|  |  |
| --- | --- |
| Número de serie | {report\_number} |
| Fecha | {report\_date} |

**{target\_host}**

**Informe de detección difusa de la API de la plataforma**

Version 1.2

2020/ 12

© 2020 Packer FuzzeR TEAM

Poc-Sir、KpLi0rn、Liucy、RachesseHS、Lupin-III

* **Aviso de derechos de autor**

La plantilla del Informe de Inspección del Packer Fuzzer (en adelante, este informe) tiene los derechos de autor del equipo de desarrollo del Packer Fuzzer (en adelante, el equipo) y está protegida por la ley. El equipo tiene el derecho de modificar e interpretar esta plantilla de informe. Cuando modifique el contenido de esta plantilla de informe, deberá conservar el correspondiente aviso de derechos de autor. La herramienta Packer Fuzzer (en lo sucesivo denominada "la herramienta") no puede utilizarse de ninguna manera con fines comerciales sin la autorización de este equipo. El equipo se reservará el derecho de seguir persiguiendo la responsabilidad legal de cualquier individuo o empresa que viole la declaración anterior.

* **Declaraciones de aplicación**

Este informe se aplica a todos los sistemas de objetivos probados con esta herramienta, así que manténgalo seguro y no lo transmita sin el permiso del propietario del sistema de objetivos.

* **Descargo de responsabilidad**

Este informe es generado automáticamente por la herramienta en base a los resultados de las pruebas del usuario, y el contenido del informe no representa la posición y la opinión de nuestro equipo. Las consecuencias y pérdidas directas o indirectas causadas por la difusión o el uso de las funciones de ensayo que ofrece este instrumento son responsabilidad del usuario, y el equipo no asume ninguna responsabilidad al respecto. Por favor, cumpla con las leyes y regulaciones locales del usuario y del país donde se encuentra el sistema de objetivos cuando utilice esta herramienta, no se permite ninguna prueba no autorizada.

* **Revisión de los registros**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **N°de ver** | **Fecha** | **Modificador** | **Modifi** | **Ratificador** |
| 1.0 | 2020/8/5 | Lupin-III | Ninguno | Poc-Sir |
| 1.2 | 2020/12/18 | Lupin-III | Add More | Poc-Sir |

**I. Resumen del informe**

**Plataformas escaneadas：{target\_host}**

Valores de los parámetros de entrada：{target\_url}

Este escaneo utiliza el modo de escaneo{scan\_type}，El uso de {scan\_ip} como IP de escaneo toma un total de {scan\_time} segundos.

Iniciar el tiempo de exploración：{start\_time}

Tiempo de finalización de la exploración：{end\_time}

Este escaneo encontró un total de {api\_num} interfaces API válidas.

Un total de {js\_num} archivos JS relacionados fueron encontrados, respectivamente：

{js\_list}

Se encontraron un total de {vuln\_num} vulnerabilidades de seguridad, incluyendo alto riesgo {vuln\_h\_num}, medio riesgo {vuln\_m\_num} y bajo riesgo {vuln\_l\_num}. respectivamente：

{vuln\_list}

Información adicional sobre las cookies：{extra\_cookies}

Información adicional del encabezamiento de la transmisión：{extra\_head}

**El nivel de riesgo de seguridad de la plataforma objetivo analizado por esta herramienta：{sec\_lv}**

**II. Detalles de la vulnerabilidad**

{vuln\_deta}

**III. Lista de API**

{api\_list}

**IV. Recomendaciones de seguridad**

{suggest\_foryou}

**V. Información adicional**

extra

**VI. Apéndice**

* **Descripción de las vulnerabilidades**

**Vulnerabilidad CORS**: el intercambio de recursos entre dominios puede relajar la política de homología del navegador, permitiendo que diferentes sitios web y diferentes servidores se comuniquen entre sí a través del navegador. Supongamos que un usuario se conecta a vuln.com, un sitio web que contiene una configuración CORS, y también accede a vuln.com, un enlace proporcionado por el atacante. El sitio web vuln.com hace una solicitud a vuln.com para obtener datos sensibles, y la capacidad del navegador para recibir la información depende de la configuración de vuln.com. Si vuln.com está configurado con el encabezado Access-Control-Allow-Origin y se espera, entonces se permite recibirlo, de lo contrario el navegador no lo recibirá debido a la misma política de origen.

**Vulnerabilidad de acceso no autorizado:** El acceso no autorizado a la interfaz, como su nombre indica, puede acceder y operar directamente las funciones lógicas comerciales correspondientes sin solicitar autorización. Esto suele deberse a una página de autenticación defectuosa o no autenticada, a una configuración de seguridad inadecuada, etc.

**Vulnerabilidad a la revelación de información sensible:** La revelación de información se refiere a la divulgación de información sensible en una página web o en un archivo JS. A través de esta información sensible, un atacante puede comprometer aún más el servidor.

**Vulnerabilidad de anulación horizontal:** una vulnerabilidad de anulación es cuando una aplicación no verifica estrictamente los permisos de identidad de las operaciones del usuario actual, lo que da lugar a que los usuarios puedan operar funciones que están más allá de sus privilegios administrativos, operando así algunos comportamientos que no están disponibles para ese usuario. La anulación de nivel puede dar lugar a que los usuarios de entre el mismo nivel tengan acceso a la información sensible de los demás, como el nombre, el número de teléfono, la dirección de contacto, los datos personales, el historial de pedidos, etc. También puede ser posible realizar una línea de funciones, tales como borrar, añadir, modificar, etc., como otros usuarios con privilegios de anulación de nivel.

**Vulnerabilidad de la inyección SQL:** La vulnerabilidad de la inyección SQL surge porque la aplicación web no está escrita para que el usuario envíe datos al servidor para verificar la legitimidad de los datos (tipo, longitud, legitimidad de los parámetros de negocio, etc.), y no hay un filtrado eficaz de caracteres especiales de los datos introducidos por el usuario, de modo que éste los introduce directamente en la ejecución de la base de datos, más allá de los resultados esperados del diseño original de la declaración SQL, lo que da lugar a una vulnerabilidad de la inyección SQL.

**Débil vulnerabilidad de las contraseñas:** el personal de gestión y operaciones del sitio web utiliza contraseñas muy fáciles de recordar o adopta directamente la contraseña predeterminada del sistema debido a una insuficiente conciencia de la seguridad, a fin de facilitar y evitar que se olviden las contraseñas. Los atacantes pueden utilizar esta vulnerabilidad para entrar directamente en el sistema de aplicación o en el sistema de gestión, a fin de manipular y eliminar el sistema, las páginas web, los datos, acceder ilegalmente al sistema, los datos de los usuarios, e incluso puede provocar la caída del servidor.

**Vulnerabilidad de carga de archivos arbitraria:** El sistema de aplicación comprueba la legitimidad del tipo de archivo, el formato y el contenido del archivo cargado por el usuario en la función de carga de archivos, lo que permite a un atacante cargar un archivo de script de Web malicioso (.php, .jsp, .asp, etc.) o un archivo de formato no esperado como: archivo HTML, archivo SHTML, etc. Al mismo tiempo, puede utilizar los caracteres de salto de directorio o controlar la carga. que puede dar lugar a la ejecución de archivos de escritura maliciosos arbitrarios en un servidor remoto para obtener acceso directo al sistema de aplicación.

* **Niveles de vulnerabilidad**

Este informe tiene tres niveles de vulnerabilidad incorporados, que son: bajo, medio y alto riesgo. Los tipos de vulnerabilidad de alto riesgo son: vulnerabilidad de contraseñas débiles, vulnerabilidad de carga de archivos arbitrarios, vulnerabilidad de inyección SQL; los tipos de vulnerabilidad de riesgo medio son: vulnerabilidad de salto horizontal, vulnerabilidad de divulgación de información sensible, vulnerabilidad de acceso no autorizado; los tipos de vulnerabilidad de bajo riesgo son: vulnerabilidad de CORS.

El nivel de confianza de los resultados del nivel "bajo" de detección reducirá automáticamente la vulnerabilidad de un nivel de daño, si se encuentra en el nivel de vulnerabilidad más bajo no es un descenso. Por ejemplo, una vulnerabilidad para: vulnerabilidad de inyección SQL, debería ser una vulnerabilidad de alto riesgo, pero el nivel de confianza es "bajo", se rebaja automáticamente al riesgo de vulnerabilidad.

* **Nivel de riesgo**

Este informe tiene cuatro niveles de riesgo: sin riesgo, riesgo bajo, riesgo medio y riesgo alto, con una escala de puntuación de 0, 5, 10 y 18, respectivamente. Por ejemplo, en un cierto escaneo se encuentran una vulnerabilidad de alto riesgo, dos de riesgo medio y cinco de bajo riesgo, la puntuación se calcula como 1 x 6 + 2 x 2 + 5 x 1 = 15 (puntos), la puntuación es mayor de 10 y menor de 18, por lo que el nivel de riesgo es "de riesgo medio".

**（Conclusión del informe, con los siguientes espacios en blanco）**