Asfiya $ha!kh

Follow 434 Followers About

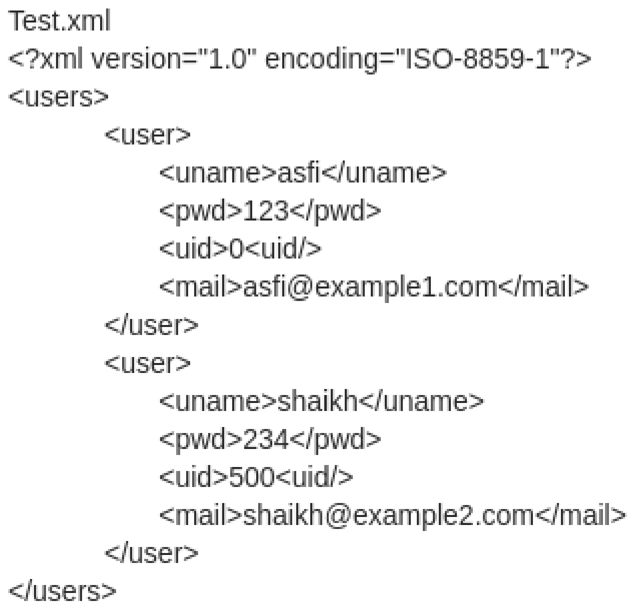
XML Injection

Asfiya $ha!kh Apr 27, 2019 · 3 min read

Hello Pentester, this blog will walk you through how the XML injections are performed and remediated.

XML Injection can be used to compromise the logic of an XML based application or web service. The injection of unexpected XML content into an XML input can change the intended logic of the application. Also, injecting XML tags can cause the insertion of malicious content into the resulting document/database/API/ web service wherever the data is getting stored .

Let's take an example of XML injection:



```
Test.xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
        <user>
             <uname>asfi</uname>
             <pwd>123</pwd>
             <uid>0<uid/>
             <mail>asfi@example1.com</mail>
        </user>
        <user>
             <uname>shaikh</uname>
             <pwd>234</pwd>
             <uid>500<uid/>
             <mail>shaikh@example2.com</mail>
        </user>
</users>
```

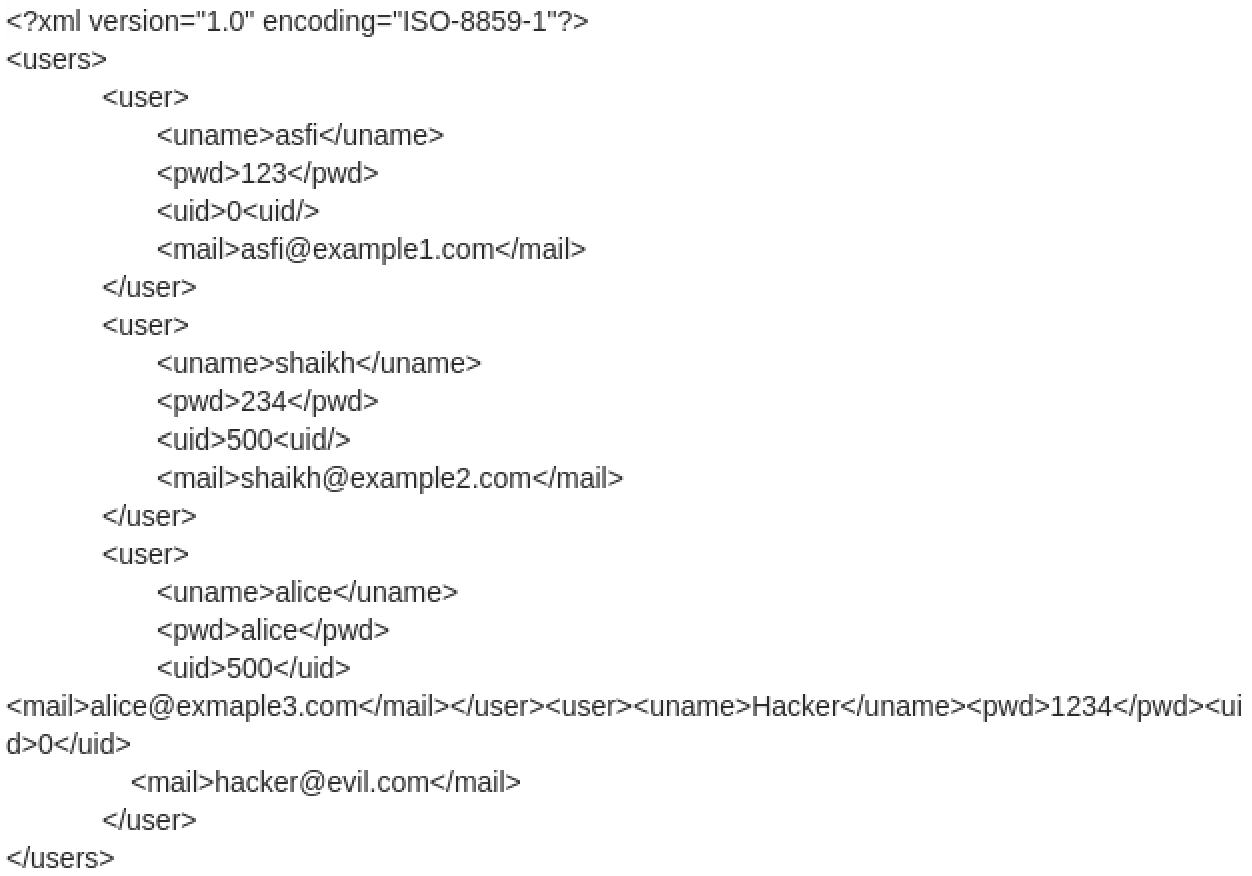
If the attacker injects the following values for a new user in the XML based application fields.

Username: alice

Password: alice

E-mail:alice@example3.com</mail></user><user><uname>Hacker</uname><pwd>1234</pwd><uid>0</uid><mail>hacker@evil.com</mail>

Then the resulting XML document would be:



```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
        <user>
            <uname>asfi</uname>
            <pwd>123</pwd>
            <uid>0<uid/>
            <mail>asfi@example1.com</mail>
        </user>
        <user>
            <uname>shaikh</uname>
            <pwd>234</pwd>
            <uid>500<uid/>
            <mail>shaikh@example2.com</mail>
        </user>
        <user>
            <uname>alice</uname>
            <pwd>alice</pwd>
            <uid>500</uid>
<mail>alice@exmaple3.com</mail></user><user><uname>Hacker</uname><pwd>1234</pwd><ui
d>0</uid>
          <mail>hacker@evil.com</mail>
        </user>
</users>
```

In the example shown above, a new user (Hacker) will be inserted into the table with user ID 0. In most cases, the second user ID instance will override the first. This results in injected new user 'Hacker' being logged in with userid=0 (which is often used as the administrator uid).

Another type of XML injection?

Yeah… There exist.

It’s when CDATA elements are used to insert malicious content.

Let’s take an example — where XML payloads that contain a CDATA field is used to inject illegal characters/content that are ignored by the XML parser.

<HTML>

<![CDATA[<IMG SRC=http://www.exmaple.com/siteLogo.gif onmouseover=javascript:alert(‘XSS’);>]]>

</HTML>

In this example an XML/HTML application can be exposed to XSS. This is possible because the CDATA content is unparsed and hence will be missed by schema based input validation filters.

Discover-

Let’s test the application for XML Injection vulnerability step by step using XML Metacharacters -

1. *Single quote:’*
2. *Double quote:”*
3. *Angular parentheses: > and <*
4. *Comment tag: <! —/→*
5. *Ampersand: &*
6. *CDATA section delimiters: <![CDATA[/]]> OR <![CDATA[**]]>**]]>*

If any of the above test is successful in throwing an exception during XML parsing, then we can proceed for XML tag injection.

Let me explain why parsing error will be thrown-

Suppose we are inserting single quotes, injected value will be the part of an attribute value in tag.

<node attribute=’$input’/>

So if input is foo’

input = foo’

then it will be inserted as shown below

<node attribute=’foo”/>

Making XML document as not well formed and causing the XML parsing error.

Most famous examples of XML injections are

1. *Modification of payment data — Violation of Integrity*
2. *Unauthorised admin login by overriding uid — Violation of Access Control*

Remediation-

The application must validate or sanitize the user input(security rule zero) before taking it into an XML document or SOAP web service. We can block any input containing XML metacharacters such as < and >. Also, these characters can be replaced with entities such as &lt; and &gt;

References-

Testing for XML Injection (OTG-INPVAL-008) - OWASP

This section describes practical examples of XML Injection. First, an XML style communication will be defined and its…

www.owasp.org

XML injection

XML or SOAP injection vulnerabilities arise when user input is inserted into a server-side XML document or SOAP message…

portswigger.net

Cybersecurity Penetration Testing Hacking Owasp Xml