Auditando seguridad de una Aplicación Web: Autenticación Defectuosa

Francisco Luque

¿Por qué es importante tener buena seguridad de autenticación?

La prevalencia de la autenticación vulnerable es lamentablemente mucho más común de lo que uno cree debido al diseño y la implementación de la mayoría de los controles de identidad y acceso. La gestión de sesiones es la base de los controles de autenticación y acceso, y está presente en todas las aplicaciones con estado.
Los atacantes pueden detectar fallas en sistemas de autenticación usando medios manuales y explotarlos usando herramientas automatizadas como ser listas de contraseñas y ataques de diccionario.

Mi Objetivo a probar: Planarally

Planarally es una aplicación web open source desarrollada para jugar ciertos juegos de mesa y de rol por internet. Posee un sistema de cuentas, en las cuales los usuarios pueden crear partidas. A estas pueden invitar a otros usuarios, cargar imágenes y otros archivos para usar en un tablero, y llenar datos de tanto este juego como datos personales suyos.

Esta aplicación sigue en desarrollo y es usada por miles de personas alrededor del mundo.

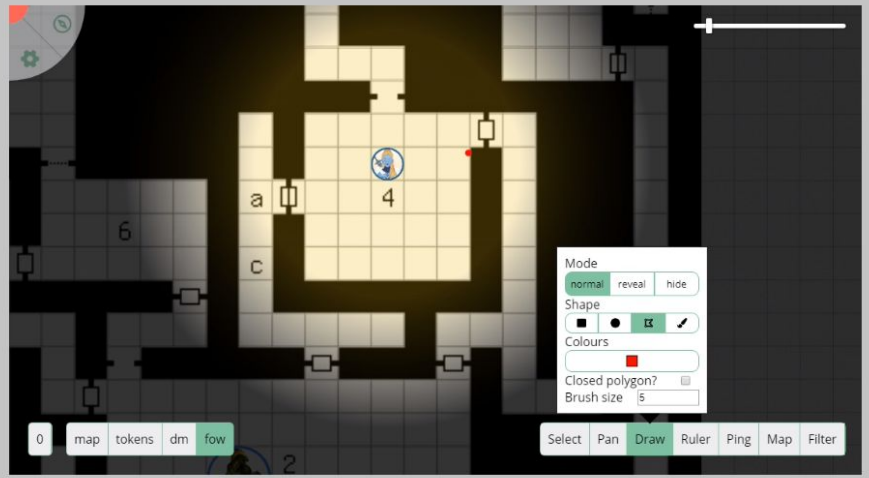
Evitar el reconocimiento manual de la existencia de usuarios en el sistema

Política de Contraseñas dada por la OWASP

- No se debería poder reconocer de forma rápida cuando un usuario existe o no en el sistema. De fallar una autenticación se debe devolver un mensaje genérico, no si está únicamente mal la contraseña o que el usuario no exista.

Welcome to PlanarAlly !

PlanarAlly is an opensource virtual tabletop that aims to help you and your players discover the various fictive worlds out there.



Immersive lighting & vision system

Username

weaktestcase

Password

enter

OR

register

! Username and/or Password do not match CLOSE

Need help? Visit our user documentation over on planarally.io or join the community on discord!

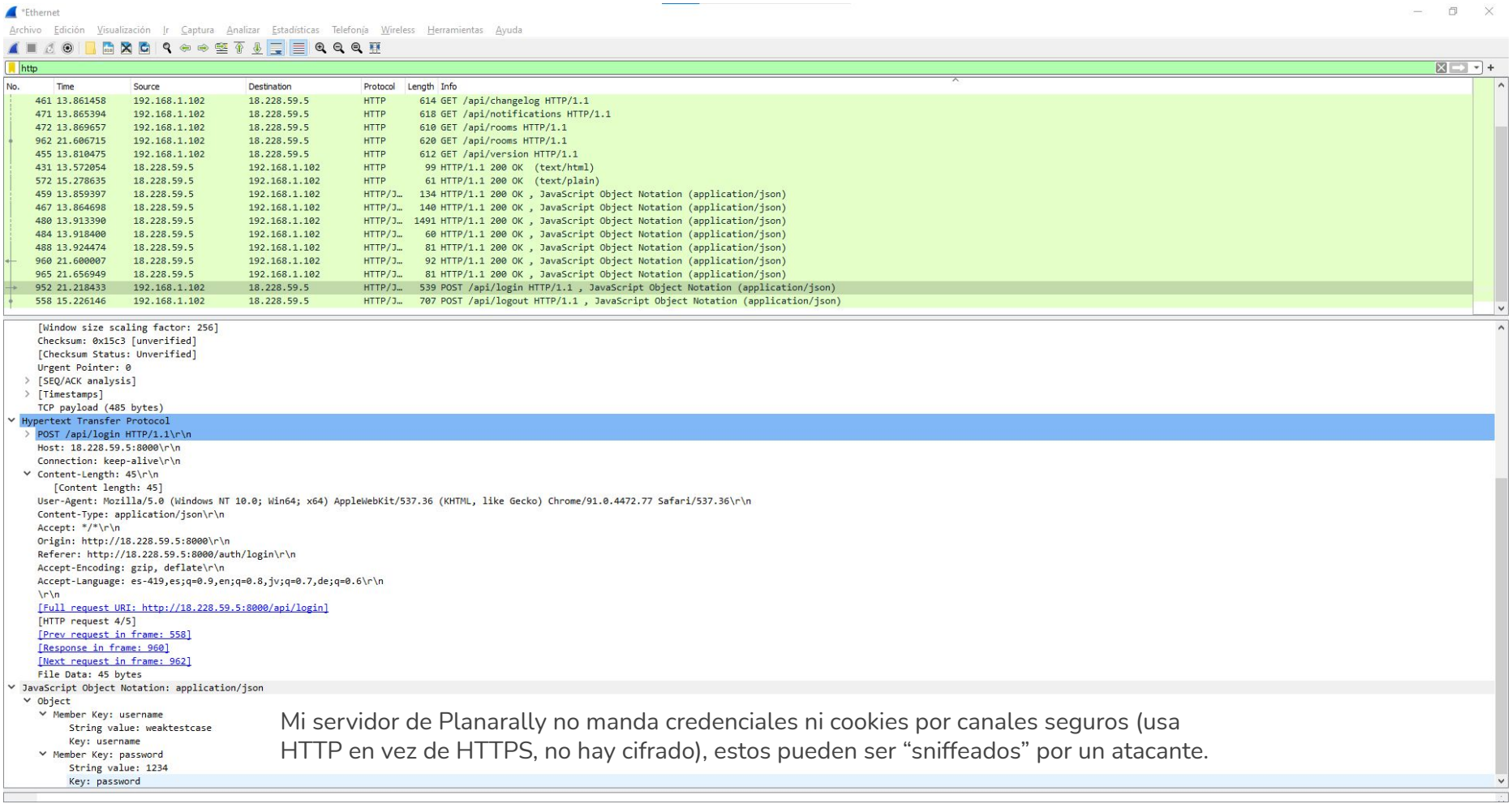
Se usa un mensaje genérico a fin de no permitir reconocimiento de los usuarios de la red.

Mandar la información mediante canales seguros

- Al registrarse y unirse al sistema, los parámetros deben ser pasados por HTTPS u otros canales seguros, a fin de que un atacante que estuviera observando la red no pueda interceptar la información.

¿Cómo probar si la información se manda por canales seguros?

Utilizando herramientas como Wireshark o la consola del navegador, se puede observar como se manda la información. En una aplicación segura, esperamos que la información importante se mande por canales https, y que intente usar estos aun cuando sea forzada a usar http. Si admite usos de http para información importante, o si la usa por defecto, es una falla enorme de seguridad.



Mi servidor de Planarally no manda credenciales ni cookies por canales seguros (usa HTTP en vez de HTTPS, no hay cifrado), estos pueden ser “sniffeados” por un atacante.

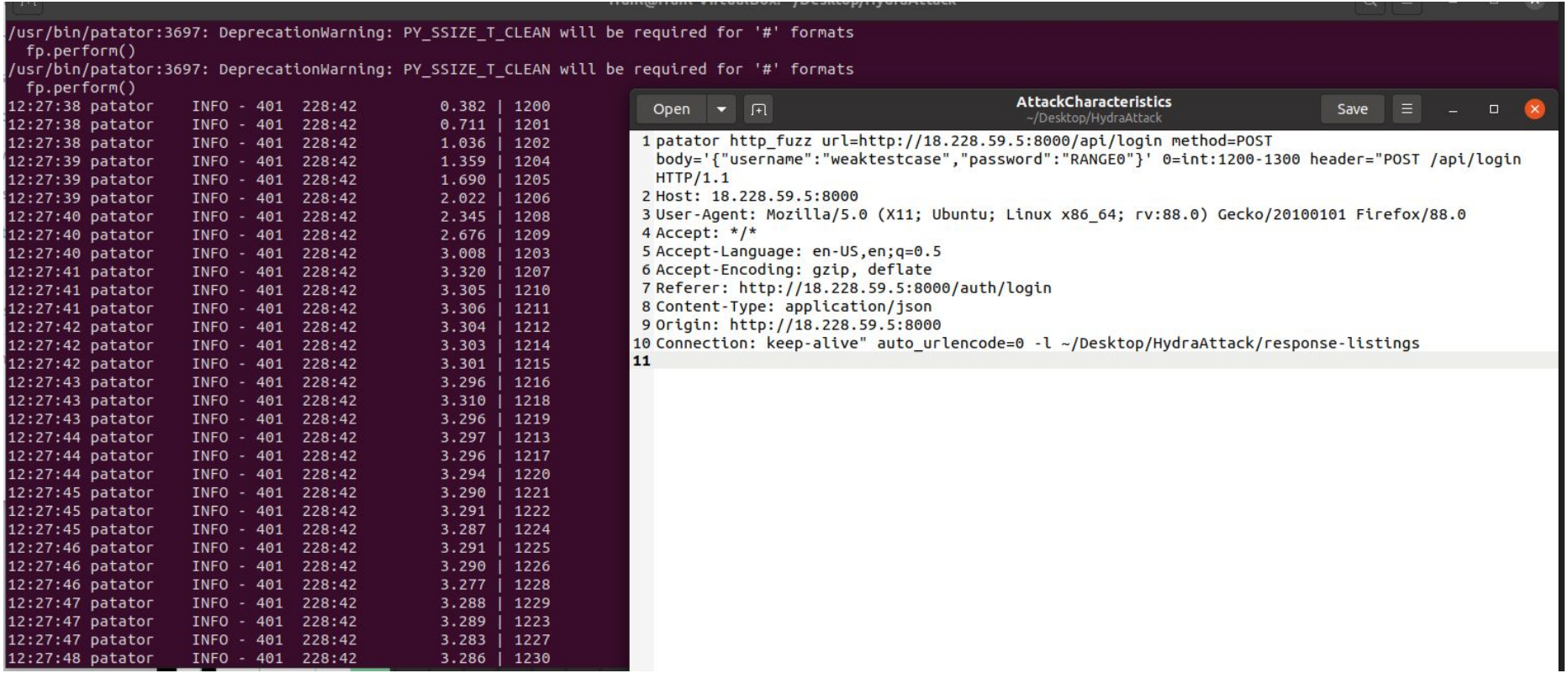
Defensas contra ataques de fuerza bruta.

- El sistema debería incentivar a los usuarios a usar contraseñas fuertes, difíciles de generar o adivinar.

- El sistema debería tener un sistema de protección contra ataques de fuerza bruta, dando intentos limitados a un usuario para poner una contraseña. Aunque este no debería poder ser utilizado por un atacante para bloquear la contraseña de otro.

¿Cómo probamos la defensa de un sistema contra ataques de fuerza bruta?

- Probar ingresando contraseñas correctas e incorrectas múltiples veces de un usuario conocido. Si el sistema después de 5-7 intentos incorrectos seguidos nos permite entrar con la contraseña correcta podría existir la posibilidad de un ataque de fuerza bruta.
- Realizar un ataque de penetración de prueba con THC Hydra, Patator, u otras herramientas.



La aplicación es vulnerable a ataques de fuerza bruta, se pueden forzar contraseñas probando cientos de combinaciones a la vez.

Defensas contra cambios de contraseñas

- El sistema debería permitir a usuarios recuperar su contraseña, dado que presenten la información que los acredite.

- Para poder cambiar la contraseña de una cuenta se debería necesitar re autenticar que es la persona, a fin de evitar que un atacante que tome control de una sesión pueda tomar control de la cuenta en sí.

Resguardado seguro de contraseñas

- Las contraseñas almacenadas deben hashearse, utilizando algoritmos fuertes y “salteados”. A fin de evitar que un atacante que consiga acceso a la base de datos tenga acceso a las contraseñas.

	id	name	email	password_hash	efault_opt
	Filter	Filter		Filter	Filter
1	1	bigmen	NULL	$2b$12$Q2ghuinVKHr3QH675BsdFu/NaFruJdfAoA8IaHuD2OKOU.FZPqk8a	1
2	2	as	NULL	$2b$12$bF7t5RnXjqL8gwQq9/e4iepOgE60stZIOXb5eKEw3QwaQAy.GGHVy	2
3	3	Santy	NULL	$2b$12$xpIvlUMsqOPORMbG7HcHg.7qNhN/Zgn/ms2fAlRj.6e.3Vm4i4QK2	3
4	4	el macho de s...	NULL	$2b$12$pgajsmBJKHYRR5qUFIFMweNBoylxLhQQrRG9iexzxi6xF3vXJKVxa	4
5		Tormenta			

Conclusiones y Preguntas