



21-3-2017

Análisis de vulnerabilidad de wordpress



Elaborado por: Galindo Díaz Sergio Iván

Resumen:

En el presente documento de auditoría técnica de seguridad informática, se muestra los resultados finales de las vulnerabilidades del Servidor Manejador de Contenidos (CMS), conocido como "Wordpress".

Objetivos:

Este análisis tiene como objetivo detectar las vulnerabilidades presentes del CMS y dar a conocer los tipos de ataques que se presentan, para poder en un futuro disminuir los incidentes y poder mermar esas vulnerabilidades.

Alcance:

Nuestro análisis se enfoca en la búsqueda de vulnerabilidades presentes en wordpress, para poder ser notificadas y dar una posible solución, con el fin de disminuir riesgos en la empresa.

Hallazgos:

Se realizó un escaneo con nmap, para encontrar servicios activos.

Se realizó un ingreso al login de la aplicación

Se analizó contra contraseñas más comunes, siendo esta la principal fuente de vulnerabilidad

Se encontró la vulnerabilidad de Cross-Site-Scripting

Recomendaciones:

Al configurar las aplicaciones hay que tomar en cuenta que las contraseñas deben cambiarse.

Tener configurado el firewall para impedir conexiones no deseadas

Validar los datos introducidos por los usuarios

Negar el servicio si el tiempo de logueo dura más de 10 min.

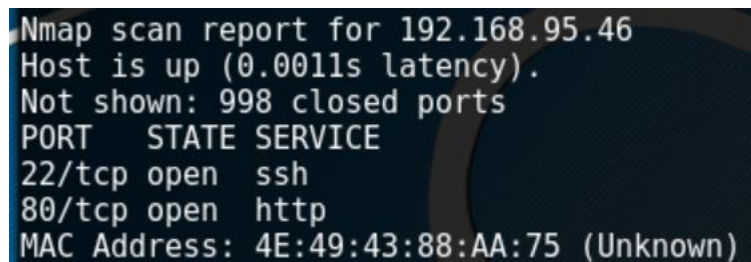
Evitar que se pueda escalar privilegios dentro de la aplicación

Si es el servicio no va estar en uso deshabilitarlo

Generar bitácoras.

Anexos:

Escaneo de puertos con NMAP



```
Nmap scan report for 192.168.95.46
Host is up (0.0011s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 4E:49:43:88:AA:75 (Unknown)
```

Loguin de la aplicación mediante la siguiente dirección 192.168.95.46/wordpress/wp-login.php e ingreso a la misma mediante el uso de contraseñas más frecuentes.

Lel

Username

Password

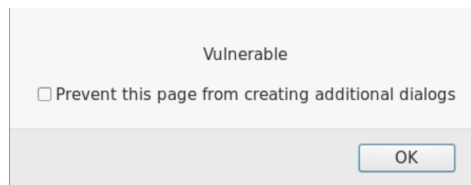
☐ Remember Me

[Lost your password?](#)

[← Back to Lel](#)

Vulnerabilidad cross-site-scripting

```
<li>  
<a href="http://wordpress.local/wordpress/index.php/2017/03/21/alertvulnerable/"><script>alert("Vulnerable")</script></a>  
.. </li>  
..
```



<https://nvd.nist.gov/CVSS/v3-calculator>