VELKRO PRIVATE TEAM

22/08/2023

v1.0

Resumen

Se descubrió una vulnerabilidad crítica de ejecución remota de código en el sitio web, una vulnerabilidad de Cross-Site Scripting (XSS) en áreas del sitio web donde los datos de entrada del usuario no son debidamente filtrados y se informa de un vector de ataque que puede ser importante para la fase de reconocimiento de los ciberdelincuentes.

Recuento de vulnerabilidades en función de su severidad:

CRÍTICO	ALTO	MEDIO	BAJO	INFORMATIVO
1	0	1	0	1

Tabla de contenidos

Las limitaciones que se presentaron fueron:

- No se puedo explorar más vectores de ataque debido a la falta de accesos.

- Se tuvo un periodo de tiempo limitado para la exploración y explotación de las vulnerabilidades.

- No se pueden brindar recomendaciones exhaustivas y/o profundizadas debido al límite de conocimiento interno organizacional que dispone el equipo de auditoria sobre el entorno.

Se realizó la prueba de penetración como “Black-Box”.

El equipo de auditoría informa que este reporte enumerará exclusivamente las vulnerabilidades encontradas para el objetivo que se buscaba explotar, y únicamente dentro del alcance de "securgo.com/*". Esto no implica que sea un informe completo de todas las vulnerabilidades pasadas, presentes o futuras que pueda tener la aplicación en cuestión.

Periodo de auditoría y personal involucrado

El equipo de auditoria se conforma por los siguientes integrantes:

SaXX [1] - Ven1n [2] - DoXiLaA [3]

Fecha de inicio: 17/08/2023 - Fecha de finalización: 21/08/2023

Última revisión del reporte: 26/08/2023

Calificación de riesgo

La metodología de calificación de riesgo que se utilizará en este reporte será el “OWASP Risk

Rating” [4] el cuál evalúa el riesgo, estimación de probabilidad de ataque, estimación de impacto, severidad del riesgo, decidir qué solucionar y finalmente dar paso al auditor a personalizar su propia calificación de riesgo a su medida.

Reconocimiento

Nombre: Nessus. [5]

Descripción: Durante la fase de reconocimiento, se utilizó la herramienta de escaneo de seguridad Nessus para identificar posibles vulnerabilidades en el sitio web. A través de análisis de los resultados, se detectó un punto de entrada en el sistema que permitiría a un atacante ejecutar código malicioso de manera remota.

Nombre: Burp-Suite Professional. [6]

Descripción: Durante el análisis de seguridad, se utilizó la herramienta de escaneo web Burp Suite para explorar posibles vulnerabilidades. Se descubrió que ciertas páginas del sitio web no sanitizaban adecuadamente la entrada del usuario, lo que podría permitir ataques de Cross-Site Scripting (XSS).

Observaciones

Ejecución Remota de Código (RCE)

1.1

Nombre: RCE en Uploader

Descripción: Esta vulnerabilidad se origina en un punto de entrada no adecuadamente protegido en la aplicación web, lo que permite al atacante manipular datos de manera que los comandos maliciosos sean interpretados y ejecutados por el servidor.

Detalle del negocio: El contexto del ataque se basa en un usuario autenticado en el sistema con privilegios normales. La vulnerabilidad se encuentra en una función de carga de archivos, donde un atacante puede cargar un archivo con código malicioso, que posteriormente se ejecutaría en el servidor.

Riesgo: Impacto: 7.5 (Alto) – Riesgo Global: 8.0 (Crítico)

CVE: CVE-2023-5678 [7]

CVSS: CVSS:4.0/AV:A/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/S:U

Tipo de vulnerabilidad: RCE

Categoría: Ejecución de código remoto

Ubicación de explotabilidad: “securgo.com/upload”

Impacto real: Compromiso completo del servidor, posible robo de datos sensibles.

Impacto mínimo: Acceso no autorizado a ciertas áreas del servidor.

Impacto máximo: Control total del servidor y filtración de información confidencial.

Pasos a seguir:

- Se identificó una función de carga de archivos en el sitio web.

- Se creó un archivo malicioso que contenía comandos de ejecución de código.

- El archivo malicioso se cargó en la función de carga de archivos.

- Mediante la manipulación de parámetros, se ejecutó el código malicioso en el servidor.

Escenarios de riesgo:

- Un atacante podría tomar el control del servidor y realizar modificaciones no autorizadas en el sitio web, afectando la integridad de la información, con respecto al negocio, el atacante podría modificar información sensible almacenada dentro de los servidores y así generar pérdidas económicas de soporte y/o seguridad.

- Datos sensibles almacenados en el servidor podrían ser robados y utilizados con fines maliciosos, con respecto al negocio, el atacante podría filtrar información clasificada de la organización generándole infracciones monetarias.

Recomendaciones:

- Parchear y actualizar la aplicación para corregir esta vulnerabilidad.

- Implementar una revisión de código y pruebas de seguridad regulares para identificar y corregir posibles problemas de seguridad.

Cross-Site Scripting (XSS)

1.2

Nombre: XSS en formulario de comentarios

Descripción: Permite a un atacante insertar y ejecutar código malicioso en las páginas web vistas por otros usuarios.

Detalle del negocio: La vulnerabilidad se encuentra en formularios de comentarios donde los usuarios pueden ingresar texto. Un atacante podría insertar código malicioso en los comentarios que se ejecutaría en el navegador de otros usuarios que vean esos comentarios.

Riesgo: Impacto: 5.3 (Medio) – Riesgo Global: 6.0 (Medio)

CVE: CVE-2023-6789 [8]

CVSS: CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:R/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/S:C

Tipo de vulnerabilidad: XSS

Categoría: Inyección de código / Cookies desprotegidas

Ubicación de explotabilidad: “ securgo.com/noticias/* ”

Impacto real: Inyección de código en páginas visitadas por otros usuarios.

Impacto mínimo: Inyección de código en la sesión del propio usuario.

Impacto máximo: Robo de cookies y datos personales de usuarios.

Pasos a seguir:

- Se identificó un formulario de comentarios que no sanitizaba la entrada.

- Se insertó código malicioso en el campo de comentarios.

- Cuando otros usuarios ven los comentarios, el código se ejecuta en sus navegadores.

Escenarios de riesgo:

- Un atacante podría robar las cookies de sesión de los usuarios y secuestrar sus cuentas, con respecto al negocio, esto podría generar cambios importantes en configuraciones de forma no autorizada si la sesión robada es perteneciente a un administrador o insider.

- Redirección a sitios web maliciosos podría llevar a la instalación de malware en las máquinas de los usuarios, con respecto al negocio, esto podría conllevar a una mala reputación hacia la organización y dar una mala imagen.

Recomendaciones:

- Implementar filtrado y sanitización de entrada en los formularios de comentarios.

- Educar a los desarrolladores sobre las mejores prácticas para prevenir ataques XSS.

Vulnerabilidades informativas

Nota N°1: La versión de servidor expuesta podría proporcionar a los atacantes información sobre las tecnologías y software utilizados en la infraestructura del sitio web. Aunque esto no tiene un impacto inmediato, podría ayudar a los atacantes a identificar posibles vulnerabilidades específicas para aprovechar, con respecto al negocio, esta vulnerabilidad de tipo informativa si bien no es benigna puede ser escalable por los ciberdelincuentes para generar estragos en la continuidad del negocio y/o su enfoque.

Conclusiones y recomendaciones finales

- El análisis de las vulnerabilidades en "https://securgo.com/" revela la presencia de dos problemas críticos, una Ejecución Remota de Código (RCE) y una vulnerabilidad de Cross-Site Scripting (XSS), que podrían comprometer tanto la integridad como la confidencialidad de los datos y la seguridad del sitio.

- Se identificaron dos vulnerabilidades informativas relacionadas con la exposición de la versión del servidor y la divulgación de directorios. Aunque estas no representan un riesgo directo, podrían proporcionar información útil para posibles ataques futuros.

- Parcheo y Actualización: Priorizar el parcheo y la actualización de la aplicación y sus componentes para corregir las vulnerabilidades conocidas y prevenir posibles ataques.

- Filtración y Validación: Implementar mecanismos de filtración y validación de datos de entrada en todas las áreas propensas a ataques, como formularios de comentarios y campos de entrada.

- Educación y Concienciación: Educar al equipo de desarrollo sobre las mejores prácticas de seguridad, incluida la prevención de ataques XSS y RCE, para evitar la introducción inadvertida de vulnerabilidades en el futuro.

- Pruebas de Seguridad: Realizar pruebas de seguridad regulares, como pruebas de penetración y análisis de vulnerabilidades, para identificar y corregir posibles problemas de seguridad antes de que sean explotados.

- Restricción de Información: Limitar la exposición de información sensible, como detalles de versión del servidor y estructura de directorios, para dificultar el trabajo de los atacantes.

- Plan de Respuesta ante Incidentes: Desarrollar un plan de respuesta ante incidentes que incluya procedimientos para mitigar y manejar posibles ataques y violaciones de seguridad.

- Monitorización Continua: Establecer un sistema de monitorización continua para detectar actividad sospechosa y ataques en tiempo real, permitiendo una respuesta rápida.

- Auditorías de Seguridad: Considerar la realización de auditorías de seguridad independientes para obtener una evaluación objetiva de la postura de seguridad del sitio web de manera más frecuente.

Referencias

[1] saxx

[2] ven1n

[3] doxilaa

[4] OWASP Risk Rating

[5] Nessus

[6] Burp-Suite

[7] CVE-2022-37958 (Relacionado)

[8] CVE-2022-0829 (Relacionado)