Projeto Final 9192 Follow Guide

Tips for the Project 9192 for the big guy

The following project consists on a vulnerability reporting. Basicamente vamos ser contratados para fazer um ataque ao site que nos é dado. Usando basicamente apenas as vulnerabilidades do OWASP Top 10.

Nada demais, consists em atacar o site com o que aprendemos. Vou fazer um tips guide para todos os tópicos do OWASP e tentar ajudar com tools métodos e dicas.

1. Broken Access Control

Existe alguns tipos de BAC, mas eu vou apenas de falar do mais básico, pois o projeto não deve requerer algo muito avançado.

Broken Access Control basicamente resume-se em encontrar-mos algo que não somos suposto ver. Imagina uma pagina que é suposto estar atrás de um login, ou atrás de uma algum tipo autenticação. Basicamente um aceder-mos a algo que não temos autorização.

Simplesmente falando, isto basicamente é um atacante dar bypass de autorização que o permite ver data sensível ou executar funções que não era suposto.

Se não fui explicito vou tentar explicar com o seguinte exemplo. Que é o mesmo do TryHackMe que acho bastante fácil de entender.

IDOR

O IDOR é um tipo de BAC que é bastante facil de dar exploit.

Vamos imaginar que entramos na nossa conta de Facebook. E olhamos para o link e vemos:

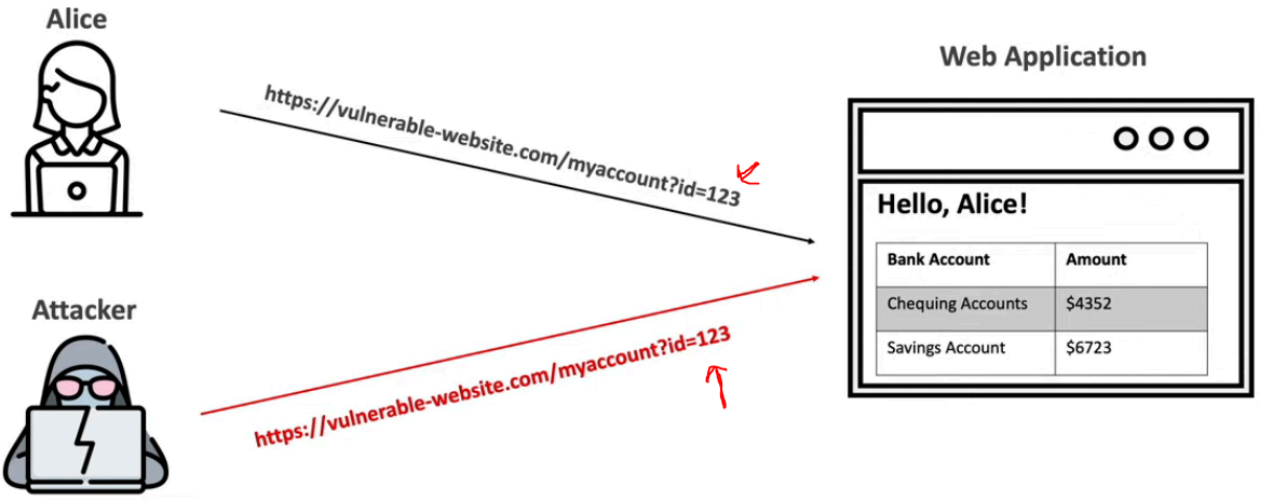
```
www.facebook.com/profile?id=1904
```

Para alguns é só um link normal, para nós gays, é mais que um link. É uma porta de entrada. hihihi. Mano tenho de deixar de escrever tanto. My bad.

Basicamente se virem essa merda no link. Tentem alterar:

```
www.facebook.com/profile?id=1111
```

Por vezes trocam a conta e vêm informação que não deviam.

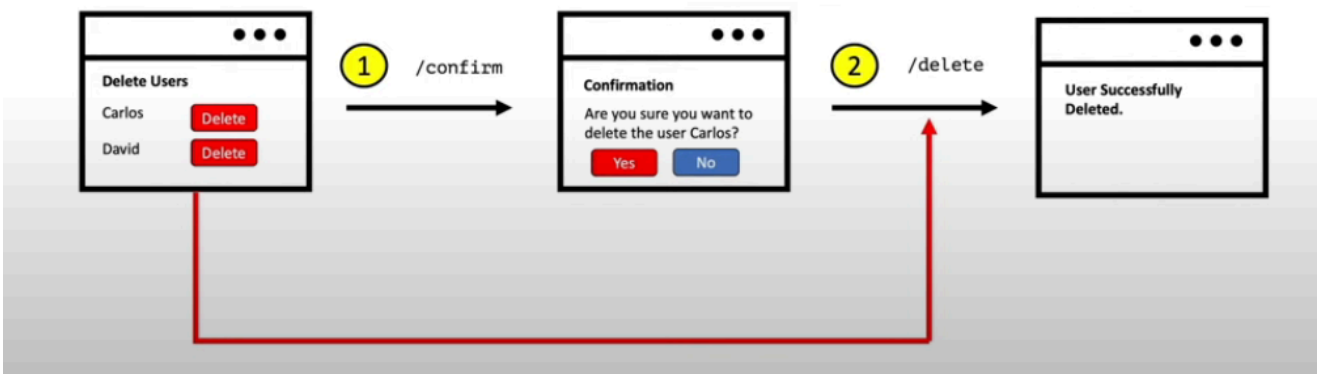


Este maneira é a mais fácil de fazer e entender. Há no entanto mais maneiras.

Qualquer parâmetro que consigam trocar para vos dar mais acesso.

MULTI STEP

Duvido que apareça mas é uma merda tipo assim. Ficam só com a info.



Other

Algumas vezes tambem podemos mudar certas coisas no POST, basicamente como fariamos com o SQL injection, mas isto é apenas para o WebServer.

Ou até manipular a cookie.

Main	Descrição
Tools	BurpSuite ou ZAP - Pode ajudar em alguns casos de BAC, em que tenhamos de alterar o parâmetro lá.
Sumario do IDOR	Alterar um campo no URL que nos permite alterar o Objeto no server e que nós permite ver algo que não devíamos
Multi	Trocar outros campos que permitam saltar alguma step que normalmente iriamos encontrar.
Gobuster	Enumerarem as directories pode ajudar a apanhar estes campos.

2. Falhas de Criptografia

Metido muito básico, quando o nome diz. Quando falhamos em encriptar algo.

Qualquer pessoa que se meta no meio da nossa ligação pode ver tudo.

Causas:

Uso de Algoritmos fracos e deprecados. (Tipo MD5 hashing)
Poor key management (Às vezes a chave da encriptação tá no source code)
Falta de encriptação em data sensível (estar guardado no server em plain-text)
Transmissão insegura dessa mesma data também (TLS 1.0)
Protocolos mal implementados

Ataque:

Man in the middle apanha bem as transições desta falha de merda.

Databases podem ser stored as files, isto não seria um rpoblema mas o que acontece é que a database as vezes está na root do site. e podemos aceder á DB por causa disso.

Tipo: `https://www.anaclidesde4.com/data.db`

Ou seja em vez de atacarmos o servidor da DB que devia estar remotamente
o atacker só precisa do endereço certo, baixar o file, e pronto: tem acesso a tudo.

Em conjunto com o SQL-Injection podemos ter acesso também as hashes. E se o algoritmo de encriptação for uma merda, boom tens a pass, deste crack.

TOOLS e MAIN	**Description**
Wireshark	Podem usar para ver o http em plain text
John the ripper	Dar crack das hashes, peçam ajuda se nao souberem usar o João estripador
SQL MAP	Falo disto mais tarde mas achei que tinha de meter só naquela referência de terem as passes.
Crackstation	https://crackstation.net/
Ethercap	Man in the middle - usamos com o roger (nao vai ser preciso)