HACKING ÉTICO

Tarea 1

ESTHER CARRILLO GÁLVEZ

Índice

1. Apartado 1: Diseñar el plan de auditoría 3
2. Apartado 2: Organiza las fases de la auditoría 6
   2.1. Calendario de auditorías 2026 8
3. Apartado 3: Presentación y valoración de vulnerabilidades especificando los grupos de métricas base y temporal 9
   3.1. Vulnerabilidad en sistema de correo mediante ejecución remota de código (RCE) 9
   3.2. Vulnerabilidad de inyección SQL (base de datos de contabilidad) 12
   3.3. Vulnerabilidad RCE en Servidor FTP 16
4. Bibliografía: 21

1. Apartado 1: Diseñar el plan de auditoría

Nombre de la Auditoría	**Justificación de la Auditoría**	**Activo(s) y justificación**	**Enfoque (manual, automática, etc)**	**Origen (interna o externa)**	**Información proporcionada (tipo de caja)**	**Objetivo**
Auditoría de intrusión a activos críticos	Esta auditoría se enfoca en el Test de intrusión manual externo de caja negra, cuya finalidad es la necesidad de proteger los 3 activos expuestos que representan la mayor amenaza para el negocio. Para ello, se demuestra la explotación de las vulnerabilidades y el impacto de un ataque.	· **Servidor de correo electrónico**: muy crítico debido a la información confidencial que contiene acerca de la empresa (phishing, robo de mensajes). · **Servidor FTP**: es un acceso muy crítico debido a la vulnerabilidad de ejecución remota de código y permite el movimiento lateral a la red. · **Servidor web**: impacto muy crítico para el negocio, ya que compromete la integridad de los datos financieros sensibles.	Para activos de alta criticidad, la detección rápida se logra con herramientas automáticas, pero la penetración profunda se logra con el análisis manual. Para el reconocimiento activo, se utilizarán herramientas de scanning, lo que permitirá descubrir fallos o vulnerabilidades.	El origen es externo con el objetivo de simular el ataque anónimo que intenta acceder al sistema.	El origen externo es respaldado por el enfoque de caja negra. Esto es, la persona auditora no recibirá ninguna información interna, ya sean credenciales de acceso o código fuente.	Realizar una auditoría externa de ciberseguridad con el fin de determinar su exposición a un ataque dirigido hacia al menos uno de los 3 activos críticos de modo que el atacante consiga escalar privilegios sobre el sistema comprometido.
Auditoría de	Tiene como objetivo proteger y salvaguardar	·**Pasarela de compra:** muy crítico ya que cualquier formulario que	Es un enfoque principalmente manual. Sin	Externa. El objetivo es	Caja gris. La persona atacante	El objetivo es identificar y explotar fallos críticos

Nombre de la Auditoría	Justificación de la Auditoría	Activo(s) y justificación	Enfoque (manual, automática, etc)	Origen (interna o externa)	Información proporcionada (tipo de caja)	Objetivo
aplicaciones web	la integridad del negocio y de los datos más sensibles que maneja la aplicación mediante una auditoría manual externa de caja gris.	maneje datos bancarios debe tener una correcta sanitización de los datos para evitar fallos. · **Bases de datos de usuarios**: es muy crítico porque está vinculada a la aplicación web y podrían exfiltrarse los datos de clientes.	embargo, se trata de un test de penetración híbrido porque la automatización se queda en la superficie y el enfoque híbrido puede modelar al atacante y garantizar una lógica de negocio protegida.	simular un ataque remoto por un atacante previamente autenticado.	tiene cierta información porque ya se ha autenticado en el sistema previamente al ataque.	con el fin de conseguir el robo de datos mediante una escalada de privilegios.
Auditoría de seguridad perimetral	La auditoría de seguridad perimetral automática y de caja negra tiene como objetivo: ·**Prevención de intrusiones:** Identificación de puntos débiles en firewalls, IDS/IPS y otros sistemas	Incluye los activos perimetrales que no son críticos para el negocio, es decir, aquellos servicios secundarios que la empresa expone sin darse cuenta. Así como, cualquier host de desarrollo que esté expuesto públicamente por error o la página de blogs.	Enfoque automático. Prioriza la velocidad mediante el uso de scanners que permitan comprobar las vulnerabilidades que tiene una organización en su perímetro exterior.	Externa. Esta elección simula un ataque automatizado para evaluar el nivel de	Caja negra. No se proporcionan credenciales de acceso o información interna, de modo que la auditoría simula un ataque real basándose en la información	Evaluación exhaustiva de la infraestructura, analizando los puntos de entrada potenciales y las vulnerabilidades existentes. Uso de herramientas avanzadas de escaneo y auditoría para identificar los riesgos de

Nombre de la Auditoría	Justificación de la Auditoría	Activo(s) y justificación	Enfoque (manual, automática, etc)	Origen (interna o externa)	Información proporcionada (tipo de caja)	Objetivo
	de protección. ·**Evaluación de configuraciones:** Revisión de políticas de seguridad, reglas de acceso y segmentación de red. ·**Análisis de vulnerabilidades:** Detección de brechas explotables por ciberdelincuentes.			exposición real.	accesible desde internet.	seguridad y determinar el nivel de exposición de la red. Identificación de posibles brechas de seguridad y puntos débiles en la red.

2. Apartado 2: Organiza las fases de la auditoría

Auditoría	Duración	Fases				
		Toma de requisitos	**Realización de pruebas**	**Seguimiento de pruebas**	**Reporting**	**Cierre de auditoría**
Auditoría de intrusión a activos críticos	Duración total 17 días: Toma de requisitos 2 días. Realización de pruebas 8 días. Seguimiento de pruebas 2 días. Reporting 3 días. Cierre de auditoría 2 días.	· Firma de contrato y definición de las autorizaciones. · Técnica que se utilizará para la intrusión. · Preparación del entorno de la persona auditora. · Reconocimiento pasivo (recopilación de información pública).	· Reconocimiento activo mediante escaneo de puertos y servicios con herramientas automáticas como *Nmap* o *Exploit-db.* · Explotación: obtener un primer acceso. · Post-explotación: escalar privilegios una vez dentro del sistema y conseguir movimiento lateral hacia la red interna.	Se debe llevar a cabo reuniones periódicas para aclarar dudas y avisar de incidencias graves.	Elaboración del informe técnico con evidencia (capturas de pantalla). Redacción del informe ejecutivo, incluyendo, una calificación de severidad según el estándar CVSS.	Reunión final de cierre de auditoría para presentar las soluciones para estas vulnerabilidades que podrían comprometer a la empresa.
Auditoría de aplicaciones web	Duración total 12 días:	· Se detallarán las rutas de negocio y	La fase de ejecución	Se debe llevar a cabo reuniones	El proyecto concluye con el	Presentación de documentos

	Toma de requisitos 1 día. Realización de pruebas 6 días. Seguimiento de pruebas 2 días. Reporting 2 días Cierre de auditoría 1 día.	la estructura de la aplicación. · Definir el rol de usuario una vez se hayan obtenido las credenciales. · Acordar con el cliente hasta qué punto se explotarán las vulnerabilidades en base a los límites establecidos por el mismo.	comienza con la el rastreo de tráfico sospechoso mediante un mapeo de la aplicación web con el uso de herramientas proxy, como Burp Suite. Finalmente, se procede a la explotación para demostrar el impacto de las vulnerabilidades.	periódicas para aclarar dudas y avisar de incidencias graves al cliente.	informe técnico final, donde se incluye una descripción detallada de las vulnerabilidades explotadas. Además del informe ejecutivo que se centra en el impacto real y crítico de los datos y lógica de negocio	técnicos donde se muestren los compromisos más críticos.
Auditoría de seguridad perimetral	Duración 10 días. Toma de requisitos 1 día. Realización de pruebas 6 días. Seguimiento de pruebas 1 día. Reporting 1 día. Cierre de auditoría 1 día.	Redacción de la lista de los activos no críticos que se van a escanear. Establecer límite de horarios en los que se podrá trabajar sin afectar a los empleados.	Reconocimiento activo mediante escaneo de puertos y servicios con herramientas automáticas. Detección de brechas explotables.	Control de calidad: se procesarán los resultados del escaneo con el fin de filtrar falsos positivos.	Elaboración del informe técnico detallando la lista de vulnerabilidades encontradas. Redacción del informe ejecutivo, incluyendo, una calificación de severidad según el estándar CVSS.	Reunión de cierre formal para la presentación de los fallos más críticos y poner en común los conocimientos con el cliente.

2.1. Calendario de auditorías 2026

Abril			
1	Mi		
2	**Ju**	**Jueves Santo**	
3	**Vi**	**Viernes Santo**	
4	**Sá**		
5	**Do**	Domingo de Pascua	
6	Lu	Lunes de Pascua	15
7	Ma	**Inicio** ASP-TOMA REQUISITOS	
8	Mi	ASP-REALIZACIÓN PRUEBAS	
9	Ju		
10	Vi		
11	**Sá**		
12	**Do**		
13	Lu		16
14	Ma		
15	Mi		
16	Ju	ASP-SEGUIMIENTO PRUEBAS	
17	Vi	ASP-REPORTING	
18	**Sá**		
19	**Do**		
20	Lu	ASP-CIERRE AUDITORÍA	17
21	Ma		
22	Mi		
23	Ju		
24	Vi		
25	**Sá**		
26	**Do**		
27	Lu		18
28	Ma		
29	Mi		
30	Ju		

Mayo			
1	**Vi**	**Fiesta del Trabajo**	
2	**Sá**		
3	**Do**	Día de la Madre	
4	Lu	**Inicio** AW-TOMA REQUISITOS	19
5	Ma	AW-REALIZACIÓN PRUEBAS	
6	Mi		
7	Ju		
8	Vi		
9	**Sá**		
10	**Do**		
11	Lu		20
12	Ma		
13	Mi	AW-SEGUIMIENTO PRUEBAS	
14	Ju		
15	Vi	AW-REPORTING	
16	**Sá**		
17	**Do**		
18	Lu		21
19	Ma	AW-CIERRE AUDITORÍA	
20	Mi		
21	Ju		
22	Vi		
23	**Sá**		
24	**Do**	Pentecostés	
25	Lu		22
26	Ma		
27	Mi		
28	Ju		
29	Vi		
30	**Sá**		
31	**Do**		

Junio			
1	Lu	**Inicio** AIAC-TOMA REQUISITOS	23
2	Ma		
3	Mi	AIAC- REALIZACIÓN PRUEBAS	
4	Ju		
5	Vi		
6	**Sá**		
7	**Do**		
8	Lu		24
9	Ma		
10	Mi		
11	Ju		
12	Vi		
13	**Sá**		
14	**Do**		
15	Lu	AIAC-SEGUIMIENTO PRUEBAS	25
16	Ma		
17	Mi	AIAC-REPORTING	
18	Ju		
19	Vi		
20	**Sá**		
21	**Do**		
22	Lu	AIAC-CIERRE AUDITORÍA	26
23	Ma		
24	Mi		
25	Ju		
26	Vi		
27	**Sá**		
28	**Do**		
29	Lu		27
30	Ma		

3. Apartado 3: Presentación y valoración de vulnerabilidades especificando los grupos de métricas base y temporal

3.1. Vulnerabilidad en sistema de correo mediante ejecución remota de código (RCE).

Calificación métrica base: 10 (Crítica)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:F/RL:O/RC:C

MÉTRICA BASE	Valor seleccionado	Justificación
Attack vector (AV)	Network (N)	El servidor está expuesto en internet
Attack Complexity (AC)	Low (L)	Exploit público y accesible desde *exploit-db*
Privileges Required (PR)	None (N)	No existe acceso a credenciales de usuario
User Interaction (UI)	None (N)	No requiere acción de usuario
Scope (S)	Changed (C)	Se ha obtenido control total con capacidad de suplantación
Confidentiality (C)	High (H)	Acceso a los mensajes de cualquier usuario
Integrity (I)	High (H)	Capacidad del atacante de suplantar identidades
Availability (A)	High (H)	El control total del servidor por parte del atacante

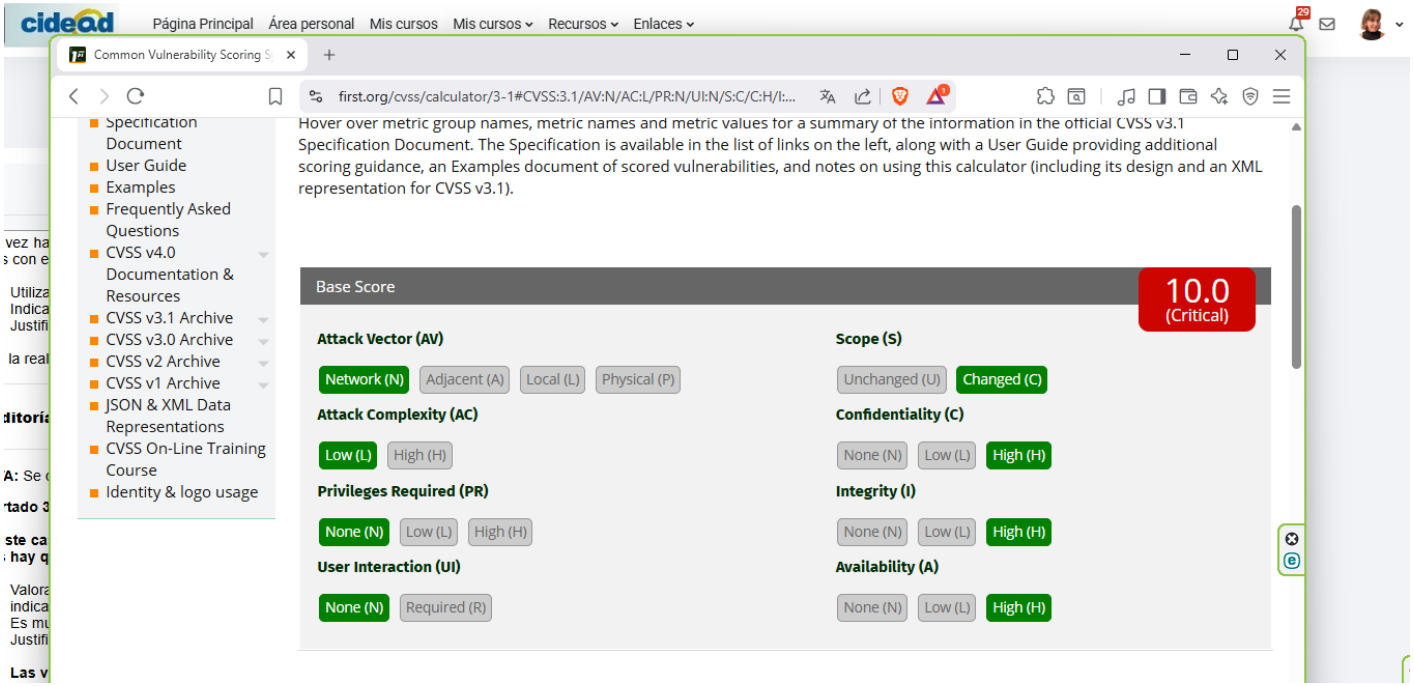

Figura 1. Métrica base vulnerabilidad de servidor de correo.

Calificación métrica temporal: 9,3 (Crítica)

MÉTRICA TEMPORAL	Valor seleccionado	Justificación
Exploit Code Maturity (E)	Functional (F)	Exploit público y fiable disponible en *exploit-db*
Remediation Level (RL)	Official Fix (O)	El fabricante ha publicado un parche oficial para solucionar la vulnerabilidad
Report Confidence (RC)	Confirmed (C)	La vulnerabilidad es pública y confirmada por una empresa externa

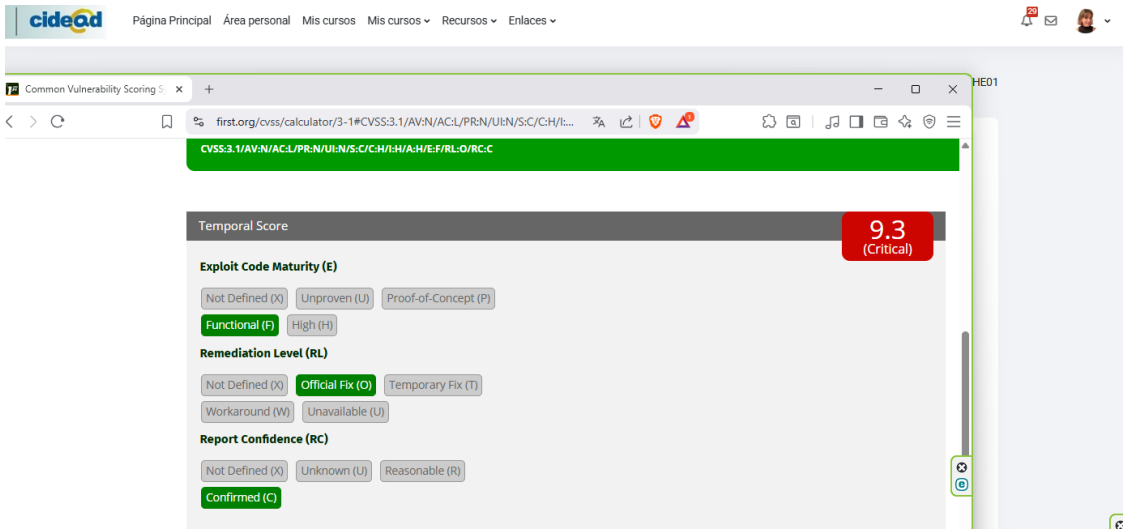

Figura 1. Métrica temporal vulnerabilidad de servidor de correo.

3.2. Vulnerabilidad de inyección SQL (base de datos de contabilidad)

Calificación métrica base: 9,9 (Crítica)

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:L/E:P/RL:U/RC:C

MÉTRICA BASE	Valor seleccionado	Justificación
Attack vector (AV)	Network (N)	El servidor está expuesto en internet
Attack Complexity (AC)	Low (L)	Baja complejidad, ya que no depende de condiciones ambientales difíciles
Privileges Required (PR)	Low (L)	Autenticación de usuario para acceder a vulnerabilidad
User Interaction (UI)	None (N)	No requiere acción de usuario
Scope (S)	Changed (C)	El incidente implica una expansión del alcance, permitiendo la propagación desde la Base de Datos Web hasta la Base de Datos de Contabilidad
Confidentiality (C)	High (H)	Exposición de la Base de Datos de Contabilidad

Integrity (I)	High (H)	Capacidad del atacante de modificación o destrucción de los datos
Availability (A)	Low (L)	No existe riesgo de interrupción del servicio

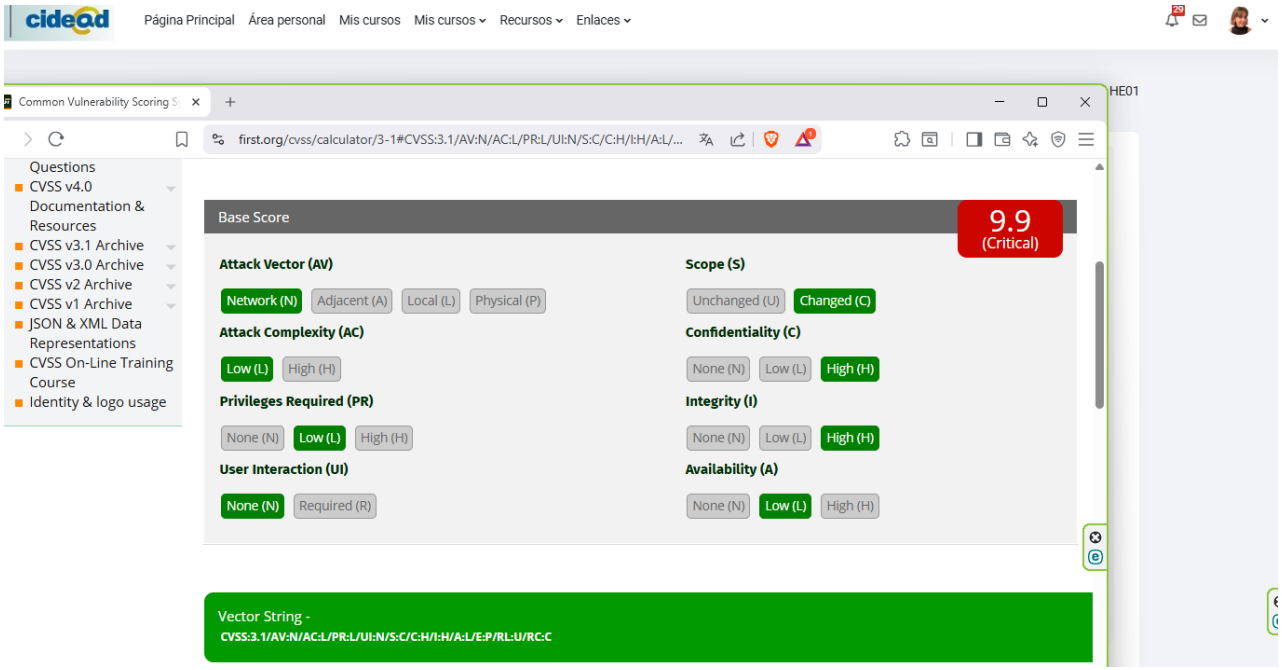

Figura 3. Métrica base vulnerabilidad de inyección SQL.

Calificación métrica temporal: 9,4 (Crítica)

MÉTRICA TEMPORAL	Valor seleccionado	Justificación
Exploit Code Maturity (E)	Proof of concept (P)	Vulnerabilidad localizada a tiempo al inicio de la auditoría (Zero-Day)
Remediation Level (RL)	Unavailable (U)	El fabricante aún no ha publicado un parche oficial para solucionar la vulnerabilidad
Report Confidence (RC)	Confirmed (C)	La vulnerabilidad es confirmada por la persona auditora

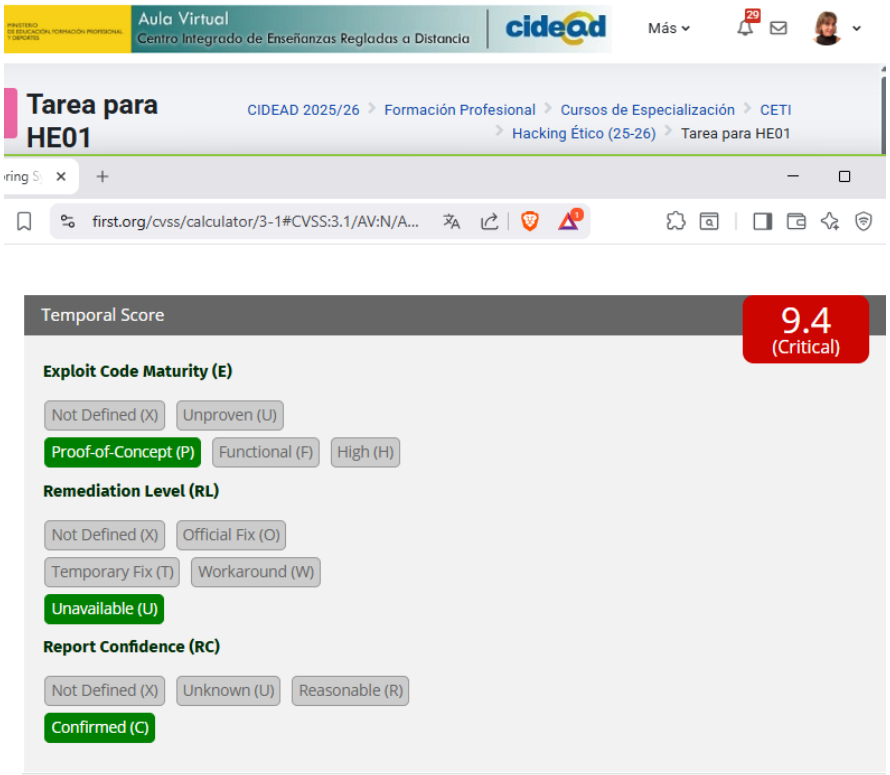

Figura 4. Métrica temporal vulnerabilidad de inyección SQL.

3.3. Vulnerabilidad RCE en Servidor FTP

Calificación métrica base: 8,3 (Alta)

Vector CVSS: **CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C**

MÉTRICA BASE	Valor seleccionado	Justificación
Attack vector (AV)	Adjacent (A)	El servidor FTP está en la red interna, por lo que se necesita que el atacante esté en la misma red
Attack Complexity (AC)	High (H)	Alta complejidad. El hecho de que la prueba de concepto (PoC) requiriera modificaciones complejas sugiere que solo un atacante con un alto nivel de experiencia técnica podría aprovecharla
Privileges Required (PR)	None (N)	Sin autenticación de usuario para acceder a vulnerabilidad
User Interaction (UI)	None (N)	No requiere acción de usuario, ya que la explotación es directa contra el servicio FTP
Scope (S)	Changed (C)	El incidente implica una expansión del alcance, permitiendo la

		propagación a un dominio de seguridad diferente
Confidentiality (C)	High (H)	Impacto alto, ya que permite robar información de la red de administración
Integrity (I)	High (H)	Capacidad del atacante de modificación o destrucción de los datos
Availability (A)	High (H)	Existe riesgo de la interrupción del servicio

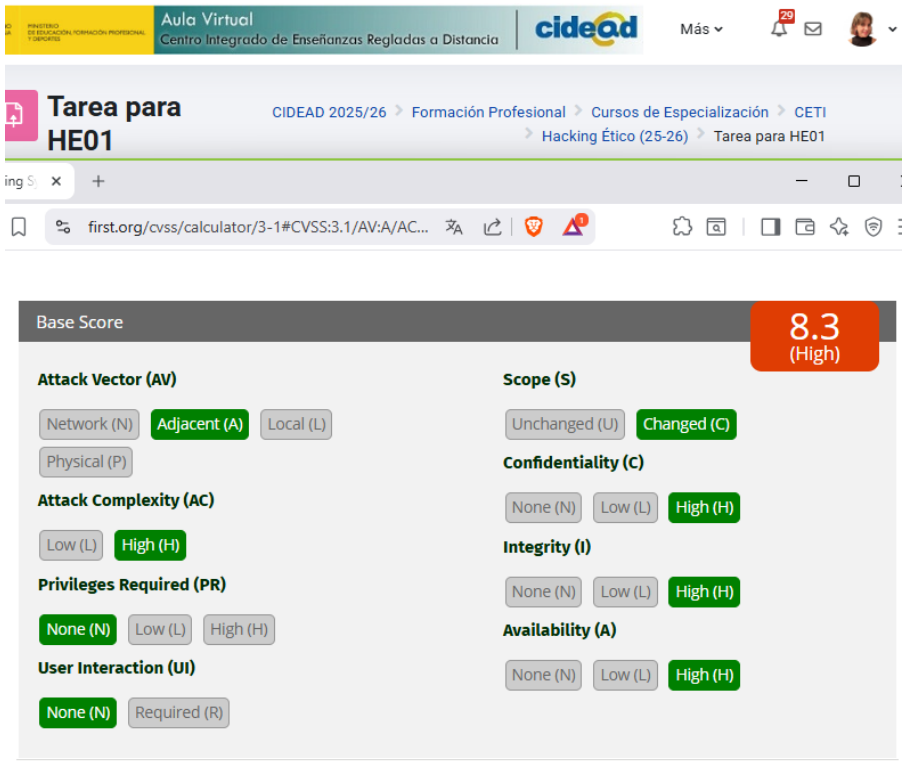

Figura 5. Métrica base vulnerabilidad en Servidor FTP.

Calificación métrica temporal: 7,5 (Alta)

MÉTRICA TEMPORAL	Valor seleccionado	Justificación
Exploit Code Maturity (E)	Proof of concept (PoC)	No hay código de ataque público, lo que requiere conocimiento especializado para adaptar una PoC y lograr la explotación
Remediation Level (RL)	Unavailable (U)	El fabricante ha publicado un parche oficial para solucionar la vulnerabilidad
Report Confidence (RC)	Confirmed (C)	La vulnerabilidad es confirmada y explotada por la persona auditora

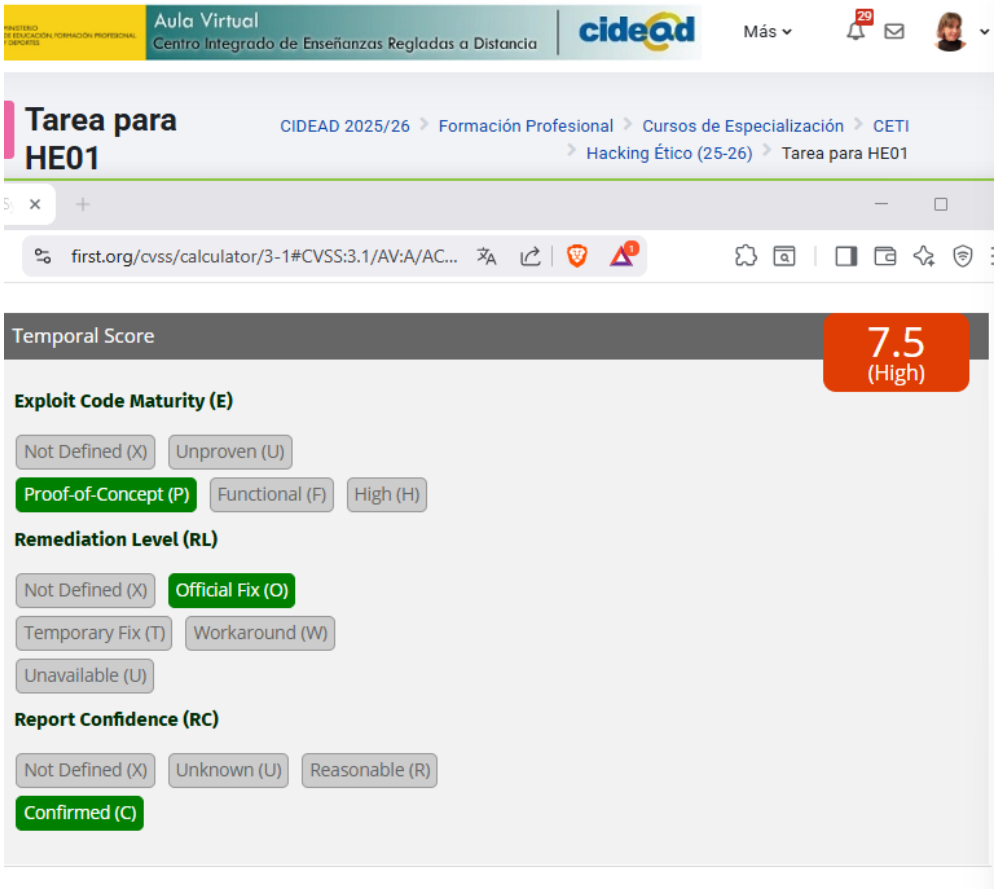

Figura 6. Métrica temporal vulnerabilidad en Servidor FTP.

4. Bibliografía:

INCIBE. (2019, 4 de julio). *¿Qué es el pentesting? Auditando la seguridad de tus sistemas*. INCIBE. https://www.incibe.es/empresas/blog/el-pentesting-auditando-seguridad-tus-sistemas

CREST. (2022). *CREST Defensible Penetration Test (CDPT) Guidance for commercially reasonable assurance activity* (Versión 5.2). https://www.crest-approved.org/wp-content/uploads/2022/12/CREST-Defensible-Penetration-Test-v5-2.pdf

Dolbuck. (s.f.). *Auditoría de seguridad perimetral*. Dolbuck. https://dolbuck.net/auditoria-seguridad-perimetral/

INCIBE. (s.f.). *Análisis de CVE-2023-49274*. [Originalmente Miggo]. Miggo. https://www.miggo.io/vulnerability-database/cve/CVE-2023-49274

Inforges. (s.f.). *¿Qué es el Hacking Ético y cómo se lleva a cabo?* Inforges. https://inforges.es/blog/que-es-el-hacking-etico-y-como-se-lleva-a-cabo/

IsecAuditors. (s.f.). *Auditoría de aplicación web*. IsecAuditors. https://www.isecauditors.com/auditoria-de-aplicacion-web

National Institute of Standards and Technology (NIST). (2008). *Technical Guide to Information Security Testing and Assessment* (NIST Special Publication 800-115). U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

Nivel 13 Ciberseguridad. (s.f.). *Auditoría perimetral*. Nivel 13 Ciberseguridad. https://www.nivel13.es/auditoria-perimetral/

OpenWebinars. (s.f.). *Fases del Pentesting: pasos para asegurar tus sistemas*. OpenWebinars. https://openwebinars.net/blog/fases-del-pentesting-pasos-para-asegurar-tus-sistemas/

Penetration Testing Execution Standard (PTES). (s.f.). *Main Page*. http://www.pentest-standard.org/index.php/Main_Page

SonicWall. (s.f.). *SMTP Smuggling*. SonicWall Blog. https://www.sonicwall.com/blog/smtp-smuggling