Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Git Happens – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Git Happens – Alexandre Gualiume Coruquieri |
| **N° Revisão** | 1 |
| **Data de publicação** | 07/10/2024 |
| **Link** | https://tryhackme.com/r/room/githappens |

|  |  |  |
| --- | --- | --- |
| **Redação** | Alexandre Gualiume Coruquieri | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 07/10/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 2](#_Toc179223175)

[Desenvolvimento 2](#_Toc179223176)

[Find the super secret password 2](#_Toc179223177)

[Conclusão 7](#_Toc179223178)

[Referências 7](#_Toc179223179)

Contextualização

O CTF Git Happens apresenta uma vulnerabilidade com o controle de versionamento do Git e desafia o conhecimento do usuário em relação aos comandos do Git e sua respectiva teoria.

Desenvolvimento

Find the super secret password

Para enumerar a máquina, utiliza-se o **Nmap** no parâmetro agressivo (-A). Assim, ele mostrará as portas abertas e possíveis vulnerabilidades:

Texto

Descrição gerada automaticamente

O resultado da enumeração mostra que há um serviço Web rodando na porta 80 e um repositório Git na aplicação.

A página Web é uma simples página de login. Porém, ao analisar o código html, é notável um script criptografado:

Tela de um aparelho eletrônico

Descrição gerada automaticamente com confiança média

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Para explorar mais sobre o controle de versionamento dessa aplicação, é recomendável fazer o download dos arquivos. Então, com a ferramenta **Wget** é possível transferir os arquivos para a máquina local. Use o parâmetro (-r) para transferir os arquivos de maneira recursiva.

Texto

Descrição gerada automaticamente

Na pasta local há um arquivo git, na qual podemos ter o controle de versionamento da aplicação. Ao consultar os registros do git com o comando “git log”, exibe um commit com o nome de “Made the login page, boss!” que foi feito antes das atualizações de segurança.

Texto

Descrição gerada automaticamente

Ao retornar a versão com o comando “git checkout {código do commit}, obtém-se a primeira versão do código e sem criptografia.

Texto

Descrição gerada automaticamente

Abrindo o arquivo local ‘index.html’ e revisando o código-fonte, o script já não está criptografado, expondo as credenciais de autenticação.

Texto

Descrição gerada automaticamente

Ao colocar as credenciais na página de autenticação, o site redireciona para o arquivo ‘dashboard.html’ que contém um texto dizendo que a senha da credencial é a flag do desafio.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Conclusão

Esse CTF cumpre seu papel em demonstrar vulnerabilidades relacionadas ao Git. Além disso, serve como uma oportunidade de aprendizado e estudo sobre essa ferramenta de controle de versionamento, ajudando a fixar os comandos em geral.

Referências

* <https://git-scm.com/docs/git>