Nombre Taller:  Lab 0x03

Bypassing Account Lockout

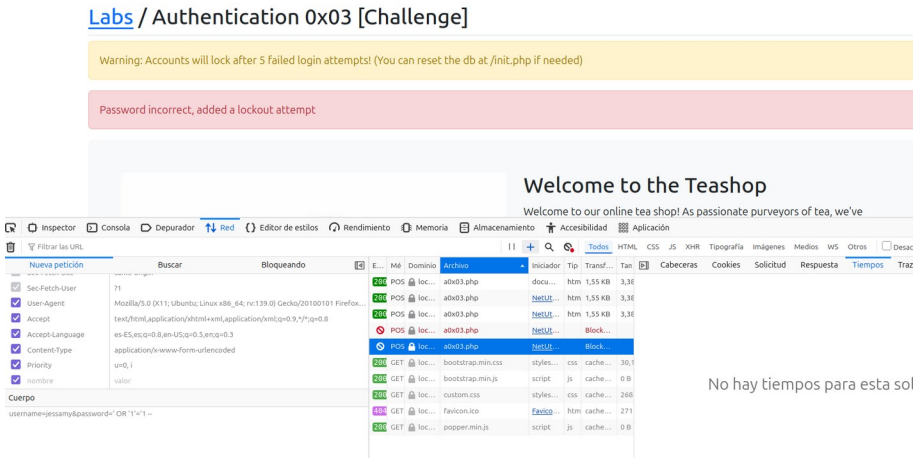
## Detalles Prácticos:

Descripción:Acceder con éxito al sistema de login envitando el bloqueo de cuentas tras múltiples intentos fallidos. El sistema bloquea al usuario tras 5 contraseñas incorrectas, por lo que se requiere una estrategia para evitarlo.
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

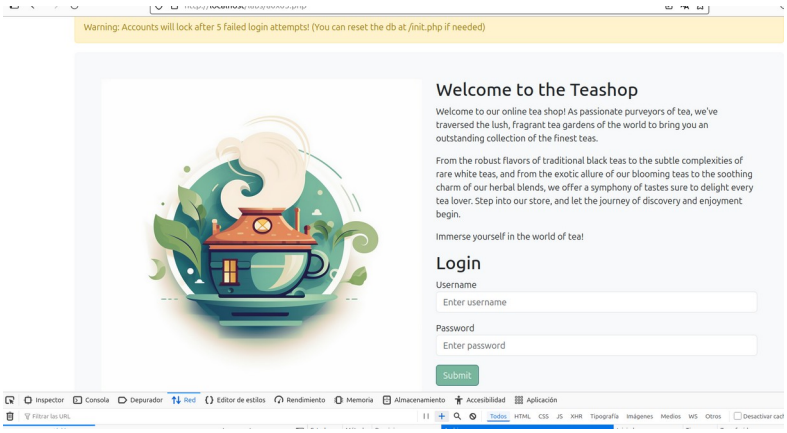
## Tabla de contenidos:



**Introduccion:**
*Análisis inicial:*
- El formulario de login acepta username y password vía método Post
- Si se realizan más de cinco intentos fallidos con un mismo usuario, **la cuenta se bloquea**



- Se puede(debe) reiniciar la base de datos visitando /init.php




**Metodología usada:**

**<u>Identificación de usuarios válidos</u>**

- Probé con usuarios admin, jeremy, jessamy y pepe
- Confirme los que existian observando, si el mensaje decia “Password incorrect, added o lockout attempt” el usuario era válido
- En cambio para pepe no aparecía el mensaje

**<u>Técnica de Evasión</u>**

- En lugar de probar muchas contraseñas para un solo usuario, alterné los intentos:
  - 2 intentos con jeremy
  - 2 con admin

- 1 con jessamy

- Esto **evitar** alcanzar el umbral de bloqueo en cualquier cuenta

**<u>Script autómatizado de fuerza bruta desde consola.</u>**

Antes de usar la técnica final del baypass por inyección SQL, probé un script en la consola del navegador, que realizba múltiples intentos de login combinando varios usuarios y contraseñas de prueba.

*Script:*

```
const usuarios = ["admin", "jeremy", "jessmy", "pepe"];
const contraseñas = ["1234", "admin", "password", "jeremy", "admin123", "pass", "123456"];

usuarios.forEach((user) => {
  contraseñas.forEach((pass) => {
    fetch("http://localhost/login.php", {
      method: "POST",
      headers: {
        "Content-Type": "application/x-www-form-urlencoded",
      },
      body: `username=${encodeURIComponent(user)}&password=${encodeURIComponent(pass)}`,
    })
      .then((res) => res.text())
      .then((text) => {
        if (!text.includes("Password incorrect")) {
          console.log(`🎯 Posible éxito con -> ${user}:${pass}`);
        } else {
          console.log(`❌ Fallo -> ${user}:${pass}`);
        }
      });
  });
});
```

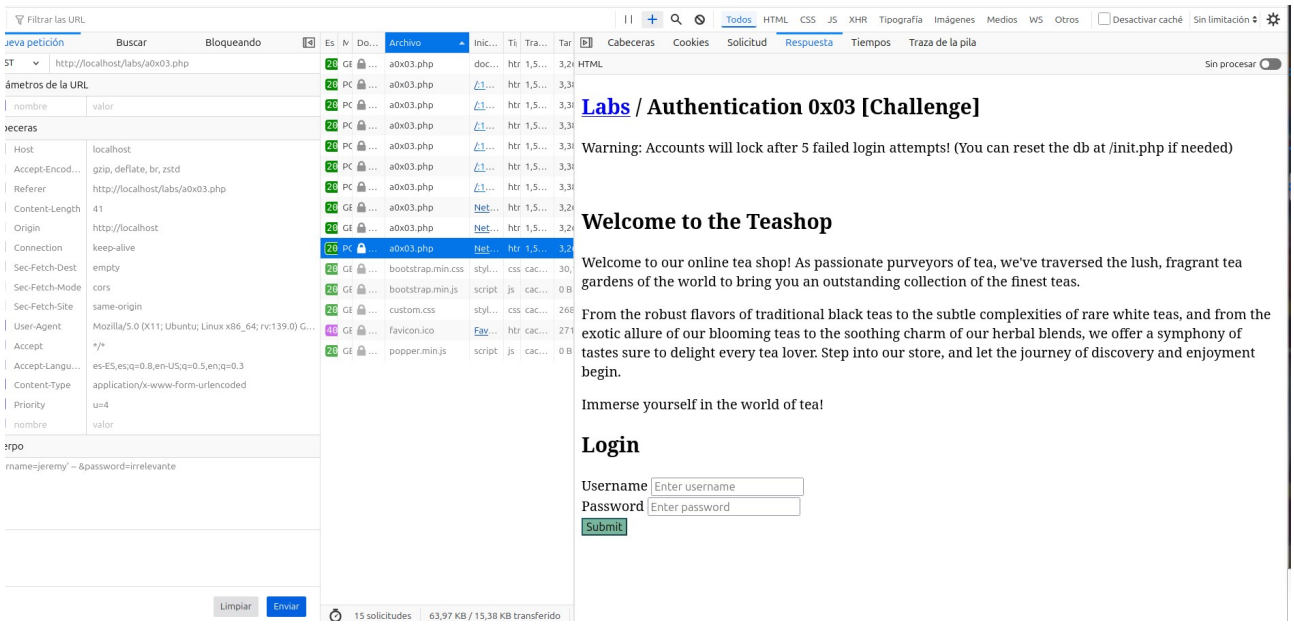
<u>Observaciones:</u>

- Aunque el script devolvía muchas veces “🎯 Posible éxito”, eso no implica que hubiese accedido realmente
- Aprendí que el contenido del response.text() **no cambiaba** significativamente lo cual me dificultaba detectar acceso exitoso

- Además, tras varios intentos el usuario quedaba bloqueado, confirmando que el sistema tenía protección contra fuerza bruta
  Este experimento me fue útil para entender la lógica de bloqueo, aunque finalmente fue la inyeccion SQL la que permitió acceder sin restricciones

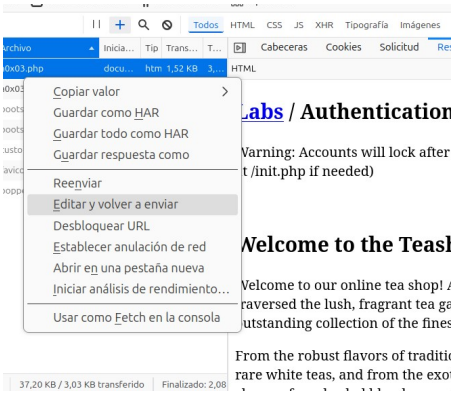
## Bypass con inyección SQL simple

- Utilicé este payload modificado directamente desde la consola, accediendo al metodo post y modificando su cuerpo para romper la query.

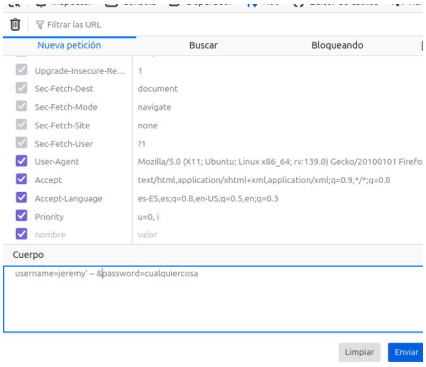



## Técnica Bypass Utilizada:

Desde la consola del navegador (f12) accedí a la pestaña **Network.**
Intente iniciar sesión normalmente para capturar el Post que se envía al servidor




Hice click derecho sobre la petición y seleccione “Editar y Enviar”




Modifique manuamente el campo
Deje el password con otro valor
indiferente ya que no se evalua despues de la coma

Envie la petición modificada y accedi sin bloquear la cuenta

**¿Por qué funciona?**
Este payload hace uso de la **inyección SQL básica:** ‘ -- cierra la comilla de la consulta SQL y comenta el resto, (tambien podia hacerse /--), anulando así la verficiación de contraseña. Así el sistema sólo válida que el nombre de usuario exista.

**Resultado** 💡:
Se accede correctamente con **jeremy** usando el payload anterior, **sin que aparezca el mensaje “password incorrect”** ni se **bloqueen** la cuenta

El entorno se mantuvo estable, y se comprobó que el sistema no detectó el acceso como erróneo. Se verificó por:
- Ausencia del mensaje de error
- Tiempo de respuesta diferente
- Vista ligeramente distinta tras el login (aunque boostrap no cargaba correctamente)