

# Writeup

---

## IDOR easy

Conseitos de segurança na web.

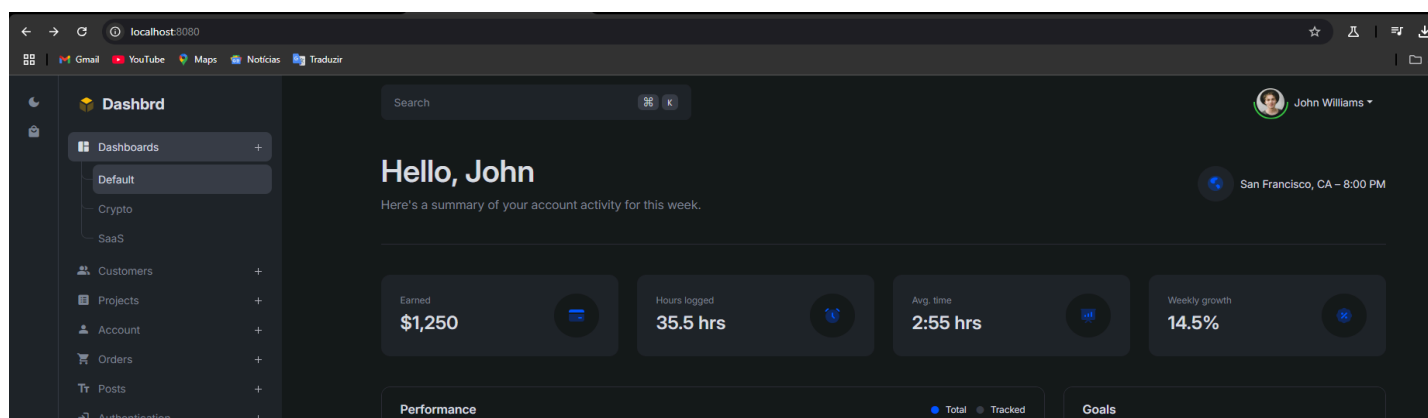


# Indexação

A vulnerabilidade de IDOR(Insecure Direct Object Reference) ocorre quando a aplicação não valida corretamente se o usuário tem permissão para acessar um determinado recurso ao alterar, por exemplo, o identificador (ID) na URL..

## Indexação de conteúdo

Quando criamos e disponibilizamos algum site o navegador disponibiliza todos os arquivos do site para busca, para limitar quais arquivos o navegador pode disponibilizar para a busca usamos o arquivo “**robots.txt**”, que não deve estar acessível ao público, pois pode mostrar arquivos ou pastas sensíveis.



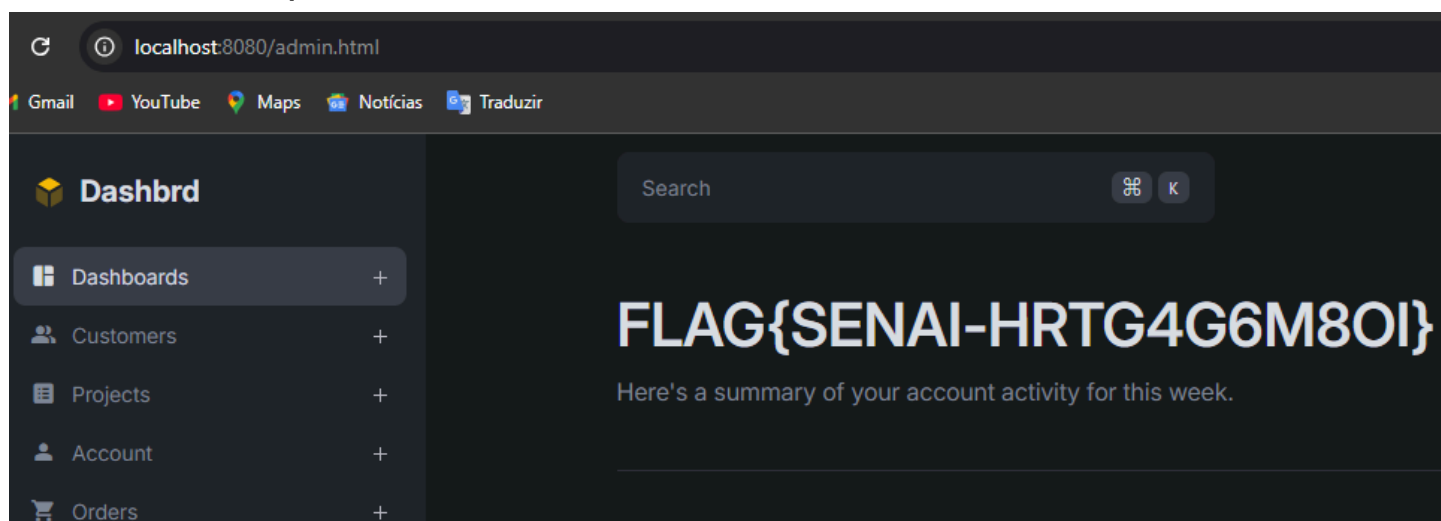
## robots.txt

Conferindo se o arquivo “**robots.txt**” está acessível notamos isso:

```
localhost:8080/robots.txt

Disallow: /admin.html
Allow: /
```

Aqui vemos que o arquivo “robots.txt” está acessível, e descobrimos um outro arquivo não indexado no google, o arquivo “admin.html”. Vamos ver o que há nesse arquivo.



Conseguimos acessar a página e pegar nossa flag.