Nombre Taller:

http://localhost/labs/a0x01.php

Detalles Prácticos:

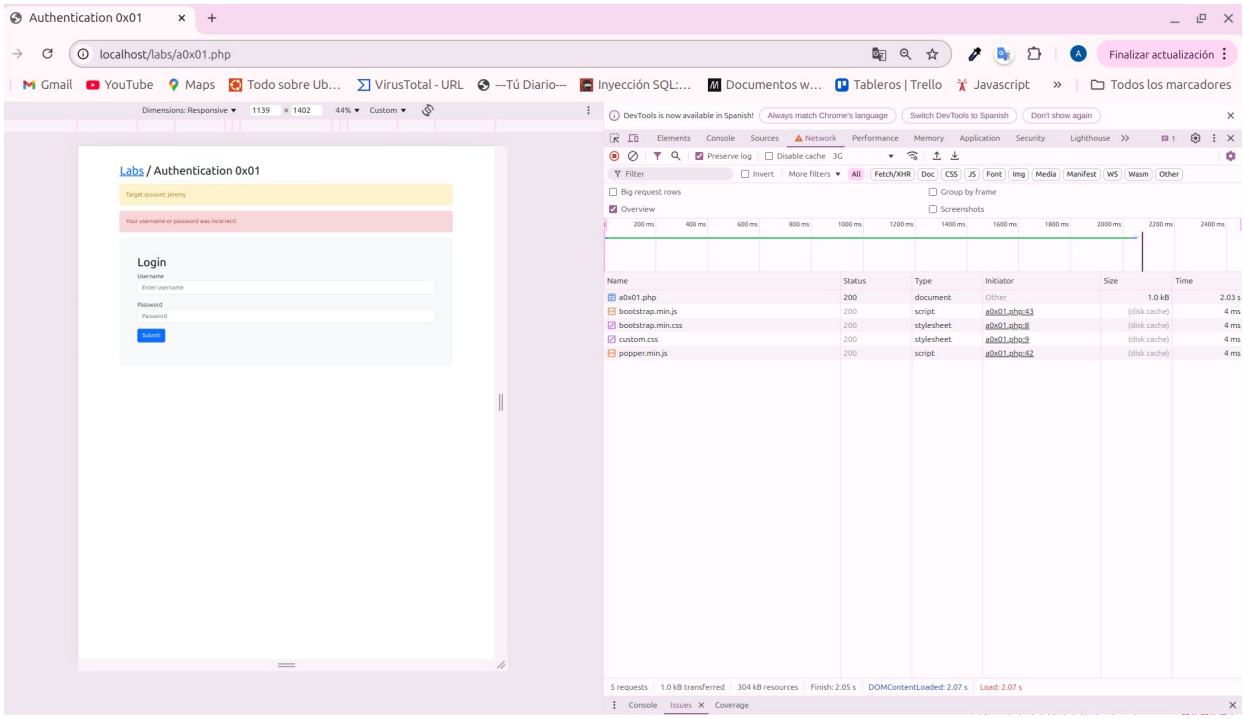
Descripción: Ataque de fuerza bruta sobre loggin vulnerable
Nivel(Básico/Intermedio o avanzado): Básico
Instructores: Rieradipe

Tabla de contenidos:

Introducción:
En este taller se explora un formulario de loggin sin medidas de seguridad que protegen contra ataques automatizados.

Materiales Necesarios:
Navegador(con DevTools), diccionario de contraseñas, y BurpSuite(opcional)

Metodologia:
1. Análisis del formulario

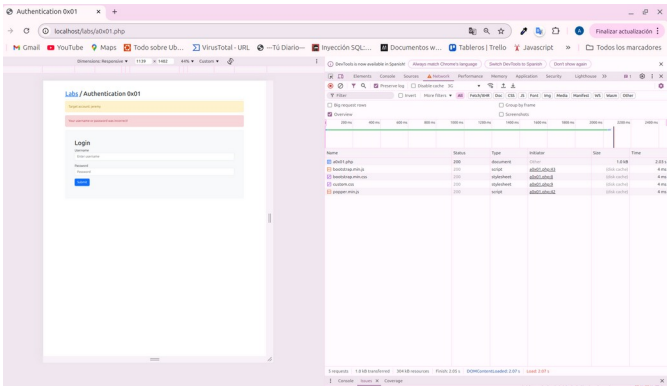


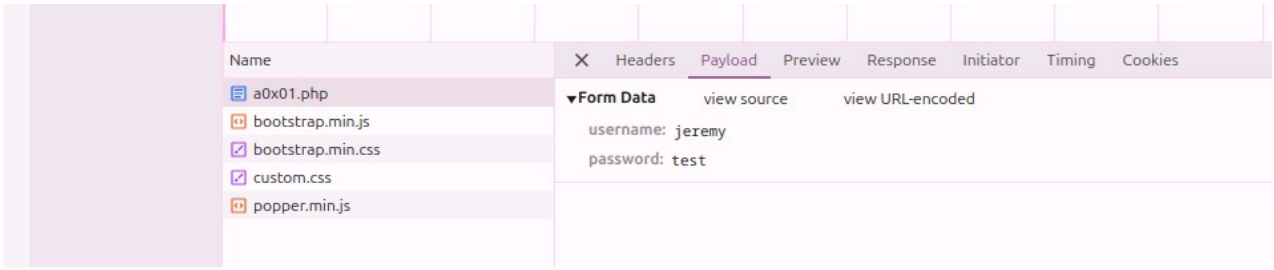
2. Pruebas manuales con contraseñas comunes.

3. Posible uso de herramientas automáticas

Ejercicios prácticos:
Captura y modificación de petiones POST, pruebas manuales con diccionario, análisis de respuestas del servidor

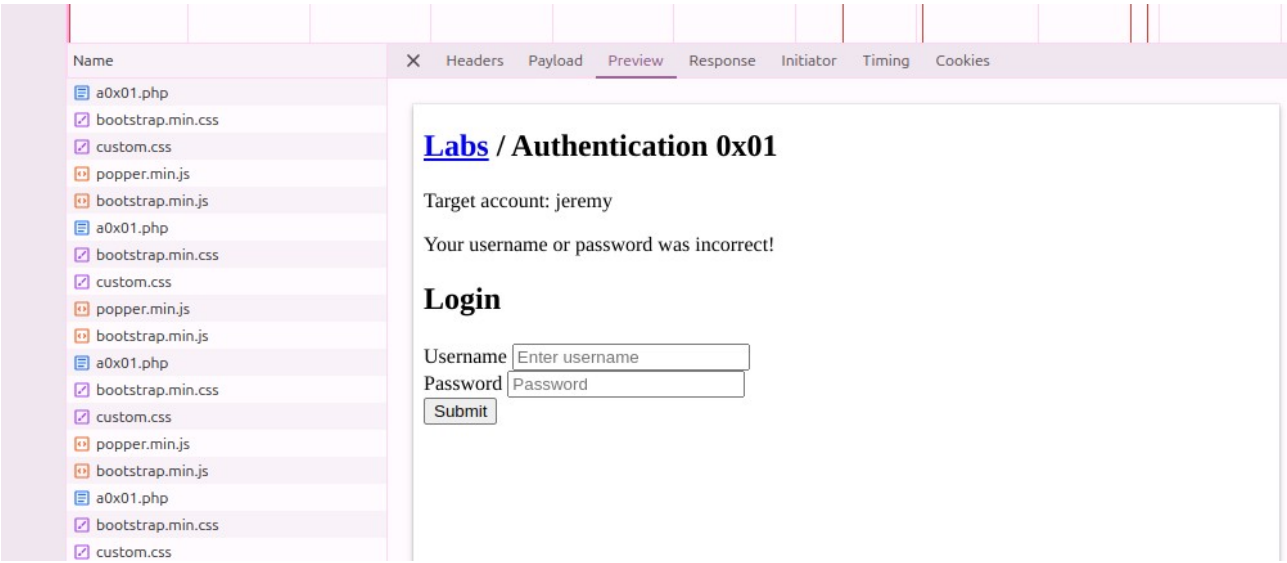
1. *Analisis con herramientas de desarrollo(f12)*
   Desde la pestaña **Network,** Se interceptó la petición POST enviada al pulsar el boton SUBMIT. Se confirma que los parametros enviados eran



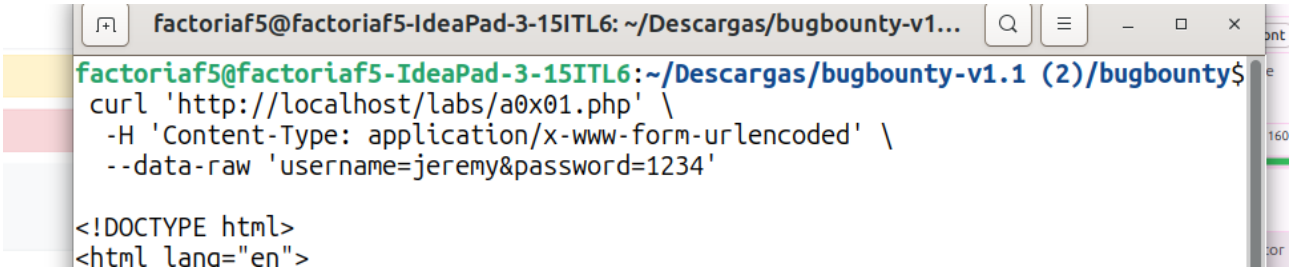


Pruebo manualmente con contraseñas comunes, como 1234, o admin...

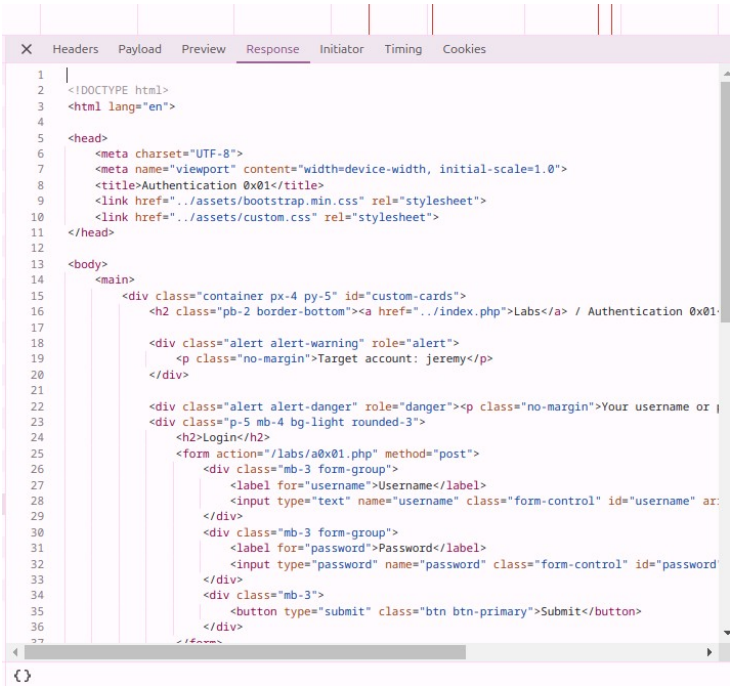
2. Comprobación de la Respuesta
En la pestaña **Response** y **Preview,** se identifica el mensaje: “Your username or password was incorrect!”
Esto indica que no se aplican mecanismos de protección como bloqueo por intentos o captchas, y que el sistema permite repetir inicios de sesion ilimitadamente.



3.Repetición automatica con curl.
Desde la consola, se replica la solicitud con curl para simular fuerza bruta manual.



La salida HTML confirma si el intento de sesion fue exitoso o no, permitiendo analizar la vulnerabilidad sin herramientas avanzadas.



Resultados esperados:
Acceso como el usuario *jeremy* tras encontrar una contraseña válida. Se considera superado si se detecta y explota la debilidad correctamente.

Mitigación y buenas prácticas:
- Implementar limites de intentos por IP o usuario
- Añadir Captcha tras varios faloos
- Usar mensajes de error genéricos
- Aplicar autenticación en dos pasos(2FA)
- Registrar actividad sospechosa en logs

Evaluación:
Este laboratorio permite entender cómo un login sin protección puede ser comprometido fácilmente y cómo prevenirlo desde el backend.
En el he aprendido que un atacante podría explotar un sistema sin protección ante el login por fuerza bruta, y que con solo el navegador y curl ya pueden realizarse pruebas efectivas.
Se documenta el comportamiento.