12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

SOCHISI
DIGITAL SECURITY THINK TANK

"Ethical Hacking y buenas practicas para el Desarrollo de software"

Speaker:

Andres Barrientos Cisternas – Seguridad de la Información – Ethical Hacking

Linkedin

https://www.linkedin.com/in/andresbarrientosc/

SOCHISI.CL/ENVIVO

¡Bienvenidos a la charla de hoy!

El menú

01 Ethical Hacking

02 Software Confiable

03 Proceso Integrado de Desarrollo

04 ¿Qué Controlamos?

05 Preguntas Clave

06 Repaso Controles Comunes

07 Datos En Transito

08 Almacenamiento

09 Tip Sorpresa

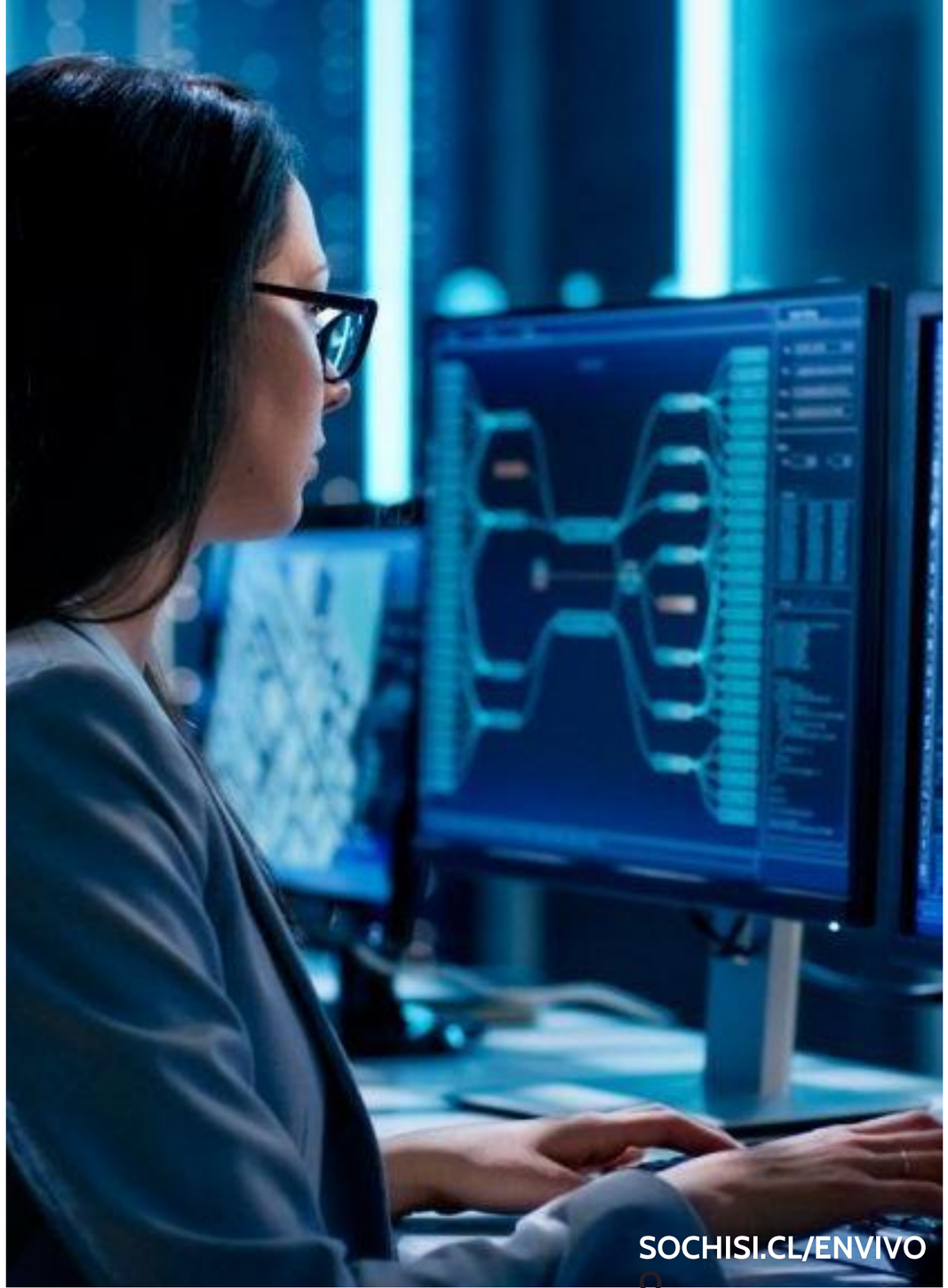
SOCHISI
DIGITAL SECURITY
THINK TANK

Ethical Hacking

Definición

Para las corporaciones el ethical hacking, es una validación de seguridad amplia, la cual enfrenta a la aplicación, a un entorno real en el cual se pueden presentar ataques para intentar vulnerar o defraudar un sistema informático.

Realidad = Punto de Control



Ethical Hacking + desarrollo seguro

=

Software confiable

Integridad

El software responde al objetivo del negocio, manteniendo su integridad en los datos.

Traza

Se dispone de trazabilidad completa del viaje a nivel de datos y servicios.

Control

Se establecen puntos de control definidos, extracción de datos , y se cubre el control de la aplicación interna mediante logs i/o revisión de los mismos.

Autentificación

Se asegura la identificación y autorización del usuario al sistema. Se implementan controles como 2FA o OTG

SOCHISI
DIGITAL SECURITY THINK TANK

Proceso de Desarrollo

Inserción del ethical hacking en el proceso de desarrollo software = consultoría interna

SOCHISI
DIGITAL SECURITY
THINK TANK

Salida a producción, apoyo y control a las remediaciones

Se realiza consultoría a los componentes, recursos y tecnologías a utilizar

Ethical Hacking a la aplicación y a su funcionamiento (test y retest)

Se entrega consultas directas a la equipo de desarrollo , consultas directas por componente

¿Qué es lo que controlamos?

Proceso SDL — Proceso SDLC — S-SDLC

Código Estático — Código Dinámico

Herramienta automatizada
+ Ethical Hacking

↓

Pruebas manuales → Herramientas

¿Qué es lo que controlamos?

Pruebas manuales → Herramientas

VERIFICACION FLUJO MANUAL DE LA APLICACION

↓

CONSULTOR VERIFICA COMPORTAMIENTO VS FLUJO ESTABLECIDO DE DATOS

Verificaciones de resultados y descarte de positivos

↓

Extracción evidencia

↓

Explotación de la vulnerabilidad

↓

Calificación nivel vulnerabilidad

Experiencia del consultor buscando falencias en la aplicación.

↓

Criterio de evaluación al proceso por el consultor

↓

Calificación según CVE

↓

Calificacion según top ten OWASP

Preguntas que buscamos responder

Pregunta 1

¿En metodología agile, el Salto de Sprint afecta la evaluación de seguridad?

Pregunta 2

La reevaluación de Seguridad. ¿Por que es necesaria? ¿Concluye la remediación ?

Controles, y auditorias en producción. Scope de revisión.

HACER USO DE LIBRERÍAS Y FRAMEWORKS DE SEGURIDAD

CONSULTAS SEGURAS A LAS BASES DE DATOS

CODIFICAR Y ENMASCARAR LOS DATOS

VALIDACIÓN DE DATOS

SOCHISI
DIGITAL SECURITY THINK TANK

Controles, y auditorias en producción. Scope de revisión.

HACER USO DE LIBRERÍAS Y FRAMEWORKS DE SEGURIDAD

CONSULTAS SEGURAS A LAS BASES DE DATOS

CODIFICAR Y ENMASCARAR LOS DATOS

VALIDACIÓN DE DATOS

IMPLEMENTAR MECANISMOS DE AUTENTICACIÓN SEGUROS

- NIVEL 1: CONTRASEÑAS
- NIVEL 2: MULTIFACTOR / 2FA / OTP

IMPLEMENTAR MECANISMOS DE MANEJO DE SESIÓN

IMPLEMENTACIÓN DE MATRIZ DE PERFILES

USO DE COOKIE UNICA PARA MANEJO DE SESIÓN

USO DE TOKENS DE SESIÓN

SENSIBILIDAD AL CIFRADO

USAR DATOS PERSONALES O CONOCIDOS

SOCHISI
DIGITAL SECURITY THINK TANK

Clasificación de datos

Los datos sensibles o críticos deben estar identificados para poder implementar las protecciones que requieran de forma correcta. Por ejemplo, si se manejan datos sensibles de ciudadanos, se requieren algunas protecciones específicas que deben estar presentes.

IDENTIFICACIÓN Y CLASIFICACION DE DATOS

Datos en tránsito

Las comunicaciones de los componentes que transporten información de los usuarios entre sistemas, deberán siempre estar protegidas mediante TLS, y los sistemas correctamente configurados para seleccionar el cifrado más fuerte disponible.

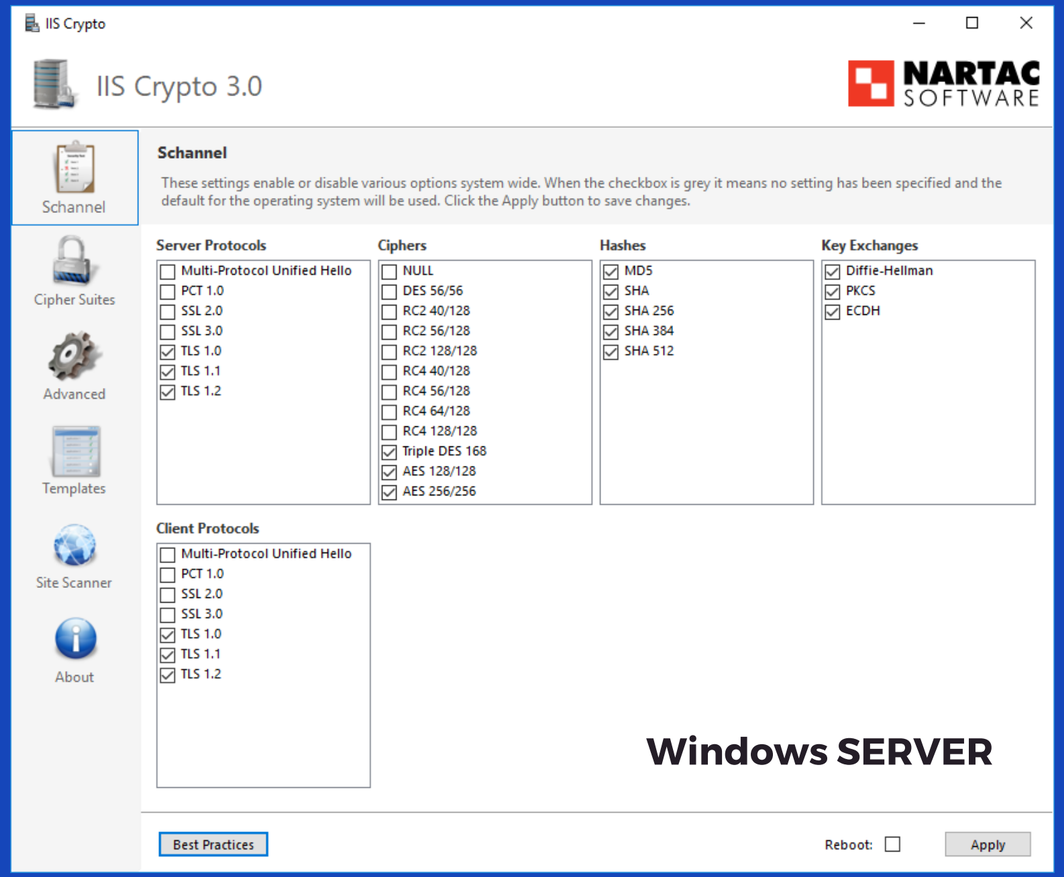
El servidor dispone del soporte de la configuración del TLS.

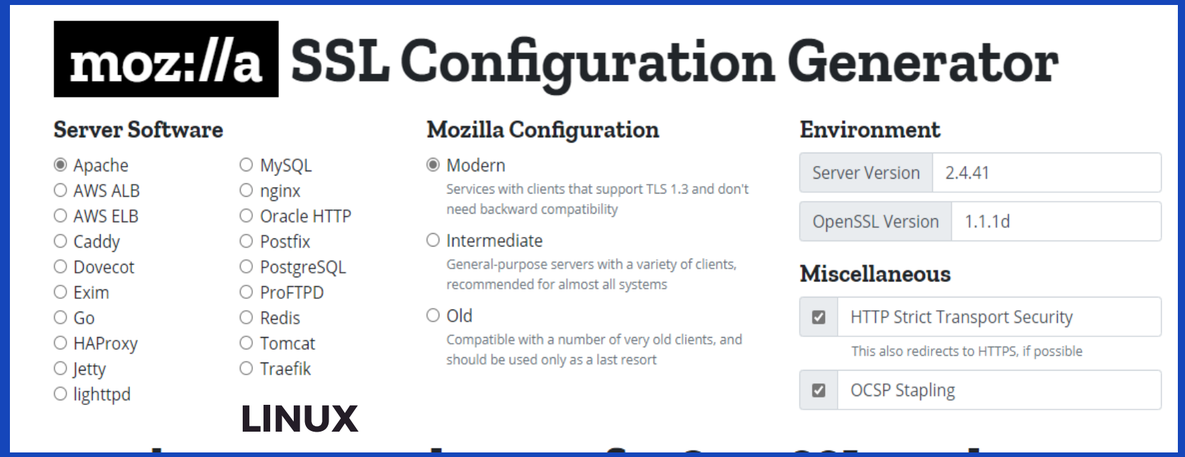
Windows SERVER **LINUX**

¿Qué TLS SOPORTA MI SERVIDOR?

SOCHISI
DIGITAL SECURITY THINK TANK

Observa estas imágenes





Caso TLS

LINUX-MODERN

```
</VirtualHost>

# modern configuration
SSLProtocol             all -SSLv3 -TLSv1 -TLSv1.1 -TLSv1.2
SSLHonorCipherOrder     off
SSLSessionTickets       off

SSLUseStapling On
SSLStaplingCache "shmcb:logs/ssl_stapling(32768)"
```

LINUX-OLD

```
</VirtualHost>

# old configuration
SSLProtocol             all -SSLv3
SSLCipherSuite          ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-
CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-
SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-
SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-
SHA:DES-CBC3-SHA
SSLHonorCipherOrder     on
SSLSessionTickets       off

SSLUseStapling On
SSLStaplingCache "shmcb:logs/ssl_stapling(32768)"
```

Copy

Almacenamiento de Datos

Éstos deben ser debidamente protegidos y deben tener sus respaldos correspondientes.

Los datos son uno de los activos mas valuables de las organizaciones.

DRP – DISASTER RECOVERY PLAN - PLAN DE RECUPERACION DE DESASTRE

BCP – BUSSINES CONTINUITY PLAN – PLAN DE CONTINUIDAD DEL NEGOCIO

Su implementación y revisión depende del gobierno de datos a utilizar.

La acción de simulación y pruebas de contingencia se establecen anualmente / simulacro /

SOCHISI
DIGITAL SECURITY THINK TANK

IMPLEMENTAR MECANISMOS DE REGISTRO

Se deben registrar distintos eventos del sistema para permitir que éstos sean monitoreados de forma automatizada para efectos de seguridad.

Utilizar un formato común de registros al interior de la organización. Esto permite facilitar la configuración y parametrización de los mecanismos de monitoreo.

Registrar la cantidad de información correcta.

Siempre registrar un timestamp e información de identificación (IP, usuario, etc).

Nunca registrar información sensible en los logs.

El archivo error-log, debe quedar privado. El permiso sobre el directorio debe ser solo al administrador.

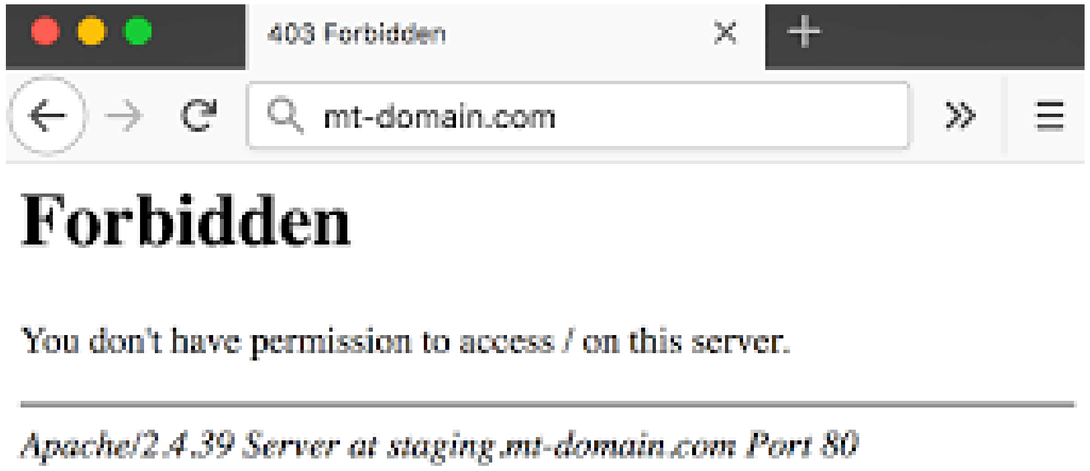
MANEJO SEGURO DE ERRORES Y EXCEPCIONES

TIP

Asegurarse de que una excepción o fallo no comprometa la seguridad por un error de programación en el sistema.
Por ejemplo, causar una denegación de servicio o ejecución de código con privilegios incorrectos.

TIP

Evitar exponer en servidores cualquier mensaje diferente código 200, tienen que responder a pagina de error estándar. Se da en el error información del tipo de servidor, dando información al atacante.



MANEJO SEGURO DE ERRORES Y EXCEPCIONES

Apache » Http Server » 2.4.39 : Security Vulnerabilities

Cpe Name:*cpe:/a:apache:http_server:2.4.39*

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2019-10098	601			2019-09-25	2019-10-09	5.8	None	Remote	Medium	Not required	Partial	Partial	None
	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.													
2	CVE-2019-10097	119		Overflow	2019-09-26	2019-09-27	6.0	None	Remote	Medium	Single system	Partial	Partial	Partial
	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.													
3	CVE-2019-10092	79		XSS	2019-09-26	2019-09-30	4.3	None	Remote	Medium	Not required	None	Partial	None
	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.													
4	CVE-2019-10082	416			2019-09-26	2019-09-27	6.4	None	Remote	Low	Not required	Partial	None	Partial
	In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.													
5	CVE-2019-10081	119		Overflow	2019-08-15	2019-08-30	5.0	None	Remote	Low	Not required	None	None	Partial
	HTTP/2 (2.4.20 through 2.4.39) very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.													

Total number of vulnerabilities : **5** Page : 1 (This Page)

Bibliografia

Ethical hacking - EC-Council Official Blog

El DRP y BCP: ¿qué son y en qué se diferencian? - CCM

Mozilla SSL Configuration Generator

Nartac Software - IIS Crypto

Apache Http Server : CVE security vulnerabilities, versions and detailed reports (cvedetails.com)

12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

¡Muchas Gracias!

SOCHISI
DIGITAL SECURITY THINK TANK

Speaker:

Andres Barrientos Cisternas – Seguridad de la Información – Ethical Hacking

Linkedin

https://www.linkedin.com/in/andresbarrientosc/

SOCHISI.CL/ENVIVO