Vulnerabilidad web

Informe de escaneo

Rutavity

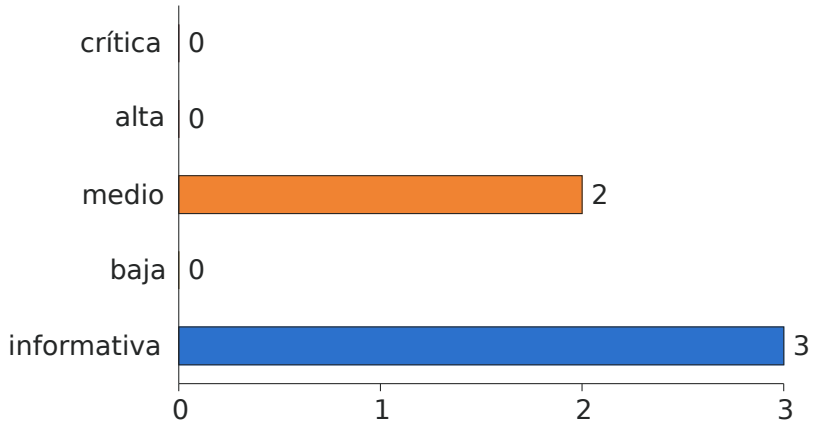
11 Jan 24 19:47 CET
https://www.rutavity.com

CONTENIDO

1 DESCRIPCIÓN GENERAL

1.1 RESUMEN DE VULNERABILIDAD

Según nuestras pruebas, identificamos 5 vulnerabilidades.



ESTADO	DESCRIPCIÓN	PUNTUACIÓN BASE
INFORMACIÓN	Los hallazgos informativos no representan ninguna amenaza, sino que tienen únicamente un propósito informativo.	0
BAJA	Los hallazgos de baja gravedad no imponen una amenaza inmediata. Dichos hallazgos deben revisarse para determinar su impacto específico en la solicitud y corregirse en consecuencia.	0.1 - 3.9
MEDIO	Los hallazgos medios pueden causar daños graves en combinación con otras vulnerabilidades de seguridad. Estos hallazgos deben considerarse durante la planificación del proyecto y solucionarse en poco tiempo.	4 - 6.9
ALTA	Los hallazgos en esta categoría representan una amenaza inmediata y deben solucionarse de inmediato.	7 - 8.9
CRÍTICA	Estos hallazgos son muy críticos y al mismo tiempo representan una amenaza inmediata. Solucionar estos problemas debe ser la máxima prioridad, independientemente de cualquier otro problema.	9 - 10

1.2 DESCRIPCIÓN GENERAL DEL ESCÁNER

1.2.1 Escáneres usados

Durante el análisis, el análisis dinámico, buscó los siguientes tipos de vulnerabilidades y problemas de seguridad:

- ✔ Huella digital de la versión del servidor
- ✔ Versión de la aplicación web Huellas digitales
- ✔ Comparación de CVE
- ✔ Sangrado del corazón
- ✔ ROBOT
- ✔ INCUMPLIMIENTO
- ✔ BESTIA
- ✔ Versión antigua de SSL/TLS
- ✔ Orden de cifrado SSL/TLS
- ✔ Secreto directo perfecto SSL/TLS
- ✔ Reanudación de sesión SSL/TLS
- ✔ Algoritmo seguro SSL/TLS
- ✔ Tamaño de clave SSL/TLS
- ✔ Cadena de confianza SSL/TLS
- ✔ Fecha de vencimiento de SSL/TLS
- ✔ Revocación SSL/TLS (CRL, OCSP)
- ✔ Grapado SSL/TLS OCSP
- ✔ Encabezados de seguridad
- ✔ Encabezados de política de seguridad de contenido
- ✔ escaneo de puertos

1 . 2 . 2 Escáneres adicionales

Los siguientes escáneres también están disponibles en Dynamic Analysis, pero solo están disponibles para escaneos completos.

- ✗ Inyección SQL ciega basada en booleanos
- ✗ Inyección SQL ciega basada en tiempo
- ✗ Inyección SQL basada en errores
- ✗ Inyección SQL basada en consultas UNION
- ✗ Consultas apiladas Inyección SQL
- ✗ Inyección SQL fuera de banda
- ✗ Secuencias de comandos entre sitios reflejados (XSS)
- ✗ Secuencias de comandos entre sitios almacenadas (XSS)
- ✗ Falsificación de solicitudes entre sitios (CSRF)
- ✗ Inclusión de archivos
- ✗ Difusor de directorio
- ✗ Fuzzer de archivos
- ✗ Inyección de comando
- ✗ Procesamiento de entidades externas XML (XXE)
- ✗ Inyección LDAP

1 .2.3 Estado de los escáneres ejecutados

ESCÁNER	PORCENTAJE	ESTADO
Fingerprinting	100%	1 terminada
Portscan	100%	1 terminada
HTTP Header	100%	1 terminada
Transport Layer Security (TLS/SSL)	100%	1 terminada
	100%	**4 terminada**

1.3 Datos del proyecto

GENERAL	
Tipo de objetivo	Única página
URL del proyecto	www.rutavity.com
Alcance	Análisis rápido
Modo rastreador	Rastreo inteligente
Límite de limitación	200
Duración máxima del escaneo	4320 minutos
Duración máxima del escaneo	3600 minutos

1. 4 LISTA DE COMPROBACIÓN DE BÚSQUEDA

1.4.1 ESCANEO DE PUERTOS

ESTADO	ENCONTRAR EL RESULTADO	OBSERVÓ	FIXED
0.0	Se encontró el puerto abierto "80/tcp" con el nombre de servicio "Varnish"	2	2
0.0	Se encontró el puerto abierto "443/tcp" con el nombre de servicio "Varnish"	2	2

1 .4.2 SSL/TLS

ESTADO	ENCONTRAR EL RESULTADO	OBSERVÓ	FIXED
0.0	Registro de recursos de autorización de autoridad de certificación (CAA) de DNS/RFC6844: no se ofrece	2	2

1.4.3 HTTPHEADER

ESTADO	ENCONTRAR EL RESULTADO	OBSERVÓ	FIXED
6.5	A la política de seguridad de contenido le falta la directiva de notificación. Esto se encontró en la URL https://www.rutavity.com	2	2
4.3	El encabezado Referrer-Policy no está configurado para la URL https://www.rutavity.com.	2	2

1. 5 OWASP TOP TEN LISTA DE VERIFICACIÓN

CATEGORÍA	DESCRIPCIÓN	ESCANEADA
Control de acceso roto A1:2021	El control de acceso garantiza que los usuarios solo puedan actuar dentro de sus autorizaciones asignadas. Las fallas comúnmente resultan en la divulgación no autorizada de información, modificación o destrucción de todos los datos o en la realización de una posición comercial fuera de los límites del usuario.	✗
Fallo criptográfico A2:2021	En primer lugar, se debe determinar la necesidad de protección de los datos, tanto durante la transmisión como en reposo. En este caso, las contraseñas, los números de tarjetas de crédito, los datos de salud, la información personal y los secretos comerciales, entre otros, requieren seguridad adicional, especialmente cuando estos datos están sujetos a leyes de protección de datos (p. E. GDPR) o regulaciones (p. E. PCI DSS).).	✓
Inyección A3:2021	El concepto es el mismo para todos los tipos de inyecciones. Estos tipos incluyen inyecciones populares como SQL, NoSQL, comando OS, ObjectRelationalMapping(ORM), LDAP y ExpressionLanguage(EL) o inyección de biblioteca de navegación de gráficos de objetos (OGNL).	✗
Diseño inseguro* A4:2021	Si bien el diseño inseguro es una categoría amplia y representa muchas vulnerabilidades diferentes, se lo denomina "diseño de control faltante o ineficaz". Sin embargo, no es la causa principal de todos los 10 riesgos principales de OWASP. Más bien se distingue entre diseño inseguro e implementación insegura, y no sin razón. Esto se debe a que las deficiencias de diseño e implementación tienen diferentes causas y medidas de mitigación. Los defectos de implementación también pueden ocurrir con un diseño seguro. Esto, a su vez, puede generar vulnerabilidades que pueden explotarse. Sin embargo, un diseño inseguro no puede solucionarse mediante una implementación perfecta. Los controles de seguridad necesarios no se crearon para defenderse de ataques específicos. Sin embargo, lo que puede conducir a un diseño inseguro es no crear un perfil de riesgo empresarial para el software o sistema que se está desarrollando. Por tanto, es imposible determinar qué nivel de diseño de seguridad se requiere.	✗
Seguridad Mala configuración A5:2021	La configuración incorrecta de seguridad puede ocurrir en cualquier etapa de una pila de aplicaciones. Incluye servicios de red, la plataforma, servidor web, servidor de aplicaciones, base de datos, marcos, código personalizado y máquinas virtuales, contenedores o almacenamiento preinstalados.	✓
Vulnerable y Componentes obsoletos A6:2021	Las herramientas de terceros utilizadas en el software podrían ser componentes vulnerables y obsoletos. Estas herramientas deben actualizarse periódicamente para evitar ataques a la aplicación web. No actualizarlos puede provocar ataques de usuarios malintencionados que aprovechen vulnerabilidades conocidas.	✓
Identificación y Fallos de autenticación A7:2021	Para protegerse contra ataques relacionados con la autenticación, se debe confirmar la identidad, la autenticación y la gestión de la sesión del usuario.	✗

CATEGORÍA	DESCRIPCIÓN	ESCANEADA
Software y datos Fallos de integridad A8:2021	Cuando las aplicaciones dependen de complementos, bibliotecas o módulos de fuentes, repositorios y redes de entrega de contenido que no son de confianza, se producen fallas de integridad del software y de los datos. Se refieren a códigos e infraestructuras que no protegen contra violaciones de integridad.	✗
Registro de seguridad y Monitoreo de fallas* A9:2021	Fallas de monitoreo y registro de seguridad es una categoría diseñada para ayudar a detectar, escalar y responder a violaciones de seguridad que están ocurriendo activamente. Cabe señalar que sin supervisión y registro, no se detectarán infracciones.	✗
Solicitud del lado del servidor Falsificación (SSRF) A10:2021	Una vez que las aplicaciones web recuperan un recurso remoto sin verificar la URL proporcionada por el usuario, pueden ocurrir vulnerabilidades SSRF. Con este ataque, un atacante puede obligar a la aplicación a enviar solicitudes manipuladas a destinos inesperados. Esto puede suceder incluso si está protegido por un firewall, VPN u otro tipo de control de acceso a la red. La recuperación de una URL se produce a diario, ya que las aplicaciones web modernas brindan comodidad a los usuarios finales. Como resultado, los ataques de la SSRF van en aumento.	✗

* Nota: La categoría respectiva no se puede probar automáticamente y requiere revisión humana.

2 RECOMENDACIONES

2.1 SSL/TLS

2.1.1 ¿Qué es un escáner SSL?

Transport Layer Security (TLS), más conocido por su predecesor Secure Sockets Layer (SSL), es un protocolo de cifrado híbrido para la transmisión segura de datos a través de Internet. Cifra la comunicación entre el servidor y el cliente. La parte más obvia es HTTPS, con el que los proveedores pueden proteger todas las comunicaciones entre sus servidores y navegadores web. Esto garantiza que nadie que analice el tráfico de la red pueda robar información valiosa como nombres de usuario, contraseñas e información de tarjetas de crédito. La "S" en HTTPS significa SSL. Para una conexión segura con HTTPS se necesita un certificado. Esos certificados ofrecen diferentes niveles de seguridad y tienen una fecha de inicio y de vencimiento fija. Para garantizar una conexión segura, los servidores web deben utilizar certificados bien configurados. Con algunos certificados mal configurados es posible eludir el cifrado, otros pueden ser bloqueados por los navegadores web porque están desactualizados o son desconocidos.

2.1.2 Falta registro SSL CAA

Gravedad

Puntuación básica:	informativo (0/10)
Impacto:	informativo (0/10)
Explotabilidad:	baja (3.9/10)

Todos los valores se basan en el Sistema de puntuación de vulnerabilidad común v3.

Descripción

La zona DNS del dominio no especifica ningún registro de Autorización de autoridad de certificación (CAA). Esto significa que todas las autoridades certificadoras (CA) pueden emitir certificados para este dominio. Para disminuir el riesgo de certificados falsos, agregue la configuración CAA a los registros DNS.

Hallazgo

+ Registro de recursos de autorización de autoridad de certificación (CAA) de DNS/RFC6844: No se ofrece

Como arreglar

La zona DNS del dominio no especifica ningún registro de Autorización de autoridad de certificación (CAA). Esto significa que todas las autoridades certificadoras (CA) pueden emitir certificados para este dominio. Para disminuir el riesgo de certificados falsos, es necesario agregar la configuración CAA a los registros DNS. Se pueden encontrar más detalles sobre cómo configurar la configuración CAA en la base de datos de conocimientos (ver Recomendaciones)

Recomendaciones

Habilitar registros SSL CAA faltantes

La zona DNS del dominio no especifica ningún registro de Autorización de autoridad de certificación (CAA). Todas las autoridades certificadoras (CA) pueden emitir certificados para este dominio.

2.2 HTTPHEADER

2.2.1 ¿Qué es un escáner de encabezados HTTP?

Al visitar un sitio web, la respuesta del servidor incluirá encabezados de respuesta HTTP. Estos encabezados le indican al navegador cómo comportarse mientras el usuario interactúa con el sitio web. Los navegadores modernos admiten una variedad de encabezados de seguridad, que forman parte de los encabezados de respuesta HTTP. Este escáner comprobará si los encabezados de seguridad recomendados están configurados y también verificará si los encabezados están configurados de forma segura.

2 .2.2 Contenido - Seguridad - Encabezado de Política

Gravedad

Puntuación básica:	medio (6.5/10)
Impacto:	bajo (2.5/10)
Explotabilidad:	bajo (3.9/10)

Todos los valores se basan en el Sistema de puntuación de vulnerabilidad común v3.

Descripción

El encabezado Content-Security-Policy le indica al navegador qué dominios están en la lista blanca para descargar más recursos, como scripts, imágenes u hojas de estilo. Esto puede prevenir varios ataques XSS y otros ataques de Cross-Site-Scripting.

Hallazgo

+ A la política de seguridad de contenido le falta la directiva de notificación. Esto se encontró en la URL https://www.rutavity.com

Como arreglar

Configure el encabezado Content-Security-Policy de manera que solo permita cargar recursos desde recursos confiables como "propio". No incluya 'unsafe-eval' o 'unsafe-inline' para evitar inyecciones directas en el sitio web.

Recomendaciones

Habilitar encabezados de seguridad

Los encabezados de seguridad pueden prevenir eficazmente una variedad de intentos de piratería. Por lo tanto, debe considerar los títulos Strict-Transport-Security, ContentSecurity-Policy, X-Frame-Options o X-XSS-Protection.

2 .2.3 Referencia - Encabezado de política

Gravedad

Puntuación básica:	medio (4.3/10)
Impacto:	bajo (1.4/10)
Explotabilidad:	bajo (2.8/10)

Todos los valores se basan en el Sistema de puntuación de vulnerabilidad común v3.

Descripción

El encabezado Referrer-Policy define cuánta información sobre el referente se envía cuando el usuario hace clic en un enlace. Una configuración incorrecta o un encabezado faltante pueden filtrar información confidencial a sitios web de terceros que se visitan al hacer clic en un enlace.

Hallazgo

+ El encabezado Referrer-Policy no está configurado para la URL https://www.rutavity.com.

Como arreglar

Establezca el encabezado Referrer-Policy en un valor seguro como 'estricto-origen-cuando-cruz-origen' para sobrescribir el encabezado Referer con su dominio en lugar de la ruta completa al hacer clic en enlaces externos y mantenga el Referer para enlaces internos, pero sólo cuando la conexión no se degrada de

Recomendaciones

Habilitar encabezados de seguridad

Los encabezados de seguridad pueden prevenir eficazmente una variedad de intentos de piratería. Por lo tanto, debe considerar los títulos Strict-Transport-Security, Content-Security-Policy, X-Frame-Options o X-XSS-Protection.

2.3 ESCANEO DE PUERTOS

2 . 3 . 1 ¿Qué es un Ports Scan?

Un puerto es una especie de puerta en el servidor que se puede utilizar para conectarse a un servicio específico. Para un servidor web, lo más probable es que el puerto 80 y el puerto 443, que son para HTTP/HTTPS, estén abiertos para ofrecer el sitio web a los usuarios. Otros puertos deberían cerrarse si no son necesarios para ningún servicio. El escáner de puertos prueba el servidor web con un escaneo SYN para detectar una amplia gama de puertos posiblemente abiertos y los informa. Si hay otros puertos abiertos excepto el puerto 80 y el puerto 443, el firewall debe bloquearlos si no son necesarios.

2 . 3 . Escáner de 2 puertos

Gravedad

Puntuación básica:	informativo (0/10)
Impacto:	informativo (0/10)
Explotabilidad:	informativo (0/10)

Todos los valores se basan en el Sistema de puntuación de vulnerabilidad común v3.

Descripción

Los puertos abiertos innecesarios en el servidor web abren una gran superficie de ataque para un usuario malintencionado. Esto se puede utilizar para encontrar servicios de red sin mantenimiento y posiblemente vulnerables a los que se pueda atacar.

Hallazgo

+ Se encontró el puerto abierto "80/tcp" con el nombre del servicio "Varnish"
+ Se encontró el puerto abierto "443/tcp" con el nombre de servicio "Varnish"

Como arreglar

Los puertos innecesariamente abiertos se pueden cerrar configurando un firewall y bloqueando las conexiones a todos los puertos excepto aquellos que necesita el servidor. Además, se deben desinstalar los servicios que no sean necesarios.

Recomendaciones

Servicios de red seguros

Los servicios de red inseguros pueden exponer toda una infraestructura de red a riesgos y compromisos de seguridad. Esto es lo que son los servicios de red inseguros, qué vulnerabilidades crean y qué medidas puede tomar.

Los dispositivos y servicios que están expuestos a Internet y que utilizan servicios de red inseguros o innecesarios corren el riesgo de exponer los datos que transmiten y el servidor web en el que se ejecutan. En el caso de dispositivos conectados que forman parte del Internet de las cosas (IoT), los servicios de red inseguros también pueden exponer dichos dispositivos al control remoto y utilizarse como botnet.