Nombre Taller:

Authentication 0x02

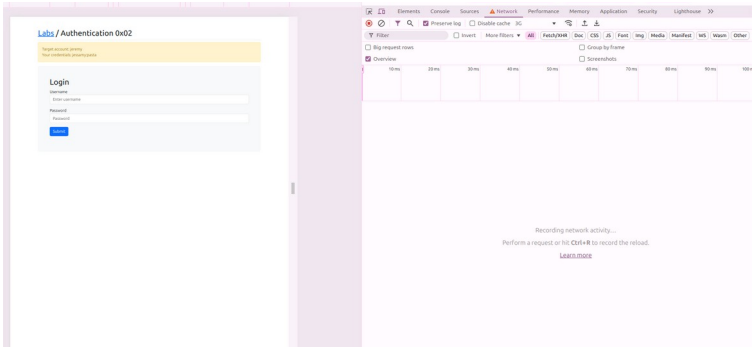
Detalles Prácticos:

Descripción: Este laboratorio demuestra cómo la exposición accidental de credenciales puede permitir a un atacante eludir la autenticación primaria.
Además se incluye un sistema de autenticación en dos pasos(MFA), cuya debilidad también puede ser aprovechada si el código está mal protegido
Nivel(Básico/Intermedio o avanzado)
Instructores:Rieradipe

Tabla de contenidos:

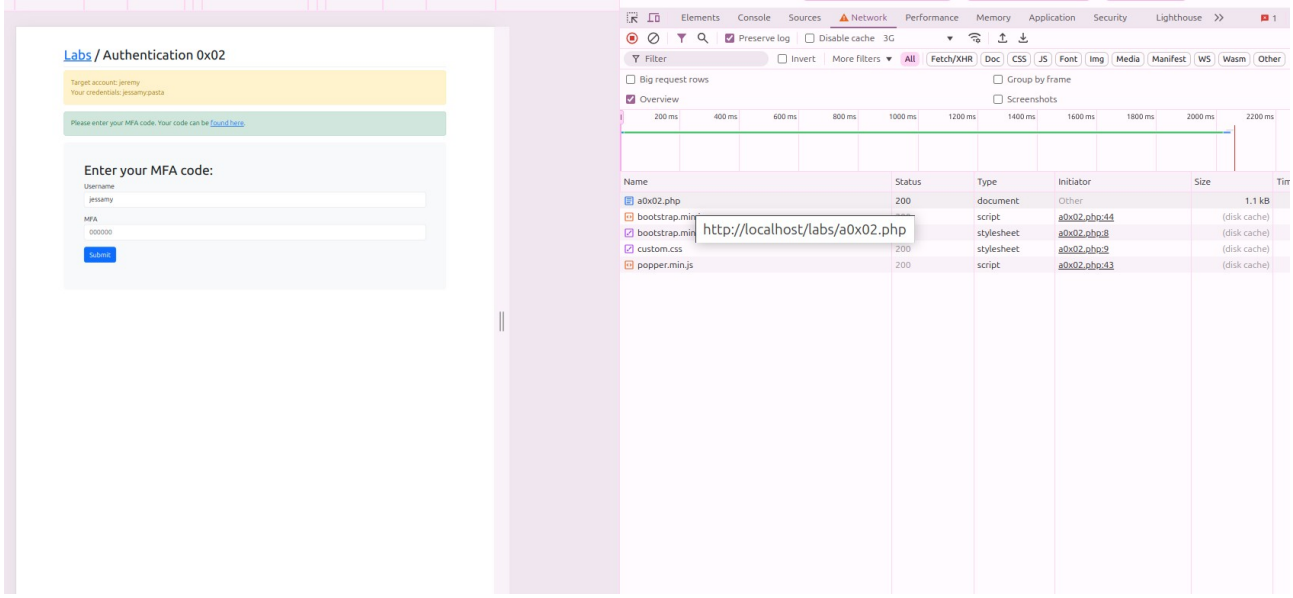
Ejercicios Prácticos:

1. Se accede a la URL del laboratorio

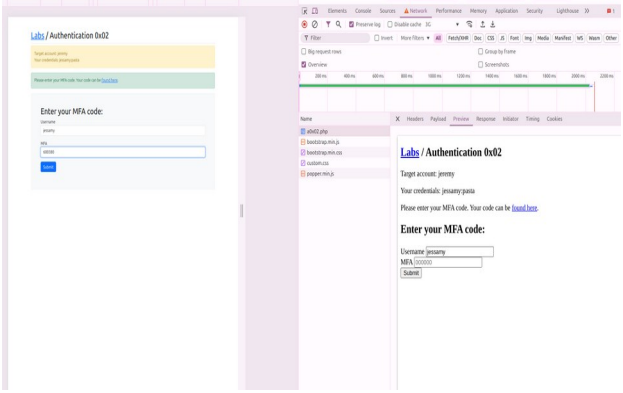


2. Aparece en pantalla las credenciales que debemos usar

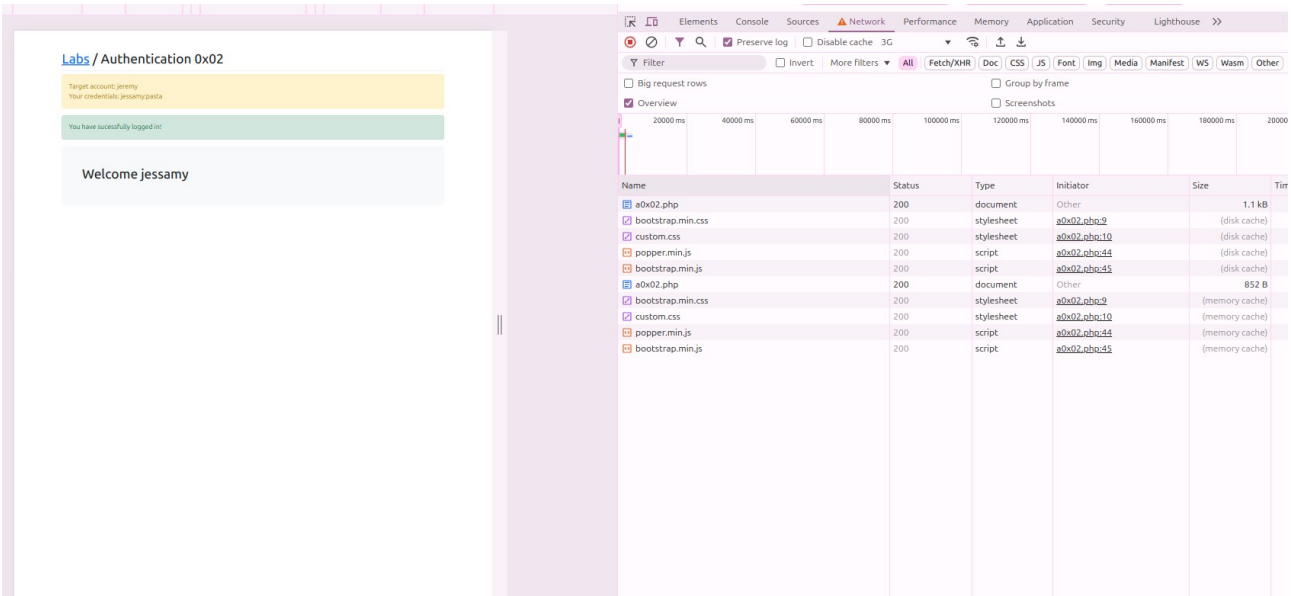
3. Se introducen en el formulario
4. El sistema solicita un código de verificación MFA y muestra el enlace para obtenerlo



5. Se accede al enlace, se copia el código MFA y se introduce en el campo correspondiente



6. El sistema confirma el login y muestra el mensaje de bienvenida



Resultados esperados:
Acceso completo como usuaria jessamy sin ningun intento de fuerza bruta, simplemente gracias a una fuga directa de credenciales y código MFA

Medidas de mitigación recomendadas

Riesgo destacado	**M**edida recomendada
Fuga de credenciales visibles	Nunca mostrar credenciales en UI, login ni mensajes internos
Código MFA accesible desde enlace directo	Proteger los tokens 2FA con rotoración o entrega segura (por correo, app o dispositivo confiable)
Ausencia de control de acceso por rol	Aunque se entra como jessamy, deberia haber controles que impiden escalar a jeremy
Exceso de información en pantalla	Mostrar solo mensajes necesarios, nunca información técnica ni sensible

Conclusion:
El laboratorio demuestra que una aplicación web no solo debe proteger sus formularios, sino también controlar toda la información que entrega al usuario. El uso de MFA no es seguro si el código puede obtenerse con un clic.
La defensa debe ser integral y considerar tanto el flujo visual como el interno.