ACELERA IT
Informe de resultados de la evaluación de seguridad

Business Confidential

Fecha: 1 agosto, 2023
Proyecto: DC-001
Version 1.0

Tabla de contenidos

Declaración de confidencialidad

Este documento es propiedad exclusiva de Acelera IT y ALV Security (ALVS). Este documento contiene información confidencial y de propiedad exclusiva. La duplicación, redistribución o uso, en su totalidad o en parte, en cualquier forma, requiere el consentimiento tanto de Acelera IT como de ALVS.

Acelera IT puede compartir este documento con auditores bajo acuerdos de confidencialidad para demostrar el cumplimiento de los requisitos de prueba de penetración.

Renuncia

Una prueba de penetración se considera una instantánea en el tiempo. Las conclusiones y recomendaciones reflejan la información reunida durante la evaluación pero no los cambios o modificaciones realizados fuera de ese período.

Los compromisos de tiempo limitado no permiten una evaluación completa de todos los controles de seguridad. ALVS priorizó la evaluación para identificar los controles de seguridad más débiles que un atacante explotaría. ALVS recomienda realizar evaluaciones similares anualmente por parte de evaluadores internos o externos para garantizar el éxito continuo de los controles.

Información de contacto

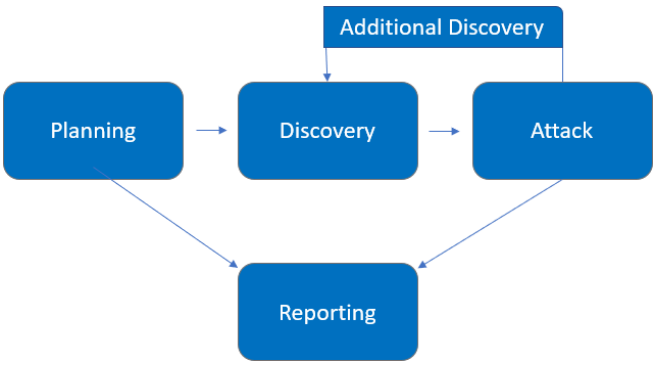
Nombre	Título	Información de contacto
Acelera IT		
Juan Herrero	Gerente Global de Seguridad de la Información	Correo electrónico: jsmith@acelerait.com
ALV Security		
Álvaro De La Fuente	Pentester	Correo electrónico: alvaro@alv-sec.com

Descripción general de la evaluación

Desde el 1 de agosto de 2023 hasta el 14 de agosto de 2023, Acelera IT contrató a ALVS para evaluar la postura de seguridad de su infraestructura en comparación con las mejores prácticas actuales de la industria que incluyeron una prueba de penetración de red interna. Todas las pruebas realizadas se basan en la Guía técnica del NIST *SP 800-115 para las pruebas y evaluación de la seguridad de la información, la Guía de pruebas OWASP (v4) y los marcos de prueba personalizados*.

Las fases de las actividades de pruebas de penetración incluyen las siguientes:

- Planificación: se recopilan los objetivos del cliente y se obtienen las reglas de compromiso.
- Detección: realice análisis y enumeración para identificar posibles vulnerabilidades, áreas débiles y vulnerabilidades.
- Ataque: confirme posibles vulnerabilidades a través de la explotación y realice descubrimientos adicionales ante un nuevo acceso.
- Informes: documente todas las vulnerabilidades y vulnerabilidades encontradas, los intentos fallidos y las fortalezas y debilidades de la empresa.



Componentes de evaluación

Prueba de penetración externa

Una prueba de penetración externa emula el papel de un atacante que intenta obtener acceso a una red interna sin recursos internos o conocimiento interno. Un ingeniero de ALVS intenta recopilar información confidencial a través de inteligencia de código abierto (OSINT), incluida la información de los empleados, las contraseñas históricas violadas y más que se pueden aprovechar contra los sistemas externos para obtener acceso a la red interna. El ingeniero también realiza escaneo y enumeración para identificar posibles vulnerabilidades con la esperanza de explotarlas

Encontrar clasificaciones de gravedad

En la tabla siguiente se definen los niveles de gravedad y el intervalo de puntuación CVSS correspondiente que se utilizan en todo el documento para evaluar la vulnerabilidad y el impacto del riesgo.

Severidad	CVSS V3 Rango de puntuación	Definición
Crítico	9.0-10.0	La explotación es sencilla y generalmente resulta en un compromiso a nivel del sistema. Se recomienda formar un plan de acción y parchear inmediatamente.
Alto	7.0-8.9	La explotación es más difícil, pero podría causar privilegios elevados y potencialmente una pérdida de datos o tiempo de inactividad. Se recomienda formar un plan de acción y parchear lo antes posible.
Moderado	4.0-6.9	Las vulnerabilidades existen pero no son explotables o requieren pasos adicionales como la ingeniería social. Se recomienda formar un plan de acción y parchear después de que se hayan resuelto los problemas de alta prioridad.
Bajo	0.1-3.9	Las vulnerabilidades no son explotables, pero reducirían la superficie de ataque de una organización. Se recomienda formar un plan de acción y parche durante la próxima ventana de mantenimiento.
Informativo	N/A	No existe ninguna vulnerabilidad. Se proporciona información adicional sobre los elementos observados durante las pruebas, controles sólidos y documentación adicional.

Factores de riesgo

El riesgo se mide por dos factores: Probabilidad e impacto:

Probabilidad

La probabilidad mide el potencial de que se explote una vulnerabilidad. Las calificaciones se otorgan en función de la dificultad del ataque, las herramientas disponibles, el nivel de habilidad del atacante y el entorno del cliente.

Impacto

El impacto mide el efecto de la vulnerabilidad potencial en las operaciones, incluida la confidencialidad, integridad y disponibilidad de los sistemas y/o datos del cliente, el daño a la reputación y la pérdida financiera.

Alcance

Evaluación	Detalles
Prueba de penetración interna	82.223.0.0/16

Exclusiones de alcance

Por solicitud del cliente, ALVS no realizó ninguno de los siguientes ataques durante las pruebas:

- Denegación de servicio (DoS)
- Phishing/Ingeniería Social

Todos los demás ataques no especificados anteriormente fueron permitidos por Acelera IT.

Asignaciones del cliente

Acelera IT no ha proporcionado niguna asignación para ayudar a las pruebas.

Resumen ejecutivo

ALVS evaluó la postura de seguridad interna de Acelera IT a través de pruebas de penetración del 1 de agosto de 2023 al 14 de agosto de 2023. En las secciones siguientes se proporciona una descripción general de alto nivel de las vulnerabilidades descubiertas, los intentos exitosos y fallidos, y las fortalezas y debilidades.

Alcance y limitaciones de tiempo

El alcance durante el compromiso no permitió la denegación de servicio o la ingeniería social en todos los componentes de prueba.

Se establecieron limitaciones de tiempo para las pruebas. Se permitieron pruebas de penetración de red interna para diez (10) días hábiles.

Notas y recomendaciones del probador

Los resultados de las pruebas de la red Acelera IT son indicativos de que una organización se somete a su primera prueba de penetración, que es el caso que nos concierne. Muchos de los hallazgos descubiertos son vulnerabilidades dentro del marco Cross-Site Scripting.

Durante las pruebas, dos constantes se destacaron: una política de contraseñas media y parches débiles. Recomendamos que Acelera IT reevalúe su política de contraseñas actual y considere una política de 15 caracteres o más para sus cuentas de usuario normales y 30 caracteres o más para sus cuentas de administrador de dominio. También recomendamos que Acelera IT explore la lista negra de contraseñas y proporcionará una lista de contraseñas de usuario descifradas para que el equipo las evalúe. Finalmente, se debe considerar una solución de administración de acceso de privilegios.

Recomendamos que el equipo de Acelera IT revise las recomendaciones de parches hechas en la sección Hallazgos técnicos del informe junto con la revisión de los escaneos Nessus proporcionados para obtener una descripción completa de los elementos que se van a parchar. También recomendamos que Acelera IT mejore sus políticas y procedimientos de administración de parches para ayudar a prevenir posibles ataques dentro de su red.

En una nota positiva, nuestro equipo de pruebas activó varias alertas durante el compromiso. El equipo de operaciones de seguridad de Acelera IT descubrió nuestro escaneo de vulnerabilidades y fue alertado cuando intentamos usar ataques ruidosos en una máquina comprometida. Si bien no todos los ataques se descubrieron durante las pruebas, estas alertas son un comienzo positivo. Se ha proporcionado orientación adicional sobre alertas y detección para los hallazgos, cuando es necesario, en la sección Hallazgos técnicos.

En general, la red de Acelera IT funcionó como se esperaba para una prueba de penetración por primera vez. Recomendamos que el equipo de Acelera IT revise a fondo las recomendaciones hechas en este informe, revise los hallazgos y vuelva a realizar pruebas anualmente para mejorar su postura general de seguridad interna.

Fortalezas y debilidades clave

A continuación se identifican las fortalezas clave identificadas durante la evaluación:

1. Se observó algún escaneo de herramientas de enumeración comunes (Nessus)
2. La política de contraseñas es media, no deja crear cuenta sin un mínimo de 8 caracteres especiales.
3. Detectado protocolo TLS Version 1.0
4. Detectado TLS Version 1.1 de protocolo obsolete
5. Métodos HTTP TRACE / TRACK permitidos en el servidor web remoto

Resumen de vulnerabilidades y boleta de calificaciones

En las tablas siguientes se ilustran las vulnerabilidades detectadas por el impacto y las correcciones recomendadas:

Resultados de la prueba de penetración interna

0	0	3	0	27
Crítico	Alto	Moderado	Bajo	Informativo

Hallazgo	Severidad	Recomendación
Prueba de penetración interna		

Hallazgo	Severidad	Recomendación
TLS Version 1.0 Protocol Detection	Moderado	Habilite la compatibilidad con TLS 1.2 y 1.3 y deshabilite la compatibilidad con TLS 1.0.
TLS Version 1.1 Protocol Deprecated	Moderado	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
HTTP TRACE / TRACK Methods Allowed	Moderado	Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información.
Additional DNS Hostnames	Informativo	Use la sintaxis especial de vhost, como: www.example.com[192.0.32.10]
Apache HTTP Server Version	Informativo	Es posible obtener el número de versión del servidor HTTP Apache remoto.
Common Platform Enumeration (CPE)	Informativo	Es posible enumerar los nombres de CPE que coincidían en el sistema remoto.
Device Type	Informativo	Es posible adivinar el tipo de dispositivo remoto.
HSTS Missing From HTTPS Server	Informativo	Configure el servidor web remoto para utilizar HSTS.
HTTP Server Type and Version	Informativo	Este plugin intenta determinar el tipo y la versión del servidor web remoto.
HyperText Transfer Protocol (HTTP) Information	Informativo	Se puede extraer cierta información sobre la configuración HTTP remota.

Nessus SYN scanner	Informativo	Proteja su objetivo con un filtro IP.
Nessus Scan Information	Informativo	Este plugin muestra información sobre el escaneo de Nessus.
OS Identification	Informativo	Es posible adivinar el sistema operativo remoto.
OpenSSL Detection	Informativo	El servicio remoto parece utilizar OpenSSL para cifrar el tráfico.
SSL / TLS Versions Supported	Informativo	El servicio remoto cifra las comunicaciones.
SSL Certificate Chain Contains Unnecessary Certificates	Informativo	Quite los certificados innecesarios de la cadena de certificados.
SSL Certificate Chain Not Sorted	Informativo	Vuelva a ordenar los certificados en la cadena de certificados.
SSL Certificate Information	Informativo	Este plugin muestra el certificado SSL.
SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)	Informativo	Póngase en contacto con la autoridad de certificación para que se vuelva a emitir el certificado.
SSL Cipher Block Chaining Cipher Suites Supported	Informativo	El servicio remoto admite el uso de cifrados SSL Cipher Block Chaining, que combinan bloques anteriores con otros posteriores.
SSL Cipher Suites Supported	Informativo	SSL Cipher Suites Supported
SSL Perfect Forward Secrecy Cipher Suites Supported	Informativo	El servicio remoto admite el uso de cifrados SSL Perfect Forward Secrecy, que mantienen la confidencialidad incluso en caso de robo de la clave.
SSL Root Certification Authority Certificate Information	Informativo	Asegúrese de que el uso de este certificado raíz de la entidad de certificación cumple con las directivas de uso y seguridad aceptables de su organización.
SSL/TLS Recommended Cipher Suites	Informativo	Solo habilite la compatibilidad con conjuntos de cifrado recomendados.
Service Detection	Informativo	Se pudo identificar el servicio remoto.
TLS Version 1.1 Protocol Detection	Informativo	Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1.
TLS Version 1.2 Protocol Detection	Informativo	El servicio remoto acepta conexiones cifradas mediante TLS 1.2.
Traceroute Information	Informativo	Fue posible obtener información de traceroute hasta el host remoto.
Web Server No 404 Error Code Check	Informativo	El servidor web remoto no devuelve códigos de error 404.

Web Application Cookies Are Expired	Informativo	Cada cookie debe revisarse cuidadosamente para determinar si contiene datos confidenciales o si se confía en ella para una decisión de seguridad. Establezca una fecha de caducidad en el futuro para que la cookie persista o elimine el atributo Expires cookie por completo para convertir la cookie en una cookie de sesión.

Hallazgos técnicos

Resultados de la prueba de penetración

Sensible a XXS Stored (Moderado)

Descripción:	En su web Acelera IT es sensible a XXS mediante el campo Apellido, puedes guardar el siguiente código: <script>prompt(1)</script> y aparece una prompt con la que puedes inyectar secuencias de código maliciso o scripts.
Riesgo:	Tiene riesgo ya el ataque se produce en el código del sitio web que se ejecuta en el navegador, y no en el servidor del sitio. Puede robar cookies, datos personales, credenciales, acceso al control del equipo.
Sistema:	82.223.66.125
Referencias:	mitre.org: Ataques de xxs https://portswigger.net/web-security/cross-site-scripting

Evidencia

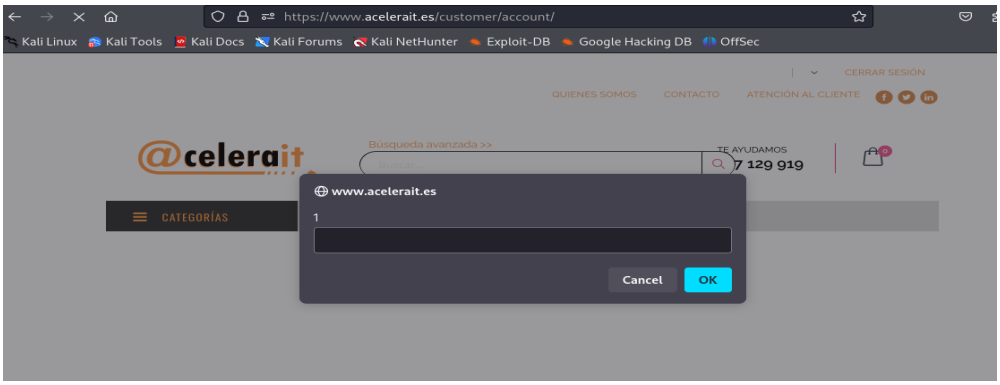


Figura 1: Prompt

Mitigación

Filtra la entrada de datos del usuario lo más específicamente possible y codifica los datos de salida para los usuarios (HTML, URLs, JavaScript y CSS). Consulte la guía de OWASP aquí.

Implementa un WAF (Web Application Firewall) al igual que con las inyecciones SQL, un firewall de apliaciones web ayuda a impeder la ejecución de ataques XSS, filtrando y monitoreando el tráfico HTTP entre una apliación e Internet.

Missing Content-Type Header (Moderado)

Descripción:	Se detectó un encabezado faltante , lo que significa que este sitio web podría estar en riesgo de ataques de detección de MIME.
Riesgo:	El rastreo de tipos MIME es una funcionalidad estándar en los navegadores para encontrar una forma adecuada de representar datos donde los encabezados HTTP enviados por el servidor no son concluyentes o faltan. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen un rastreo MIME en el cuerpo de la respuesta, lo que podría causar que el cuerpo de la respuesta se interprete y muestre como un tipo de contenido diferente al tipo de contenido previsto. El problema surge una vez que un sitio web permite a los usuarios cargar contenido que luego se publica en el servidor web. Si un atacante puede llevar a cabo un ataque XSS (Cross-site Scripting) manipulando el contenido de manera que sea aceptado por la aplicación web y representado como HTML por el navegador, es posible inyectar código, por ejemplo, en un archivo de imagen y hacer que el la víctima lo ejecuta viendo la imagen.
Sistema:	82.223.66.125
Referencias:	https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/

Mitigación

Cuando sirva recursos, asegúrese de enviar el encabezado de tipo de contenido para que coincida adecuadamente con el tipo de recurso que se está dando. Agregue el encabezado X-Content-Type-Options con un valor de "nosniff" para informar al navegador que confíe en que lo que el sitio ha enviado es el tipo de contenido apropiado.

TLS Version 1.1 Protocol Deprecated (Moderado)

Descripción:	El servicio remoto cifra el tráfico mediante una versión anterior de TLS.
Riesgo:	El servicio remoto acepta conexiones cifradas mediante TLS 1.1. TLS 1.1 carece de soporte para conjuntos de cifrado actuales y recomendados. Los cifrados que admiten el cifrado antes del cálculo MAC y los modos de cifrado autenticados como GCM no se pueden usar con TLS 1.1 A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web y los principales proveedores.
Sistema:	82.223.66.125
Referencias:	http://www.nessus.org/u?c8ae820d https://datatracker.ietf.org/doc/html/rfc8996

Mitigación

Habilite la compatibilidad con TLS 1.2 y/o 1.3 y deshabilite la compatibilidad con TLS 1.1. Siga la guía de Microsoft aquí.

HTTP TRACE / TRACK Methods Allowed (Moderado)

Descripción:	El servidor web remoto admite los métodos TRACE y/o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web
Riesgo:	Un ataque Cross-Site Tracing (XST) implica el uso de Cross-Site Scripting (XSS) y los métodos TRACE o TRACK HTTP. De acuerdo con RFC 2616 , "TRACE le permite al cliente ver lo que se recibe en el otro extremo de la cadena de solicitud y usar esos datos para probar o diagnosticar información". El método TRACK funciona de la misma manera pero es específico para IIS de Microsoft. Servidor web. XST podría usarse como un método para robar las cookies del usuario a través de Cross-site Scripting (XSS), incluso si la cookie tiene el indicador " HttpOnly " establecido o expone el encabezado de autorización del usuario.
Sistema:	82.223.66.125
Referencias:	http://www.apacheweek.com/issues/03-01-24 https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf

Mitigación

Deshabilite estos métodos HTTP. Consulte la salida del complemento para obtener más información. Siga la guía de OWASP aquí. En las versiones de Apache 1.3.34, 2.0.55 y posteriores, configure la directiva TraceEnable en "off" en el archivo de configuración principal y luego reinicie Apache. Consulte TraceEnable para obtener más información.

Última página