integrando testes de segurança no Cypress

@5minsec

> Ben-Hur Santos Ott

CWI Software
Security Champion
Funko Pop
Desnível entre noção e coragem

Cypress + Docker


???
nmap
sqlmap
python
C:\

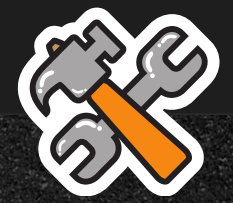
```yaml
version: "3.9"
services:
  nmap:
    build:
      context: ./
      dockerfile: Dockerfile.nmap
    container_name: nmap
  sqlmap:
    build:
      context: ./
      dockerfile: Dockerfile.sqlmap
    container_name: sqlmap
  python-scripts:
    build:
      context: ./      You, 7 hours ago
      dockerfile: Dockerfile.python
    container_name: python-scripts
```

```dockerfile
FROM parrotsec/tools-nmap

ENTRYPOINT ["tail", "-f", "/dev/null"]
```

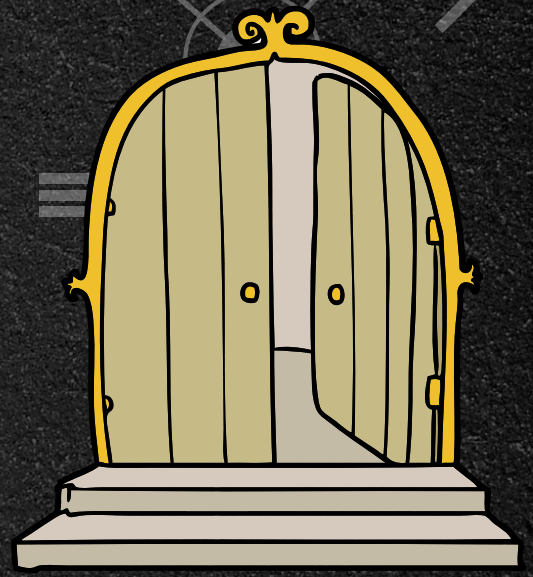
```dockerfile
FROM python:3.7-stretch

COPY python-scripts .

RUN pip install -r requirements.txt

ENTRYPOINT ["tail", "-f", "/dev/null"]
```

```
/// <reference types="cypress" />

context('NMAP', () => {
    describe('Validating ports in cwi.com.br', () => {
        const HOST = 'cwi.com.br'

        it('Only 80 and 443 ports should be open', () => {
            const expectedOpenedPorts = [80, 443]
            cy.nmapScanCommonPorts(HOST)
                .then(openedPorts => {
                    expect(openedPorts).to.deep.equal(expectedOpenedPorts)
                })
        })
    })
})
```

```
Cypress.Commands.add('nmapScanCommonPorts', (host) => {
    const command = `docker exec -i nmap nmap -F ${host} | grep "open"`
    return cy.exec(
        command,
        {failOnNonZeroExit: false}
    ).then(nmapRawResponse => {
        if (nmapRawResponse.code > 0 || !nmapRawResponse.stdout) {
            return []
        }

        const lines = nmapRawResponse.stdout.split('\n')
        const ports = lines.map(line => {
            return +line.split('/')[0]
        })

        return ports
    })
})
```



Port Scan



O que é?

Verificação de portas abertas no host alvo.

```
$ nmap -F -Pn cwi.com.br
Starting Nmap 7.80 ( https://nmap.org ) at 2020-1
Nmap scan report for cwi.com.br (189.114.75.94)
Host is up (0.066s latency).
Not shown: 97 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
8008/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 10
```

Falhas?

Um servidor pode estar com portas "indevidas" abertas por descuido com configurações.

21 - FTP
22 - SSH
27017 - MongoDB
9200 - ElasticSearch

```
$ ncrack 10.0.0.130:21 192.168.1.2:22

Starting Ncrack 0.6 ( http://ncrack.org ) at 2016-01-03 22:10 E

Discovered credentials for ftp on 10.0.0.130 21/tcp:
10.0.0.130 21/tcp ftp: admin hello1
Discovered credentials for ssh on 192.168.1.2 22/tcp:
192.168.1.2 22/tcp ssh: guest 12345
192.168.1.2 22/tcp ssh: admin money$

Ncrack done: 2 services scanned in 156.03 seconds.

Ncrack finished.
```

Testes

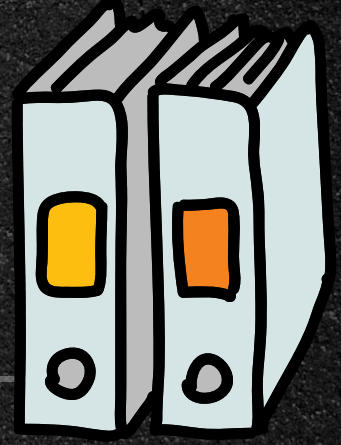
Apenas as portas que devem de fato estar disponíveis para a internet devem aparecer no resultado do nmap.

https://nmap.org/

nmap -F -Pn {HOST}

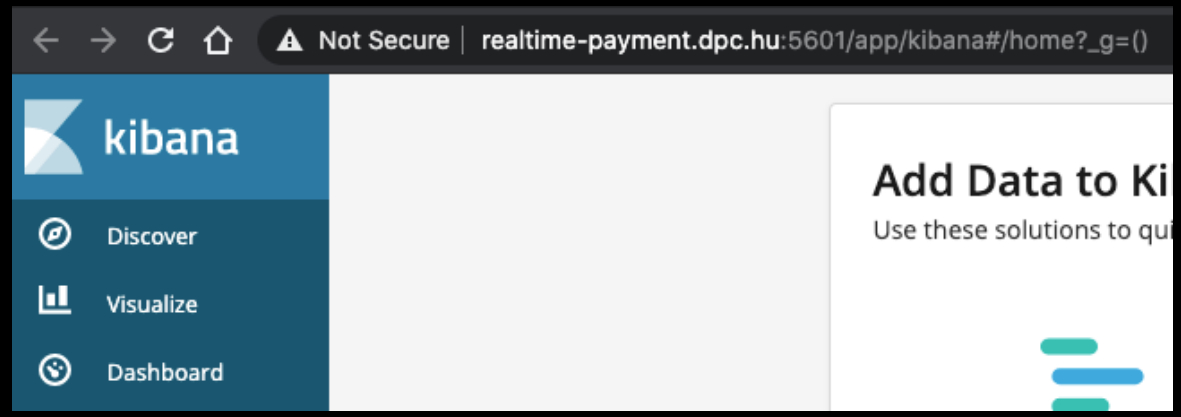
80/8080 - HTTP
443 - HTTPS

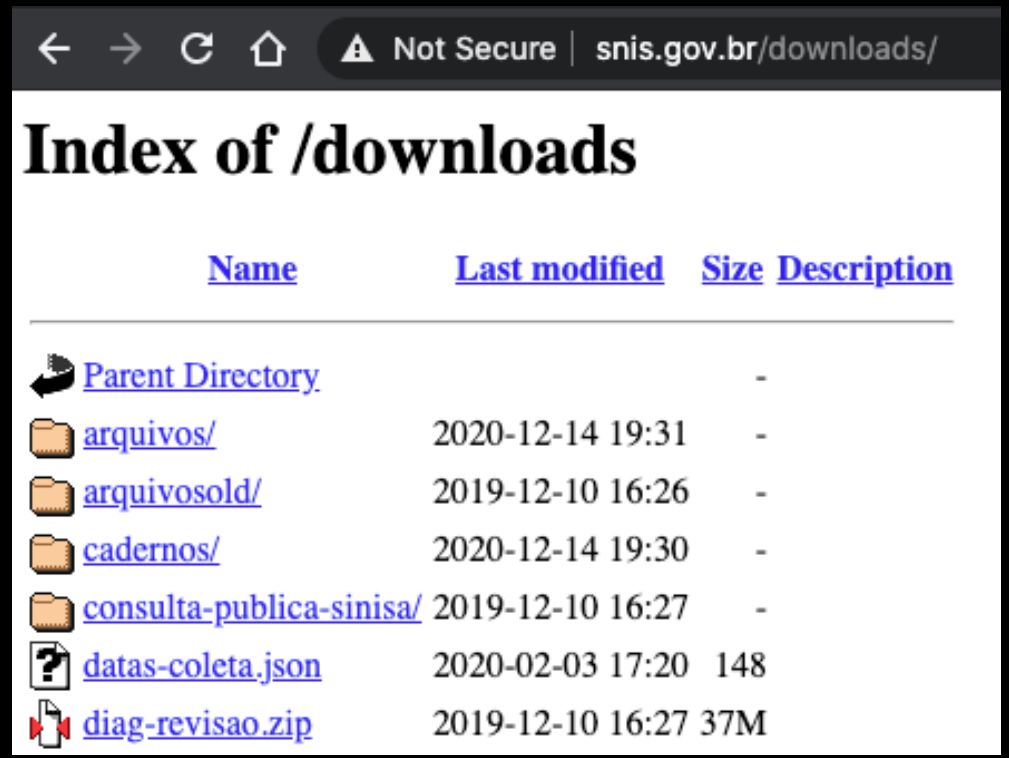
Exploração de Rotas, Diretórios e Arquivos



O que é?

Rotas da aplicação, pastas e arquivos expostos indevidamente permitem que naveguemos nos arquivos do servidor ou encontremos paineis com informações.

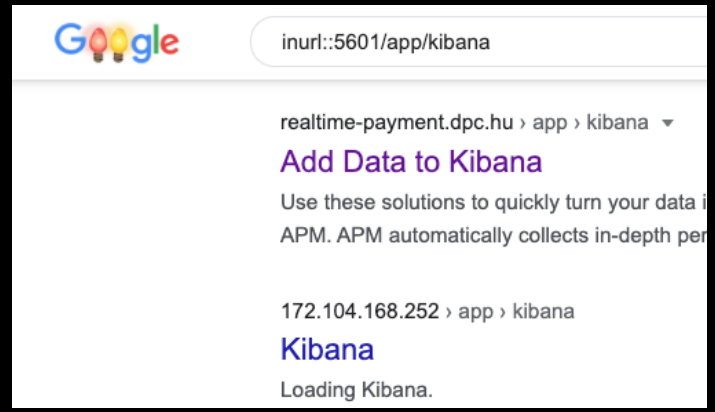




Falhas?

Arquivos de código fonte e informações sigilosas ficam de fácil acesso para atacantes.

Podendo resultar em vazamento de dados ou comprometimento de serviços.



Testes

Pode-se utilizar o Dirb ou Nikto para fazer scan de diretórios da aplicação.

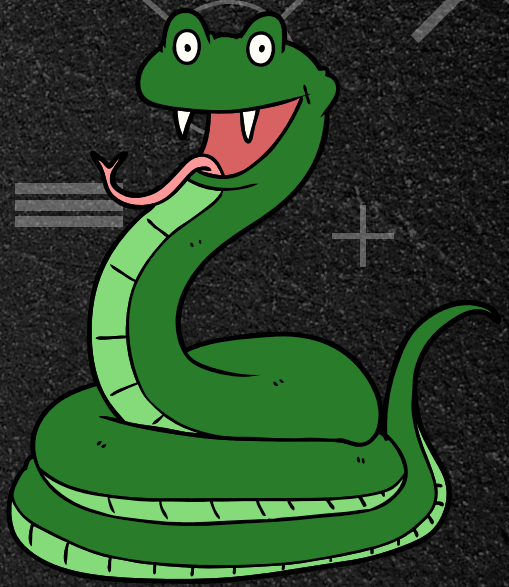
Em conjunto, colocar na automação por verificação de rotas conhecidas.

https://tools.kali.org/information-gathering/nikto

```
$ nikto -h 127.0.0.1 -port 3000
- Nikto v2.1.6
---------------------------------------------------------------
+ Target IP:          127.0.0.1
+ Target Hostname:    127.0.0.1
+ Target Port:        3000
+ Start Time:         2020-12-16 21:59:53 (GMT-3)
---------------------------------------------------------------
+ Server: No banner retrieved
+ ETag header found on server leaks inodes via ETags, header found with fil
+ The X-XSS-Protection header is not defined. This hea

+ Uncommon header 'feature-policy' found, with content
+ No CGI Directories found (use '-C all' to force chec
+ Entry '/ftp/' in robots.txt returned a non-forbidden
+ "robots.txt" contains 1 entry which should be manual
+ OSVDB-3092: /css: This might be interesting...
+ OSVDB-3092: /ftp/: This might be interesting...
+ OSVDB-3092: /public/: This might be interesting...
```

```
Cypress.Commands.add('urlStatusCheck', (url) => {
    const command = `curl --head ${url} | grep "200 OK"`
    return cy.exec(
        command,
        {
            failOnNonZeroExit: false
        }
    ).then(result => {
        return result.code == 0 && !!result.stdout
    })
})
```

Sql Injection



O que é?

Um parâmetro enviado para o servidor pode ser interpretado como uma instrução e não como um valor.

http://api.com/products?q=shoes

```
SELECT * FROM products
WHERE category = '${categ}'
```

http://api.com/products?q=' or 1=1 --

```
SELECT * FROM products
WHERE category = '' or 1=1 --'
```

Falha?

Um atacante pode baixar todos os dados da base de dados ou alterar registros.

```
sqlmap
  -u http://mytestsite.com/page.php?id=5
  --dump-all
```

```
-a, --all           Retrieve everything
-b, --banner        Retrieve DBMS banner
--current-user      Retrieve DBMS current user
--current-db        Retrieve DBMS current database
--passwords         Enumerate DBMS users password hashes
--tables            Enumerate DBMS database tables
--columns           Enumerate DBMS database table columns
--schema            Enumerate DBMS schema
--dump              Dump DBMS database table entries
--dump-all          Dump all DBMS databases tables entries
```

Teste

Em novas APIs que possuam parâmetros na URL executar uma validação de Sql Injection.

```
docker exec
  -i sqlmap sqlmap
  -u "${url}"
  --answers="follow=Y"
  --batch
  --banner
  --level=2
```

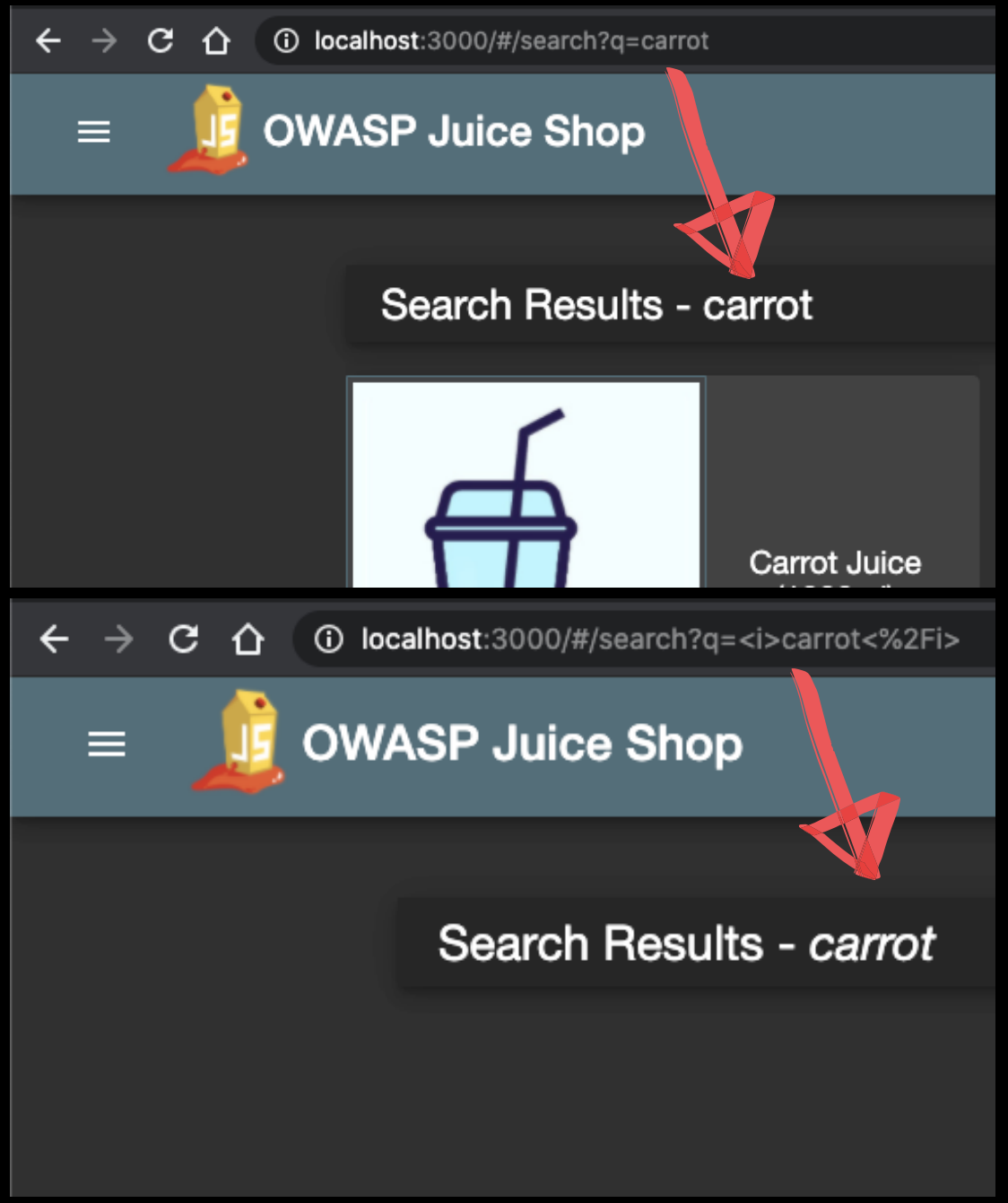
```
---
Parameter: q (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: q=test%' AND 4080=4080 AND 'kNdw%'='kNdw

    Type: time-based blind
    Title: SQLite > 2.0 AND time-based blind (heavy query)
    Payload: q=test%' AND 4808=LIKE('ABCDEFG',UPPER(HEX(RAND
---
[22:22:47] [INFO] the back-end DBMS is SQLite
[22:22:47] [INFO] fetching banner
[22:22:47] [INFO] resumed: 3.31.1
back-end DBMS: SQLite
banner: '3.31.1'
```

XSS Injection

O que é

Inputs são executados e não exibidos como valor.

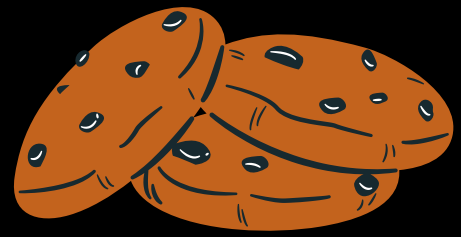
No HTML costumam vir do backend ou da URL.



Falha?

Atacantes podem enviar e-mails com links reais e scripts no parâmetro.

Estes scripts podem roubar informações ou executar ações no lugar do usuário logado.



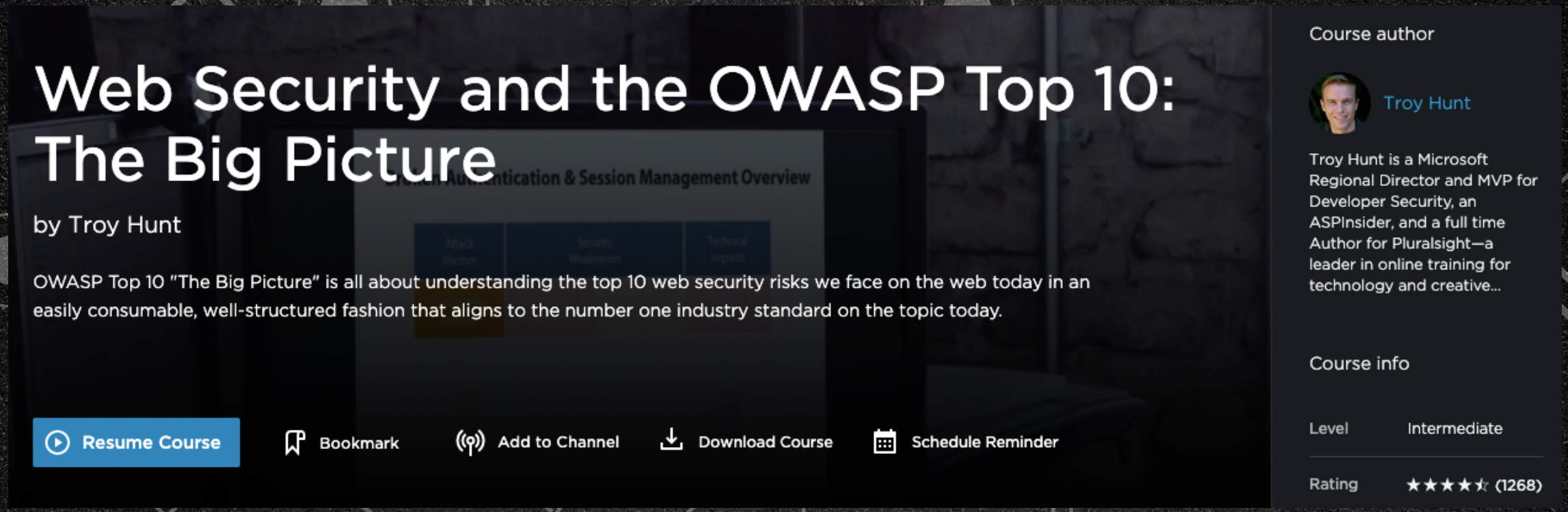
Teste

"Basta" incluir uma tag no lugar do parâmetro, realizar o encoding e verificar se consegue buscar o elemento pelo seu seletor.

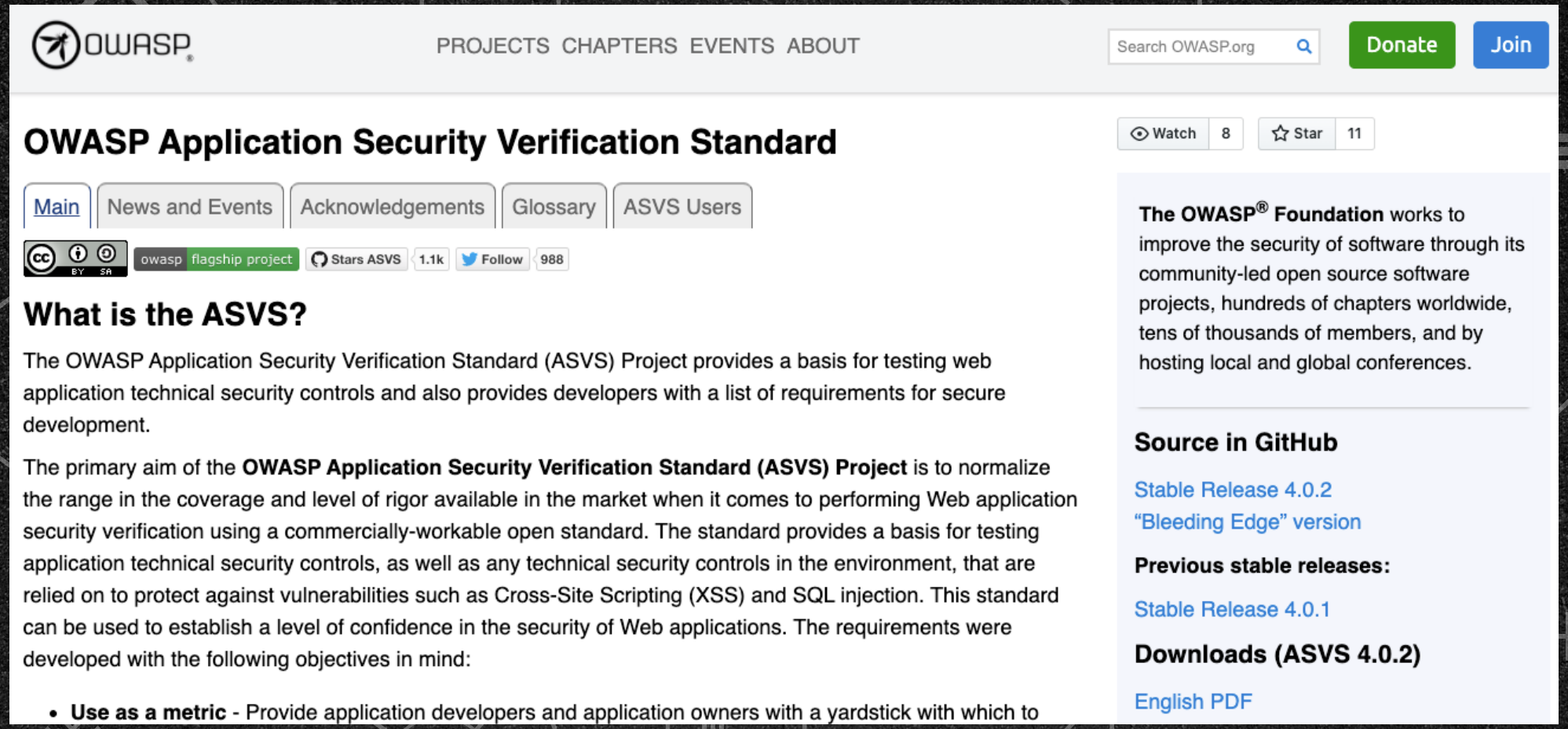
```
context('XSS', () => {
    describe('Validating routes', () => {
        const url = 'http://localhost:3000/#/search?q=*XSS*'

        it('Should not have xss injection', () => {
            cy.xssUrlQueryExists(url)
                .then(status => {
                    expect(status).to.be.false
                })
        })
    })
})
```

```
Cypress.Commands.add('xssUrlQueryExists', (url) => {
    const injection = '<i id="xss-test">HACKED</i>'
    const urlWithInjection = url.replace('*XSS*', encodeURIComponent(injection))

    return cy.visit(urlWithInjection, {timeout: 10000})
             .get('#xss-test')
                .then(el => {
                    return !!el && el.length && el[0].innerText === 'HACKED'
                })
})
```

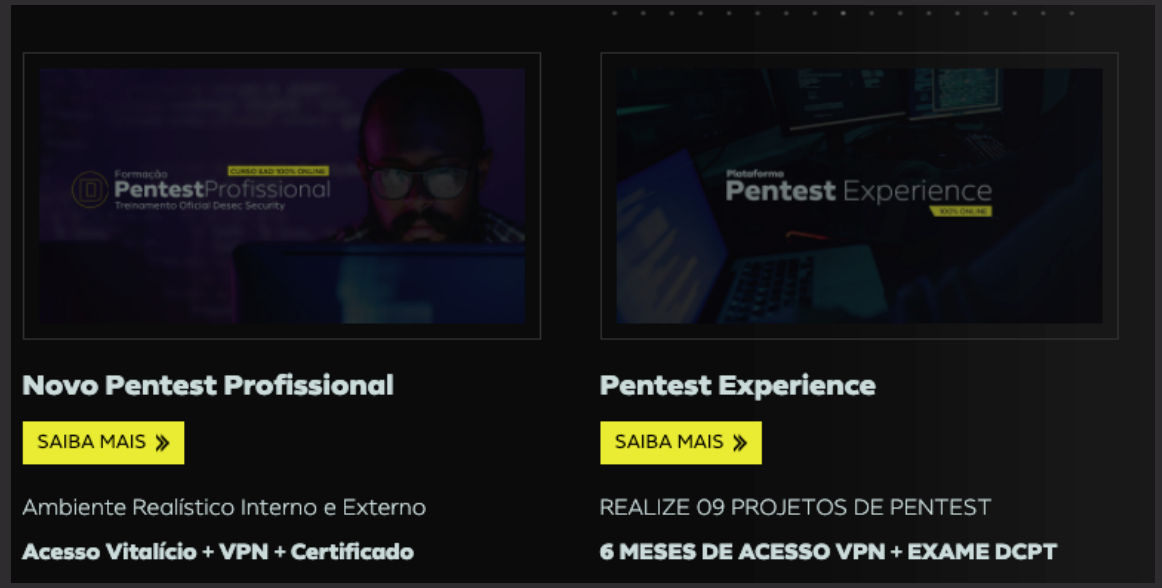
Extras



https://www.pluralsight.com/courses/web-security-owasp-top10-big-picture



https://owasp.org/www-project-application-security-verification-standard/



https://desecsecurity.com/cursos

WSS
A SEGURANÇA DIGITAL DO SEU MUNDO

contato@wss.business

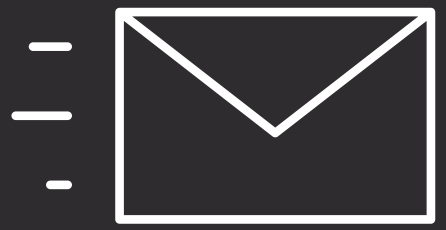
5 min sec

CWI SOFTWARE

Segue lá:

@5minsec

@cwisoftware



ben-hur@outlook.com