

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)
	<p>cabecera Link en F12)</p> <ul style="list-style-type: none"> * Servidor Web: LiteSpeed * Lenguaje: PHP/8.1.32 * Plataforma: Hostinger 	<p>Modified (Cargado desde caché).</p> <ul style="list-style-type: none"> * Interacción: No se utiliza POST. Los formularios de contacto abren clientes de correo o WhatsApp.
https://www.monteria.gov.co/ (Gubernamental)	<ul style="list-style-type: none"> * CMS: WordPress 6.5.7 * Builder: Elementor 3.21.4 * Servidor Web: nginx 	<ul style="list-style-type: none"> * 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)	<ul style="list-style-type: none"> * Plataforma (CMS): Moodle (Confirmado por cookies y cabecera X-Redirect-By) * Servidor Web: Apache/2.4.56 * PaaS: Amazon Web Services (AWS) 	<ul style="list-style-type: none"> * 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/>

	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/a...png,*/*;q=0.8					
Accept-Encoding	gzip, deflate, br, zstd					

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



Wappalyzer

TECNOLOGÍAS MÁS INFORMACIÓN Export

Seguridad	PaaS
HSTS	Amazon Web Services
Servidor Web	Proxy reverso
Nginx	Nginx
CDN	
Amazon S3	

¿Algo funciona mal o falta?

Name	Headers	Preview	Response	Initiator	Timing	Adblock	Cookies
www.monteria.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...							
bloqueTabs2.css?nxcache=1...							
bloqueFooter.min.css?nxcac...							
bloqueAccesibilidad.min.css...							
bloqueDynamic.min.css?nxcc...							
animate.min.css?nxcache=1...							
192 requests 541 kB transferred	▼ Request Headers						

Name	Headers	Payload	Preview	Response	Initiator	Timing	Adblock	Cookies
buscar/?q=Centroamericanos				'https://canevirtual.bucaramanga.gov.co' 'https://tramites.risaralda.gov.co'				
select2.min.css				'https://tramites.risaralda.gov.co', payment=0				
select2-bootstrap.min.css				no-cache				
bootstrap.min.css				strict-origin				
font-awesome.min.css				nginx				
jquery-ui.min.css				_Secure_=; HttpOnly; Secure; Path=/; SameSite=Strict				
slick.css				max-age=15768000; includeSubDomains; preload				
slick-theme.css				max-age=15768000				
jquery-ui-timepicker-addon...				Accept-Encoding				
bloqueTabs2.css?nxcache=1...				nosniff ↗				
bloqueFooter.min.css?nxcac...				SAMEORIGIN				
bloqueAccesibilidad.min.css...				X-Powered-By				
bloqueDynamic.min.css?nxcc...				n/a				
animate.min.css?nxcache=1...				X-Xss-Protection				
104 requests 995 kB transferred	▼ Request Headers							

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

Wappalyzer

TECNOLOGIAS MÁS INFORMACIÓN Export

Herramienta de Documentación Gráficos JavaScript YUI Doc MathJax 2.7.9

Tienda Web Lenguaje de programación Shopify 50% sure PHP

Framework JavaScript CDN RequireJS 2.3.5 jsDelivr

Reproductor de Video Chat en vivo VideoJS WhatsApp Business Chat Zoho SalesIQ

Tipografía Google Font API

Name digital.cun.edu.co Headers Preview Response Initiator Timing Adblock Cookies

Request URL https://cdigital.cun.edu.co/ Request Method GET Status Code 200 OK Remote Address [2600:1f10:4:30:9d01:b7ce:6194:3ee6:b65f]:443 Referer Policy strict-origin-when-cross-origin

Response Headers

Accept-Ranges none Cache-Control no-store, no-cache, must-revalidate, post-check=0, pre-check=0, no-transform Content-Language es Content-Script-Type text/javascript Content-Style-Type text/css Content-Type text/html; charset=utf-8 Date Tue, 11 Nov 2025 04:01:34 GMT

Name digital.cun.edu.co Headers Preview Response Initiator Timing Adblock Cookies

Date Tue, 11 Nov 2025 04:01:34 GMT Expires Mon, 20 Aug 1969 09:23:00 GMT Last-Modified Tue, 11 Nov 2025 04:01:34 GMT Pragma no-cache Server Apache/2.4.56 (Amazon Linux)

Set-Cookie AWSALBAPP-0=_remove_; Expires=Tue, 18 Nov 2025 04:01:34 GMT; Path=/; SameSite=None; Secure Set-Cookie AWSALBAPP-1=_remove_; Expires=Tue, 18 Nov 2025 04:01:34 GMT; Path=/; SameSite=None; Secure Set-Cookie AWSALBAPP-2=_remove_; Expires=Tue, 18 Nov 2025 04:01:34 GMT; Path=/; SameSite=None; Secure Set-Cookie AWSALBAPP-3=_remove_; Expires=Tue, 18 Nov 2025 04:01:34 GMT; Path=/; SameSite=None; Secure X-UA-Compatible IE=edge

Request Headers

81 requests | 318 kB transferred

Name index.php Headers Payload Preview Response Initiator Timing Adblock Cookies

Request URL https://cdigital.cun.edu.co/login/index.php Request Method POST Status Code 303 See Other Remote Address [2600:1f10:4:c30:9d01:b7ce:6194:3ee6:b65f]:443 Referer Policy strict-origin-when-cross-origin

Response Headers

Cache-Control no-store, no-cache, must-revalidate Content-Language es Content-Type text/html; charset=utf-8 Date Tue, 11 Nov 2025 04:03:48 GMT Expires Thu, 19 Nov 1981 08:52:00 GMT Location https://cdigital.cun.edu.co/login/index.php?loginredirect=1

Name index.php Headers Payload Preview Response Initiator Timing Adblock Cookies

Pragma no-cache Server Apache/2.4.56 (Amazon Linux)

Set-Cookie AWSALBAPP-0=_remove_; Expires=Tue, 18 Nov 2025 04:03:48 GMT; Path=/; SameSite=None; Secure Set-Cookie AWSALBAPP-1=_remove_; Expires=Tue, 18 Nov 2025 04:03:48 GMT; Path=/; SameSite=None; Secure Set-Cookie AWSALBAPP-2=_remove_; Expires=Tue, 18 Nov 2025 04:03:48 GMT; Path=/; SameSite=None; Secure Set-Cookie AWSALBAPP-3=_remove_; Expires=Tue, 18 Nov 2025 04:03:48 GMT; Path=/; SameSite=None; Secure X-Redirect-By Moodle

Request Headers

:authority cdigital.cun.edu.co :method POST :path /login/index.php

59 requests | 87.6 kB transferred

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 238)
| 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
|_Open ssh   OpenSSH 4.7p1 Debian Bubuntul (protocol 2.0)
|_ssh-hostkey:
|   1024 60:0f:cfc:f1:c0:5f:6a:74:d6:90:24:fa:c4:d5:d6:c0:cd (RSA)
|   2048 56:56:24:9f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smtpd
|_smtp-dataline: 25-11-11T04:53:20-0400 --23m10s from scanner time.
ssl-cert: Subject: commonName=ubuntu04-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: 2010-04-16T14:07:45
|_Not valid after: 2010-04-16T14:07:45
sslv2:
|_SSLv2 supported
|_ciphers:
|   SSL2_RC4_128_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC4_128_EXPORT56_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|_http-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
|_dnssec-support: yes
|_bind-version: 9.4.2
80/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      45089/tcp  nlockmgr
```

```

kali-linux (KALI LIMPIO Y INTERFAZ MODERNA) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
www 4.2.2.x 4.2.2.x
1 100003 2,3,4 2049/udp nfs
100005 1,2,3 47597/udp mounted
1 100005 1,2,3 50962/tcp mounted
1 100005 1,2,3 45000/tcp aliosnugr
1 100021 1,2,3 51123/udp blockmgr
1 100024 1 32924/tcp status
1 100024 1 34469/udp status
139/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
513/tcp open login
513/tcp open shell Netkit rshd
1099/tcp open Java-vmi GNU Classpath gmiregistry
1324/tcp open bindshell Metasploitable root shell
1324/tcp open bindshell 2>1 RPC #100003
2221/tcp open ftp ProFTPD 3.1.1
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-Ubuntu5
|   Vendor: MySQL
|   Vendor ID: 8
|   Capabilities Flags: 43564
|   Some Capabilities: SupportsTransactions, SupportsCompression, SwitchToSSLAfterHandshake, Support41Auth, LongColumnFlag, Speaks41ProtocolNew, ConnectWithDatabase
|   Status: Autocommit
|   Ssl: eykAABg95a...HHzelnf
34469/tcp open blockmgr
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
| ssl-date: 2025-11-17T04:52:40+00:00; -23m0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu04-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2019-03-17T14:07:45
| Not valid after: 2019-04-10T14:07:45
5900/tcp open vnc VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|     VNC Authentication (2)
|   6000/tcp open vnc VNC Authentication (2) (access denied)
|   6667/tcp open irc UnrealIRCd
|   6667/tcp open irc UnrealIRCd
|   8089/tcp open ajp13 Apache Jserv (Protocol v1.3)
|   8089/tcp open httpd Apache Tomcat/Coyote JSP engine 1.1
|_ajp-methods: Failed to get a valid response for the OPTION request
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
8787/tcp open db Ruby DBM (Ruby 1.8; path /usr/lib/ruby/1.8/dbm)
8787/tcp open dbm Ruby DBM (Ruby 1.8; path /usr/lib/ruby/1.8/dbm)
3400/tcp open java-vmi GNU Classpath gmiregistry
45089/tcp open blockmgr 1-4 (RPC #100021)
50962/tcp open mounted 1-3 (RPC #100005)
MAC Address: 08:00:27:45:C1:C3 (PSC Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc, Metasploitable, LAN; OSs: Unix, Linux; CPE: cpe:/orlinux: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)

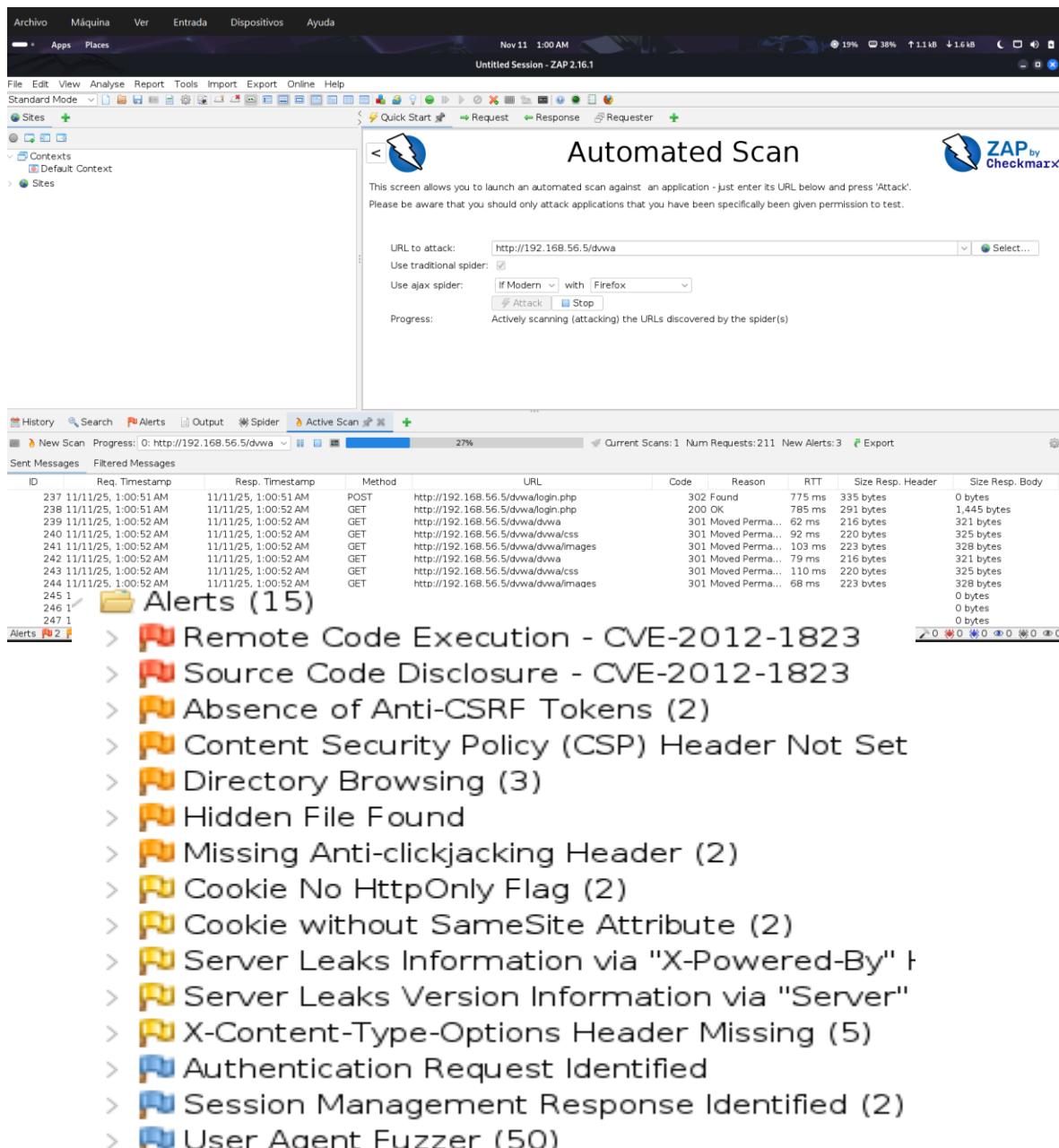
- **Herramienta:** Nmap
- **Puerto y Servicio:** 23/tcp - Telnet
- **Descripción:** Telnet es un protocolo de administración remota que no cifra el tráfico. Todas las comunicaciones, incluyendo credenciales de inicio de sesión (como msfadmin/msfadmin), se envían como texto plano. Esto permite a un atacante 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. At the top, there's a toolbar with various icons and a menu bar. Below that is a main panel titled "Automated Scan" which includes fields for "URL to attack" (set to "http://192.168.56.5/dvwa"), "Spider Type" (set to "Traditional Spider"), and "Attack Type" (set to "If Modern with Firefox"). A progress bar indicates the scan is at 27%. Below this panel, the "Alerts" tab is selected, showing a list of 15 identified issues. The alerts include various security vulnerabilities such as Remote Code Execution, Source Code Disclosure, Absence of Anti-CSRF Tokens, Content Security Policy Header Not Set, Directory Browsing, Hidden File Found, Missing Anti-clickjacking Header, Cookie No HttpOnly Flag, Cookie without SameSite Attribute, Server Leaks Information via "X-Powered-By", Server Leaks Version Information via "Server", X-Content-Type-Options Header Missing, Authentication Request Identified, Session Management Response Identified, and User Agent Fuzzer.

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" !
- > ! Server Leaks Version Information via "Server"
- > ! X-Content-Type-Options Header Missing (5)
- > ! Authentication Request Identified
- > ! Session Management Response Identified (2)
- > ! User Agent Fuzzer (50)

El escaneo reveló una vulnerabilidad crítica de inyección de comandos:

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

- **Herramienta:** OWASP ZAP
- **Descripción:** ZAP identificó una vulnerabilidad de Ejecución Remota de Código (CVE-2012-1823) en el script php.cgi del servidor. Esta vulnerabilidad permite a un atacante enviar una solicitud HTTP maliciosa que engaña al intérprete de PHP para que ejecute comandos del sistema operativo en el servidor, lo que resulta en un control total.
- **Solución Propuesta:** Actualizar la versión de PHP en el servidor a una versión parcheada que no sea vulnerable a CVE-2012-1823.

2.2.3. Interceptación y Análisis Manual (Burp Suite)

Finalmente, se utilizó Burp Suite para interceptar y analizar manualmente las solicitudes a los servicios web que requieren autenticación. Esta técnica se utilizó para confirmar las vulnerabilidades de autenticación encontradas por Nmap.

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

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A single request is highlighted in the list:

```
Time Type Direction Method URL Status code Length  
04/19/4811... HTTP → Request GET http://192.168.56.5:8180/manager/html 200 1024
```

The 'Request' pane shows the raw HTTP traffic:

```
Pretty Raw Hex  
1 GET /manager/html HTTP/1.1  
2 Host: 192.168.56.5:8180  
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0  
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  
5 Accept-Language: en-US,en;q=0.5  
6 Accept-Encoding: gzip, deflate, br  
7 Authorization: Basic dG9tY2FO0RvbWNhdA==  
8 Connection: keep-alive  
9 Upgrade-Insecure-Requests: 1  
0 Priority: u=0, l  
1  
2
```

The 'Inspector' pane shows the following details for the selected request:

- Request attributes: 2
- Request query parameters: 0
- Request body parameters: 0
- Request cookies: 0
- Request headers: 9

Vulnerabilidad 4: Fallos de Identificación y Autenticación (A07:2021)

- **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/>