PEN20230001: XXE in Test Shop

Asset	CWE	Severity (CVSS v3.1 Base Score)	CVSS v3.1 Vektor
Test Shop	CWE-611	Critical (9.1)	*CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N*

Description

This type of vulnerability arises, if an application processes XML and is configured to support external entities.

Exemplary Payload:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE abcd [ <!ENTITY xxe SYSTEM "file:///etc/passwd"> ]>
<example>
    <item>&xxe;</item>
</example>
```

Recommendation

It is recommended to completely disable external entities (DTDs). Further guidance can be found in OWASP's *XML External Entity Prevention Cheat Sheet*.

References

- OWASP: XML External Entity (XXE) Processing