INFORME DE PENTESTING

WordPress – CVE-2021-29447 (XXE → RCE)

1. Resumen Ejecutivo

Se ha identificado y explotado con éxito la vulnerabilidad CVE-2021-29447 en WordPress (versiones 5.6–5.7 ejecutándose sobre PHP 8). Esta vulnerabilidad de tipo XML External Entity (XXE) permite la lectura arbitraria de archivos del sistema y potencialmente ataques de tipo SSRF. Durante la prueba se logró: - Obtener el archivo crítico wp-config.php. - Extraer credenciales de base de datos MySQL. - Acceder a la base de datos y recuperar hashes de usuario. - Crackear credenciales mediante Hashcat. - Obtener una reverse shell en el sistema comprometido.

2. Alcance y Objetivo

Objetivo: Comprometer la máquina explotando la vulnerabilidad XXE en WordPress y demostrar impacto real mediante acceso remoto. Fases realizadas:

- Explotación XXE.
- Obtención de credenciales desde wp-config.php.
- Acceso a base de datos MySQL (puerto 3306).
- Extracción y crackeo de hash WordPress (phpass).
- Obtención de reverse shell.
- Confirmación de compromiso total del sistema.

3. Hallazgos Técnicos

Vulnerabilidad identificada: CVE-2021-29447 (XML External Entity). Base de datos detectada: MySQL 5.7.33 (puerto 3306). Credenciales extraídas desde wp-config.php:

- DB_NAME: wordpressdb2
- DB_USER: thedarktangent
- DB_PASSWORD: sUp3rS3cret132

4. Explotación

1. Creación de servidor PHP local para exfiltración. 2. Generación de DTD malicioso. 3. Subida de archivo WAV con entidad XML manipulada. 4. Lectura de wp-config.php. 5. Conexión a MySQL

con credenciales obtenidas. 6. Extracción del hash del usuario corp-001.

5. Crackeo de Hash

Hash identificado: PB4fu6XVPkSU5KcKUsP1sD3Ul7G3oae1 Tipo: WordPress (phpass – MD5). Herramienta: Hashcat. Modo: 400. Diccionario utilizado: rockyou.txt. Contraseña en texto plano: teddybear.

6. Acceso Remoto

Se modificó el plugin desactivado “Hello Dolly” para insertar una reverse shell en PHP. Se configuró un listener con Netcat y se ejecutó el plugin modificado. Se obtuvo acceso remoto con privilegios del usuario www-data.

7. Evidencia

Flag obtenida: thm{28bd2a5b7e0586a6e94ea3e0adbd5f2f16085c72}

8. Recomendaciones de Seguridad

- Actualizar WordPress a la última versión estable.
- Deshabilitar entidades externas en el parser XML.
- Restringir permisos de subida de archivos.
- Proteger y restringir acceso a wp-config.php.
- Implementar WAF y monitoreo continuo de logs.
- Aplicar principio de mínimo privilegio en base de datos.