

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.



Let's try

- The goal of this challenge is to make it look like username "admin" succeeded in logging in.
- The red area below shows what will be logged in the web server's log file.
- Want to go beyond? Try to elevate your attack by adding a script to the log file.

username	password	Submit
Log output:		
Login failed for username:		

OWASP

En el primer campo **username** agrega:

```
tester Login succeeded for username: admin
```

☒

Congratulations. You have successfully completed the assignment.

Log output:

Login failed for username:tester Login succeeded for username: admin

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

➔ 1 2 3 4 5 ➔

Let's try

- Some servers provide Administrator credentials at the boot-up of the server.
- The goal of this challenge is to find the secret in the application log of the WebGoat server to login as the Admin user.
- Note that we tried to "protect" it. Can you decode it?

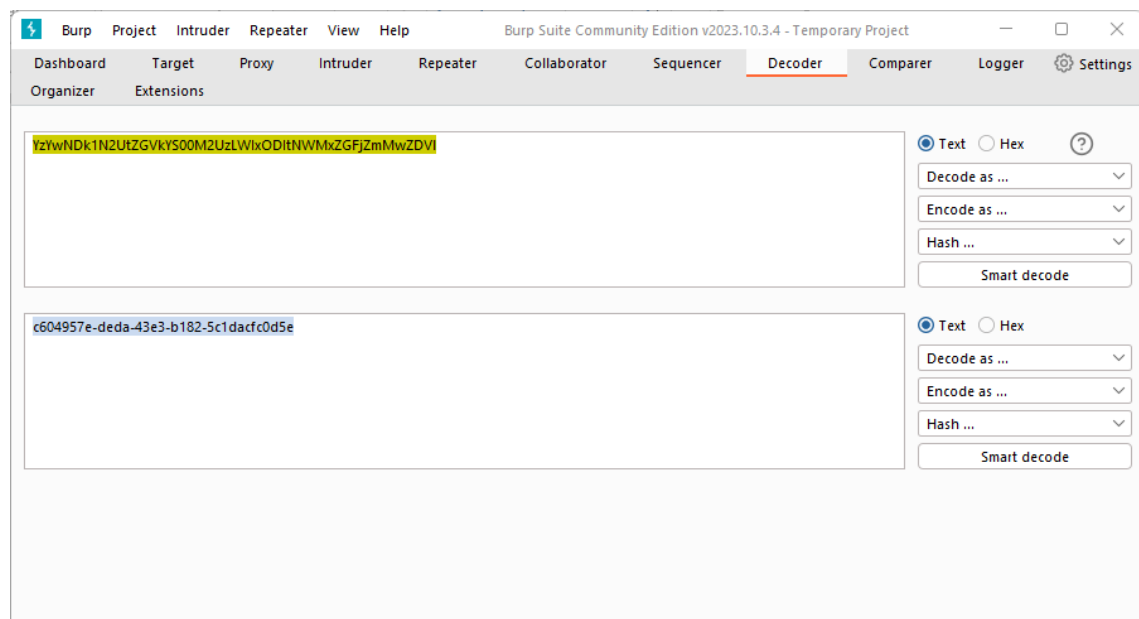
Revisa el log de la aplicación WebGoat

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.

```
2023-11-15 16:33:05.457 INFO 1 --- [main] o.o.w.lessons.logging.LogBleedingTask : Password for admin: NmU0MzY2NDYtNTMwZS00MjUzLWl0I0
DRtMDA3ZjVjN2ZzMTUz
unknown token:
unexpected token: AND auth_tan =
unexpected token: AND auth_tan =
data type of expression is not boolean
2023-11-15 17:05:10.391 INFO 1 --- [main] o.o.w.lessons.logging.LogBleedingTask : Password for admin: YzYwNDk1N2U0ZGVkYS00M2UzLWl0I0
DItNWmXZGFjZmMwZDVL
[root@centos-s-1vcpu-1gb-35gb-intel-sfo3-01 ~]#
```



Ingresa el valor decodificado.



Let's try

- Some servers provide Administrator credentials at the boot-up of the server.
- The goal of this challenge is to find the secret in the application log of the WebGoat server to login as the Admin user.
- Note that we tried to "protect" it. Can you decode it?

Submit

Verifica que el resultado sea exitoso.



Let's try

- Some servers provide Administrator credentials at the boot-up of the server.
- The goal of this challenge is to find the secret in the application log of the WebGoat server to login as the Admin user.
- Note that we tried to "protect" it. Can you decode it?

☒

Submit

Congratulations. You have successfully completed the assignment.