30/05/2023 – TryHackMe – Git Happens

Link: <https://tryhackme.com/room/githappens>

1. Instalando ferramenta *git-dumper* no kali:

$ git clone <https://github.com/arthaud/git-dumper.git>

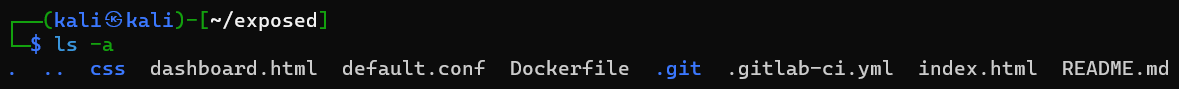
1. Esta ferramenta verifica se uma aplicação possui a vulnerabilidade “Git exposed”. Se possuir, ela baixa a pasta “.git” em um diretório especificado. Utilizando isso no alvo, baixando o “relatório” na pasta “exposed”:

$ python3 git\_dumper.py http://<ip>/.git/ ~/exposed

1. Entrando na pasta especificada

$ cd ~/exposed

1. Utilizando o comando a seguir, verifica-se que a ferramenta encontrou uma pasta .git:



1. Entrando no diretório

$ cd .git

1. Verificando os commits dados

Texto

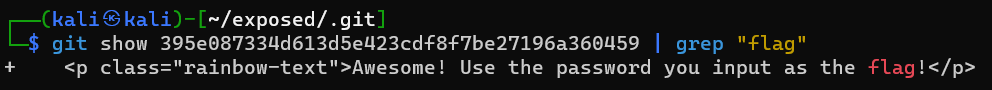
Descrição gerada automaticamente

Texto

Descrição gerada automaticamenteTexto

Descrição gerada automaticamente

1. Observando o commit de mensagem “Made the login page, boss!”, verifica um arquivo criado pelo commit. Dando uma filtrada na pesquisa, verifica-se:



1. Então, sabe-se que a chave é representada pela senha. Verificando o outro commit de mensagem “Obfuscate the source code. Hopefully security will be happy!” e filtrando pela senha:

Texto

Descrição gerada automaticamente com confiança média

Logo, a “flag” é $flag