

Ingeniería en Desarrollo de Software

Actividad: Número 3.

Nombre de la Actividad: Cross Site Scripting (XSS).

Nombre del Curso: Auditoria informática.

Tutor: Jessica Hernández Romero.

Alumno: Omar Juárez Carmona.

Fecha: 11 – Octubre – 2023.

INDICE

Contextualización y actividad.....	3
Introducción.....	4
Descripción.....	5
Justificación.....	6
ETAPA 1.....	7
- Descripción del sitio web.....	7
- Ataque al sitio web.....	8
ETAPA 2.....	11
- Ataque al sitio.....	11
ETAPA 3.....	19
- Ataque al sitio web.....	19
- Conclusión.....	26
- Referencias y link.....	27

CONTEXTUALIZACION Y ACTIVIDAD

Contextualización:

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 BurpSuite, modificar la información para comprobar si se puede iniciar sesión o no.

Actividad:

Utilizando el sitio web que se subió a Internet en la primera actividad, y el programa utilizado en la Actividad 2, trabajar con la vulnerabilidad Cross Site Scripting (XSS). Así, con la ayuda de Burp Suite, captar las credenciales que se ingresen cuando se inicie sesión, y comprobar si se puede modificar.

INTRODUCCION

En esta actividad numero 3 o proyecto final, estaremos tratando y estudiando conocimientos relacionados a nuestra materia de auditoria informática, temas que ya hemos venido aprendiendo y estudiando desde actividades pasadas, pero en esta unidad-actividad final nos enfocaremos principalmente a el estudio de Cross-Site scripting o XSS, también conocido como inyección de scripts entre sitios, es una vulnerabilidad de seguridad en aplicaciones web que permite a los atacantes ejecutar código malicioso en los navegadores de los usuarios aprovechando vulnerabilidades en las páginas web que estos visitan. Esta vulnerabilidad se aprovecha de la falta de validación y filtrado de datos de entrada por parte de las aplicaciones web, lo que permite que los atacantes inserten código JavaScript u otro código ejecutable en las webs visitadas por otros usuarios. El concepto detrás del XSS es que el atacante puede engañar a la aplicación web para que muestre contenido inseguro a los usuarios, haciéndoles creer que proviene de la página web legítima.

Trabajaremos con un sitio web no seguro (sitio web que utilizamos en nuestra actividad número 1 de esta materia) para así posteriormente ejecutar nuestra herramienta de trabajo de BurpSuite, y analizar o más bien rastrear los datos con los que iniciaremos en la web no segura.

Modificaremos datos de usuario en el correo electrónico como así mismo las contraseñas dentro de la herramienta de trabajo de BurpSuite, para que podamos visualizar los datos ingresados y de igual manera poder visualizar las modificaciones que haremos con estos datos de usuario ingresados en el sitio web no seguro.

Sin más preámbulo, comenzaremos con la elaboración de esta actividad final y aprenderemos a como poder visualizar la vulnerabilidad Cross-Site scripting o XSS de nuestro sitio web no seguro.

DESCRIPCION

Acá describiremos lo que en realidad nos pide la contextualización de esta actividad final y para ello debemos de saber qué hace mención sobre una empresa de software y esta 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 BurpSuite, modificar la información para comprobar si se puede iniciar sesión o no.

Antes de ello, debemos de conocer el significado de Cross Site Scripting (XSS).

El Cross-Site Scripting (XSS) es una vulnerabilidad de seguridad común en aplicaciones web que permite a los atacantes injectar y ejecutar código malicioso en las páginas web vistas por otros usuarios. Esta vulnerabilidad se da cuando una aplicación web no valida adecuadamente los datos de entrada proporcionados por los usuarios o presenta fugas, lo que permite que los atacantes inserten código JavaScript u otros tipos de código ejecutable en las webs visitadas por otros usuarios.

Ahora nos inclinaremos a utilizar la página web no segura mencionada en la actividad número 1, en donde a través de la herramienta de trabajo de Burp Suite, le haremos algunos hackeos a la información del usuario con la cual estamos ingresando a la plataforma web y así poder visualizar los cambios que le haremos directamente desde la herramienta de trabajo como el usuario y la contraseña con la cual estamos ingresando a dicha plataforma.

Sin más preámbulo, continuaremos con este maravilloso mundo de poder hackear información importante en un lugar web no seguro de la red.

Manos a la obra para poder iniciar a robar información confidencial.

JUSTIFICACION

El Cross-Site Scripting (XSS) es una vulnerabilidad de seguridad común en aplicaciones web que permite a los atacantes inyectar y ejecutar código malicioso en las páginas web vistas por otros usuarios. Esta vulnerabilidad se da cuando una aplicación web no valida adecuadamente los datos de entrada proporcionados por los usuarios o presenta fugas, lo que permite que los atacantes inserten código JavaScript u otros tipos de código ejecutable en las webs visitadas por otros usuarios.

Las ventajas de esta vulnerabilidad son para los atacantes, ya que les permite robar información personal, como contraseñas, datos bancarios y otra información confidencial. Además, también pueden utilizar esta vulnerabilidad para redirigir a los usuarios a sitios web maliciosos o para propagar malware.

Para evitar ataques XSS, es importante que las aplicaciones web validen adecuadamente los datos de entrada proporcionados por los usuarios y filtren o escapen adecuadamente los datos proporcionados por los usuarios en la URL u otros parámetros de la solicitud. También es importante que las aplicaciones web no almacenen datos de entrada no validados en la base de datos.

Hemos notado las ventajas más sobre salientes del por qué utilizar esta vulnerabilidad, principalmente para la persona atacante, ya que así se permite robar información personal de suma importancia y así poder hacer modificaciones en algún sistema o sitio web principalmente no seguro.

Por esta ventaja, muchos usuarios o personas que se dedican a hackear información, utilizan esta herramienta de trabajo.

ETAPA 1.

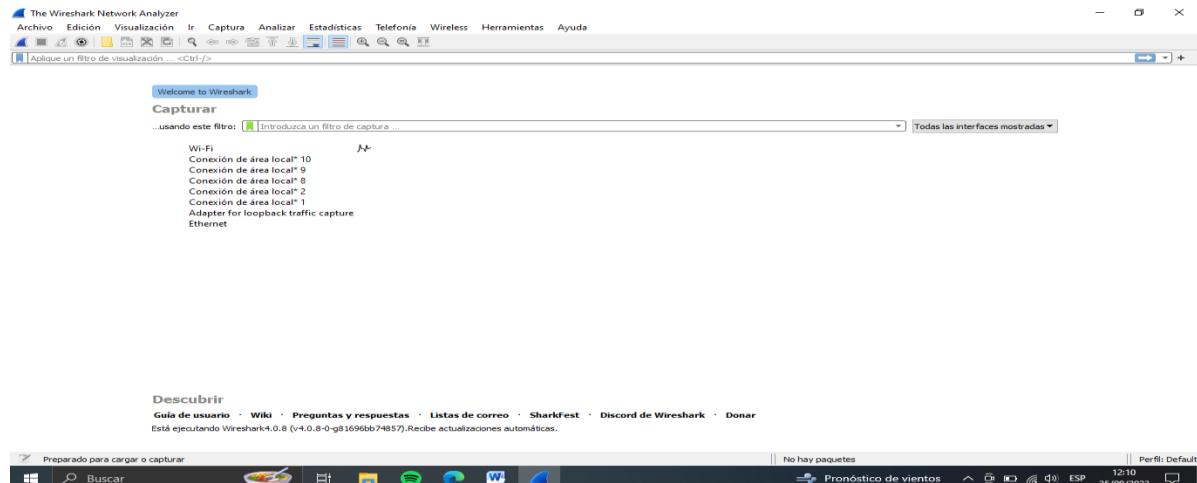
DESCRIPCION DEL SITIO WEB

Sitio web oficial llamado CELFI, donde el principal objetivo se refiere a Ministerio de Ciencia Tecnología Innovación Argentina, donde tiene vulnerabilidad y con una leyenda de modo no seguro del sitio web que es acá en donde haremos nuestra primera prueba utilizando la herramienta de trabajo de Wireshark.

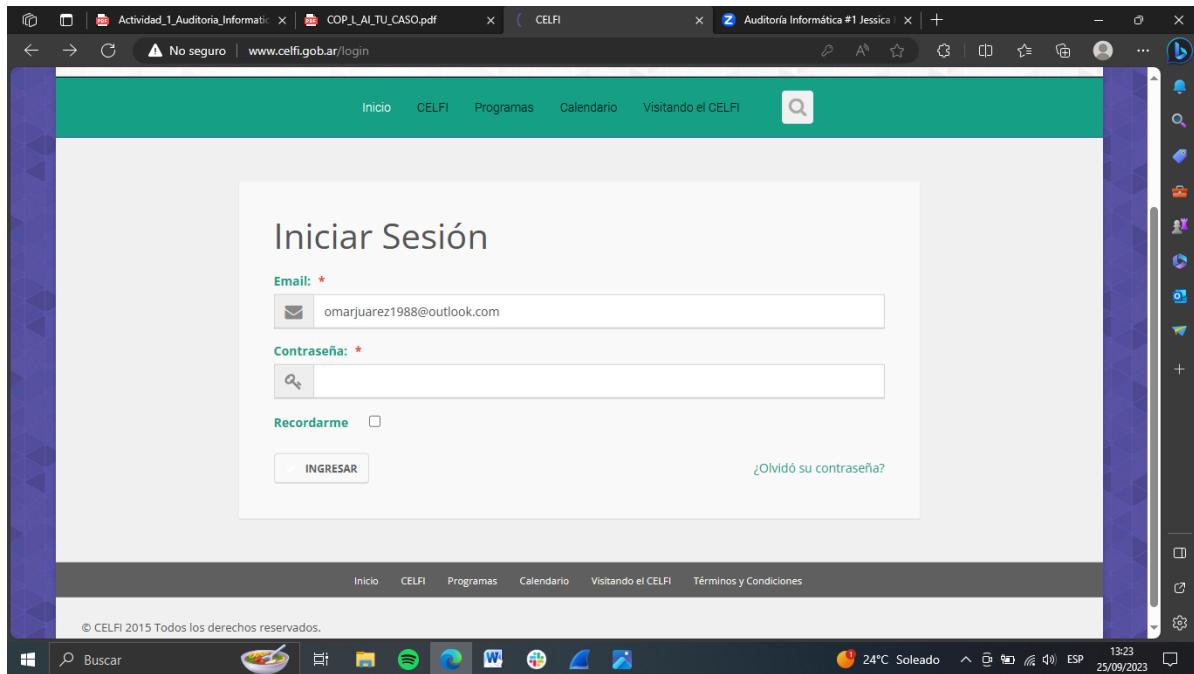
Daremos a detalle cómo se realiza el hacker, ya que el protocolo de transferencia de hipertexto es muy vulnerable, hoy en día las páginas que lo llegan a usar son demasiado vulnerables al ataque y robo de datos, para comprobar que se utilizó un analizador de paquetes llamado Wireshark. Nos introduciremos en una página web de http, para poder observar lo fácil que es extraer los datos del usuario. Cabe recalcar que esto funciona solo si el usuario al cual extraeremos sus datos, debe estar conectado a la misma red que nosotros, es decir que para poder extraer datos del usuario con un analizador de paquetes. Ambos, tanto el como yo debemos de estar conectado a la misma red.

ATAQUE AL SITIO WEB

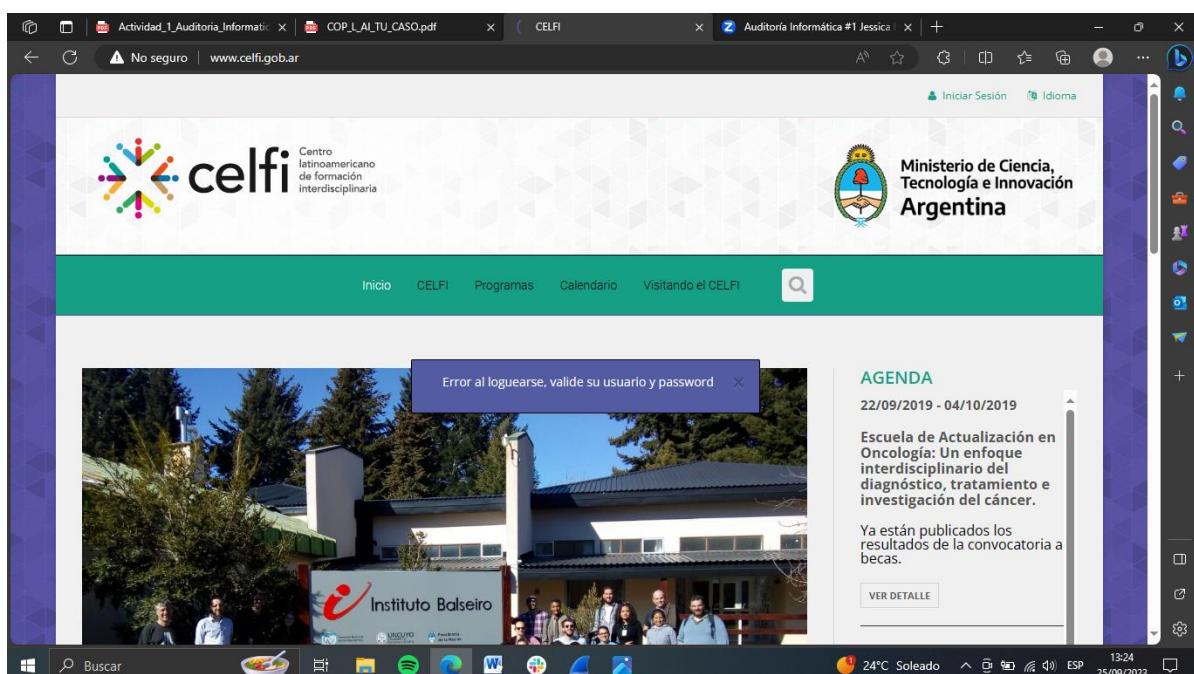
Página principal de herramienta de trabajo Wireshark.



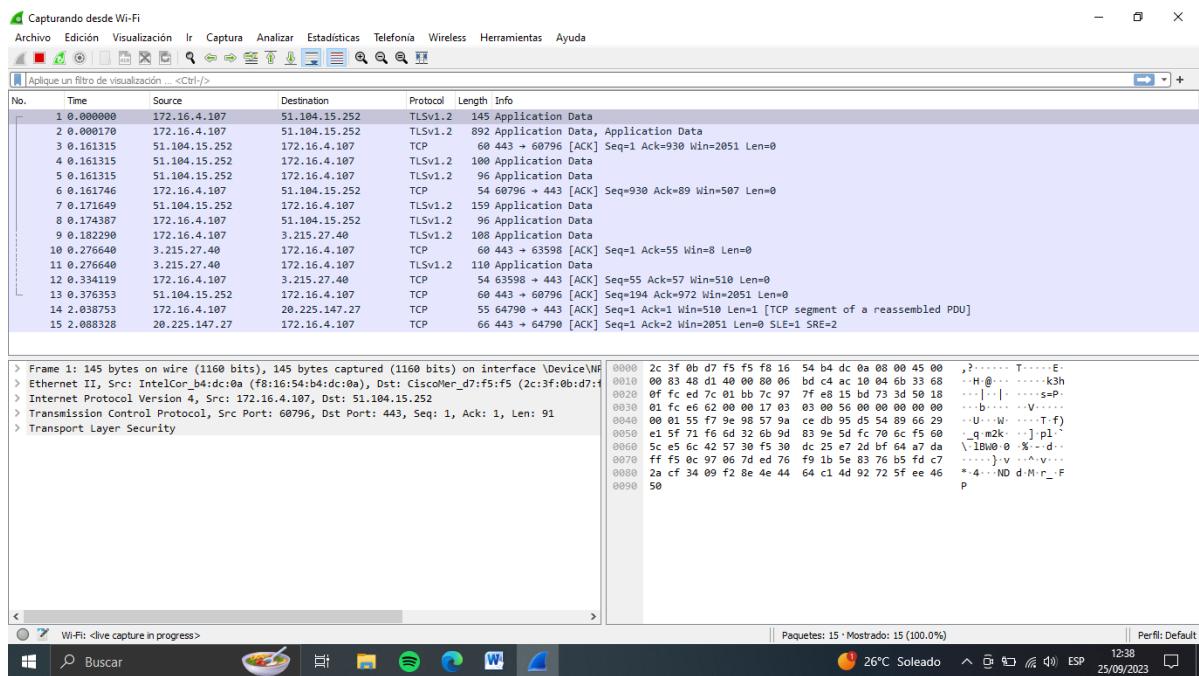
Página Celfi no segura paraloguearnos.



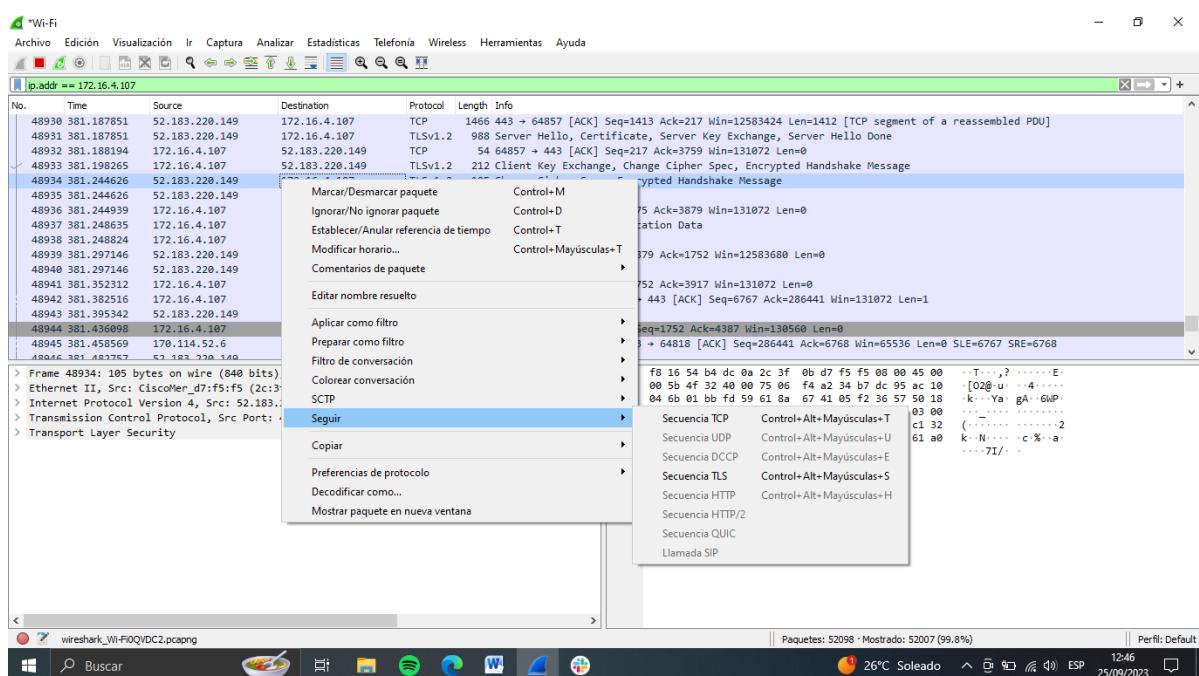
Página Celfilogueada con nuestro usuario y contraseña.



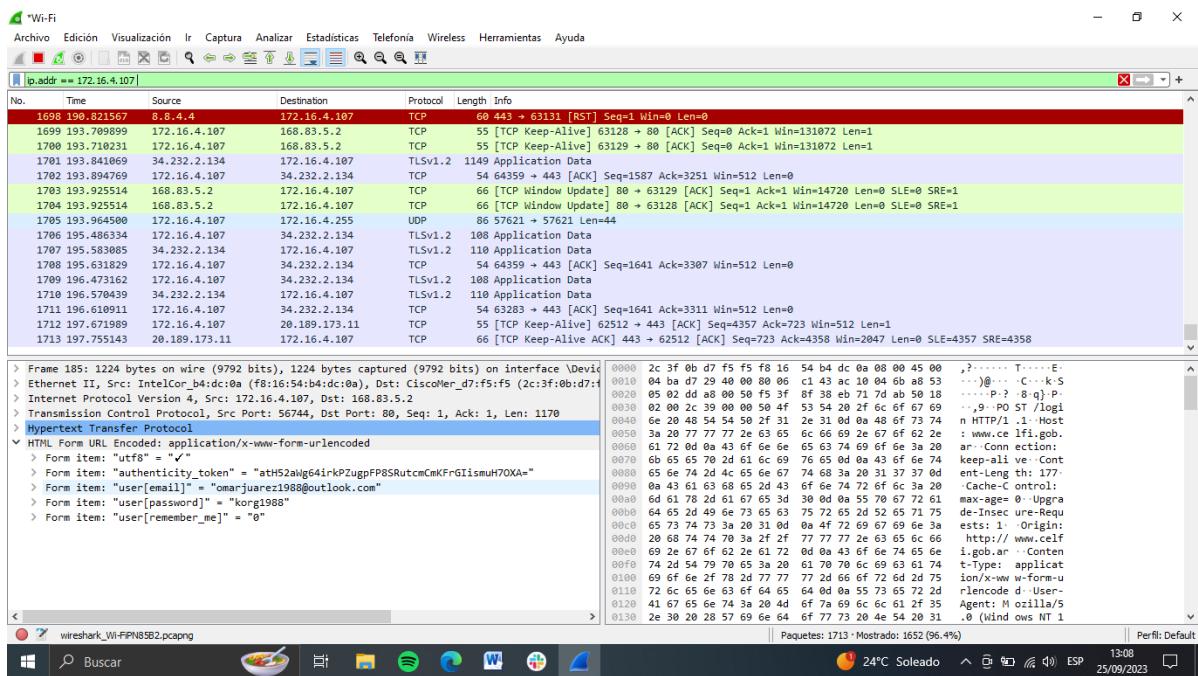
Comenzando a ejecutar nuestra herramienta de trabajo Wireshark modo wi-fi.



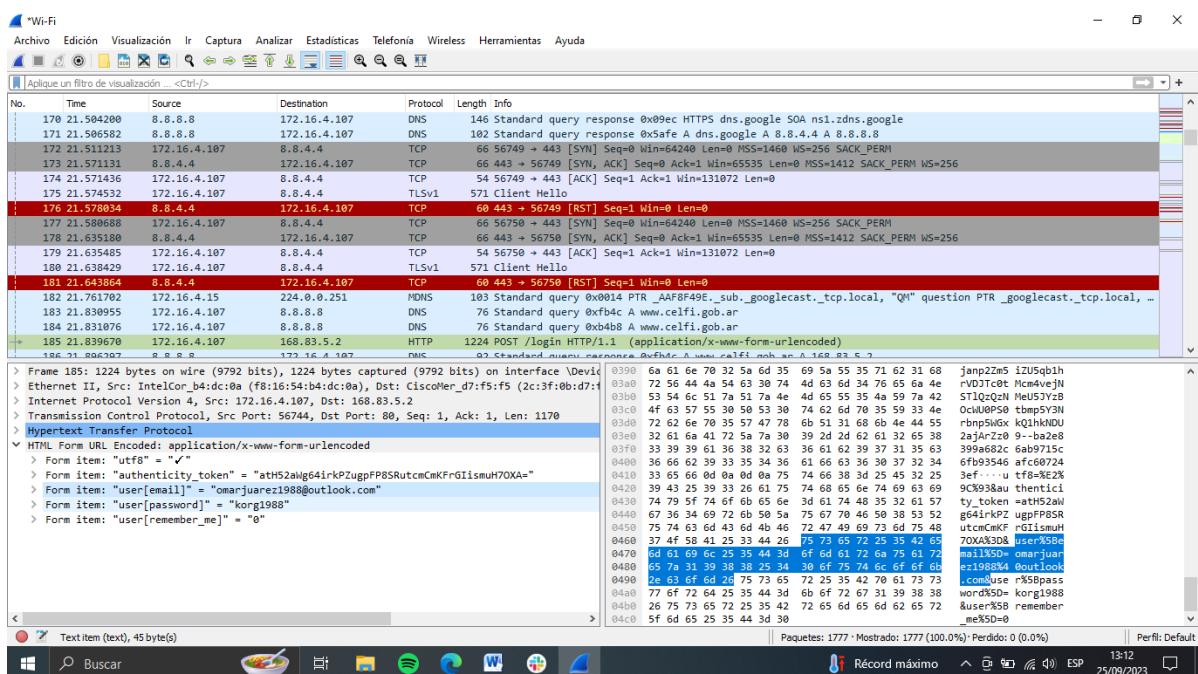
Utilizando comando ip.add == dirección IP para saber usuario y contraseña de usuario.



Resultado obtenido correctamente de usuario y contraseña con Wireshark.



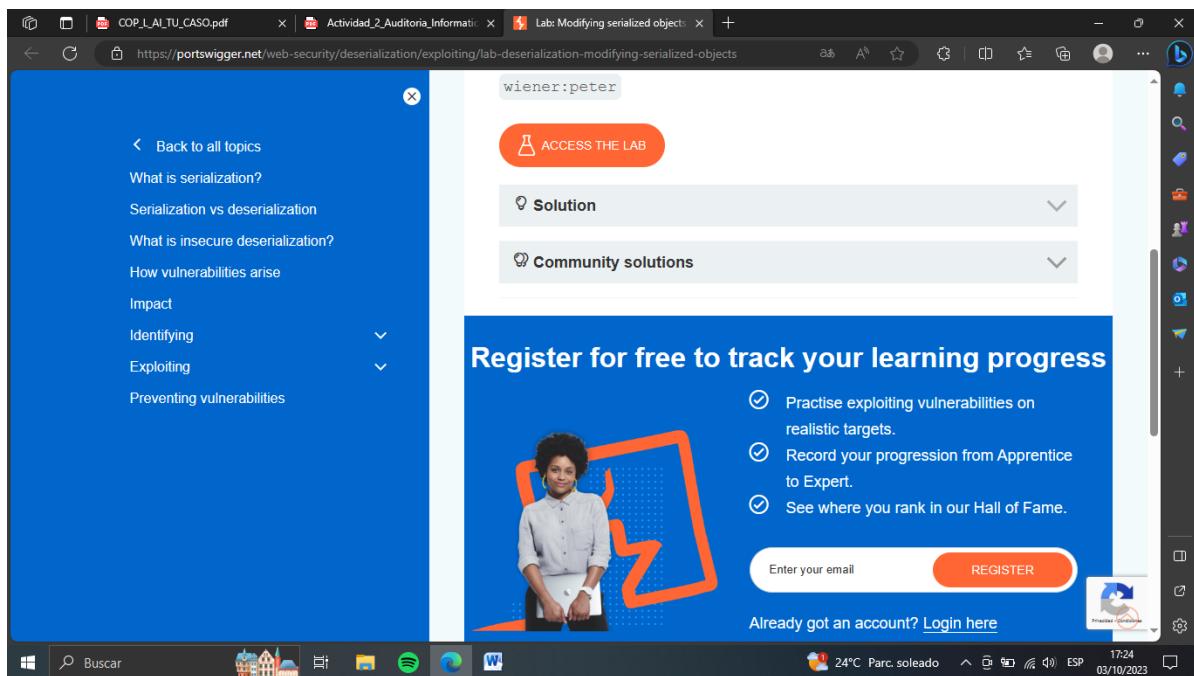
Resultados obtenidos correctamente al saber usuario y contraseña de página web.



ETAPA 2.

ATAQUE AL SITIO WEB

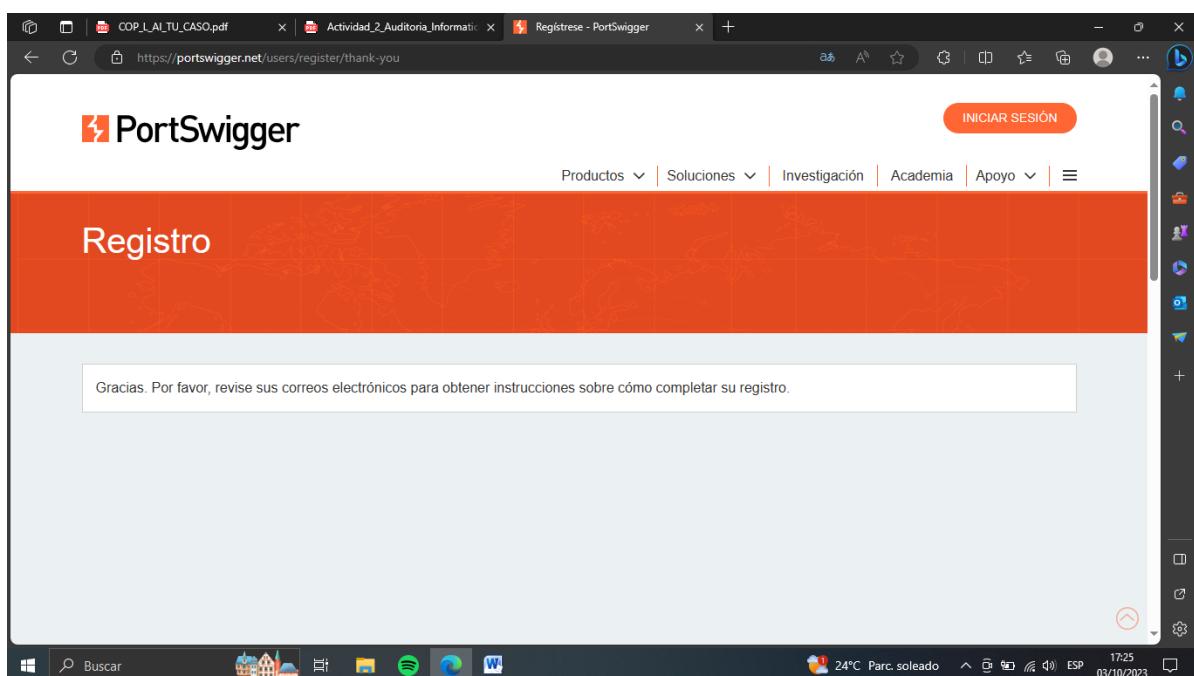
Acceso al laboratorio.



The screenshot shows a Microsoft Edge browser window with the following details:

- Address bar: <https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects>
- User info: wiener:peter
- Left sidebar:
 - Back to all topics
 - What is serialization?
 - Serialization vs deserialization
 - What is insecure deserialization?
 - How vulnerabilities arise
 - Impact
 - Identifying
 - Exploiting
 - Preventing vulnerabilities
- Top right: ACCESS THE LAB button
- Middle section:
 - Solution dropdown
 - Community solutions dropdown
- Banner: Register for free to track your learning progress
 - Practise exploiting vulnerabilities on realistic targets.
 - Record your progression from Apprentice to Expert.
 - See where you rank in our Hall of Fame.
- Buttons: Enter your email, REGISTER, Login here
- Bottom right: Provided by PortSwigger
- System tray: Windows 10 icons, 24°C, Parc. soleado, 17:24, 03/10/2023

Registro en PortSwigger.



The screenshot shows a Microsoft Edge browser window with the following details:

- Address bar: <https://portswigger.net/users/register/thank-you>
- PortSwigger logo
- Navigation menu: INICIAR SESIÓN, Productos, Soluciones, Investigación, Academia, Apoyo
- Main content: Registro
- Message: Gracias. Por favor, revise sus correos electrónicos para obtener instrucciones sobre cómo completar su registro.
- Bottom right: Provided by PortSwigger
- System tray: Windows 10 icons, 24°C, Parc. soleado, 17:25, 03/10/2023

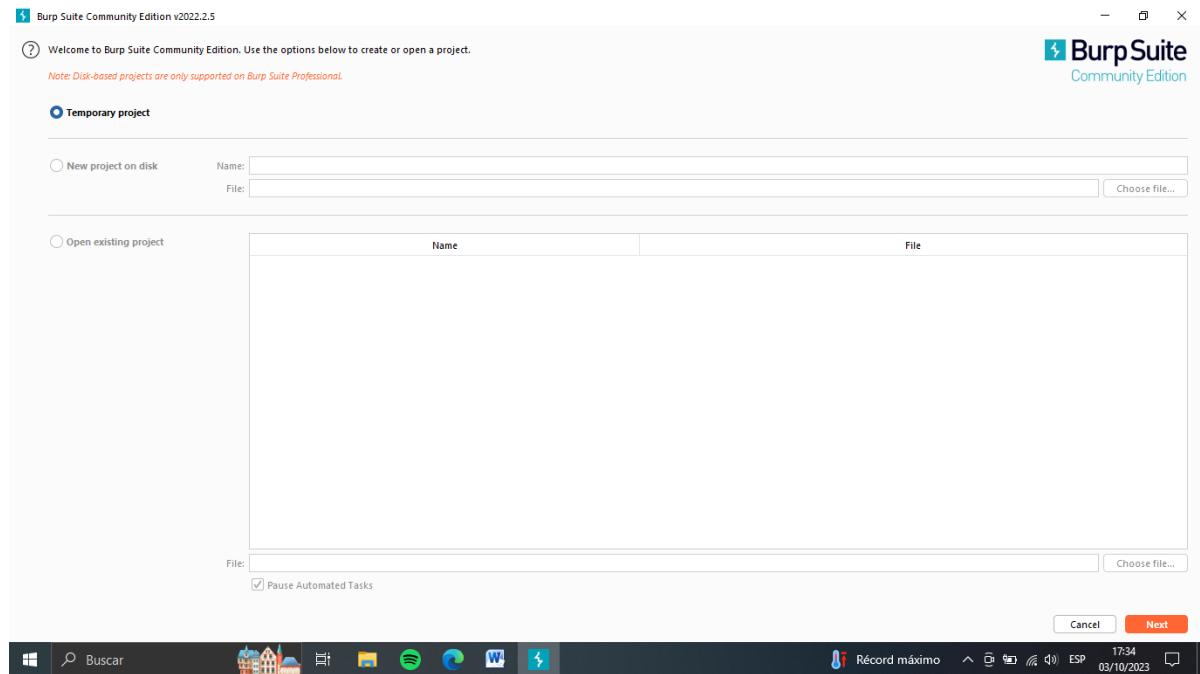
Registro con usuario en PortSwigger.

The screenshot shows a browser window with the URL <https://portswigger.net/users/register/complete?token=853a660a4e3fdad79706c6bac9eee15f0a2f87a756a47554105458a8...>. The page has an orange header with the word 'Registro'. Below it, a message says 'Por favor, introduzca sus datos para completar su registro.' There is a single input field labeled 'Nombre' containing 'Omar Juarez Carmona'. A green button labeled 'Registro' is below the input field. The browser's address bar shows the full URL. The taskbar at the bottom includes icons for various applications like Spotify and Microsoft Word, along with system status indicators like battery level and signal strength.

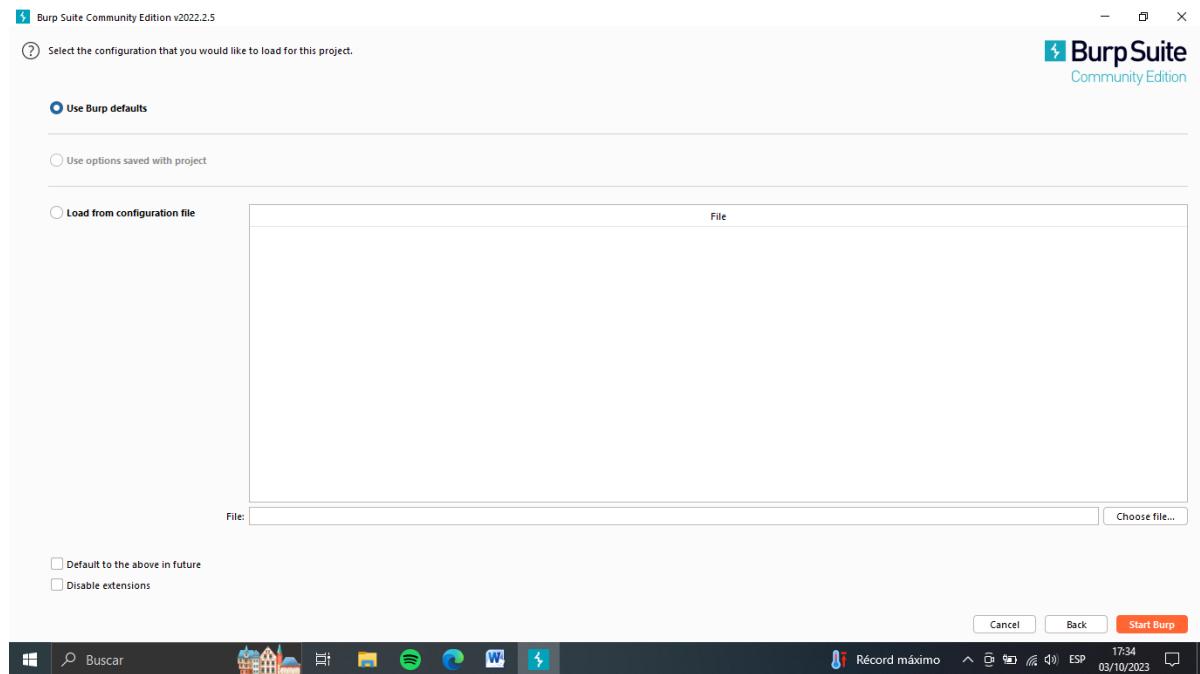
Registro con clave de parte de PortSwigger.

The screenshot shows a browser window with the URL <https://portswigger.net/users>. The page has an orange header with the word 'INICIAR SESIÓN'. Below it, a message says 'Introduzca su dirección de correo electrónico y contraseña para iniciar sesión.' There are two input fields: 'Dirección de correo electrónico' with the value 'juareztrucha12@gmail.com' and 'Contraseña' with a redacted value. Below the password field is a link 'Olvidó su contraseña?'. There is a checkbox 'Recordarme en este equipo' with a checked state. At the bottom are two buttons: a dark blue 'Inicia sesión' button and a grey 'Crear cuenta' button. The browser's address bar shows the full URL. The taskbar at the bottom includes icons for various applications like Spotify and Microsoft Word, along with system status indicators like battery level and signal strength. Below the main content, there is a small graphic of three people and the text 'Comunidad de eructos'.

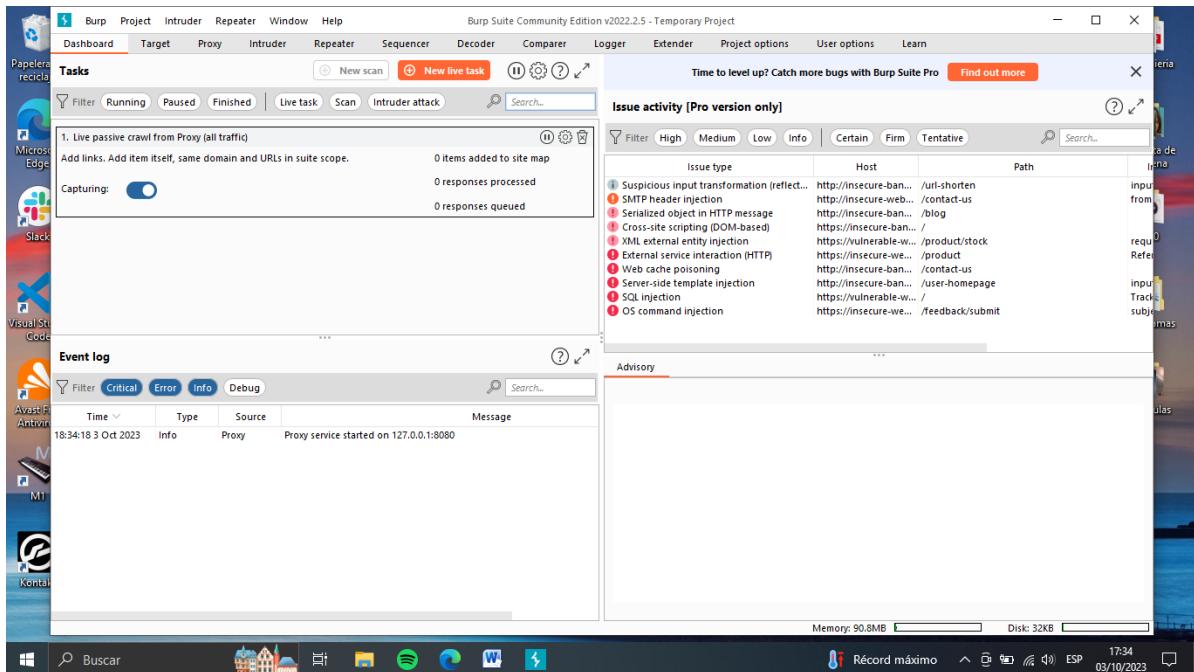
Accediendo a BurpSuite.



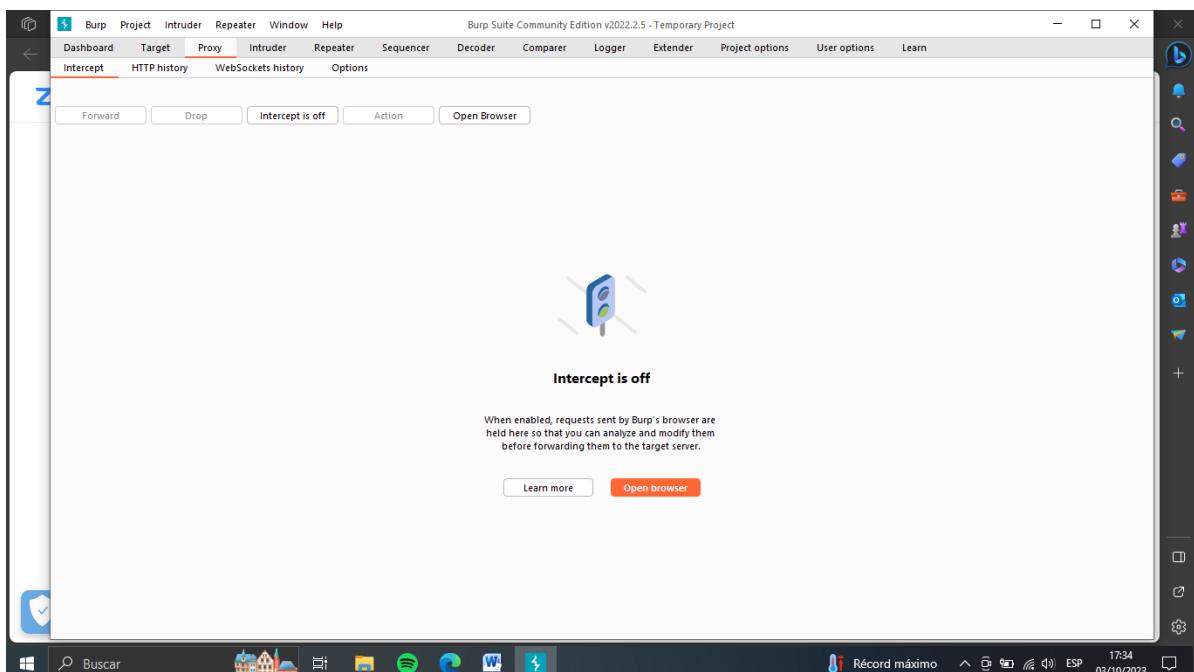
Accediendo a BurpSuite.



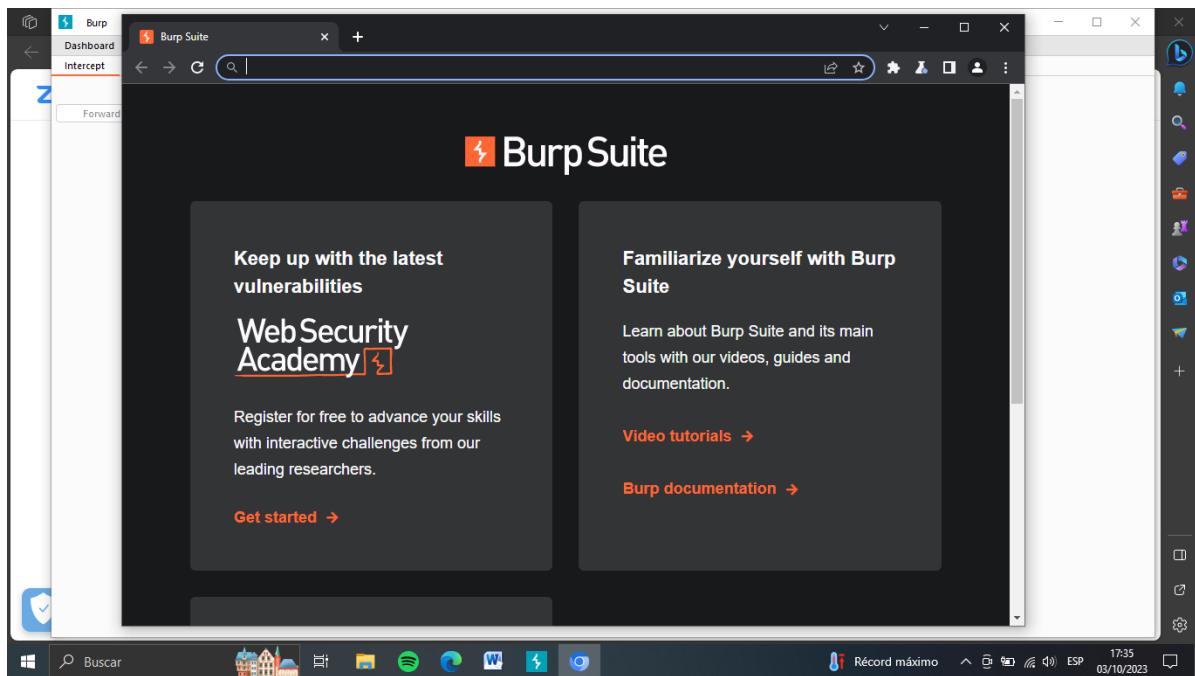
Página principal de BurpSuite.



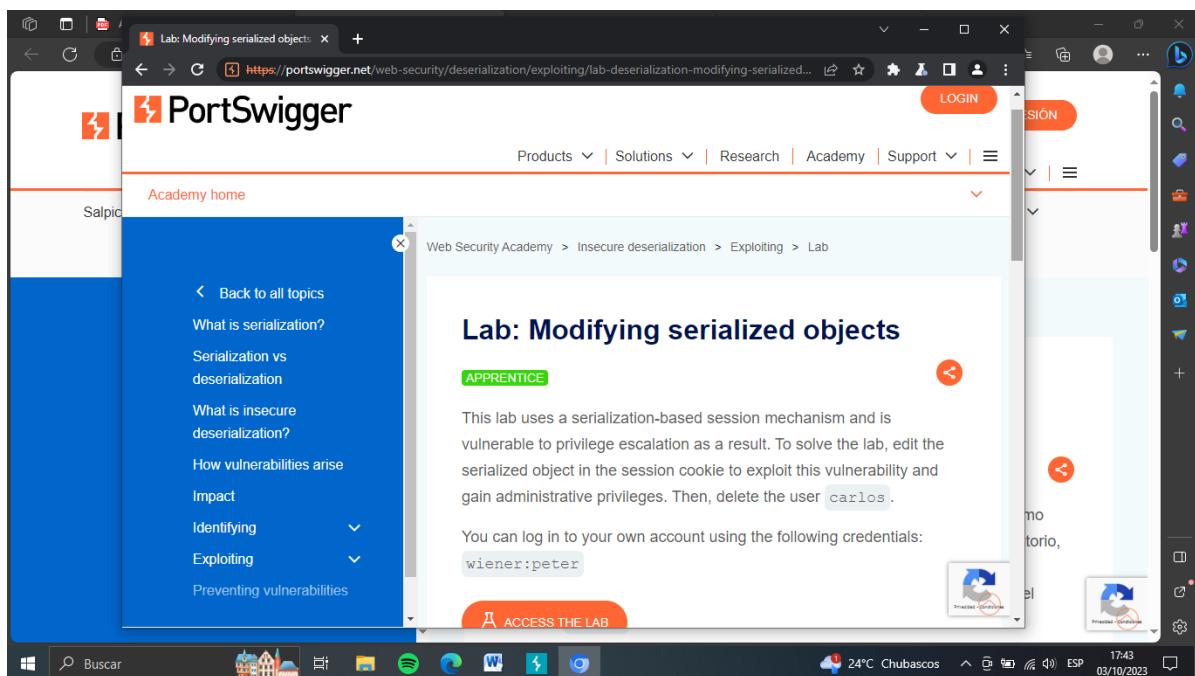
Accediendo al Proxy dentro de Burp Suite.



Corriendo el Browser de BurpSuite.



Link de PortSwigger.



Accediendo a cuenta de PortSwigger.

The screenshot shows the 'My Account' page of PortSwigger.net. At the top, there's a navigation bar with links for Products, Solutions, Research, Academy, Support, and a 'MY ACCOUNT' button. Below the navigation is a dark blue header bar with the text 'My Account'. On the left, there's a sidebar with options like Personal Details, Certifications, Subscriptions, and Order History. The main content area is titled 'Personal Details' and shows a profile for 'Omar' with the email 'omarjuarez1988@outlook.com' and a 'Change Password' link. To the right is a section for 'Account Address' which states 'No address associated with this account'. Below these sections is a 'Saved Cards' area with a placeholder 'Add new card'. The bottom of the screen shows a Windows taskbar with various icons and system status information.

Intentando ingresar en el Browser con wiener y Peter.

The screenshot shows a browser window with a redacted URL. The page displays a login form with the instruction 'Please enter your email address and password to log in.' It has fields for 'Email address' containing 'wiener' and 'Password' containing '.....'. There's a 'Forgot your password?' link and a 'Remember me on this computer' checkbox. Below the form are 'Log in' and 'Create account' buttons. The background features a large orange banner with the text 'Lab: Modifying serialized objects' and 'Login - PortSwigger'. The bottom of the screen shows a Windows taskbar with various icons and system status information.

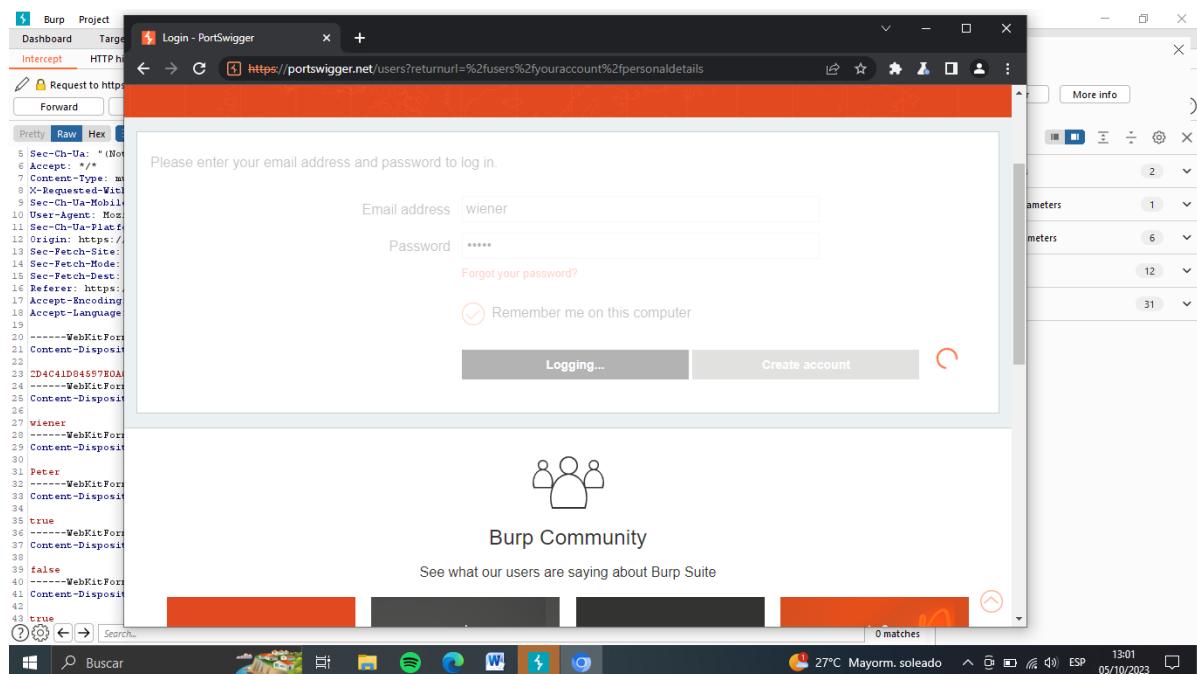
Código descrito al momento de ingresar donde arroja información de usuario y contraseña.

```

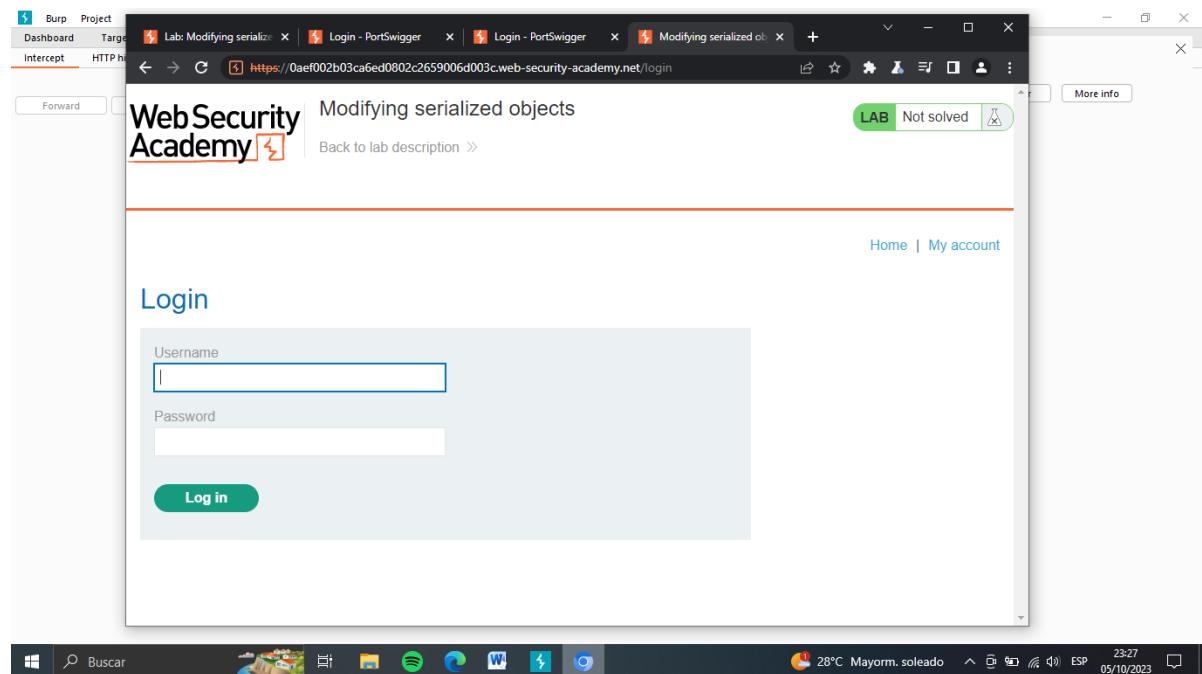
1 POST /users?returnUrl=%2Facademy%2Flab%2Flaunch%2Fad237c65112d5171d435fd674dbc3fe60b13777c9eef764ec7797b802%3Freferrer%3D%25cfweb-security%25cfde
2 Host: portswigger.net
3 Cookie: AWSALBAPP-0=_remove_; AWSALBAPP-2=_remove_; AWSALBAPP-3=_remove_; stg_traffic_source_priority=1;
4 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryH6KAJbPN5sdX6Cf
5 Sec-Ch-Ua: "Not(A BRAND);v=100"
6 Accept: */*
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryH6KAJbPN5sdX6Cf
8 X-Requested-With: XMLHttpRequest
9 Sec-Ch-Ua-Mobile: ?0
10 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
11 Sec-Ch-Ua-Platform: "Windows"
12 Origin: https://portswigger.net
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Dest: empty
16 Referer: https://portswigger.net/users?returnUrl=%2Facademy%2Flab%2Flaunch%2Fad237c65112d5171d435fd674dbc3fe60b13777c9eef764ec7797b802%3Freferrer%3D%25cfweb-security%25cfde
17 Accept-Encoding: gzip, deflate
18 Accept-Language: es-419,es;q=0.9
19
20 -----WebKitFormBoundaryH6KAJbPN5sdX6Cf
21 Content-Disposition: form-data; name="RequestVerificationToken"
22
23 62D115D56491AAAD01774C70E5C11FC171E5ADF3D3037CBE6C36A89728EDD08333BCC70347CECDB651CDB0C154794A49C7AEDD0C3DB4379C4516349ZFFB03
24 -----WebKitFormBoundaryH6KAJbPN5sdX6Cf
25 Content-Disposition: form-data; name="EmailAddress"
26
27 wiener
28
29 -----WebKitFormBoundaryH6KAJbPN5sdX6Cf
30
31 Peter
32 -----WebKitFormBoundaryH6KAJbPN5sdX6Cf
33 Content-Disposition: form-data; name="EmailAddress"
34
35 true
36 -----WebKitFormBoundaryH6KAJbPN5sdX6Cf
37 Content-Disposition: form-data; name="RememberMe"
38
39 false
40 -----WebKitFormBoundaryH6KAJbPN5sdX6Cf
41 Content-Disposition: form-data; name="RememberMe"
42
43 true

```

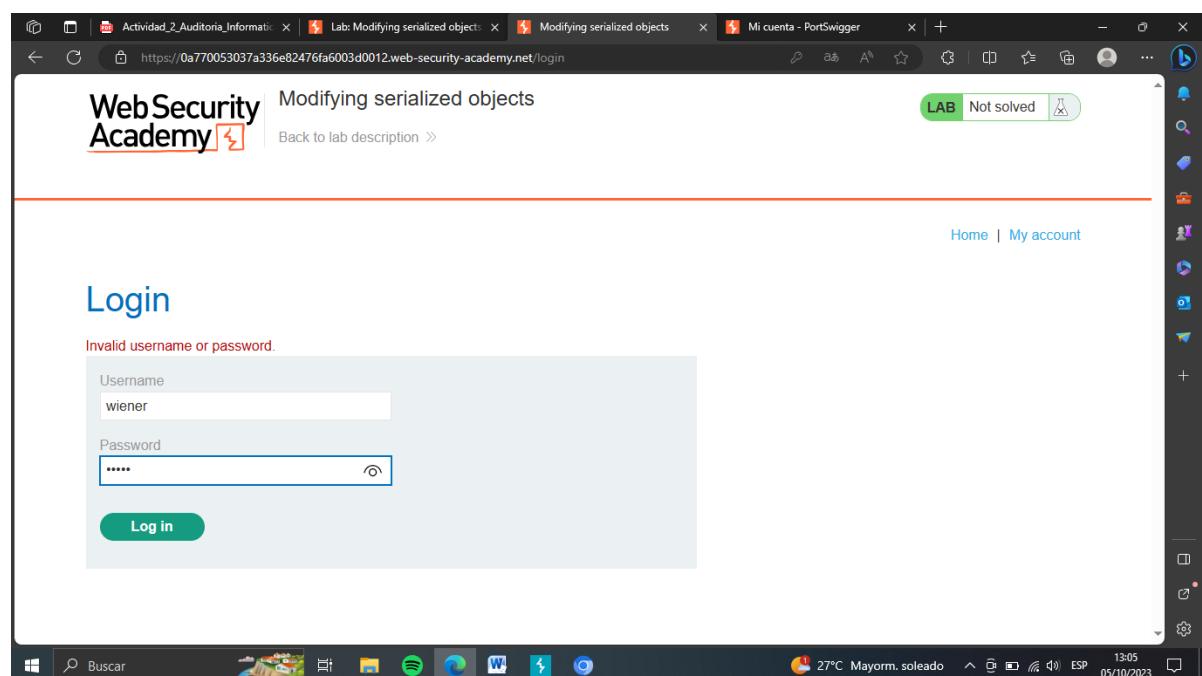
Cargando al tratar de iniciar sesión.



Accediendo a BurpSuite para iniciar sesión con wiener y Peter.



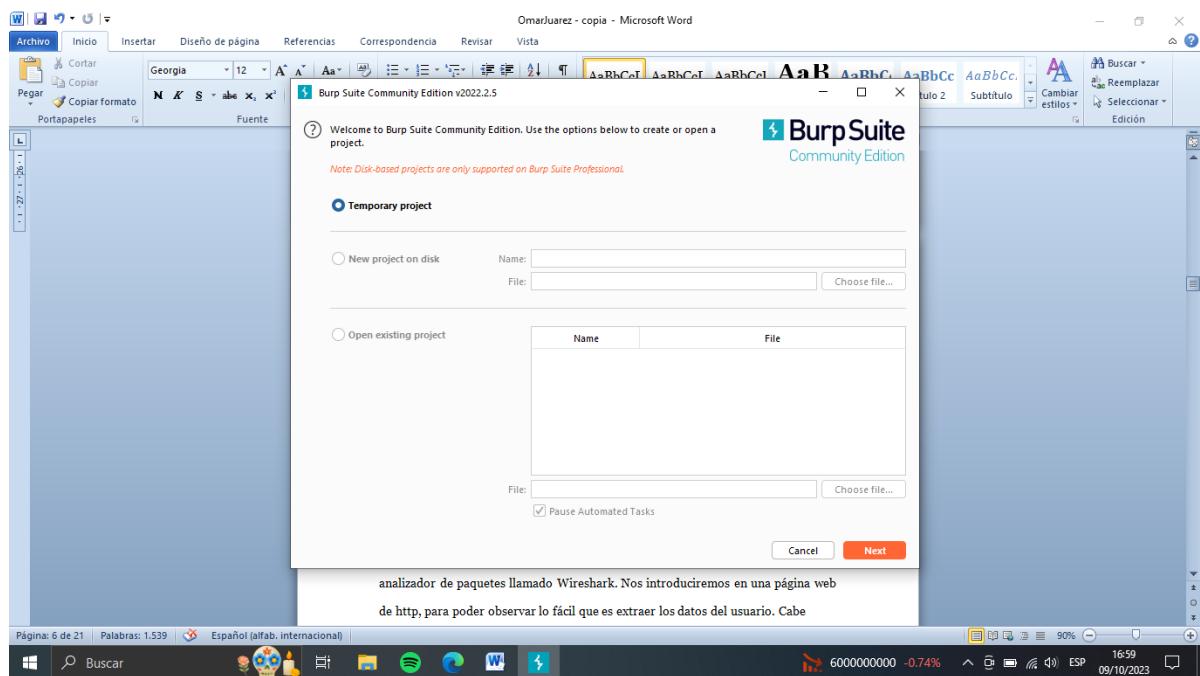
Login en BurpSuite.



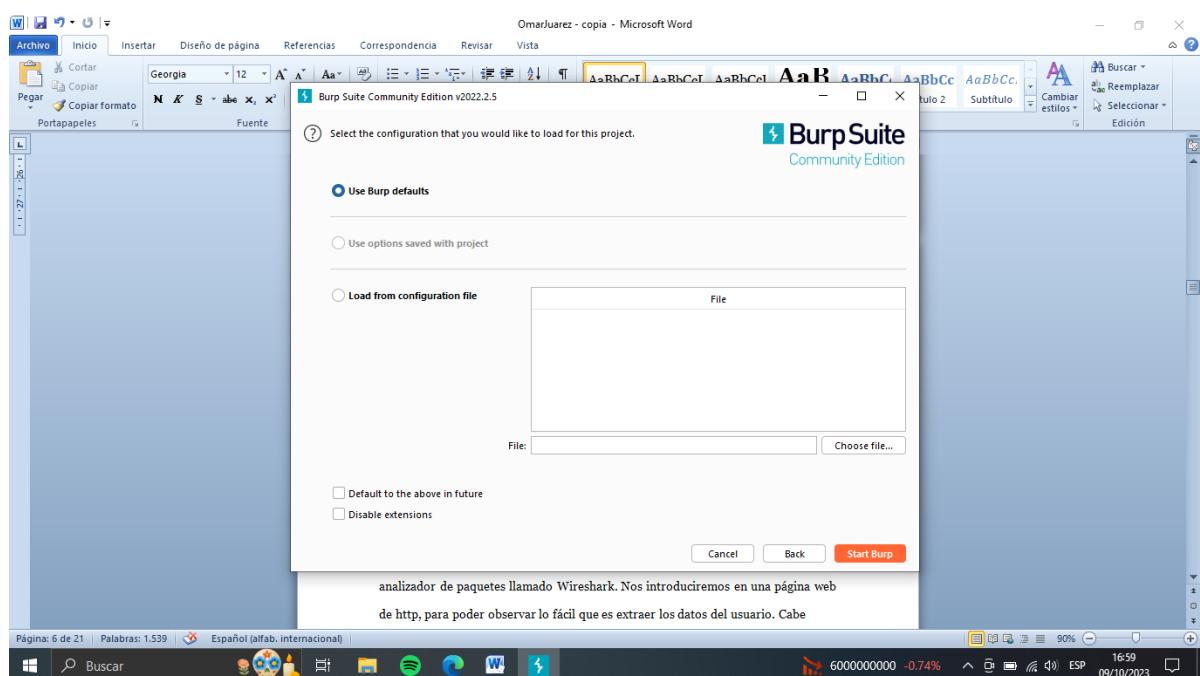
ETAPA 3.

ATAQUE AL SITIO WEB

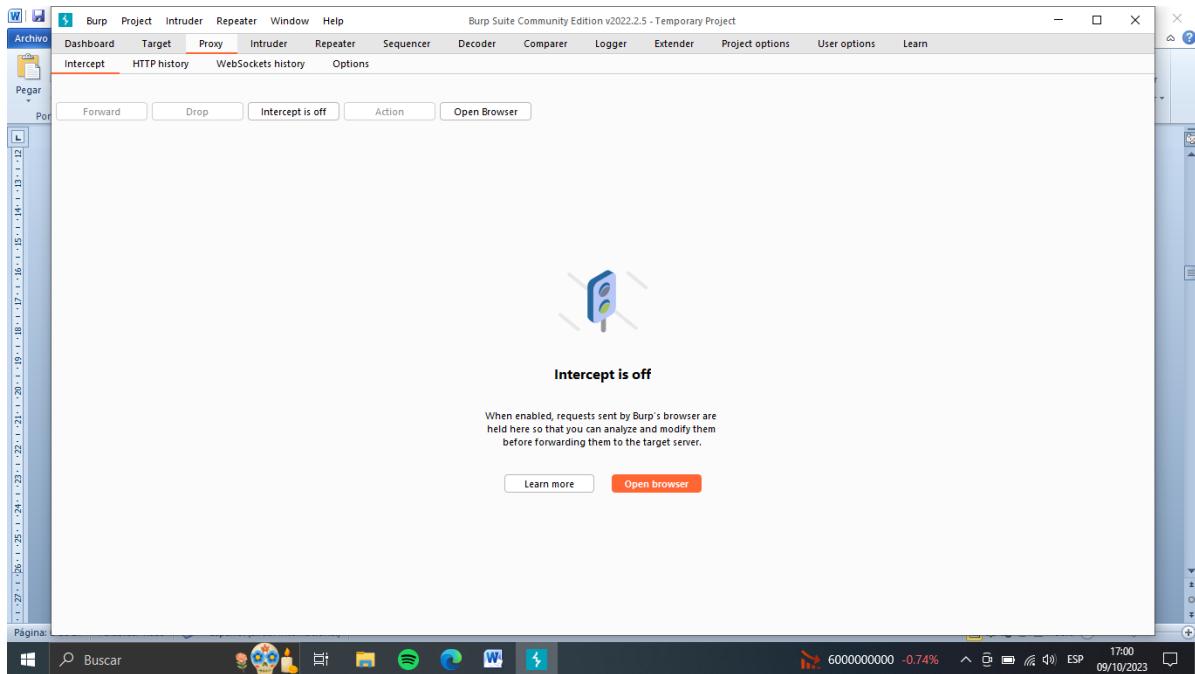
Creando nuevo proyecto en Burp Suite.



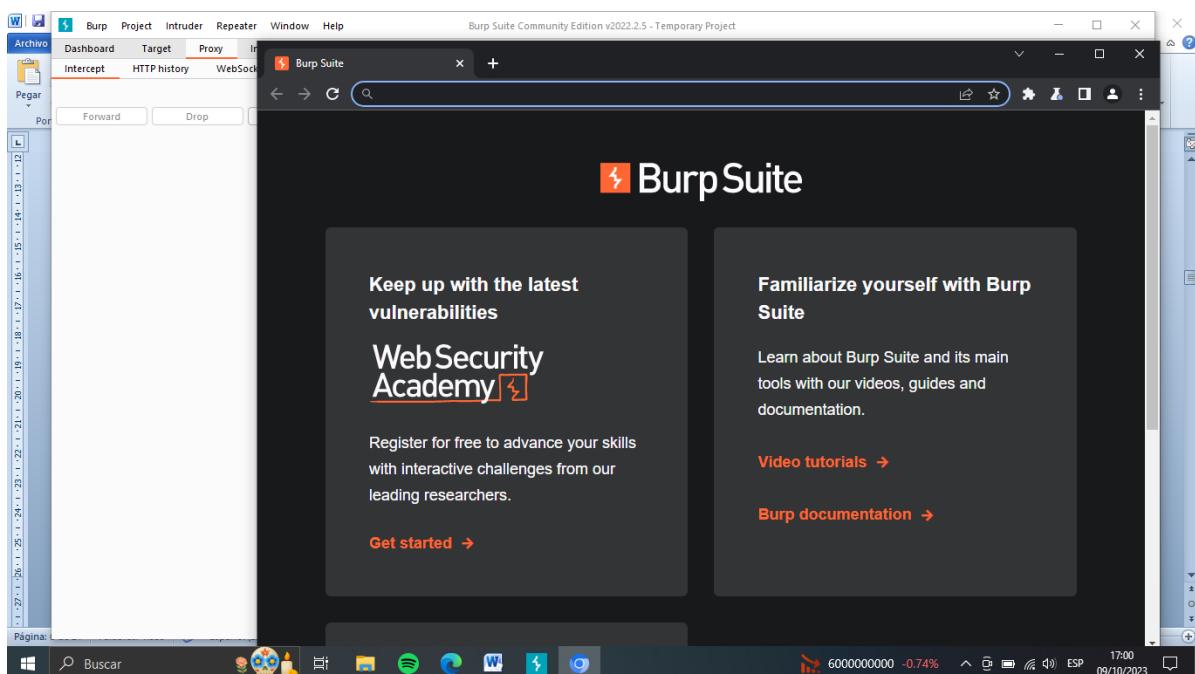
Creando nuevo proyecto en Burp Suite.



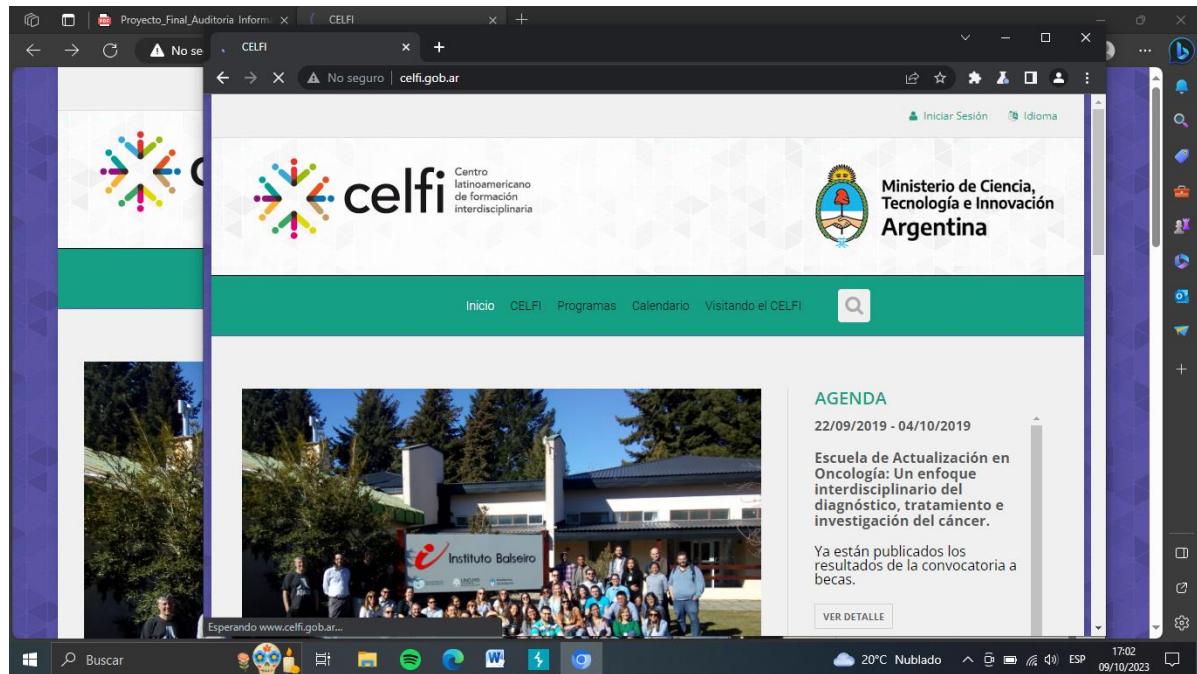
Página principal de Burp Suite en apartado Proxy.



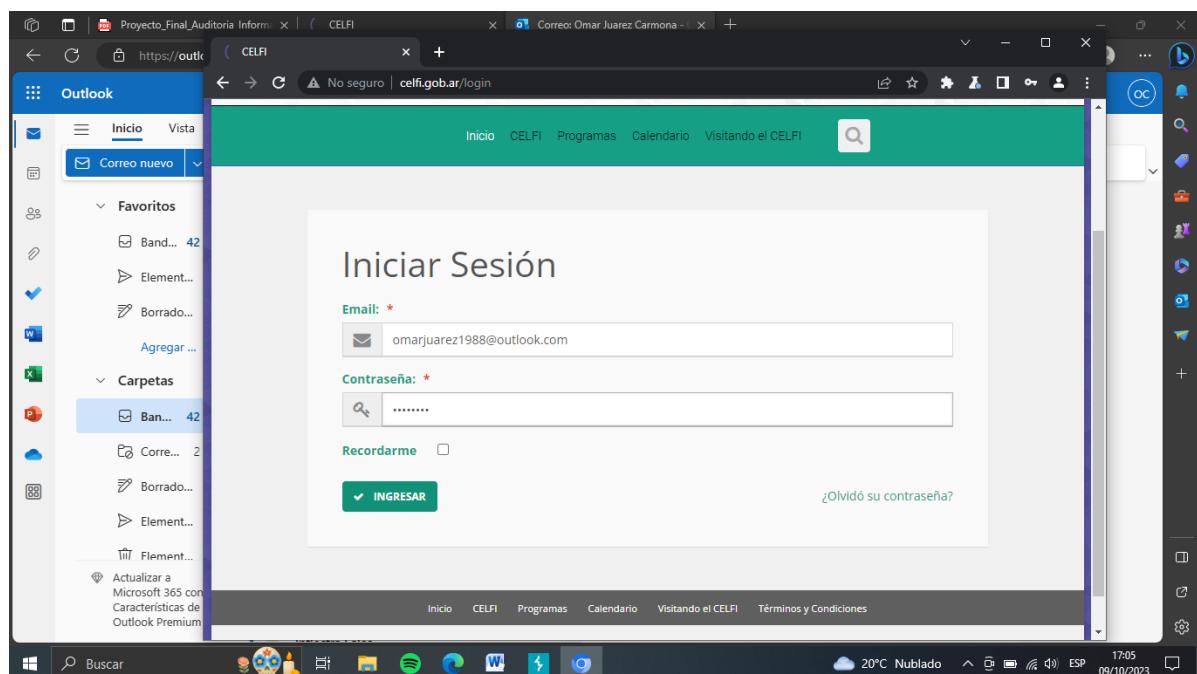
Iniciando el apartado de Browser de Burp Suite para iniciar practica.



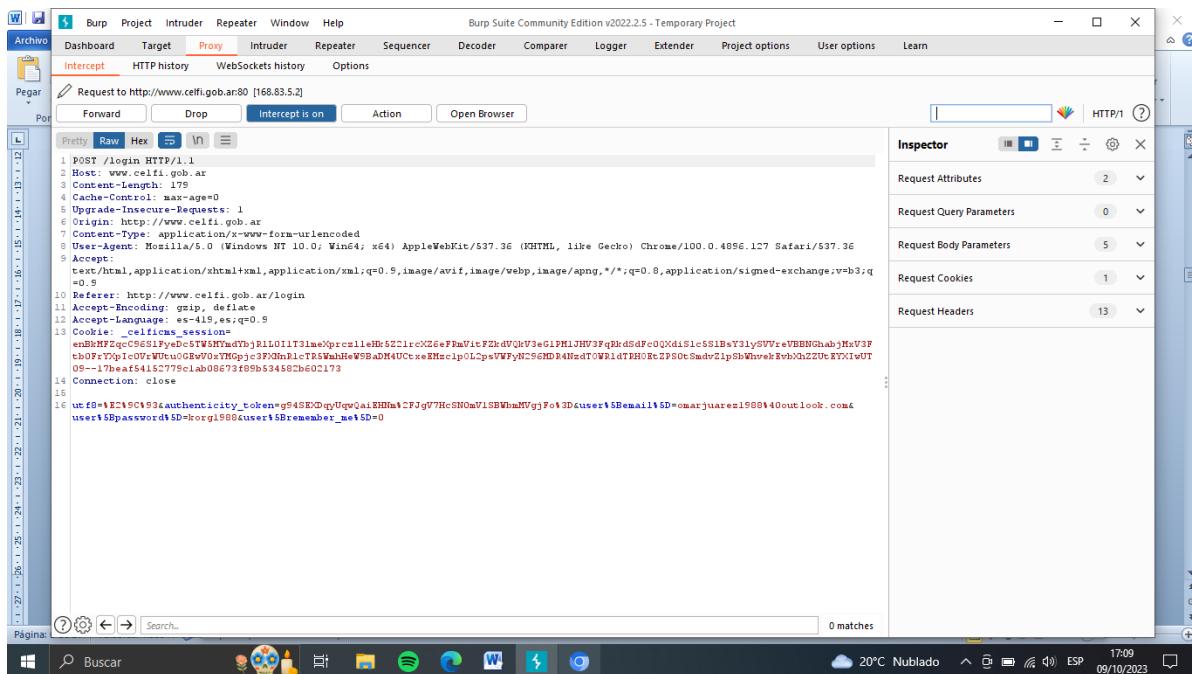
Copiando link de web no seguro en Burp Suite..



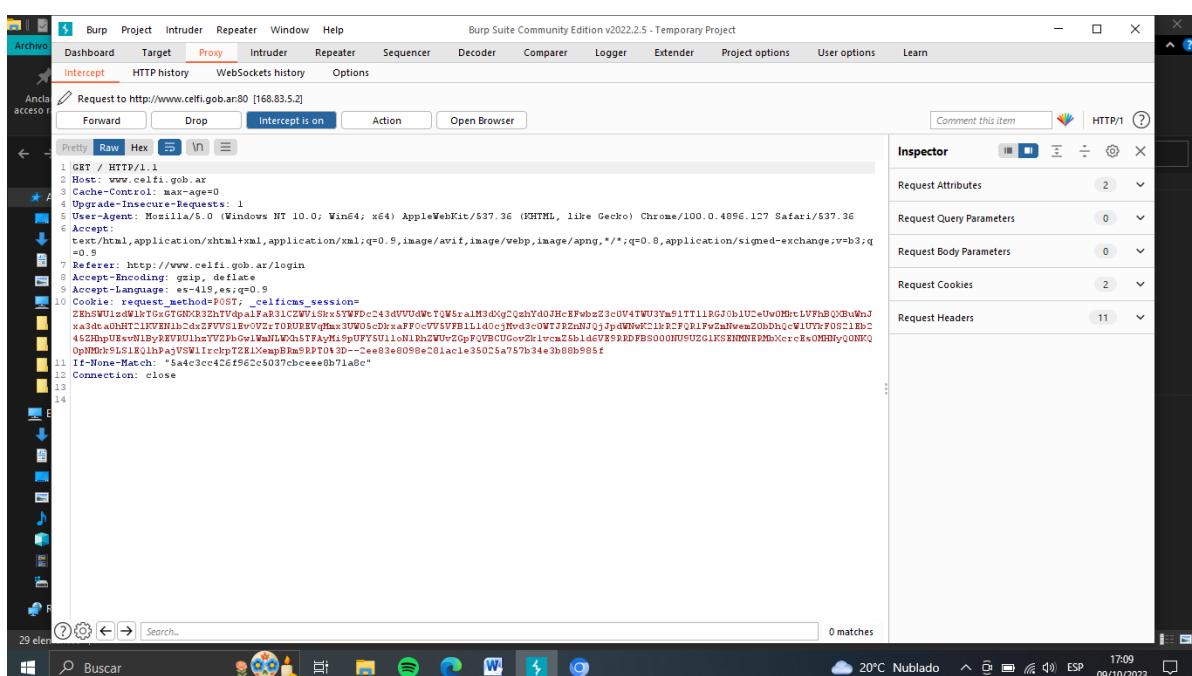
Iniciando sesión en Burp Suite para robar datos personales.



Iniciando interceptor para visualizar información personal ya robada al entrar a web.



Interceptor visualizando información personal ya robada al entrar a web no seguro.



Modificando usuario para alterar credenciales en web abierto (usuario).

Burp Suite Community Edition v2022.2.5 - Temporary Project

Request to http://www.celfi.gob.ar:80 [168.83.5.2]

POST /login HTTP/1.1

Host: www.celfi.gob.ar

Content-Length: 179

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/100.0.4896.127 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=0.9

Referer: http://www.celfi.gob.ar/login

Accept-Encoding: gzip, deflate

Accept-Language: es-415,es;q=0.9

Cookie: _celfi_session=...; authenticity_token=g4SEX0qUqQoQaiHm+2FJgV7HcSN0mV1SBWnMVgjF+3D&user123@email+SD=omarjuarez198012@outlook.com&user123password=Korgi588&user123remember_me=0

Connection: close

Content-Type: application/x-www-form-urlencoded

Content-Length: 179

Selected text: omarjuarez198012

Decoded from: URL encoding

Request Attributes: 2

Request Query Parameters: 0

Request Body Parameters: 5

Request Cookies: 1

Request Headers: 13

0 matches

Buscar 20°C Nublado 17:15 09/10/2023

Notificando información personal modificada (usuario)

Burp Suite Community Edition v2022.2.5 - Temporary Project

CELFI

No seguro | celfi.gob.ar

Iniciar Sesión | Idioma

Centro latinoamericano de formación interdisciplinaria

Ministerio de Ciencia, Tecnología e Innovación Argentina

Error al loguearse, valide su usuario y password

GENDA

22/09/2019 - 04/10/2019

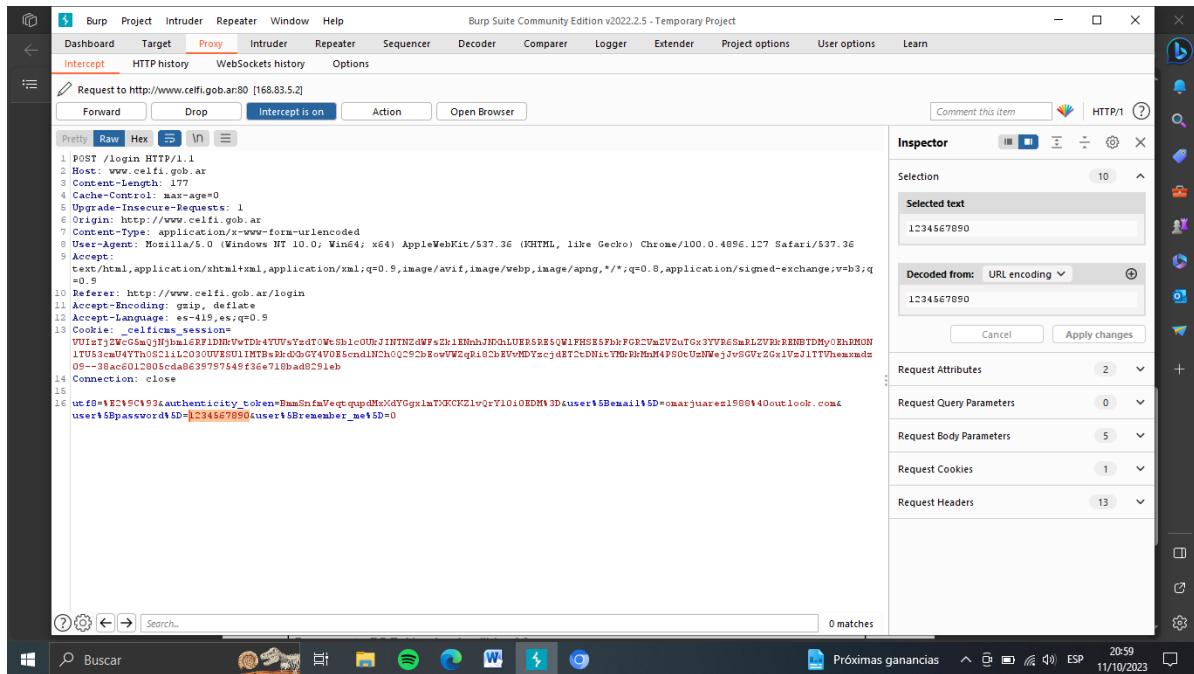
Escuela de Actualización en Oncología: Un enfoque interdisciplinario del diagnóstico, tratamiento e investigación del cáncer.

Ya están publicados los resultados de la convocatoria a becas.

VER DETALLE

19°C Nublado 17:47 09/10/2023

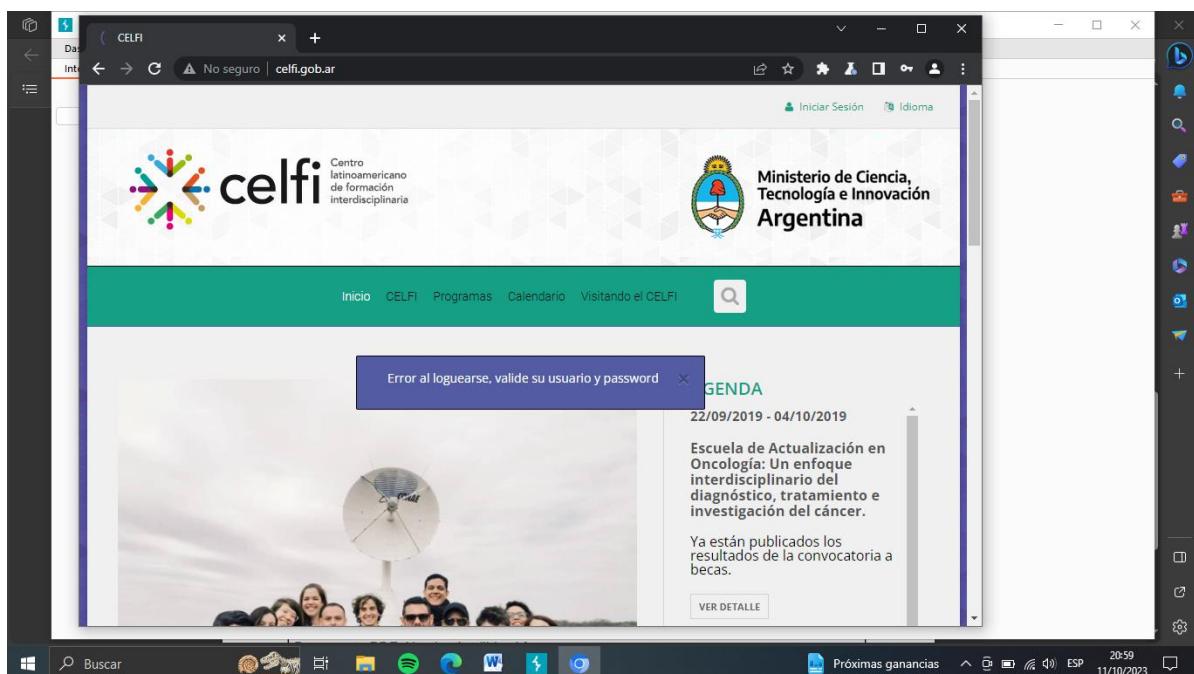
Modificando contraseña.



The screenshot shows the Burp Suite interface in Proxy mode. A POST request to `/login` is selected. The raw request body is as follows:

```
POST /login HTTP/1.1
Host: www.celfi.gob.ar
Content-Length: 177
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://www.celfi.gob.ar
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/100.0.4856.127 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=0.9
Referer: http://www.celfi.gob.ar/login
Accept-Encoding: gzip, deflate
Accept-Language: es-415,es;q=0.9
Cookie: celfi_session=VUf1tjZEWG5aQMNhml6RFIDmWvT0d4YUVsYzdT0WeSb1c0U8J1NTN2dWFsZk1ENnhJNQhLUEB5RE5QW1FHSE5FbFG8ZVmZV2uTGc3YVRE6SmRLZVRkRENhTDMy0EhEMON1TU53cmU4YTHoSC21lC030JW8S11MTBz8kd0bGYAV0EScn1lCh0QCSCb8owWZqBi8CbEvvMDYzcjdETzEdN1t7MhRkMnM4P8otUzNw3JvSGVrZGx1VzJ1TTWhemmdz09--38acd013b05cd8639797545f36e71b8ad0291eb
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 156
utf8=1E218C193&authenticity_token=BmzSmfxVeqcup=dMaXdyGgxiuTXKCKZ1vQrY1o1ORDM3D&user[email]=omarjuarez1980@outlook.com&user[password]=5c34667890&user[remember_me]=0
```

Alerta de error al cambiar contraseña.



The screenshot shows a browser window for the website `celfi.gob.ar`. The page displays the CELFI logo and the Ministry of Science, Technology and Innovation Argentina logo. A navigation bar includes links for Inicio, CELFI, Programas, Calendario, Visiting the CELFI, and a search bar. A prominent error message box in the center states: "Error al loguearse, valide su usuario y password". To the right, there is a sidebar with the word "AGENDA" and a list of events, including one from 22/09/2019 to 04/10/2019 about an oncology update course. The bottom of the screen shows the Windows taskbar with various pinned icons.

Iniciando con credenciales correctas a web.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A browser window is open to the 'CELFI' website at <http://www.celfi.gob.ar/login>. The page displays a login form with fields for 'Email:' and 'Contraseña:', both filled with placeholder text. Below the form are 'Recordarme' and 'INGRESAR' buttons. To the right of the form is a link to '¿Olvidó su contraseña?'. At the bottom of the page, there's a footer with links to 'Inicio', 'CELFI', 'Programas', 'Calendario', 'Visitando el CELFI', and 'Términos y Condiciones'. The status bar at the bottom of the screen shows the date as 09/10/2023 and the time as 17:16.

Notificando acceso al sitio web.

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. A browser window is open to the 'CELFI' website at <http://www.celfi.gob.ar>. The page displays the CELFI logo and the text 'Iberoamericano de formación interdisciplinaria'. Below the logo is a large photograph of a group of people posing in front of a building. Overlaid on the image is the text 'Escuela de Actualización en Oncología'. To the right of the image, there's a section titled 'AGENDA' with two entries: '22/09/2019 - 04/10/2019' and '09/09/2019 - 13/09/2019'. The status bar at the bottom of the screen shows the date as 09/10/2023 and the time as 17:18.

CONCLUSION

La vulnerabilidad de Cross Site Scripting (XSS) es una falla de seguridad que permite a un atacante insertar scripts maliciosos en el navegador web de un usuario. Los ataques XSS pueden tener diversas consecuencias para los usuarios, como el robo de credenciales, el redireccionamiento a sitios maliciosos, el acceso al control del equipo de la víctima y el cambio de la apariencia visual del sitio.

Existen tres tipos principales de ataques XSS: reflejado, almacenado y basado en DOM.

- El ataque reflejado se produce cuando una aplicación recibe datos maliciosos en una solicitud HTTP y los incluye dentro de la respuesta inmediata.
- El ataque almacenado se produce cuando una aplicación recibe datos de una fuente que no es de confianza y los incluye en sus respuestas HTTP posteriores.
- El ataque basado en DOM surge cuando una aplicación que tiene código JavaScript del lado del cliente procesa datos de una fuente maliciosa, generalmente escribiendo los datos en el DOM.

Para prevenir los ataques XSS, se recomienda mantener las aplicaciones y sistemas actualizados. Los navegadores utilizan distintos filtros que analizan las solicitudes HTTP, el código HTML y las URLs para advertir o eliminar funciones sospechosas que se ejecutarán en el navegador.

Como hemos notado en esta práctica de vulnerabilidad XSS, pudimos robar información y así mismo poder alterarla en un sitio web no seguro, esto significa que como personas maliciosas, podemos robar información muy importante de un usuario con estas herramientas de trabajo. Podemos llamarnos Hackers pequeños, porque ya nos está enseñando las vulnerabilidades de los sitios web tutora y así poder aprovecharnos de usuarios que no tienen conocimientos básicos de Auditorias informáticas. Excelente materia tutora, nos vemos pronto para poder robar más información de su persona (conocimientos).

REFERENCIAS Y LINK

Wireshark · go deep. (n.d.). Wireshark. Retrieved September 21, 2023, from

<https://www.wireshark.org/>

CELFI. (n.d.). Gob.Ar. Retrieved September 25, 2023, from

<http://www.celfi.gob.ar/>

Professional / Community 2022.2.5. (2022, April 20). Burp Suite Release Notes.

<https://portswigger.net/burp/releases/professional-community-2022-2-5?requestededition=community&requestedplatform>

Lab: Modifying serialized objects. (n.d.). Portswigger.net. Retrieved October 6,

2023, from <https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects>

LINK DE GITHUB

[Omarsitho1988 \(github.com\)](https://github.com/Omarsitho1988)