

## Actividad [3] - [- Cross Site Scripting (XSS)-]

### [Auditoría Informática]

## Ingeniería En Desarrollo De Software

Tutor: Jessica Hernández Romero

Alumno: Josué de Jesús Laveaga Valenzuela

Fecha: 15/10/2023

## **INDICE**

Introducción.....	1
Interpretación y Argumentación Del texto solicitado.....	1.1
Justificación .....	1.2
Actividades 1 y 2 .....	2
Ataque Cibernetico.....	3-8
Referencias/Conclusion.....	9

# Introducción

La seguridad informática es un campo en constante evolución que enfrenta desafíos crecientes debido a la expansión del uso de la tecnología. Entre las amenazas más prominentes se encuentra el Cross Site Scripting (XSS), una vulnerabilidad común y peligrosa que puede comprometer la seguridad de sitios web y la privacidad de los usuarios. Esta actividad se centra en abordar esta amenaza crítica y en comprender cómo un atacante podría explotarla para obtener credenciales de usuario. A medida que la web se convierte en una parte esencial de nuestra vida cotidiana, la importancia de abordar y comprender las vulnerabilidades de seguridad, como el XSS, se vuelve más crucial que nunca.

En esta actividad, exploraremos en profundidad las implicaciones de esta vulnerabilidad y cómo se puede abordar de manera ética y controlada. Comprender el XSS es esencial para fortalecer las defensas cibernéticas y garantizar la seguridad de los sistemas y datos. La actividad no solo se centrará en la detección de vulnerabilidades, sino también en la concienciación sobre los riesgos y las mejores prácticas para prevenir futuros ataques.

## Interpretación y Argumentación Del texto solicitado

En el contexto de un mundo cada vez más interconectado y digitalizado, la seguridad informática se ha convertido en una preocupación crítica para individuos, empresas y organizaciones. Entre las amenazas cibernéticas más significativas, el Cross Site Scripting (XSS) emerge como un riesgo tangible y omnipresente. XSS permite a los atacantes inyectar código malicioso en páginas web, lo que a su vez puede llevar a la exposición de datos sensibles, robo de información confidencial y una potencial pérdida de integridad en sistemas y aplicaciones.

En esta actividad, nos adentraremos en el mundo de las vulnerabilidades XSS, explorando en profundidad sus aspectos técnicos y su impacto en la seguridad. Es crucial comprender cómo un atacante podría explotar esta vulnerabilidad, ya que esto arroja luz sobre la necesidad imperiosa de abordarla de manera efectiva. La actividad plantea el desafío de detectar y comprender cómo se pueden capturar credenciales de usuario a través de ataques XSS y, posteriormente, cómo se puede manipular la información para comprobar si es posible la entrada no autorizada.

La finalidad de esta actividad es doble: primero, concienciar sobre la importancia de comprender y prevenir el XSS, y segundo, proporcionar un entorno controlado para experimentar y aprender sobre esta amenaza en lugar de enfrentarla en situaciones no controladas y potencialmente perjudiciales. A través de esta exploración, esperamos que los participantes no solo adquieran conocimientos críticos sobre seguridad informática, sino que también estén mejor preparados para proteger sistemas y datos contra ataques XSS en un mundo digital en constante evolución.

## Justificación

La justificación para emplear esta solución, es decir, la realización de pruebas de vulnerabilidad de XSS, es más pertinente que nunca en el entorno actual. A medida que la tecnología desempeña un papel esencial en nuestras vidas y en las operaciones de las organizaciones, la seguridad de la información es una prioridad crítica. Esta actividad ofrece una oportunidad valiosa para concienciar sobre los riesgos y preparar a profesionales de la seguridad y desarrolladores web para defenderse de amenazas reales.

La realización de pruebas éticas y controladas, como las de XSS, no solo ayuda a identificar vulnerabilidades en sistemas y aplicaciones, sino que también promueve la concienciación sobre las mejores prácticas de seguridad. Además, contribuye a la prevención de ataques cibernéticos que podrían tener graves consecuencias, como la pérdida de datos confidenciales y la exposición de la privacidad de los usuarios.

En un mundo donde la información y la tecnología son activos cruciales, la seguridad informática se convierte en un imperativo. Esta actividad es una parte esencial de ese esfuerzo, ya que ayuda a fortalecer la ciberseguridad y a proteger tanto a los individuos como a las organizaciones de las amenazas en constante evolución.

Actividades 1 y 2 en donde se vio previamente el proceso que básicamente se vera en esta nueva 3er actividad.

Etapa 1 (Pérdida de Autenticación y Gestión de Sesiones)

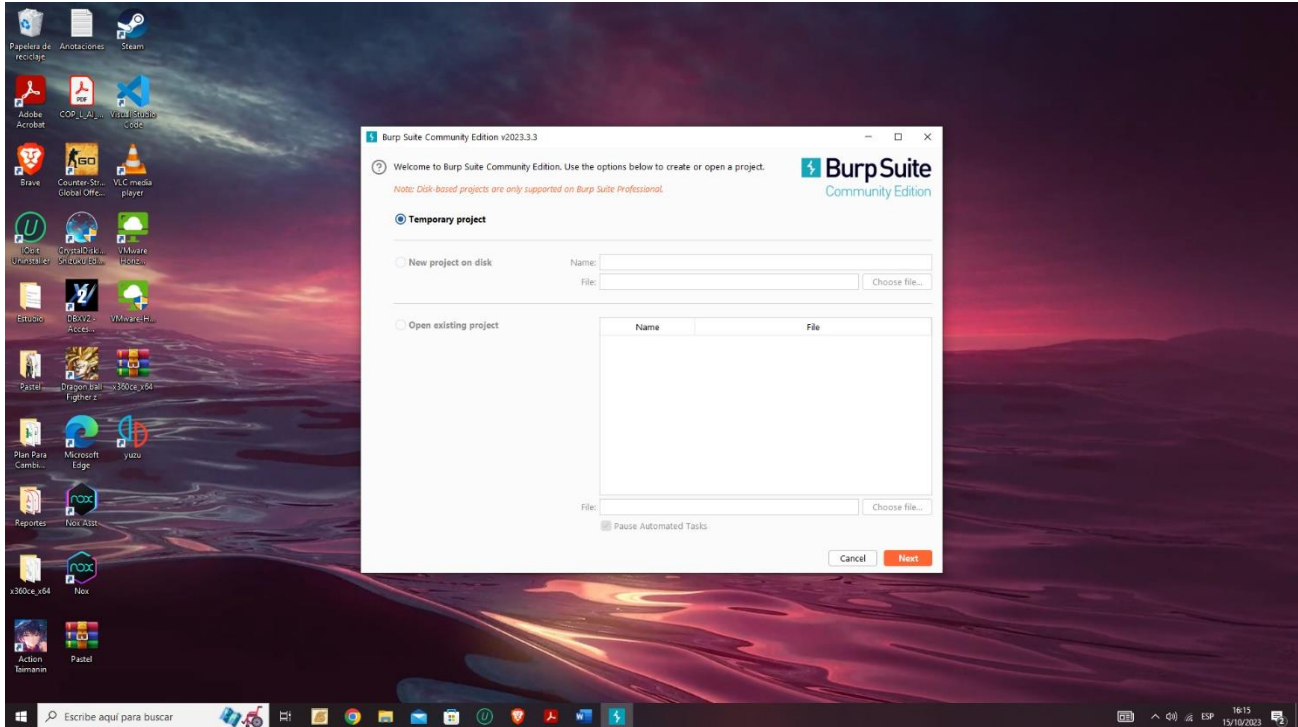
[https://drive.google.com/file/d/1IcJ5HZSFyf2yMoWUS3TC22PoxFHm39pa/view?usp=drive\\_link](https://drive.google.com/file/d/1IcJ5HZSFyf2yMoWUS3TC22PoxFHm39pa/view?usp=drive_link)

Etapa 2 (Deserialización Insegura)

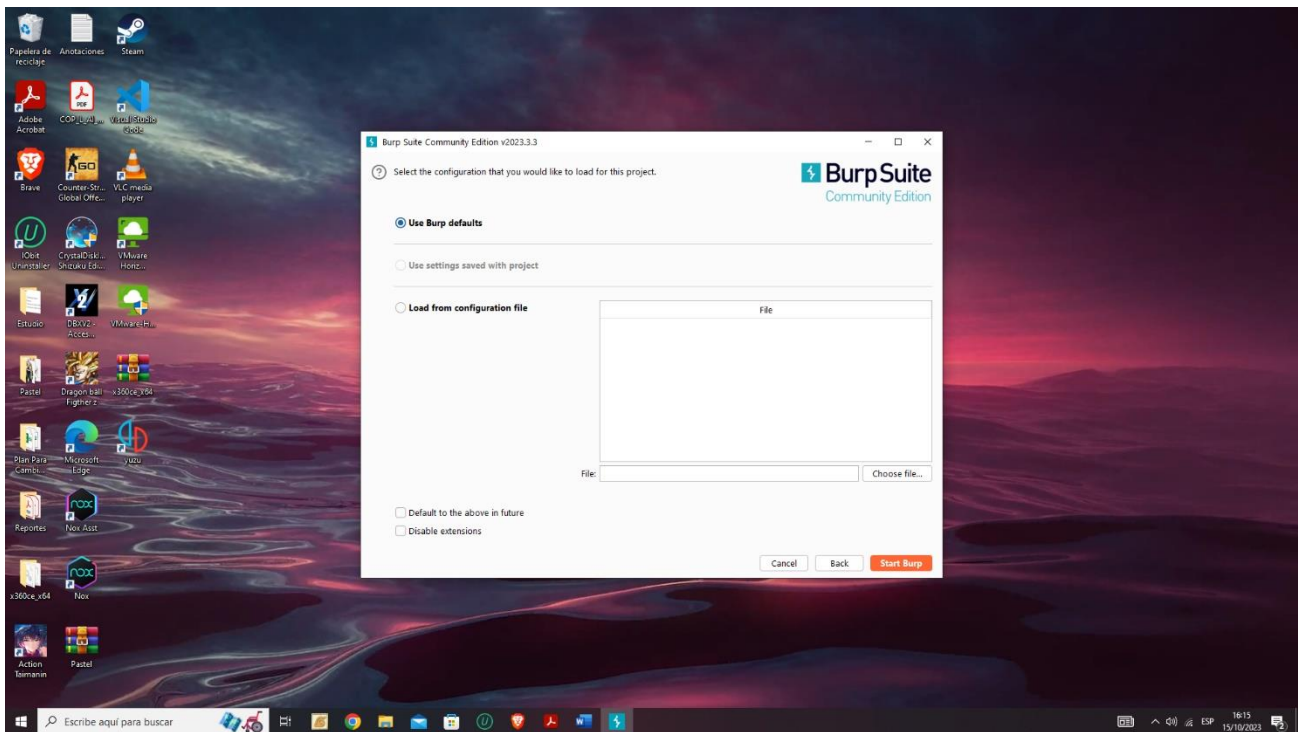
[https://drive.google.com/file/d/1CTEwOzYiATQjKChOqwn8zj\\_q4glF-OqL/view?usp=sharing](https://drive.google.com/file/d/1CTEwOzYiATQjKChOqwn8zj_q4glF-OqL/view?usp=sharing)

# Ataque Cibernético

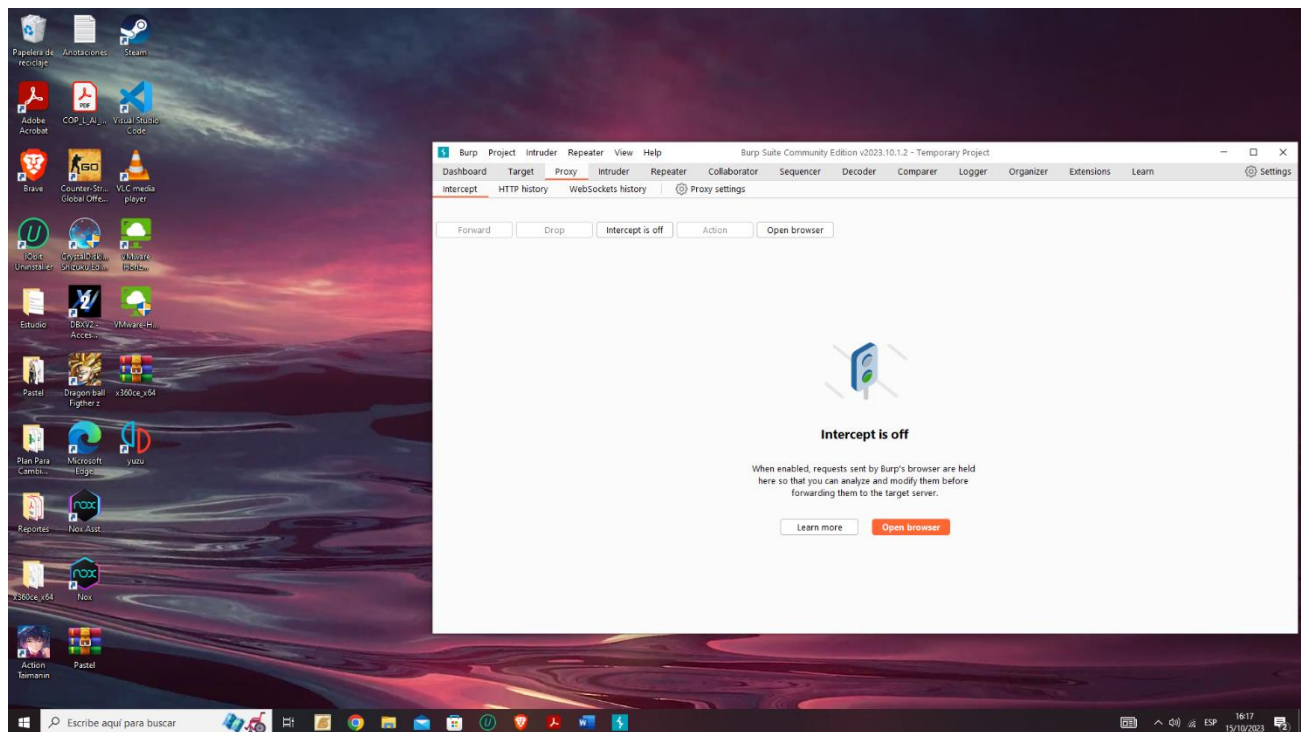
Primero se abrirá el programa Burp Suite(se realizan pasos de la actividad 2)



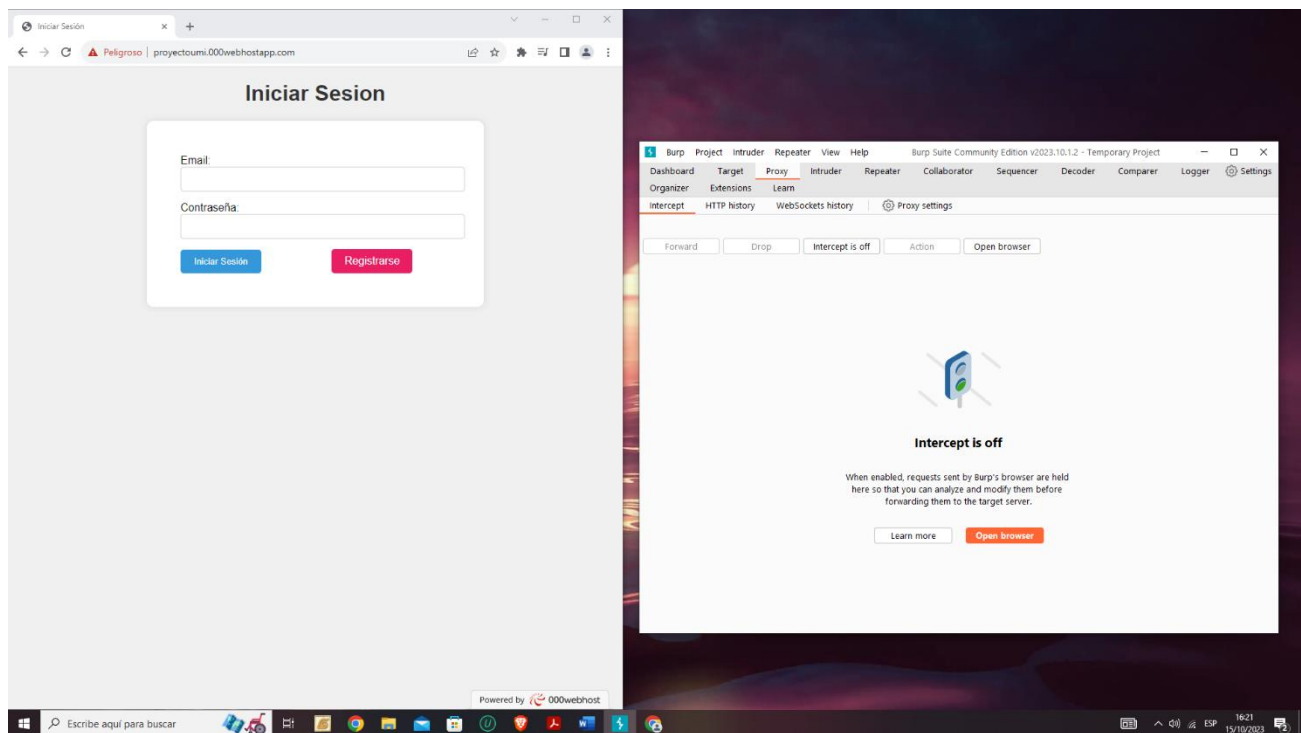
Damos clic en Start Burp



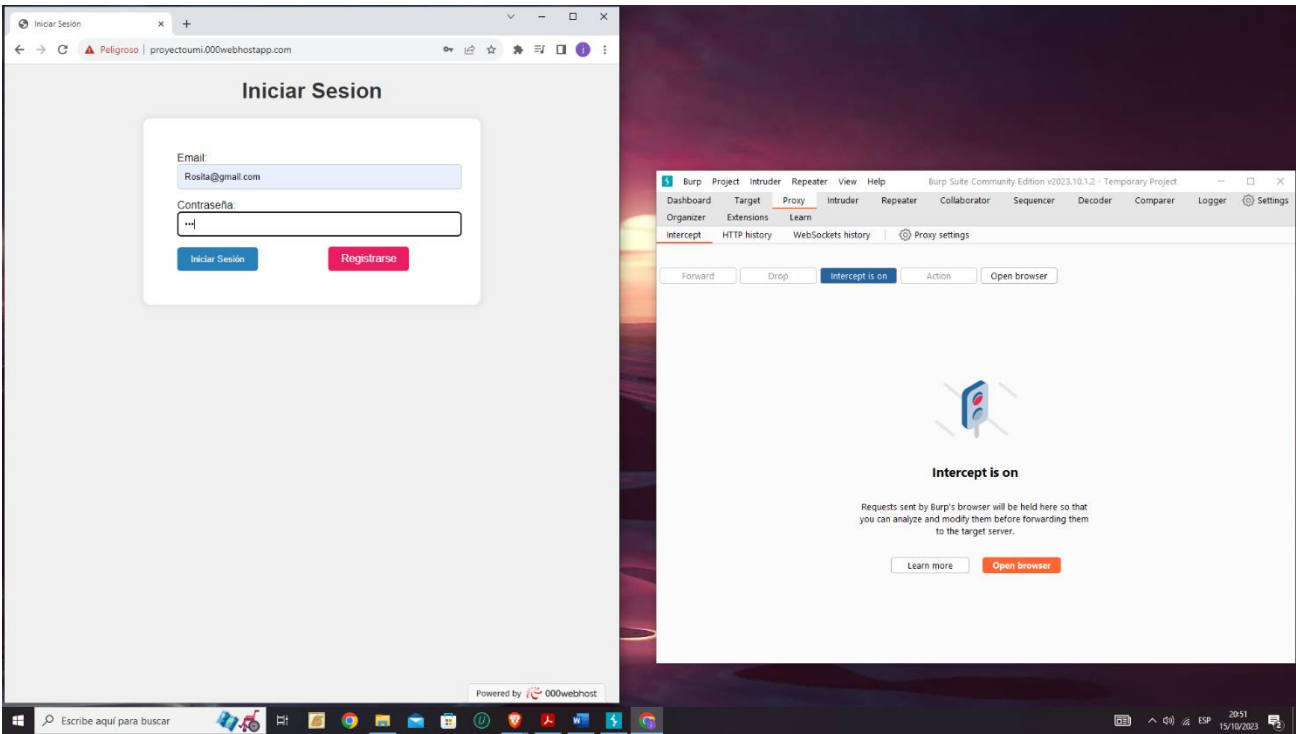
Nos vamos a la parte de proxy e intercept



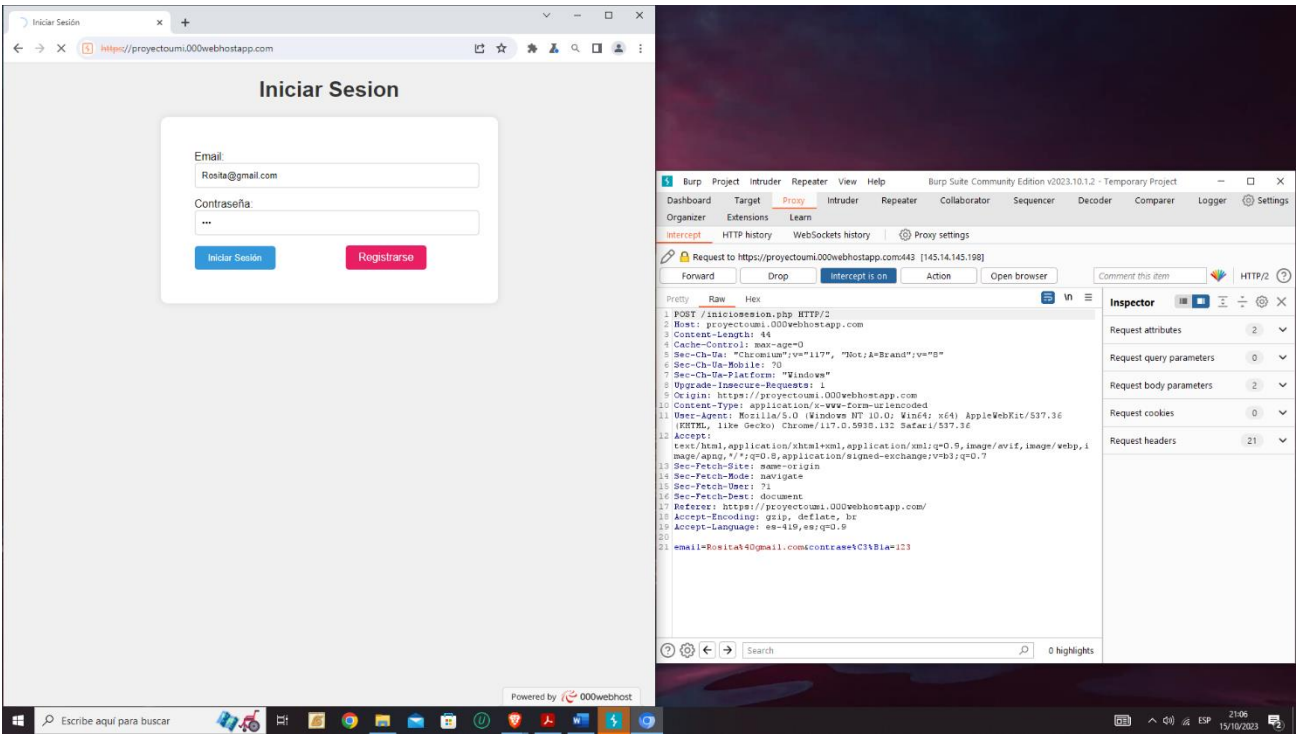
Una vez echo los pasos anteriores, vamos a irnos al sitio que vamos a atacar



Ahora vamos a iniciar sesión

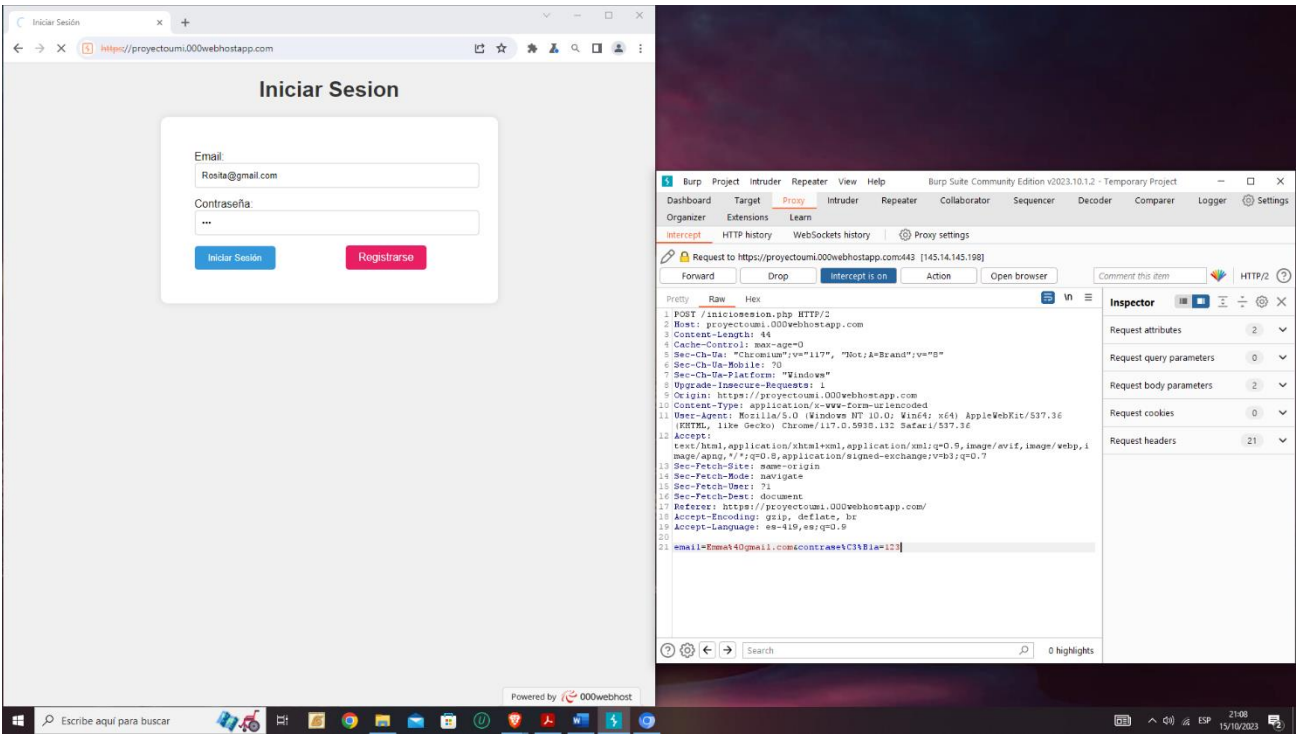


Como podemos observar ya atacamos el sitio, ya que nos aparece el usuario y la contraseña

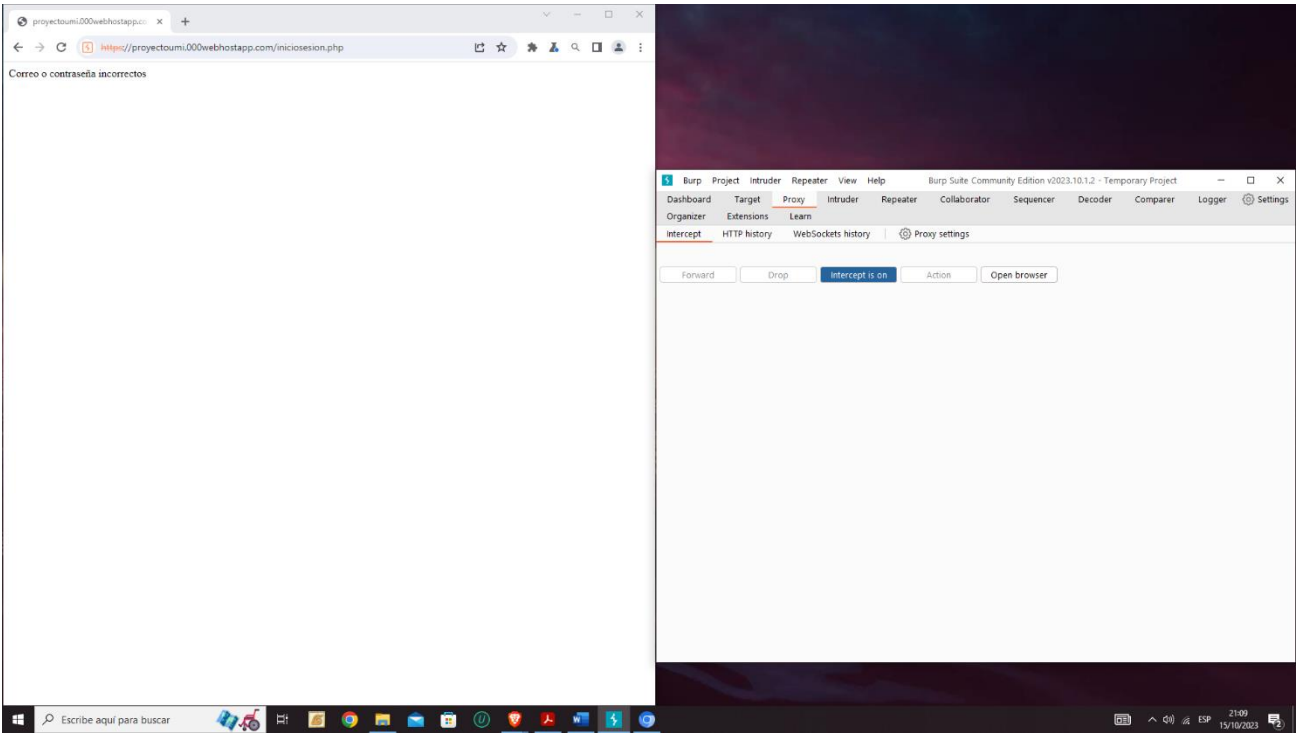




Cambiamos primero el correo a ver si accede /Rosita por Emma

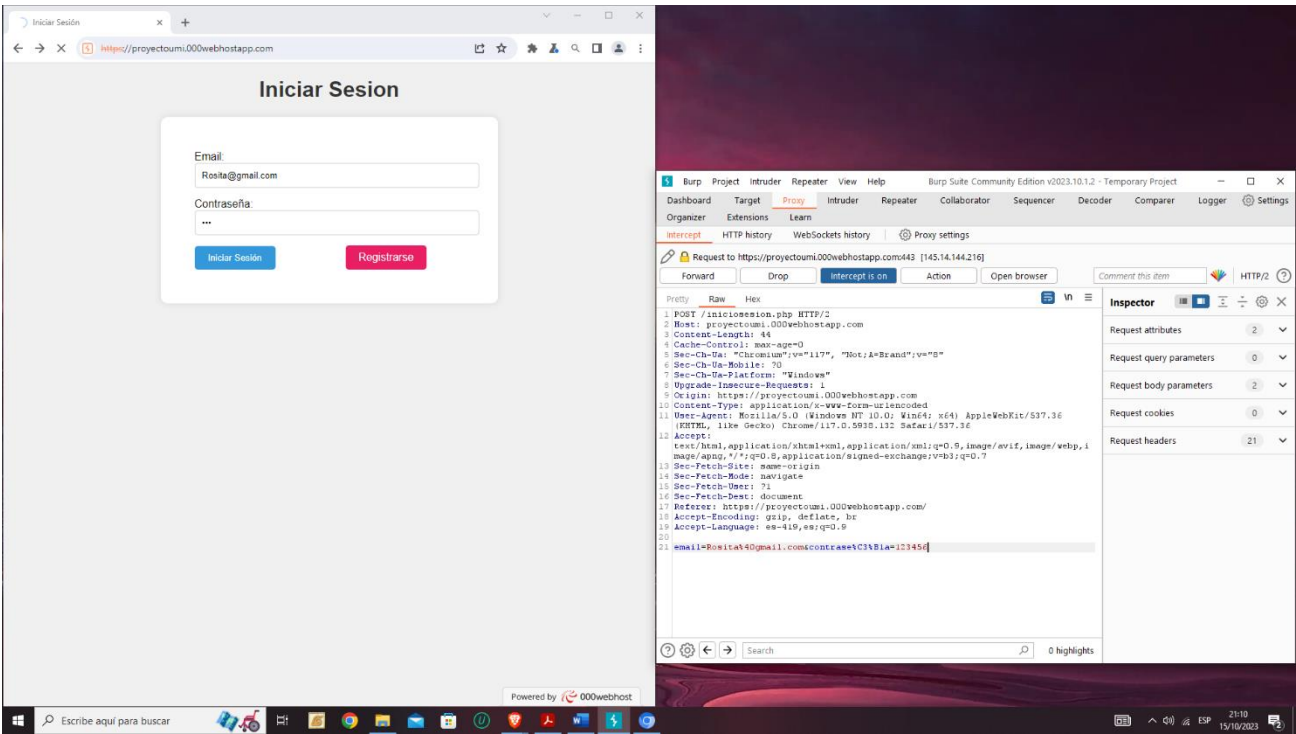


Damos clic en forward/ como vemos no pudo acceder

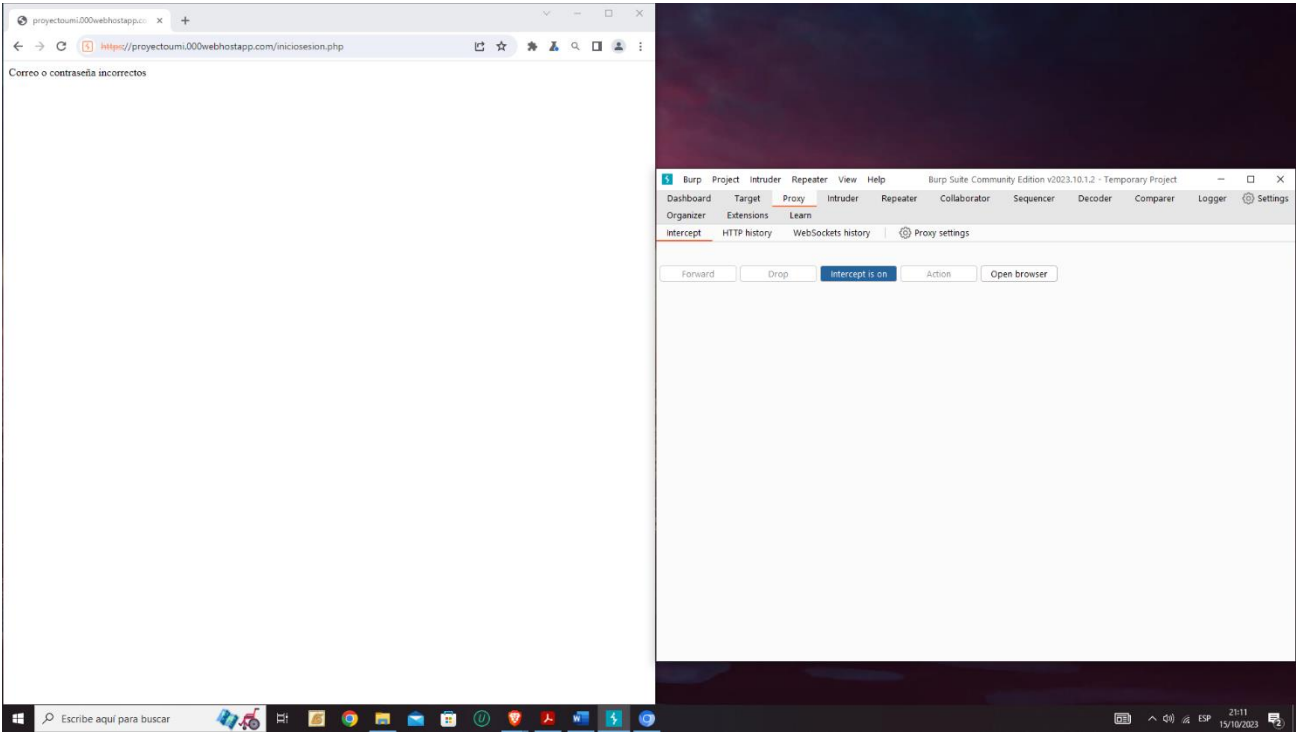




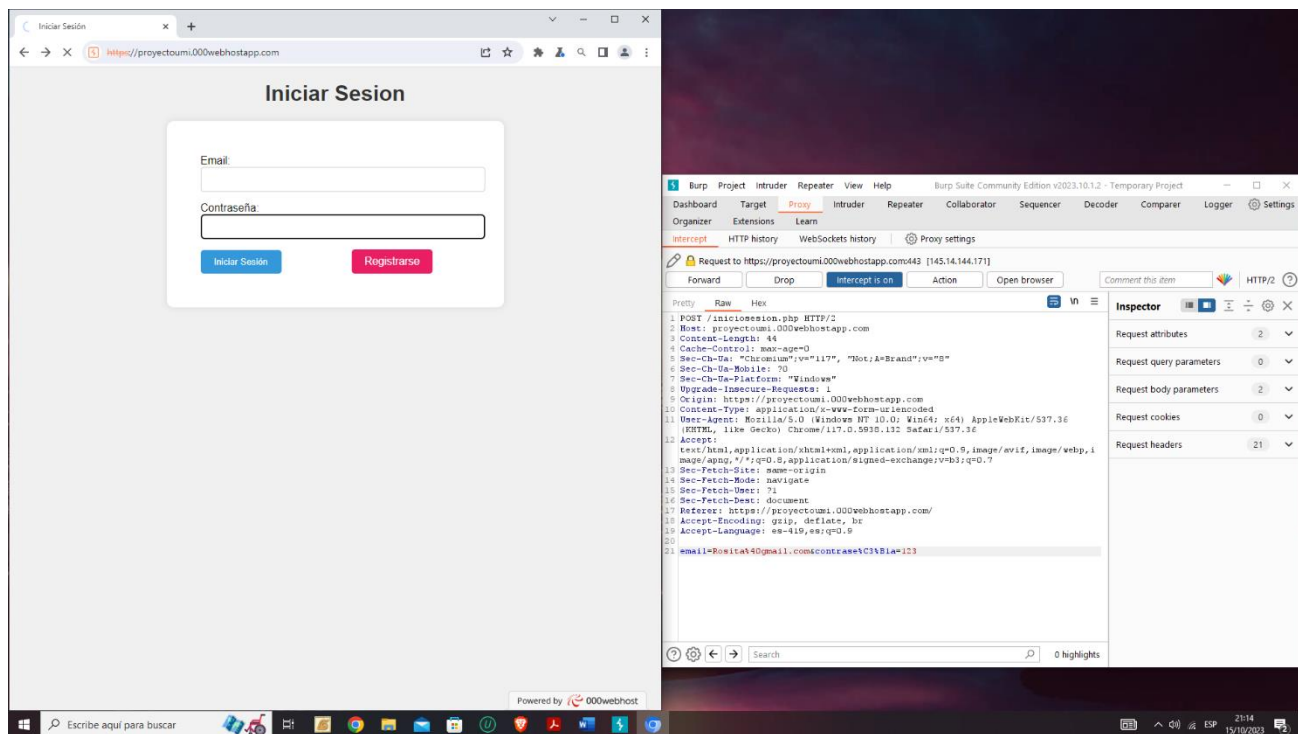
Ahora vamos a cambiar la contraseña



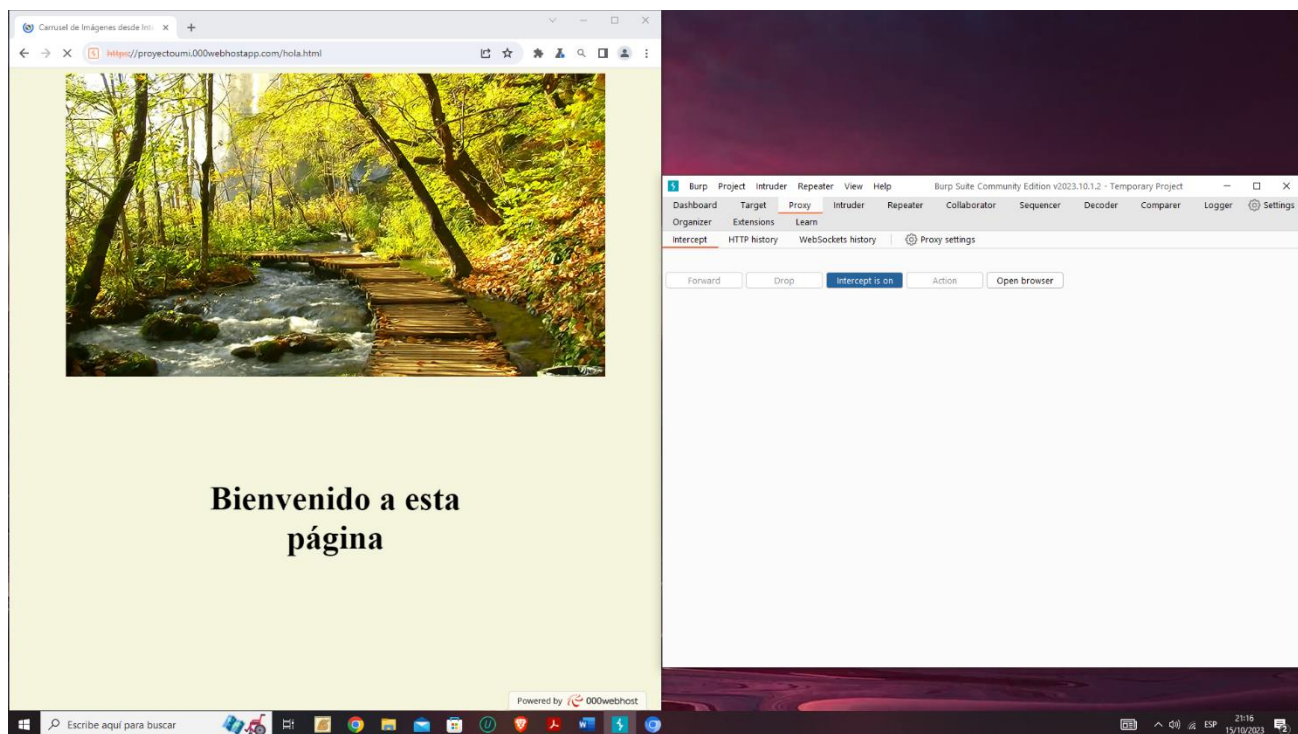
Como vemos también no podemos acceder



Ahora vamos a poner el inicio de sesión y contraseña correcta en forward daremos para que entre a la pagina sin problema



Listo, se logro ingresar desde Burp Suite



## Conclusión

La actividad que hemos llevado a cabo para explorar la vulnerabilidad de Cross Site Scripting (XSS) ha demostrado ser fundamental en términos de su relevancia tanto en el ámbito laboral como en la vida cotidiana. El entendimiento y la capacidad de abordar amenazas cibernéticas como el XSS se han convertido en habilidades esenciales en un mundo cada vez más digitalizado.

En el contexto laboral, esta actividad arroja luz sobre la importancia de la seguridad informática. Las organizaciones deben estar preparadas para proteger sus sistemas y datos de amenazas cibernéticas, y el XSS es una de las vulnerabilidades más comunes. Al adquirir conocimientos y experiencia en la detección y prevención de XSS, los profesionales de la seguridad informática pueden fortalecer la ciberseguridad de sus organizaciones y proteger la confidencialidad de los datos.

En la vida cotidiana, la actividad destaca la necesidad de estar alerta ante las amenazas cibernéticas que acechan en la web. Los usuarios de Internet deben comprender cómo protegerse contra ataques como el XSS, ya que pueden ser víctimas involuntarias. En última instancia, la concienciación y la educación en seguridad cibernética son esenciales para garantizar una experiencia en línea segura y proteger la privacidad personal.

Esta actividad subraya la importancia de la seguridad informática en todos los aspectos de la vida, desde el entorno laboral hasta la navegación cotidiana por la web. El conocimiento y la preparación en seguridad cibernética son claves para enfrentar los desafíos en constante evolución del mundo digital.

## Referencias

<https://proyectoumi.000webhostapp.com/>