



Actividad 1 - Pérdida de Autenticación y Gestión de Sesiones Auditoría Informática Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero.

Alumno: Carlos Alberto Fuentes Mendoza

Fecha: 28-septiembre-2023

Índice

Introducción	3
Descripción	4
Justificación	5
Descripción del sitio web	6
Ataque al sitio	7
Conclusión	14
Referencias	15

Introducción

El proyecto abierto de seguridad en aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a facultar a las organizaciones a desarrollar, adquirir y mantener aplicaciones y APIs que pueden ser confiables. Su proyecto de documentación más conocido es el TOP TEN, en el cual se listan las 10 vulnerabilidades (security risks) más habituales y cómo prevenirlas.



En su lista de TOP 10, se encuentra en segundo lugar A2-Perdida de autenticación y gestión de sesiones. En esta vulnerabilidad, las fallas generalmente conducen a la divulgación de información no autorizada, la modificación de todos los datos, la ejecución de una función de negocio fuera de los límites del usuario, suplantación de identidad, hackeo y pérdida de toda nuestra información, pérdida del control sobre documentos en los que hemos invertido gran parte de nuestro tiempo y esfuerzo, terceras personas pueden utilizar nuestra información con fines comerciales, nuestra privacidad deja de tener sentido, perdemos la autoridad sobre nuestra información confidencial, pérdida de la confianza de nuestros clientes, hasta el cierre del negocio.

Una de las recomendaciones para contrarrestar este riesgo, es el certificado SSL. Este es un certificado digital que autentica la identidad de un sitio web y habilita una conexión cifrada. La sigla SSL significa Secure Sockets Layer (Capa de sockets seguros), un protocolo de seguridad que crea un enlace cifrado entre un servidor web y un navegador web para mantener la privacidad de las interacciones en línea, esto garantiza a los usuarios que el sitio web es auténtico, que es seguro compartir información privada mediante él, evita que los atacantes creen una versión falsa del sitio y esto genera confianza a los usuarios.

Descripción

Una empresa de software solicita realizar varias pruebas de seguridad en páginas web que no cuentan con los candados de seguridad.

Para esta primera etapa, se debe de realizar una prueba de la vulnerabilidad de la pérdida de autenticación y gestión de sesiones utilizando la aplicación WireShark, el objetivo de esta prueba es obtener las credenciales de autenticación que se ingresaron y que estas se puedan mostrar.

Para realizar esta actividad, se deberá elegir un proyecto web que se haya realizado con anterioridad, en caso de no contar con uno, se deberá elegir un sitio web que contenga las siguientes características:

- Función de inicio de sesión y registro de usuarios
- Conexión con una base de datos

En esta actividad vamos a aprender la manera de explotar una vulnerabilidad de un sitio web, en la cual, con la ayuda de la aplicación WirwShark, podremos observar la pérdida de autenticación y gestión de sesiones, obteniendo las credenciales del Login, debido a la falta de certificación SSL.

Justificación

Los sitios web necesitan certificados SSL para mantener la seguridad de los datos del usuario, verificar la propiedad del sitio web, evitar que los atacantes creen una versión falsa del sitio y para transmitir confianza a los usuarios. Si un sitio web solicita a los usuarios que inicien sesión, ingresen datos personales, como sus números de tarjeta de crédito, o vean información confidencial, como los beneficios de salud o información financiera, entonces es esencial mantener la confidencialidad de los datos. Los certificados SSL ayudan a mantener la privacidad de las interacciones en línea y garantizan a los usuarios que el sitio web es auténtico y que es seguro compartir información privada mediante él.

Más relevante para las empresas es el hecho de que se necesita un certificado SSL para una dirección web HTTPS. El protocolo HTTPS es la versión segura del protocolo HTTP, lo que significa que los sitios web HTTPS tienen su tráfico cifrado mediante certificados SSL. La mayoría de los navegadores clasifican los sitios HTTP, aquellos sin certificados SSL, como “no seguros”. Para los usuarios, esta es una clara señal de que el sitio puede no ser confiable, lo que incentiva a las empresas que no lo han hecho a migrar al protocolo HTTPS.

Un certificado SSL ayuda a proteger información como la siguiente:

- Credenciales de inicio de sesión
- Transacciones con tarjeta de crédito o información de la cuenta bancaria
- Información de identificación personal, como nombre completo, dirección, fecha de nacimiento o número de teléfono
- Documentos y contratos legales
- Historia clínica
- Información de propiedad

Descripción del sitio web

Las Páginas Verdes es el directorio impreso y en línea más completo de productos y servicios sustentables en México que genera un movimiento de consumo responsable.

Las Páginas Verdes, con siete años promoviendo el crecimiento de la economía sustentable en México, reúne más de 5,100 productos y servicios sustentables.

A continuación, se muestra la captura de pantalla del sitio web a atacar, el cual tiene la siguiente url:

<http://laspaginasverdes.com>



Ataques del sitio

Iniciamos obteniendo la ip de la página web que deseamos atacar con url <http://laspaginasverdes.com/>, para esto nos dirigimos al sitio web <https://who.is> y capturamos la url del sitio web.

Como se puede observar en la siguiente captura, el sitio web nos devuelve la información de dicha página, la cual la que más nos interesa es la ip 162.243.211.192.

The screenshot shows the who.is website interface. At the top, a search bar contains the URL `https://who.is/tools/laspaginasverdes.com?id=03AFcWeA4psuMzvglkXhflcXdr4gKW1TCT4kDlyqEYCzSRzLC02ti6lhg9LAHKkXfku5E4ZOAcudVnDnpyajSnY4oquuslEX-OTp05VmWYVYnzWv9wR...`. Below the search bar, a message states: **laspaginasverdes.com is already registered.** Interested in buying it? [Make an Offer](#).

A table displays domain availability for various TLDs:

TLD	Price	Status
.com		Taken
.net	\$14.99	Available
.org	\$8.99	Available
.co	\$12.99	Available
.io	\$34.99	Available
.app	\$16.99	Available
.live	\$3.99	Available

A green button labeled "Purchase Selected Domains" is located below the table.

Below the table, the website name **laspaginasverdes.com** is displayed, followed by "diagnostic tools". Three buttons are visible: "Whois", "DNS Records", and "Diagnostics".

The "Ping" section shows the following output:

```
PING laspaginasverdes.com (162.243.211.192) 56(84) bytes of data:
64 bytes from 162.243.211.192: icmp_seq=1 ttl=45 time=8.90 ms
64 bytes from 162.243.211.192: icmp_seq=2 ttl=45 time=7.97 ms
64 bytes from 162.243.211.192: icmp_seq=3 ttl=45 time=8.02 ms
64 bytes from 162.243.211.192: icmp_seq=4 ttl=45 time=7.96 ms
64 bytes from 162.243.211.192: icmp_seq=5 ttl=45 time=8.13 ms

--- laspaginasverdes.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 7.962/8.197/8.901/0.374 ms
```

The "Traceroute" section shows the following output:

```
traceroute to laspaginasverdes.com (162.243.211.192), 30 hops max, 60 byte packets
1 ip-10-0-0-14.ec2.internal (10.0.0.14) 1.316 ms 1.300 ms 1.289 ms
2 216.182.231.42 (216.182.231.42) 15.119 ms 216.182.238.133 (216.182.238.133) 6.659 ms 216.182.238.139 (216.182.238.139) 52.125 ms
3 100.65.83.176 (100.65.83.176) 71.971 ms 100.65.82.96 (100.65.82.96) 4.016 ms 100.65.80.176 (100.65.80.176) 8.204 ms
4 100.66.40.172 (100.66.40.172) 3.101 ms 100.66.40.248 (100.66.40.248) 8.191 ms 100.66.15.138 (100.66.15.138) 17.256 ms
5 100.66.63.60 (100.66.63.60) 22.266 ms 241.0.4.196 (241.0.4.196) 1.948 ms 100.66.42.22 (100.66.42.22) 21.088 ms
6 242.0.171.209 (242.0.171.209) 2.464 ms 242.0.171.211 (242.0.171.211) 1.558 ms 241.0.4.213 (241.0.4.213) 1.263 ms
7 240.2.88.13 (240.2.88.13) 7.897 ms 242.0.170.87 (242.0.170.87) 1.934 ms 240.2.88.12 (240.2.88.12) 7.433 ms
8 240.2.88.14 (240.2.88.14) 7.411 ms 240.2.88.13 (240.2.88.13) 7.570 ms 52.93.50.156 (52.93.50.156) 7.466 ms
9 52.93.50.142 (52.93.50.142) 33.000 ms 99.83.89.107 (99.83.89.107) 7.802 ms 52.93.50.162 (52.93.50.162) 8.106 ms
10 138.197.244.10 (138.197.244.10) 8.136 ms * 99.83.89.107 (99.83.89.107) 7.743 ms
```

*Ethernet
— □ ×

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 162.243.211.192
✖
+

No.	Time	Source	Destination	Protocol	Length	Info
1374	129.500018	192.168.0.101	162.243.211.192	ICMP	74	Echo (ping) request id=0x0001, seq=25/6400, ttl=128 (reply in 1376)
1376	129.574583	162.243.211.192	192.168.0.101	ICMP	74	Echo (ping) reply id=0x0001, seq=25/6400, ttl=54 (request in 1374)
1380	130.511557	192.168.0.101	162.243.211.192	ICMP	74	Echo (ping) request id=0x0001, seq=26/6656, ttl=128 (reply in 1381)
1381	130.585458	162.243.211.192	192.168.0.101	ICMP	74	Echo (ping) reply id=0x0001, seq=26/6656, ttl=54 (request in 1380)
1383	131.520658	192.168.0.101	162.243.211.192	ICMP	74	Echo (ping) request id=0x0001, seq=27/6912, ttl=128 (reply in 1384)
1384	131.594352	162.243.211.192	192.168.0.101	ICMP	74	Echo (ping) reply id=0x0001, seq=27/6912, ttl=54 (request in 1383)
1387	132.529149	192.168.0.101	162.243.211.192	ICMP	74	Echo (ping) request id=0x0001, seq=28/7168, ttl=128 (reply in 1388)
1388	132.602815	162.243.211.192	192.168.0.101	ICMP	74	Echo (ping) reply id=0x0001, seq=28/7168, ttl=54 (request in 1387)

```

> Frame 1374: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on in
> Ethernet II, Src: EliteGro_09:89:bd (94:c6:91:09:89:bd), Dst: TP-Link_ad:19
> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 162.243.211.192
> Internet Control Message Protocol
        
```

0000	48 22 54 ad 19 6a 94 c6	91 09 89 bd 08 00 45 00	H" T . . j E .
0010	00 3c 70 5f 00 00 80 01	00 00 c0 a8 00 65 a2 f3	. < p _ e .
0020	d3 c0 08 00 4d 42 00 01	00 19 61 62 63 64 65 66 MB abcdef
0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72 73 74 75 76	g h i j k l m n o p q r s t u v
0040	77 61 62 63 64 65 66 67	68 69	w a b c d e f g h i

C:\WINDOWS\system32\CMD.exe

```

C:\Users\chatl>ping 162.243.211.192

Haciendo ping a 162.243.211.192 con 32 bytes de datos:
Respuesta desde 162.243.211.192: bytes=32 tiempo=74ms TTL=54
Respuesta desde 162.243.211.192: bytes=32 tiempo=73ms TTL=54
Respuesta desde 162.243.211.192: bytes=32 tiempo=73ms TTL=54
Respuesta desde 162.243.211.192: bytes=32 tiempo=73ms TTL=54

Estadísticas de ping para 162.243.211.192:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 73ms, Máximo = 74ms, Media = 73ms

C:\Users\chatl>
        
```

wireshark_EthernetQF38B2.pcapng
Paquetes: 7816 • Mostrado: 8 (0.1%)
Perfil: Default

En la siguiente pantalla se observa la página del Login en la cual colocamos las siguientes credenciales:

Carlos.fuentes@hotmail.com y en password= jessica hernandez romero


Browser address bar: No es seguro | laspaginasverdes.com/login/

Error message: NoSuchBucketThe specified bucket does not existgraphicsmxW0H58HEGHNS6SZVTma4rGmmoCKJofxIO8mp+53XOIRvkvh1+N5T4kozN6p1h7A/dgiKJ

Navigation bar: CONTACTO | [f](#) [t](#) [i](#)

Logo: **las páginas verdes**
Piensa Sustentable

Menu: DIRECTORIO | B2B | ECOFEST | HERRAMIENTAS | **INGRESAR**



ACCESO A USUARIOS

LOGIN

Accede a tu cuenta para continuar tu experiencia verde

☐ Recuérdame

[¿Has perdido tu contraseña?](#)

ACCEDER

¿USUARIO NUEVO? ¡REGÍSTRATE!


Conviértete en un usuario verde y sé parte de la experiencia de ayudar al ambiente.

En la siguiente captura se puede observar que las credenciales son incorrectas debido a que no me encuentro registrado en este sitio web.


← → ↻ 🏠 No es seguro | laspaginasverdes.com/login/?login=failed

NoSuchBucketThe specified bucket does not existgraphicsmxBKF2ATVEJMRKPV5jZ5QMqQ4Xf24L7ifUhw825KxTuSRfPDwEaG+JJsyzyC7gidC6D7ori

CONTACTO 📧 📱 📺

 **las páginas verdes**
Piensa Sustentable

DIRECTORIO B2B ECOFEST HERRAMIENTAS INGRESAR



ACCESO A USUARIOS

LOGIN

Accede a tu cuenta para continuar tu experiencia verde

Error: Nombre de usuario o contraseña incorrectos.

Usuario/Correo electrónico Contraseña

☐ Recuérdame

[¿Has perdido tu contraseña?](#)

ACCEDER

En la siguiente captura se observan los paquetes capturados por la aplicación, en los cuales encontramos el protocolo HTTP que es el que nos interesa.

Ethernet

Archivo Edición Visualización Ir Captura Analizar Estadísticas Telefonía Wireless Herramientas Ayuda

ip.addr == 162.243.211.192

No.	Time	Source	Destination	Protocol	Length	Info
17618	1563.389279	192.168.0.101	162.243.211.192	TCP	54	53244 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262400 Len=0
17621	1563.464093	162.243.211.192	192.168.0.101	TCP	60	80 → 53245 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
17622	1563.464096	162.243.211.192	192.168.0.101	TCP	60	80 → 53244 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
17623	1563.475137	192.168.0.101	162.243.211.192	TCP	54	53245 → 80 [ACK] Seq=2 Ack=2 Win=262400 Len=0
17624	1563.475342	192.168.0.101	162.243.211.192	TCP	54	53244 → 80 [ACK] Seq=2 Ack=2 Win=262400 Len=0
19446	1709.202599	192.168.0.101	162.243.211.192	TCP	66	53266 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19447	1709.202762	192.168.0.101	162.243.211.192	TCP	66	53267 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19486	1709.276143	162.243.211.192	192.168.0.101	TCP	66	80 → 53267 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
19487	1709.276156	162.243.211.192	192.168.0.101	TCP	66	80 → 53266 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
19488	1709.276192	192.168.0.101	162.243.211.192	TCP	54	53266 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
19489	1709.276194	192.168.0.101	162.243.211.192	TCP	54	53267 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
19490	1709.277506	192.168.0.101	162.243.211.192	HTTP	1178	POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
19494	1709.350336	162.243.211.192	192.168.0.101	TCP	60	80 → 53267 [ACK] Seq=1 Ack=1125 Win=31488 Len=0
19499	1709.839970	162.243.211.192	192.168.0.101	HTTP	774	HTTP/1.1 302 Found
19501	1709.847177	192.168.0.101	162.243.211.192	HTTP	992	GET /login/?login=failed HTTP/1.1
19506	1709.919853	162.243.211.192	192.168.0.101	TCP	60	80 → 53267 [ACK] Seq=721 Ack=2063 Win=33792 Len=0
19512	1710.149672	162.243.211.192	192.168.0.101	TCP	1466	80 → 53267 [ACK] Seq=721 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19513	1710.149672	162.243.211.192	192.168.0.101	TCP	1466	80 → 53267 [ACK] Seq=2133 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19514	1710.149672	162.243.211.192	192.168.0.101	TCP	1466	80 → 53267 [ACK] Seq=3545 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19515	1710.149672	162.243.211.192	192.168.0.101	TCP	1466	80 → 53267 [ACK] Seq=4957 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19516	1710.149672	162.243.211.192	192.168.0.101	HTTP	170	HTTP/1.1 200 OK (text/html)
19517	1710.149758	192.168.0.101	162.243.211.192	TCP	54	53267 → 80 [ACK] Seq=2063 Ack=6485 Win=262400 Len=0
19606	1715.154521	162.243.211.192	192.168.0.101	TCP	60	80 → 53267 [FIN, ACK] Seq=6485 Ack=2063 Win=33792 Len=0

> Frame 19490: 1178 bytes on wire (9424 bits), 1178 bytes captured (9424 bits) on interface 0

> Ethernet II, Src: EliteGro_09:89:bd (94:c6:91:09:89:bd), Dst: TP-Link_ad:19:6a (48:9e:f3:94:c6:91:09:89:bd)

> Internet Protocol Version 4, Src: 192.168.0.101, Dst: 162.243.211.192

> Transmission Control Protocol, Src Port: 53267, Dst Port: 80, Seq: 1, Ack: 1, Len: 1178

> Hypertext Transfer Protocol

> HTML Form URL Encoded: application/x-www-form-urlencoded

0000 48 22 54 ad 19 6a 94 c6 91 09 89 bd 08 00 45 00 H T T P

0010 04 8c 71 12 40 00 80 06 00 00 c0 a8 00 65 a2 f3 . . q @

0020 d3 c0 d0 13 00 50 ae c7 8e 1a 43 ea 65 23 50 18 P . . . C e # P

0030 04 01 3c 40 00 00 50 4f 53 54 20 2f 77 70 2d 6c . . < @ . . P O S T / w p - l

0040 6f 67 69 6e 2e 70 68 70 20 48 54 54 50 2f 31 2e o g i n . p h p H T T P / 1 .

0050 31 0d 0a 48 6f 73 74 3a 20 6c 61 73 70 61 67 69 1 . . H o s t : l a s p a g i

0060 6e 61 73 76 65 72 64 65 73 2e 63 6f 6d 0d 0a 43 n a s v e r d e s . c o m . C

0070 6f 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65 65 70 2d o n n e c t i o n : k e e p -

0080 61 6c 69 76 65 0d 0a 43 6f 6e 74 65 6e 74 2d 4c a l i v e . C o n t e n t - L

0090 65 6e 67 74 68 3a 20 31 32 35 0d 0a 43 61 63 68 e n g t h : 1 2 5 . . C a c h

00a0 65 2d 43 6f 6e 74 72 6f 6c 3a 20 6d 61 78 2d 61 e - C o n t r o l : m a x - a

00b0 67 65 3d 30 0d 0a 55 70 67 72 61 64 65 2d 49 6e g e = 0 . . U p g r a d e - I n

00c0 73 65 63 75 72 65 2d 52 65 71 75 65 73 74 73 3a s e c u r e - R e q u e s t s :

00d0 20 31 0d 0a 4f 72 69 67 69 6e 3a 20 68 74 74 70 1 . . O r i g i n : h t t p

00e0 3a 2f 2f 6c 61 73 70 61 67 69 6e 61 73 76 65 72 . : / / l a s p a g i n a s v e r

00f0 64 65 73 2e 63 6f 6d 0d 0a 43 6f 6e 74 65 6e 74 d e s . c o m . . C o n t e n t

0100 2d 54 79 70 65 3a 20 61 70 70 6c 69 63 61 74 69 - T y p e : a p p l i c a t i

0110 6f 6e 2f 78 2d 77 77 77 2d 66 6f 72 6d 2d 75 72 o n / x - w w w - f o r m - u r

0120 6c 65 6e 63 6f 64 65 64 0d 0a 55 73 65 72 2d 41 l e n c o d e d . . U s e r - A

0130 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e g e n t : M o z i l l a / 5 .

0140 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 0 (W i n d o w s N T 10

0150 2e 30 3b 20 57 69 6e 36 34 3b 20 78 36 34 29 20 . ; W i n 6 4 ; x 6 4)

0160 41 70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e A p p l e W e b K i t / 5 3 7 .

0170 33 36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 3 6 (K H T M L , l i k e

0180 47 65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 31 31 G e c k o) C h r o m e / 11

0190 37 2e 30 2e 30 2e 30 20 53 61 66 61 72 69 2f 35 7 . 0 . 0 . 0 S a f a r i / 5

01a0 33 37 2e 33 36 0d 0a 41 63 63 65 70 74 3a 20 74 3 7 . 3 6 . . . A c c e p t : t

Frame (frame), 1,178 byte(s) Paquetes: 20368 · Mostrado: 632 (3.1%) Perfil: Default

Después de haber localizado HTTP – POST que nos interesa, damos clic en la opción seguir y en secuencia TCP.

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. Packet 19490 is selected, which is an HTTP POST request to /wp-login.php. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol, and Hypertext Transfer Protocol. The packet bytes pane shows the raw data. A context menu is open over packet 19490, with the 'Seguir' (Follow) option selected, and a submenu showing 'Secuencia TCP' (Follow in TCP Sequence) selected.

No.	Time	Source	Destination	Protocol	Length	Info
17618	1563.389279	192.168.0.101	162.243.211.192	TCP	54	53244 → 80 [FIN, ACK] Seq=1 Ack=1 Win=262400 Len=0
17621	1563.464093	162.243.211.192	192.168.0.101	TCP	60	80 → 53245 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
17622	1563.464096	162.243.211.192	192.168.0.101	TCP	60	80 → 53244 [FIN, ACK] Seq=1 Ack=2 Win=29312 Len=0
17623	1563.475137	192.168.0.101	162.243.211.192	TCP	54	53245 → 80 [ACK] Seq=2 Ack=2 Win=262400 Len=0
17624	1563.475342	192.168.0.101	162.243.211.192	TCP	54	53244 → 80 [ACK] Seq=2 Ack=2 Win=262400 Len=0
19446	1709.202599	192.168.0.101	162.243.211.192	TCP	66	53266 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19447	1709.202762	192.168.0.101	162.243.211.192	TCP	66	53267 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
19486	1709.276143	162.243.211.192	192.168.0.101	TCP	66	80 → 53267 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
19487	1709.276156	162.243.211.192	192.168.0.101	TCP	66	80 → 53266 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1412 SACK_PERM WS=128
19488	1709.276192	192.168.0.101	162.243.211.192	TCP	54	53266 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
19489	1709.276194	192.168.0.101	162.243.211.192	TCP	54	53267 → 80 [ACK] Seq=1 Ack=1 Win=262400 Len=0
19490	1709.277506	192.168.0.101	162.243.211.192	HTTP	1178	POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
19494	1709.350336					80 → 53267 [ACK] Seq=1 Ack=1125 Win=31488 Len=0
19499	1709.839970					HTTP/1.1 302 Found
19501	1709.847177					SET /login/?login=failed HTTP/1.1
19506	1709.919853					80 → 53267 [ACK] Seq=721 Ack=2063 Win=33792 Len=0
19512	1710.149672					80 → 53267 [ACK] Seq=721 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19513	1710.149672					80 → 53267 [ACK] Seq=2133 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19514	1710.149672					80 → 53267 [ACK] Seq=3545 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19515	1710.149672					80 → 53267 [ACK] Seq=4957 Ack=2063 Win=33792 Len=1412 [TCP segment of a reassembled PDU]
19516	1710.149672					HTTP/1.1 200 OK (text/html)
19517	1710.149758					53267 → 80 [ACK] Seq=2063 Ack=6485 Win=262400 Len=0
19606	1715.154521					80 → 53267 [FIN, ACK] Seq=6485 Ack=2063 Win=33792 Len=0

The packet details pane for packet 19490 shows the following structure:

- Ethernet II, Src: Ethernet II, Src: Internet Protocol, Destination: Internet Protocol, Protocol: Hypertext Transfer Protocol, Length: 1178
- Internet Protocol, Src: 192.168.0.101, Destination: 162.243.211.192, Protocol: SCTP, Length: 1178
- Hypertext Transfer Protocol, Method: POST, URI: /wp-login.php, Version: HTTP/1.1, Content-Type: application/x-www-form-urlencoded, Content-Length: 1178

The packet bytes pane shows the raw data of the selected packet, starting with the Ethernet II header and followed by the IP and HTTP headers.

Por último, en la siguiente captura se puede observar que en el seguimiento a la secuencia TCP, nos proporciona las credenciales con las cuales intentamos realizar el logeo.

Log = carlos.fuentes@hotmail.com y en pwd: jessica+hernandez+romero

The image shows a Wireshark network traffic capture. The left pane displays a list of packets, with packet 19777 (1737.298348) selected. The middle pane shows the details of this packet, which is a POST request to /wp-login.php. The right pane shows the raw packet data in ASCII format.

Packet List:

No.	Time	Source
19447	1709.202762	192.168.0.101
19486	1709.276143	162.243.211.192
19489	1709.276194	192.168.0.101
19490	1709.277506	192.168.0.101
19494	1709.350336	162.243.211.192
19499	1709.839970	162.243.211.192
19501	1709.847177	192.168.0.101
19506	1709.919853	162.243.211.192
19512	1710.149672	162.243.211.192
19513	1710.149672	162.243.211.192
19514	1710.149672	162.243.211.192
19515	1710.149672	162.243.211.192
19516	1710.149672	162.243.211.192
19517	1710.149758	192.168.0.101
19606	1715.154521	162.243.211.192
19607	1715.154697	192.168.0.101
19777	1737.298348	192.168.0.101

Packet Details (19777):

- Frame 19490: 1178 bytes on wire (9424 bits)
- Ethernet II, Src: EliteGro_09:89:bd (94:89:bd:09:89:bd), Dst: 192.168.0.101
- Internet Protocol Version 4, Src: 192.168.0.101, Dst: 162.243.211.192
- Transmission Control Protocol, Src Port: 54321, Dst Port: 80
- Hypertext Transfer Protocol
- HTML Form URL Encoded: application/x-www-form-urlencoded

Raw Data (ASCII):

```
POST /wp-login.php HTTP/1.1
Host: laspaginasverdes.com
Connection: keep-alive
Content-Length: 125
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://laspaginasverdes.com
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://laspaginasverdes.com/login/
Accept-Encoding: gzip, deflate
Accept-Language: es,es-ES;q=0.9,zh-TW;q=0.8,zh-CN;q=0.7,zh;q=0.6,en;q=0.5
Cookie: __utma=139871022.2123642107.1695674080.1695674080.1695674080.1; __utmc=139871022; __utmz=139871022.1695674080.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none); wordpress_test_cookie=WP+Cookie+check; jetpack_sso_original_request=http%3A%2F%2Flaspaginasverdes.com%2Fwp-login.php; __utmt=1; __utmb=139871022.6.10.1695674080
log=carlos.fuentes%40hotmail.com&pwd=jessica+hernandez+romero&wp-submit=Acceder&redirect_to=http%3A%2F%2Flaspaginasverdes.comHTTP/1.1 302 Found
Date: Mon, 25 Sep 2023 21:15:52 GMT
Server: Apache/2.4.18 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Set-Cookie: wordpress_test_cookie=WP+Cookie+check; path=/
X-Frame-Options: SAMEORIGIN
Set-Cookie: jetpack_sso_original_request=http%3A%2F%2Flaspaginasverdes.com%2Fwp-login.php; expires=Mon, 25-Sep-2023 22:15:52 GMT; Max-Age=3600; path=/; httponly
Set-Cookie: jetpack_sso_nonce=yw2hmkrumrjlfms8qlr; expires=Mon, 25-Sep-2023 21:25:52 GMT; Max-Age=600; path=/
Location: http://laspaginasverdes.com/login/?login=failed
Content-Length: 0
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8

GET /login/?login=failed HTTP/1.1
Host: laspaginasverdes.com
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://laspaginasverdes.com/login/
Accept-Encoding: gzip, deflate
Accept-Language: es,es-ES;q=0.9,zh-TW;q=0.8,zh-CN;q=0.7,zh;q=0.6,en;q=0.5
Cookie: __utma=139871022.2123642107.1695674080.1695674080.1695674080.1; __utmc=139871022; __utmz=139871022.1695674080.1.1.utmcsr=(direct)|utmccn=(direct)|utmcid=(none); wordpress_test_cookie=WP+Cookie+check; jetpack_sso_original_request=http%3A%2F%2Flaspaginasverdes.com%2Fwp-login.php; __utmt=1; __utmb=139871022.6.10.1695674080; jetpack_sso_nonce=yw2hmkrumrjlfms8qlr

HTTP/1.1 200 OK
Date: Mon, 25 Sep 2023 21:15:52 GMT
Server: Apache/2.4.18 (Ubuntu)
X-Pingback: http://laspaginasverdes.com/xmlrpc.php
Link: <http://laspaginasverdes.com/wp-json/>; rel="https://api.w.org/"
Link: <https://wp.me/P93eMn-5gR>; rel=shortlink
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 5339
Keep-Alive: timeout=5, max=99
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
```

Conclusión

En esta actividad aprendí muchas cosas importantes, entre las cuales destacan que entendí que cuando las claves o información sensible no son protegidas adecuadamente, el atacante aprovecha estas vulnerabilidades que generalmente son aprovechadas en: el cierre de sesión, en la gestión de las contraseñas, en el tiempo de desconexión y en la función de recordar contraseña, para robar la información sensible, incluyendo un script en una página web que se ejecuta cuando el usuario la utiliza.

También conocí y aprendí que el certificado SSL mantiene seguras las conexiones a Internet y evita que los delincuentes lean o modifiquen la información transferida entre dos sistemas. Ahora sé que cuando se ve un ícono de candado junto a la URL en la barra de direcciones, significa que hay un certificado SSL que protege el sitio web que se está visitando, francamente, solo sabía que era una página segura, ahora sé, él porque es segura.

También conocí OWASP y su proyecto de documentación más conocido TOP TEN, en el cual se listan las 10 vulnerabilidades más habituales y lo principal, cómo prevenirlas.

También aprendí como aprovechar una vulnerabilidad por falta de certificado SSL con la ayuda del software wireshark, en el cual obteniendo su ip del sitio web vulnerable y dando seguimiento a los paquetes TCP, pude obtener las credenciales que se capturan para realizar login en esta página.

A continuación, se comparte el link de acceso a la actividad en GitHub

https://github.com/charlyfu/Auditoria_informatica

Referencias

A07 Fallas de Identificación y Autenticación - OWASP Top 10:2021. (s. f.).

https://owasp.org/Top10/es/A07_2021-Identification_and_Authentication_Failures/

Rivera, D. (2021, 29 noviembre). Riesgo A2 en OWASP - Pérdida de autenticación y gestión de sesiones.

<https://blog.pleets.org/article/es/owasp-a2-broken-authentication>

Kaspersky. (2023, 29 agosto). Qué es un certificado SSL: definición y explicación. latam.kaspersky.com.

<https://latam.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate>

A2-Pérdida autenticación y gestión sesiones :: PROYECTO SEGURIDAD INFORMÁTICA. (s. f.).

<https://liliseguridadinformatica.webnode.es/guia-de-buenas-practicas/disenio/a2/>

Da Silva, D. (2023, 18 septiembre). ¿Qué es SSL certificado y por qué tener en tu sitio web? Zendesk

MX. <https://www.zendesk.com.mx/blog/que-es-ssl-certificado/>