Proyecto 1 Hack-Proof Inc.

Pablo Painceiras Martínez

Mayo 29, 2024

Índice

Introducción

En ciberseguridad, las vulnerabilidades en aplicaciones web son fallos que permiten ataques como inyecciones SQL, XSS y fallos de autenticación. Identificarlas y mitigarlas es crucial para proteger los datos y servicios web.

Selección de vulnerabilidades - Bases de datos de CV, NVD, ExploitDB y OWASP - Informes Symantec y McAfee

CVE-2018-7600 - Drupalgeddon 2

- Fecha de Publicación: 29/03/2018
- CVSS v3.1 Vector : AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Score: 9.8
- CWE-94: Mal control de generación de código ('Code Injection')
- Severidad: Crítica
- Descripción: Permite a los atacantes remotos ejecutar código arbitrario en Drupal.
- Versiones afectadas: Anteriores a la 7.58, 8.x anteriores a la 8.3.9, 8.4.x anteriores a la 8.4.6 y 8.5.x anteriores a la 8.5.1
- Solución: Actualización de Drupal

CVE-2020-28035 - WordPress XML-RPC

- Fecha de Publicación: 03/11/2020
- CVSS v3.1 Vector:/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Score: 9.8
- CWE-264: Debilidad en el manejo de permisos, privilegios y otras características de seguridad para el control de acceso.
- Severidad: Crítica
- Descripción: Permite a los atacantes obtener privilegios a través del protocolo XML-RPC en - WordPress.
- Versiones afectadas: Antes de la versión 5.5.2
- Solución: Actualización de plugins

CVE-2022-23795 - Joomla!

- Fecha de Publicación: 30/03/2022
- CVSS v3.1 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Score: 9.8
- CWE-287 Autenticación inadecuada
- Severidad: Crítica
- Descripción: Vulnerabilidad de autenticación inadecuada en Joomla!
- Solución: Actualizar a las versiones 4.1.2 o 3.10.8

Conclusión

- En ciberseguridad, identificar y mitigar vulnerabilidades en aplicaciones web es crucial para proteger datos y servicios. Este proyecto ha analizado vulnerabilidades críticas en sistemas y plataformas populares como Drupal, WordPress y Joomla.
- Las vulnerabilidades en aplicaciones web representan una seria amenaza para la seguridad de los sistemas. Inyecciones de código, fallos en gestión de sesiones y problemas de autenticación son vectores comunes. Mitigarlas requiere buenas prácticas de desarrollo, monitoreo y actualizaciones regulares.

Recomendaciones

- Implementar controles de seguridad como OWASP ESAPI.
- Mantener actualizados sistemas y aplicaciones.
- Realizar auditorías de seguridad y usar herramientas de escaneo.
- Capacitar continuamente a los desarrolladores sobre amenazas y técnicas de mitigación