

Introdução - Web Recon

- + Identificar o WebServer
- + Identificar a tecnologia
- + Diretórios
- + Arquivos
- + Possíveis controles e bloqueios
- + Métodos http permitidos
- + Listagem de diretórios
- + Estrutura da página
- + Código fonte
- + Analisar arquivos encontrados

~~~~~

Para isso, usaremos as seguintes técnicas

- |                            |                               |
|----------------------------|-------------------------------|
| + Parsing HTML/JS          | + Burp Suite (Proxy)          |
| + Mirror Website           | + Whatsweb                    |
| + Robots.txt/Sitemap.xml   | + Wappalyzer                  |
| + Análise de resostas HTTP | + Análise de extensões e Icon |
| + Bypass User-Agent        | + Análise de erros e banners  |

~~~~~

Mapear a página

- | | |
|-----------------------------------|-------------------|
| → Login? | → Upload? |
| → Cadastro? É possível cadastrar? | → Download? |
| → Busca? | → Erros? |
| → Posts? | → Banco de dados? |
| → Redirecionamento? | → Envio de dados? |