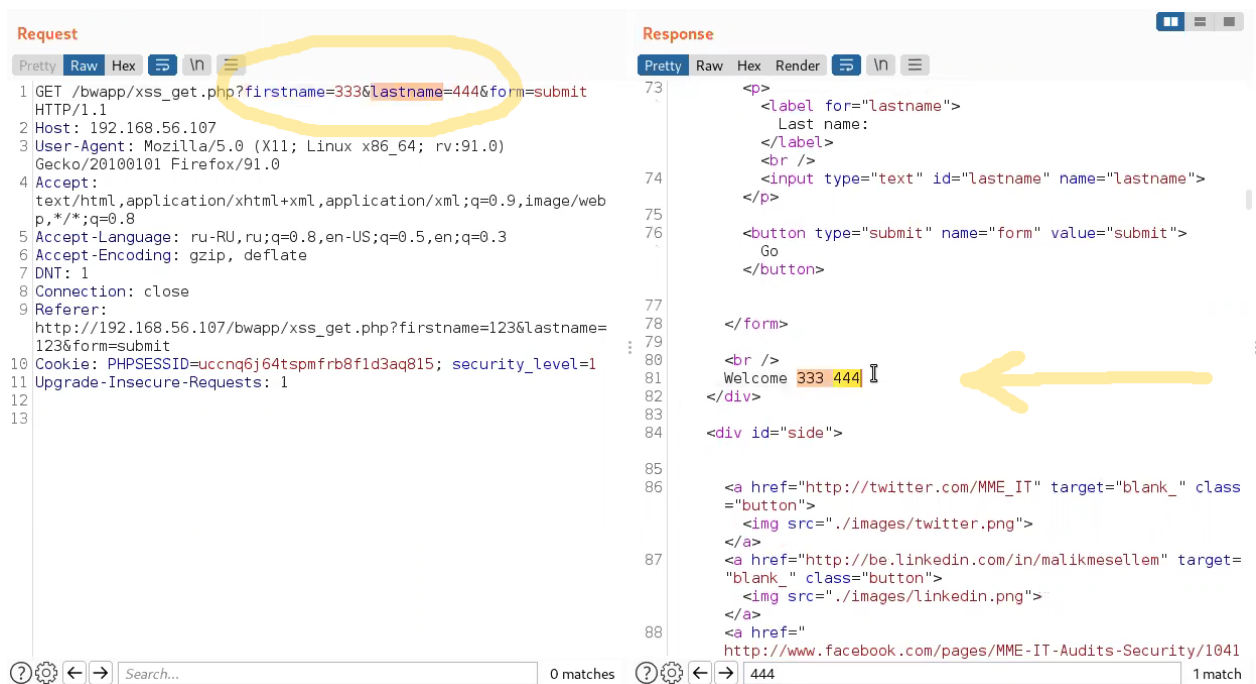


Домашнее задание к 3 уроку.

Исследование уязвимости мы начинаем с анализа того, как страница работает. Нам надо понять какими данными обменивается приложение с серверной частью, где у нас точки отражения и какой контекст. В bWAPP у нас есть два поля ввода – First name и Last name.

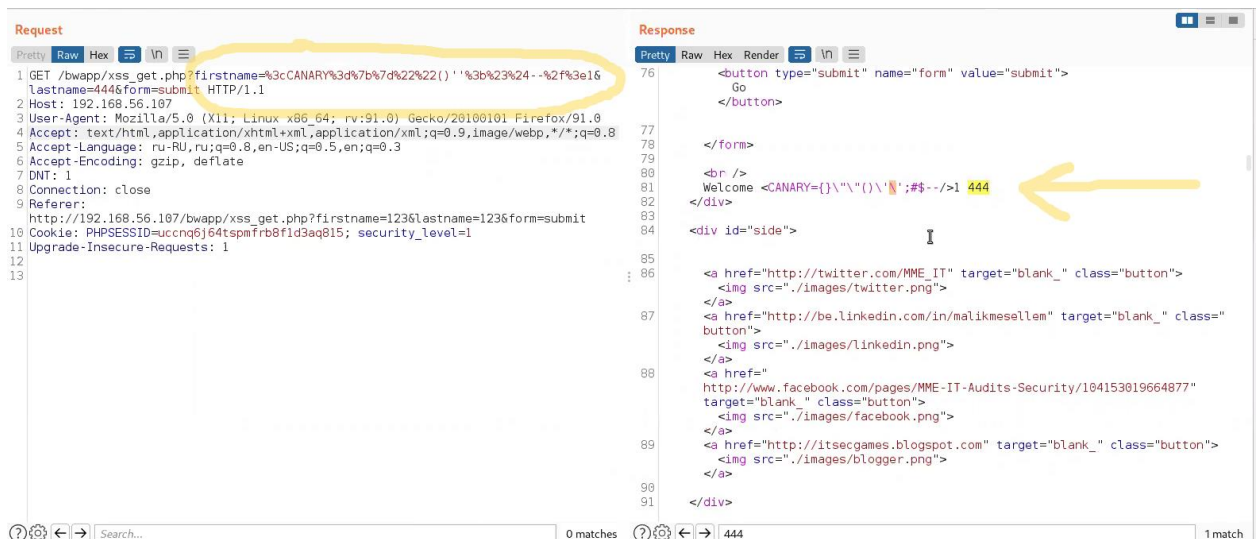


Запустим Burp.



Значения обоих параметров - first name и last name отражаются через html контекст внутри тега <div>, т.е. вектором может быть любая валидная html сущность.

Добавим вектор, который среагирует на фильтры <CANARY={}'"()';#\${--}/>1



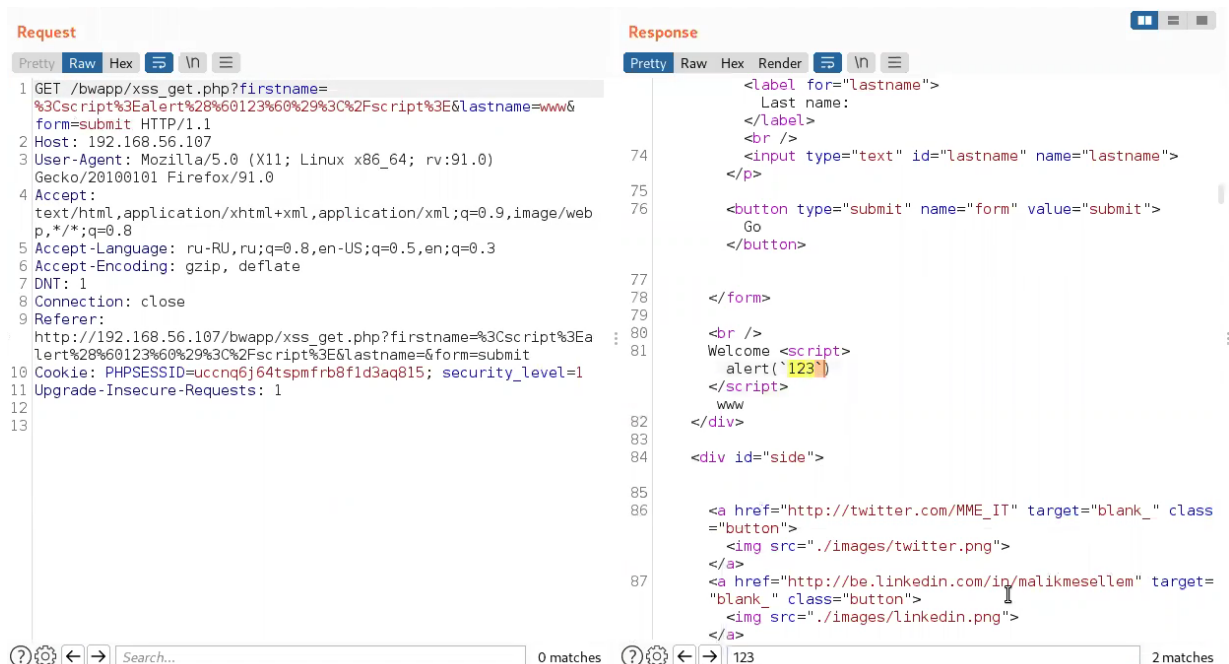
И мы видим, что все кавычки у нас экранируются \ обратным слешом. Это стандартный способ скейпинга различных символов, чтобы они не имели какого-то смысла. Т.е. векторы работать будут, но с ограничениями использования различных сущностей. Например, такой вектор будет работать прекрасно:

```
<script>alert(123) </script>
```

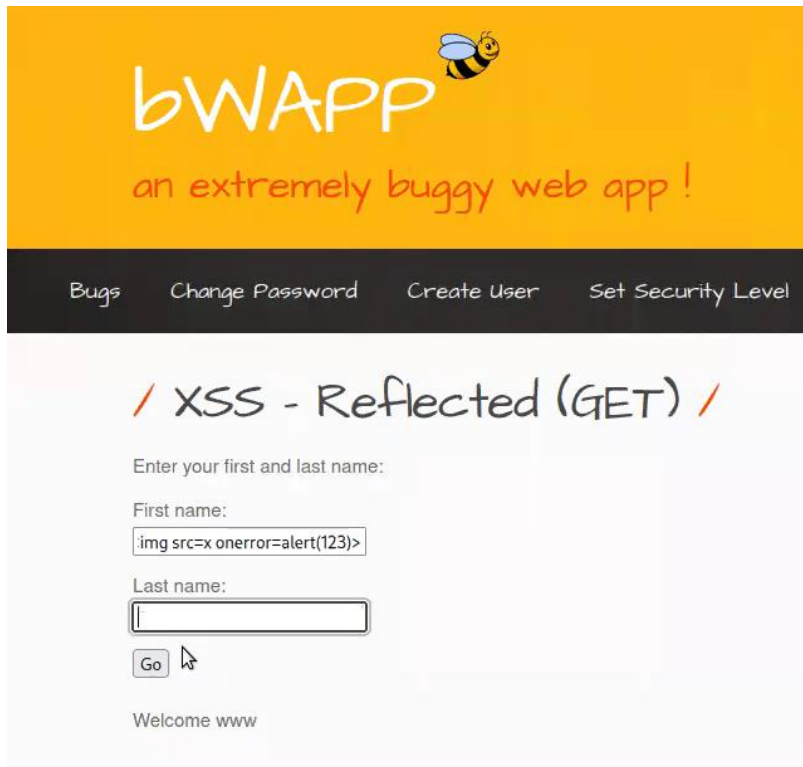
Но если мы берем вектор, где есть хоть какая-то кавычка – возникает проблема.


```
<script>alert('123') </script>
```

Данные будут экранироваться. Злоумышленника это не остановит, но потенциал атаки будет снижен. Но обойти это всё-таки можно - с помощью обратной кавычки ` . Соответственно, при попадании в html контекст этот символ будет интерпретироваться как обычная кавычка. Проблема в том, что фильтр настроен на один вид спецсимволов.



Событие onerror (<img src=x onerror=alert(123)) мы помещаем в поле ввода



bwAPP 

an extremely buggy web app !

Bugs Change Password Create User Set Security Level

/ XSS - Reflected (GET) /

Enter your first and last name:

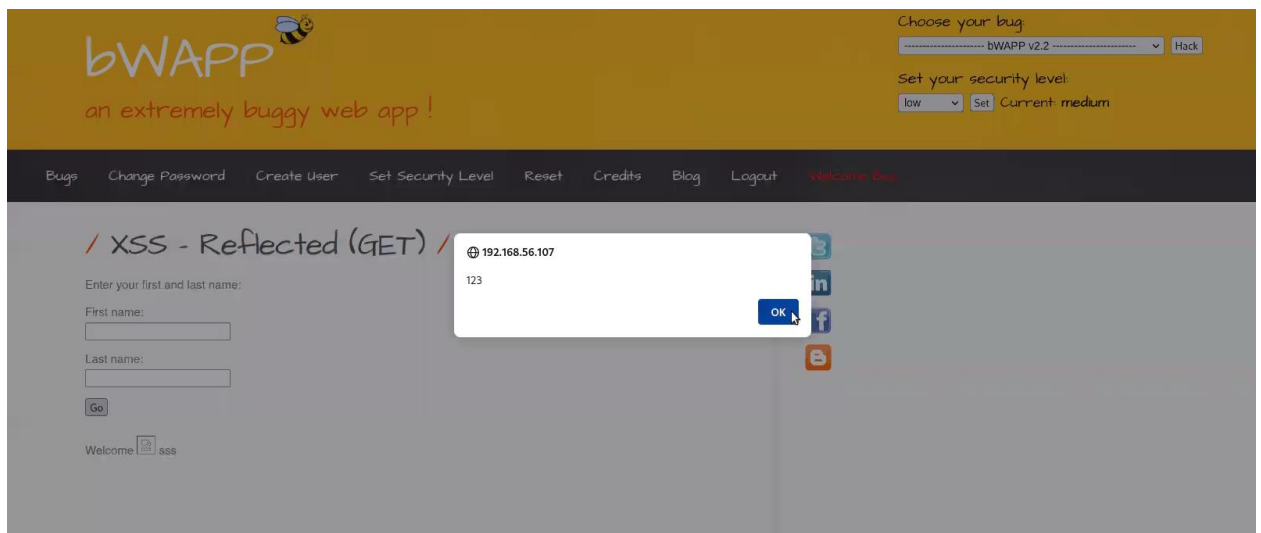
First name:


Last name:

Go

Welcome www

И видим, что он выполняется. Экранирования не происходит, так как данный вектор не содержит кавычек, фильтр не работает.



bwAPP 

an extremely buggy web app !

Choose your bug: bwAPP v2.2 Hack

Set your security level: low Set Current medium

Bugs Change Password Create User Set Security Level Reset Credits Blog Logout Welcome Pwn


/ XSS - Reflected (GET) /

Enter your first and last name:

First name:

Last name:

Go

Welcome  ass

192.168.56.107
123
OK