Ingeniería de la Ciberseguridad
Curso 2023/2024

Práctica 1
Sesión práctica 4:

Cornucopia

Análisis y Gestión del Riesgo

Realizado por:

Gabriel Izquierdo González

Mario Ruano Diaz

Juan Antonio Suárez Suárez

ÍNDICE

1. Autenticación

Mario

6	Esta debilidad se origina porque las contraseñas son enviadas a través de email y no se establece ni se requiere que el usuario las cambie dentro de un intervalo de tiempo definido.
5	Esta vulnerabilidad se presenta debido a que la empresa emplea la configuración predeterminada de los buckets de S3, lo que implica que acceder a esa información podría permitir que un atacante con experiencia descifre las credenciales de acceso. Además, la empresa no establece políticas para eliminar elementos periódicamente, lo que implica que las cuentas antiguas o inactivas podrían permanecer en los sistemas y ser objeto de explotación por parte de un atacante.
8	Se podría dar la casuística de que un usuario pudiera realizar un ataque PassTheHash y acceder a contenido no autorizado.

Juan

10	Existe la posibilidad de que Pavin pueda eludir el control de autenticación en esta situación. Aunque la aplicación emplea JSON Web Token (JWT) para la autenticación y utiliza un middleware personalizado para la gestión de permisos, carece de la implementación de un sistema de autenticación centralizado, estándar y aprobado, separado del recurso solicitado.
7	Si, Cecilia podría recurrir a la táctica de forzar contraseñas o a ataques basados en diccionario si no se imponen restricciones en los intentos de inicio de sesión. A pesar de que se especifican ciertos criterios para la creación de contraseñas, como la inclusión de letras mayúsculas, minúsculas, números y caracteres especiales, no se hace mención de ninguna medida de defensa frente a posibles ataques de fuerza bruta.
9	Sí, es posible que Claudia pueda utilizar funciones más críticas debido a que los requisitos de autenticación en el contexto proporcionado son relativamente débiles. Aunque se utiliza JSON Web Token (JWT) para la autenticación y se cuenta con un middleware personalizado para la gestión de permisos, no se menciona la implementación de autenticación de doble factor (2FA) para aumentar la seguridad.

Gabriel

2	Esta vulnerabilidad se produce por la falta de implementación de una política de autenticación de doble factor (2FA) por parte de la empresa. Esto implica que un atacante que logre obtener las credenciales de un usuario podría acceder a la cuenta sin la necesidad de una segunda forma de autenticación. Además, la empresa envía contraseñas temporales en texto plano a través del correo electrónico, lo que las expone a posibles interceptaciones.
4	Existe la posibilidad de que Sebastien pueda acceder al bucket que almacena archivos XLS o CSV que contienen información confidencial, como facturas, declaraciones de impuestos u otros documentos similares. Dado que estos archivos no están cifrados, podrían contener nombres de usuario u otra información sensible, lo que los hace vulnerables y fácilmente accesibles para personas no autorizadas.

3	Esta vulnerabilidad se da debido a la ausencia de políticas en la empresa que regulen el cambio y la caducidad de contraseñas. Además, se permite que los empleados tengan privilegios de administrador en sus propios dispositivos, lo que implica que un atacante que logre acceder a uno de estos dispositivos podría obtener contraseñas o respuestas a preguntas de seguridad almacenadas en la memoria o en la caché.

2. Autorización

Mario

7	La situación descrita se debe a que la empresa ha optado por un middleware personalizado en ExpressJS para controlar los permisos de los usuarios. Si este middleware no se hubiese implementado de manera adecuada, existe la posibilidad de que Yuanjing pueda acceder a funciones y datos para los cuales no tiene autorización.
K	Este ataque se origina principalmente debido a la ausencia de políticas de seguridad efectivas y una gestión deficiente de los permisos de usuario en la empresa. Los empleados cuentan con privilegios de administrador en sus dispositivos portátiles, lo que contribuye a la vulnerabilidad del sistema.
9	Esta situación se daría debido a la ausencia de restricciones en la cantidad de solicitudes que pueden realizarse en un lapso de tiempo definido. Esto podría desencadenar una sobrecarga de recursos o situaciones de competencia, generando potenciales denegaciones de servicio.

Juan

4	Debido a que los controles de autorización predeterminados están configurados para permitir el acceso, cualquier individuo que esté familiarizado con la estructura interna de la organización podría iniciar sesión con privilegios de administrador. Esto abre la puerta a una serie de posibles consecuencias dañinas, como la exposición de datos o la introducción de malware, entre otras. ***Mario***: También se menciona que la aplicación utiliza JSON Web Tokens para la autenticación interna. Sin embargo, no se detalla la seguridad del proceso de autenticación que aseguren la integridad de los tokens JWT y así prevenir posibles robos o falsificaciones.
J	Es posible ejecutar un ataque de Spear Phishing o dirigido con el fin de obtener información de los perfiles que cuentan con acceso a las listas.
10	Debido a la ausencia de restricciones en el tráfico interno, cualquier dispositivo tendría la capacidad de comunicarse con cualquier otro mediante cualquier puerto dentro de la red. Si Richard consiguiera acceso a la red de la empresa, podría intentar acceder a la base de datos o a los archivos almacenados en el servicio de hosting, lo que podría resultar en la obtención de información confidencial.

Gabriel

Q	La vulnerabilidad radica en la concesión de permisos de administrador a todos los empleados en sus dispositivos. Esto implica que un atacante que obtenga acceso al equipo de un empleado podría ejecutar comandos con los mismos privilegios de administrador.
2	En nuestra aplicación, carecemos de medidas adecuadas para prevenir ataques de XSS almacenado. Esto significa que un atacante podría introducir código malicioso al enviar una solicitud a través del formulario de inicio de sesión.
3	Dado que todos los empleados tienen privilegios de administrador en sus propios dispositivos, como Christian, esto les otorga acceso a funciones y datos para los cuales no deberían tener autorización.

3. Cornucopia

Mario

Q	Dado que ChaseMyCash no realiza ningún tipo de monitoreo a la aplicación no se podrán detectar los ataques en tiempo real.
8	Dado que el bucket S3 carece de cifrado y no tiene un control de acceso apropiado, existe el riesgo de que cualquier persona pueda acceder a los datos almacenados en él.
3	En el caso de que un atacante logre acceder al ordenador de un empleado, podrían obtener acceso al código de la empresa. Esta situación se debe a la falta de un segundo factor de autenticación y a la ausencia de cifrado en los repositorios del código fuente.

Juan

10	Si el software utilizado en la aplicación contiene código malicioso o presenta vulnerabilidades, tanto en las soluciones de código abierto como en las comerciales, Xavier podría aprovechar estas debilidades para acceder a datos encriptados y/o alterar los secretos criptográficos.
K	Si Gareth lograra acceder a la base de datos y la eliminara parcial o totalmente, podría provocar una denegación de servicio. Esta situación se debe a que si Gareth fuera un empleado insatisfecho o lograra obtener credenciales a través de un ataque de phishing dirigido a algún otro empleado, podría obtener una cuenta con privilegios de administración. Además, es importante destacar que no se realizan copias de seguridad automáticas.
6	Si no se manejan correctamente los errores y las excepciones, Aaron podría aprovechar esta debilidad para eludir los controles establecidos en la aplicación.

Gabriel

2	El uso de la licencia de Teams de GitHub podría ofrecer a los equipos de desarrollo recursos y funcionalidades adicionales que contribuyan a evitar estos problemas, al mismo tiempo que facilitan una colaboración más efectiva y una mejor supervisión del código. ***Juan***: En el caso de que la aplicación emplee funciones de lenguaje de programación consideradas riesgosas en lugar de opciones más seguras, o presente errores en la conversión de tipos de datos, Lee podría aprovechar estas fallas para eludir los controles de la aplicación.
4	La ausencia de una política de auditoría o seguimiento de las acciones de los usuarios posibilita que Keith realice acciones sin dejar registros, lo que podría resultar en que sus actividades pasen desapercibidas.
J	Es posible que ChaseMyCash utilice lenguajes de programación desactualizados, como Python 2, o que contenga código reutilizado en un lenguaje que ya no está actualizado. Además, la falta de documentación agrava esta situación.

4. Criptografía

Mario

2	Esta posibilidad se origina debido a la escasez de controles criptográficos implementados, agravada por la falta de cifrado incluso en el bucket de almacenamiento.
3	La ausencia de un sistema de verificación de integridad de los datos es preocupante. Si los datos no son sometidos a este proceso, Axel podría alterarlos sin dejar rastro de su manipulación.
8	Los datos en los buckets de S3 están sin cifrar, mientras que las contraseñas de los usuarios de la aplicación se almacenan en la base de datos utilizando el algoritmo de hash unidireccional SHA-256. Aunque el uso de SHA-256 mejora la seguridad de las contraseñas almacenadas, estas aún podrían ser vulnerables a ataques de fuerza bruta o de diccionario si un atacante logra acceder a la base de datos. Además, las contraseñas temporales se envían por correo electrónico en texto plano y algunas comunicaciones no están cifradas.

Juan

J	La información de los usuarios se guarda de forma segura en la base de datos mediante el uso de cifrado en reposo SHA-256, una medida de seguridad robusta y confiable para proteger las contraseñas. ***Gabriel***: Se podrían aumentar la seguridad si, por ejemplo, se almacenaran las cifraran las contraseñas.
10	Los archivos en los buckets de S3 no cuentan con cifrado, lo cual representa un riesgo para la seguridad de los datos almacenados. Además, las contraseñas de los usuarios están encriptadas en la base de datos utilizando el algoritmo SHA-256, que,

	aunque es seguro, no es la mejor opción para almacenar contraseñas debido a la falta de salting y un factor de lentitud. Esto deja una potencial vulnerabilidad en la seguridad del sistema. Adicionalmente, el envío de contraseñas temporales por correo electrónico en texto plano y la falta de cifrado en algunas comunicaciones también representan preocupaciones en términos de seguridad.
Q	La falta de un sistema de gestión de claves y algoritmos criptográficos adecuado puede llevar a una situación donde los secretos criptográficos sean fácilmente predecibles o estén insuficientemente protegidos. Esto podría permitir a un individuo no autorizado, como Randolph, acceder a estos secretos y descifrar la información protegida.

Gabriel

7	La ausencia de una política de seguridad sólida para las comunicaciones encriptadas plantea riesgos significativos. Si el protocolo de encriptación está mal implementado o configurado de manera débil, o si los certificados no son válidos o confiables, existe la posibilidad de que Gunter pueda interceptar y descifrar los datos encriptados. Incluso si el tráfico entre el frontend y el backend está cifrado, si la comunicación entre el backend y otros servicios carece de cifrado, Gunter podría intentar interceptar la comunicación en ese punto para acceder a la información sensible.
5	La viabilidad de estas acciones se debe a la escasez de controles criptográficos implementados.
4	Aunque la aplicación emplea HTTPS para todas las comunicaciones incluyendo desde el navegador hasta el almacenamiento de datos en la base de datos, se ha identificado que hay otras capas o protocolos donde no se utiliza encriptación. Esto significa que si Paulo logra interceptar la comunicación en alguna de esas capas o protocolos sin encriptar, podría acceder a los datos en tránsito. Por ejemplo, si el tráfico entre el frontend y el backend está cifrado, pero la comunicación entre el backend y otros servicios carece de encriptación, Paulo podría intentar interceptar la comunicación en ese punto.

5. Gestión de la sesión

Mario

3	Sí, parece que Ryan podría usar una sola cuenta simultáneamente, ya que no hay indicación de restricciones para sesiones concurrentes. En sí, la utilización de JSON Web Tokens (JWT) para la autenticación no previene automáticamente la creación de sesiones concurrentes. Cada vez que un usuario inicia sesión, se emite un nuevo JWT, y si no se aplican medidas adicionales para restringir el número de sesiones activas por usuario, es posible que un usuario tenga varios JWT válidos y activos al mismo tiempo.
10	La ausencia de tokens anti-CSRF hace que el sistema sea vulnerable a ese tipo de

	ataque.
8	El sistema presenta una vulnerabilidad potencial en el manejo de sesiones debido al uso del token JWT, el cual incluye los roles del usuario y no tiene un tiempo de expiración. Esta configuración permite que incluso después de que los roles o permisos de un usuario sean revocados, el token seguirá otorgando acceso según los roles previos a la revocación.

Juan

7	Existe la posibilidad de que un usuario cierre el navegador sin que la sesión expire. En tal caso, otro usuario diferente podría potencialmente reutilizar la sesión accediendo al historial del navegador o a las cookies almacenadas.
Q	Es posible que algunas rutas de la aplicación web estén protegidas por medidas de seguridad, mientras que otras no lo lleguen a estar.
K	Debido a la falta de una implementación segura del token, existe el riesgo de que este pueda ser interceptado, manipulado o predicho, lo que permitiría obtener una sesión válida y acceder al sistema de forma no autorizada.

Gabriel

J	Dado que no se han aplicado medidas de seguridad, como el uso de tokens de un solo uso o números aleatorios, los atacantes podrían utilizar un token o ID de sesión previamente utilizado por un usuario legítimo para enviar solicitudes repetidas y acceder de forma no autorizada a recursos corporativos. Esto podría facilitar actividades maliciosas como la manipulación de datos, la realización de transacciones no autorizadas o el robo de información confidencial.
2	Si la aplicación no implementa una gestión adecuada de identificadores de sesión, existe el riesgo de que William pueda generar identificadores de sesión inválidos o duplicados. Esto podría permitir que un atacante tome el control de la sesión de otro usuario. ***Maria***: Existen ciertos endpoints específicos, desde los cuales se manejan los procesos de inicio de sesión en la aplicación y se solicita y envía la información de los usuarios.
9	La falta de una implementación adecuada de la seguridad en la transmisión de datos puede ser una vulnerabilidad significativa. Si los identificadores de sesión se envían a través de canales inseguros, se registran en registros, se revelan en mensajes de error o se incluyen en URLs, Ivan podría interceptarlos y utilizarlos para acceder a la cuenta de otro usuario.

6. Resultados

	Mario	Juan	Gabriel
Requisitos	Cada tarjeta y contribución adicional relevante ha sido valorada con 1 punto.		
Rondas	15	15	15
Puntos	19	20	17

7. Cronología del juego

PRIMERA RONDA:

- **Mario:** 9 (Autorización): +2
- **Juan:** 7 (Autenticación): +1
- **Gabriel:** 4 (Cornucopia): +1

SEGUNDA RONDA:

- **Mario:** 5 (Autorización): +1
- **Juan:** 9 (Autorización): +2
- **Gabriel:** 7 (Criptografía): +1

TERCERA RONDA:

- **Mario:** Q (Cornucopia): +3
- **Juan:** 7 (Gestión de la sesión): +0
- **Gabriel:** 2 (Gestión de la sesión): +1

CUARTA RONDA:

- **Mario:** 3 (Cornucopia): +0
- **Juan:** 10 (Criptografía): +2
- **Gabriel:** 4 (Autenticacion): +1

QUINTA RONDA:

- **Mario:** 3 (Criptografía): +1
- **Juan:** 9 (Cornucopia): +1
- **Gabriel:** Q (Autorización): +2

SEXTA RONDA:

- **Mario:** 8 (Autenticación): +2
- **Juan:** 6 (Cornucopia): +1
- **Gabriel:** 3 (Autenticacion): +1

SÉPTIMA RONDA:

- **Mario:** 10 (Gestión de la sesión): +1
- **Juan:** J (Autorización): +2
- **Gabriel:** 5 (Criptografía): +1

OCTAVA RONDA:

- **Mario:** 2 (Criptografía): +1
- **Juan:** 10 (Autorización): +0
- **Gabriel:** J (Cornucopia): +2

NOVENA RONDA:

- **Mario:** 3 (Gestión de la sesión): +1
- **Juan:** J (Criptografía): +1
- **Gabriel:** 9 (Gestión de la sesión): +2

DECIMA RONDA:

- **Mario:** K (Autorización): +2
- **Juan:** Q (Criptografía): +1
- **Gabriel:** 7 (Criptografía): +1

UNDÉCIMA RONDA:

- **Mario:** 8 (Gestión de la sesión): +3
- **Juan:** 4 (Autorización): +1
- **Gabriel:** 4 (Criptografía): +1

DUODÉCIMA RONDA:

- **Mario:** 6 (Autenticacion): +0
- **Juan:** 10 (Autenticacion): +1
- **Gabriel:** J (Gestión de la sesión): +2

DECIMOTERCERA RONDA:

- **Mario:** 8 (Gestión de la sesión): +1
- **Juan:** 10 (Cornucopia): +2
- **Gabriel:** 2 (Autenticacion): +1

DECIMOCUARTA RONDA:

- **Mario:** 8 (Criptografia): +1
- **Juan:** 9 (Autorización): +2
- **Gabriel:** 3 (Autorización): +0

DECIMOQUINTA RONDA:

- **Mario:** 8 (Cornucopia): +1
- **Juan:** K (Gestión de la sesión): +3
- **Gabriel:** 2 (Cornucopia): +0