XML External Entity(XXE)

ghostlulz Follow
Jun 22 · 3 min read

Slack Group

Before we get started I have started a slack group dedicated to hacking. We welcome everyone from beginner to advanced to join. I will be on everyday answer questions, doing CTFs, and talking about cool hacks. If you enjoy hacking and are looking for like minded people join below:

NEW Hacking Group Slack Channel

Introduction

XML External Entity(XXE) is a vulnerability that can appear when an application parses XML. Before diving into what XXE is you need to have a solid understanding of XML first.

. . .

XML Basics

Extensible Markup Language(XML) is a language designed to store and transport data similar to JSON. A sample of what XML looks like can be found below:

```
<?xml version="1.0" encoding="UTF-8"?>
<bookstore>

  <book category="cooking">
    <title lang="en">Everyday Italian</title>
    <author>Giada De Laurentiis</author>
    <year>2005</year>
    <price>30.00</price>
  </book>

  <book category="children">
    <title lang="en">Harry Potter</title>
    <author>J K. Rowling</author>
    <year>2005</year>
    <price>29.99</price>
  </book>

</bookstore>
```

On the first line you can see the prolog which contains the XML version and encoding. Pro tip if you ever see this in burp you should immediately test for XXE:

```
<?xml version="1.0" encoding="UTF-8"?>
```

Under that you see the *“<bookstore>”* tag which represents the root node. There are two child nodes called *“<book>”* and each of these contain subchild nodes called *“<title>,<author>,<year>,<price>”*.

```
<root>
  <child>
    <subchild>.....</subchild>
  </child>
</root>
```

Thats the basic structure of XML but there is a little more you should know. There is something called document type definition (DTD) which defines the structure and the legal elements and attributes of an XML document as shown below:

```
<?xml version="1.0"?>
<!DOCTYPE note [
<!ENTITY user "Ghostlulz">
<!ENTITY message "got em">
]>

<test><name>&user;</name></test>
```

As shown above there is something called an *ENTITY.* This acts a variable. In this example the entity *“user”* holds the text *“Ghostlulz”*. This entity can be called by typing *“&user;”* and it will be replaced by the text *“Ghostlulz”*.

You can also use something called an external entity which will load its data from an external source. This can be used to get contents from a url or a file on disk as shown below:

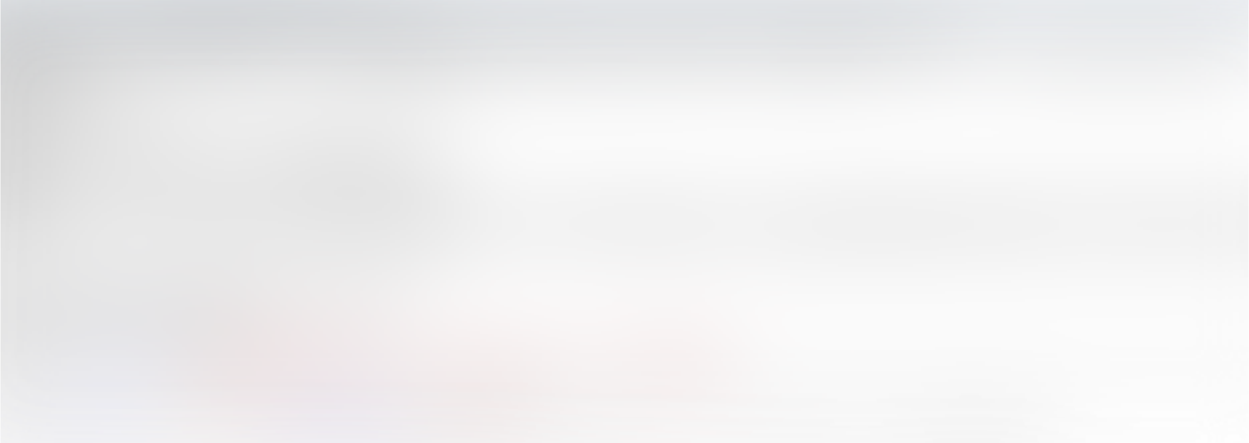
```
<!DOCTYPE foo [ <!ENTITY ext SYSTEM "http://example.com" > ]>

<!DOCTYPE foo [ <!ENTITY ext SYSTEM "file:///path/to/file" > ]>
```

. . .

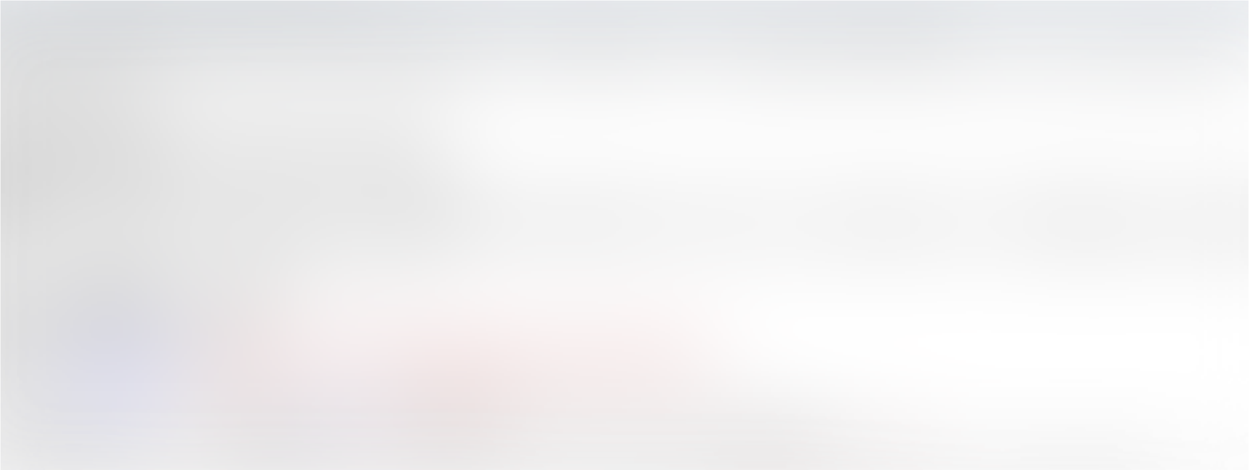
XML External Entity(XXE) Attack

I mentioned that you can use external entities to grab data from a file on disk and store it in a variable. What if we tried to read data from the *“/etc/passwd”* file and store it in a variable? Note that in order to read the data the entity must be returned in the response. Knowing that lets try to exploit our test environment.

While in burp I captured the following POST request which seems to be using XML to send data to the back end system. When ever you see XML you should test for XXE.



To test for XXE simply put in your malicious external entity and replace each node value with it as shown below:



As shown above I created an external entity to grab the data in the */etc/passwd* file and stored it in the entity xxe. I then placed the variable in the *<productID>* node. If the server doesnt block external entities the response will be reflected you. You will then be able to retrieve the contents of the */etc/passwd* file as shown below:

. . .

Conclusion

Most application transmit data using JSON but you may run into applications using XML. When you do make sure to always test for XXE. Abusing this vulnerability allows you to read arbitrary files which can lead to fully compromising a machine. The vulnerable application I used can be found at the web security academy put on by portswigger, its free and their labs are neat:

Web Security Academy

Welcome to the Web Security Academy. This is a brand new learning resource providing free training on web security...

portswigger.net