

Estudando a Lógica do Programa

- + O objetivo é fazer uma requisição na mão do tipo GET e analisar a response
- + O HTTP 200 indica que a página existe. Caso não existisse, o retorno seria 404
- + Os programas como o dirb mandam requisições http e analisam a resposta do servidor

```
root@pentest:~/Desktop# nc -v businesscorp.com.br 80
DNS fwd/rev mismatch: businesscorp.com.br != ip225.ip-37-59-174.eu
businesscorp.com.br [37.59.174.225] 80 (http) open
GET /app/ HTTP/1.0

HTTP/1.1 200 OK
Date: Thu, 26 Sep 2019 09:00:36 GMT
Server: Apache/2.2.22 (Debian)
X-Powered-By: PHP/5.4.45-0+deb7u2
Vary: Accept-Encoding
Content-Length: 185
Connection: close
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" />
```