BLACKSTONE REPORT TOOL

Informe de Pentesting para
TryHackMe

Fecha: 2025-11-16
Nombre del documento: Pickle Rick

Pentesting Report
Generated by BlackStone

1 INTRODUCCIÓN

Durante las pruebas se simulan las actividades que realizaría un atacante real, descubriendo las vulnerabilidades, su nivel de riesgo, y generando recomendaciones que permitan al cliente realizar la remediación de estas. En cada sección de este informe se detallan los aspectos importantes de la forma en que un atacante podría utilizar la vulnerabilidad para comprometer y obtener acceso no autorizado a información sensible. Se incluyen además directrices que al ser aplicadas mejoraran los niveles de confidencialidad, integridad y disponibilidad de los sistemas analizados.

1.1 OBJETIVO

El objetivo de la evaluación de seguridad es detectar las vulnerabilidades de seguridad existentes en los sistemas analizados para posteriormente generar un informe con los hallazgos y recomendaciones que permitan la remediación de estas.

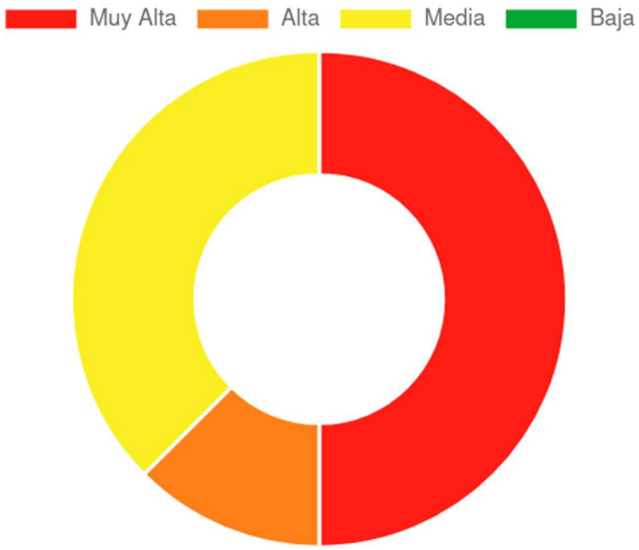
1.2 ALCANCE

La evaluación realizada se ha centrado en los objetivos aprobados en el alcance del contrato, en el cual se establece:

No.	Objetivos
1	Mapear la superficie de ataque
2	Enumerar la aplicación web
3	Obtener acceso al portal web mediante credenciales válidas
4	Identificar y explotar vulnerabilidades
5	Obtener acceso al sistema
6	Acceder a los ficheros que contienen los “ingredientes”

2 RESUMEN EJECUTIVO

Tienes que capturar pantalla de este gráfico para insertarlo dentro del Word.



vulnerabilidad	Cantidad	Porcentaje
Muy Alta	4	50%
Alta	1	12.5%
Media	3	37.5%
Baja	0	0

3 RESULTADO DE LAS PRUEBAS

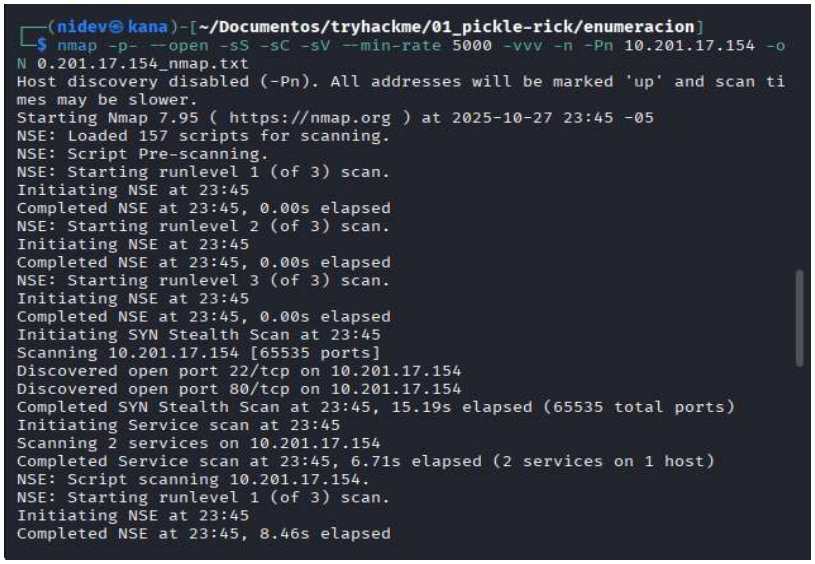
3.1 Detalles de los objetivos

Mapear la superficie de ataque

Nombre: Puertos y servicios identificados
Criticidad: Media

Descripción

Se realizo un mapeo de puertos y servicios con la herramienta nmap



Aquí agregar captura de nmap mostrando el puerto 80 y 22 abiertos

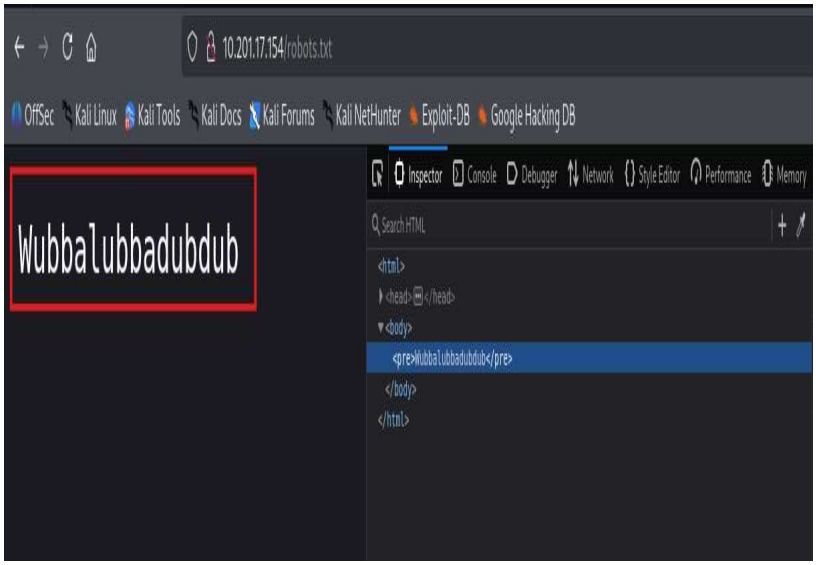
Recomendación:

Enumerar la aplicación web

Nombre: A05 – Security Misconfiguration
Criticidad: Alta

Descripción

El archivo /robots.txt contiene información crítica expuesta, incluyendo la cadena que es utilizada como contraseña del login.



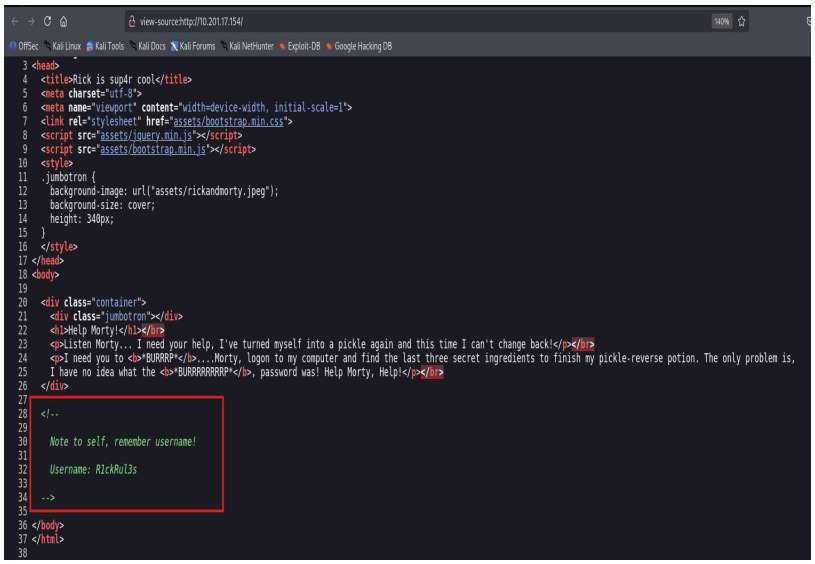
captura de /robots.txt

Recomendación: Nunca almacenar credenciales en rutas accesibles. Configurar reglas adecuadas para controlar la exposición de estos archivos.

Nombre: A01 – Broken Access Control / Information Disclosure
Criticidad: Media

Descripción

Se encontraron credenciales expuestas en el código fuente de la página principal. Esto permite a un atacante autenticarse en el sistema sin necesidad de técnicas adicionales.



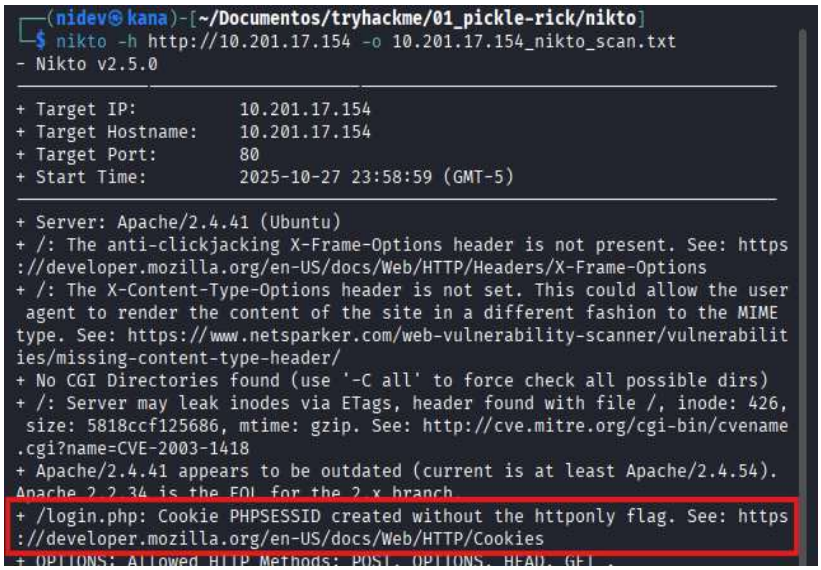
captura del código fuente con el comentario HTML del /login

Recomendación: Eliminar comentarios que revelen información sensible. Implementar procesos de revisión de código antes de despliegue.

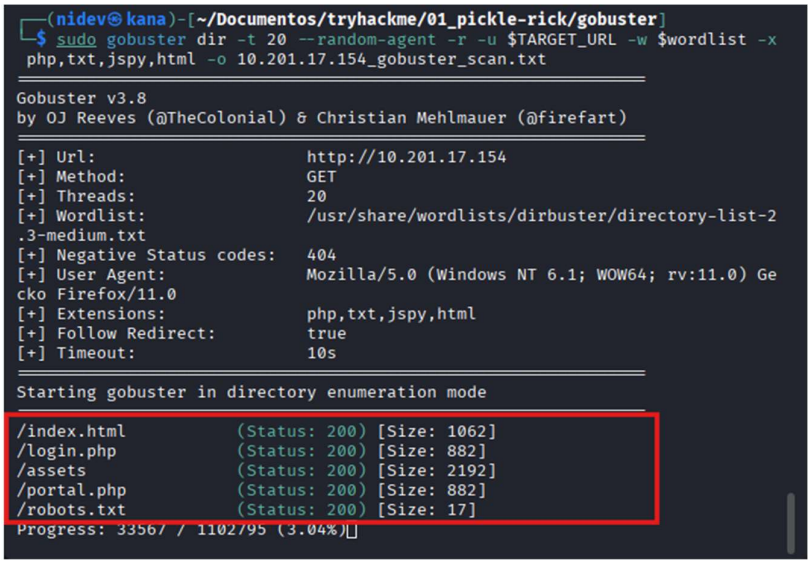
Nombre: A01 – Broken Access Control
Criticidad: Media

Descripción

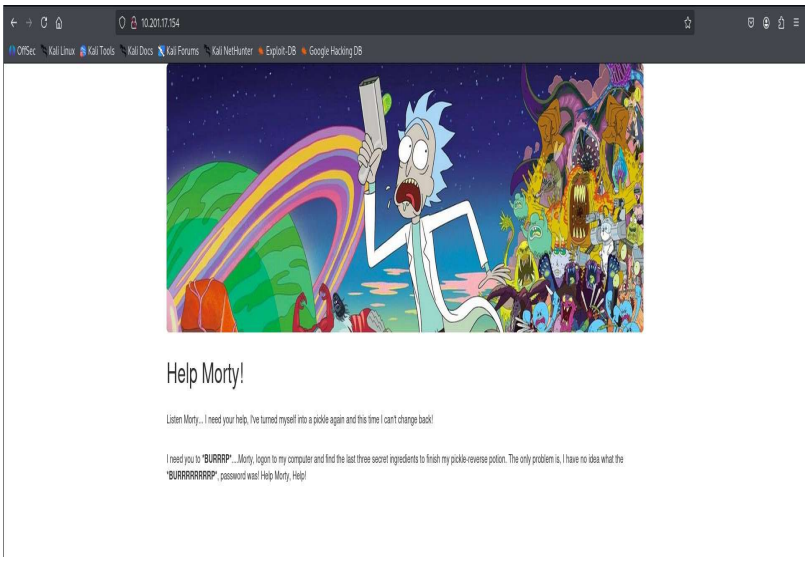
Gobuster reveló rutas sensibles y funcionales como /portal, /login.php, /assets, entre otras. Esto facilita la identificación de puntos de entrada adicionales.



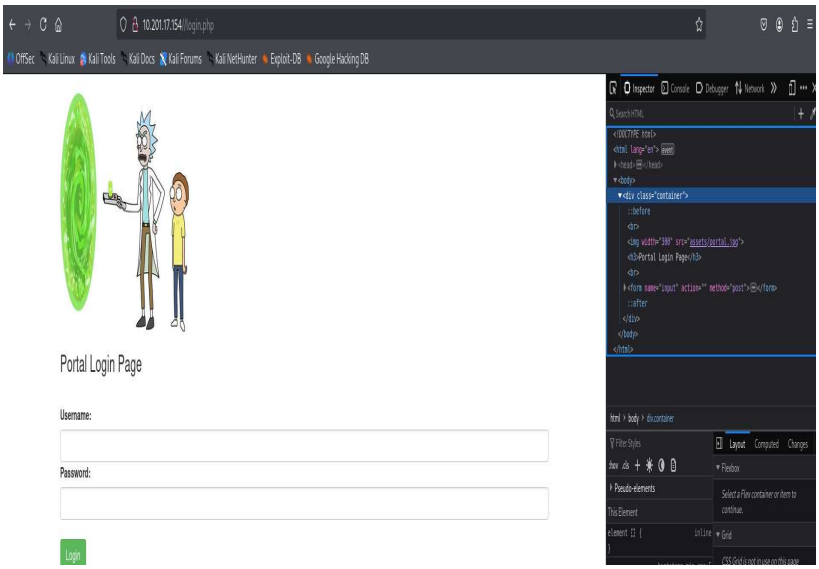
se realizon una enumeracion con nikto pero no nos da mucha informacion solo encontramos un /login.php donde encontramos el usuario "R1ckRul3s"



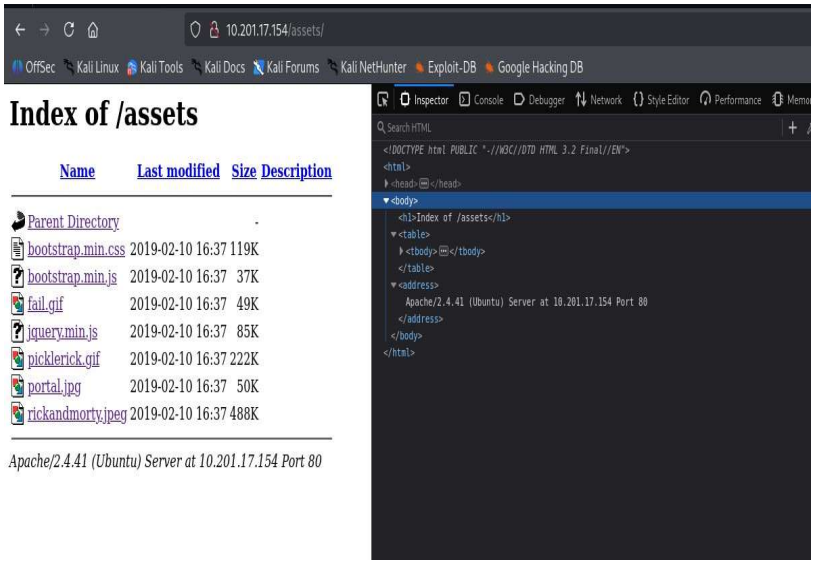
salida de gobuster, mostrando algunos resultados



captura de /index.html



captura de /login.html



captura de /assets

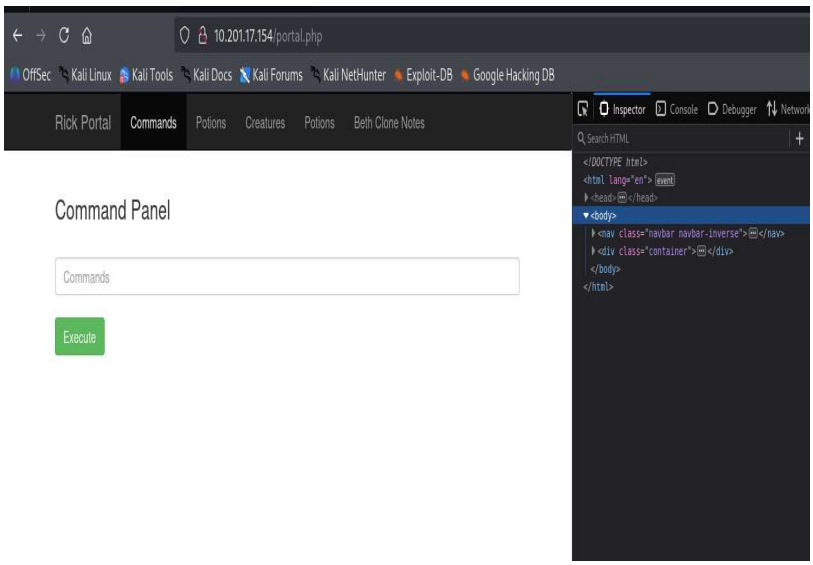
Recomendación: Limitar el acceso a rutas internas y archivos mediante autenticación o moviéndolos fuera del directorio público.

Obtener acceso al portal web mediante credenciales válidas

Nombre: Ingreso exitoso con credenciales
Criticidad: Muy Alta

Descripción

Usuario: R1ckRul3s Contraseña: Wubbalubbadubdub



captura de login exitoso dentro del sistema.

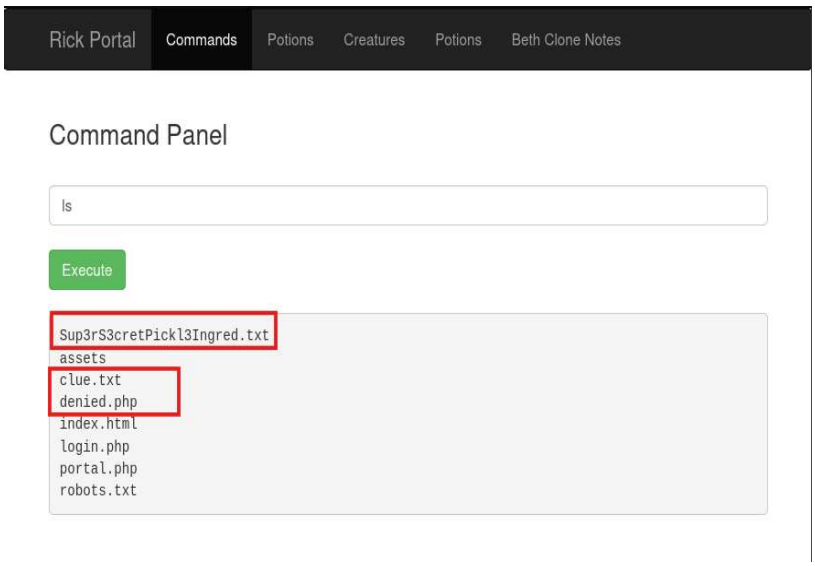
Recomendación: No se considera vulnerabilidad adicional más allá de las expuestas anteriormente.

Identificar y explotar vulnerabilidades

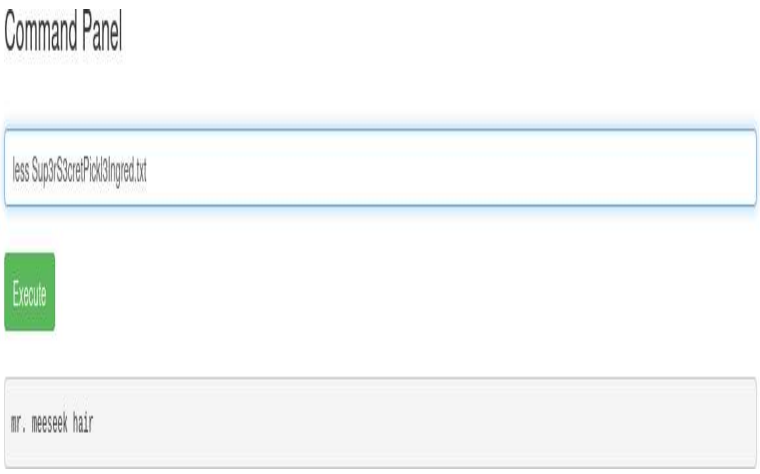
Nombre: A03 – Injection
Criticidad: Muy Alta

Descripción

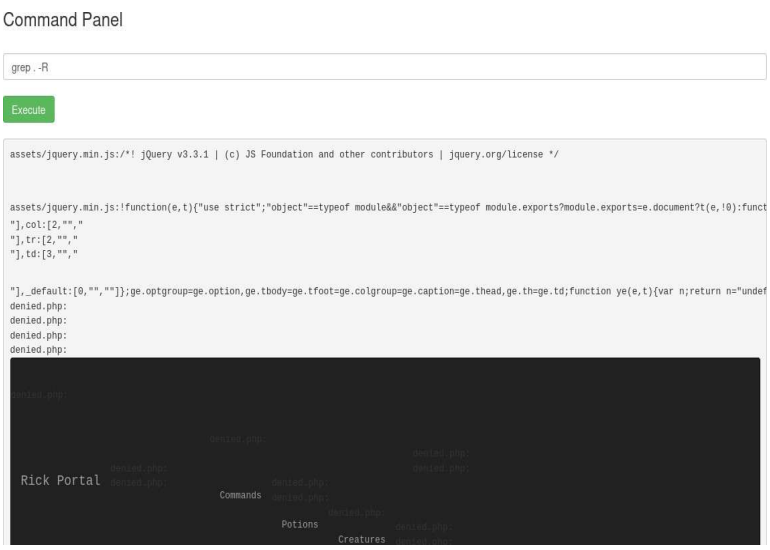
El "Command Panel" permite ejecutar comandos del sistema sin sanitización adecuada. Aunque existe una blacklist, esta no bloquea todos los comandos (grep, ls, cat, etc.), lo que permite explorar directorios y archivos sensibles.



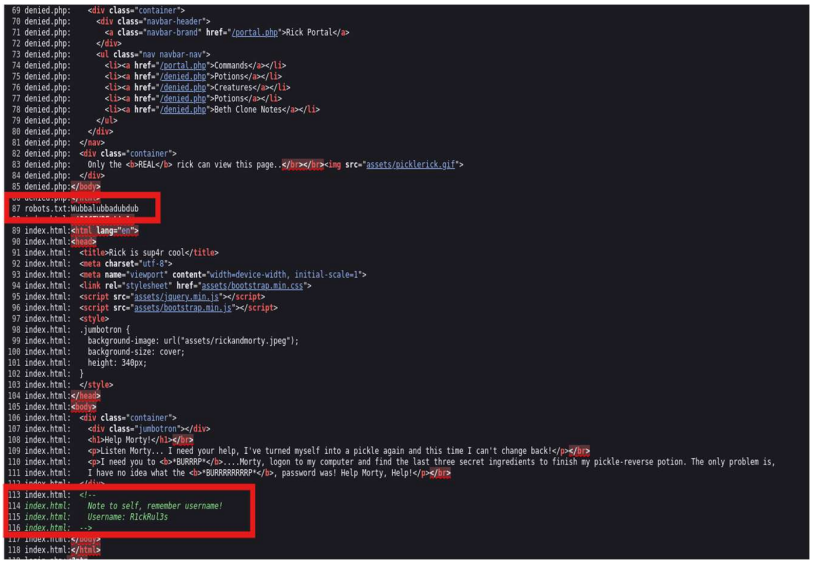
pantalla ejecutando un ls en commad panel



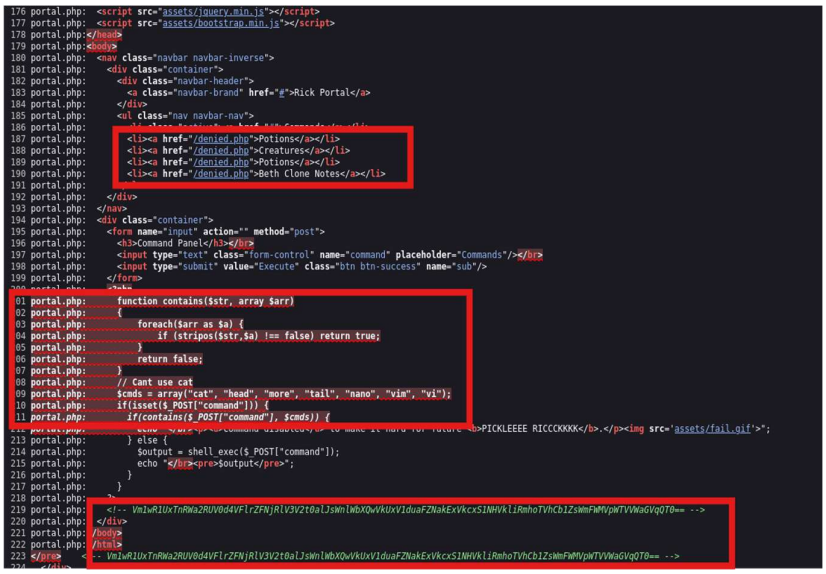
ejecutando la lectura de archivo Sup3rS3cretPickl3Ingred.txt y encontramos el 1er ingrediente



pantalla ejecutando una busqueda recursiva con gred en commad panel

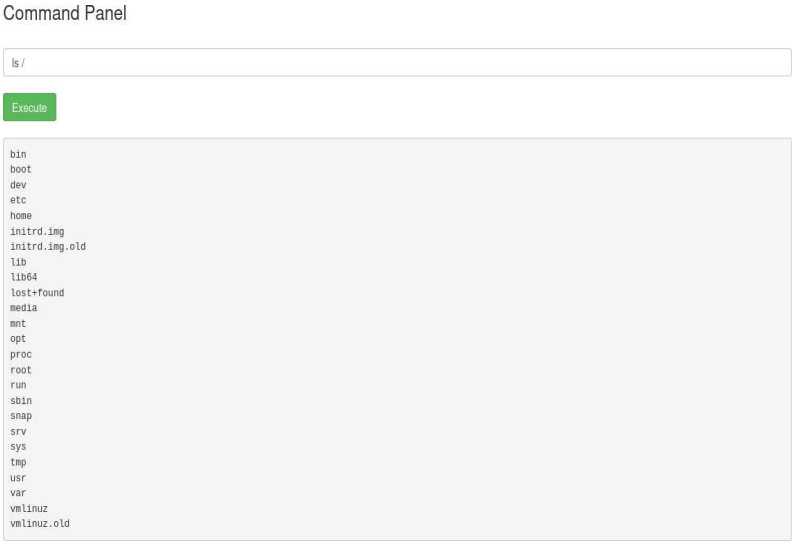


analisis del codigo encontramos el usuario y contraseña

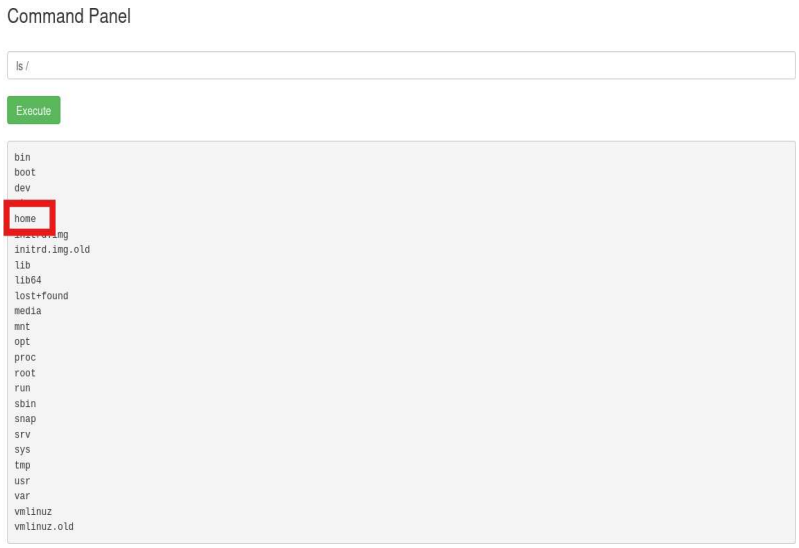


encontramos la lista negra de comandos

se analiza el archivo clue.txt



se trara de listar el directorio raiz ls /



encontramos que podemos acceder a directorio home y listar los usuarios

listamos los usuarios de /home

encontramos el archivo del segundo ingrediente

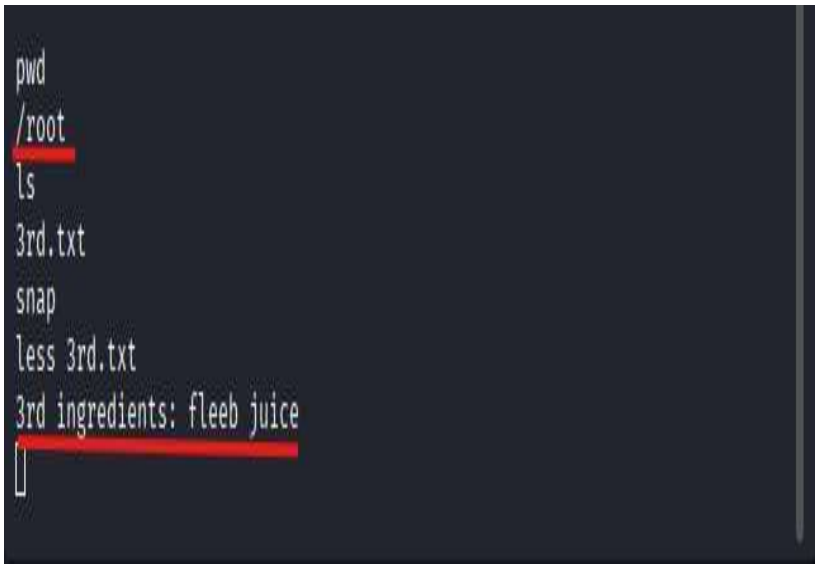
Recomendación: - Implementar validación estricta del input (whitelist). - Deshabilitar funciones de sistema en backend: exec(), shell_exec(), system(). - Aislar el backend en un sandbox o contenedor.

Obtener acceso al sistema

Nombre: A03 – Injection → Command Injection → RCE
Criticidad: Muy Alta

Descripción

La vulnerabilidad del Command Panel permite ejecutar una reverse shell usando bash, brindando acceso completo al sistema víctima.



ejecucion de reverse shell desde la manquina victima y acceso

interaactivo al sistema

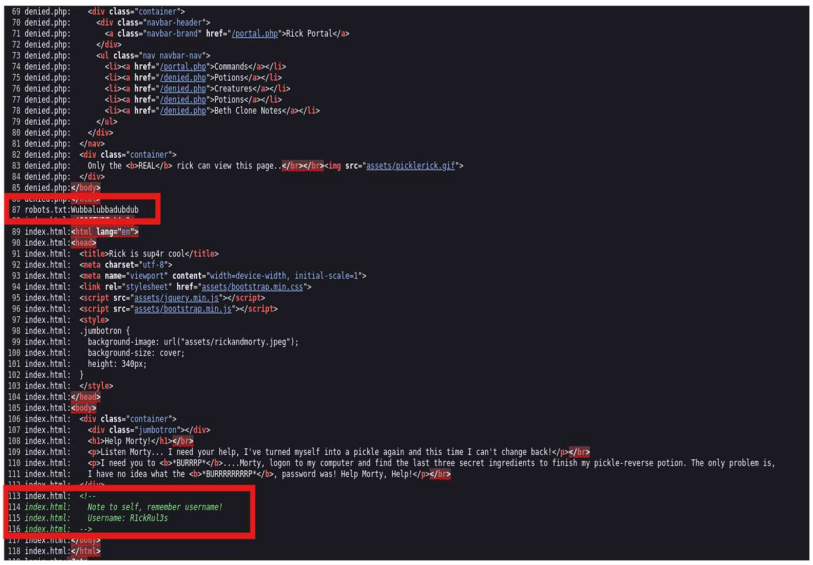
Recomendación: - Mitigar la inyección de comandos (ver vulnerabilidad anterior). - Restringir funciones peligrosas. - Añadir mecanismos de aislamiento (chroot, RBAC, AppArmor).

Acceder a los ficheros que contienen los “ingredientes”

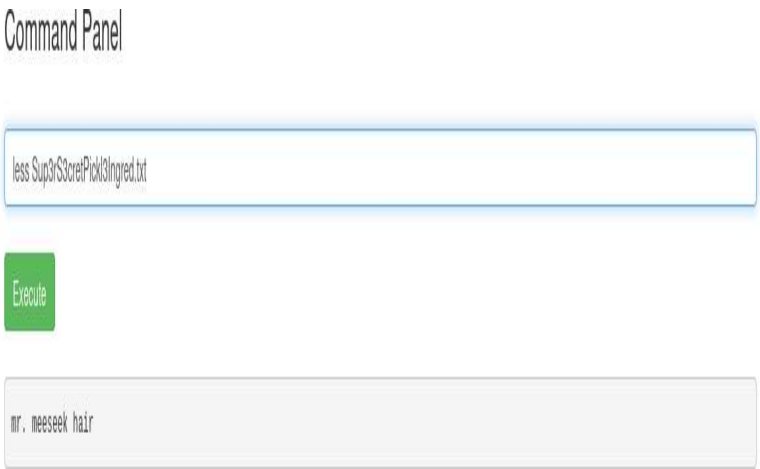
Nombre: Recolección de información
Criticidad: Muy Alta

Descripción

Accediendo con shell inversa y exploración del sistema se identificaron los 3 y usuario y contraseña para acceder al sitio



encontrando el usuario y contraseña para el acceso a /portal.php



mr. meeseek hair

1 jerry tear

fleeb juice

Recomendación:

---

4 Tabla de criticidad

Mapear la superficie de ataque

Nombre	Criticidad
Puertos y servicios identificados	Media

Enumerar la aplicación web

Nombre	Criticidad
A05 – Security Misconfiguration	Alta
A01 – Broken Access Control / Information Disclosure	Media
A01 – Broken Access Control	Media

Obtener acceso al portal web mediante credenciales válidas

Nombre	Criticidad
Ingreso exitoso con credenciales	Muy Alta

Identificar y explotar vulnerabilidades

Nombre	Criticidad
A03 – Injection	Muy Alta

Obtener acceso al sistema

Nombre	Criticidad
A03 – Injection → Command Injection → RCE	Muy Alta

Acceder a los ficheros que contienen los “ingredientes”

Nombre	Criticidad
Recolección de información	Muy Alta

5 Conclusiones

El sistema evaluado presenta múltiples fallas de configuración y validación que permiten comprometerlo completamente. Se pudo: - Acceder al portal mediante credenciales expuestas - Ejecutar comandos del sistema mediante inyección - Obteneer un reverse shell y acceso total - Acceder al directorio /root - Extraer todos los ingredientes requeridos Es fundamental aplicar las recomendaciones mencionadas y reforzar la seguridad del entorno.