

*integrando testes  
de segurança no*  
**Cypress**

@5minsec



> Ben-Hur Santos Ott

CWI Software  
Security Champion  
Funko Pop  
Desnível entre noção e coragem

🌙  
*5 min  
sec*



# Cypress + Docker



???



u map



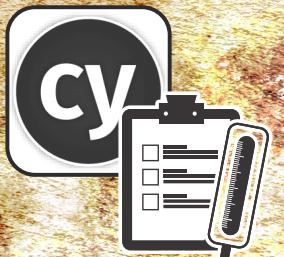
python



sqlmap



C:\

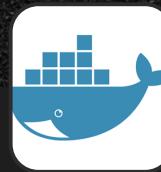


```
version: "3.9"
services:
  nmap:
    build:
      context: ./nmap
      dockerfile: Dockerfile.nmap
      container_name: nmap
  sqlmap:
    build:
      context: ./sqlmap
      dockerfile: Dockerfile.sqlmap
      container_name: sqlmap
  python-scripts:
    build:
      context: ./python-scripts
      dockerfile: Dockerfile.python
      container_name: python-scripts
```



```
FROM parrotsec/tools-nmap
ENTRYPOINT ["tail", "-f", "/dev/null"]

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'

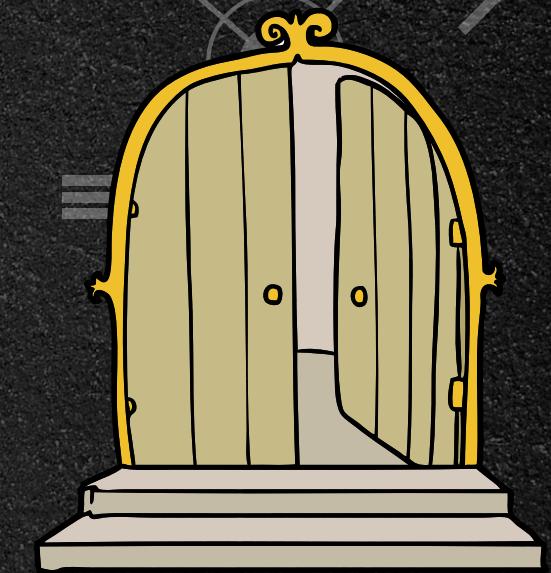
    it('Only 80 and 443 ports should be open', () => {
      const expectedOpenedPorts = [80, 443]
      cy.nmapScanCommonPorts(HOST)
        .then(openedPorts => {
          expect(openedPorts).to.deep.equal(expectedOpenedPorts)
        })
    })
  })
})
```

```
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 hello!
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

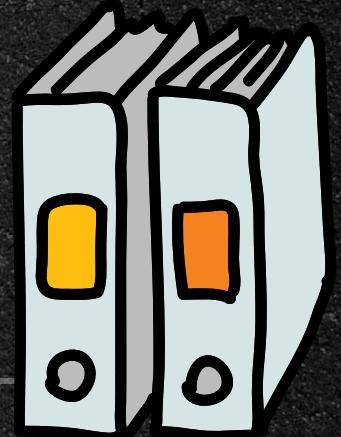
Apenas as portas que devem de fato estar disponíveis para a internet devem aparecer no resultado do nmap.

<https://nmap.org/>

nmap -F -Pn {HOST}

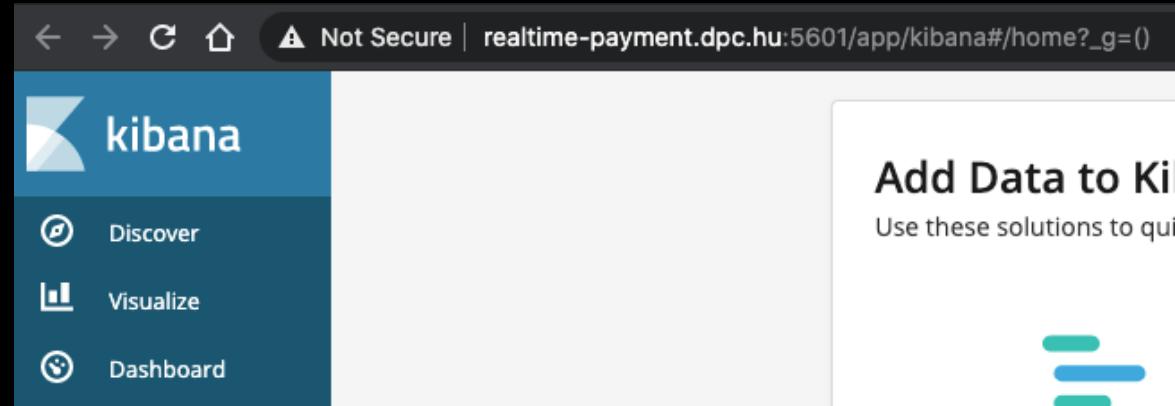
80/8080 - HTTP  
443 - HTTPS

# Exploração de Rotas, Diretórios e Arquivos

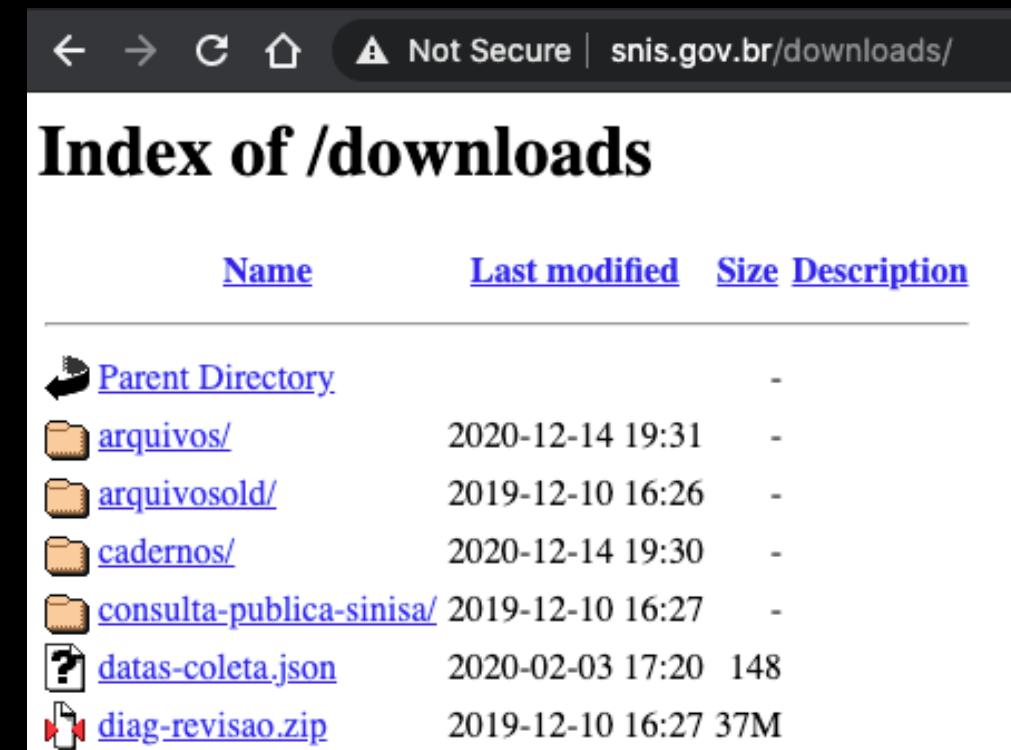


# O que é?

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



A screenshot of a web browser showing the Kibana interface at [realtime-payment.dpc.hu:5601/app/kibana#/home?\\_g=\(\)](http://realtime-payment.dpc.hu:5601/app/kibana#/home?_g=()). The page title is "Not Secure". The left sidebar has three items: "Discover" (with a magnifying glass icon), "Visualize" (with a bar chart icon), and "Dashboard" (with a clock icon). To the right, there is a section titled "Add Data to Ki" with the sub-instruction "Use these solutions to qui".



A screenshot of a web browser showing an "Index of /downloads" page at [snis.gov.br/downloads/](http://snis.gov.br/downloads/). The page title is "Not Secure". The content is a table with columns: Name, Last modified, Size, and Description. The table lists several entries:

Name	Last modified	Size	Description
<a href="#">Parent Directory</a>		-	
<a href="#">arquivos/</a>	2020-12-14 19:31	-	
<a href="#">arquivosold/</a>	2019-12-10 16:26	-	
<a href="#">cadernos/</a>	2020-12-14 19:30	-	
<a href="#">consulta-publica-sinisa/</a>	2019-12-10 16:27	-	
<a href="#">datas-coleta.json</a>	2020-02-03 17:20	148	
<a href="#">diag-revisao.zip</a>	2019-12-10 16:27	37M	

# Falhas?

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

Podendo resultar em vazamento de dados ou comprometimento de serviços.

The screenshot shows the Exploit Database interface. At the top, there's a logo of a red and black exploit bug and the text "EXPLOIT DATABASE". Below that, it says "Google Hacking Database". There's a dropdown menu labeled "Show 15". Underneath, there are search filters for "Date Added" and a "Dork" field. The main area displays search results:

- 2020-08-31 inurl:/app/kibana "Kibana" -discuss -ipaddress -git
- 2019-07-15 inurl:app/kibana intext:Loading Kibana
- 2018-03-07 inurl::5601/app/kibana

The screenshot shows a Google search results page. The search query "inurl::5601/app/kibana" is entered in the search bar. The results show two entries:

- realtime-payment.dpc.hu › app › kibana ▾ Add Data to Kibana Use these solutions to quickly turn your data into insights. APM. APM automatically collects in-depth performance metrics and logs from your application.
- 172.104.168.252 › app › kibana Kibana Loading Kibana.

# *Testes*

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

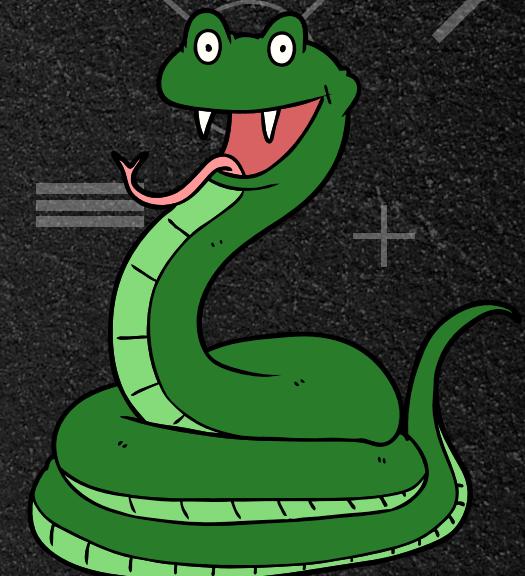
Em conjunto, colocar na automação por verificação de rotas conhecidas.

<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
+ Server leaks inodes via ETags, header found with file /index.html
+ The X-XSS-Protection header is not defined. This header
+ Uncommon header 'feature-policy' found, with content "cross-origin"
+ No CGI Directories found (use '-C all' to force check)
+ Entry '/ftp/' in robots.txt returned a non-forbidden status
+ "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 --`

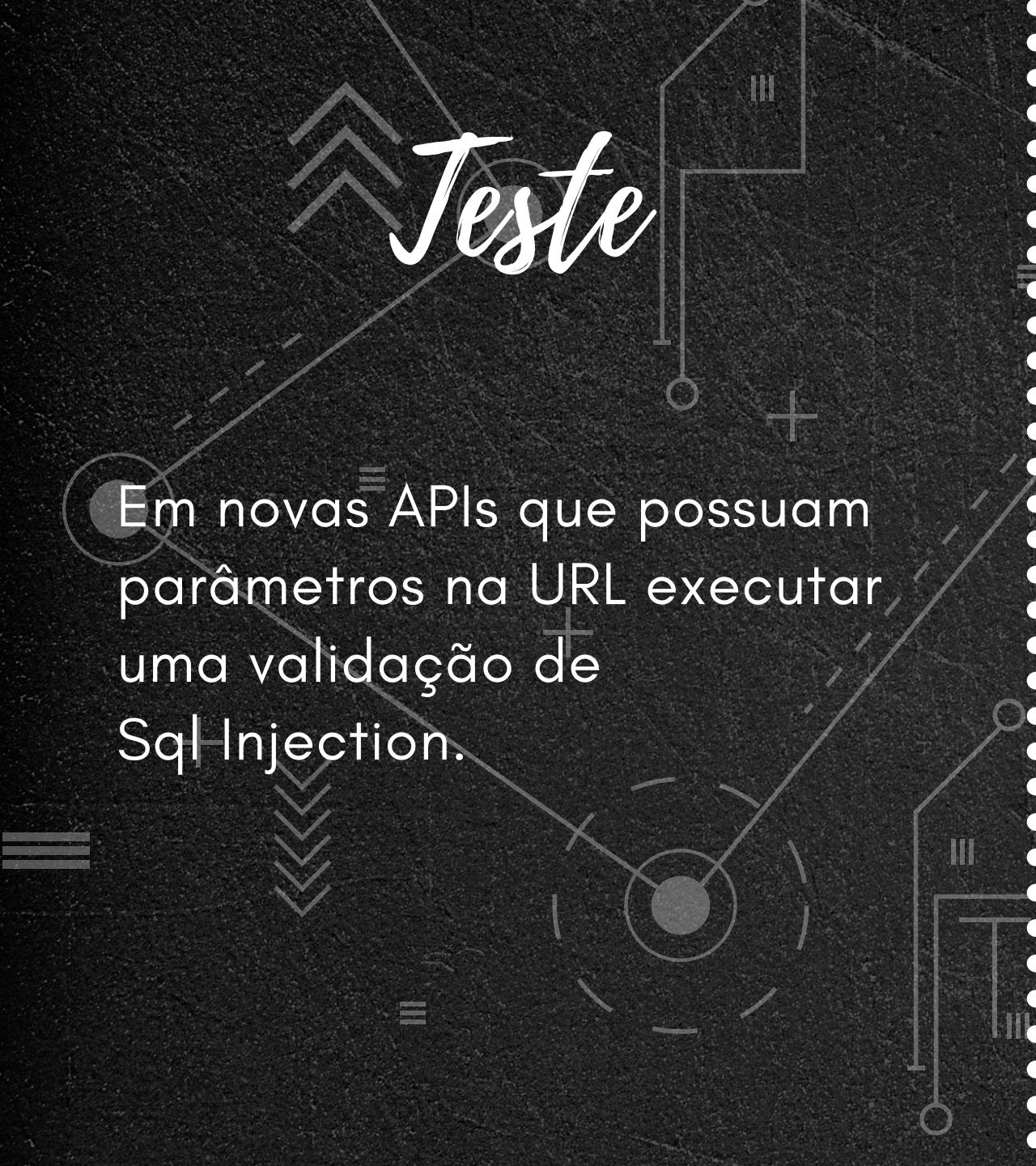
```
SELECT * FROM products  
WHERE category = " or 1=1 --"
```

# 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 <u>databases</u> tables entries



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

# Jeste

```
● 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.

The image displays two screenshots of the OWASP Juice Shop application, which is a web-based penetration testing environment. Both screenshots show the same search results page for the query "carrot".

**Screenshot 1:** The URL is `localhost:3000/#/search?q=carrot`. The search results show an image of a blue juice cup with a straw and the text "Carrot Juice". A red arrow points from the text "Search Results - carrot" down to the juice cup image.

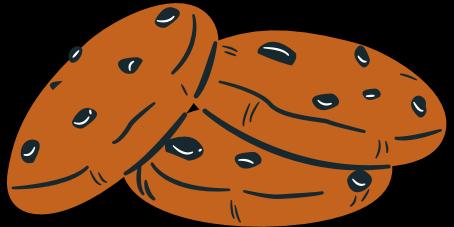
**Screenshot 2:** The URL is `localhost:3000/#/search?q=<i>carrot<%2Fi>`. The search results show the same juice cup image and the text "Carrot Juice". A red arrow points from the text "Search Results - carrot" down to the juice cup image.

In both cases, the search results are identical despite the different URLs, illustrating a search result injection vulnerability where user input is being executed on the server side.

# 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.



# Jeste

"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



# Web Security and the OWASP Top 10: The Big Picture

by Troy Hunt

OWASP Top 10 "The Big Picture" is all about understanding the top 10 web security risks we face on the web today in an easily consumable, well-structured fashion that aligns to the number one industry standard on the topic today.

Resume Course

Bookmark

Add to Channel

Download Course

Schedule Reminder

Course author



Troy Hunt

Troy Hunt is a Microsoft Regional Director and MVP for Developer Security, an ASPInsider, and a full time Author for Pluralsight—a leader in online training for technology and creative...

Course info

Level Intermediate

Rating ★★★★☆ (1268)

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



# OWASP Application Security Verification Standard

[Main](#) [News and Events](#) [Acknowledgements](#) [Glossary](#) [ASVS Users](#)



owasp flagship project

Stars ASVS

1.1k

Follow

988

## What is the ASVS?

The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development.

The primary aim of the **OWASP Application Security Verification Standard (ASVS) Project** is to normalize the range in the coverage and level of rigor available in the market when it comes to performing Web application security verification using a commercially-workable open standard. The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. This standard can be used to establish a level of confidence in the security of Web applications. The requirements were developed with the following objectives in mind:

- **Use as a metric** - Provide application developers and application owners with a yardstick with which to

[Watch](#) 8 [Star](#) 11

The OWASP® Foundation works to improve the security of software through its community-led open source software projects, hundreds of chapters worldwide, tens of thousands of members, and by hosting local and global conferences.

## Source in GitHub

[Stable Release 4.0.2](#)  
["Bleeding Edge" version](#)

## Previous stable releases:

[Stable Release 4.0.1](#)

## Downloads (ASVS 4.0.2)

[English PDF](#)

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

**Novo Pentest Profissional**

SAIBA MAIS »

Ambiente Realístico Interno e Externo

**Acesso Vitalício + VPN + Certificado**

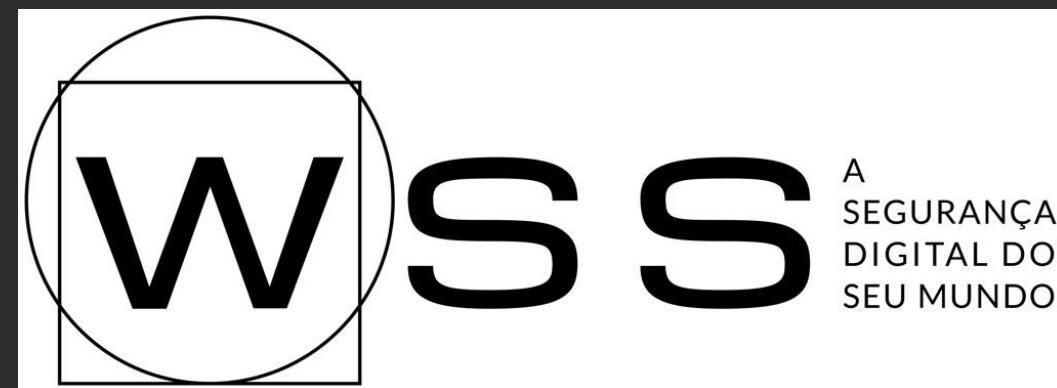
**Pentest Experience**

SAIBA MAIS »

REALIZE 09 PROJETOS DE PENTEST

**6 MESES DE ACESSO VPN + EXAME DCPT**

<https://desecsecurity.com/cursos>



[contato@wss.business](mailto:contato@wss.business)



5 min  
sec

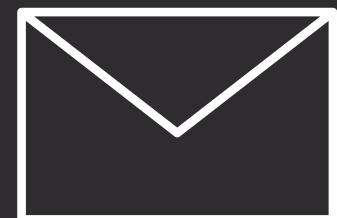


CWI SOFTWARE

Segue lá:

@5minsec

@cwisoftware



ben-hur@outlook.com