

Ingeniería en Desarrollo de Software.

Nombre de la Actividad.

Actividad 2. Deserialización Insegura.

Actividad [#2]

Etapas #2 – Deserialización Insegura.

Nombre del Curso.

Auditoría Informática

Tutor: Jessica Hernández Romero.

Alumno: José Luis Martín Martínez.

Fecha: 07/10/2023.

Índice.

Contextualización y Actividades.....	4
Introducción.....	6
Descripción.....	8
Justificación.....	12
Ataque al sitio.....	16
Conclusión.....	17
Referencias.....	18

Contextualización y Actividades.

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

Para esta segunda etapa, pide realizar una prueba de deserialización insegura en una página específica. Esta debe ser mediante las *cookies*. Para lograrlo, utilizar el programa *Burp Suite Community Edition*. El objetivo de esta prueba es que se inicie sesión como un usuario normal y luego pasar a modo administrador a través de las *cookies*.

Actividad:

Con la ayuda de la plataforma *PortSwigger*, realizar el ataque a una página proporcionada por ellos. En ella, iniciar sesión con las credenciales que se proporcionan, las cuales son para usuarios normales; no obstante, a través de las *cookies*, entrar al modo administrador.

Cabe mencionar que este laboratorio utiliza un mecanismo de sesión basado en serialización. Por ende, es vulnerable a la escalada de privilegios. En consecuencia, hay editar el objeto serializado en la *cookie* de sesión para aprovechar esta vulnerabilidad y obtener privilegios administrativos. Finalmente, el objetivo es eliminar la cuenta de *Carlos*.

Hay que iniciar sesión en la propia cuenta con las siguientes credenciales:

Usuario: wiener

Contraseña: peter

Introducción.

En esta segunda actividad, se nos pide realizar una prueba de deserialización insegura en una página específica. Esta debe ser mediante las *cookies*. Utilizando el programa *Burp Suite Community Edition*. El objetivo de esta prueba es que se inicie sesión como un usuario normal y luego pasar a modo administrador a través de las *cookies*. La deserialización insegura es una vulnerabilidad de seguridad que puede ocurrir en aplicaciones informáticas cuando se manejan datos serializados de manera incorrecta o sin una adecuada validación y control. Esto puede ser un tema importante en la auditoría de seguridad informática, ya que puede dar lugar a ataques y violaciones de seguridad. La serialización es el proceso de convertir datos en un formato que pueda ser fácilmente almacenado o transmitido y luego volver a convertirlos en su forma original (deserialización). En el contexto de la programación, esto a menudo se utiliza para guardar objetos en archivos o para transmitirlos a través de una red. Sin embargo, cuando la deserialización no se realiza de forma segura, un atacante puede manipular los datos serializados para ejecutar código malicioso en la aplicación o realizar otras acciones dañinas.

Algunos problemas comunes relacionados con la deserialización insegura incluyen:

Ejecución de código malicioso: Un atacante podría manipular los datos serializados para ejecutar código arbitrario en el servidor o en la aplicación, lo que podría dar lugar a un ataque de inyección de código o incluso tomar el control del sistema.

Denegación de servicio: Un atacante podría diseñar datos serializados maliciosos que causen una sobrecarga en la aplicación, lo que podría llevar a una denegación de servicio (DoS) si no se maneja adecuadamente.

Fuga de información: La deserialización insegura también puede llevar a la fuga de información confidencial si un atacante puede acceder a datos que no debería.

En una auditoría informática, se busca identificar y remediar estas vulnerabilidades de deserialización insegura mediante la revisión del código fuente, pruebas de penetración y otros métodos de evaluación de seguridad. Los auditores se aseguran de que las aplicaciones validen y controlen de manera adecuada los datos serializados antes de procesarlos y que sigan prácticas recomendadas de seguridad en este aspecto. Para prevenir la deserialización insegura, es importante seguir buenas prácticas de programación, como utilizar bibliotecas de deserialización segura, validar y verificar los datos serializados antes de procesarlos, restringir el acceso a clases y métodos sensibles, y mantenerse actualizado con las últimas amenazas de seguridad y parches disponibles.

Descripción.

Como mencionamos en la introducción, nos pide realizar una prueba de deserialización insegura en una página específica. Esta debe ser mediante las *cookies*. Para lograrlo, utilizar el programa *Burp Suite Community Edition*. El objetivo de esta prueba es que se inicie sesión como un usuario normal y luego pasar a modo administrador a través de las *cookies*.

Con la ayuda de la plataforma *PortSwigger*, realizar el ataque a una página proporcionada por ellos. En ella, iniciar sesión con las credenciales que se proporcionan, las cuales son para usuarios normales; no obstante, a través de las *cookies*, entrar al modo administrador. Cabe mencionar que este laboratorio utiliza un mecanismo de sesión basado en serialización. Por ende, es vulnerable a la escalada de privilegios. En consecuencia, hay editar el objeto

serializado en la *cookie* de sesión para aprovechar esta vulnerabilidad y obtener privilegios administrativos. Finalmente, el objetivo es eliminar la cuenta de *Carlos*.

Debemos de saber que la deserialización insegura se clasifica como la vulnerabilidad número ocho en la lista de OWASP-Top 10. La deserialización insegura es una vulnerabilidad que ocurre cuando los datos no confiables se usan para abusar de la lógica de una aplicación, infligir un ataque de denegación de servicio (DoS) o incluso ejecutar código arbitrario.

Para entender esta vulnerabilidad, es necesario entender el proceso de serialización. La serialización es el proceso de traducir estructuras de datos o estados de objetos a un formato que puede almacenarse y reconstruirse con posterioridad. La deserialización, por otro lado, es lo opuesto a la serialización, es decir, transformar los datos serializados provenientes de un archivo, secuencia o socket de red en un objeto. Es en este último proceso donde reside la vulnerabilidad.

La mayoría de los lenguajes de programación ofrecen la posibilidad de personalizar los procesos de deserialización. Desafortunadamente, con frecuencia es posible que un atacante abuse de estas características de deserialización cuando la aplicación de serializa datos no confiables que controla el atacante. Los ataques de deserialización inseguros permiten que un atacante realice ataques de denegación de servicio, omisiones de autenticación y ataques de ejecución remota de código.

Justificación.

Es momento de poder justificar el por qué debemos de conocer a detalle la implementación. Burp Suite, es una plataforma capaz de llevar a cabo las auditorías de seguridad, de una organización con el objetivo de evitar ataques de software maliciosos.

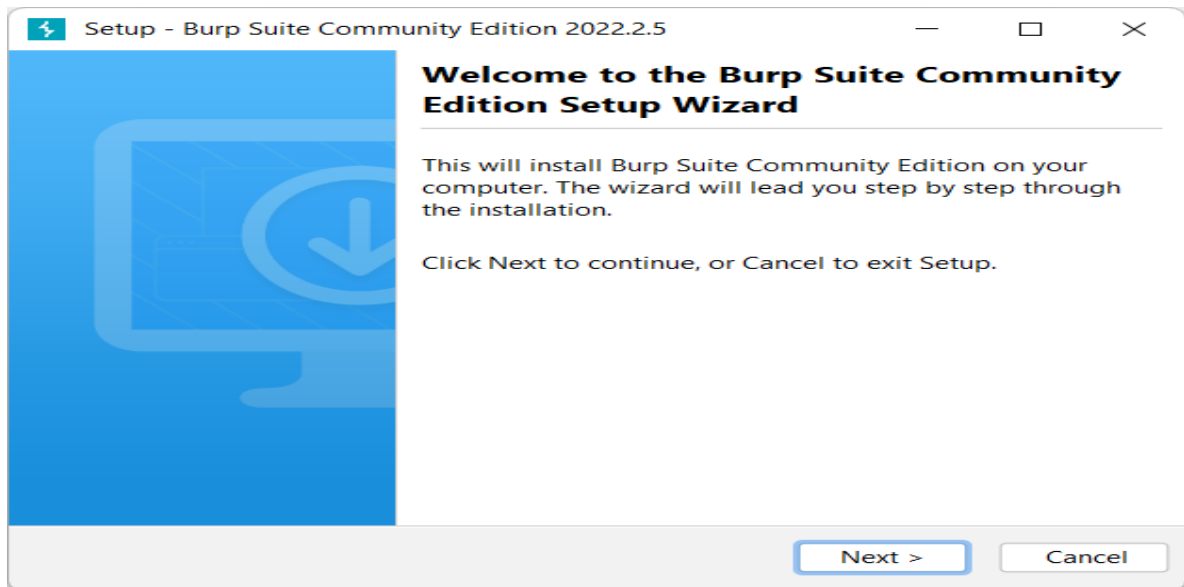
Ahora bien, en este apartado analizaremos con mayor profundidad que se puede hacer con Burp Suite, qué herramientas ofrece esta plataforma para el cuidado de la ciber seguridad de una empresa. Burp Suite es una herramienta de pruebas de seguridad diseñada para evaluar la seguridad de aplicaciones web y sistemas. Funciona como un proxy web que intercepta las solicitudes y respuestas HTTP entre un cliente web (como un navegador) y el servidor web. Aquí te explicaré cómo funciona Burp Suite en sus funciones básicas:

1. Interceptación de tráfico: - Burp Suite actúa como un intermediario entre el cliente web y el servidor web. Configura tu navegador para que utilice Burp Suite como proxy. - Cuando el cliente web realiza una solicitud HTTP (por ejemplo, al cargar una página web o enviar un formulario), Burp Suite intercepta esa solicitud antes de que llegue al servidor. Se trata de una herramienta que le da mucho potencial a la plataforma. Existen dos formas de instalar una extensión, las cuales describiremos más adelante. Otra de las herramientas que ofrece Burp Suite. Burp Intruder y Burp Intruder se relaciona con la función de realizar ataques que ofrece. Con ella se pueden realizar ataques programados que pongan a prueba nuestro sistema. Si bien es una herramienta que está disponible en la versión gratuita de Burp Suite, ofrece su máximo potencial con Burp Professional, la versión paga. Cuando nos referimos a que se puede hacer con Burp Suite, no podemos dejar de mencionar su herramienta target. Esta última, disponible en Burp Free, permite fijar un objetivo y construir un SiteMap a partir de él. Como bien marcamos al principio, Burp Suite puede realizar ciertas acciones de manera automatizada. Recordemos que su principal funcionalidad es la de encontrar vulnerabilidades en las aplicaciones web para evitar que sufran intromisiones maliciosas. Es para eso, en particular, que existe la herramienta que los desarrolladores han llamado spider. Se trata de un instrumento por el cual es posible inspeccionar las páginas web y recursos de la aplicación de forma automática. Además, con la herramienta repeater, es posible controlar de forma

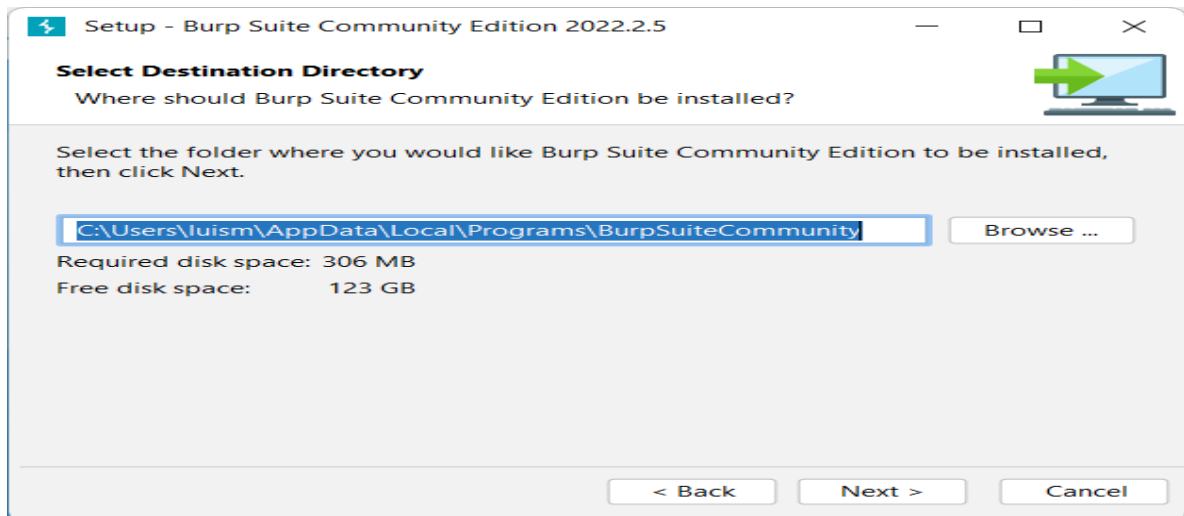
manual las peticiones HTTP interceptadas por el proxy, cambiar parámetros, cabeceras y reenviarlas nuevamente. Por esta razón recomiendo utilizar el software para una auditoria informática.

Ataque al sitio.

Instalar Burp Suite Community Edition



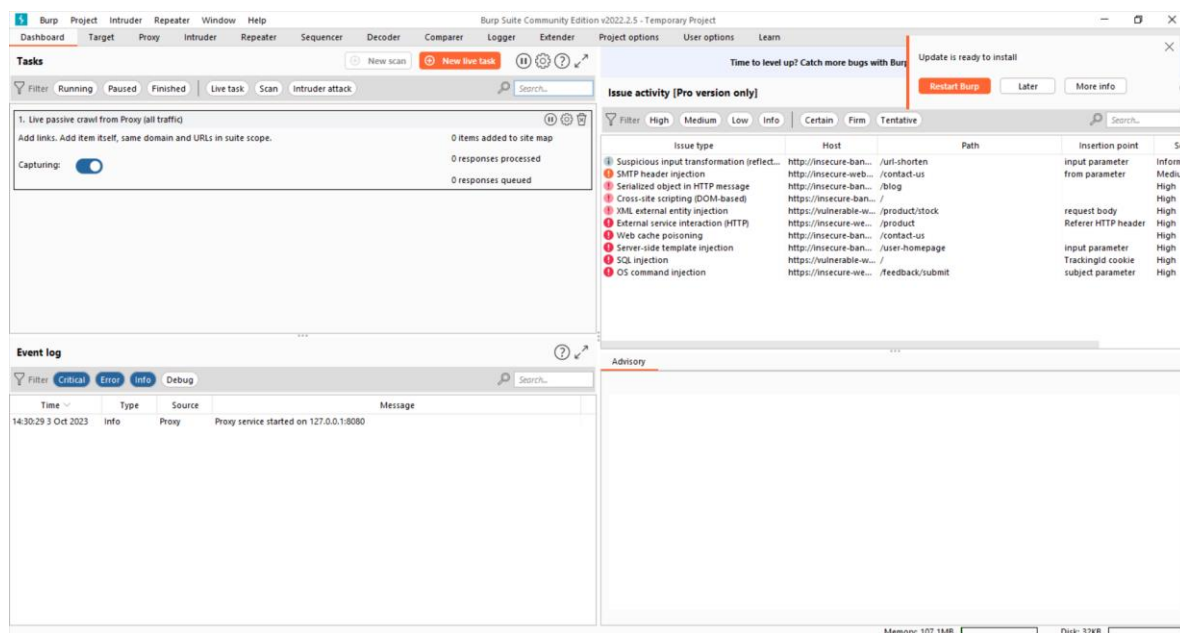
Seleccionar directorio de destino



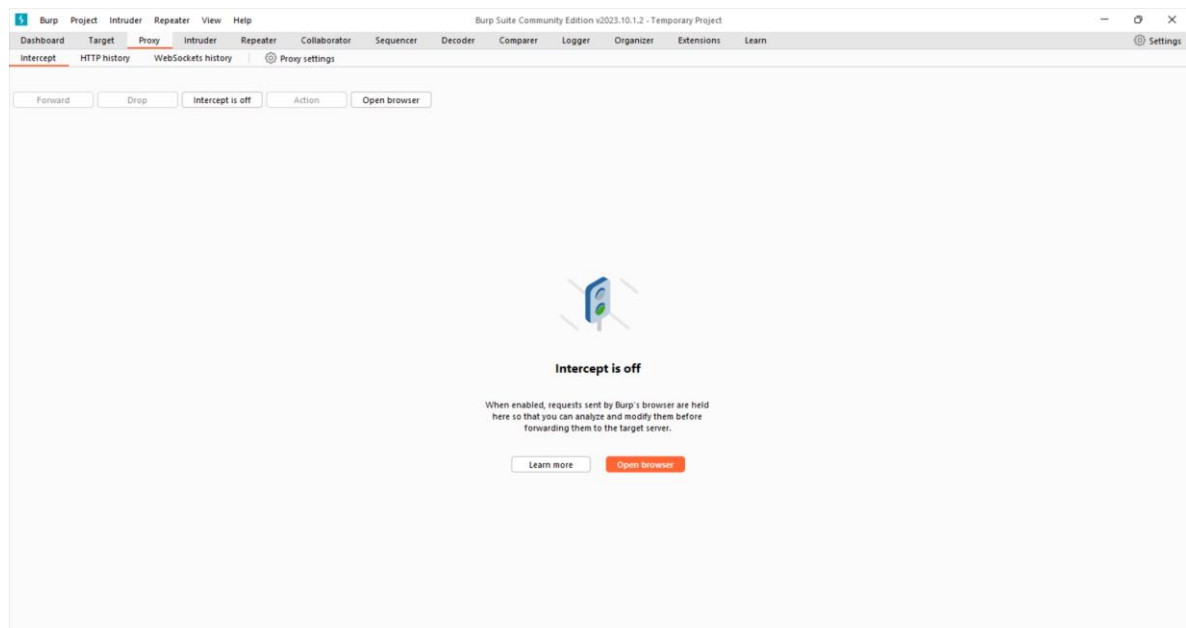
Inicio de pantalla principal.



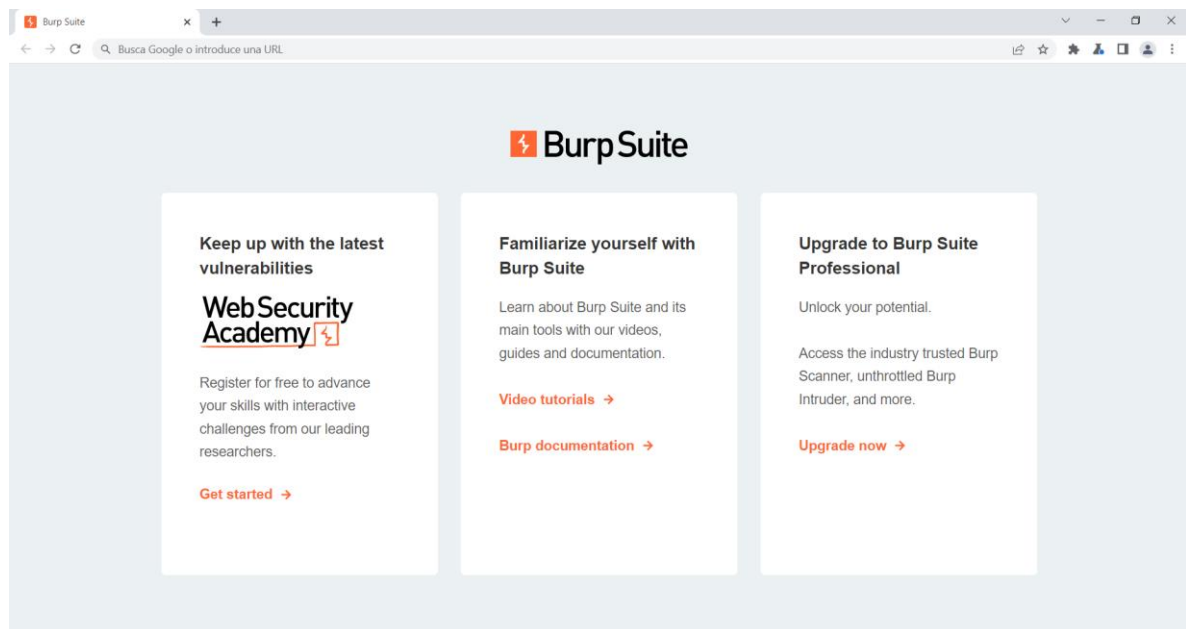
Interfaz principal.



Accediendo al Proxy dentro de Burp Suite



Navegador del Burp Suite.



Se obtuvo información en cookie sesión de usuario en post /login

Burp Suite Community Edition v2023.5.5 - Temporary Project

Dashboard Target Proxy Intruder Repeater Window Help

Intercept HTTP history WebSockets history Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener po
84	https://0a6700f6040684ad...	GET	/academyLabHeader			200	147	HTML		Modifying serialized...		✓	79.125.84.16		22:27:32 ...	8080
85	https://0a6700f6040684ad...	GET	/my-account			200	362	HTML		Modifying serialized...		✓	79.125.84.16		22:27:32 ...	8080
86	https://0a6700f6040684ad...	GET	/login			200	3148	HTML		Modifying serialized...		✓	79.125.84.16		22:27:32 ...	8080
87	https://0a6700f6040684ad...	GET	/academyLabHeader			101	147	HTML		Modifying serialized...		✓	79.125.84.16		22:27:33 ...	8080
88	https://0a6700f6040684ad...	POST	/login		✓	200	3226	HTML		Modifying serialized...		✓	34.246.129.62		22:38:01 ...	8080
89	https://0a6700f6040684ad...	GET	/academyLabHeader			101	147	HTML		Modifying serialized...		✓	34.246.129.62		22:38:03 ...	8080
90	https://0a6700f6040684ad...	POST	/login		✓	302	238	HTML		Modifying serialized...		✓	34.246.129.62	session=TzoO...	22:38:44 ...	8080
91	https://0a6700f6040684ad...	GET	/my-account?id=wiener		✓	200	3243	HTML		Modifying serialized...		✓	34.246.129.62		22:38:45 ...	8080
92	https://0a6700f6040684ad...	GET	/academyLabHeader			101	147	HTML		Modifying serialized...		✓	34.246.129.62		22:38:45 ...	8080
93	https://0a6700f6040684ad...	GET	/my-account?id=wiener		✓	200	3243	HTML		Modifying serialized...		✓	34.246.129.62		22:50:47 ...	8080

Request

```

1 POST /login HTTP/2
2 Host: 0a6700f6040684ad800b582f0db200e4.web-security-academy.net
3 Cookie: session=
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://0a6700f6040684ad800b582f0db200e4.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/svg+xml,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
14 Sec-Fetch-Site: same-origin
15 Sec-Fetch-Mode: navigate
16 Sec-Fetch-User: ?1
17 Sec-Fetch-Dest: document
    
```

Response

```

1 HTTP/2 302 Found
2 Location: /my-account?id=wiener
3 Set-Cookie: session=Tso0iJ3vcVYIyjoYnto0sg6InVwZKJuTWl1jcs0gYeIndpZWslci17cso10jh2GlpbiI7Tysow030k3d; Secure: HttpOnly; SameSite=None
4 X-Frame-Options: SAMEORIGIN
5 Content-Length: 0
    
```

Inspector

Selection 82 ^

Selected text

```

Tso0iJ3vcVYIyjoYnto0sg6InVwZKJuTWl1jcs0gYeIndpZWslci17cso10jh2GlpbiI7Tysow030k3d
    
```

Decoded from: URL encoding

```

Tso0iJ3vcVYIyjoYnto0sg6InVwZKJuTWl1jcs0gYeIndpZWslci17cso10jh2GlpbiI7Tysow030k3d
    
```

Decoded from: Base64

```

0: {"User":2;":{"s:0:"username";s:6:"wiener";s:5:"admin";b:0;}}
    
```

Request Attributes 2

Crear cuenta de PortSwinger.

Laboratorio: Modificar objeto: x

Crear su cuenta - PortSwigger x

← → ↺

https://portswigger.net/users/register

PortSwigger

INICIAR SESION

Productos | Soluciones | Investigación | Academia | Apoyo | ☰

Crear su cuenta

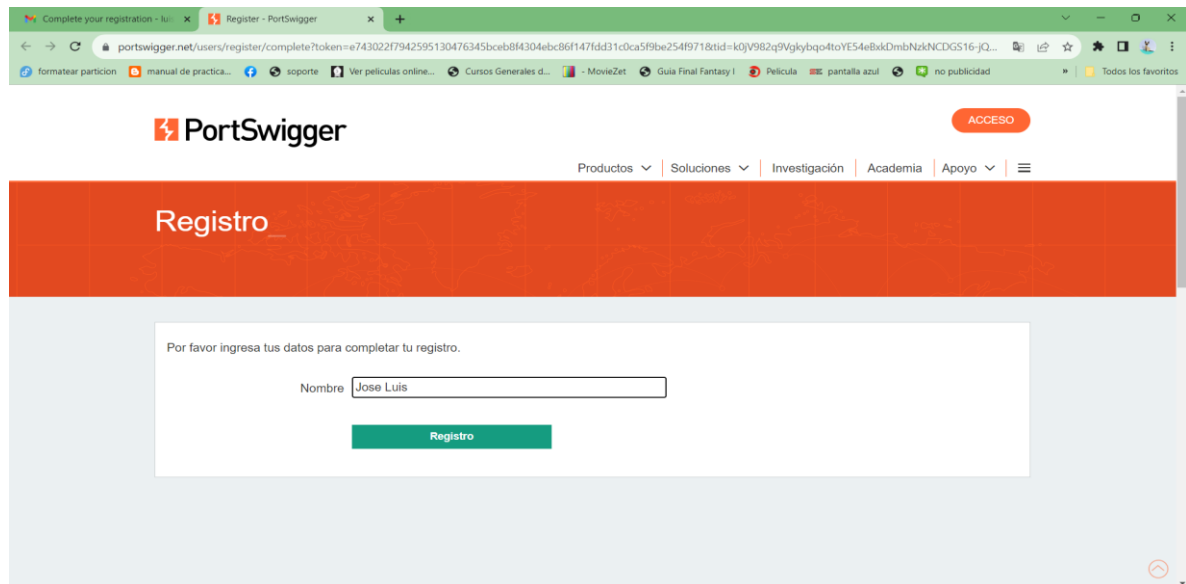
Por favor ingrese su dirección de correo electrónico para registrarse.

Dirección de correo electrónico

Register

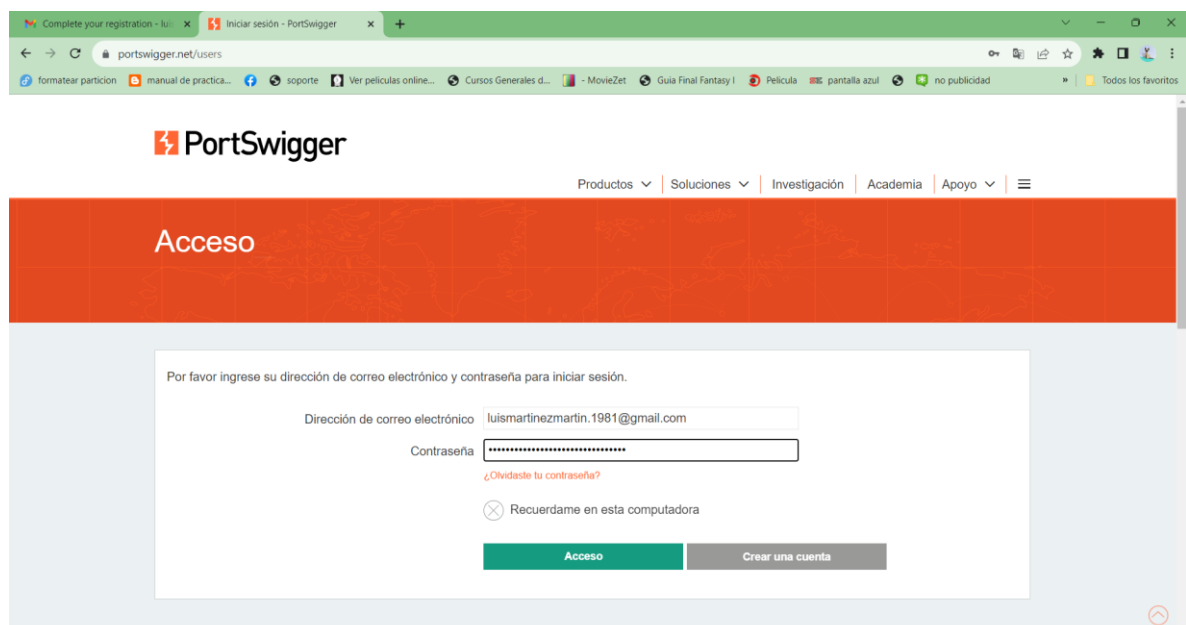
Ya se inscrito? Haz clic [aquí](#) para iniciar sesión.

Ingresar datos personales.



The screenshot shows the PortSwigger registration page. The browser's address bar displays a URL with a token. The page features a navigation bar with links to 'Productos', 'Soluciones', 'Investigación', 'Academia', and 'Apoyo'. A prominent orange banner at the top reads 'Registro'. Below this, a white box contains the instruction 'Por favor ingresa tus datos para completar tu registro.' and a form with a 'Nombre' field filled with 'Jose Luis' and a green 'Registro' button.

Acceso.



The screenshot shows the PortSwigger login page. The browser's address bar displays 'portswigger.net/users'. The page features a navigation bar with links to 'Productos', 'Soluciones', 'Investigación', 'Academia', and 'Apoyo'. A prominent orange banner at the top reads 'Acceso'. Below this, a white box contains the instruction 'Por favor ingrese su dirección de correo electrónico y contraseña para iniciar sesión.' and a form with fields for 'Dirección de correo electrónico' (filled with 'luismartinezmartin.1981@gmail.com') and 'Contraseña' (masked with dots). There is a link for '¿Olvidaste tu contraseña?' and a checkbox for 'Recuérdame en esta computadora'. At the bottom are green 'Acceso' and grey 'Crear una cuenta' buttons.

Mi cuenta.

PortSwigger

Cerrar sesión MI CUENTA

Productos | Soluciones | Investigación | Academia | Apoyo

Mi cuenta

- Detalles personales
- Certificaciones
- Suscripciones
- Historial de pedidos

Detalles personales

José Luis
luismartinezmartin.1981@gmail.com
[Cambiar la contraseña](#)

Dirección de cuenta

No hay dirección asociada con esta cuenta

Tarjetas guardadas

[Agregar nueva tarjeta](#)

Acceso al laboratorio.

PortSwigger

INICIAR SESIÓN

Productos | Soluciones | Investigación | Academia | Apoyo

Dashboard | Vías de aprendizaje | Los últimos tópicos | Todo contenido | Salón de la fama | Empieza | Conseguirse y obtener la certificación

Academia de Seguridad Web > Desserialización Insegura > Explorando > Laboratorio

Laboratorio: Modificar objetos en serie

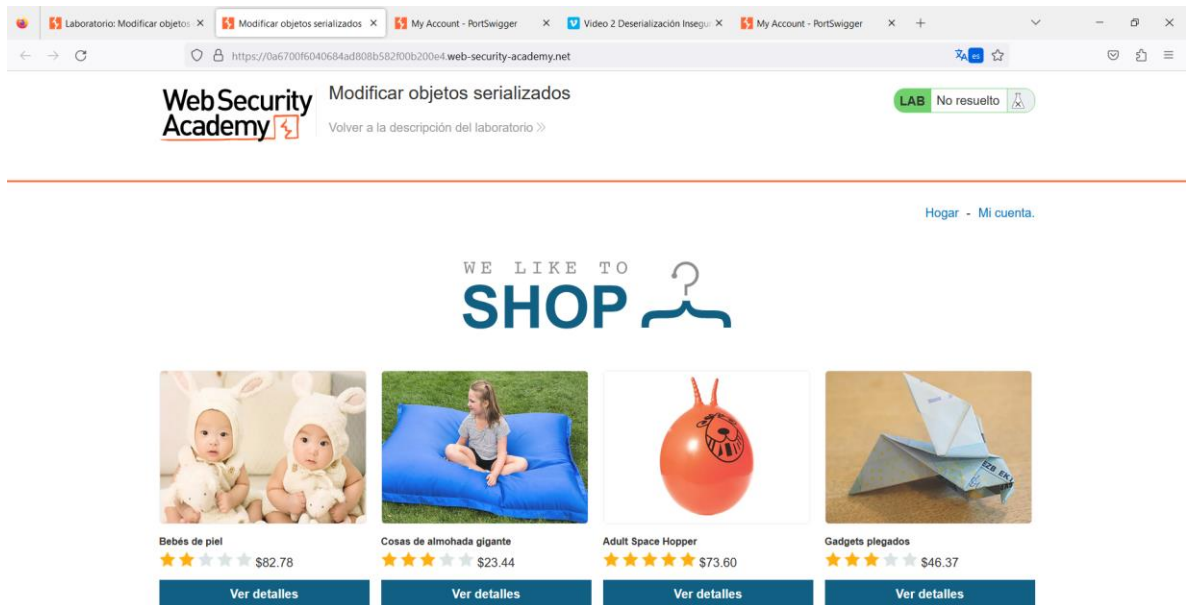
APPRENTICE

Este laboratorio utiliza un mecanismo de sesión basado en la serialización y es vulnerable a la escalada de privilegios como resultado. Para resolver el laboratorio, edite el objeto serializado en la cookie de sesión para explotar esta vulnerabilidad y obtener privilegios administrativos. Luego, borra al usuario `carlos`. Puede iniciar sesión en su propia cuenta usando las siguientes credenciales: `wiener:peter`

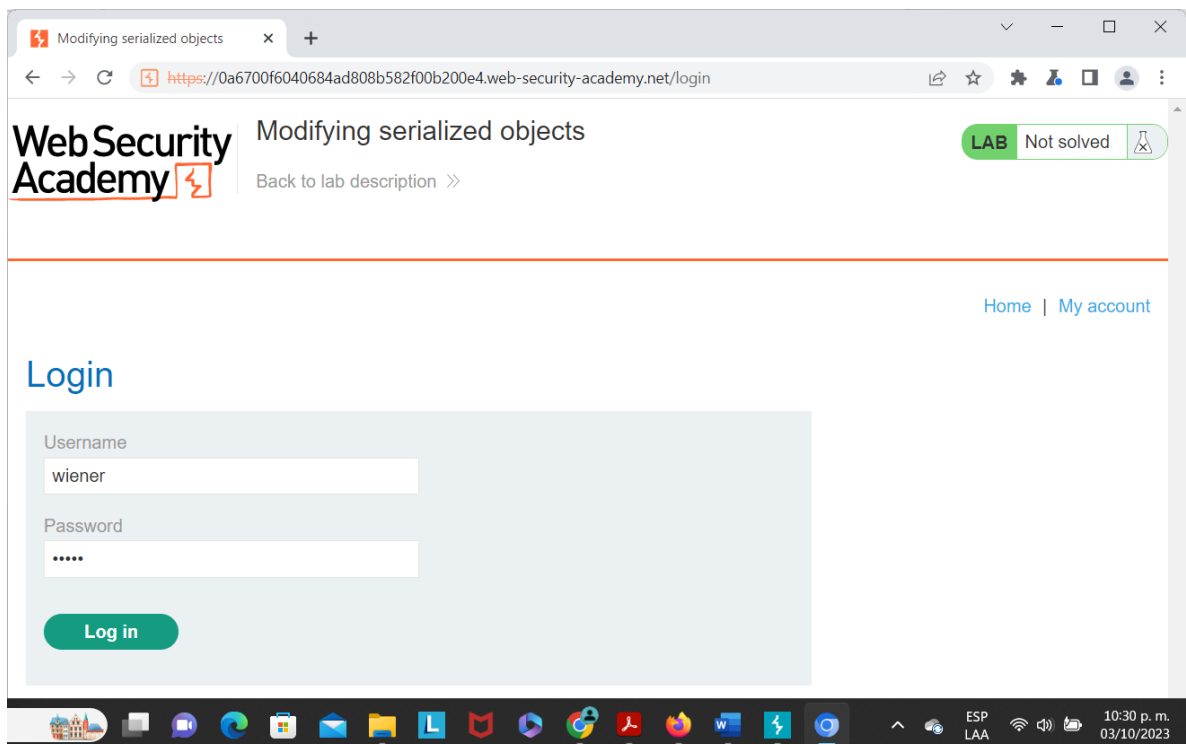
[ACCESO EL LAB](#)

[Solución](#)

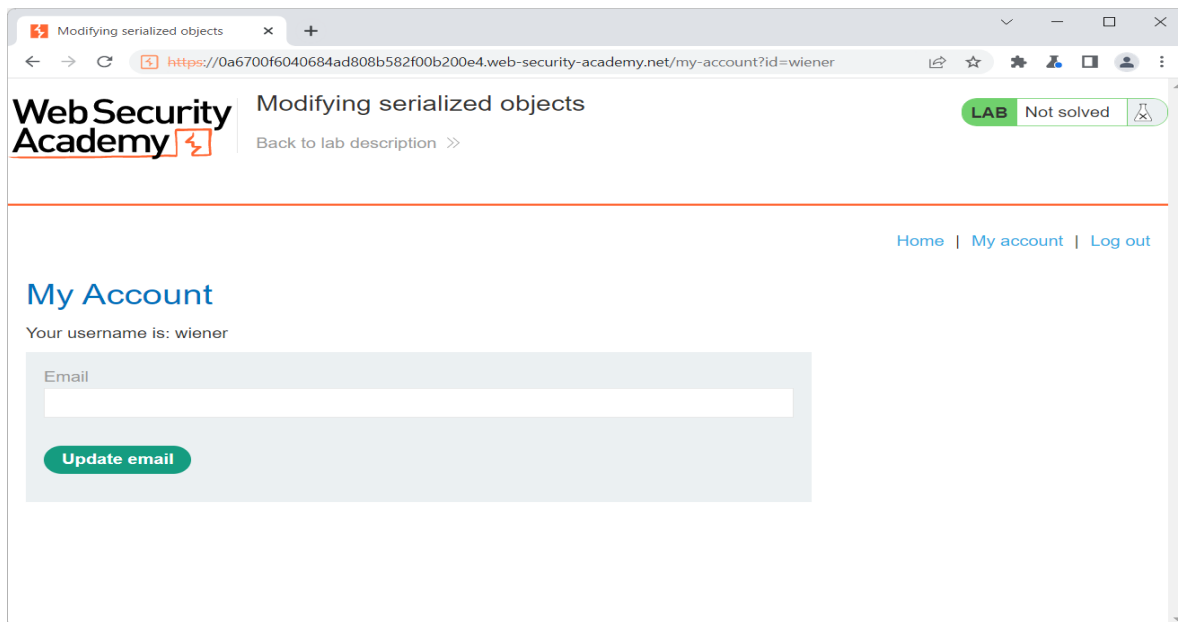
Navegador



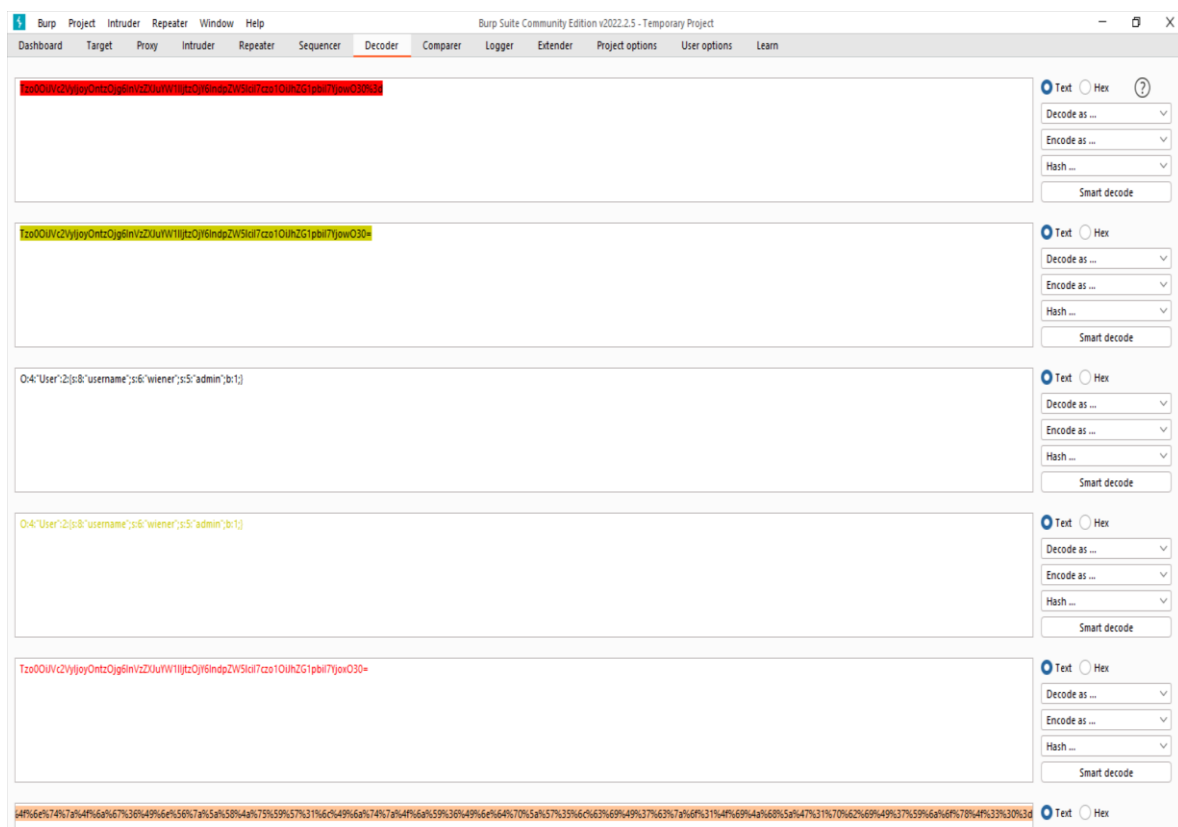
Iniciar sesión my account



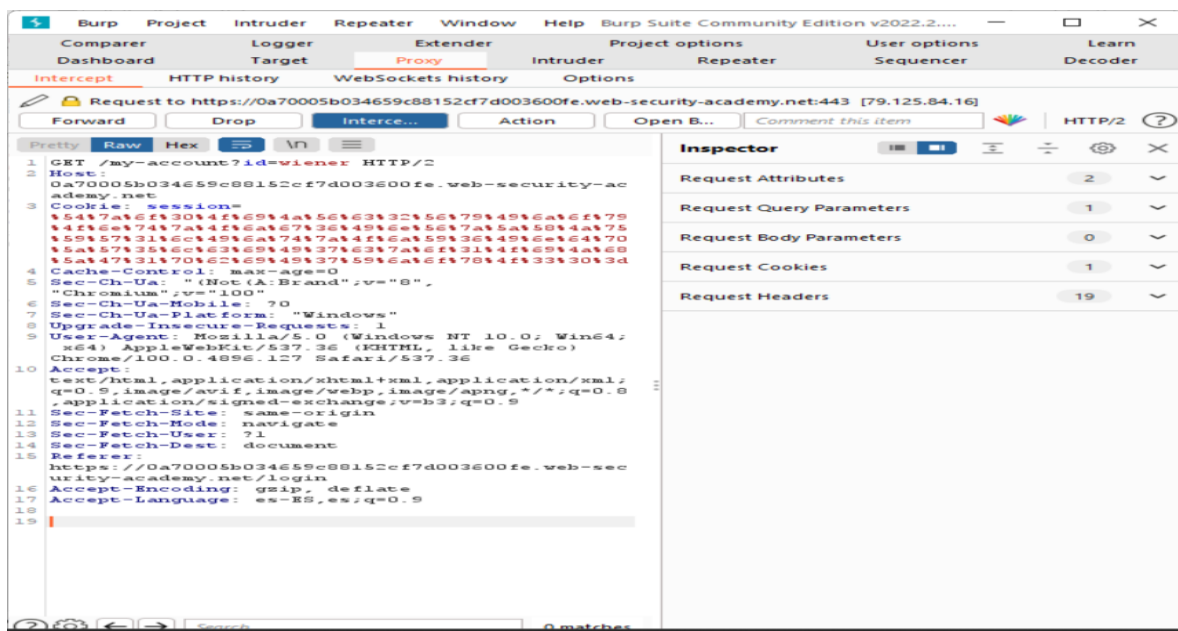
Usar nombre de Wiener y contraseña Peter.



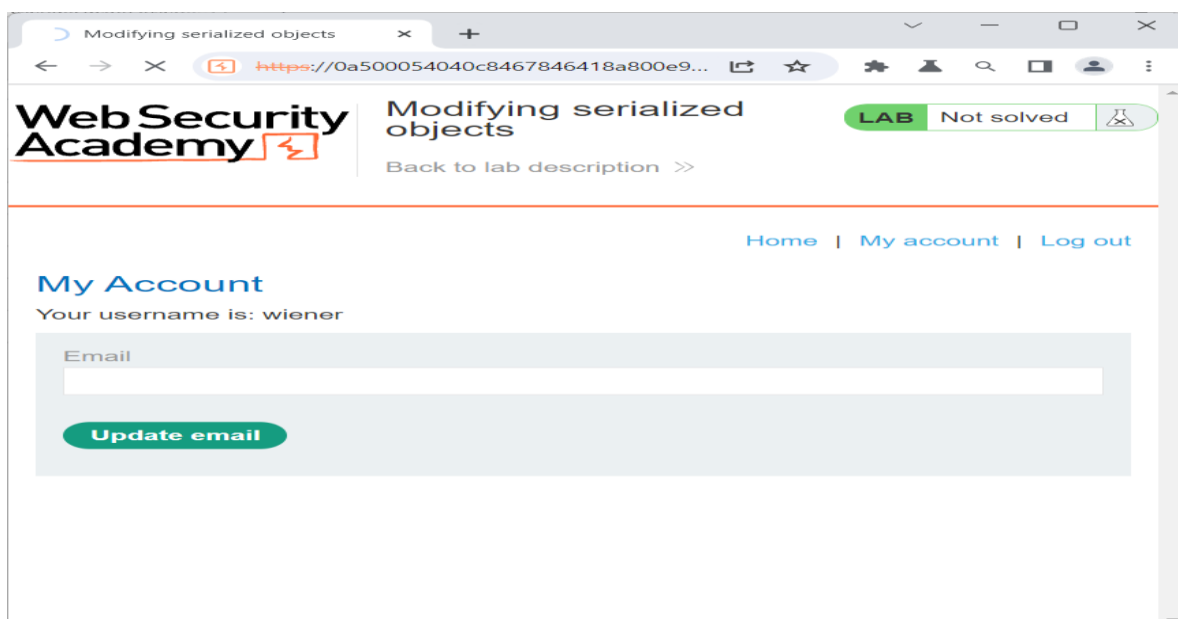
Cambio de credenciales de usuario normal a admin. en Decoder



Borrar la información anterior y pegar la que ya está codificada. Para que te pueda generar el Admin panel en el navegador.



Una vez se hace el cambio de credenciales se actualiza el navegador, mi laptop se queda pensando...este paso es para que en el navegador aparezca el (admin panel). Y poder continuar con el siguiente paso borrar el nombre de Carlos.



Conclusión.

La deserialización insegura es una vulnerabilidad crítica que ocurre cuando una aplicación o una API de serializa datos manipulados por un atacante en el lado del servidor. Durante este proceso, un atacante puede abusar de la lógica de la aplicación y realizar ataques de denegación de servicio (DoS), omitir autenticaciones o incluso ejecutar código malicioso de forma remota. Para prevenir esta vulnerabilidad, es importante implementar medidas de seguridad adecuadas, como la validación y autenticación de datos, y utilizar bibliotecas y marcos de trabajo seguros. El impacto de las amenazas a las vulnerabilidades de los sitios web ha sido tan alto queOWASP ha realizado año con año la lista de las 10 amenazas más peligrosas para los softwares y sus usuarios, incluidas las dos amenazas que vimos en esta unidad número dos. En esta actividad hemos aprendido a utilizar la herramienta de trabajo de BurpSuite. y así poder hackear la información, para entrar en modo incognito a cierta página para poder hacer modificaciones en sus sistemas sin que se den cuenta los usuarios.

REFERENCIAS.

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>

Castillo, A. (1586827274000). *Deserialización insegura – OWASP Top 8*.

Linkedin.com.

<https://es.linkedin.com/pulse/deserializaci%C3%B3n-insegura-owasp-top-8-alexander-castillo>

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

2023, from [https://portswigger.net/web-](https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects)

[security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects](https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects)