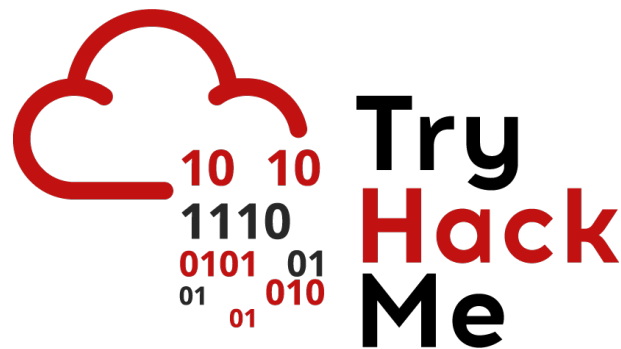


Writeup: Sala *Security Engineer Intro*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 – Introducción	2
2.2. Tarea 2 - ¿Qué es un ingeniero de seguridad?	2
2.3. Tarea 3 - Responsabilidades principales de un ingeniero de seguridad .	2
2.4. Tarea 4 - Mejora continua	3
2.5. Tarea 5 - Funciones y responsabilidades adicionales	4
2.6. Tarea 6 - Caminando en sus zapatos	4
3. Conclusión sobre la Sala	12

1. Introducción

En esta sala obtendremos una comprensión clara y práctica del rol que desempeña un Security Engineer dentro de una organización. Aprenderemos conceptos, sus responsabilidades y desafíos relevantes que enfrenta este perfil profesional.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera tarea, nos explica que en esta sala aprenderemos una visión general del rol del Security Engineer y familiarizarnos con sus actividades diarias y responsabilidades principales.

Pregunta: I have reviewed the learning objectives.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - ¿Qué es un ingeniero de seguridad?

Aprenderemos que un Security Engineer es un profesional responsable de minimizar permanentemente el riesgo cibernético para la organización. alguna de sus funciones principales es asegurar que las medidas de seguridad estén siempre activas y alineadas con los objetivos del negocio.

Una vez comprendido qué es un ingeniero de seguridad, procedemos a responder la siguiente pregunta.

Pregunta: Who ensures that an organization's cyber security risk is minimized at all times?

Respuesta: **Security engineer**

2.3. Tarea 3 - Responsabilidades principales de un ingeniero de seguridad

En esta tarea aprenderemos las responsabilidades esenciales que asume un Security Engineer para proteger y fortalecer la postura de seguridad de una organización. Las responsabilidades que encontramos son:

- **Gestión de activos/Inventario de activos**
- **Políticas de seguridad y excepciones**

- **Seguridad desde el diseño**
- **Evaluación y garantía de seguridad**

Una vez comprendemos las responsabilidades un ingeniero de seguridad, pasamos a responder las siguientes preguntas.

Pregunta: Where are details about an organization's digital assets, such as name, IP address, and owner, stored?

Respuesta: **Asset inventory**

Pregunta: Sometimes security policies can't be followed because of business needs. What avenue does a security engineer have to fulfil business needs in these cases?

Respuesta: **Exceptions**

Pregunta: What philosophy, if followed, provides the most Return on Investment (ROI)?

Respuesta: **Secure by design**

2.4. Tarea 4 - Mejora continua

Vamos a aprender que la seguridad debe evolucionar continuamente y que los siguientes pasos ayudan al ingeniero de seguridad a desempeñar esta función:

- **Garantizar la concientización**
- **Gestión de riesgos**
- **Gestión del cambio**
- **Gestión de vulnerabilidades**
- **Cumplimiento y auditorías**

Ahora que sabemos como un ingeniero de seguridad puede desempeñar una mejora continua, procedemos a responder las siguientes preguntas.

Pregunta: What is considered the weakest link in an organization's security?

Respuesta: **humans**

Pregunta: An organization's security evolves with the organization. What helps a security engineer keep the organization secure through these changes?

Respuesta: **Change management**

2.5. Tarea 5 - Funciones y responsabilidades adicionales

Aprenderemos que en ciertas organizaciones, un ingeniero de seguridad podría necesitar asumir responsabilidades adicionales para ayudar a otros equipos. Algunas responsabilidades adicionales son:

- **Gestión de herramientas de seguridad**
- **Ejercicios de mesa**
- **Recuperación ante desastres y gestión de crisis**

Una vez entendido estas responsabilidades adicionales, responderemos las siguientes preguntas.

Pregunta: What is a theoretical exercise carried out to gauge the operational readiness of an organization from a security point of view?

Respuesta: **Tabletop exercise**

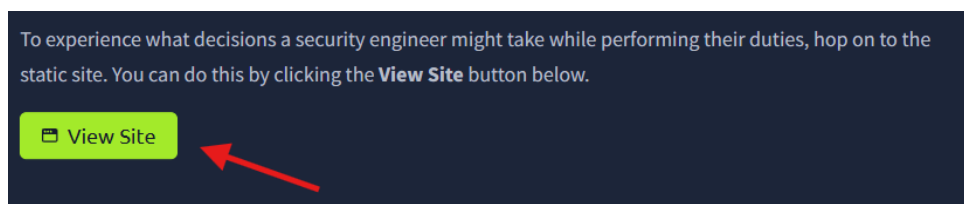
Pregunta: What is the priority of the management in case of a disaster or crisis?

Respuesta: **Business Continuity**

2.6. Tarea 6 - Caminando en sus zapatos

Realizaremos un ejercicio donde se revisa un reporte de VAPT (Vulnerability Assessment & Penetration Test). A partir de los reportes, el Security Engineer propone acciones concretas (como parches, restricciones de acceso, uso de VPN, etc.), mostrando cómo se aplican medidas tangibles dentro de un contexto real.

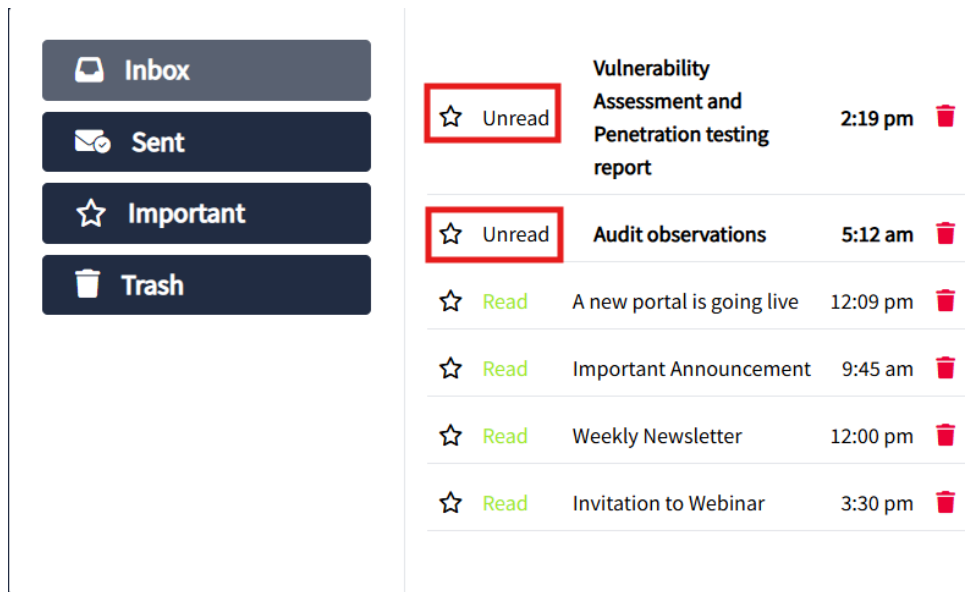
Para desplegar el sitio de práctica debemos hacer clic en **View Site** en el lado inferior de la tarea.



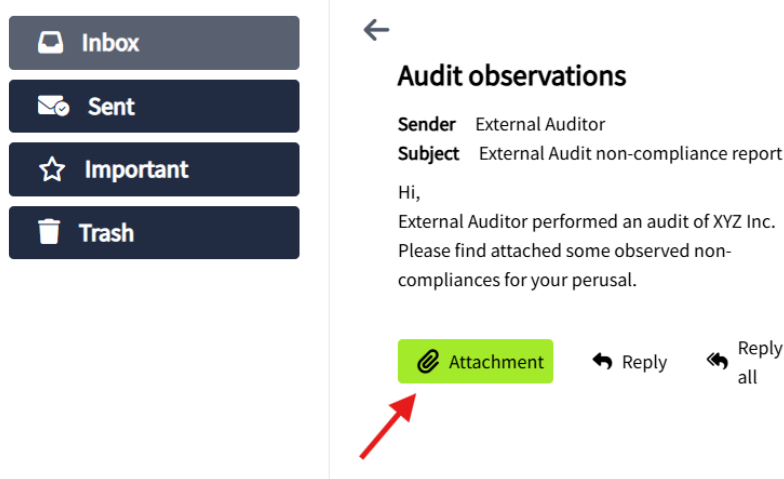
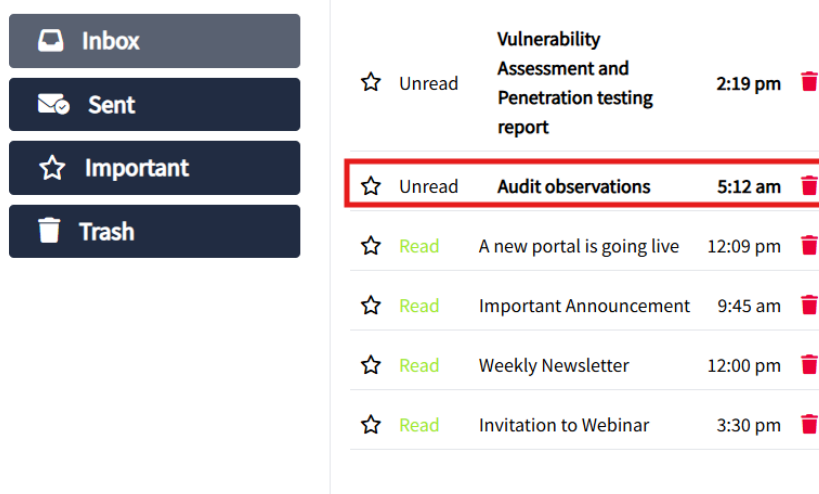
Una vez desplegado el sitio, procederemos a realizar el ejercicio.

Pregunta: What is the flag shown on the completion of the static site?

Para lograr obtener la flag debemos responder los distintos correos que se encuentran en no leído.



Comenzaremos con el primer correo (Audit observations) que nos llegó a las 5:12 am. Haremos clic en el correo y leeremos el contenido, una vez leído haremos clic en la opción de **Attachment** para adjuntar los incumplimientos observados.



Una vez hecho clic, debemos leer el informe de incumplimiento de la auditoría y seleccionar la respuesta que mejor se adapte de las opciones disponibles para mitigar los incumplimientos de acuerdo con la información.

Remaining Attempts 2/2

Question 1/2

External Audit non-compliance report

Observation 1

Requirements

All assets of XYZ Inc. should have the latest Operating System security updates installed.

Observation

Though most systems had the latest OS security updates, some legacy systems that supported XYZ Inc.'s older hardware didn't have the latest security updates.

XYZ Inc. Comments

These systems are older and installing security updates on them might break the functionality of these systems.

Keep as it is

Rebuild the legacy servers so that they don't break with security updates

Install security updates

Restrict accessibility of the servers to only required usage

Remaining Attempts 2/2

Question 1/2

External Audit non-compliance report

Observation 1

Requirements

All assets of XYZ Inc. should have the latest Operating System security updates installed.

Observation

Though most systems had the latest OS security updates, some legacy systems that supported XYZ Inc.'s older hardware didn't have the latest security updates.

XYZ Inc. Comments

These systems are older and installing security updates on them might break the functionality of these systems.

Keep as it is

Rebuild the legacy servers so that they don't break with security updates

Install security updates

Restrict accessibility of the servers to only required usage

Después que seleccionamos la opción correcta, pasamos a la siguiente observación.

Remaining Attempts 2/2

Question 2/2

External Audit non-compliance report

Observation 2

Requirements

All network communication, user activity, and security device logs shall be aggregated in a single platform (SIEM) and monitored continuously.

Observation

XYZ Inc. has some assets in the cloud and others on-prem. It was observed that the cloud assets were not integrated with the SIEM, which is present on-prem.

XYZ Inc. Comments

The logs from the cloud are not integrated with the SIEM because this will require enabling internet access to the SIEM, which is not desirable.

Aggregate cloud logs in a single place. Forward the logs from that place to on-prem network using a restricted tunnel

Keep as it is

Rebuild the applications on the cloud to on-prem or vice versa

Forward cloud logs to SIEM regardless of concerns of XYZ Inc

Remaining Attempts 2/2

Question 2/2

External Audit non-compliance report

Observation 2

Requirements

All network communication, user activity, and security device logs shall be aggregated in a single platform (SIEM) and monitored continuously.

Observation

XYZ Inc. has some assets in the cloud and others on-prem. It was observed that the cloud assets were not integrated with the SIEM, which is present on-prem.

XYZ Inc. Comments

The logs from the cloud are not integrated with the SIEM because this will require enabling internet access to the SIEM, which is not desirable.

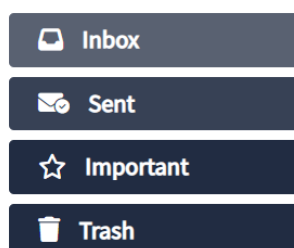
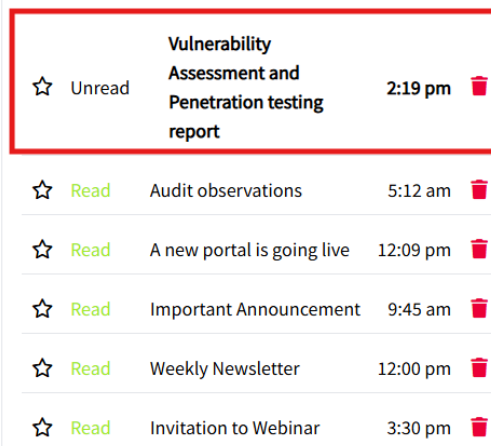
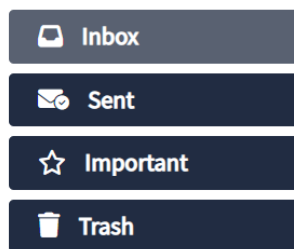
Aggregate cloud logs in a single place. Forward the logs from that place to on-prem network using a restricted tunnel

Keep as it is

Rebuild the applications on the cloud to on-prem or vice versa

Forward cloud logs to SIEM regardless of concerns of XYZ Inc

Ahora que logramos completar la primera tarea, pasaremos con el siguiente correo no leído. Para ello, haremos clic en el correo y realizaremos los mismos pasos previos que hicimos para responder al primer correo.




Vulnerability Assessment and Penetration testing report

Sender External Pentest Vendor

Subject VAPT results - XYZ Inc.

Hi,

External Pentest Vendor performed VAPT of XYZ Inc.'s external facing infrastructure. Please find attached the report for the VAPT activity.

 Attachment

 Reply

 Reply all



Remaining Attempts 2/2

Question 1/3

VAPT report

Vulnerability 1

Asset Name

Oracle-backend-DB-Server
ORACLE MYSQL VULNERABILITY: CVE-2022-21417

Description

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows a high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Recommended Solution

Upgrade to the latest version of Oracle MySQL
Download and apply the upgrade from: <http://dev.mysql.com/downloads/mysql>

Restrict accessibility of the server
only through VPN or internal
network

Patch the vulnerability

Rebuild the server

Keep as it is

Remaining Attempts 2/2

Question 1/3

VAPT report

Vulnerability 1

Asset Name

Oracle-backend-DB-Server
ORACLE MYSQL VULNERABILITY: CVE-2022-21417

Description

Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Easily exploitable vulnerability allows a high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

Recommended Solution

Upgrade to the latest version of Oracle MySQL
Download and apply the upgrade from: <http://dev.mysql.com/downloads/mysql>

Restrict accessibility of the server
only through VPN or internal
network

Patch the vulnerability

Rebuild the server

Keep as it is

Remaining Attempts 2/2

VAPT report

Question 2/3

Vulnerability 2

Asset Name

corporate-client-portal
OPENSSL THE C. REHASH SCRIPT ALLOWS COMMAND INJECTION (CVE-2022-2068)

Description

In addition to the c. rehash shell command injection identified in CVE-2022-1292, further circumstances where the c. rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed, it was not discovered that there were other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c. rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

Recommended Solution

- Upgrade to OpenSSL version 1.0.2zf
- Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-1.0.2zf.tar.gz>
Upgrade to version 1.0.2zf of OpenSSL (<http://www.openssl.org>). The source code for this release can be downloaded from OpenSSL's website (<http://ftp.openssl.org/source/openssl-1.0.2zf.tar.gz>). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.
- Upgrade to OpenSSL version 1.1.1p
- Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-1.1.1p.tar.gz> Upgrade to version 1.1.1p of OpenSSL (<http://www.openssl.org>). The source code for this release can be downloaded from OpenSSL's website (<http://ftp.openssl.org/source/openssl-1.1.1p.tar.gz>). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.
- Upgrade to OpenSSL version 3.0.4 Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-3.0.4.tar.gz> Upgrade to version 3.0.4 of OpenSSL (<http://www.openssl.org>). The source code for this release can be downloaded from OpenSSL's website (<http://ftp.openssl.org/source/openssl-3.0.4.tar.gz>). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

Patch the vulnerability

Rebuild the server

Restrict accessibility of the server only through VPN or internal network

Keep as it is

Remaining Attempts 2/2

VAPT report

Question 2/3

Vulnerability 2

Asset Name

corporate-client-portal
OPENSSL THE C. REHASH SCRIPT ALLOWS COMMAND INJECTION (CVE-2022-2068)

Description

In addition to the c. rehash shell command injection identified in CVE-2022-1292, further circumstances where the c. rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed, it was not discovered that there were other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c. rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).

Recommended Solution

- Upgrade to OpenSSL version 1.0.2zf
- Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-1.0.2zf.tar.gz>
Upgrade to version 1.0.2zf of OpenSSL (<http://www.openssl.org>). The source code for this release can be downloaded from OpenSSL's website (<http://ftp.openssl.org/source/openssl-1.0.2zf.tar.gz>). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.
- Upgrade to OpenSSL version 1.1.1p
- Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-1.1.1p.tar.gz> Upgrade to version 1.1.1p of OpenSSL (<http://www.openssl.org>). The source code for this release can be downloaded from OpenSSL's website (<http://ftp.openssl.org/source/openssl-1.1.1p.tar.gz>). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.
- Upgrade to OpenSSL version 3.0.4 Download and apply the upgrade from: <http://ftp.openssl.org/source/openssl-3.0.4.tar.gz> Upgrade to version 3.0.4 of OpenSSL (<http://www.openssl.org>). The source code for this release can be downloaded from OpenSSL's website (<http://ftp.openssl.org/source/openssl-3.0.4.tar.gz>). To obtain binaries for your platform, please visit your vendor's site. Please note that many operating system vendors choose to apply the most recent OpenSSL security patches to their distributions without changing the package version to the most recent OpenSSL version number.

Patch the vulnerability

Rebuild the server

Restrict accessibility of the server only through VPN or internal network

Keep as it is

Remaining Attempts 2/2

Question 3/3

VAPT report

Vulnerability 3

Asset Name

corporate-website-public

APACHE HTTPD: MOD_LUA USE OF UNINITIALIZED VALUE OF IN R:PARSEBODY (CVE-2022-22719)

Description

A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

Recommended Solution

- Apache HTTPD ≥ 2.4 and $< 2.4.53$
- Upgrade to Apache HTTPD version 2.4.53
- Apache HTTPD version 2.4.53 Download and apply the upgrade from:
<http://archive.apache.org/dist/httpd/httpd2.4.53.tar.gz>
- Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

Keep as it is

Patch the vulnerability

Restrict accessibility of the server only
through VPN or internal network

Rebuild the server

Remaining Attempts 2/2

Question 3/3

VAPT report

Vulnerability 3

Asset Name

corporate-website-public

APACHE HTTPD: MOD_LUA USE OF UNINITIALIZED VALUE OF IN R:PARSEBODY (CVE-2022-22719)

Description

A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

Recommended Solution

- Apache HTTPD ≥ 2.4 and $< 2.4.53$
- Upgrade to Apache HTTPD version 2.4.53
- Apache HTTPD version 2.4.53 Download and apply the upgrade from:
<http://archive.apache.org/dist/httpd/httpd2.4.53.tar.gz>
- Many platforms and distributions provide pre-built binary packages for Apache HTTP server. These pre-built packages are usually customized and optimized for a particular distribution, therefore we recommend that you use the packages if they are available for your operating system.

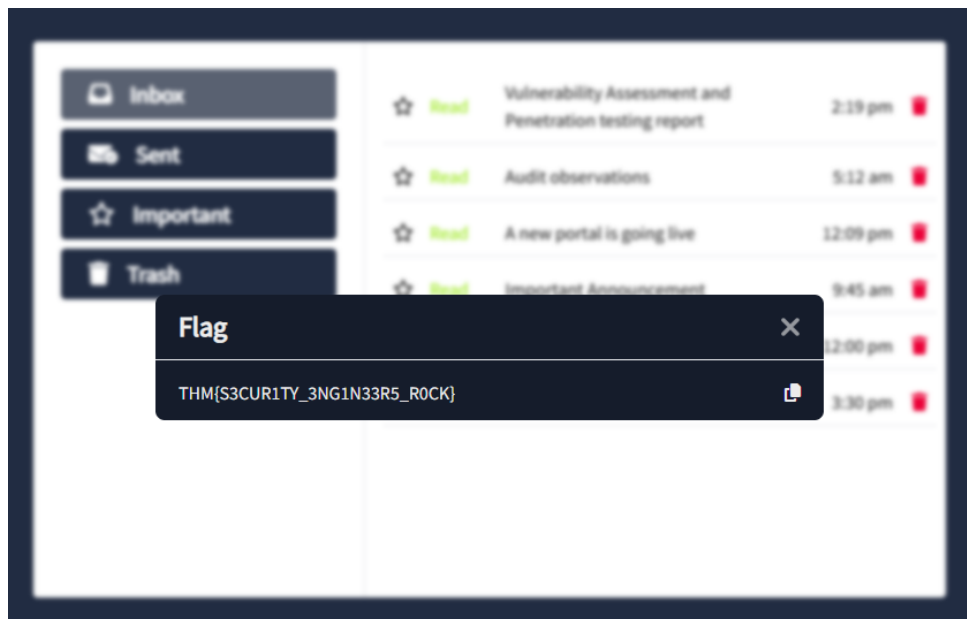
Keep as it is

Patch the vulnerability

Restrict accessibility of the server only
through VPN or internal network

Rebuild the server

Una vez que logramos responder correctamente, lograremos obtener la flag para completar la tarea.



Respuesta: **THM{S3CUR1TY_3NG1N33R5_R0CK}**

3. Conclusión sobre la Sala

Una vez finalizamos la sala, obtenemos una visión integral del trabajo que realiza un Security Engineer y su impacto en la postura de seguridad de una organización.

Logramos comprender en profundidad sus principales funciones, como la creación de políticas, la aplicación del principio de secure by design y la planificación de evaluaciones de seguridad. Además, aprendimos la importancia de la mejora continua y de una colaboración efectiva con otros equipos técnicos y de negocio.