

# Enumerando HTTP

~~~~~  
O que buscamos?  
~~~~~

- + Versões do Web Server (IIS, Apache, Nginx, etc)
- + Tecnologias utilizadas (PHP, ASP, JSP, etc)
- + Métodos aceitos (PUT, POST, DELETE, etc)

~~~~~  
Como fazer?  
~~~~~

- + Portas comuns: 80,8080,81,8081 (podemos ter um servidor web rodando em qualquer porta TCP)
- + Versões do protocolo: HTTP/1.0 | HTTP/1.1 (usar o Host:)
- + Requisições: GET | HEAD | OPTIONS
- + Utilitários: nc | curl | telnet

- ~~~~~
- + Importância de passar o host quando for usar o HTTP/1.1:  
→ as vezes o mesmo endereço de IP pode ser usado para diferentes host, por ser compartilhado (isso também pode acontecer quando for usado um proxy)

```
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 / HTTP/1.1
Host: businesscorp.com.br

HTTP/1.1 200 OK
Date: Sun, 06 Oct 2019 02:19:32 GMT
Server: Apache/2.2.22 (Debian)
Last-Modified: Wed, 25 Sep 2019 17:05:45 GMT
ETag: "20463-1bb6-59363a9ea0957"
Accept-Ranges: bytes
Content-Length: 7094
Vary: Accept-Encoding
Content-Type: text/html

<!DOCTYPE html>
<!--[if lt IE 8 ]><html class="no-js ie ie7" lang="en"> <![endif]-->
<!--[if IE 8 ]><html class="no-js ie ie8" lang="en"> <![endif]-->
<!--[if (gte IE 8)!(IE)]><!--><html class="no-js" lang="en"> <!-->
<head>

<!-- Basic Page Needs
===== -->
<meta charset="utf-8">
```

- + **OBS:** As vezes a versão da tecnologia não é evidenciada de cara numa requisição do tipo GET.  
Para resolver isso, devemos fazer uma busca por arquivos que usem

essa tecnologia, mesmo que eles não existam.

+ Exemplo: Identifiquei que é usada a tecnologia ASP. Pra que eu saiba qual a versão, devo fazer uma requisição por arquivos dessa extensão:

GET /index.aspx HTTP/1.0