



Actividad 3 - Cross Site Scripting (XSS)

Auditoría Informática

Ingeniería en Desarrollo de Software

Tutor: Jessica Hernández Romero.

Alumno: Carlos Alberto Fuentes Mendoza

Fecha: 12-octubre-2023

Índice

Introducción	3
Descripción	5
Justificación	6
Etapa 1	
Descripción del sitio web	8
Ataque al sitio	9
Etapa 2	
Ataque al sitio	15
Etapa 3	
Ataque al sitio	29
Conclusión	40
Referencias	41

Introducción

En esta tercera etapa estudiaremos sobre Cross Site Scripting, también conocida como XSS, una de las vulnerabilidades más comunes desde 2014. De hecho, según OWASP, esta vulnerabilidad será incluida dentro de la categoría de inyecciones, y forma parte del top 10 de vulnerabilidades más frecuentes en aplicaciones web de 2021, así como las vulnerabilidades que hemos estudiado en las actividades anteriores.

En primer lugar, es importante tener en cuenta que, con esta vulnerabilidad, los atacantes explotan la confianza que un usuario tiene en un sitio en particular, y esto nos da una dimensión del impacto que puede tener. Este tipo de vulnerabilidad puede ser explotada de dos maneras: de forma reflejada y de forma almacenada. A continuación, una breve explicación de cada una:

- **XSS Reflejado:** Consiste en modificar valores que la aplicación web usa para pasar variables entre dos páginas. Un clásico ejemplo de esto es hacer que a través de un buscador se ejecute un mensaje de alerta en JavaScript. Con XSS reflejado, el atacante podría robar las cookies para luego robar la identidad, pero para esto, debe lograr que su víctima ejecute un determinado comando dentro de su dirección web. Para esto, los cibercriminales suelen enviar correos engañosos para que sus víctimas hagan clic en un enlace disfrazado y así se produzca el robo.
- **XSS Almacenado (o Persistente):** Consiste en insertar código HTML (programación web) peligroso en sitios que lo permitan; de esta forma quedará visible a los usuarios que ingresen en el sitio modificado.
- **XSS Basado en DOM:** Esta variante de XSS no implica la inyección de código en la respuesta del servidor, sino que el código malicioso modifica el Document Object Model (DOM) de una página web después de que se ha cargado en el navegador del usuario. Esto puede ocurrir cuando se

manipulan elementos HTML o scripts en tiempo real.

- Las consecuencias del XSS pueden ser graves e incluyen el robo de cookies de sesión, el secuestro de sesiones de usuario, el robo de información confidencial, la redirección a sitios web maliciosos, la ejecución de acciones no autorizadas en nombre del usuario y más.
- Para prevenir el XSS, las aplicaciones web deben implementar medidas de seguridad, como la validación y escape de datos de entrada, la configuración adecuada de encabezados HTTP (como Content Security Policy o CSP), y la educación y concienciación del personal de desarrollo sobre las mejores prácticas de seguridad. También es importante mantener el software y las bibliotecas actualizadas para parchear posibles vulnerabilidades de XSS.

La manera más básica de evitar ataques por XSS consiste en validar y sanitizar toda la entrada de datos del usuario. Cualquier dato introducido en la página por los usuarios se tiene que considerar poco seguro, y por lo tanto, nunca debemos confiar que no puede resultar en un ataque, especialmente cuando esos datos luego se van a volcar dentro del propio sitio, como un sistema de comentarios, en donde los mensajes enviados por los usuarios aparecerán más tarde como contenido del propio web, es de suma importancia realizar todo tipo de operaciones que aseguren que las cadenas de texto introducidas son inofensivas.

Todos los lenguajes de programación tienen mecanismos para validar y sanitizar, siendo importante que estas operaciones se realicen del lado del servidor, pues es el entorno donde podemos estar seguros que nuestro código de validación y sanitización será ejecutado sin alteraciones. También es clave usar mecanismos que nos aseguren que los datos volcados en la página son inofensivos. Por ejemplo, convirtiendo cualquier valor de una cadena en sus caracteres especiales del HTML, tal como se hace con las funciones htmlspecialchars() o htmlentities() de PHP.

Descripción

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

Para esta tercera etapa se solicita realizar una prueba de vulnerabilidad de Cross Site Scripting (XSS). En ella se debe obtener las credenciales que se ingresen para iniciar sesión. Después, desde Burp Suite, modificar la información para comprobar si se puede iniciar sesión o no.

Para este proyecto final, utilizando un sitio web vulnerable, y el programa utilizado en la Actividad 2, vamos a trabajar con la vulnerabilidad Cross Site Scripting (XSS). Así, con la ayuda de la aplicación Burp Suite, vamos a captar las credenciales que se ingresen cuando se inicie sesión, y comprobar si se puede modificar.

En Primer lugar, vamos a alterar el correo electrónico ingresado o nombre de usuario, después, debemos ver que el sistema mandó alerta de que las credenciales ingresadas son incorrectas. Esto se debe a que se modificó el correo electrónico o nombre de usuario, por uno que no está registrado.

En segundo lugar, vamos a alterar la contraseña, después, debemos ver que el sistema mandó alerta de que las credenciales ingresadas son incorrectas. Esto se debe a que se modificó la contraseña, por una que no está registrada.

En tercer lugar, vamos a ingresar un correo electrónico y contraseña diferentes que estén registrados en el sitio web, con esto se podrá iniciar sesión

Justificación

Prevenir ataques de Cross-Site Scripting (XSS) es de vital importancia para la seguridad de las aplicaciones web y la protección de los datos y la privacidad de los usuarios. Aquí tienes algunas razones que destacan la importancia de prevenir los ataques XSS:

- **Protección de Datos Sensibles:** Los ataques XSS pueden permitir a los atacantes robar datos sensibles de los usuarios, como contraseñas, información de tarjetas de crédito, datos personales y más. Prevenir XSS protege la confidencialidad de estos datos.
- **Integridad de Datos:** Los atacantes pueden manipular los datos en una página web si logran ejecutar código malicioso. Esto puede llevar a la corrupción de datos, la creación de registros falsos y otros problemas que afectan la integridad de la información.
- **Privacidad de los Usuarios:** Los ataques XSS pueden permitir a los atacantes tomar el control de la sesión de un usuario, lo que les permite acceder a la cuenta del usuario y realizar acciones en su nombre sin su consentimiento. Esto viola la privacidad de los usuarios y puede tener consecuencias graves.
- **Reputación de la Organización:** Los ataques XSS exitosos pueden dañar la reputación de una organización. Los usuarios pueden perder la confianza en una aplicación o sitio web si se enteran de que es vulnerable a ataques de este tipo.
- **Cumplimiento Normativo:** En muchos lugares, existen regulaciones y leyes que requieren la protección de datos personales y la seguridad de las aplicaciones web. No prevenir XSS puede llevar a incumplir estas regulaciones y enfrentar sanciones legales.

- Efectos en la Experiencia del Usuario: Los ataques XSS pueden interrumpir la experiencia del usuario al redirigirlos a sitios web maliciosos, mostrar contenido no deseado o ralentizar el rendimiento del sitio. Esto puede llevar a la pérdida de usuarios y clientes.
- Reducción de Riesgos Financieros: Evitar ataques XSS puede ayudar a evitar costos financieros significativos asociados con la recuperación de incidentes de seguridad, la atención al cliente y las sanciones legales.
- Mantenimiento de la Confianza del Cliente: La seguridad de la aplicación web es fundamental para mantener la confianza de los clientes y usuarios. Los usuarios tienden a preferir aplicaciones y sitios web que se preocupan por su seguridad y privacidad.

Etapa 1

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>

The screenshot shows the homepage of laspaginasverdes.com. At the top, there is a navigation bar with links for CONTACTO, DIRECTORIO, B2B, ECOFEST, HERRAMIENTAS, and INGRESAR. Below the navigation bar, a large green banner features the text "ESCOGE TU PAÍS" above a circular image of the Angel of Independence in Mexico City. The background of the banner is a grayscale city skyline. Below the banner, a green section titled "¿DONDÉ PUEDO ENCONTRARLO?" lists various service locations with their names and logos. Some of the listed locations include "Cocoa Coyoacán", "Rafaela", "Drupa", "Cielito Parque Delta", "Cielito Plaza Universidad", "Cielito Pabellón del Valle", "Cielito Reforma 234", "Cielito Centro Coyoacán", "Cielito Prado Norte", "Cielito WTC", "Cielito Parroquia", and "Cielito Michoacán".

Ataque al 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, there is a search bar with the URL "https://who.is/tools/laspaginasverdes.com?id=03AfCWeA4psuMzvglkbXHflcXdR4gKw1TCT4kDlyqEYCzSrZLC02tl6lhg9LAHKkXfku5E4ZOAcudVnDNpyajSnY4oquuslEX-OTp0SVmWYVYnzWv9wR...". Below the search bar, the who.is logo and navigation links for Premium Domains, Transfer, Features, Login, and Sign Up are visible. A message states ".laspaginasverdes.com is already registered. Interested in buying it? [Make an Offer](#)". A row of domain extension buttons (.com, .net, .org, .co, .io, .app, .live) shows availability status: .com is taken, .net is available (\$14.99), .org is available (\$8.99), .co is available (\$12.99), .io is available (\$34.99), .app is available (\$16.99), and .live is available (\$3.99). A green "Purchase Selected Domains" button is located below the extensions. In the bottom right corner of the main content area, there is a "cached" link. Below this, a section titled "laspaginasverdes.com" contains diagnostic tools (Whois, DNS Records, Diagnostics). The "Diagnostics" tab is selected, showing a "Ping" section with command-line output for pinging the site's IP (162.243.211.192) and a "Traceroute" section with detailed network path information.

laspaginasverdes.com is already registered. Interested in buying it? [Make an Offer](#)

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

Purchase Selected Domains

cached

laspaginasverdes.com

diagnostic tools

Whois DNS Records Diagnostics

Ping

```
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
```

Traceroute

```
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
```

En la siguiente pantalla se observa la captura de paquetes de la aplicación wireshark al hacer ping desde la terminal de Windows en la página web <http://laspaginasverdes.com/> con la ip 192.243.211.192.

The screenshot shows the Wireshark interface with the following details:

- Network Interface:** *Ethernet
- File Filter:** ip.addr == 162.243.211.192
- Table Headers:** No., Time, Source, Destination, Protocol, Length, Info
- Table Data:** A list of 13 captured ICMP Echo requests and replies between the source IP 192.168.0.101 and destination IP 162.243.211.192. The first request (Frame 1374) has an info field: "id=0x0001, seq=25/6400, ttl=128 (reply in 1376)". Subsequent frames show increasing sequence numbers (seq=26, 27, 28) and decreasing TTL values (54, 53, 52).
- Selected Frame Details:**
 - Frame 1374:** 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface Ethernet II, Src: EliteGro_09:89:bd (94:c6:91:09:89:bd), Dst: TP-Link_ad:19 (162.243.211.192)
 - Protocol:** Internet Protocol Version 4, Src: 192.168.0.101, Dst: 162.243.211.192
 - Type:** Internet Control Message Protocol
- Hex and ASCII Dump:** Displays the raw hex and ASCII representation of the selected frame.
- CMD Window:**

```
C:\Users\chat1>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\chat1>
```
- Bottom Status Bar:** wireshark_EthernetQF3882.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

The screenshot shows a web browser window with the URL 'laspaginasverdes.com/login/' in the address bar. A warning message 'No es seguro' is displayed above the address bar. The main content area features a large blue banner with a woman jumping and holding a laptop, with the text 'ACCESO A USUARIOS'. Below the banner is a login form with fields for email ('carlos.fuentes@hotmail.com') and password ('.....'). There are checkboxes for 'Recuérdame' and '¿Has perdido tu contraseña?'. A red 'ACCEDER' button is at the bottom right of the form. To the right of the form, there is a link '¿USUARIO NUEVO? ¡REGÍSTRATE!' and a small explanatory text. The top navigation bar includes links for 'CONTACTO', social media icons, and menu items like 'DIRECTORIO', 'B2B', 'ECOFEST', 'HERRAMIENTAS', and 'INGRESAR'.

No es seguro | laspaginasverdes.com/login/

NoSuchBucketThe specified bucket does not existgraphicsmxW0H58HEGHNS6SZVTma4rGmmoCKJofxIO8mp+53XOIRvkvh1+N5T4kozN6p1h7A/dgiK]

CONTACTO f

las páginas verdes Piensa Sustentable

DIRECTORIO B2B ECOFEST HERRAMIENTAS INGRESAR

ACCESO A USUARIOS

LOGIN

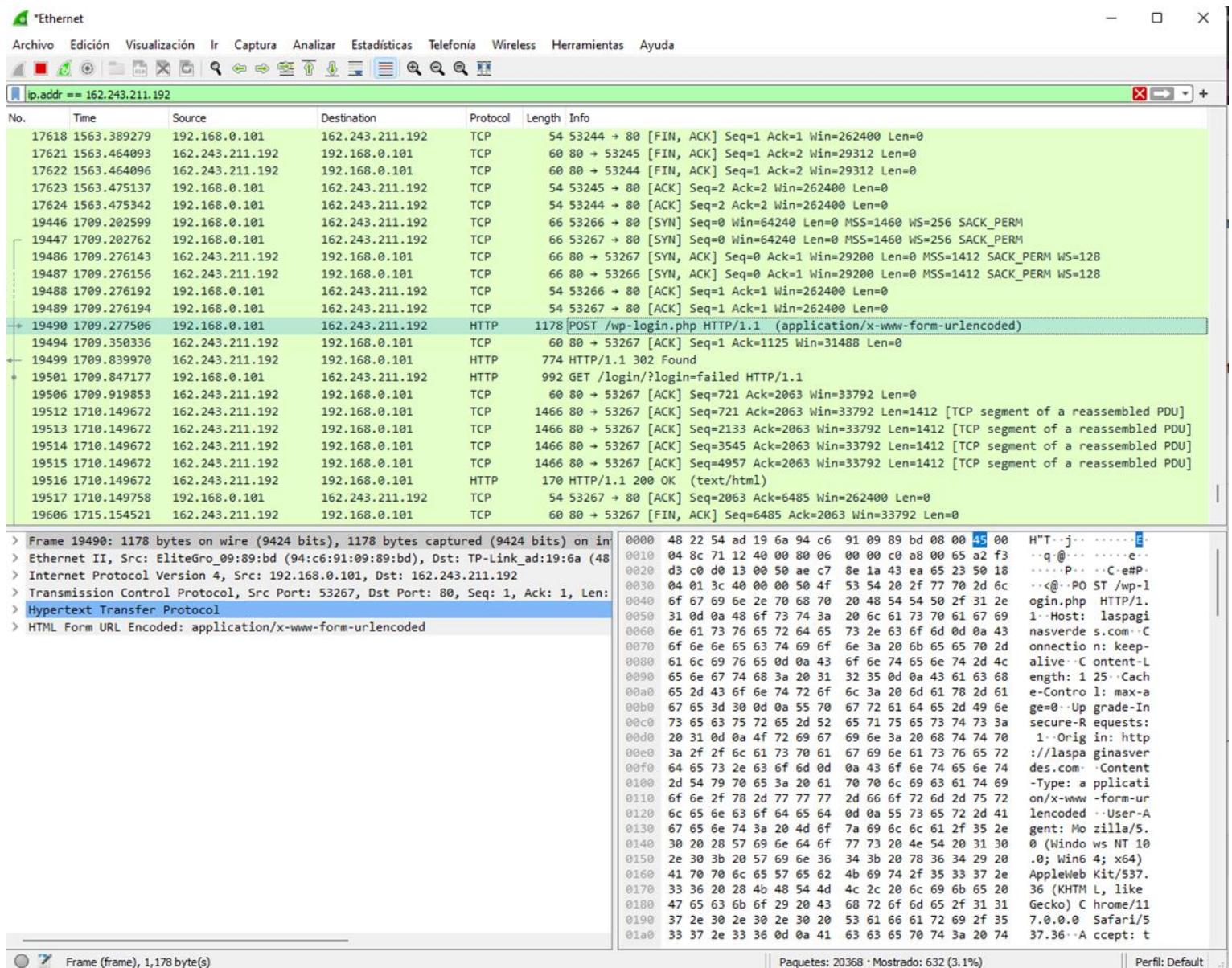
Accede a tu cuenta para continuar tu experiencia verde

carlos.fuentes@hotmail.com
 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 observan los paquetes capturados por la aplicación, en los cuales encontramos el protocolo HTTP que es el que nos interesa.



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

The screenshot shows a Wireshark capture window with the following details:

- Selected Packet:** 1178 POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
- Protocol:** HTTP
- Source:** 192.168.0.101
- Destination:** 162.243.211.192
- Info:** 1178 POST /wp-login.php HTTP/1.1 (application/x-www-form-urlencoded)
- Content:** Marcar/Desmarcar paquete, Ignorar/No ignorar paquete, Establecer/Anular referencia de tiempo, Modificar horario..., Comentarios de paquete, Editar nombre resuelto, Aplicar como filtro, Preparar como filtro, Filtro de conversación, Colorear conversación, SCTP, Seguir, Copiar, Preferencias de protocolo, Decodificar como..., Mostrar paquete en nueva ventana
- Hex View:** Shows the raw bytes of the selected packet, including the form-urlencoded data.
- Text View:** Shows the decoded text of the selected packet, including the form-urlencoded data.
- Panels:** Frame (frame), 1,178 byte(s); Paquetes: 20918 · Mostrado: 634 (3.0%); Perfil: Default

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

```

* Ethernet
Wireshark - Seguir secuencia TCP (tcp.stream eq 195) - Ethernet

Archivo Edición Visualización Ir Captura A
tcp.stream eq 195

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

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; __utmx=139871022.1695674080.1.1.utmc=(direct)|utmccn=(direct)|utmcmd=(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=ypw2hmkrumrjlfms8qlr; 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; __utmx=139871022.1695674080.1.1.utmc=(direct)|utmccn=(direct)|utmcmd=(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=ypw2hmkrumrjlfms8qlr
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
2 client pkts, 6 server pkts, 3 sum(s).

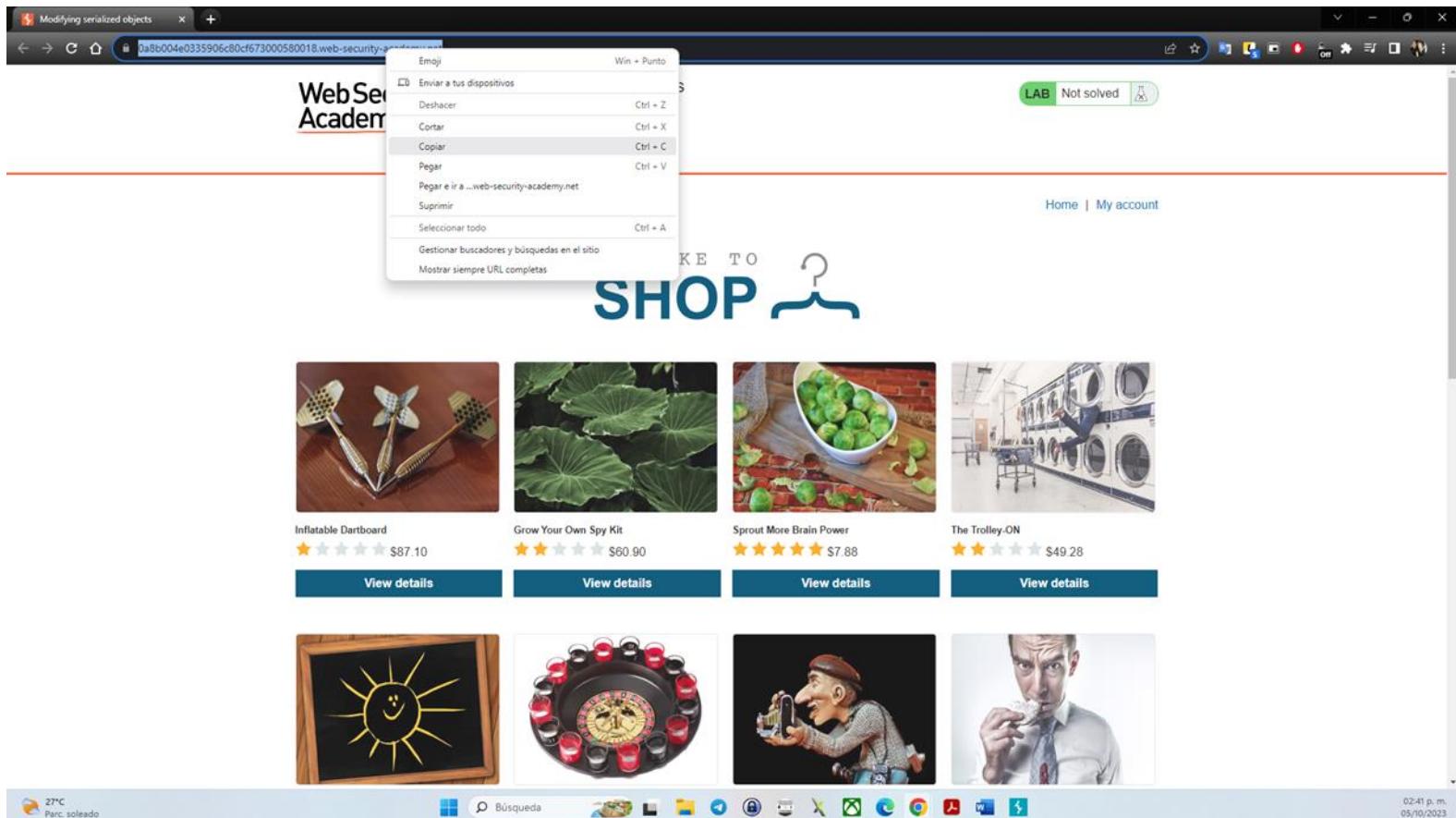
Conversación completa (8546 bytes) Mostrar datos como ASCII
Buscar: Secuencia 195 Buscar siguiente

```

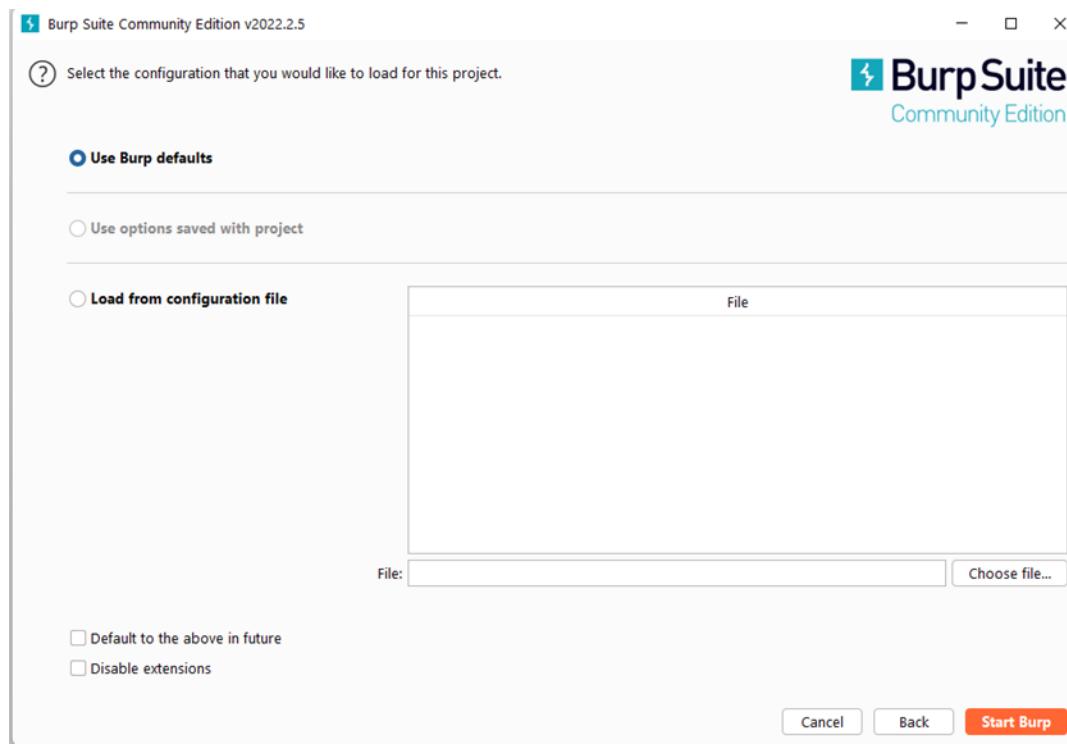
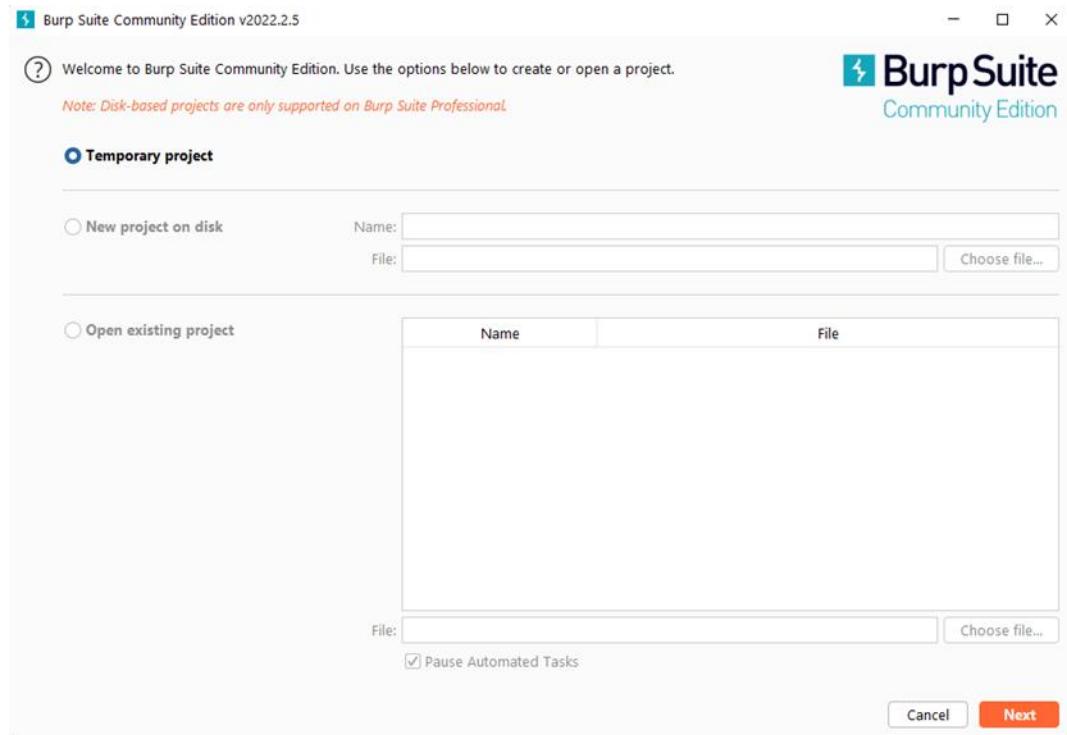
Etapa 2

Ataque al sitio

Para comenzar este ataque, nos dirigimos al laboratorio de la página y copiamos la dirección url del sitio web.



Enseguida pegamos el enlace de la página en la aplicación Burp Suite, para esto, se crea un proyecto temporal con las opciones default.



Una vez abierto el panel de trabajo de la aplicación, nos dirigimos a la sección proxy, en donde dando clic en el botón open browser, se abrirá el navegador de la aplicación y pegaremos la url que copiamos.

The screenshot shows the Burp Suite interface. On the left, the 'Intercept' tab is highlighted in red, while 'Forward', 'Drop', and 'Action' tabs are in grey. Below these are buttons for 'Forward', 'Drop', 'Intercept is off' (which is currently active), 'Action', and 'Open Browser'. A small icon of a traffic light with a red light is displayed. The text 'Intercept is off' is centered below the traffic light icon. A detailed description follows: 'When enabled, requests sent by Burp's browser are held here so that you can analyze and modify them before forwarding them to the target server.' Below this are two buttons: 'Learn more' and 'Open Browser' (in orange). On the right, a browser window is open to a page titled 'Modifying serialized objects' from 'Web Security Academy'. The page features a large banner with the text 'WE LIKE TO SHOP' and a hanger icon. Below the banner are four product cards: 'Inflatable Dartboard' (rating 3 stars, \$87.10), 'Grow Your Own Spy Kit' (rating 4 stars, \$60.90), 'Sprout More Brain Power' (rating 5 stars, \$7.88), and 'The Trolley-ON' (rating 3 stars, \$49.28). Each card has a 'View details' button. Further down are two more rows of products: a sun drawing on a chalkboard and a roulette wheel game.

Procedemos entrando al sitio web con las credenciales proporcionadas en el PDF de la actividad.

Usuario: wiener

Contraseña: peter

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The Burp Suite interface has tabs for Project, Intruder, Repeater, Window, Help, and a temporary project titled "Modifying serialized objects". The Proxy tab is selected, showing "Dashboard", "Target", and "Proxy" sub-tabs. Below these are buttons for "Forward", "Drop", "Intercept is off" (which is highlighted in red), "Action", and "Open Browser". A small icon of a traffic light is displayed. The status bar at the bottom of the Burp window says "Intercept is off". The browser window shows a login page for "WebSecurity Academy". The URL is "https://0a8b004e0335906c80cf673000580018.web-security-academy.net/login". The page title is "Modifying serialized objects". The login form has fields for "Username" (wiener) and "Password" (peter). A green "Log in" button is at the bottom. The status bar at the bottom of the browser window says "Home | My account". The task bar at the bottom of the screen shows various application icons, including a weather icon (27°C, Parc. soleado), a search icon, and a date/time icon (02:55 p. m., 05/10/2023).

Nos dirigimos nuevamente a la sección Proxy en la pestaña HTTP history, en donde buscamos en el encabezado URL, la dirección /login con el método POST, aquí seleccionamos la Cookie session (las letras que aparecen en rojo) y enviamos a Decoder.

Burp Suite Community Edition v2022.2.5 - Temporary Project

HTTP history

Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
https://ua08b004e0335906c80cf...	GET	/resources/labheader/js/labHeader.js			200	7258	script	js			✓	/9.125.84.16		15:49:40 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/resources/images/shop.svg			200	8852	XML	svg			✓	79.125.84.16		15:49:47 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/resources/labheader/images/logoAc...			200	942	XML	svg			✓	79.125.84.16		15:49:47 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:49:47 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/my/account			302	86					✓	79.125.84.16		15:54:40 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/login			200	3148	HTML			Modifying serialized obj...	✓	79.125.84.16		15:54:41 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/academyLabHeader			101	147					✓	79.125.84.16		15:54:42 5 Oc...	8080
https://ua08b004e0335906c80cf...	POST	/login		✓	200	3226	HTML			Modifying serialized obj...	✓	34.246.129.62		15:56:46 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/academyLabHeader			101	147					✓	34.246.129.62		15:56:47 5 Oc...	8080
https://ua08b004e0335906c80cf...	POST	/login		✓	302	238					✓	34.246.129.62	session=Tzo0IJVc...	15:56:58 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/my-account?id=wiener		✓	200	3243	HTML			Modifying serialized obj...	✓	34.246.129.62		15:56:58 5 Oc...	8080
https://ua08b004e0335906c80cf...	GET	/academyLabHeader			101	147					✓	34.246.129.62		15:56:58 5 Oc...	8080

Request

Pretty Raw Hex

```
1 POST /login HTTP/2
2 Host: ua08b004e0335906c80cf673000580018.web-security-academy.net
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 30
5 Cache-Control: max-age=0
6 Sec-Ch-Ua: "(Not(A BRAND);v="8", "Chromium";v="100"
7 Sec-Ch-Ua-Mobile: ?0
8 Sec-Ch-Ua-Platform: "Windows"
9 Upgrade-Insecure-Requests: 1
10 Origin: https://ua08b004e0335906c80cf673000580018.web-security-academy.net
11 Content-Type: application/x-www-form-urlencoded
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
13 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: no-user
16 Set-Cookie: session=Tzo0IJVc2Yy1jeyOntzOjg6InVzZXJuYW1lztz0jY6IndpZW5lc1...
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 302 Found
2 Location: /my-account?id=wiener
3 Set-Cookie: session=Tzo0IJVc2Yy1jeyOntzOjg6InVzZXJuYW1lztz0jY6IndpZW5lc1...
```

Decoder Context Menu (highlighted):

- Scan
- Send to Intruder
- Send to Repeater
- Send to Sequencer
- Send to Comparer
- Send to Decoder**
- Show response in browser
- Request in browser
- Engagement tools [Pro version only]
- Copy URL
- Copy as curl command
- Copy to file
- Save item
- Convert selection
- Cut
- Copy
- Paste

Decoded from: URL encoding

```
0:4:"User":1:(m:0:"username":m:6:"wiener";m:5:"admin":b:0:)
```

Decoded from: Base64

```
Tzo0IJVc2Yy1jeyOntzOjg6InVzZXJuYW1lztz0jY6IndpZW5lc17czoi0JhZGipbi17Yjow030V3d
```

Request Attributes

Request Body Parameters

Request Cookies

Request Headers

Response Headers

Time: 03:00 p.m. 05/10/2023

En la siguiente captura se observa la pantalla decoder, en esta sección decodificaremos la cookie, para esto, en la primera opción elegimos decodificar a url y en la segunda a decodificar a base 64.

En la tercera opción, ya tenemos la información serializada, esto lo comprobamos ya que al final de la línea aparece “b:0;” el cual el cero significa que este usuario no tiene privilegios de administrador.

The screenshot shows the Burp Suite Community Edition v2022.2.5 interface with the Decoder tab selected. There are three rows of data being processed:

- Row 1:** Shows the raw hex data: Tzo0OjVc2VyljoyOntzOjg6lnVzZXJuYW1l|jtzOjY6IndpZW5lcil7czo1OjhZG1pbil7yjowO30%3d. To its right are buttons for Text (selected), Hex, Decode as ..., Encode as ..., Hash ..., and Smart decode.
- Row 2:** Shows the decoded URL: Tzo0OjVc2VyljoyOntzOjg6lnVzZXJuYW1l|jtzOjY6IndpZW5lcil7czo1OjhZG1pbil7yjowO30=. To its right are buttons for Text (selected), Hex, Decode as ..., Encode as ..., Hash ..., and Smart decode.
- Row 3:** Shows the serialized JSON object: O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:0;} To its right are buttons for Text (selected), Hex, Decode as ..., Encode as ..., Hash ..., and Smart decode.

En la siguiente captura se puede observar que se dan privilegios de administrador cambiando el “0” al final de la información serializada por el “1”, para posteriormente codificarla a base 64 y por último a url.

Seleccionamos y copiamos toda la información del último renglón ya que es la que tiene permisos de administrador.

The screenshot shows a Burp Suite interface with several requests and responses. The last request in the sequence is highlighted:

```
Tzo0OiUvc2VyljoyOntzOjg6InVzZXJuYW1lJtzQjY6indpZW5lcil7cz01OjhZG1pbil7yjoxO30=
```

The response body contains the serialized data:

```
O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}
```

The response is then processed through a series of encoding steps:

- Text → Hex
- Decode as ...
- Encode as ...
- Hash ...
- Smart decode

After decoding, the data is shown again:

```
O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}
```

Finally, the data is encoded back into a URL:

```
Tzo0OiUvc2VyljoyOntzOjg6InVzZXJuYW1lJtzQjY6indpZW5lcil7cz01OjhZG1pbil7yjoxO30=
```

The bottom status bar shows the system temperature at 27°C and the date/time as 05/10/2023 03:15 p.m.

Procedemos a pasar nuevamente a la opción de proxy y encendemos el interceptor, posteriormente actualizamos el navegador para que nos dé nuevamente la información de la sesión del usuario.

Continuamos cambiando la información de sesión del usuario (las letras en rojo) por las que codificamos con permisos de administrador.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite 'Proxy' tab, a request to `https://0a8b004e0335906c80cf673000580018.web-security-academy.net:443` is displayed. The 'Raw' tab shows the modified serialized object with red highlights on certain characters. The browser window shows a login page for 'WebSecurity Academy'. The 'My Account' section displays the message 'Your username is: wiener'. Below it is a form with an 'Email' input field and a green 'Update email' button. The status bar at the bottom right indicates the date and time as '05/10/2023 03:19 p.m.'

Como se puede observar en la siguiente captura, en las opciones de usuario del navegador aparece una nueva opción con el título “Admin panel”.

The screenshot shows two windows side-by-side. On the left is the Burp Suite interface, specifically the Proxy tab, displaying a captured GET request to https://0a8b004e0335906c80cf673000580018.web-security-academy.net/. The request details pane shows the full HTTP header, including the 'Upgrade' field set to 'websocket'. On the right is a browser window titled 'Modifying serialized objects' from 'WebSecurity Academy'. The URL in the address bar is https://0a8b004e0335906c80cf673000580018.web-security-academy.net/my-account?id=wiener. The page content shows a 'My Account' section with a form for updating the email address. At the top of the page, there is a navigation bar with links for 'Home', 'Admin panel', 'My account', and 'Log out'. A green 'LAB' button and a 'Not solved' badge are visible in the top right corner of the browser window.

Procedemos a dar clic en la nueva opción y cambiamos nuevamente la cookie session(letras rojas) con la que tenemos con permisos de administrador y damos clic en el botón forward.

The screenshot shows the Burp Suite interface on the left and a browser window on the right. In the Burp Suite Proxy tab, a request is captured for the URL `https://0a8b004e0335906c80cf673000580018.web-security-academy.net/my-account?id=wiener`. The request details show a long, encoded cookie value. The browser window shows a login page titled "Modifying serialized objects" from "WebSecurity Academy". The page displays a "My Account" section with a placeholder "Your username is: wiener" and a form field for "Email". Below the form is a green "Update email" button. The browser's status bar indicates the URL and shows system information like temperature (27°C), date (05/10/2023), and time (03:25 p.m.).

Procedemos a cambiar nuevamente la cookie session(letras rojas) con la que tenemos con permisos de administrador y damos clic en el botón forward y de igual forma damos clic en el botón forward.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite 'Proxy' tab, a request is captured for the URL <https://0a8b004e0335906c80cf673000580018.web-security-academy.net:443>. The request contains a session cookie with red characters ('wiener') and a long session ID. The browser window shows the 'My Account' page of the Web Security Academy. The URL in the address bar is <https://0a8b004e0335906c80cf673000580018.web-security-academy.net/my-account?id=wiener>. The page displays the user's account information, including the username 'wiener'. A green button labeled 'Update email' is visible on the page.

En la siguiente captura se observa como en el navegador, ahora aparece una interfaz que solo se tiene acceso con permisos de administrador, en la cual se pueden muestrar los usuarios registrados.

The screenshot shows two windows side-by-side. On the left is the Burp Suite Community Edition v2023.3.2 interface, specifically the Proxy tab. It displays a network request to the URL <https://0a8b004e0335906c80cf673000580018.web-security-academy.net:443>. The request details show a GET request for the root path. On the right is a browser window titled "Modifying serialized objects" with the URL <https://0a8b004e0335906c80cf673000580018.web-security-academy.net/admin>. The page title is "WebSecurity Academy". The main content area is titled "Modifying serialized objects" and shows a list of users: "wiener - Delete" and "carlos - Delete". Below the users, there is a link "Back to lab description >". At the bottom of the browser window, the status bar shows the date and time: "03:37 p.m. 05/10/2023".

A continuación, eliminaremos el usuario Carlos, para esto, damos clic en la opción Delete y enseguida pegaremos nuevamente la cookie session con los permisos de administrador y damos clic en forward.

The screenshot shows the Burp Suite interface on the left and a browser window on the right. In the Burp Suite Proxy tab, a request to 'https://0a8b004e0335906c80cf673000580018.web-security-academy.net:443' is captured, showing a GET request to '/admin/delete?username=carlos'. The browser window shows a 'Modifying serialized objects' page for 'WebSecurityAcademy'. The URL is 'https://0a8b004e0335906c80cf673000580018.web-security-academy.net/admin'. The page lists users 'wiener' and 'carlos', each with a 'Delete' link. The status bar at the bottom indicates 'Calle Monte de... Carretera cerrada' and the date '05/10/2023'.

Como podemos observar en la siguiente pantalla, el usuario Carlos se ha eliminado perfectamente.

The screenshot shows two windows side-by-side. On the left is the Burp Suite Community Edition interface, specifically the Proxy tab. It displays an intercept session for a GET request to 'https://0a8b004e0335906c80cf673000580018.web-security-academy.net:443'. The request headers include 'Sec-WebSocket-Key: efVve9i74EPQd8hA4XVJUA=='. The right window is a browser window titled 'Modifying serialized objects' from 'WebSecurity Academy'. The URL is 'https://0a8b004e0335906c80cf673000580018.web-security-academy.net/admin'. The page shows a success message: 'Congratulations, you solved the lab!' and 'User deleted successfully!'. There is also a link to 'Back to lab description >'. At the bottom of the browser window, there are links for 'Home', 'Admin panel', and 'My account'. The task status is marked as 'Solved' with a green badge.

Etapa 3

Ataque al sitio

Comenzamos abriendo la aplicación Burp Suite y nos dirigimos a la sección proxy, en donde dando clic en el botón open browser, se abrirá el navegador de la aplicación y pegaremos la url del sitio web y encendemos el interceptor, posteriormente, ingresamos las credenciales para iniciar sesión en el navegador y vemos que la aplicación intercepta la información, de esta manera obtenemos las credenciales de la cuenta registrada.

Nombre de usuario: charlyfu

Contraseña: GiDAYLEE0qYxuAVuwhAU

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite's Proxy tab, a POST request to 'http://www.mvp-access.com:80 /toro/login_user.asp' is captured. The request body contains the user 'charlyfu' and the password 'GiDAYLEE0qYxuAVuwhAU'. The browser window shows a login form for 'Conectado al foro' on the website 'mvp-access.com'. The user has entered 'charlyfu' and 'GiDAYLEE0qYxuAVuwhAU'. Below the form, a message states 'No está registrado?' (Not registered?). The browser taskbar at the bottom shows various icons and the date '08/10/2023'.

Posteriormente damos clic en forward y vemos que efectivamente ingresamos al sitio web con las credenciales que capturo el interceptor de la aplicación.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The browser window displays a forum page titled "Foro de Access y VBA". The page includes a header with "** NORMAS DEL FORO **", a navigation bar with links like "Inicio del foro", "Panel perfil de usuario", "Preguntas frecuentes", "Buscar", "Eventos", "Miembros", "Mis mensajes [charlyfu]", and "Cerrar sesión [charlyfu]". Below the header, there's a message "Son las 03:56" and "Su última visita fue hace 6 minutos a las 03:50". The main content area shows several forum categories and their posts:

- Avisos Importantes**
 - Avisos de interés general**: 6 temas, 15 mensajes, última respuesta "ACTUALIZACIÓN FORO OFFLINE" por admin el 30/Marzo/2016 a las 10:42.
- Foro**
 - Access y VBA**: 2073 temas, 11584 mensajes, última respuesta "dfirst error 94" por xavi el 05/Octubre/2023 a las 06:54.
 - Access y Otros sistemas**: 47 temas, 158 mensajes, última respuesta "Consulta de datos anexados" por EPAZ el 06/Junio/2023 a las 00:50.
 - Tus Funciones Favoritas & Aportaciones & Artículos**: 17 temas, 29 mensajes, última respuesta "App musical - Access 2016" por pmartimor el 13/Junio/2023 a las 00:58.
 - Dudas ya consultadas y Resueltas**: 4 temas, 8 mensajes, última respuesta "Duda" por Bryan.spe el 03/Febrero/2022 a las 00:52.
- Relacionado con Access**
 - Curso de Access y VBA**: 3 temas, 2 mensajes, última respuesta "Curso completo Eduardo Olaz" por Mihura el 24/Julio/2022 a las 00:09.
 - Enlaces a páginas**: 6 temas, 6 mensajes, última respuesta "Nuevo Libro "Microsoft Access"..." por Cheal el 22/Mayo/2012 a las 16:07.
- Profesionales en este Foro**
 - Para Empresas: Contrate aquí Profesionales**: 21 temas, 37 mensajes, última respuesta "Aplicación para gestionar pequeña..." por dlb el 13/Septiembre/2023 a las 12:07.

Ahora, realizamos nuevamente el proceso, solo que, en esta ocasión, cambiamos el nombre de usuario de “charlyfu” a “charlyfuentes” y en contraseña la mantenemos sin ningún cambio, paso siguiente damos clic en forward.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite 'Proxy' tab, a POST request to `/foro/login_user.asp` is displayed. The 'Selected text' in the Inspector panel shows the user name `charlyfuentes`. In the browser window, the URL is `mvp-access.com/foro/login_user.asp?returnURL=`, and the page title is **** NORMAS DEL FORO ****. The login form has the user name field set to `charlyfuentes` and the password field set to `charlyfuentes`. Both 'Sí' radio buttons for 'No' are selected under the checkboxes for '¿No está registrado?' and '¿Olvidó su contraseña?'. The bottom status bar shows the date and time as 08/10/2023 08:01 p.m.

Como podemos observar en la siguiente pantalla, el sitio web nos arroja una alerta en la cual nos menciona que las contraseñas ingresadas son incorrectas, esto se debe a que la modificación del nombre de usuario por uno inexistente a funcionando correctamente.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite 'Proxy' tab, a request is captured for 'http://www.mvp-access.com:80 [92.53.241.26]'. The raw request content is as follows:

```
1 GET /foro/quick_search.asp?ID=0&SSL=True HTTP/1.1
2 Host: www.mvp-access.com
3 Upgrade-Insecure-Requests: 1
4 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/112.0.5615.50 Safari/537.36
5 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
6 Referer: http://www.mvp-access.com/foro/login_user.asp
7 Accept-Encoding: gzip, deflate
8 Accept-Language: es-ES,es;q=0.9
9 Cookies: ASPSESSIONIDSQDCCB=BBFPQDJBFODMKMKKMPHLCLJ; vvf10fID=;
vvf10MobileView=; vvf10sVisit=; vvf10sLID=; vvf10sID=
SID=913B232bb1857zdffz8791d0B23z1244097222
10 Connection: close
11
12
```

In the browser window, the URL is 'mvp-access.com/foro/login_user.asp'. The page displays an error message: 'www.mvp-access.com dice El nombre de usuario o contraseña es incorrecta. Por favor, inténtelo de nuevo.' A blue 'Aceptar' (Accept) button is visible at the bottom right of the error box.

Damos nuevamente clic en forward y veremos que el sitio web de igual forma, nos arroja un error por credenciales incorrectas.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite 'Proxy' tab, a request to 'http://www.mvp-access.com:80' is displayed. The request details show a GET /foro/login_user.asp?returnURL= HTTP/1.1 with various headers and a cookie. The 'Inspector' tab shows the request attributes, query parameters, body parameters, cookies, and headers. In the browser window, a login page titled 'Conectado al foro' is shown. The page has a red header '** NORMAS DEL FORO **'. A yellow box contains an error message: 'El nombre de usuario o contraseña es incorrecta. Por favor, inténtelo de nuevo.' Below the error message, there is a form with fields for 'Nombre de usuario' (charlyfuentes) and 'Contraseña'. There are also checkboxes for 'Mantenerme conectado en este ordenador', 'Añademe a la lista de usuarios', and 'Estoy de acuerdo con las Reglas y normas del foro'. At the bottom of the browser window, there are 'Conectado al foro' and 'Reset Form' buttons.

Realizamos nuevamente el proceso, solo que, en esta ocasión, cambiamos la contraseña de “GiDAYLEE0qYxuAVuwhAU” a “GiDAYLEE0qYxuAVuwhAUcharly” y en nombre de usuario lo mantenemos sin ningún cambio, paso siguiente, damos clic en forward.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The browser window displays a login page titled "Conectado al foro" with the URL "mvp-access.com/foro/login_user.asp?returnURL=** NORMAS DEL FORO **". The page contains fields for "Nombre de usuario" (charlyfu) and "Contraseña" (GiDAYLEE0qYxuAVuwhAUcharly), and checkboxes for "Mantenerme conectado en este ordenador" and "Añademe a la lista de usuarios". Below the form are buttons for "Conectado al foro" and "Reset Form".

Burp Suite Proxy Tab (Left):

```

POST /foro/login_user.asp HTTP/1.1
Host: www.mvp-access.com
Content-Length: 198
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.mvp-access.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/112.0.5618.50 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://www.mvp-access.com/foro/login_user.asp?returnURL=
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9
Cookie: ASPSESSIONIDCDBTCQCB=BFPPODJBFODMKKKKPHLCLJ; wft10f1D=;
wft10MobileView=; wft10sl1D=; wft10Visite=; wft10sID=;
S1B=g13B331bce9a77fc12c5f3e5cce12B935185;
Connection: close
Accept: */*;q=0.8,application/signed-exchange;v=b3;q=0.7
MemberName=733fadzzd919z=charlyfu&P75e5D4B0DDC8DeCDE74eF5F00279872855DCA23E=GiDAYLEE0qYxuAVuwhAUcharly&AutoLogin=true&MS=true&terms=true&returnURL=login_user.asp?3FreturnURL%3D4338d677zefa4=733fadzzd919z

```

Burp Suite Inspector Tab (Left):

Selected text: GiDAYLEE0qYxuAVuwhAUcharly

Browser Window (Right):

Conectado al foro

Nombre de usuario: charlyfu ¿No está registrado?

Contraseña: GiDAYLEE0qYxuAVuwhAUcharly ¿Olvidó su contraseña?

Mantenerme conectado en este ordenador (requiere cookies) No Sí

Añademe a la lista de usuarios No Sí

Estoy de acuerdo con las Reglas y normas del foro No Sí

Buttons: Conectado al foro, Reset Form

Como podemos observar en la siguiente pantalla, de igual forma que el ejemplo anterior, el sitio web nos arroja una alerta en la cual nos menciona que las contraseñas ingresadas son incorrectas, esto se debe a que se modificó la contraseña por una incorrecta desde la aplicación, y ha funcionado correctamente.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The Burp Suite proxy tab displays a captured request to 'http://www.mvp-access.com:80 [92.53.241.26]'. The request is a POST to '/foro/quick_search.asp?FID=0&SSL=True' with various headers and a long URL containing session and view parameters. The browser window shows a modal dialog from 'Conectado al foro' with the message: 'www.mvp-access.com dice El nombre de usuario o contraseña es incorrecta. Por favor, inténtelo de nuevo.' (The user name or password is incorrect. Please try again.) An 'Aceptar' (Accept) button is visible at the bottom right of the dialog. The status bar at the bottom of the browser window shows 'Esperando www.mvp-access.com...'.

Damos nuevamente clic en forward y de igual forma que en el ejemplo anterior, veremos que el sitio web, nos arroja un error por credenciales incorrectas.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the Burp Suite proxy tab, there is a captured request to 'http://www.mvp-access.com:80 [92.53.241.26]'. The request details show a POST to '/foro/login_user.asp' with various headers and parameters. The browser window shows a login page titled 'Conectado al foro' with a red error message: 'El nombre de usuario o contraseña es incorrecta. Por favor, inténtelo de nuevo.' Below the error message, there is a form with fields for 'Nombre de usuario' (charlyfu) and 'Contraseña'. There are also checkboxes for 'Mantenerme conectado en este ordenador (requiere cookies)', 'Añademe a la lista de usuarios', and 'Estoy de acuerdo con las Reglas y normas del foro'. At the bottom of the browser window, it says 'Esperando www.mvp-access.com...'.

Para nuestro último ataque, Realizamos nuevamente el proceso, solo que, en esta ocasión, cambiamos las credenciales por otra cuenta registrada, cambios el nombre de usuario “charlyfu” por “albertofu” y en contraseña de “GiDAYLEE0qYxuAVuwhAU” por “Jesica hernandez”, paso siguiente, damos clic en forward.

En la contraseña se encuentra un espacio, la aplicación interpreta este espacio por el signo “+” por esta causa, la contraseña se muestra en la aplicación como “Jesica+hernandez”

The screenshot displays the Burp Suite interface and a web browser side-by-side. On the left, the Proxy tab shows a captured POST request to `/foro/login_user.asp`. The 'Selected text' pane highlights the password field with the value `'jesica+hernandez'`. The 'Decoded from' dropdown is set to 'URL encoding'. On the right, a browser window titled 'Conectado al foro' shows the login page. The password field contains the decoded value `'jesica+hernandez'`.

```

1 POST /foro/login_user.asp HTTP/1.1
2 Host: www.mvp-access.com
3 Content-Length: 198
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://www.mvp-access.com
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
9 like Gecko) Chrome/112.0.5615.50 Safari/537.36
9 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/
e/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
10 Referer: http://www.mvp-access.com/foro/login_user.asp?returnURL=
11 Accept-Encoding: gzip, deflate
12 Accept-Language: es-419,es;q=0.9
13 Cookie: ASPSESSIONIDCDTCOCB=BBFPODJBFDODMKMKKMPHLCLJ; vfl0fID=
vfl0MobileView=; vfl0sLID=; vfl0Visit=; vfl0sId=
SID=913B3384b1e5c79cf3f62660d41402060105
14 Connection: close
15
16 MemberName=e54069012bb494+albertofu&PDB8F2C41C0858109C091371622CE3F9AD3163170=
jesica+hernandez&AutoLogin=true&NS=true&terms=true&returnURL=
login_user.asp?returnURL=3D&10246433fdcf=e54069012bb494

```

Como podemos observar en la siguiente pantalla, después de dar forward con las credenciales cambiadas, el sitio web la acepta de forma correcta y permite el acceso dando el inicio de sesión.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. In the 'Intercept' section, a request to 'http://www.mvp-access.com:80' is displayed. The request details show a GET request for '/foro/quick_search.asp?FID=0&SSL=True' with various headers and parameters. The 'Raw' tab shows the full request string. To the right, a browser window titled 'Conectado al foro' displays a forum page with the title '** NORMAS DEL FORO **'. The user profile area shows 'Cerrarse [albertofu]' with a red box highlighting it. Below the profile, a message says 'Acceso correcto' and 'Acceso correcto correcto, por favor espere mieredirige al fiven al Foro'. The status bar at the bottom indicates '15°C' and the date '08/10/2023'.

En la siguiente pantalla se puede observar que se accedió al sitio web perfectamente con las credenciales enviadas de albertofu en lugar de charlyfu que se escribieron en el navegador web.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. The browser displays the 'Foro de Access y VBA' forum homepage at <http://www.mvp-access.com/foro/>. The page title is '** NORMAS DEL FORO **'. The browser status bar indicates it's not secure and shows the URL <http://www.mvp-access.com/foro/forums.html>.

Burp Suite Proxy Tab:

```

1 GET /foro/quick_search.asp?FID=0&SSL=False HTTP/1.1
Host: www.mvp-access.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 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://www.mvp-access.com/foro/forums.html
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9
Cookie: ASPSESSIONIDCDTCQCB=BF7F0D4BFDMMKMKMMPHLCLJ; vvt10t0ID=; vvt10MobileView=; vvt10sID=SID=913823304b3e9cf5cfc3f6z6668df41482D60185; vvt10sLID=NS+0tUID=albertofu2DD1564D5ECVCDDB77n2D3948; vvt10lVisit=Lv=2033CD101ZD09+033A3BN3AO1
Connection: close
11
12

```

Burp Suite Intercept Tab:

Request details for the captured session:

```

1 GET /foro/quick_search.asp?FID=0&SSL=False HTTP/1.1
Host: www.mvp-access.com
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 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://www.mvp-access.com/foro/forums.html
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9
Cookie: ASPSESSIONIDCDTCQCB=BF7F0D4BFDMMKMKMMPHLCLJ; vvt10t0ID=; vvt10MobileView=; vvt10sID=SID=913823304b3e9cf5cfc3f6z6668df41482D60185; vvt10sLID=NS+0tUID=albertofu2DD1564D5ECVCDDB77n2D3948; vvt10lVisit=Lv=2033CD101ZD09+033A3BN3AO1
Connection: close
11
12

```

Burp Suite Inspector Tab:

Request attributes, query parameters, body parameters, cookies, and headers are listed.

Burp Suite Search Bar:

Search results: 0 matches

Browser Window:

The browser displays the forum homepage with the title 'Foro de Access y VBA'. It shows sections like 'Avisos Importantes', 'Foro', 'Access y VBA', 'Relacionado con Access', and 'Profesionales en este Foro'. The 'Avisos Importantes' section includes topics like 'Avisos de interés general' and 'Avisos importantes del Foro de Access y VBA'. The 'Foro' section lists various threads with their titles, post counts, and last messages. The 'Access y VBA' section has a large number of posts (11584). The 'Relacionado con Access' section includes links to 'Curso de Access y VBA' and 'Enlaces a páginas'. The 'Profesionales en este Foro' section includes a link to 'Para Empresas: Contrate aquí Profesionales'.

Conclusión

En esta actividad aprendí que la vulnerabilidad Cross Site Scripting, mejor conocida como XSS, se trata de un tipo de ataque que aprovecha fallas de seguridad en sitios web y que permite a los atacantes implantar scripts maliciosos en un sitio web legítimo para ejecutar un script en el navegador de un usuario que visita dicho sitio y afectarlo, ya sea robando credenciales, redirigiendo al usuario a otro sitio malicioso, o para realizar defacement en un sitio web. Otra cosa importante que aprendí fue que, si un sitio web contiene esta vulnerabilidad, un atacante puede realizar diversos tipos de ataques basándose en la confianza que inspira la plataforma en el usuario, desde redirigir a otro sitio para robar información mediante phishing, hasta hacer que se descargue alguna amenaza y se ejecute en el sistema, ahora me doy cuenta que en última instancia, un Cross-site Scripting puede volver peligroso a un sitio legítimo para sus usuarios y por lo mismo es esencial prevenir este tipo de ataques para proteger la información, la privacidad y la reputación de una organización. También aprendí que hay varias formas de intentar minimizar los ataques XSS, pero los más fáciles son, mantener actualizado el software al máximo posible, desde plugins de nuestro servidor hasta los navegadores del cliente, y siempre que sea posible, lo ideal sería mantener el servidor detrás de un WAF (firewall para aplicaciones web).

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

https://github.com/charlyfu/Auditoria_informatica

Referencias

Qué es un ataque de XSS o Cross-Site Scripting. (2021, September 28).

<https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/>

Comprendiendo la vulnerabilidad XSS (Cross-site Scripting) en sitios web. (2015, April 29).

<https://www.welivesecurity.com/la-es/2015/04/29/vulnerabilidad-xss-cross-site-scripting-sitios-web/>

Gómez, P. (2022). Qué es un ataque XSS o Cross Site Scripting. ICM.

<https://www.icm.es/2022/05/11/cross-site-scripting-ataque-xss/>

De Zúñiga, F. G. (2023). Ataques XSS: qué son y cómo evitarlos. Blog De arsys.es.

<https://www.arsys.es/blog/ataques-xss-que-son-y-como-evitarlos>

Preguntas frecuentes | AWS WAF | Amazon Web Services (AWS). (n.d.). Amazon Web Services, Inc.

<https://aws.amazon.com/es/waf/faq/>