CROSS-SITE SCRIPTING

Коломиец Никита P3408

ПЛАН ВЫСТУПЛЕНИЯ

01
Что такое XSS?

Что такое XSS? Как он работает?

02
Типы XSS атак

Какие есть типы XSS? В чем их особенности?

03
Применение XSS

Для чего можно использовать XSS?

04
Точки входа XSS

Как найти и протестировать XSS?

05
Что такое CSP?

Как CSP может помочь с защитой от XSS-атаки?

06
Избежание атаки

Как предотвратить XSS-атаку?

01.

ЧТО ТАКОЕ XSS?

CROSS-SITE SCRIPTING

Межсайтовый скриптинг — это уязвимость веб-безопасности, которая позволяет злоумышленнику поставить под угрозу взаимодействие пользователей с уязвимым приложением.

02.

ТИПЫ XSS-атак

ТИПЫ XSS-атак

Отраженный XSS

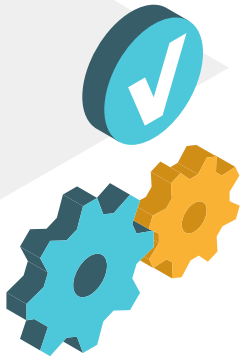
Вредоносный скрипт поступает из текущего HTTP-запроса.

Хранимый XSS

Вредоносный скрипт поступает из базы данных сайта.

XSS на основе DOM

Уязвимость существует в коде на стороне клиента, а не в коде на стороне сервера.



ОТРАЖЕННЫЙ XSS

```
https://insecure-website.com/status?message=All+is+well.
<p>Status: All is well.</p>
```

```
https://insecure-website.com/status?message=<script>/*+Ba
d+stuff+here...+*/</script>
<p>Status: <script>/* Bad stuff here... */</script></p>
```

ХРАНИМЫЙ XSS

```
POST /post/comment HTTP/1.1
Host: vulnerable-website.com
Content-Length: 100

postId=3&comment=This+post+was+extremely+helpful.&name=Ca
rlos+Montoya&email=carlos%40normal-user.net
```

```
comment=%3Cscript%3E%2F*%2BBad%2Bstuff%2Bhere...%2B*%2F%3C
%2Fscript%3E
```

XSS НА ОСНОВЕ DOM

```
var search = document.getElementById('search').value;
var results = document.getElementById('results');
results.innerHTML = 'You searched for: ' + search;
```

```
You searched for: <img src=1 onerror='/* Bad stuff
here... */'>
```

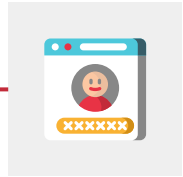
03.

ПРИМЕНЕНИЕ XSS

ПРИМЕНЕНИЕ XSS

Подмена пользователя

Выдать себя за другого юзера



Внедрение трояна

Внедрить функционал трояна

Виртуальная порча

Изменить внешний вид или содержимое веб-сайта

Кража данных

Получить учетные данные пользователя

04.

ТОЧКИ ВХОДА XSS

ТОЧКИ ВХОДА XSS

Поля ввода

Любое поле ввода на веб-сайте

Cookie

Через данные хранящиеся в куках

Заголовки HTTP

Через данные в заголовках HTTP(Referrer, User-Agent).

URL-адрес

Можно вызвать через данные из URL-адреса

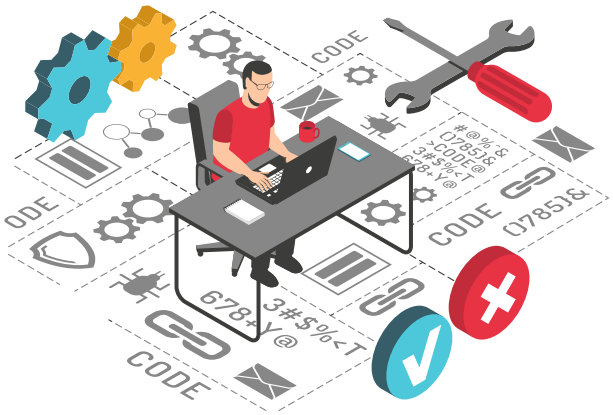
Атрибуты HTML

Можно вызвать через данные в атрибутах HTML(onclick или onload).

05.

ЧТО ТАКОЕ CSP?

ЧТО ТАКОЕ CSP?



Политика безопасности контента (CSP) — это механизм безопасности браузера, целью которого является смягчение XSS и некоторых других атак. Он работает путем ограничения ресурсов (таких как скрипты и изображения), которые может загружать страница, и ограничения возможности включения страницы в рамки других страниц.

```
default-src 'self'; script-src 'self'; object-src 'none'; frame-src 'none'; base-uri 'none';
```

06.

ИЗБЕЖАНИЕ XSS

ИЗБЕЖАНИЕ XSS

Фильтрация ввода

Делать как можно более строгую фильтрацию

1

Кодировать данные на выходе

Кодировать данные, чтобы предотвратить их использование

2

Использовать заголовки в ответах

Content-Type
X-Content-Type-Options

3

CSP

Использование политики безопасности контента

4

Немного практики