

Forum:[Hack Forums](#)

Thread: [XXE Vulnerability and Application](#)

Prisoft - April 18, 2021, 9:20 am

What?

XXE vulnerability is triggered when a specially defined XML entity is called while the server (server-side software) parses XML data.

Why it originates

Almost all XXE vulnerabilities occur because the application's XML parsing library supports potentially dangerous XML features that the application does not need or intended to use. The easiest and most effective way to prevent XXE attacks is to disable these features.

How to avoid

You can update the versions of all XML processors and libraries used in the application.

You can disable Document Type Definition (DTD) processing in XML parsers.

In XML documents, you can apply a whitelist server-side input validation or filtering process to prevent externally entered data.

SAST tools can help detect XXE in source code, but manual code inspection is the best alternative in large, complex applications with many integrations.

You can use less complex data formats such as JSON.

Orenk XXE

Bwapp Application

Yes, first of all, we go to our bwapp application and select the XXE gap, we will see such a section.

Yes, we will open a burp suite at the back, after opening we will have to open Intercept. After saying on, Any Bugs? we can press in place.

Yes, as you can see, these are the things we have to do. Right click>> Send To Repeater

After we said it, this is what we need to do here, we will use the payload, you can use the payload that I use.

```
Code <!DOCTYPE root [
<!ENTITY bvap SYSTEM "file: /// etc / passwd" gt;
] gt;
```

The DOCTYPE we write here provides some information and enables the browser to read the xml

document.

ENTITY allows to define the value of the data.

If this payload does not work, we have given the name bvap at the entity site, here bvap to run the login section; we will write and we will say send

Yes, we got what we wanted, the etc password part came out and you can reach them by making them.