

TRABAJO COLABORATIVO CONTEXTUALIZADO



SEGURIDAD DE SOFTWARE

INTEGRANTES:

Diego Andres Ospino Molina

TUTOR: LUIS ANTONIO SARRUF DURANGO

UNIVERSIDAD DE CARTAGENA

CERETE/CORDOBA

2025

1. Introducción

El presente informe documenta las actividades realizadas en cumplimiento del trabajo final colaborativo del curso, con el objetivo general de fortalecer las competencias en seguridad de software. La metodología empleada se dividió en dos áreas de enfoque principales, tal como se detalla en este documento.

La primera fase consistió en un análisis de reconocimiento pasivo (Fase 1 de la guía), donde se identificaron las tecnologías web y se analizó la comunicación del protocolo HTTP de tres sitios web de distintos sectores (educativo, comercial y gubernamental). Para esto, se utilizaron herramientas de *fingerprinting* como Wappalyzer y las herramientas de desarrollador del navegador⁵.

La segunda área de enfoque fue la realización de pruebas de penetración (Fase 3 de la guía) en un entorno de laboratorio controlado y seguro. Utilizando la máquina virtual vulnerable Metasploitable 2.0 como objetivo , se emplearon herramientas como Nmap, y OWASP ZAP para identificar y reportar vulnerabilidades críticas, alineadas con el marco de referencia OWASP Top Ten. Este informe omite deliberadamente la Fase 2 (Desarrollo de Aplicación Web) para centrarse en profundidad en las fases de reconocimiento y pentesting.

2. Desarrollo

A continuación, se presentan en detalle los hallazgos de las fases 1 y 3.

2.1. Fase 1: Análisis de Tecnologías Web y Protocolo HTTP

Para esta fase, se seleccionaron los siguientes tres sitios web representativos de los sectores solicitados. Se utilizó la extensión de navegador Wappalyzer para el *fingerprinting* de tecnologías y las herramientas de desarrollador del navegador para la inspección de las cabeceras y estados del protocolo HTTP.

Tabla 1: Resumen de Tecnologías y Análisis HTTP

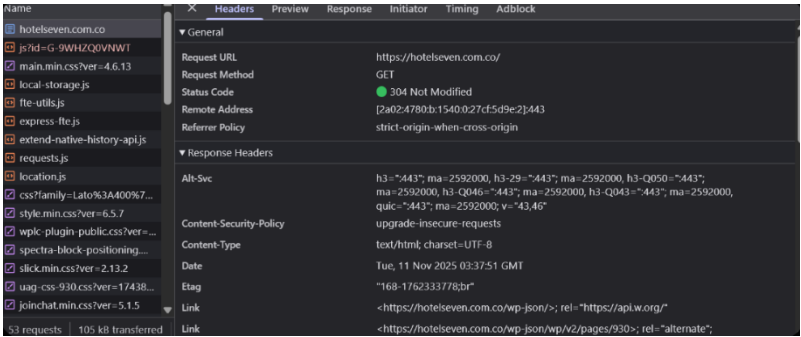
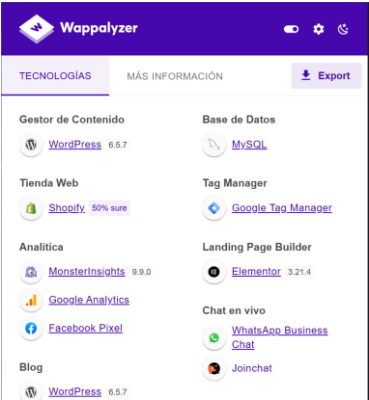
Sitio Web (Sector)	Tecnologías Identificadas (Evidencia: Wappalyzer + Herramientas para desarrollador)	Análisis de Protocolo HTTP (Estados y Cabeceras)
https://hotelseven.com.co/ (Comercial)	* CMS: WordPress (Confirmado por	* Método: GET con estado 304 Not

Sitio Web (Sector)	Tecnologías Identificadas (Evidencia: Wappalyzer + Herramientas para desarrollador)	Análisis de Protocolo HTTP (Estados y Cabeceras)
	cabecera Link en F12) * Servidor Web: LiteSpeed * Lenguaje: PHP/8.1.32 * Plataforma: Hostinger	Modified (Cargado desde caché). * Interacción: No se utiliza POST. Los formularios de contacto abren clientes de correo o WhatsApp.
https://www.monteria.gov.co/ (Gubernamental)	* CMS: WordPress 6.5.7 * Builder: Elementor 3.21.4 * Servidor Web: nginx	* Método: GET con estado 200 OK. * Cabeceras: Fuerte política de seguridad (HSTS, X-Frame-Options). * Interacción: El buscador usa GET con parámetros de consulta.

Sitio Web (Sector)	Tecnologías Identificadas (Evidencia: Wappalyzer + Herramientas para desarrollador)	Análisis de Protocolo HTTP (Estados y Cabeceras)
	* Lenguaje: Oculto (X-Powered-By: n/a)	
https://cdigital.cun.edu.co/ (Educativo)	* Plataforma (CMS): Moodle (Confirmado por cookies y cabecera X-Redirect-By) * Servidor Web: Apache/2.4.56 * PaaS: Amazon Web Services (AWS)	* Método: GET con estado 200 OK. * Interacción: El formulario de "Acceder" usa el método POST y genera una redirección 303 See Other.

EVIDENCIAS:

https://hotelseven.com.co/



X	Headers	Preview	Response	Initiator	Timing	Adblock
Link			<https://hotelseven.com.co/wp-json/wp/v2/pages/930>; rel="alternate"; type="application/json"			
Link			<https://hotelseven.com.co/>; rel=shortlink			
Panel			hpanel			
Platform			hostinger			
Server			LiteSpeed			
X-LiteSpeed-Cache			hit			
X-Powered-By			PHP/8.1.32			
Request Headers						
authority			hotelseven.com.co			
method			GET			
path			/			
scheme			https			
Accept			text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8			
Accept-Encoding			gzip, deflate, br, zstd			

https://www.monteria.gov.co/

Wappalyzer

TECNOLOGÍAS
MÁS INFORMACIÓN
Export

Seguridad

HSTS

PaaS

Amazon Web Services

Servidor Web

Nginx

Proxy reverso

Nginx

CDN

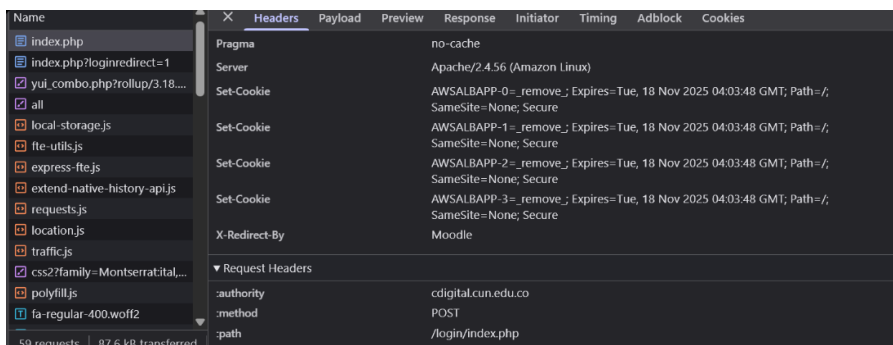
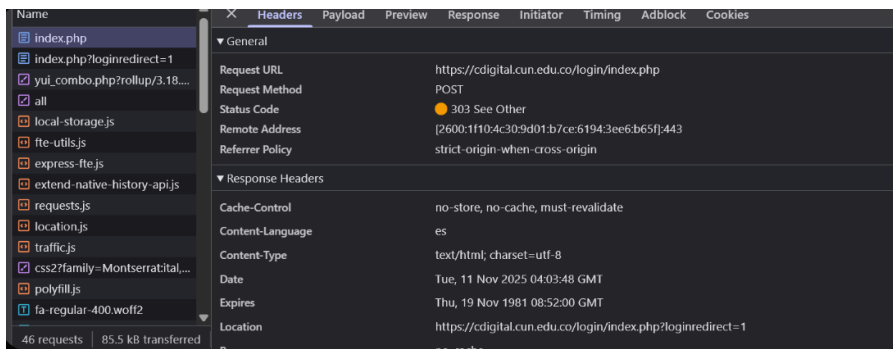
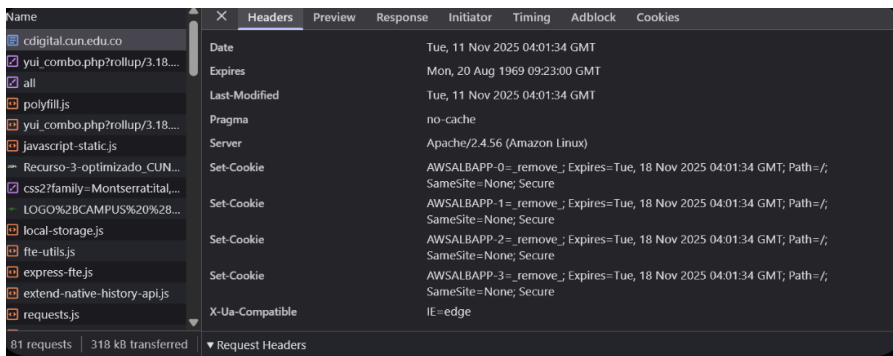
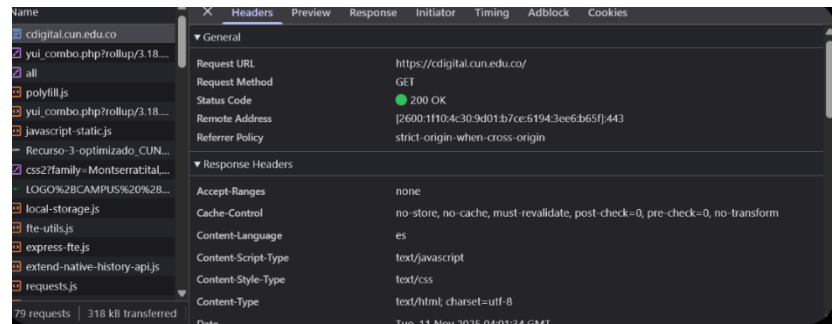
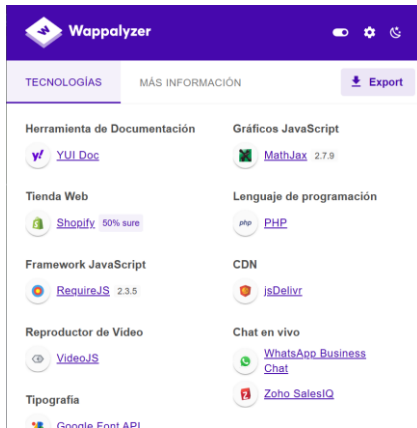
Amazon S3

¿Algo funciona mal o falta?

Name	Headers	Preview	Response	Initiator	Timing	Adblock	Cookies
www.monteria.gov.co	▼ General						
select2.min.css	Request URL	https://www.monteria.gov.co/					
select2-bootstrap.min.css	Request Method	GET					
bootstrap.min.css	Status Code	200 OK					
font-awesome.min.css	Remote Address	104.198.44.7:443					
jquery-ui.min.css	Referrer Policy	strict-origin-when-cross-origin					
slick.css	▼ Response Headers						
slick-theme.css	Access-Control-Allow-Credentials	true					
jquery-ui-timepicker-addon...	Access-Control-Allow-Headers	Accept, Authorization, Cache-Control, Content-Type, Range, DNT, If-Modified-Since, User-Agent, X-Requested-With					
bloqueIabs2.css?nxcache=1...	Access-Control-Allow-Methods	GET, POST, PUT, OPTIONS					
bloqueFooter.min.css?nxcac...	Access-Control-Allow-Origin	*					
bloqueAccesibilidad.min.css...	Cache-Control	no-store, no-cache, must-revalidate					
bloqueDynamic.min.css?nxc...	Content-Encoding	gzip					
animate.min.css?nxcache=1...							
192 requests		541 kb transferred					

Name	X	Headers	Payload	Preview	Response	Initiator	Timing	Adblock	Cookies
buscar/?q=Centroamericanos					'https://camevirtual.bucaramanga.gov.co' 'https://rentasterritoriales.adres.gov.co'				
select2.min.css									
select2-bootstrap.min.css									
bootstrap.min.css									
font-awesome.min.css									
jquery-ui.min.css									
slick.css									
slick-theme.css									
jquery-ui-timepicker-addon...									
bloqueIabs2.css?nxcache=1...									
bloqueFooter.min.css?nxcac...									
bloqueAccesibilidad.min.css...									
bloqueDynamic.min.css?nxc...									
animate.min.css?nxcache=1...									
104 requests 995 kB transferred									
Request Headers									
Pragma					no-cache				
Referrer-Policy					strict-origin				
Server					nginx				
Set-Cookie					__Secure=; HttpOnly; Secure; Path=/; SameSite=Strict				
Strict-Transport-Security					max-age=15768000; includeSubDomains; preload				
Strict-Transport-Security					max-age=15768000				
Vary					Accept-Encoding				
X-Content-Type-Options					nosniff				
X-Frame-Options					SAMEORIGIN				
X-Powered-By					n/a				
X-Xss-Protection					1; mode=block				

<https://cdigital.cun.edu.co/>



2.2. Fase 3: Pentesting y Vulnerabilidades Identificadas

Esta fase se ejecutó en un entorno de laboratorio aislado utilizando VirtualBox. La máquina atacante fue una instancia de Kali Linux (IP 192.168.56.4) y la máquina objetivo fue la máquina virtual vulnerable Metasploitable 2.0 (IP 192.168.56.5). El objetivo fue identificar un mínimo de cuatro vulnerabilidades siguiendo el marco OWASP Top Ten, utilizando las herramientas Nmap, OWASP ZAP y Burp Suite.

2.2.1. Escaneo de Red e Infraestructura (Nmap)

Se inició la fase de pentesting con un escaneo de red exhaustivo utilizando la herramienta Nmap. Se utilizó el comando `nmap -sV -sC -p- 192.168.56.5` para descubrir todos los puertos abiertos, identificar las versiones de los servicios y ejecutar scripts básicos de detección de vulnerabilidades.

"Resultados del escaneo de Nmap a Metasploitable 2.0, mostrando servicios y versiones."

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_  Connected to 192.168.56.4
|_  Logged in as ftp
|_  TYPE: ASCII
|_  No session bandwidth limit
|_  Session timeout in seconds is 300
|_  Control connection is plain text
|_  Data connections will be plain text
|_  vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian Rubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:7a:d0:98:24:fa:ck:d5:8c:cd (DSA)
|_  2048 56:56:24:df:21:1d:de:a1:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_ssl-date: 2025-11-11T04:51:40+00:00 -22m18s from scanner time.
|_ssl-cert: Subject: commonName=subuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-10T14:07:45
|_ssl-v2:
|_SSLv2 supported
|_ciphers:
|_  SSL2_RC4_128_WITH_MD5
|_  SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_  SSL2_RC4_128_EXPORT40_WITH_MD5
|_  SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-command: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
29/tcp    open  domain       ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
30/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind      2 (RPC #100000)
|_rpcinfo:
|_  program version  port/proto  service
|_  100000  2          111/tcp    rpcbind
|_  100000  2          111/udp    rpcbind
|_  100003  2,3,4      2049/tcp   nfs
|_  100003  2,3,4      2049/udp   nfs
|_  100005  1,2,3      47597/udp  mountd
|_  100005  1,2,3      56962/tcp  mountd
|_  100021  1,3,4      4243/udp   nlockmgr
```

```
Kali-linux (KALI) LIMPING Y INTERFAZ MODERNA [Comandos] - Oracle VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
|
| 100000 2,3,4 2049/udp nfs
| 100000 2,3,4 2049/udp nfs
| 100000 1,2,3 47597/udp mountd
| 100000 1,2,3 50962/tcp mountd
| 100021 1,3,4 45009/tcp nlockmgr
| 100021 1,3,4 51132/udp nlockmgr
| 100024 1 32920/tcp status
| 100024 1 34409/udp status
| 139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
| 445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
| 512/tcp open exec netkit-rsh rexecd
| 513/tcp open login
| 514/tcp open shell Netkit rshd
| 1099/tcp open java-rmi GNU Classpath gmrregistry
| 1352/tcp open bindshell Metasploitable root shell
| 2049/tcp open nfs 2-4 (RPC #100003)
| 2121/tcp open ftp ProFTPD 1.3.1
| 3306/tcp open mysql MySQL 5.0.51a-Jubuntu9
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-Jubuntu9
| Thread ID: 0
| Capabilities flags: 43504
| Some Capabilities: SupportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake, Supports4Auth, LongColumnFlag, Speaks43ProtocolNew, ConnectWithDatabase
| Status: Autocommit
| Salt: qyK.8095w].ih1zelnf
| 3632/tcp open distccd
| 3432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2025-11-17T04:52:48+00:00 - 23m18s from scanner time.
| ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2018-03-17T14:07:45
| Not valid after: 2018-04-10T14:07:45
| 5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
| Protocol version: 3.3
| Security types:
| VNC Authentication (2)
| 6080/tcp open X11 (access denied)
| 6087/tcp open irc UnrealIRCd
| 6097/tcp open irc UnrealIRCd
| 8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
| ajp-methods: Failed to get a valid response for the OPTION request
| 8388/tcp open http Apache Tomcat/Coyote JSP engine 1.1
| http-favicon: Apache Tomcat
| http-server-header: Apache-Coyote/1.1
| http-title: Apache Tomcat/5.5
| 8787/tcp open drb Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
| 32920/tcp open status 1 (RPC #100024)
| 36000/tcp open java-rmi GNU Classpath gmrregistry
| 45009/tcp open nlockmgr 1-4 (RPC #100021)
| 50962/tcp open mountd 1-3 (RPC #100003)
|
| MAC Address: 08:00:27:45:C1:C3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
| Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

El escaneo de Nmap reveló numerosos servicios obsoletos y mal configurados. A continuación, se detallan las vulnerabilidades más críticas identificadas con esta herramienta:

Vulnerabilidad 1: Componentes Vulnerables y Desactualizados (A06:2021)

- **Herramienta:** Nmap
- **Puerto y Servicio:** 21/tcp - vsftpd 2.3.4
- **Descripción:** Esta versión específica (2.3.4) de vsftpd es mundialmente famosa por contener una vulnerabilidad de puerta trasera (backdoor) (CVE-2011-2523). Un atacante puede obtener control total del sistema (shell) con solo enviar una secuencia de caracteres específica en el nombre de usuario.
- **Solución Propuesta:** Actualizar inmediatamente el servicio vsftpd a la última versión estable y parcheada. Si el servicio de FTP no es esencial para el negocio, deshabilitarlo por completo.

Vulnerabilidad 2: Fallos Criptográficos (A02:2021)

- **Herramienta:** Nmap
- **Puerto y Servicio:** 23/tcp - Telnet
- **Descripción:** Telnet es un protocolo de administración remota que no cifra el tráfico. Todas las comunicaciones, incluyendo credenciales de inicio de sesión (como msfadmin/msfadmin), se envían como texto plano. Esto permite a un atacante en la red capturar las credenciales fácilmente.

- **Solución Propuesta:** Deshabilitar permanentemente el servicio Telnet. Reemplazarlo por el servicio ssh (disponible en el puerto 22/tcp) para toda la administración remota, ya que SSH cifra toda la comunicación.

2.2.2. Escaneo de Aplicaciones Web (OWASP ZAP)

Posteriormente, se utilizó la herramienta OWASP ZAP para realizar un escaneo de seguridad de aplicaciones dinámicas (DAST) contra los servicios web alojados en el servidor.

"Resultados del Escaneo Activo de OWASP ZAP, mostrando una alerta de Ejecución Remota de Código."

The screenshot shows the OWASP ZAP interface during an automated scan. The top panel displays the 'Automated Scan' configuration, where the URL to attack is set to 'http://192.168.56.5/dvwa'. The scan is in progress, with a progress bar at 27%. The bottom panel shows a list of sent messages and a list of alerts. The alerts list includes 15 alerts, with the first two being 'Remote Code Execution - CVE-2012-1823' and 'Source Code Disclosure - CVE-2012-1823'.

ID	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
237	11/11/25, 1:00:51 AM	11/11/25, 1:00:51 AM	POST	http://192.168.56.5/dvwa/login.php	302 Found		775 ms	335 bytes	0 bytes
238	11/11/25, 1:00:51 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/login.php	200 OK		785 ms	291 bytes	1,445 bytes
239	11/11/25, 1:00:52 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/dvwa	301 Moved Perma...		62 ms	216 bytes	321 bytes
240	11/11/25, 1:00:52 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/dvwa/css	301 Moved Perma...		92 ms	220 bytes	325 bytes
241	11/11/25, 1:00:52 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/dvwa/images	301 Moved Perma...		103 ms	223 bytes	328 bytes
242	11/11/25, 1:00:52 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/dvwa	301 Moved Perma...		79 ms	216 bytes	321 bytes
243	11/11/25, 1:00:52 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/dvwa/css	301 Moved Perma...		110 ms	220 bytes	325 bytes
244	11/11/25, 1:00:52 AM	11/11/25, 1:00:52 AM	GET	http://192.168.56.5/dvwa/dvwa/images	301 Moved Perma...		68 ms	223 bytes	328 bytes
245	1								0 bytes
246	1								0 bytes
247	1								0 bytes

Alerts (15)

- > Remote Code Execution - CVE-2012-1823
- > Source Code Disclosure - CVE-2012-1823
- > Absence of Anti-CSRF Tokens (2)
- > Content Security Policy (CSP) Header Not Set
- > Directory Browsing (3)
- > Hidden File Found
- > Missing Anti-clickjacking Header (2)
- > Cookie No HttpOnly Flag (2)
- > Cookie without SameSite Attribute (2)
- > Server Leaks Information via "X-Powered-By" Header
- > Server Leaks Version Information via "Server" Header
- > X-Content-Type-Options Header Missing (5)
- > Authentication Request Identified
- > Session Management Response Identified (2)
- > User Agent Fuzzer (50)

Vulnerabilidad 3: Inyección (A03:2021) - Ejecución Remota de Código

- ### 2.2.3. Interceptación y Análisis Manual (Burp Suite)

"Burp Suite interceptando un intento de login con credenciales por defecto ('tomcat:tomcat') en el puerto 8180."



- **Herramienta: Burp Suite (y Nmap)**

- **Puerto y Servicio:** 8180/tcp - Apache Tomcat/Coyote JSP engine 1.1
- **Descripción:** Usando Burp Suite para interceptar un intento de inicio de sesión, se confirmó que la consola de administración de Tomcat (/manager/html) es accesible con las credenciales de administrador por defecto (tomcat / tomcat). Un atacante puede autenticarse y subir una aplicación web maliciosa (archivo .WAR) para ejecutar código.
- **Solución Propuesta:** Cambiar inmediatamente las credenciales por defecto del administrador de Tomcat por contraseñas robustas y únicas, e implementar una política de bloqueo de cuentas.

3. Conclusiones

La realización de este proyecto ha sido fundamental para consolidar la teoría de la seguridad de software en un contexto práctico, conectando directamente los objetivos del curso con la aplicación real de herramientas de ciberseguridad.

La **Fase 1**, de reconocimiento pasivo sobre sitios web productivos, demostró la gran cantidad de información que las aplicaciones exponen públicamente. Se constató que, si bien algunas configuraciones (como en el sitio de la alcaldía) implementan buenas prácticas de seguridad para ocultar detalles del backend (X-Powered-By: n/a), la mayoría de los sitios revelan abiertamente su pila tecnológica (CMS, servidor, lenguaje). Este análisis subraya una verdad fundamental: el primer paso de un atacante se basa en información pública, y la ofuscación de esta información es la primera línea de defensa.

La **Fase 3**, de pentesting en un entorno controlado, fue una demostración práctica del riesgo crítico que suponen los sistemas desactualizados y mal configurados. El escaneo con **Nmap** reveló una superficie de ataque inmensa, donde vulnerabilidades como el uso de protocolos inseguros (Telnet, **A02**) y software con puertas traseras conocidas (vsftpd, **A06**) representan un riesgo inminente.

El uso de **OWASP ZAP** y **Burp Suite** complementó este análisis, moviéndonos de la infraestructura a la aplicación. El hallazgo de una vulnerabilidad de Ejecución Remota de Código (A03) con ZAP demostró el poder de las herramientas DAST para identificar fallos de inyección críticos que no son visibles a simple vista. Asimismo, la interceptación con Burp Suite confirmó que las credenciales por defecto (Tomcat, **A07**) son un punto de fallo de autenticación tan peligroso como un error en el código.

En conjunto, ambas fases ilustran que la seguridad no es un solo producto, sino un ciclo de vida. Comienza con la configuración segura de la infraestructura (parchear Nmap) y debe continuar con un análisis profundo de la aplicación (probar con ZAP y Burp) para defenderse eficazmente contra el marco de referencia **OWASP Top Ten**.

4. Bibliografía

OWASP Foundation. (2021). *OWASP Top Ten 2021*. Open Web Application Security Project.
<https://owasp.org/www-project-top-ten/>

OWASP Foundation. (2023). *OWASP ZAP*. Open Web Application Security Project.
<https://www.zaproxy.org/>