Universidad Corporativa Coppel | Programas Académicos

Ingeniería en Desarrollo de Software

Actividad | 3 | Cross Site Scripting

(XSS)

Auditoría Informática

Ingeniería en Desarrollo de Software

academia global

TUTOR: Jessica Hernández Romero

ALUMNO: Christian Ibarra Corrales

FECHA: 23 de junio de 2025

Introducción

La seguridad informática es un componente esencial en el desarrollo y mantenimiento de aplicaciones web. En esta actividad se aborda una de las vulnerabilidades más comunes y peligrosas: el Cross Site Scripting (XSS). Esta amenaza permite que un atacante inyecte scripts maliciosos en páginas web vistas por otros usuarios, pudiendo robar información confidencial como credenciales, cookies o sesiones. A través del uso de Burp Suite y un sitio previamente subido en la primera actividad, se realizará una prueba de concepto para demostrar cómo puede explotarse esta vulnerabilidad para interceptar datos de inicio de sesión. Esta práctica tiene como objetivo sensibilizar sobre los riesgos reales que enfrentan los sistemas sin medidas de protección adecuadas y permite entender mejor la importancia de validar entradas, proteger formularios y aplicar buenas prácticas de codificación. Además, refuerza la necesidad de realizar auditorías constantes para identificar fallos antes de que puedan ser explotados. El conocimiento adquirido contribuirá directamente a prevenir ataques reales y a implementar sistemas más seguros.

Descripción

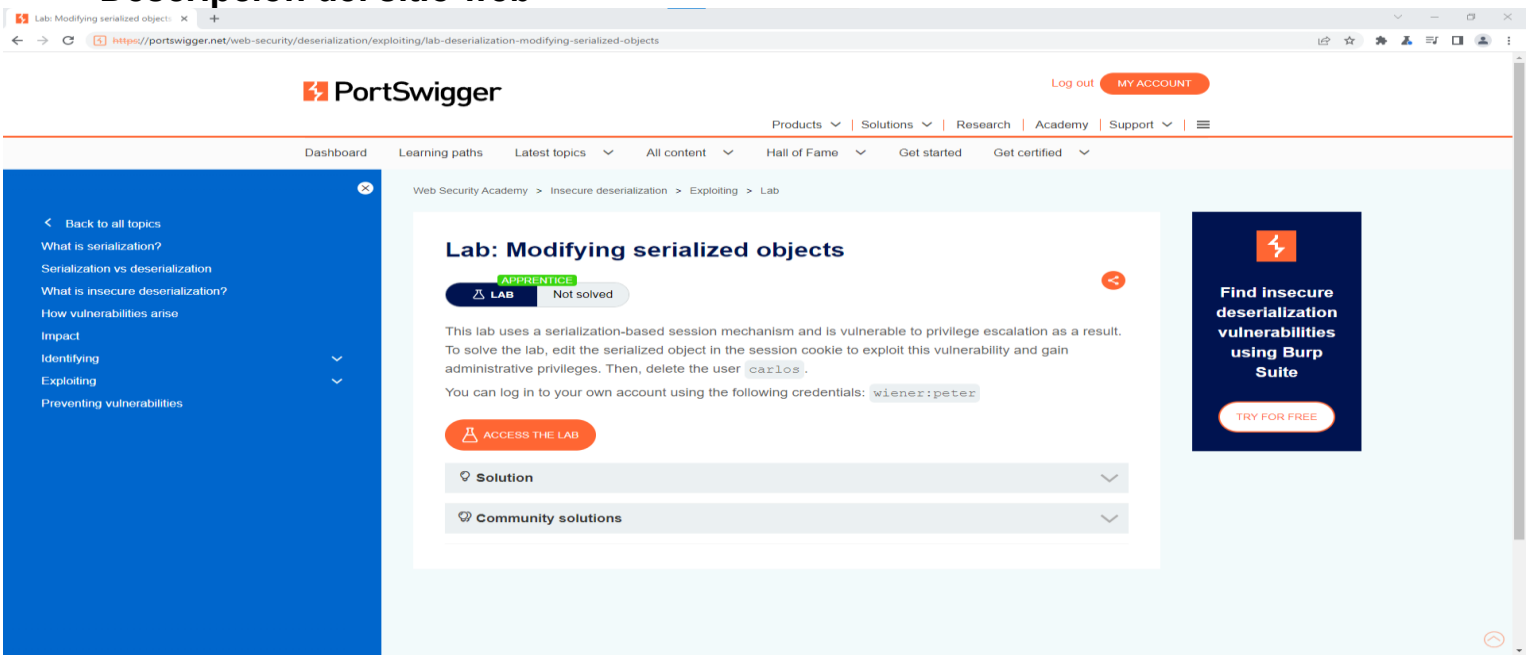
La actividad se enfoca en una prueba de vulnerabilidad basada en Cross Site Scripting (XSS), una técnica que permite ejecutar scripts maliciosos dentro del navegador de la víctima. Este tipo de ataques son especialmente peligrosos porque permiten robar información sensible como contraseñas, nombres de usuario, tokens de sesión, e incluso tomar el control de la cuenta de un usuario sin su conocimiento. En este escenario, se utiliza el software Burp Suite para interceptar y modificar peticiones HTTP generadas por un sitio web previamente creado. Se analizan los formularios de inicio de sesión, con el objetivo de capturar y alterar credenciales, simulando cómo un atacante podría utilizar esta brecha para comprometer la seguridad del sistema. Mediante este análisis se demuestra que, si un sitio no cuenta con validaciones adecuadas del lado del servidor y cliente, puede ser explotado fácilmente. Esta práctica, además de ser formativa, sirve como advertencia para administradores y desarrolladores sobre la necesidad de implementar políticas de seguridad robustas.

Justificación

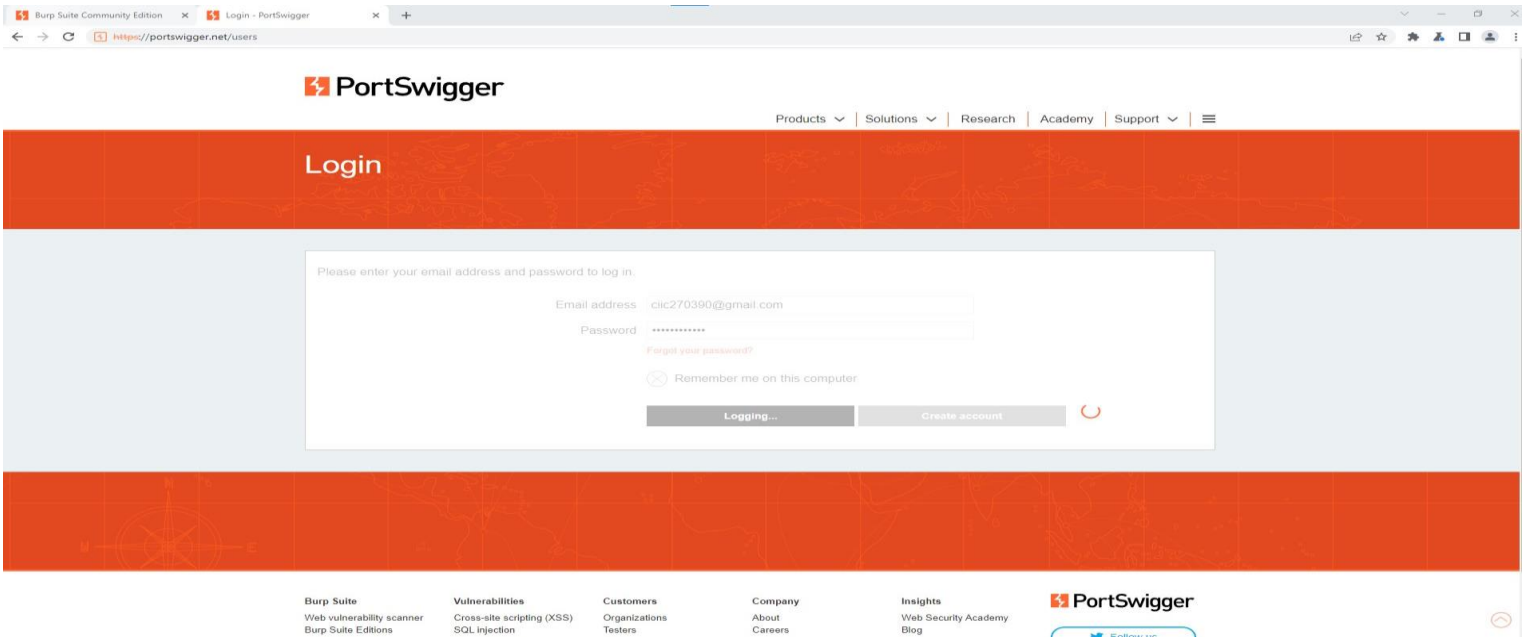
La realización de esta actividad sobre Cross Site Scripting (XSS) es fundamental para entender cómo pueden ser vulneradas las aplicaciones web y qué medidas se deben tomar para prevenirlo. Al simular un ataque real, se obtienen conocimientos prácticos sobre el funcionamiento de herramientas como Burp Suite y sobre los puntos débiles que pueden presentarse en el desarrollo de sistemas. Justificar el uso de estas pruebas radica en que permiten adelantarse a los posibles ataques externos, brindando la oportunidad de reforzar la seguridad antes de que un ciberdelincuente explote dichas debilidades. Este tipo de auditorías no solo protegen los datos sensibles de los usuarios, sino que también preservan la integridad y reputación de las organizaciones. Además, son parte clave del ciclo de vida del software seguro, ya que permiten validar que las medidas de protección como la sanitización de entradas, la codificación adecuada y el uso de cabeceras de seguridad estén siendo aplicadas correctamente. En conclusión, esta práctica es necesaria, relevante y alineada con los objetivos de la ciberseguridad actual.

Etapa 1

- **Descripción del sitio web**

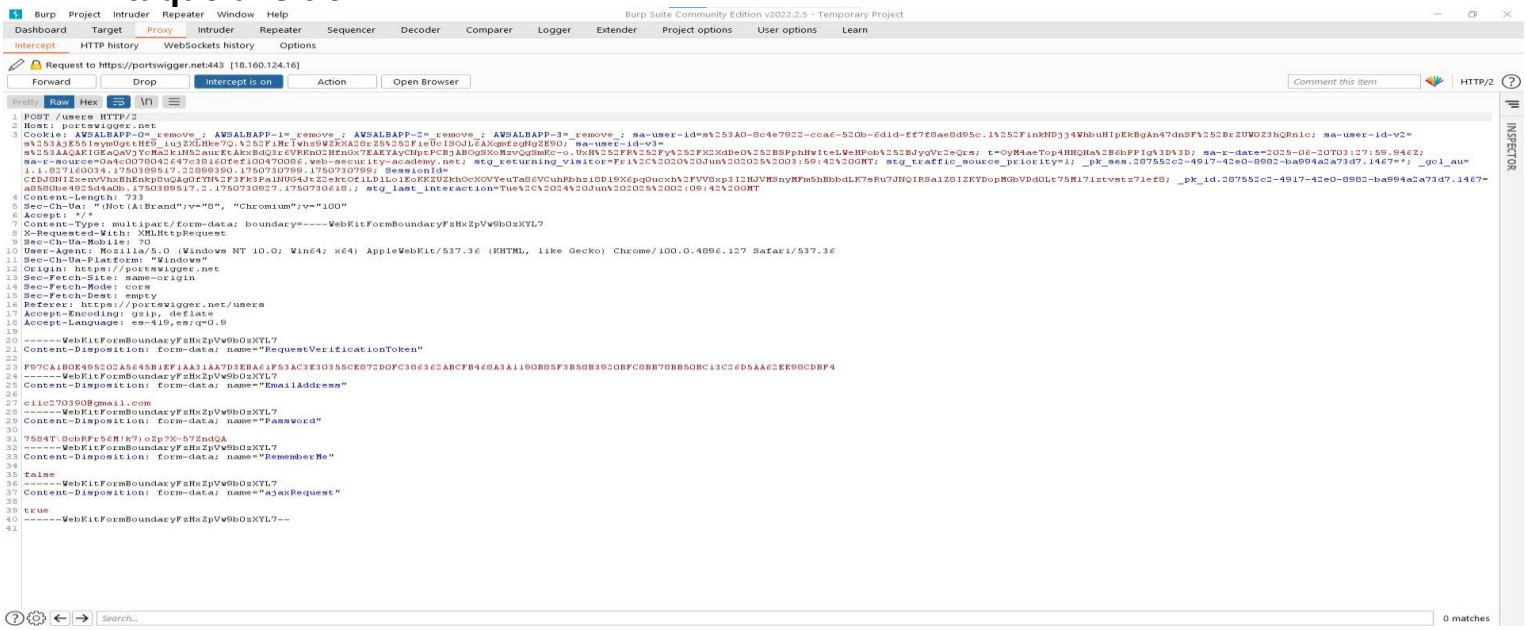


Aquí presentamos la actividad para dar nuestros siguientes ataques en los enlaces de laboratorio de trabajo.
https://portswigger.net/web-security/deserialization/exploiting/lab-deserialization-modifying-serialized-objects
En la actividad 1 y 2 vimos los diferentes tipos de ataques o exploits de contraseñas. Lamentablemente en la actividad no pude demostrar el ataque con el programa WireShark ya que tengo bloqueo por Windows 10 y su profeso de Microsoft ARK de protección.



Aquí iniciaremos con el correo y contraseña para poder usar este servicio para que nos brinde lo que se no está pidiendo.

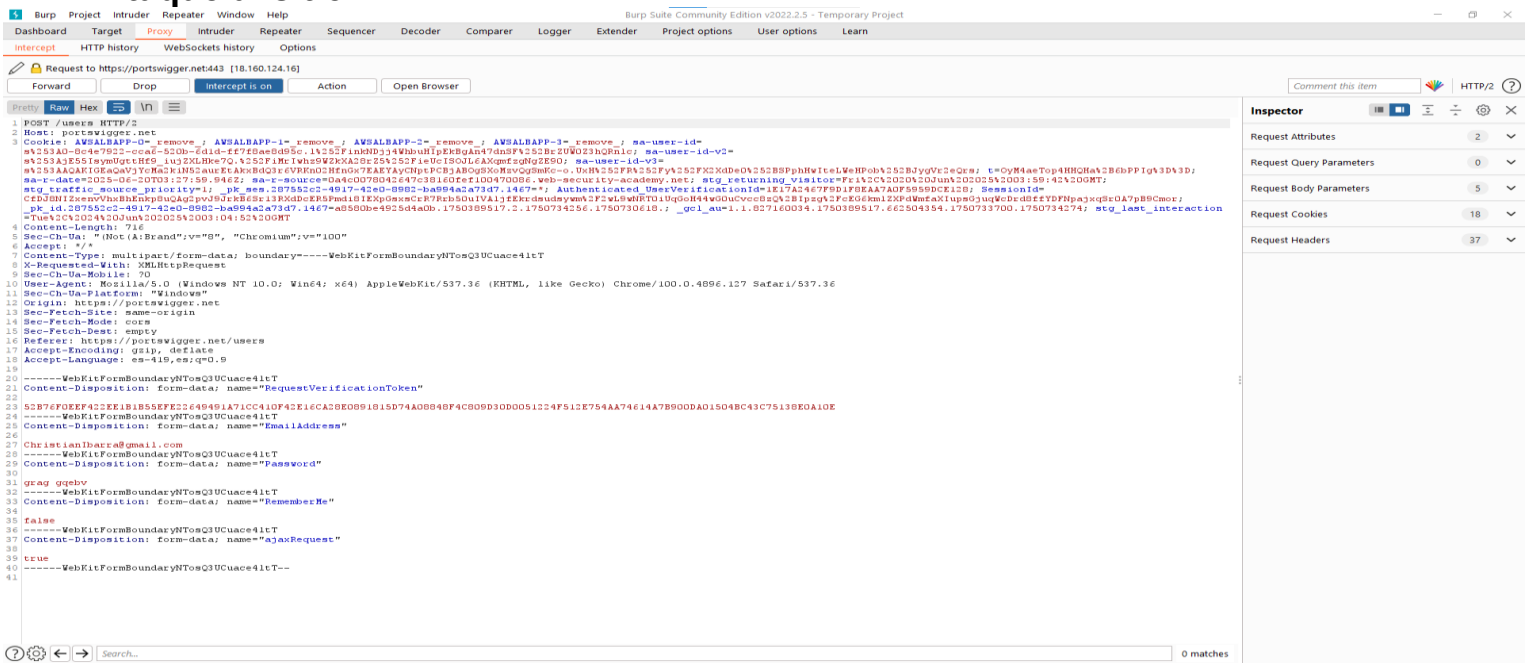
- **Ataque al sitio**



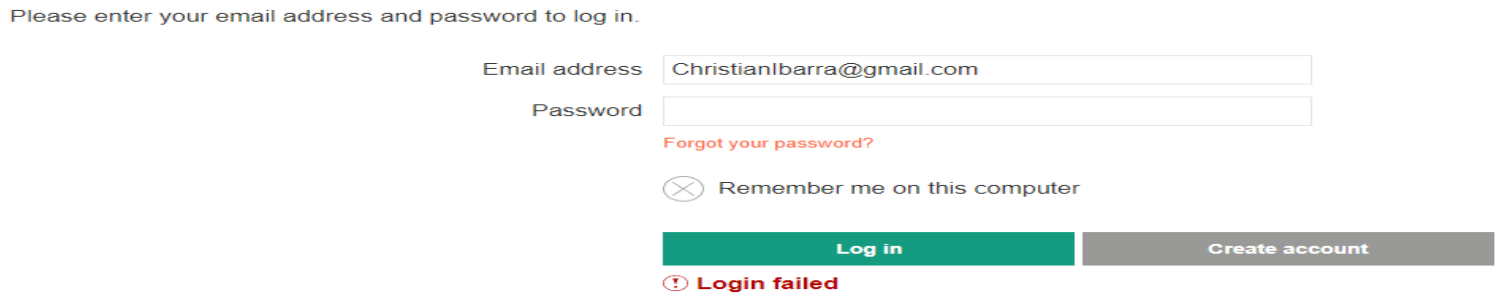
Aquí en el primer ataque seria con las credenciales correctas para iniciar al laboratorio del trabajo mostrando correo: ciic270390@gmail.com y la contraseña: 75S4T\8cbRFr56M!k7)oZp?X~57ZndQA

Etapa 2

- **Ataque al sitio**



Mostrando las credenciales incorrectas en esta etapa de ataque.

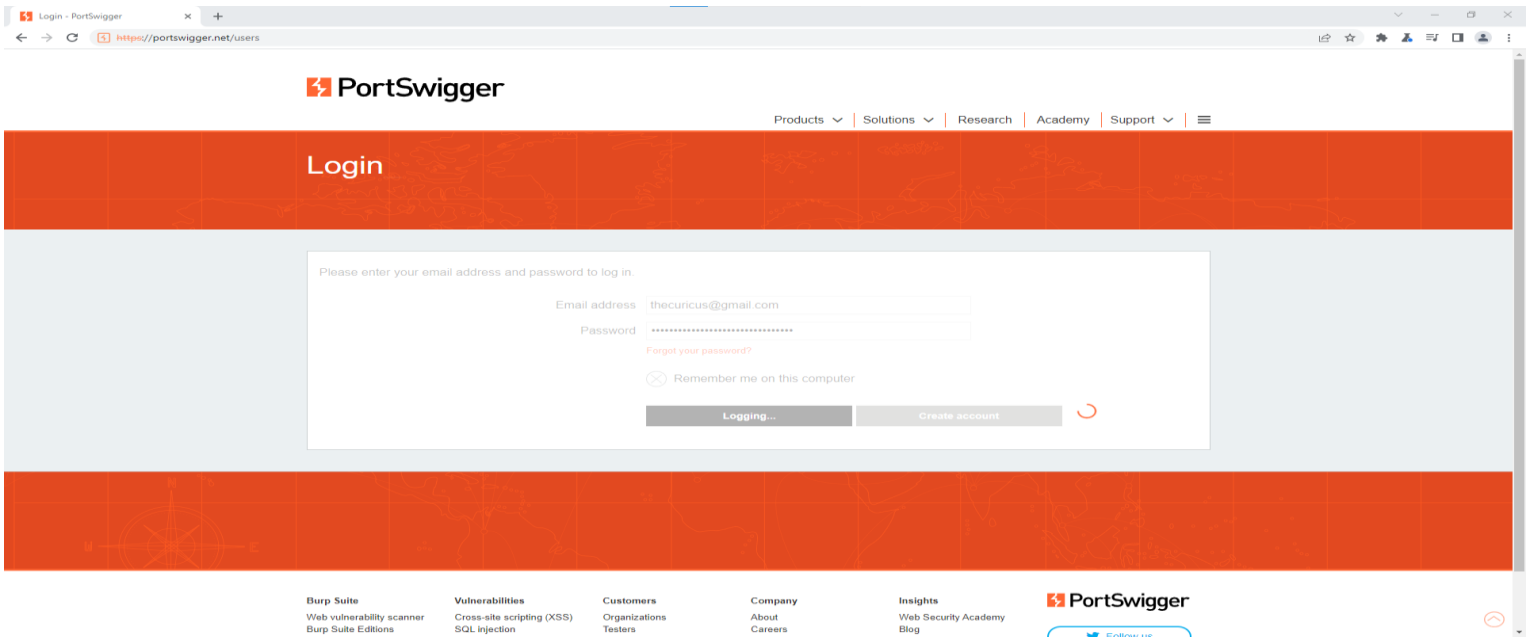


Aquí en el laboratorio del trabajo mostrando que es la información indicada.

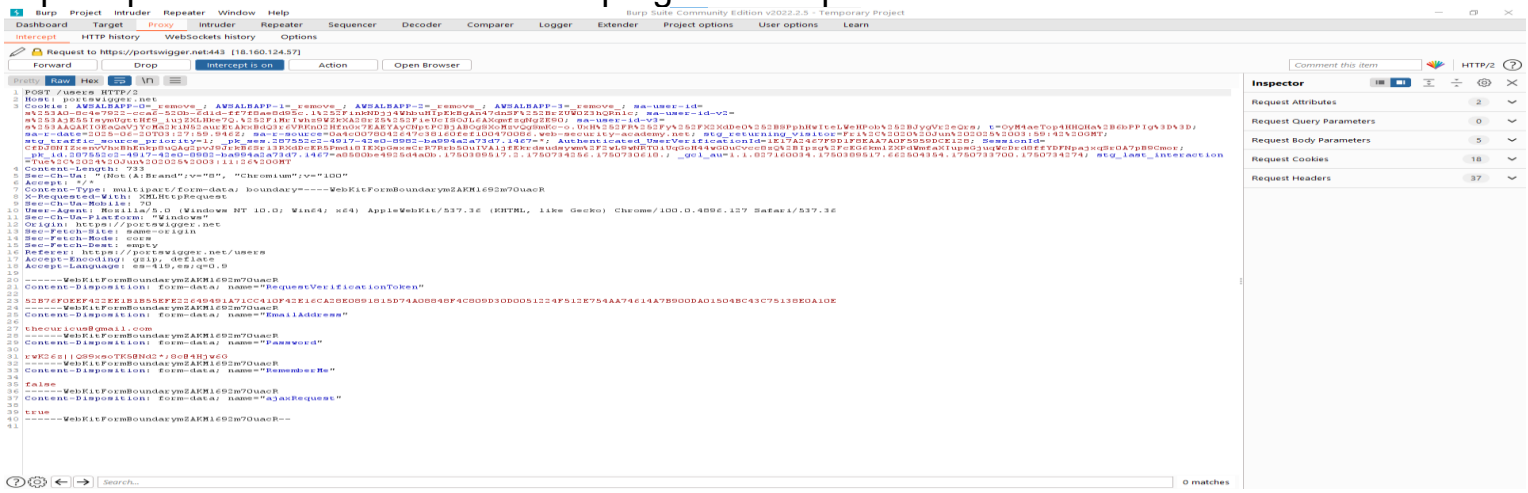
Etapa 3

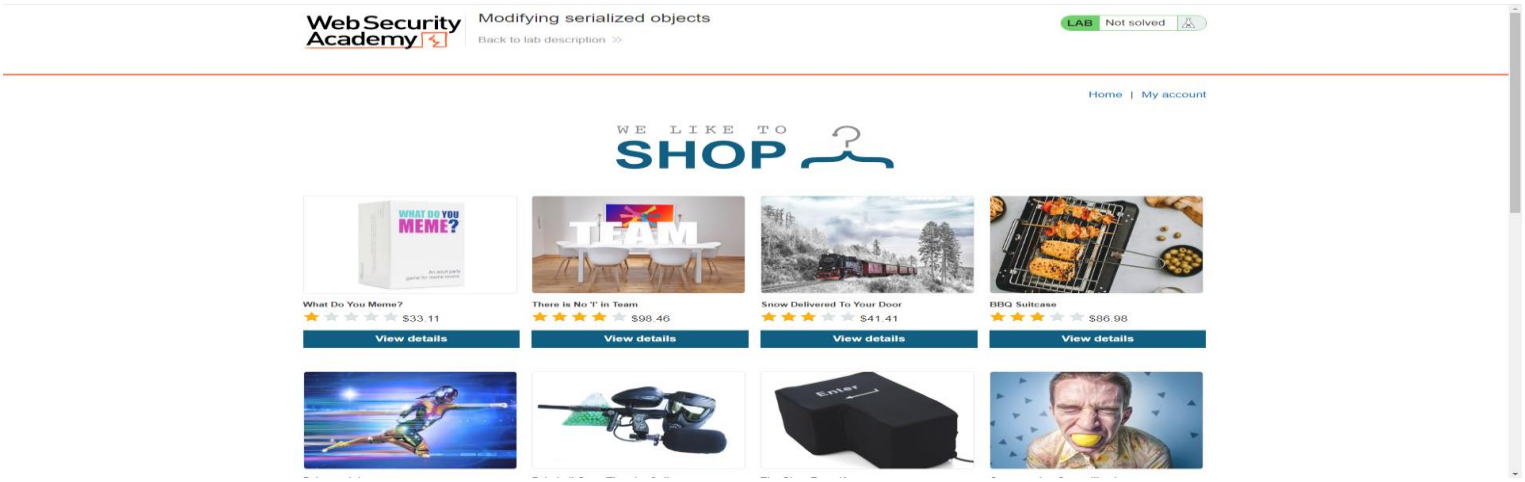
Ataque al sitio

:

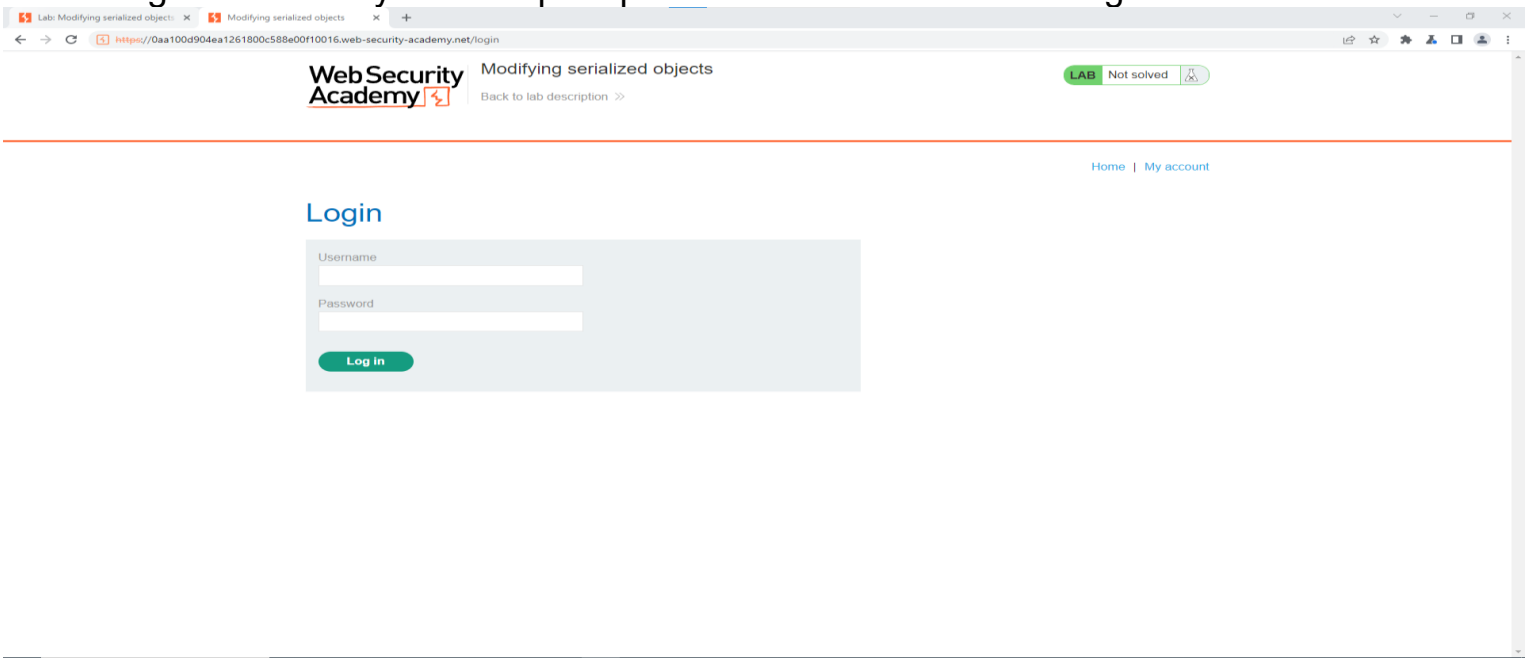


Aquí mostrando con otro correo electrónico: thecurricus@gmail.com
Contraseña: rwK26z||QS9xsoTK5@Nd2*;8c@4Hjw6G
Aquí capturando la información en el programa Burp Suite:





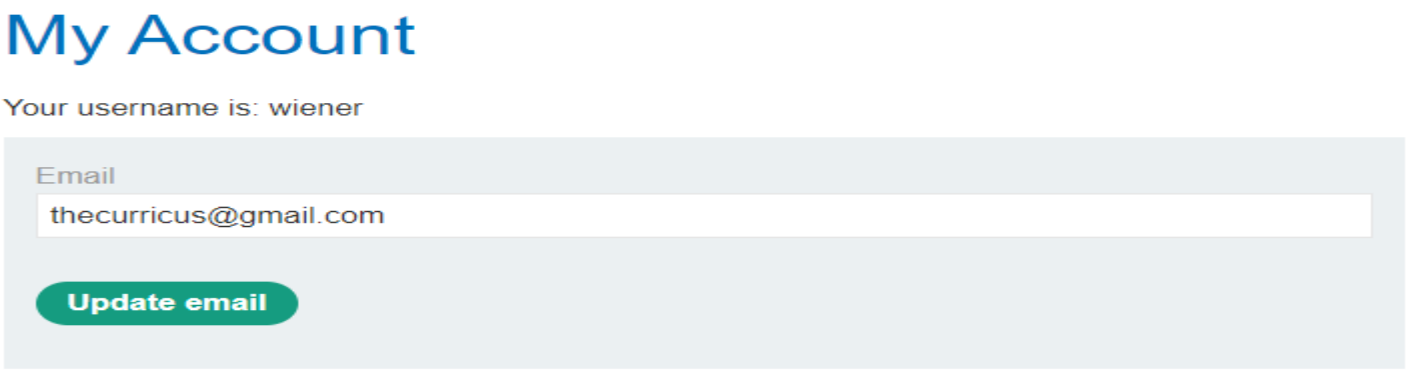
En la siguiente entraremos en modo administrador para dar con la información recopilada, damos siguientes en My account para poder brindar la información siguiente.



Aquí iniciaremos con los datos de administración:
Usuario: wiener
Contraseña: peter
Igual recopilaremos dicha información en el programa.

```
POST /login HTTP/2
Host: 0aa100d904ea1261800c588e00f10016.web-security-academy.net
Cookie: session=
Content-Length: 30
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="100"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0aa100d904ea1261800c588e00f10016.web-security-academy.net
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aa100d904ea1261800c588e00f10016.web-security-academy.net/login
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9

username=wiener&password=peter
```



Actualizaremos el correo en modo administrador.

```
POST /my-account/change-email HTTP/2
Host: 0aa100d904ea1261800c588e00f10016.web-security-academy.net
Cookie: session=Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjowO30%3d
Content-Length: 29
Cache-Control: max-age=0
Sec-Ch-Ua: "(Not(A:Brand";v="8", "Chromium";v="100"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://0aa100d904ea1261800c588e00f10016.web-security-academy.net
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
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://0aa100d904ea1261800c588e00f10016.web-security-academy.net/my-account?id=wiener
Accept-Encoding: gzip, deflate
Accept-Language: es-419,es;q=0.9

email=thecurricus%40gmail.com
```

Aquí se muestra la información de cambio de correo.
Con eso concluimos como recopilar y modificar dichos datos que se nos muestren.

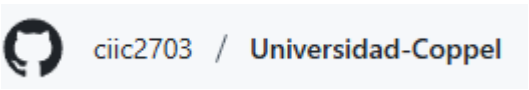
Conclusión

La actividad realizada sobre Cross Site Scripting (XSS) permitió evidenciar los riesgos que enfrentan las aplicaciones web sin una seguridad adecuada. A través del uso de Burp Suite, se demostró cómo un atacante puede capturar y modificar datos sensibles durante el proceso de autenticación. Esta práctica reafirma la importancia de realizar pruebas de penetración como parte de una auditoría informática integral. Entender cómo funcionan estas vulnerabilidades y cómo se pueden explotar permite desarrollar habilidades para prevenirlas de manera efectiva. En el ámbito profesional, estas competencias son indispensables, ya que las organizaciones dependen cada vez más de plataformas digitales que deben ser seguras, confiables y robustas. En la vida cotidiana, este conocimiento también es útil, pues ayuda a identificar sitios potencialmente peligrosos y a adoptar prácticas más seguras al navegar. Finalmente, se concluye que invertir en la seguridad desde el diseño y durante todo el desarrollo de un sistema no solo previene pérdidas económicas, sino también protege la confianza de los usuarios y la continuidad del negocio.

Referencias

Tutorías

https://academiaglobal-mx.zoom.us/rec/play/I-7kfYOJkyuY9jUG6jiwP5cL48pjCBsAYvNZHzL6uZQi3PSAc4YhCKEXCvJuXrzfKd6ia0p9EpedWiSa.yAQSAzijc4PVTLrU?eagerLoadZvaPages=sidemenu.billing.plan_management&accessLevel=meeting&canPlayFromShare=true&from=share_recording_detail&continueMode=true&componentName=rec-play&originRequestUrl=https%3A%2F%2Facademiaglobal-mx.zoom.us%2Frec%2Fshare%2F5meRQOidp7pJ0sXIhn1I3FEVhrE1pqr4x3BX0OwXwFOSd3FJt2AiZYuYnnNDtQhG.YzPBcX0P-6nv47qQ



https://github.com/ciic2703/Universidad-Coppel/tree/main/Auditor%C3%ADa%20Inform%C3%A1tica