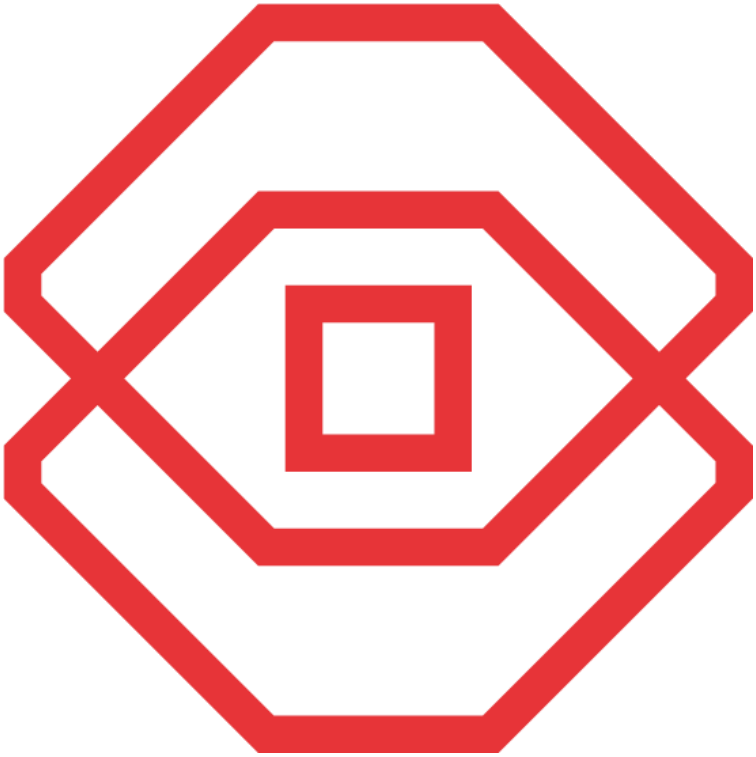

DDLR PRIVATE TEAM

08/08/2023 v2.0

Resumen

Se ha detectado una vulnerabilidad en el sitio web DDLR [1], la cual permite a un usuario malintencionado crear un usuario que posteriormente le proporcionará acceso para ver y eliminar, de forma no autorizada, una gran cantidad de comentarios ubicados en los posts de los usuarios de dicha plataforma.

Recuento de vulnerabilidades en función de su severidad:

CRÍTICO	ALTO	MEDIO	BAJO	INFORMATIVO
0	0	1	0	1

Tabla de contenidos

Las limitaciones que se presentaron fueron:

- Se pudo listar una gran variedad de comentarios de la web, pero, no se pudo listar la totalidad de ellos, por lo tanto, tampoco se podría haber eliminado absolutamente todos los comentarios de la web.
- No se pudo crear más usuarios partiendo del usuario objetivo vulnerable ya que no pareciera estar activada la tecnología de "load balancing" [2], lo cuál es un buen síntoma.

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 "*.diosdelared.com/*". Esto no implica que sea un informe completo de todas las vulnerabilidades pasadas, presentes o futuras que pueda tener la aplicación en cuestión.

Personal involucrado

El equipo de auditoria se conforma por los siguientes integrantes:

diegobardalez [3], p0mb3r0 [4], Zep7i [5] y M20191 [6]

Calificación de riesgo

La metodología de calificación de riesgo que se utilizará en este reporte será el “OWASP Risk Rating” [7] 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.

Observaciones

Subdominio

1.1

Nombre: Registro de usuario comprometedor

Descripción: Se crea un usuario web con el nombre "www", tomando el control del subdominio en sí. Debido a la falta de sanitización, un usuario malintencionado tiene la capacidad de visualizar y eliminar una gran cantidad de comentarios en las publicaciones de otros usuarios.

Riesgo: Impacto: 6 (Bajo) – Riesgo Global: 7.5 (Medio)

Tipo de vulnerabilidad: subdominio expuesto y vulnerable a eliminación de comentarios ajenos

Categoría: Validación de datos / Subdominios

Ubicación de explotabilidad: “*.diosdelared.com/” | “*.diosdelared.com/?view=admin&blogconfig=1&delx=on”

Impacto real: Es factible proceder a la eliminación de una porción significativa de los comentarios emitidos por los usuarios con respecto a las publicaciones, siempre y cuando dichos comentarios no hayan sido generados directamente en los posts por medio de los perfiles de los usuarios en específico en el dominio "*.diosdelared.com/". En lugar de ello, estos comentarios habrán sido originados a través de la página web global "diosdelared.com/*".

Pasos a seguir:

- Registrar un usuario con nombre “www”

- Dirigirse a la sección de ajustes "diosdelared.com/?view=admin"

- Seleccionar “Blog Config” "diosdelared.com/?view=admin&blogconfig=on"

- Posteriormente seleccionamos el subapartado “Comments” "https://www.diosdelared.com/?view=admin&blogconfig=1&delx=on"

- Finalmente el usuario malintencionado puede automatizar esta tarea si así lo desea y borrar comentario por comentario hasta no dejar ninguno dentro de los límites permitidos.

Recomendaciones: Realizar una revisión exhaustiva del flujo de creación de usuarios y asignación de subdominios para identificar y corregir la confusión en los enlaces

Vulnerabilidades informativas

Nota N°1: No verificar la autenticidad del factor humano en un formulario de registro daría paso a posibles ataques de DoS/DDoS llenando la base de datos de usuarios basura.

Conclusiones y recomendaciones finales

- Se recomienda aplicar mayores medidas de seguridad a la gestión de usuarios con respecto a sus blogs personales, preferentemente reinventar su gestión a través de subdominios y gestionarlo de una manera más segura.

- Se recomienda incrementar la seguridad de las entradas de usuario en formularios importantes como registro, login o cualquiera que sea de vital importancia para la gestión de usuarios o datos.

- En caso de que estuviese habilitada la tecnología "load balancing" es preferible que esta sea desactivada por seguridad.

- Se recomienda aumentar la seguridad con respecto a ataques de denegación de servicio o bots, ya sea dentro de la web o canales relacionados. Asimismo, activar las opciones que su WAF le brinde para realizar prevenciones de este.

Referencias

[1] DDLR

[2] Load Balacing - OVH

[3] diegobardalez

[4] p0mb3r0

[5] Zep7i

[6] M20191

[7] OWASP Risk Rating