

# [E]ACH inTheShell\_

Encontro GEN4 - WEB



2022

# Roteirinho =)

1

Natas (0 ao 8)

*<https://overthewire.org/wargames/natas/>*



# exploração web

---



01.

## código fonte

buscar informações relevantes no código fonte, sejam comentários, links ou sugestões de arquivos.



02.

## subdiretórios

um site contém pastas e arquivos. Cada pasta é um diretório e as pastas dentro de diretórios, há subdiretórios.

# ferramentas

---

F01.

## Gobuster

é um enumerador que utiliza ataque de dicionário e força bruta em URIs, subdomínios DNS e nomes de hosts virtuais em servidores web.

### hint:

Com dirb: `usr/share/dirb/wordlists/common.txt`  
<https://github.com/v0re/dirb/blob/master/wordlists/common.txt>

### dns

procurar um subdomínio

### dir

procura diretórios e arquivos

### -u *[string]*

url alvo da ferramenta

### -P e -U *[string]*

password e user respectivamente

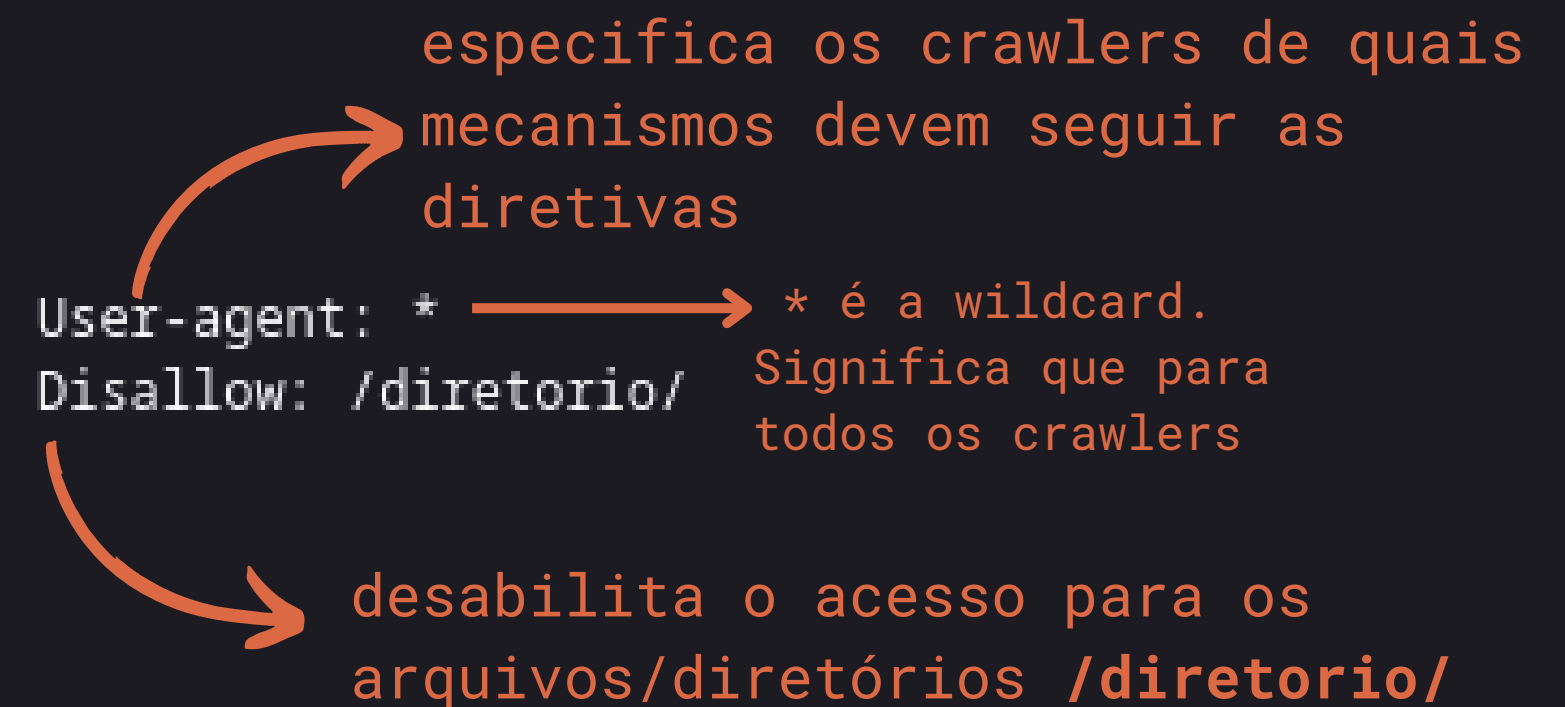
### -w *[file]*

wordlist utilizada para força bruta

# conceitos

## robots.txt

crawlers: programas ou scripts que carregam páginas web de forma automatizada para mecanismos de busca indexarem. No arquivo robots.txt, é possível restringir o que o crawler pode acessar.



especifica os crawlers de quais mecanismos devem seguir as diretivas

```
User-agent: *
```

\* é a wildcard. Significa que para todos os crawlers

```
Disallow: /diretorio/
```

desabilita o acesso para os arquivos/diretórios **/diretorio/**

# inspecionar

04.

## network

aqui você tem informações sobre a requisição feita entre cliente e servidor. o header mostra informações enviadas do usuário para o servidor e as informações devolvidas pelo servidor.

HTTP REQUEST: que o cliente envia

HTTP RESPONSE: o que o servidor retorna

05.

## cookies

é um arquivo pequeno ou pacote de dados que fica armazenado no computador do usuário enquanto ele está acessando aquela página.

06.

## url

analisar a url é essencial para ver se é possível deduzir existência de diretórios, arquivos e até mesmo mudar parâmetros (quando o site estiver em PHP, por exemplo)

# ferramentas

---

F02.

## curl

é um comando utilizado para transferir informações para ou de um servidor

### hint:

quer aprender mais sobre curl?  
<https://reqbin.com/curl>

```
-u [user:password]
```

seta o usuário e senha

```
-o [file]
```

joga o output do comando em um arquivo

```
--cookie [cookie=value]
```

envia cookies específicos para a página

```
--data [['info=value']][url]]
```

envia uma requisição personalizada

... etc

# vulnerabilidade

---

`file include vulnerability`

**GET** informações passadas no  
cabeçalho da requisição e podem  
ser vistos na URI

**POST** informações passadas no corpo  
da requisição HTTP, escondendo  
na URI

métodos de  
passagem de  
parâmetro





# vulnerabilidade



## **file include vulnerability**

aparece em sites que não foram bem escritos.

a requisição de arquivos é feita de forma vulnerável, o que permite com que o atacante consiga executar qualquer arquivo, manipulando a requisição.

no código

```
include($_GET['variavel']);
```

no site

```
site.com/index.html?variavel=[valor]
```

WEB

## outras ferramentas importantes

F03.

**nmap**

scanea um alvo, reportando quais portas estão abertas, seu estado e qual serviço está rolando em cada uma



Teste aqui!  
<http://scanme.nmap.org/>

# common vulnerabilities and exposures (CVE)

lista pública de falhas de segurança. quando são denunciadas, elas recebem um número de identificação e uma pontuação de 0 a 10 que indicam sua gravidade.

- MITRE
  - empresa que administra o sistema de CVE
- exploit DB
  - ferramenta para pesquisa de CVE e se há exploits disponíveis para determinada falha.

WEB

## outras ferramentas importantes

F04.

### whatweb

é uma ferramenta que identifica a tecnologia utilizada no site, além de informações complementares.

**-v** verboso



Teste aqui!  
<http://testphp.vulnweb.com/>

## outras ferramentas importantes



Teste aqui!  
<http://testphp.vulnweb.com/>

F05.

### nikto

essa ferramenta tem como objetivo analisar as vulnerabilidades comuns em web, encontrando arquivos, padrões e configurações inseguras

- h define o host para fazer scan
- o exporta o output
- ssl para scanear sites https

WEB

**tarefinhas**

**PicoCTF**

where are the robots

Secrets

picobrowser

Forbidden Paths

