1 A9 Security Logging and Monitoring Failures

1.1 Concepto

El registro es muy importante para los sistemas modernos. Lo usamos por varias razones:

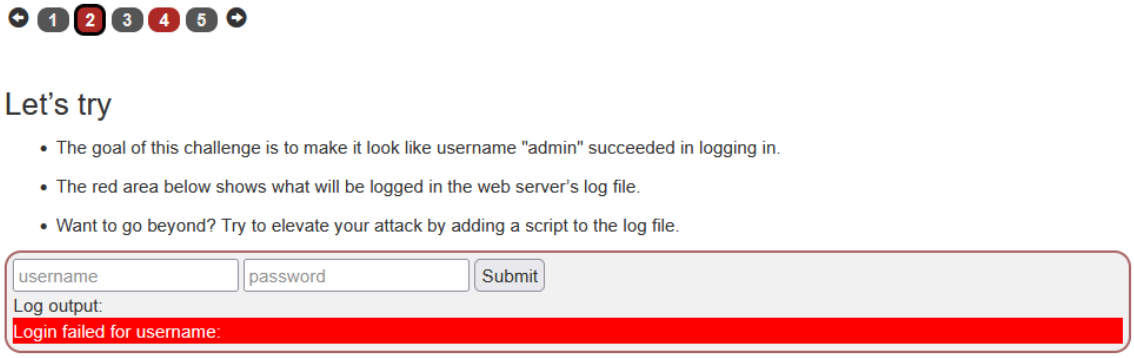
- Monitoreo y depuración de aplicaciones.
- Registro de auditoría: por ejemplo, registre acciones específicas de sus usuarios y sistemas.
- Monitoreo de eventos de seguridad: por ejemplo, proporcione información a un sistema SIEM o SOAR que se activará en función de la información proporcionada en estos registros.

Objetivos

- El usuario debe tener conocimientos básicos sobre el registro y dónde iniciar sesión.
- El usuario comprende los riesgos de la suplantación de registros y la filtración de información de registros.
- El usuario podrá realizar un simple ataque de suplantación de registros.
- El usuario podrá conocer los riesgos básicos que implica el registro.

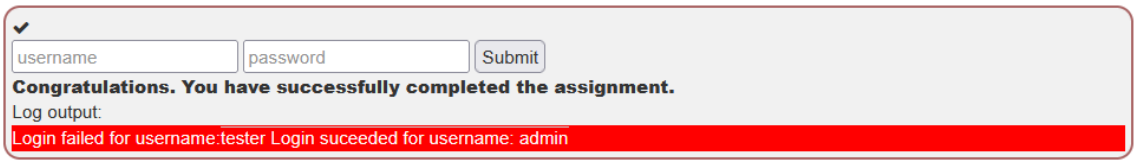
Intentemos

- El objetivo de este desafío es hacer que parezca que el nombre de usuario "admin" logró iniciar sesión.
- El área roja a continuación muestra lo que se registrará en el archivo de registro del servidor web.
- ¿Quieres ir más allá? Intente mejorar su ataque agregando un script al archivo de registro.

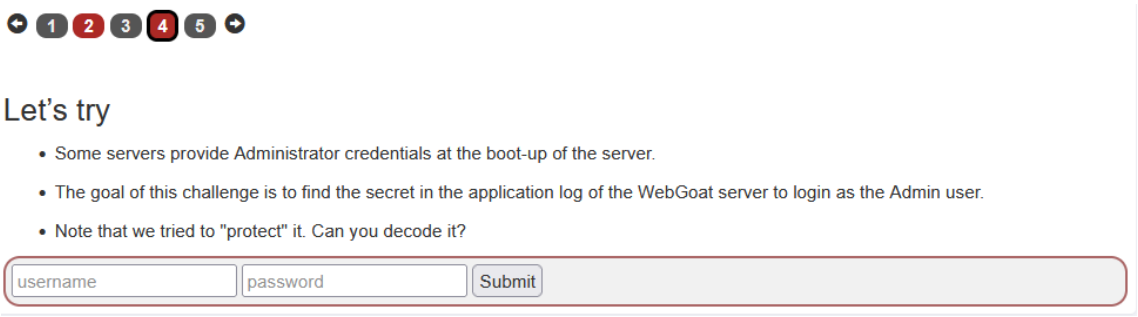


En el primer campo **username** agrega:

```
tester Login suceeded for username: admin
```



Donde tester es el usuario con el cual te conectas a WebGoat.

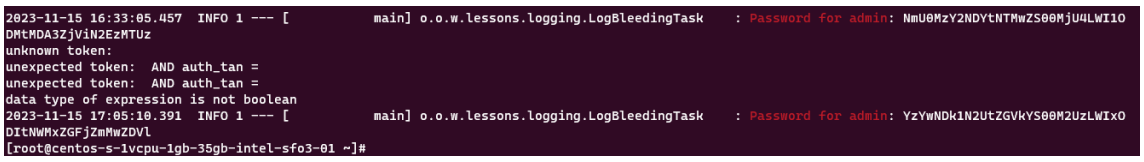


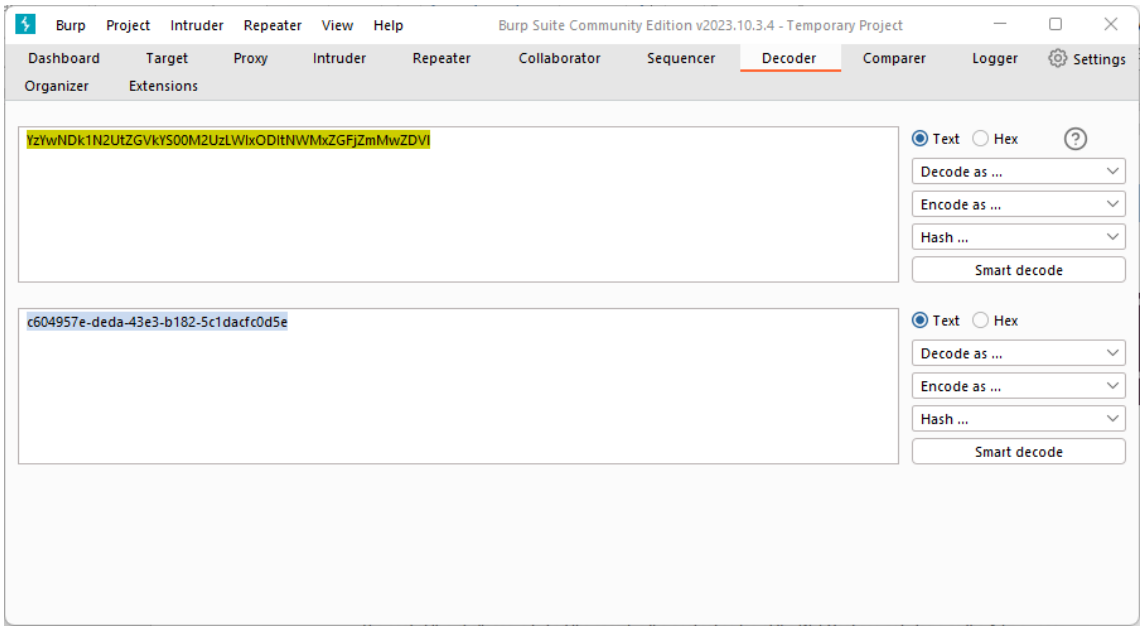
Revisa el log de la aplicación WebGoat

Filtra los mensajes del log con el siguiente comando:

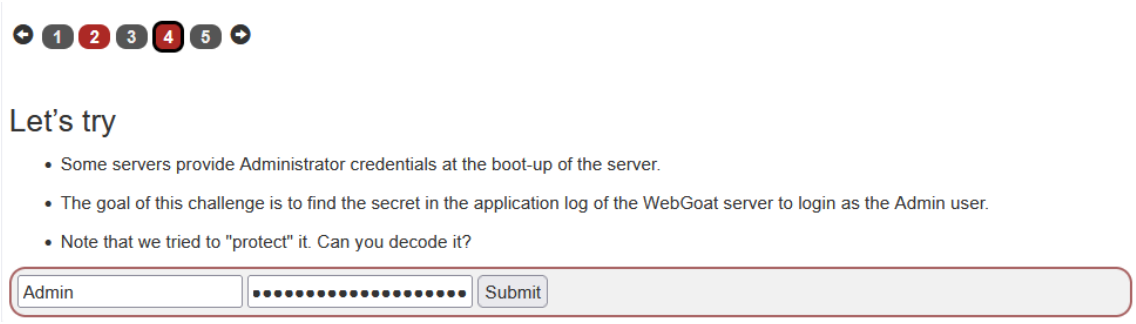
```
docker logs 7612508f4514 | grep 'Password for admin'
```

Copia el ultimo hash y decodifícalo utilizando el algoritmo con Base64.





Ingresa el valor decodificado.



Verifica que el resultado sea exitoso.