Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 2 | Deserialización Insegura.

AUDITORÍA INFORMATICÁ.

Ingenieria en Desarrollo de Software.

academia global

TUTOR: JESSICA HERNANDEZ ROMERO.

ALUMNO: JONATHAN OSWALDO CARDENAS GARCIA.

FECHA: 24-octubre -2025

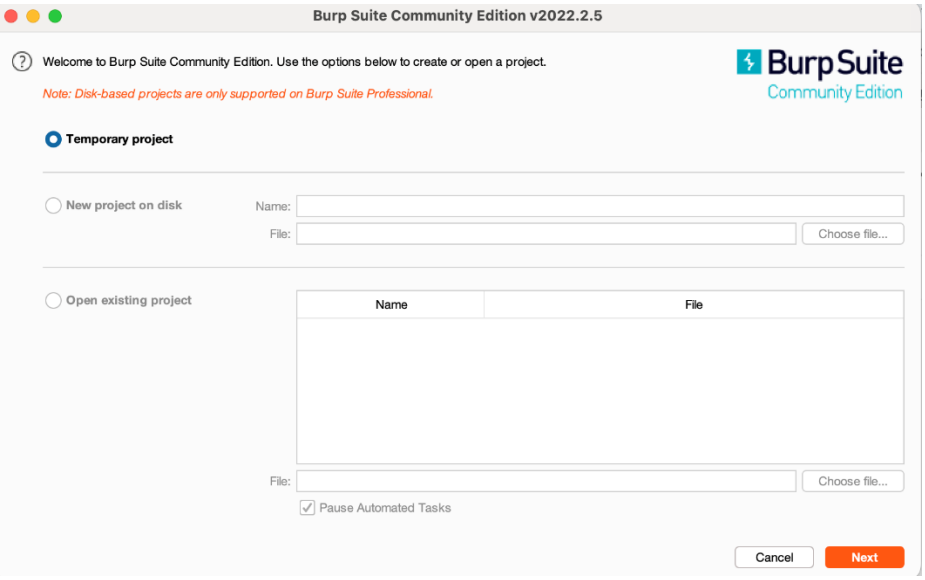
Tabla De Contenido

Desarrollo

Ataque al sitio

Figura 1

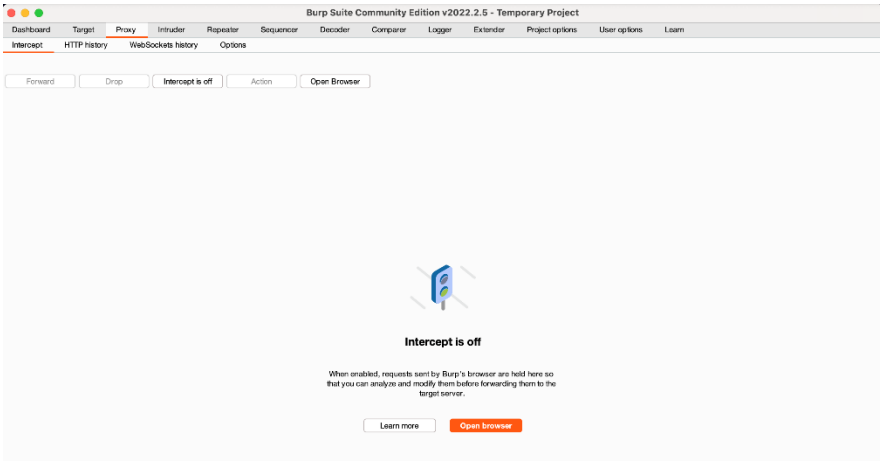
Primera pantalla



Nota. Aquí se ve la primera pantalla que sale cuando abres el programa.

Figura 2

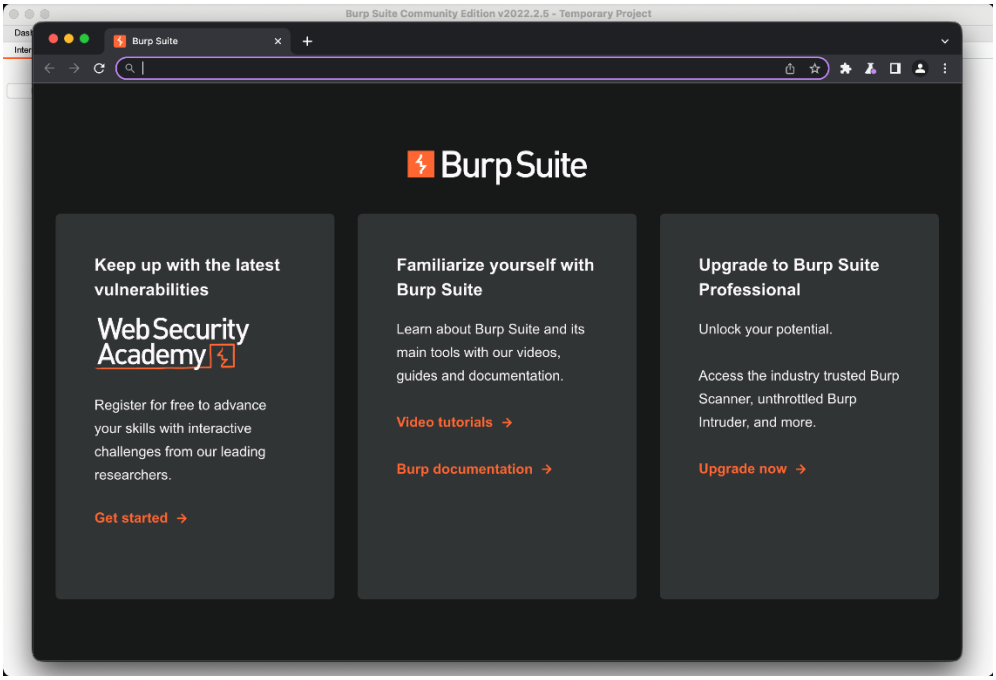
Pantalla para abrir el navegador de pruebas



Nota. En este apartado de proxy abrí el navegador de pruebas.

Figura 3

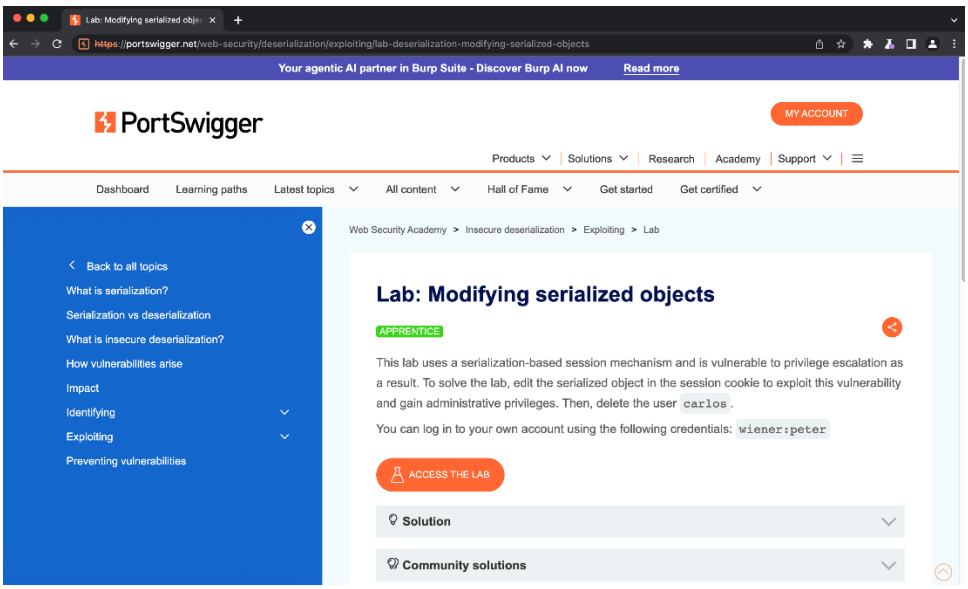
Navegador de Burp Suite



Nota. Es el navegador propio de la herramienta.

Figura 4

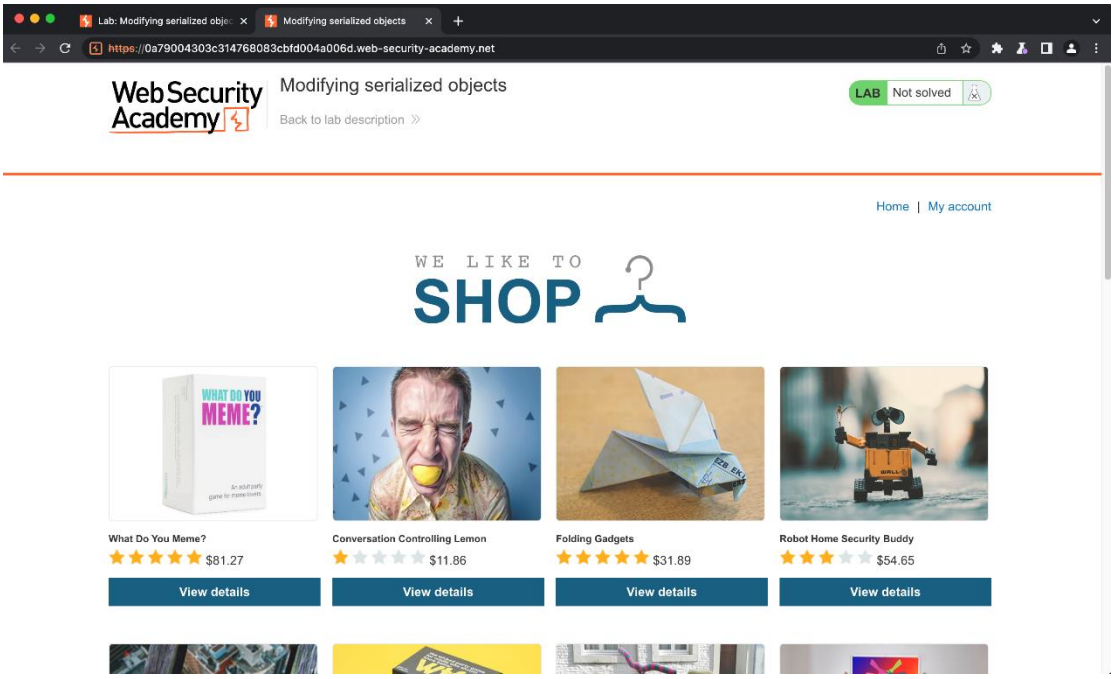
Pagina del lavoratorio



Nota. Entre a la liga del laboratorio e inicie sesión con mi cuenta de la aplicación.

Figura 5

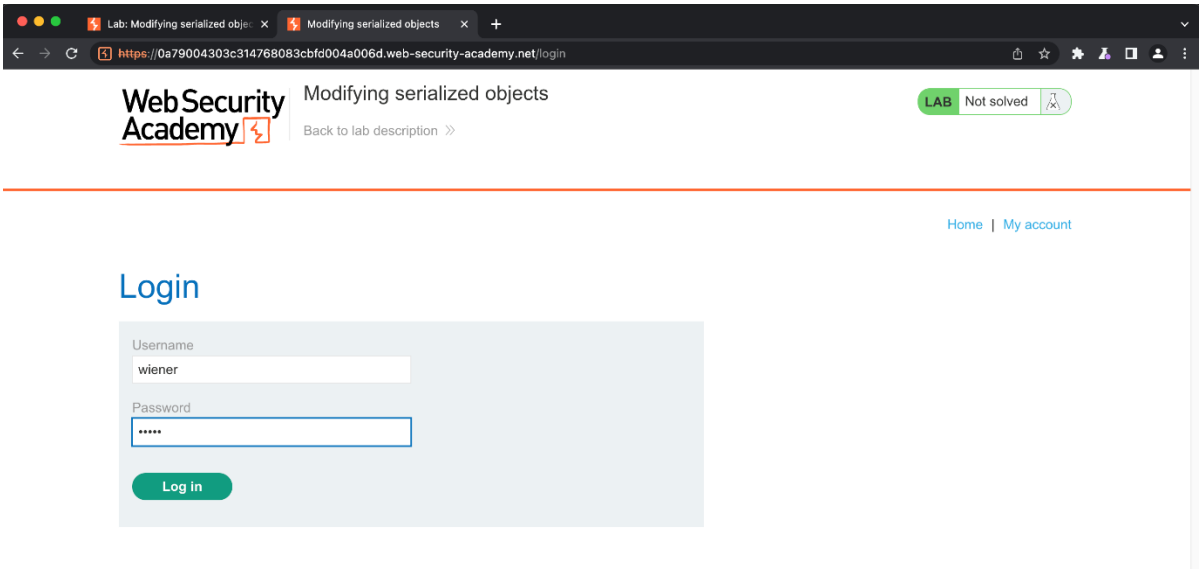
Entrar a la practica del laboratorio



Nota. Esta es la ventana principal de la practica.

Figura 6

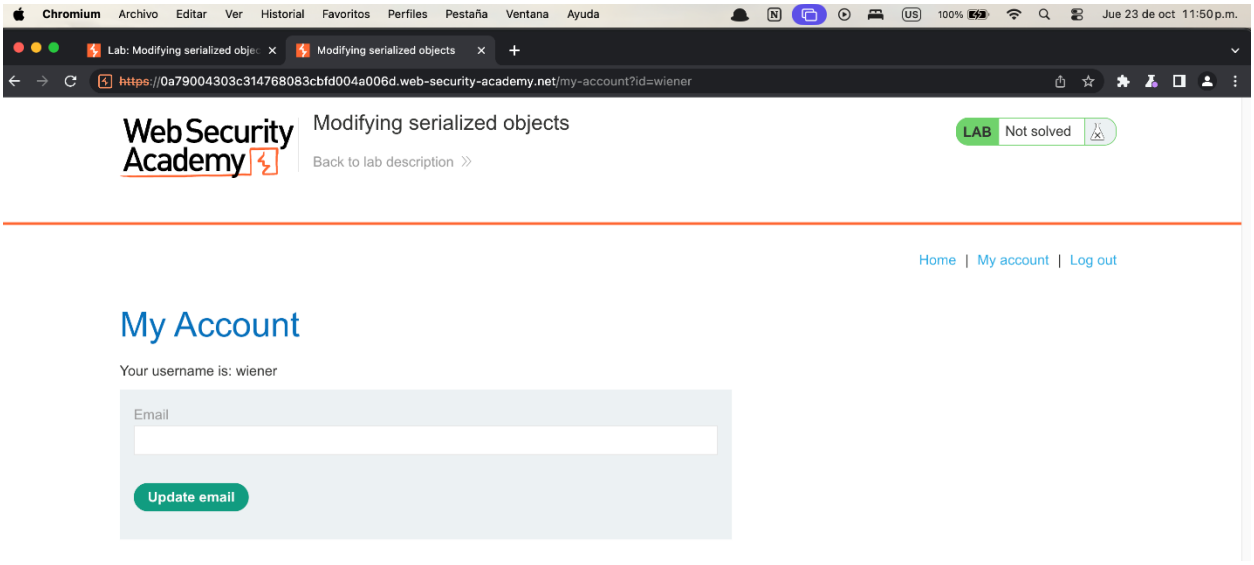
Login con las credenciales



Nota. Use el login con las credenciales que nos da la actividad.

Figura 7

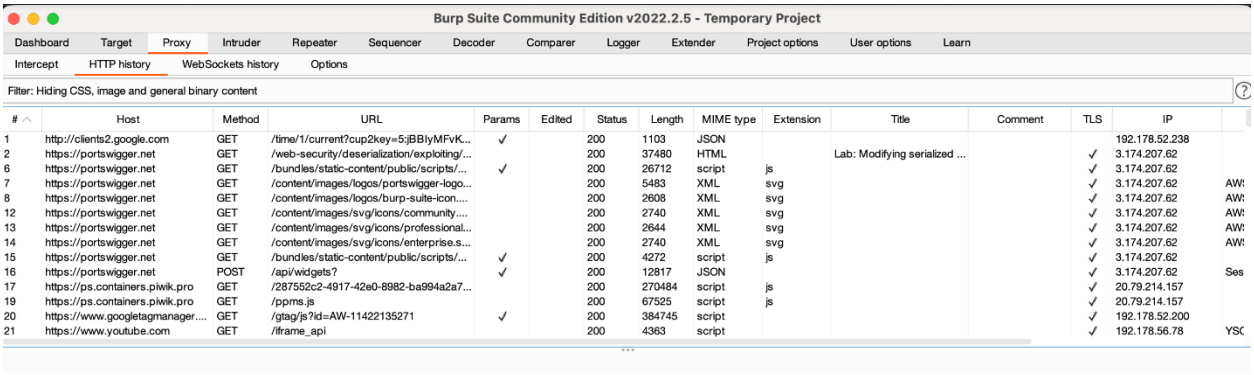
Pantalla de inicio



Nota. Nos manda a esta ventana y tenemos que pasarnos a nuestra herramienta.

Figura 8

Interceptamos la petición

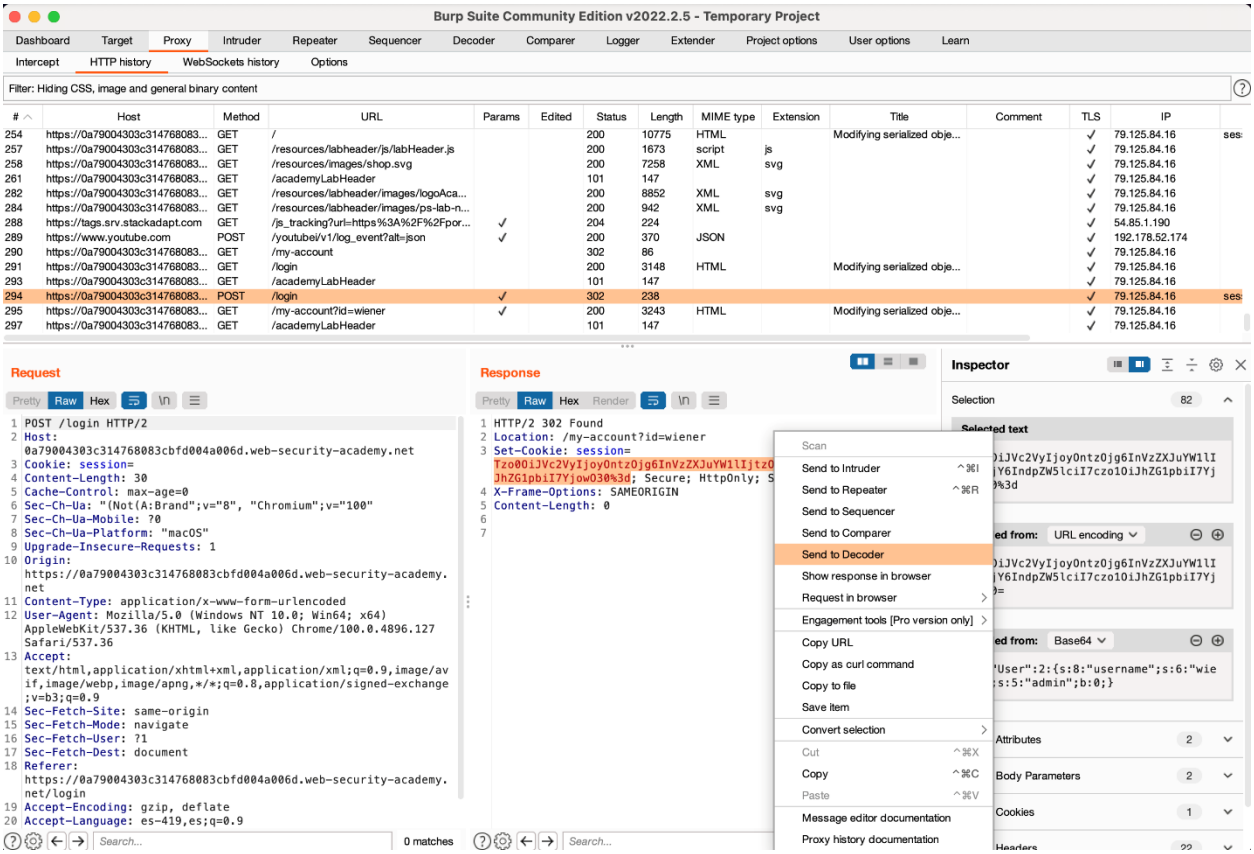


#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	
1	http://clients2.google.com	GET	/time/1/current?cup2key=5:jBBlyMFvK...	✓		200	1103	JSON					192.178.52.238	
2	https://portswigger.net	GET	/web-security/deserialization/exploiting/...			200	37480	HTML		Lab: Modifying serialized ...		✓	3.174.207.62	
6	https://portswigger.net	GET	/bundles/static-content/public/scripts/...	✓		200	26712	script	js			✓	3.174.207.62	
7	https://portswigger.net	GET	/content/images/logos/portswigger-logo...			200	5483	XML	svg			✓	3.174.207.62	AW
8	https://portswigger.net	GET	/content/images/logos/burp-suite-icon....			200	2608	XML	svg			✓	3.174.207.62	AW
12	https://portswigger.net	GET	/content/images/svg/icons/community....			200	2740	XML	svg			✓	3.174.207.62	AW
13	https://portswigger.net	GET	/content/images/svg/icons/professional...			200	2644	XML	svg			✓	3.174.207.62	AW
14	https://portswigger.net	GET	/content/images/svg/icons/enterprise.s...			200	2740	XML	svg			✓	3.174.207.62	AW
15	https://portswigger.net	GET	/bundles/static-content/public/scripts/...	✓		200	4272	script	js			✓	3.174.207.62	
16	https://portswigger.net	POST	/api/widgets?	✓		200	12817	JSON				✓	3.174.207.62	Ses
17	https://ps.containers.piwik.pro	GET	/287552c2-4917-42e0-8982-ba994a2a7...			200	270484	script	js			✓	20.79.214.157	
19	https://ps.containers.piwik.pro	GET	/ppms.js			200	67525	script	js			✓	20.79.214.157	
20	https://www.googletagmanager....	GET	/gtag/js?id=AW-11422135271	✓		200	384745	script				✓	192.178.52.200	
21	https://www.youtube.com	GET	/iframe_api			200	4363	script				✓	192.178.56.78	YSC

Nota. Buscamos la petición de login por el método de post.

Figura 9

Mandar al decoder



Nota. Encontramos la petición, seleccionamos la cookie que es lo rojo y lo mandamos a decoder.

Figura 10

Pasamos a URL

Nota. Decodeamos a url..

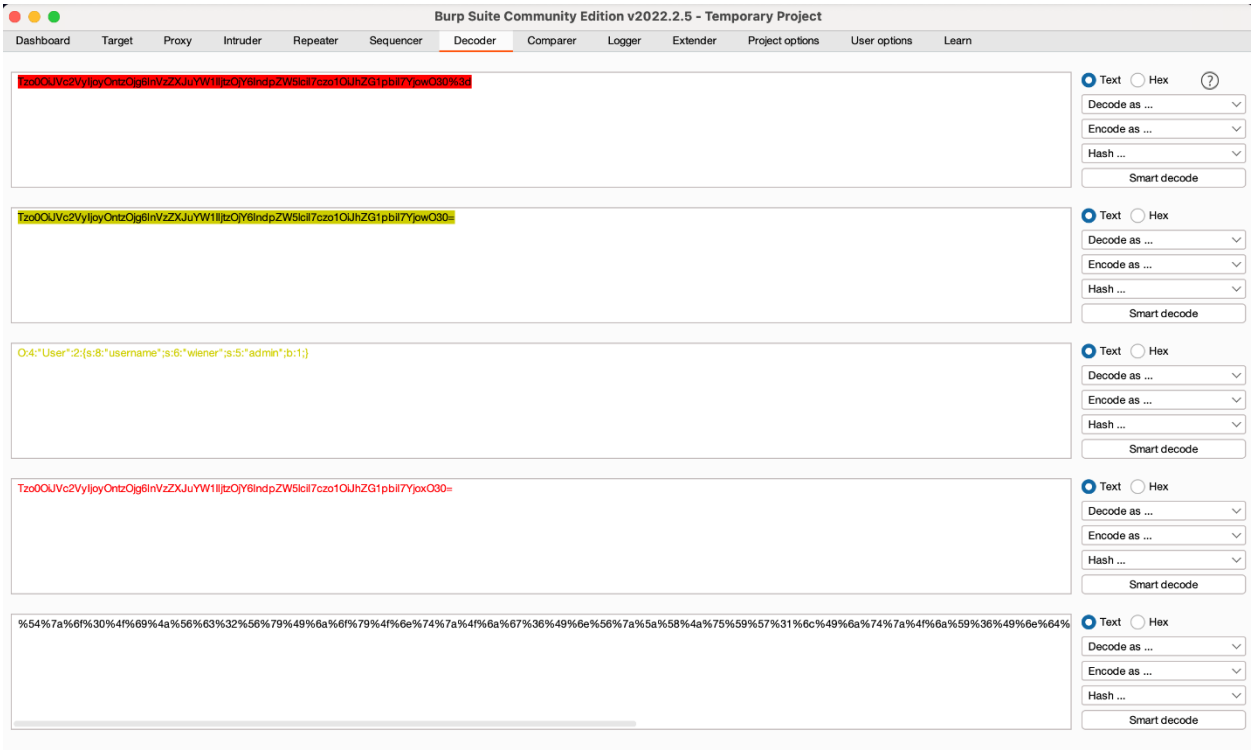
Figura 11

Decodeamos a base 64 y cambiamos nuestros permisos

Nota. Decodeamos a base 64 y cambiamos permisos de 0 a 1 que son permisos de administrador.

Figura 12

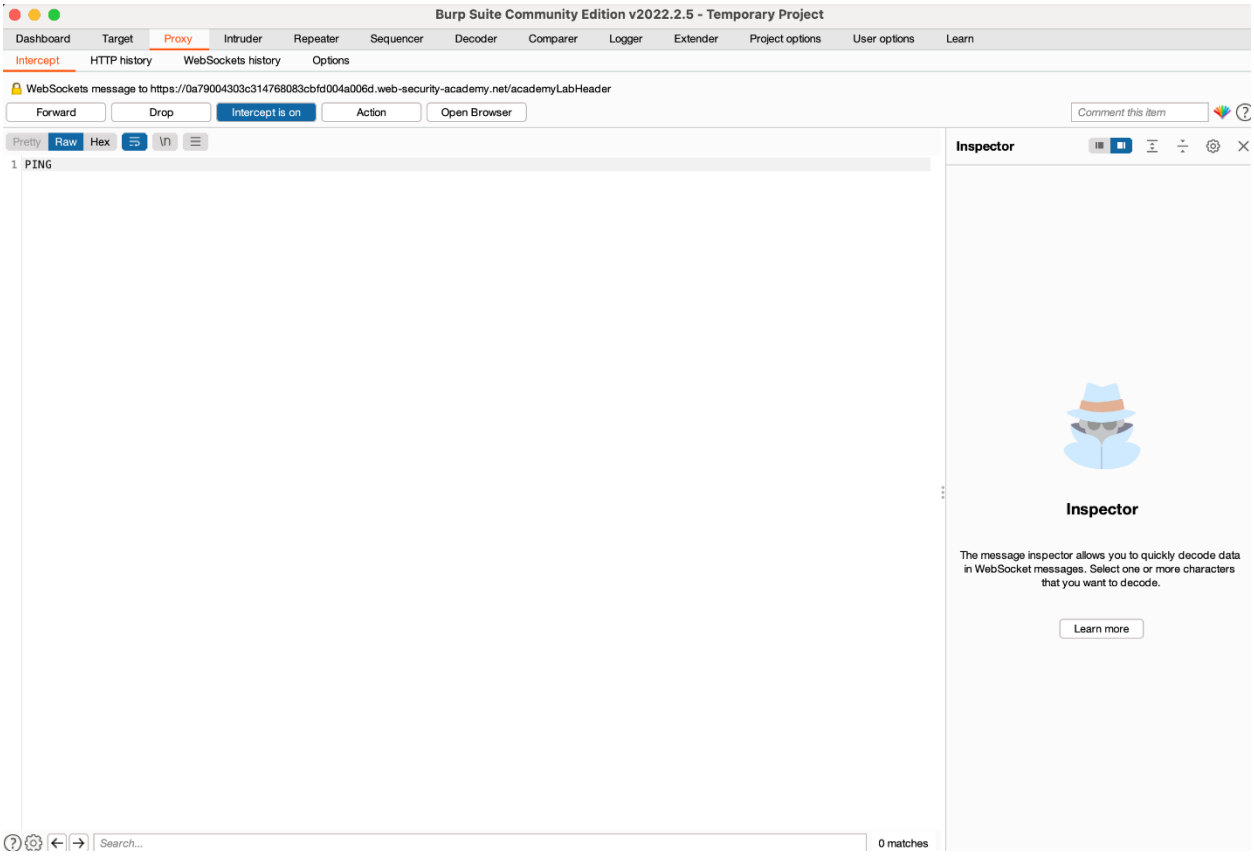
Inversa a nuestra respuesta



Nota. Volvemos a construir nuestra respuesta pasándola a base 64 después url.

Figura 13

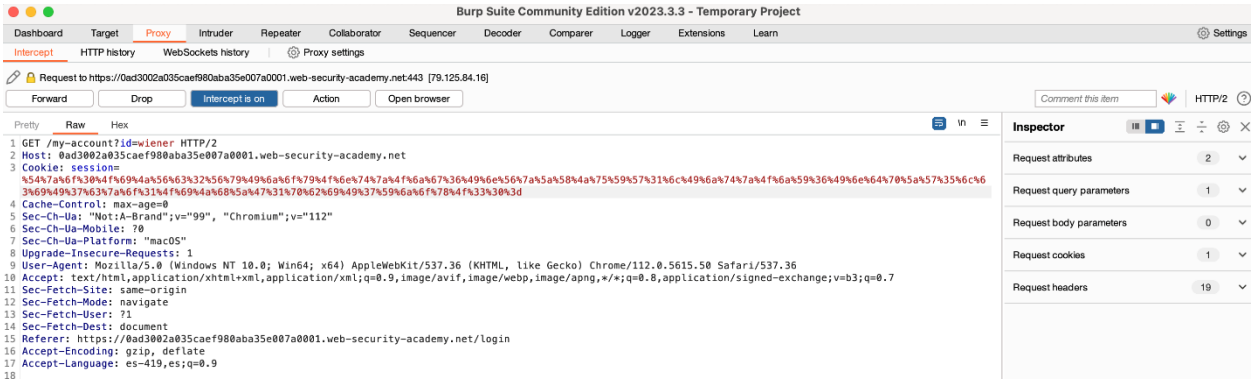
Interceptamos la respuesta



Nota. Nos regresamos a proxy, interceptamos la respuesta recargando el navegador.

Figura 14

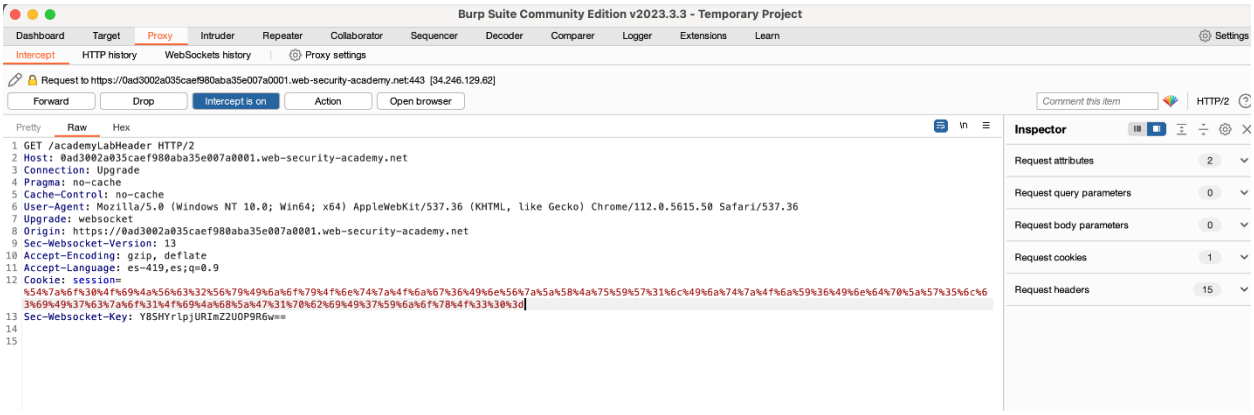
Cambiamos la cooki



Nota. Cambiamos la cooki de la sesión por la que construimos nosotros así podremos avanzar.

Figura 15

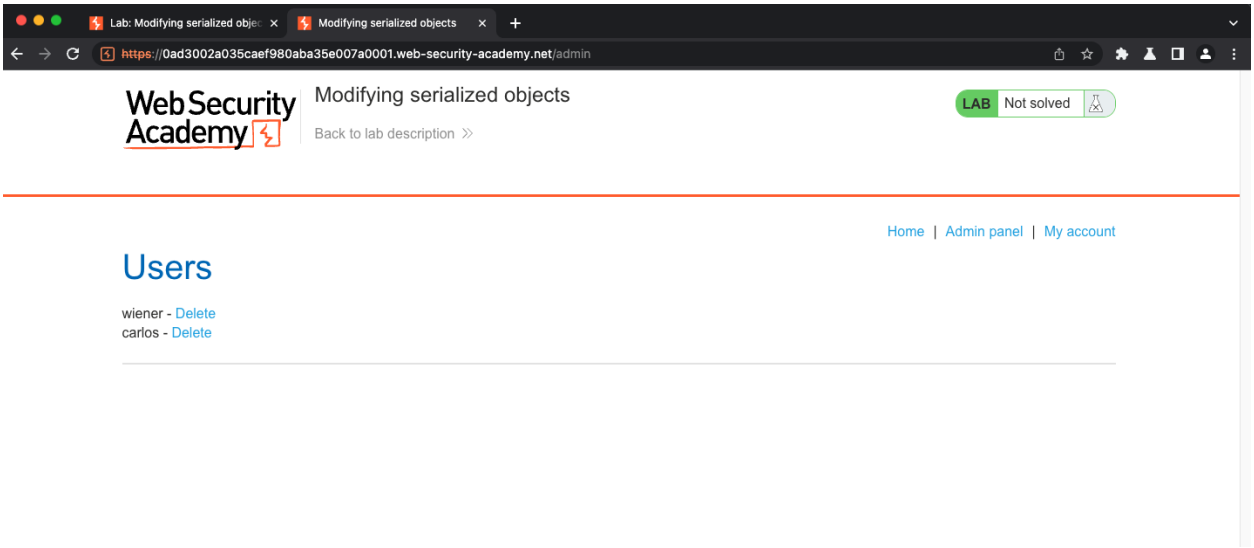
Cambiamos la cooki



Nota. Esta intercepción es lo mismo por ejemplo cuando vemos la lista de usuarios y eliminamos a Carlos.

Figura 16

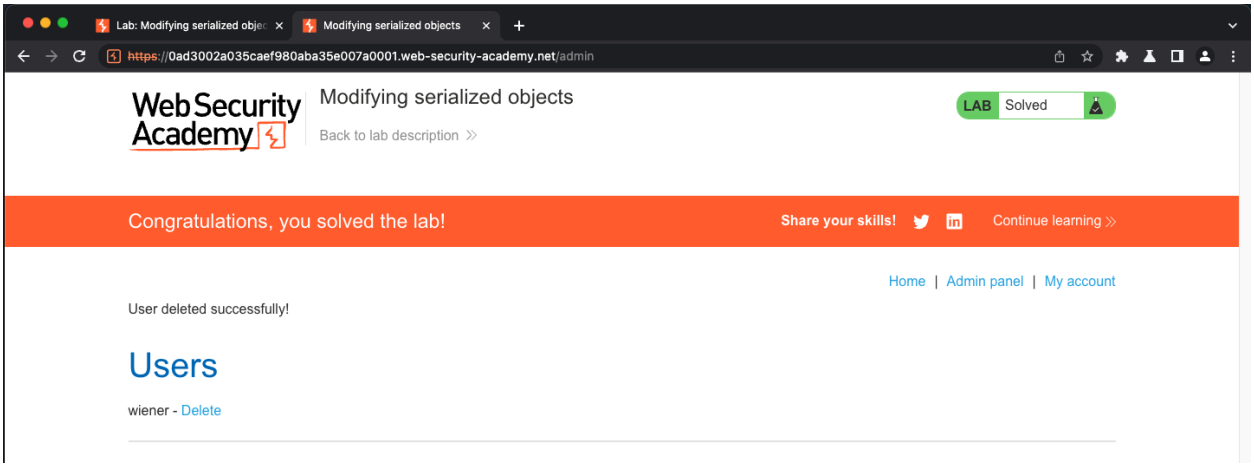
Cambiamos la cooki



Nota. En esta parte es donde vemos los usuarios y eliminamos a Carlos claro con nuestra cooki cambiada.

Figura 17

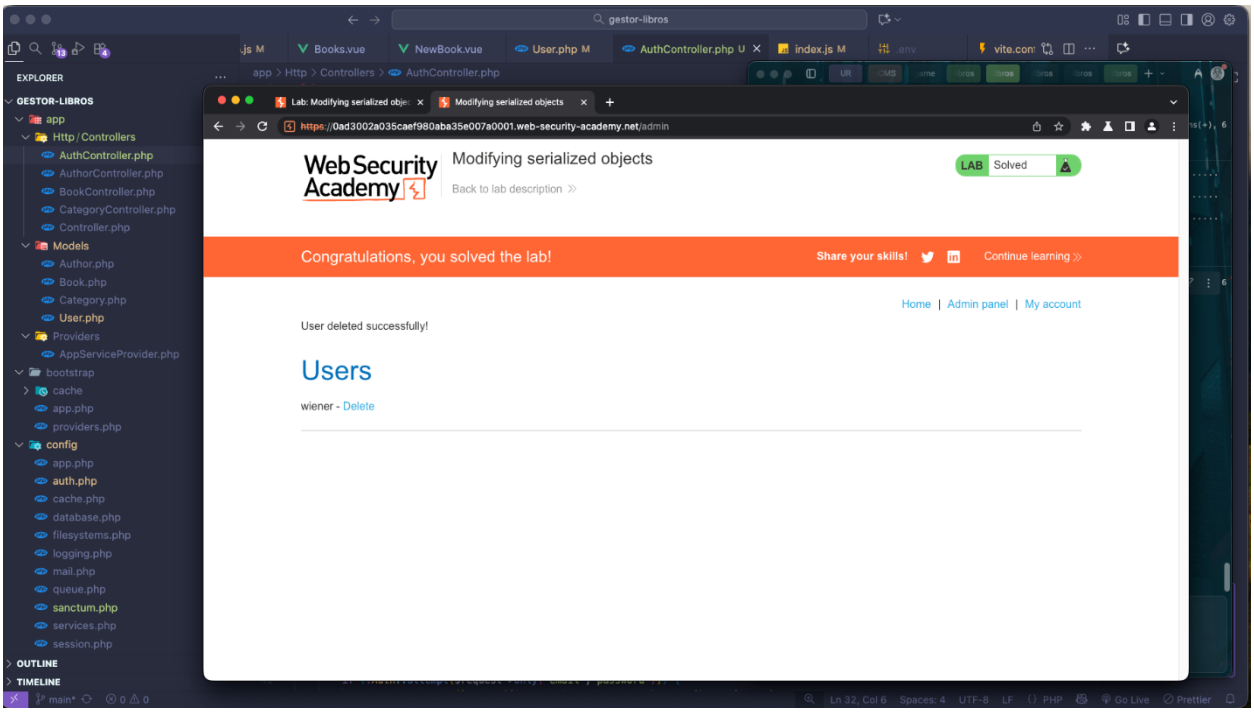
Usuario eliminado y laboratorio completo



Nota. Una vez eliminado se completa el laboratorio y cambia el status a solvet ya que se cumple.

Figura 17

Pantalla completa para que se aprecie que si es mi PC



Nota. Una captura completa para que se aprecie que si se resolvió el laboratorio.

Referencias

https://github.com/CardinalSG/JonathanCardenasAplicacionesBiometricas

Me dio unos errores pero las 3 actividades están en este repo, cuando solucione el problema las cambiare a su propio repo.