Secure Learning Platform

António Pinheiro – up201704931
Manuel Veiga – up201905924
Simão Ribeiro – up202309188

Índice

01

Contexto

02

Arquitetura

03

Security Hardening

04

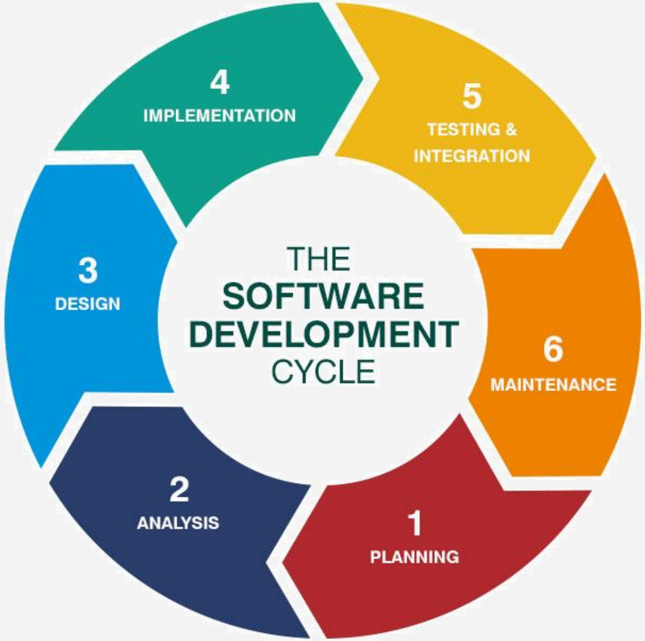
Testes de Segurança

05

Conclusão

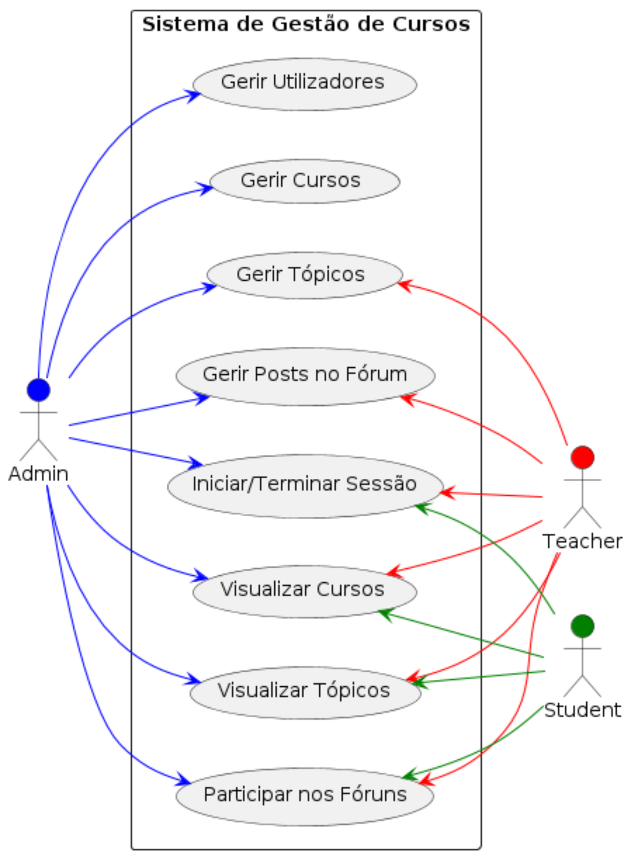
Contexto

- ***Shift-Left Security***
- ***Postura Proativa***



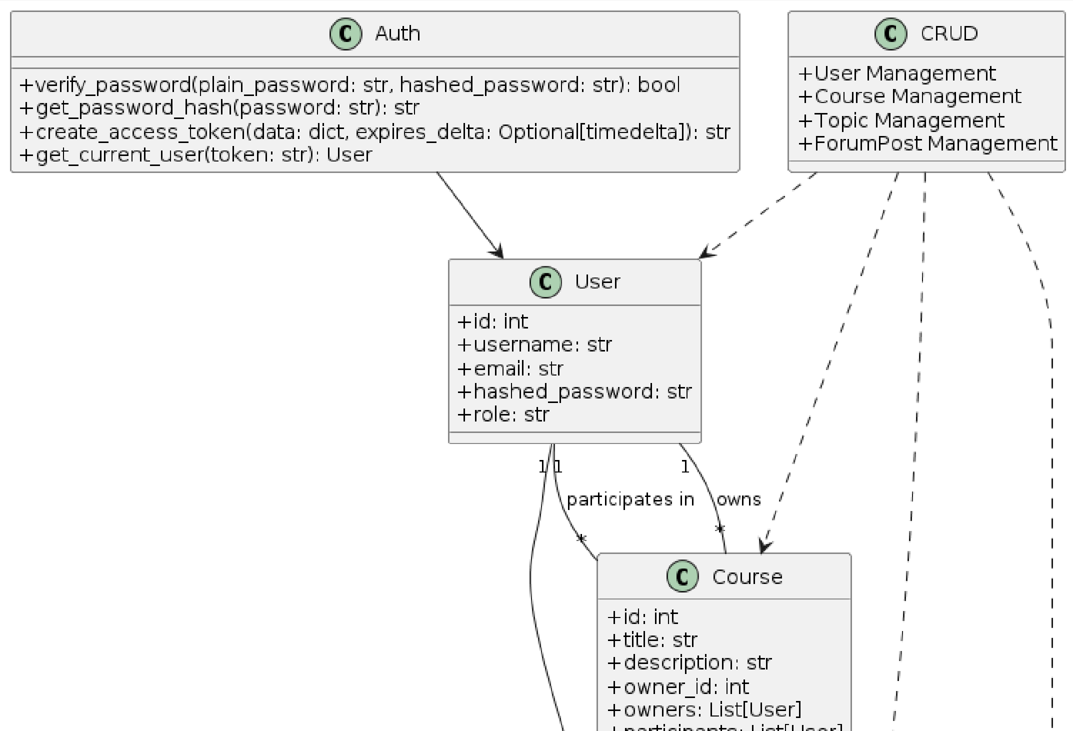
Arquitetura

- **Diagrama de Casos de Uso**
- **Controlo de Acessos**



Arquitetura

- **Diagrama de Classes**



Auth

+verify_password(plain_password: str, hashed_password: str): bool
+get_password_hash(password: str): str
+create_access_token(data: dict, expires_delta: Optional[timedelta]): str
+get_current_user(token: str): User

CRUD

+User Management
+Course Management
+Topic Management
+ForumPost Management

User

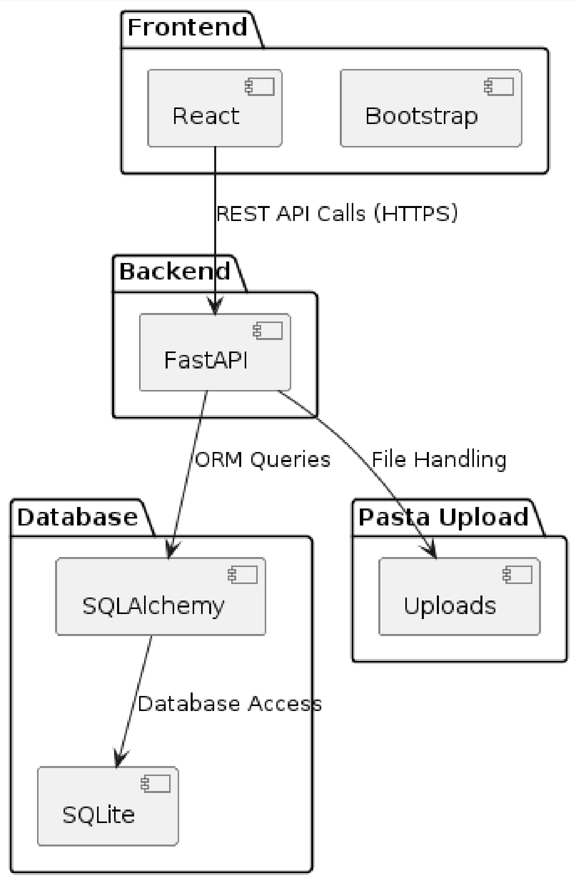
+id: int
+username: str
+email: str
+hashed_password: str
+role: str

Course

+id: int
+title: str
+description: str
+owner_id: int
+owners: List[User]
+participants: List[User]

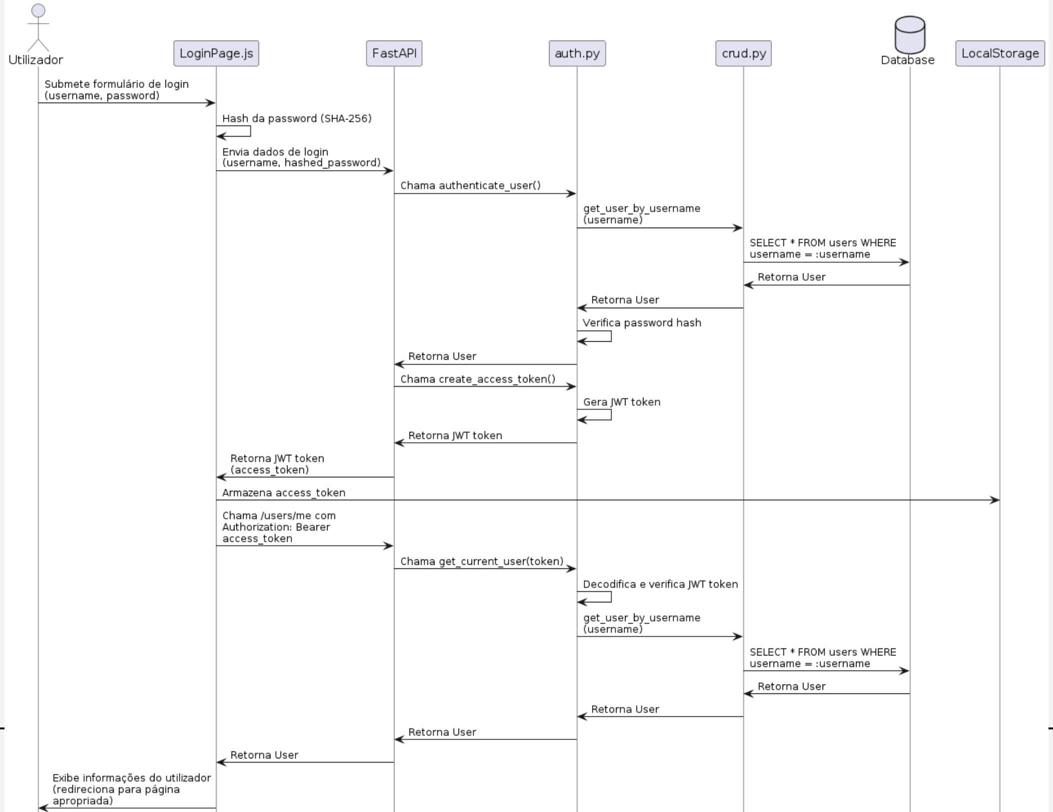
Arquitetura

- **Diagrama de Componentes**



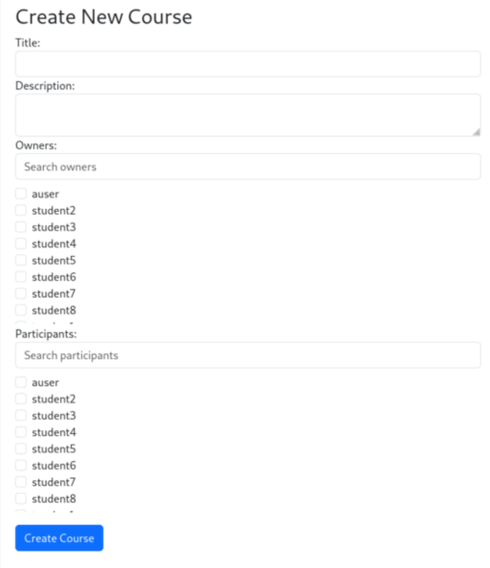
Arquitetura

- Processo de Autenticação


Utilizador
LoginPage.js
FastAPI
auth.py
crud.py
Database
LocalStorage
Submete formulário de login (username, password)
Hash da password (SHA-256)
Envia dados de login (username, hashed_password)
Chama authenticate_user()
get_user_by_username (username)
SELECT * FROM users WHERE username = :username
Retorna User
Retorna User
Verifica password hash
Retorna User
Chama create_access_token()
Gera JWT token
Retorna JWT token
Retorna JWT token (access_token)
Armazena access_token
Chama /users/me com Authorization: Bearer access_token
Chama get_current_user(token)
Decodifica e verifica JWT token
get_user_by_username (username)
SELECT * FROM users WHERE username = :username
Retorna User
Retorna User
Retorna User
Retorna User
Exibe informações do utilizador (redireciona para página apropriada)

Arquitetura

- Processo de Criação de Curso



Create New Course

Title:

Description:

Owners:

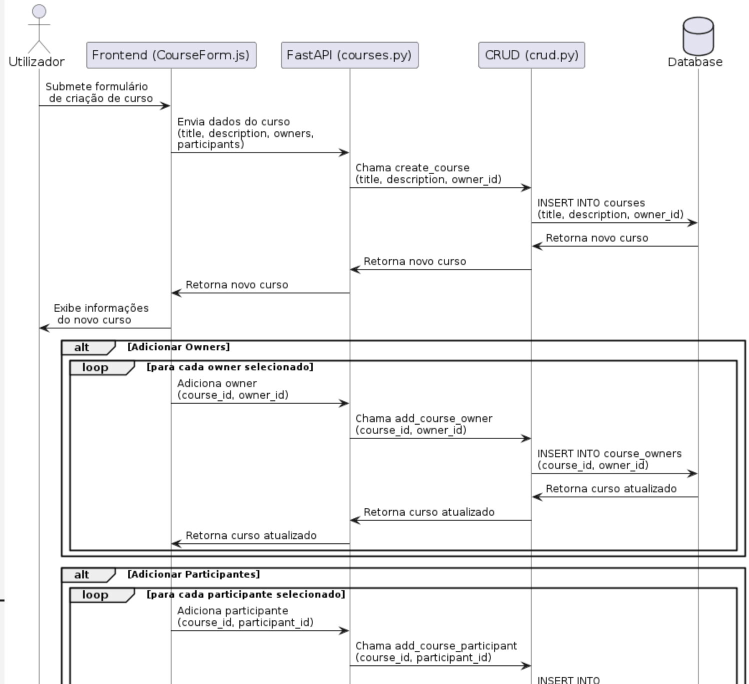
Search owners

□ auser
□ student2
□ student3
□ student4
□ student5
□ student6
□ student7
□ student8

Participants:

Search participants

□ auser
□ student2
□ student3
□ student4
□ student5
□ student6
□ student7
□ student8



Submete formulário de criação de curso

Envia dados do curso (title, description, owners, participants)

Chama create_course (title, description, owner_id)

INSERT INTO courses (title, description, owner_id)

Retorna novo curso

Retorna novo curso

Retorna novo curso

Exibe informações do novo curso

alt [Adicionar Owners]

loop [para cada owner selecionado]

Adiciona owner (course_id, owner_id)

Chama add_course_owner (course_id, owner_id)

INSERT INTO course_owners (course_id, owner_id)

Retorna curso atualizado

Retorna curso atualizado

Retorna curso atualizado

alt [Adicionar Participantes]

loop [para cada participante selecionado]

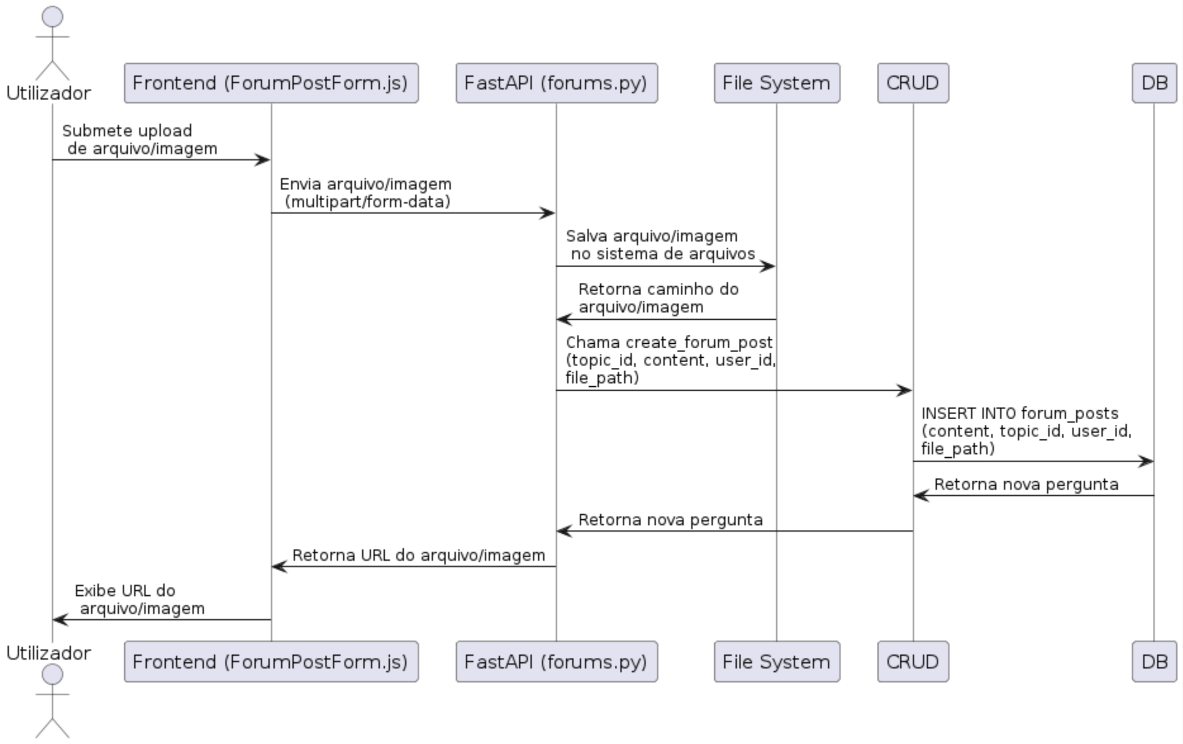
Adiciona participante (course_id, participant_id)

Chama add_course_participant (course_id, participant_id)

INSERT INTO

Arquitetura

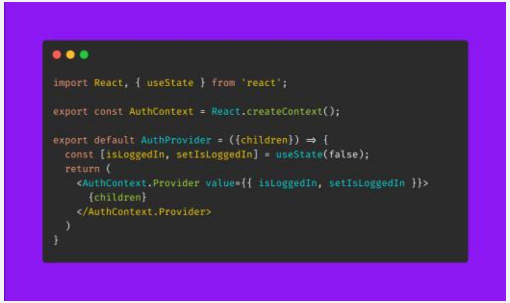
- Processo de Post Forum e Upload de Arquivo/Imagem


Utilizador
Frontend (ForumPostForm.js)
FastAPI (forums.py)
File System
CRUD
DB
Submete upload de arquivo/imagem
Envia arquivo/imagem (multipart/form-data)
Salva arquivo/imagem no sistema de arquivos
Retorna caminho do arquivo/imagem
Chama create_forum_post (topic_id, content, user_id, file_path)
INSERT INTO forum_posts (content, topic_id, user_id, file_path)
Retorna nova pergunta
Retorna nova pergunta
Retorna URL do arquivo/imagem
Exibe URL do arquivo/imagem
Utilizador
Frontend (ForumPostForm.js)
FastAPI (forums.py)
File System
CRUD
DB

Security *Hardening* – Autenticação e Sessão

- Token JWT, guardado na localstorage após log in do utilizador;

- Controlo de *Routing* e Autenticação através do token e query para obter as informação sobre o user atual;



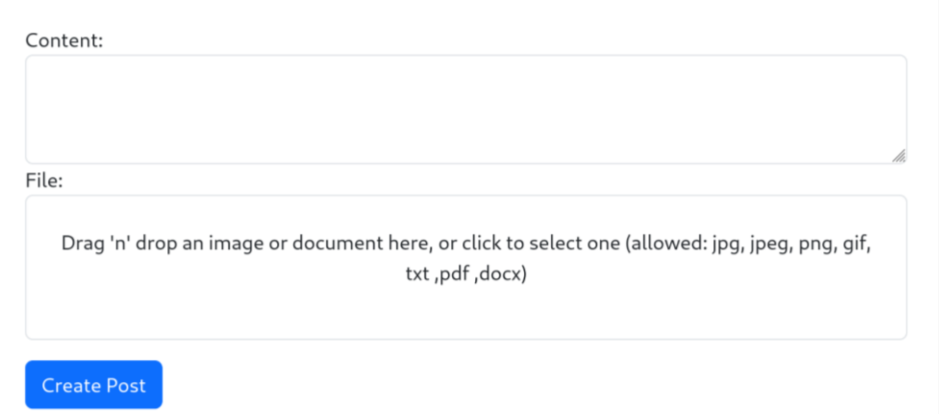
```
import React, { useState } from 'react';

export const AuthContext = React.createContext();

export default AuthProvider = ({children}) => {
  const [isLoggedIn, setIsLoggedIn] = useState(false);
  return (
    <AuthContext.Provider value={{ isLoggedIn, setIsLoggedIn }}>
      {children}
    </AuthContext.Provider>
  )
}
```

Security Hardening – Parametrização

- ORM Querying + SQLAlchemy para abstração e parametrização de queries;

Security Hardening – Injeção

- Restrição da Extensão dos ficheiros permitidos no fórum;
- Expressões Regulares para prevenir XSS nos comentários dos fórum – pattern = r’[<>]’;

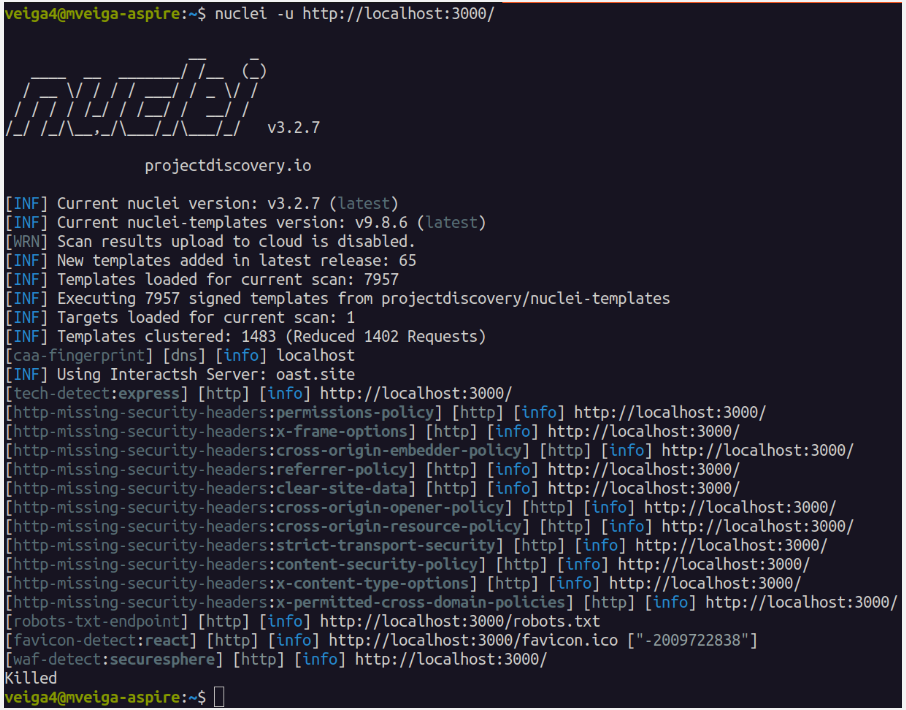


Content:

File:

Drag 'n' drop an image or document here, or click to select one (allowed: jpg, jpeg, png, gif, txt ,pdf ,docx)

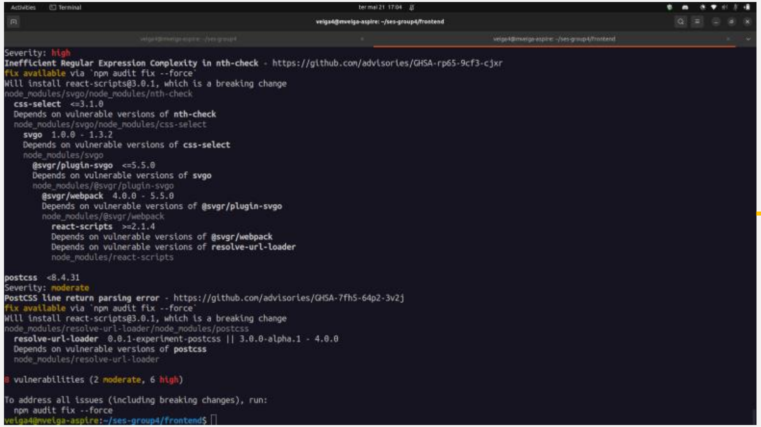
Análise Dinâmica – Wappalyzer & Nuclei



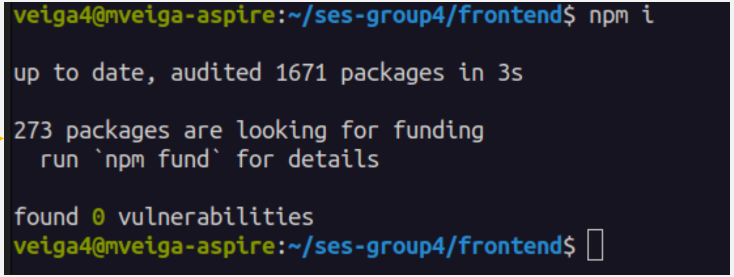
```
veiga4@mveiga-aspire:~$ nuclei -u http://localhost:3000/

                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.7

                projectdiscovery.io

[INF] Current nuclei version: v3.2.7 (latest)
[INF] Current nuclei-templates version: v9.8.6 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 65
[INF] Templates loaded for current scan: 7957
[INF] Executing 7957 signed templates from projectdiscovery/nuclei-templates
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1483 (Reduced 1402 Requests)
[caa-fingerprint] [dns] [info] localhost
[INF] Using Interactsh Server: oast.site
[tech-detect:express] [http] [info] http://localhost:3000/
[http-missing-security-headers:permissions-policy] [http] [info] http://localhost:3000/
[http-missing-security-headers:x-frame-options] [http] [info] http://localhost:3000/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://localhost:3000/
[http-missing-security-headers:referrer-policy] [http] [info] http://localhost:3000/
[http-missing-security-headers:clear-site-data] [http] [info] http://localhost:3000/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://localhost:3000/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://localhost:3000/
[http-missing-security-headers:strict-transport-security] [http] [info] http://localhost:3000/
[http-missing-security-headers:content-security-policy] [http] [info] http://localhost:3000/
[http-missing-security-headers:x-content-type-options] [http] [info] http://localhost:3000/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://localhost:3000/
[robots-txt-endpoint] [http] [info] http://localhost:3000/robots.txt
[favicon-detect:react] [http] [info] http://localhost:3000/favicon.ico ["-2009722838"]
[waf-detect:securesphere] [http] [info] http://localhost:3000/
Killed
veiga4@mveiga-aspire:~$
```

Análise Estática – NPV

- Node’s Packet Vulnerability Search (npm)

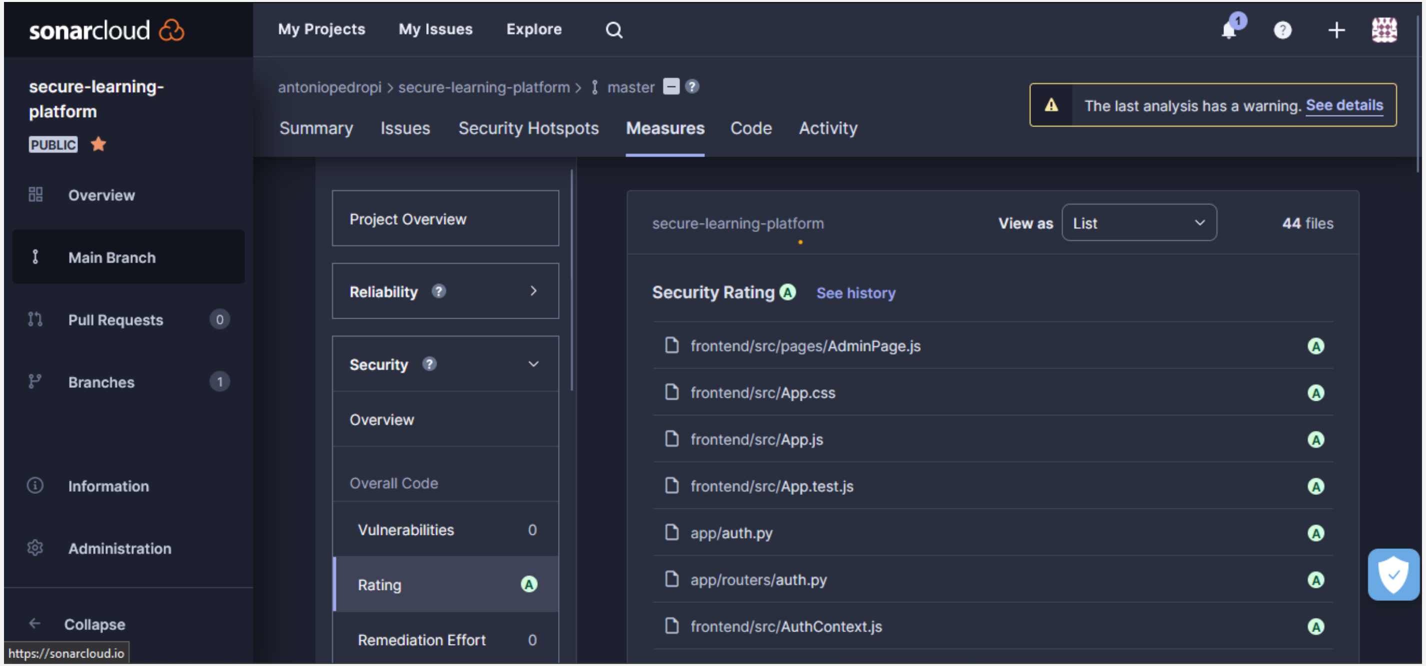

Activities
Terminal
ter mai 21 17:04
veiga4@mveiga-aspire: ~/ses-group4/frontend
veiga4@mveiga-aspire: ~/ses-group4
veiga4@mveiga-aspire: ~/ses-group4/frontend

```
Severity: high
Inefficient Regular Expression Complexity in nth-check - https://github.com/advisories/GHSA-rp65-9cf3-cjxr
fix available via `npm audit fix --force`
Will install react-scripts@3.0.1, which is a breaking change
node_modules/svgo/node_modules/nth-check
  css-select  <=3.1.0
  Depends on vulnerable versions of nth-check
  node_modules/svgo/node_modules/css-select
    svgo  1.0.0 - 1.3.2
    Depends on vulnerable versions of css-select
    node_modules/svgo
      @svgr/plugin-svgo  <=5.5.0
      Depends on vulnerable versions of svgo
      node_modules/@svgr/plugin-svgo
        @svgr/webpack  4.0.0 - 5.5.0
        Depends on vulnerable versions of @svgr/plugin-svgo
        node_modules/@svgr/webpack
          react-scripts  >=2.1.4
          Depends on vulnerable versions of @svgr/webpack
          Depends on vulnerable versions of resolve-url-loader
          node_modules/react-scripts

postcss  <8.4.31
Severity: moderate
PostCSS line return parsing error - https://github.com/advisories/GHSA-7fh5-64p2-3v2j
fix available via `npm audit fix --force`
Will install react-scripts@3.0.1, which is a breaking change
node_modules/resolve-url-loader/node_modules/postcss
  resolve-url-loader  0.0.1-experiment-postcss || 3.0.0-alpha.1 - 4.0.0
  Depends on vulnerable versions of postcss
  node_modules/resolve-url-loader

8 vulnerabilities (2 moderate, 6 high)

To address all issues (including breaking changes), run:
  npm audit fix --force
veiga4@mveiga-aspire:~/ses-group4/frontend$ 
```



```
veiga4@mveiga-aspire:~/ses-group4/frontend$ npm i

up to date, audited 1671 packages in 3s

273 packages are looking for funding
  run `npm fund` for details

found 0 vulnerabilities
veiga4@mveiga-aspire:~/ses-group4/frontend$ 
```

Análise Estática – Sonar Cloud



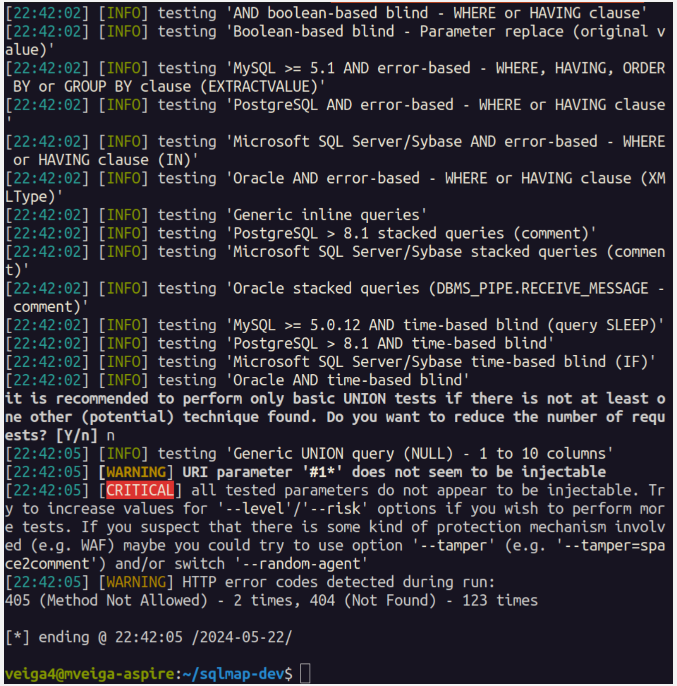
The last analysis has a warning. See details

secure-learning-platform — 44 files

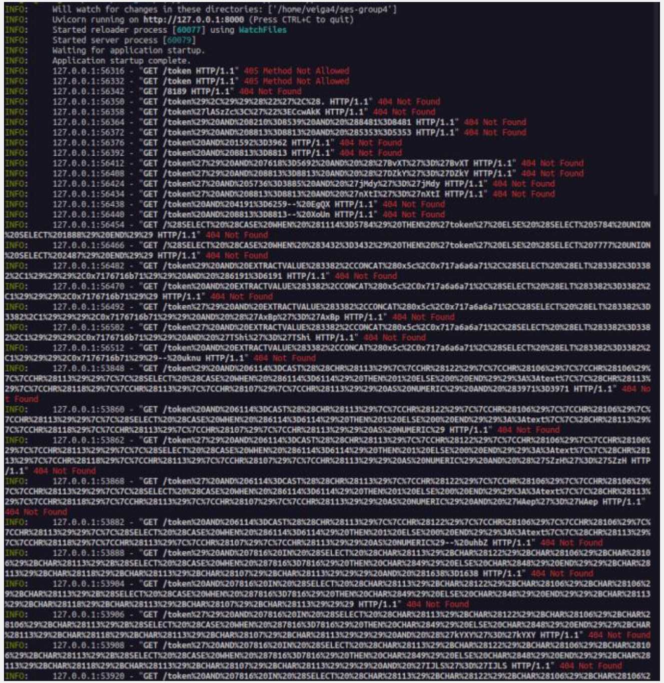
Security Rating A

frontend/src/pages/AdminPage.js	A
frontend/src/App.css	A
frontend/src/App.js	A
frontend/src/App.test.js	A
app/auth.py	A
app/routers/auth.py	A
frontend/src/AuthContext.js	A

Análise Dinâmica – SQLMap

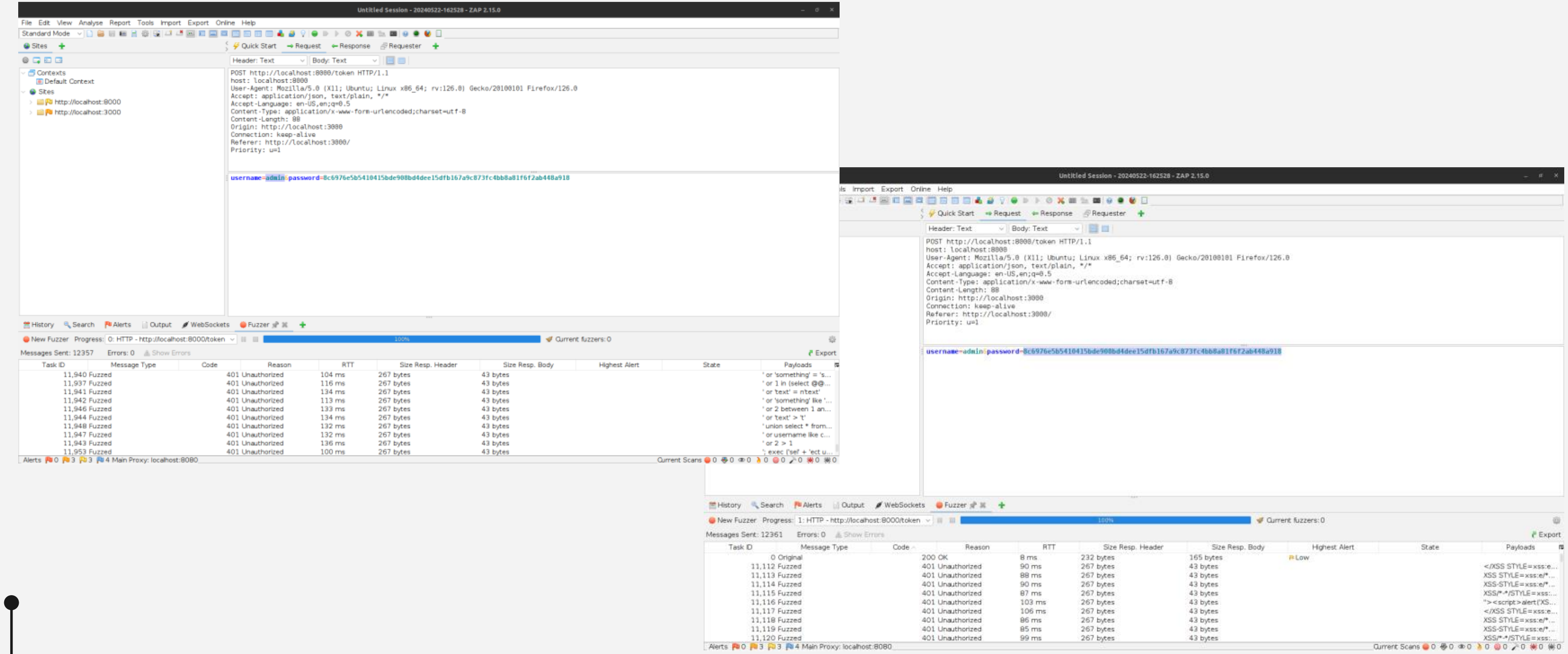


```
[22:42:02] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:42:02] [INFO] testing 'Boolean-based blind - Parameter replace (original v
alue)'
[22:42:02] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER
 BY or GROUP BY clause (EXTRACTVALUE)'
[22:42:02] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause
'
[22:42:02] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE
 or HAVING clause (IN)'
[22:42:02] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XM
LType)'
[22:42:02] [INFO] testing 'Generic inline queries'
[22:42:02] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:42:02] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (commen
t)'
[22:42:02] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE -
 comment)'
[22:42:02] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:42:02] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:42:02] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:42:02] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least o
ne other (potential) technique found. Do you want to reduce the number of requ
ests? [Y/n] n
[22:42:05] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:42:05] [WARNING] URI parameter '#1*' does not seem to be injectable
[22:42:05] [CRITICAL] all tested parameters do not appear to be injectable. Tr
y to increase values for '--level'/'--risk' options if you wish to perform mor
e tests. If you suspect that there is some kind of protection mechanism involv
ed (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=spa
ce2comment') and/or switch '--random-agent'
[22:42:05] [WARNING] HTTP error codes detected during run:
405 (Method Not Allowed) - 2 times, 404 (Not Found) - 123 times

[*] ending @ 22:42:05 /2024-05-22/

veiga4@mveiga-aspire:~/sqlmap-dev$ 
```



```
INFO:     Will watch for changes in these directories: ['/home/veiga4/ses-group4']
INFO:     Uvicorn running on http://127.0.0.1:8000 (Press CTRL+C to quit)
INFO:     Started reloader process [60077] using WatchFiles
INFO:     Started server process [60079]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     127.0.0.1:56316 - "GET /token HTTP/1.1" 405 Method Not Allowed
INFO:     127.0.0.1:56332 - "GET /token HTTP/1.1" 405 Method Not Allowed
INFO:     127.0.0.1:56342 - "GET /8189 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56350 - "GET /token%29%2C%29%29%28%22%27%2C%28. HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56358 - "GET /token%27lASzZc%3C%27%22%3ECcwAkK HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56364 - "GET /token%29%20AND%208210%3D8539%20AND%20%288481%3D8481 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56372 - "GET /token%29%20AND%208813%3D8813%20AND%20%285353%3D5353 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56376 - "GET /token%20AND%201592%3D3962 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56392 - "GET /token%20AND%208813%3D8813 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56412 - "GET /token%27%29%20AND%207618%3D5692%20AND%20%28%27BvXT%27%3D%27BvXT HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56408 - "GET /token%27%29%20AND%208813%3D8813%20AND%20%28%27DZkY%27%3D%27DZkY HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56424 - "GET /token%27%20AND%205736%3D3885%20AND%20%27jMdy%27%3D%27jMdy HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56434 - "GET /token%27%20AND%208813%3D8813%20AND%20%27nXtI%27%3D%27nXtI HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56438 - "GET /token%20AND%204191%3D6259--%20EgQX HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56440 - "GET /token%20AND%208813%3D8813--%20XoUn HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56454 - "GET /%28SELECT%20%28CASE%20WHEN%20%281114%3D5784%29%20THEN%20%27token%27%20ELSE%20%28SELECT%205784%20UNION
%20SELECT%201888%29%20END%29%29 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56466 - "GET /%28SELECT%20%28CASE%20WHEN%20%283432%3D3432%29%20THEN%20%27token%27%20ELSE%20%28SELECT%207777%20UNION
%20SELECT%202487%29%20END%29%29 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56482 - "GET /token%29%20AND%20EXTRACTVALUE%283382%2CCONCAT%280x5c%2C0x717a6a6a71%2C%28SELECT%20%28ELT%283382%3D338
2%2C1%29%29%29%2C0x7176716b71%29%29%20AND%20%286191%3D6191 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56470 - "GET /token%20AND%20EXTRACTVALUE%283382%2CCONCAT%280x5c%2C0x717a6a6a71%2C%28SELECT%20%28ELT%283382%3D3382%2
C1%29%29%29%2C0x7176716b71%29%29 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56492 - "GET /token%27%29%20AND%20EXTRACTVALUE%283382%2CCONCAT%280x5c%2C0x717a6a6a71%2C%28SELECT%20%28ELT%283382%3D
3382%2C1%29%29%29%2C0x7176716b71%29%29%20AND%20%28%27AxBp%27%3D%27AxBp HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56502 - "GET /token%27%20AND%20EXTRACTVALUE%283382%2CCONCAT%280x5c%2C0x717a6a6a71%2C%28SELECT%20%28ELT%283382%3D338
2%2C1%29%29%29%2C0x7176716b71%29%29%20AND%20%27TShi%27%3D%27TShi HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:56512 - "GET /token%20AND%20EXTRACTVALUE%283382%2CCONCAT%280x5c%2C0x717a6a6a71%2C%28SELECT%20%28ELT%283382%3D3382%2
C1%29%29%29%2C0x7176716b71%29%29--%20uknu HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53848 - "GET /token%29%20AND%206114%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28106%29%7C%7CCHR%28106%29%
7C%7CCHR%28113%29%29%7C%7C%28SELECT%20%28CASE%20WHEN%20%286114%3D6114%29%20THEN%201%20ELSE%200%20END%29%29%3A%3Atext%7C%7C%28CHR%28113%
29%7C%7CCHR%28118%29%7C%7CCHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29%20AS%20NUMERIC%29%20AND%20%283971%3D3971 HTTP/1.1" 404 No
t Found
INFO:     127.0.0.1:53860 - "GET /token%20AND%206114%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28106%29%7C%7CCHR%28106%29%7C%
7CCHR%28113%29%29%7C%7C%28SELECT%20%28CASE%20WHEN%20%286114%3D6114%29%20THEN%201%20ELSE%200%20END%29%29%3A%3Atext%7C%7C%28CHR%28113%29%
7C%7CCHR%28118%29%7C%7CCHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29%20AS%20NUMERIC%29 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53862 - "GET /token%27%29%20AND%206114%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28106%29%7C%7CCHR%28106%
29%7C%7CCHR%28113%29%29%7C%7C%28SELECT%20%28CASE%20WHEN%20%286114%3D6114%29%20THEN%201%20ELSE%200%20END%29%29%3A%3Atext%7C%7C%28CHR%281
13%29%7C%7CCHR%28118%29%7C%7CCHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29%20AS%20NUMERIC%29%20AND%20%28%27SZzH%27%3D%27SZzH HTTP
/1.1" 404 Not Found
INFO:     127.0.0.1:53868 - "GET /token%27%20AND%206114%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28106%29%7C%7CCHR%28106%29%
7C%7CCHR%28113%29%29%7C%7C%28SELECT%20%28CASE%20WHEN%20%286114%3D6114%29%20THEN%201%20ELSE%200%20END%29%29%3A%3Atext%7C%7C%28CHR%28113%
29%7C%7CCHR%28118%29%7C%7CCHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29%20AS%20NUMERIC%29%20AND%20%27WAep%27%3D%27WAep HTTP/1.1"
404 Not Found
INFO:     127.0.0.1:53882 - "GET /token%20AND%206114%3DCAST%28%28CHR%28113%29%7C%7CCHR%28122%29%7C%7CCHR%28106%29%7C%7CCHR%28106%29%7C%
7CCHR%28113%29%29%7C%7C%28SELECT%20%28CASE%20WHEN%20%286114%3D6114%29%20THEN%201%20ELSE%200%20END%29%29%3A%3Atext%7C%7C%28CHR%28113%29%
7C%7CCHR%28118%29%7C%7CCHR%28113%29%7C%7CCHR%28107%29%7C%7CCHR%28113%29%29%20AS%20NUMERIC%29--%20uhbZ HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53888 - "GET /token%29%20AND%207816%20IN%20%28SELECT%20%28CHAR%28113%29%2BCHAR%28122%29%2BCHAR%28106%29%2BCHAR%2810
6%29%2BCHAR%28113%29%2B%28SELECT%20%28CASE%20WHEN%20%287816%3D7816%29%20THEN%20CHAR%2849%29%20ELSE%20CHAR%2848%29%20END%29%29%2BCHAR%28
113%29%2BCHAR%28118%29%2BCHAR%28113%29%2BCHAR%28107%29%2BCHAR%28113%29%29%29%20AND%20%281638%3D1638 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53904 - "GET /token%20AND%207816%20IN%20%28SELECT%20%28CHAR%28113%29%2BCHAR%28122%29%2BCHAR%28106%29%2BCHAR%28106%2
9%2BCHAR%28113%29%2B%28SELECT%20%28CASE%20WHEN%20%287816%3D7816%29%20THEN%20CHAR%2849%29%20ELSE%20CHAR%2848%29%20END%29%29%2BCHAR%28113
%29%2BCHAR%28118%29%2BCHAR%28113%29%2BCHAR%28107%29%2BCHAR%28113%29%29%29 HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53906 - "GET /token%27%29%20AND%207816%20IN%20%28SELECT%20%28CHAR%28113%29%2BCHAR%28122%29%2BCHAR%28106%29%2BCHAR%2
8106%29%2BCHAR%28113%29%2B%28SELECT%20%28CASE%20WHEN%20%287816%3D7816%29%20THEN%20CHAR%2849%29%20ELSE%20CHAR%2848%29%20END%29%29%2BCHAR
%28113%29%2BCHAR%28118%29%2BCHAR%28113%29%2BCHAR%28107%29%2BCHAR%28113%29%29%29%20AND%20%28%27kYXY%27%3D%27kYXY HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53908 - "GET /token%27%20AND%207816%20IN%20%28SELECT%20%28CHAR%28113%29%2BCHAR%28122%29%2BCHAR%28106%29%2BCHAR%2810
6%29%2BCHAR%28113%29%2B%28SELECT%20%28CASE%20WHEN%20%287816%3D7816%29%20THEN%20CHAR%2849%29%20ELSE%20CHAR%2848%29%20END%29%29%2BCHAR%28
113%29%2BCHAR%28118%29%2BCHAR%28113%29%2BCHAR%28107%29%2BCHAR%28113%29%29%29%20AND%20%27IJLS%27%3D%27IJLS HTTP/1.1" 404 Not Found
INFO:     127.0.0.1:53920 - "GET /token%20AND%207816%20IN%20%28SELECT%20%28CHAR%28113%29%2BCHAR%28122%29%2BCHAR%28106%29%2BCHAR%28106%2
```

Análise Dinâmica – ZAP



```
POST http://localhost:8000/token HTTP/1.1
host: localhost:8000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded;charset=utf-8
Content-Length: 88
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Priority: u=1

username=admin&password=8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
```

Progress: 0: HTTP - http://localhost:8000/token Current fuzzers: 0

Messages Sent: 12357 Errors: 0

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
11,940	Fuzzed	401	Unauthorized	104 ms	267 bytes	43 bytes			' or 'something' = 's...
11,937	Fuzzed	401	Unauthorized	116 ms	267 bytes	43 bytes			' or 1 in (select @@...
11,941	Fuzzed	401	Unauthorized	134 ms	267 bytes	43 bytes			' or 'text' = n'text'
11,942	Fuzzed	401	Unauthorized	113 ms	267 bytes	43 bytes			' or 'something' like '...
11,946	Fuzzed	401	Unauthorized	133 ms	267 bytes	43 bytes			' or 2 between 1 an...
11,944	Fuzzed	401	Unauthorized	134 ms	267 bytes	43 bytes			' or 'text' > 't'
11,948	Fuzzed	401	Unauthorized	132 ms	267 bytes	43 bytes			' union select * from...
11,947	Fuzzed	401	Unauthorized	132 ms	267 bytes	43 bytes			' or username like c...
11,943	Fuzzed	401	Unauthorized	136 ms	267 bytes	43 bytes			' or 2 > 1
11,953	Fuzzed	401	Unauthorized	100 ms	267 bytes	43 bytes			'; exec ('sel' + 'ect u...

Alerts 0 3 3 4 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

```
POST http://localhost:8000/token HTTP/1.1
host: localhost:8000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:126.0) Gecko/20100101 Firefox/126.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencoded;charset=utf-8
Content-Length: 88
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Priority: u=1

username=admin&password=8c6976e5b5410415bde908bd4dee15dfb167a9c873fc4bb8a81f6f2ab448a918
```

Progress: 1: HTTP - http://localhost:8000/token Current fuzzers: 0

Messages Sent: 12361 Errors: 0

Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads
0	Original	200	OK	8 ms	232 bytes	165 bytes	Low		
11,112	Fuzzed	401	Unauthorized	90 ms	267 bytes	43 bytes			</XSS STYLE=xss:e...
11,113	Fuzzed	401	Unauthorized	88 ms	267 bytes	43 bytes			XSS STYLE=xss:e/*...
11,114	Fuzzed	401	Unauthorized	90 ms	267 bytes	43 bytes			XSS-STYLE=xss:e/*...
11,115	Fuzzed	401	Unauthorized	87 ms	267 bytes	43 bytes			XSS/*-*/STYLE=xss:...
11,116	Fuzzed	401	Unauthorized	103 ms	267 bytes	43 bytes			"><script>alert('XS...
11,117	Fuzzed	401	Unauthorized	106 ms	267 bytes	43 bytes			</XSS STYLE=xss:e...
11,118	Fuzzed	401	Unauthorized	86 ms	267 bytes	43 bytes			XSS STYLE=xss:e/*...
11,119	Fuzzed	401	Unauthorized	85 ms	267 bytes	43 bytes			XSS-STYLE=xss:e/*...
11,120	Fuzzed	401	Unauthorized	99 ms	267 bytes	43 bytes			XSS/*-*/STYLE=xss:...

Alerts 0 3 3 4 Main Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Conclusão

Implementação de uma aplicação de aprendizagem

Integração do conceito de segurança desde o Design

Analisamos a aplicação com ferramente de segurança avançadas

Aplicação Segura ?

Obrigado!

Dúvidas?