



Nombre Taller:

<http://localhost/labs/a0x01.php>

## Detalles Prácticos:

---

Descripción: Ataque de fuerza bruta sobre login vulnerable

Nivel(Básico/Intermedio o avanzado): Básico

Instructores: Rieradipe

## Tabla de contenidos:

---

Introducción	Contexto del taller
	Objetivos generales y específicos
Materiales Necesarios	Software requeridos
	Recursos Adicionales
Metodología	Desglose paso a paso del proceso
	Practicas recomendadas
Ejercicios Prácticos	Captura de solicitudes
	Análisis y pruebas
Resultados y Evaluación	Resultados esperados de las actividades
	Criterios de evaluación
Mitigación y Buenas Practicas	Mitigacion Propuesta para el formulario vulnerables
Conclusión	Resumen de aprendizajes
	Preguntas y próximos pasos

### Introducción:

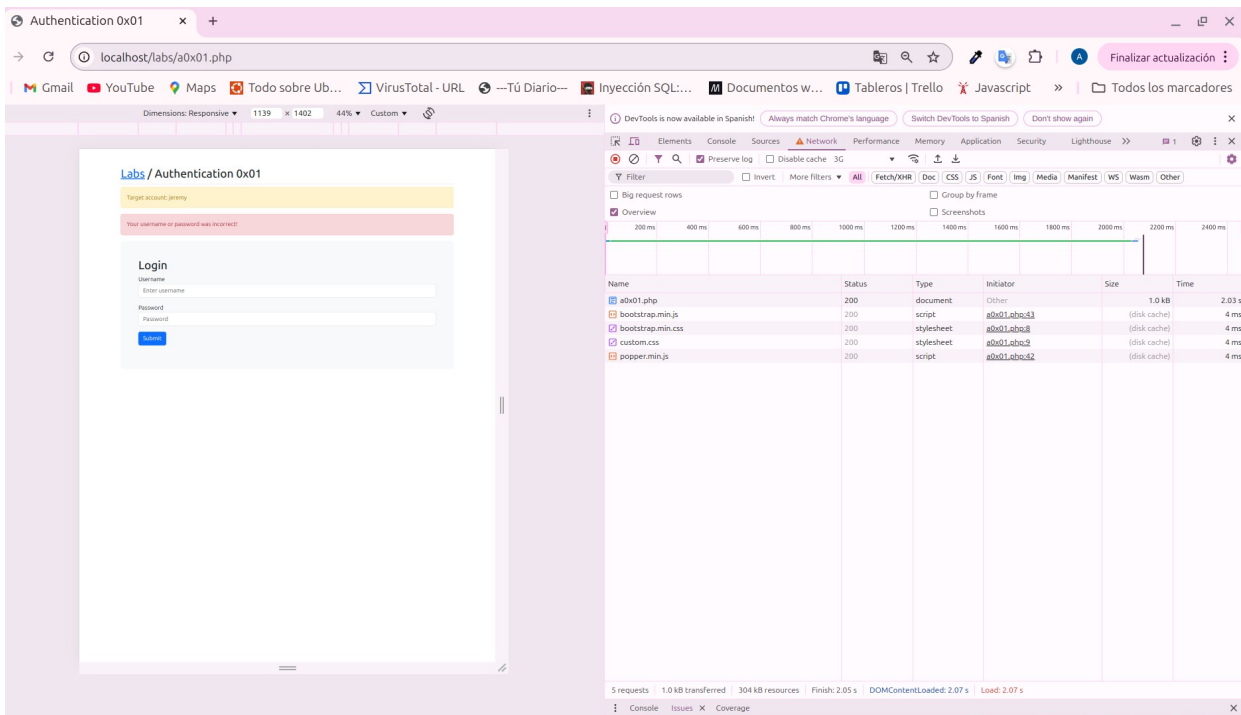
En este taller se explora un formulario de login sin medidas de seguridad que protegen contra ataques automatizados.

### Materiales Necesarios:

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

### Metodologia:

1. Análisis del formulario



2. Pruebas manuales con contraseñas comunes.

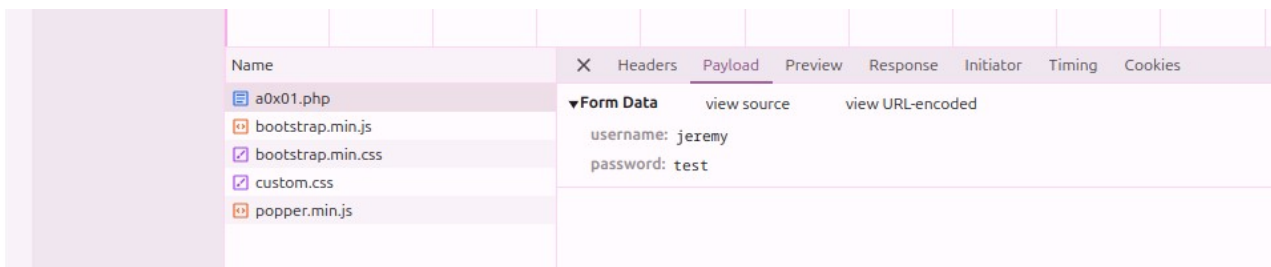
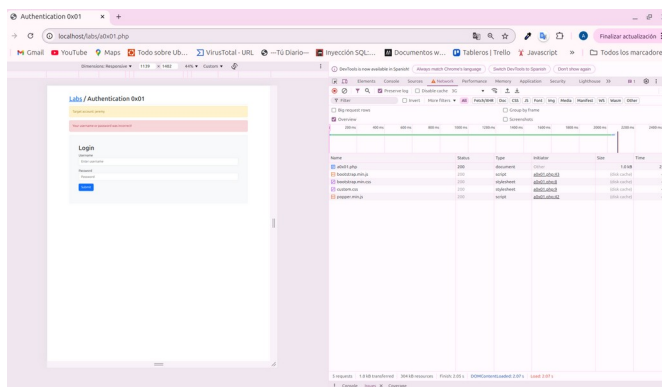
3. Posible uso de herramientas automáticas

## Ejercicios prácticos:

Captura y modificación de peticiones 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

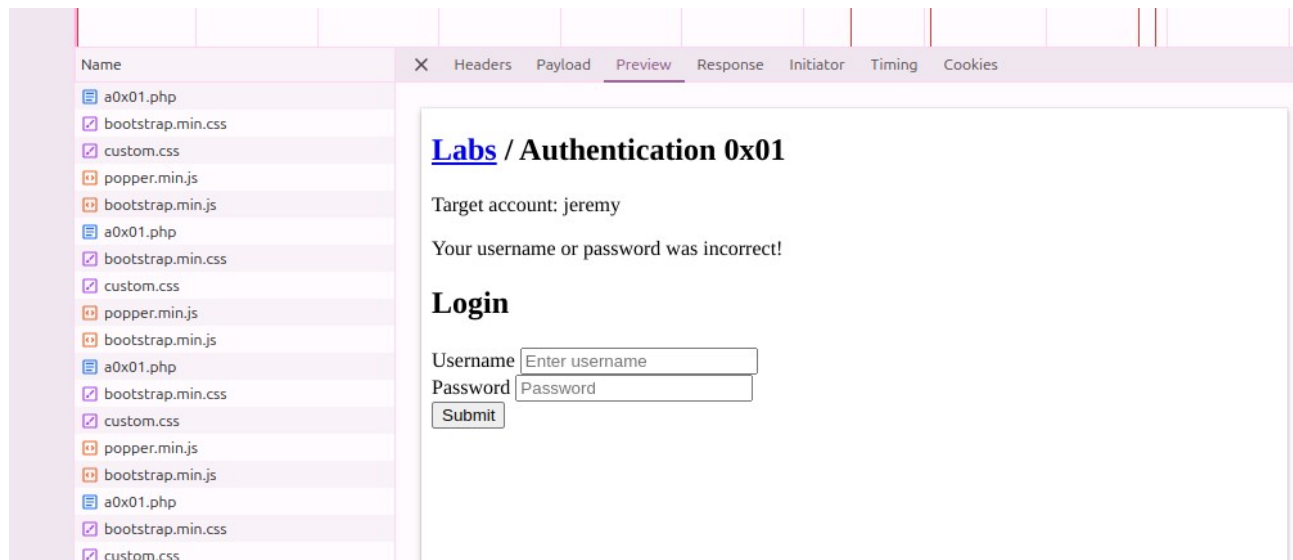


Pruebo manualmente con contraseñas comunes, como 1234, o admin...

## 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 sesión ilimitadamente.

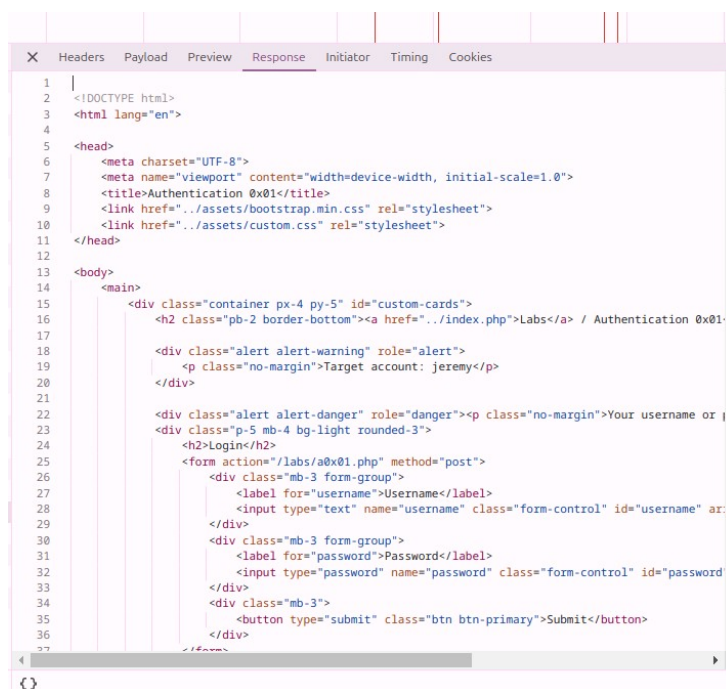


## 3. Repetición automática con curl.

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

```
factoriaf5@factoriaf5-IdeaPad-3-15ITL6: ~/Descargas/bugbounty-v1...  
factoriaf5@factoriaf5-IdeaPad-3-15ITL6:~/Descargas/bugbounty-v1.1 (2)/bugbounty$  
curl 'http://localhost/labs/a0x01.php' \  
-H 'Content-Type: application/x-www-form-urlencoded' \  
--data-raw 'username=jeremy&password=1234'  
  
<!DOCTYPE html>  
<html lang="en">
```

La salida HTML confirma si el intento de sesión 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 límites de intentos por IP o usuario
- Añadir Captcha tras varios fallos
- 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 él 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.