LAB - SEM 05 - Info Gathering WEB

LAB01: d81j237sh102k3a88njsnna12

```
dirb http://businesscorp.com.br /usr/share/dirb/wordlists/small.txt -a "Cavalo"
```

Seguimos a dica de mudar o nome do user-agent e aplicamos o bruteforce com a small.txt
do dirb.
Esperamos bastante até que se chegasse na verificação do diretório db
A key estava no arquivo encontrado em businesscorp.com.br/db/update

LAB02: 1nf0gh4t3r1ng89271882
Ao realizar a busca pelo /sitemap da business, encontramos um outro diretório indicado
que é o /painelcliente
Nele, ao inpescionarmos o código fonte, obtemos a key

```
<br>
vlab | sitemap
<br>
<!--
Olhar o codigo fonte da pagina sempre e uma boa pratica de recon! Key: 1nf0gh4t3r1ng89271882
<br>
-->
```

LAB03: g80889113568fkp9
Quando realizamos um bruteforce, encontramos um diretório chamado
~administrator
Lá teremos um arquivo.txt com a key desejada

LAB04: 65784920123nvw0f4
Aplicamos o mesmo método do LAB08, mas com extensão .txt
o arquivo era info.txt, de onde obtivemos a key

LAB05: W3bR3nc0nisN3c3ss4ry10
Quando buscamos no google por site:businesscorp.com.br api,
encontramos um diretório chamado apiCliente
Basta analisar o arquivo.xml para encontrar a key

LAB06: bkmc5502874hdkiw91244hh
Ao realizar o bruteforce com o dirb, mudando o nome do user-agent,
encontramos um diretório chamado /adminhelp
Nele, um arquivo de texto que conterá a key

```
dirb http://rh.businesscorp.com.br  /usr/share/dirb/wordlists/big.txt -a
"Cavalo"
```

A opção -a serve para mudar o user-agent

LAB07: 00289jfhsyw72ll399s1
Executando o mesmo dirb do lab06, encontramos o arquivo /webdata,
onde estará a key

LAB08: ed05a6d4d2fb2c6a35fe40c0e53386f2

Criamos um script para executar um brute force em arquivos php no site da rh.business

```
for palavra in $(cat small_php.txt)
do

curl -s -o /dev/null  -H "User-Agent: Cavalo"  -w "%{http_code}"
rh.businesscorp.com.br/$palavra

echo "Encontrado: rh.businesscorp/$palavra"

done
```

Essa wordlist foi uma modificação de uma das wordlists padrão do curl, chamada small.txt
Adicionamos um .php ao final de cada palavra com o seguinte comando

```
sed 's/$/.php/' small.txt > small_php.txt
```

A wordlist pôde ser encontrada no diretório /usr/share/dirb/wordlists

O diretório que retornou 200 foi o /backup.php

LAB09: Apache/2.4.7
Obtivemos essa resposta analisando o banner apresentado ao executar uma requisição que dava erro rh.businesscorp.com.br/jbjfksjdf

LAB10: PHP/5.5.9
Fizemos a busca no whatweb
https://whatweb.net/

```
http://rh.businesscorp.com.br [200 OK] Apache[2.4.7],
 Bootstrap, Country[FRANCE][FR],
 HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.7 (Ubuntu)],
 IP[37.59.174.229],
 JQuery, PHP[5.5.9-1ubuntu4.22],
 Script, Title[Recursos Humanos],
 X-Powered-By[PHP/5.5.9-1ubuntu4.22],
 X-UA-Compatible[IE=edge]
```