Lab name: [Exploiting XXE using external entities to retrieve files](https://portswigger.net/web-security/xxe/lab-exploiting-xxe-to-retrieve-files)

Severity: High

Lab description:

* This lab shows how an XML External Entity (XXE) vulnerability can be used to read files from the server.
* The server parses XML input from the user without disabling external entities.
* An attacker can define an entity that points to a file (e.g., /etc/passwd) and include it in the XML.
* When processed, the server reads the file and sends its content back in the response.

Impact:

* Attackers can read sensitive files from the server (e.g., password files, config files).
* This can expose usernames, system settings, API keys, or credentials stored in the server.
* In some cases, this may lead to remote code execution or privilege escalation.
* If combined with other vulnerabilities, it can allow full server compromise.
* It can also help attackers gather information for further attacks.
* Users and developers are usually unaware of the file being read and leaked.

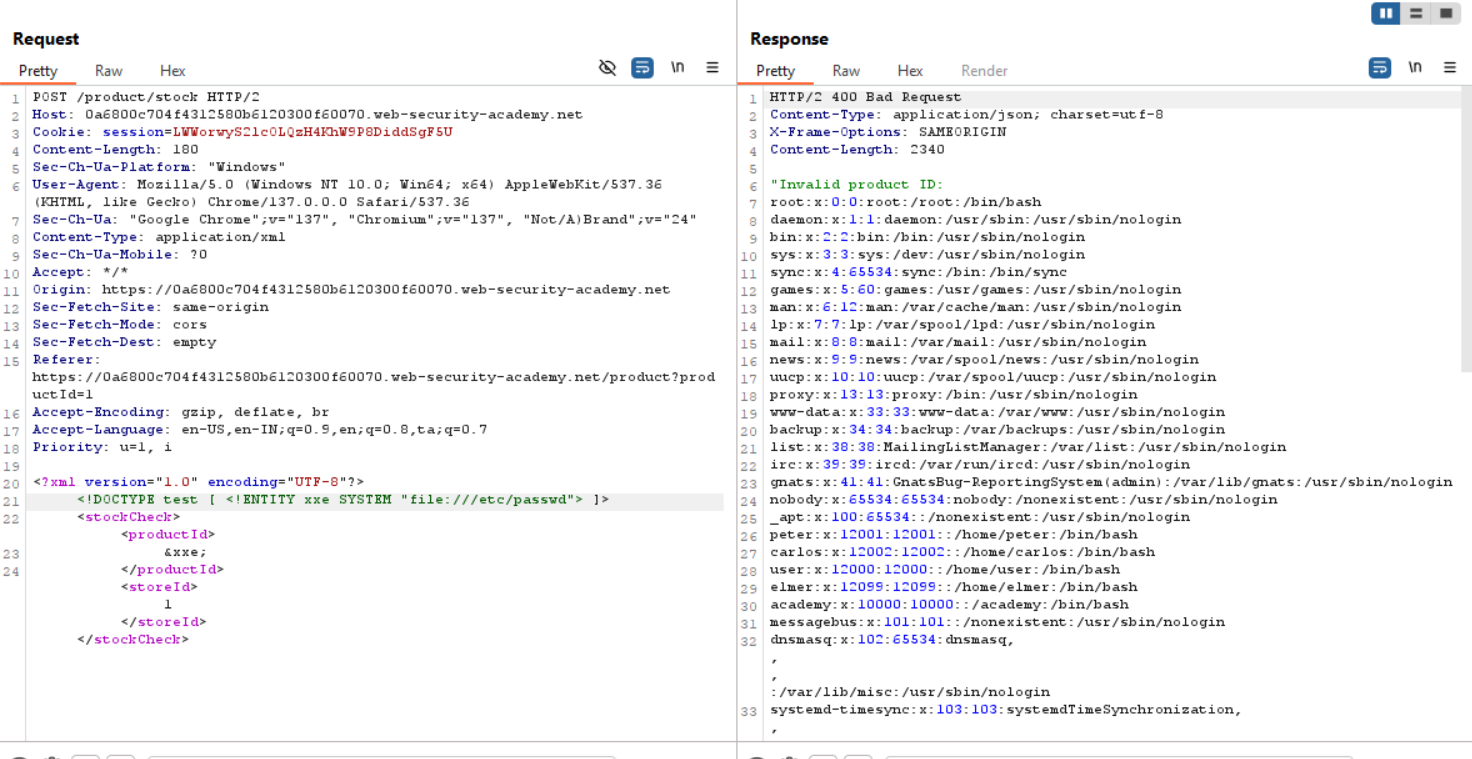
Recommendations:

* Disable support for external entities and DTDs in XML parsers (e.g., in Java, Python, .NET, etc.).
* Use simple data formats like JSON instead of XML where possible.
* Validate and sanitize all user-supplied input before processing.
* Use secure XML libraries or configurations that prevent XXE by default.
* Apply the principle of least privilege to limit file access on the server.
* Monitor logs for unusual XML input or access to unexpected files.

Steps to reproduce:

1. Open the lab and go to the "Check stock" feature (which sends XML via POST).
2. Intercept the request using Burp Suite.
3. Modify the XML to include a DOCTYPE and external entity like:

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

1. Replace <productId> value with &xxe; in the XML body.
2. Forward the request and check the response for file content (e.g., /etc/passwd).
3. The file contents are shown, the lab is solved — the server is vulnerable to XXE.