Web Hacking

Relatório

Gabriel Oliveira

**Git Exposed**

Web hacking

Relatório

# **Git Exposed**

Relatório sobre Git Exposed.

Laboratório curso da Crowsec.

Aluno: Gabriel Oliveira Souza

**Sumário**

**1 O que é Git ……………………………………………………………….. 1**

**2 Como funciona ………………………………………………………….. 1**

**2.1 Comandos ………………………………………………………… 1**

**3 Como explorar a falha? …………………………………………………1**

**1 O que é Git**

Git é uma ferramenta utilizada para controle e gerenciamente de versionamento de determinados arquivos e códigos, o mesmo visa ajudar o usuário a ter um controle maior de seu projeto, sendo assim, ajudando o mesmo a ter uma usabilidade mais confiável e mais fluída durante o processo e ciclo de vida de seu projeto.

**2 Como funciona**

**2.1 Comandos**

O Git possui diversos comandos para o determinado usuário realizar seu gerenciamento. Os principais são:

> git clone = **‘Clona um determinado diretório’**

> git status = **‘Verifica o status dos arquivos’**

> git init = **‘Cria um novo repositório’**

> git add = **‘Adiciona um arquivo/diretório’**

> git commit = **‘Realiza o commit’**

> git log = **‘Histórico de logs’**

> git show= **‘Mosta uma determinada atualização de um arquivo’**

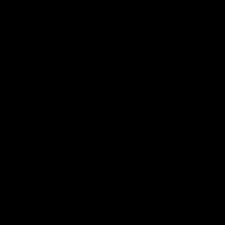
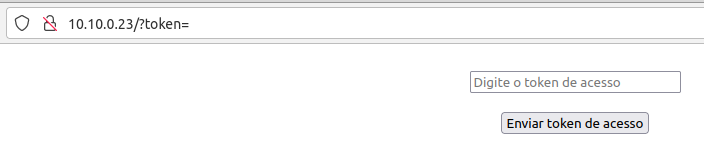
**3 Como explorar a falha?**

Neste tópico iremos utilizar a ferramenta git-dumper e realizaremos o desafio do laboratório da crowsec.

Laboratório: Git-exposed

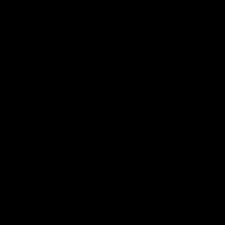
Ferrameta: Git-dumper [https://github.com/arthaud/git-dumper]

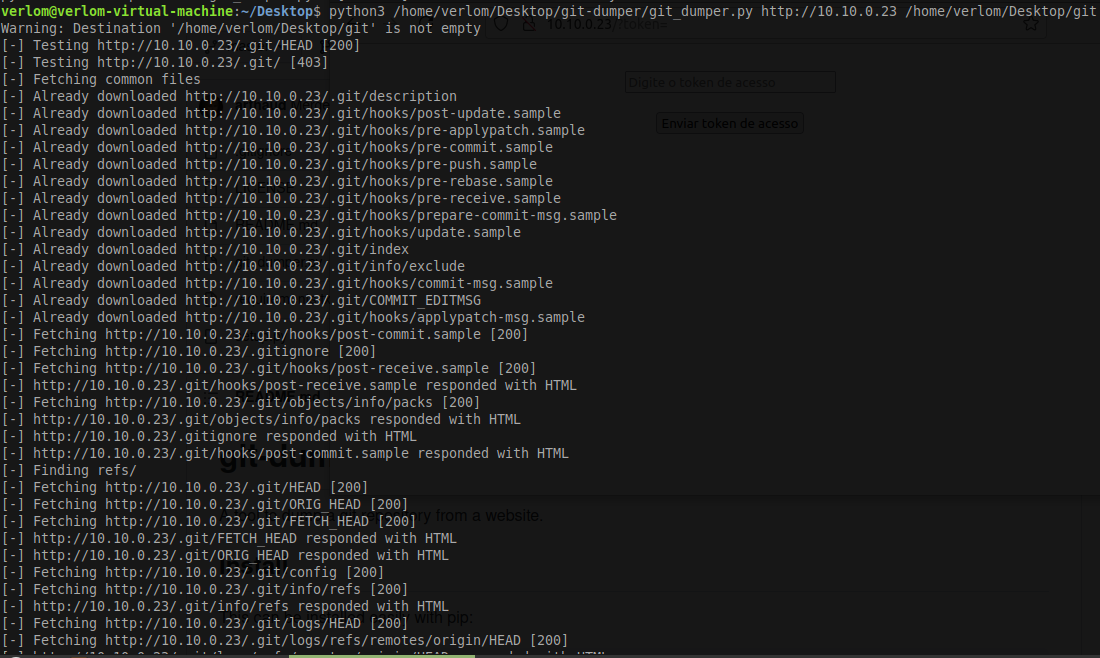
Para darmos início a resolução do laboratório, primeiro percebemos que devemos colocar uma ‘flag’ no endpoint token para a aplicação nos trazer um determinado resultado.



**Utilizando a ferramenta com o seguinte código abaixo, temos o seguinte resultado.**

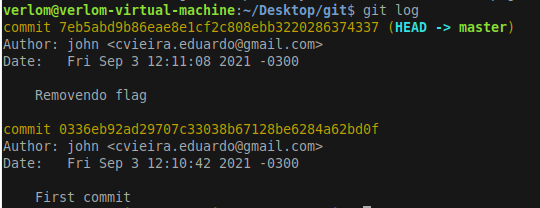
**python3 git\_dumper.py http://xx.xx.x.xx /home/verlom/Desktop/git**



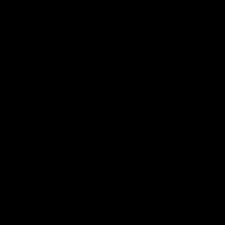
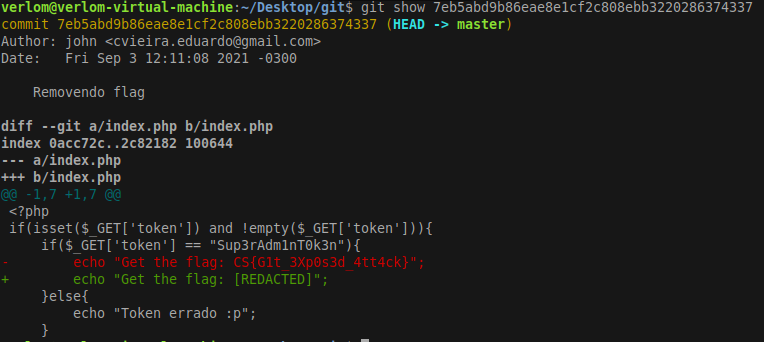
****

Logo após, verificamos que foi nos retornado um arquivo denomidado de index.php.

Podemos observar que, ao usar o comando **git init** e logo em seguida o comando **git log**, podemos perceber que existem 2 históricos, sendo o primeiro realizando o commit do arquivo e o segundo realizando uma atualização do arquivo em questão.



Para podermos ver as atualizações que o determinado arquivo sofreu, iremos utilizar o comando **git show [id commit]**, sendo assim podemos verificar o que aocnteceu de atualização em um determinado arquivo.



Sendo assim, conseguimos achar a flag do desafio.