

API Security

Cherrybomb

Cherrybomb is an CLI tool written in Rust that helps prevent incorrect code implementation early in development. It works by validating and testing your API using an OpenAPI file. Its main goal is to reduce security errors and ensure your API functions as intended.


GitHub

1. Install and usage

```
# Install Rust and Cargo
curl https://sh.rustup.rs -sSf | sh
# Install cherrybomb
cargo install cherrybomb
# usage
cherrybomb --file api_openapi.json
```

Bash

2. Issues

 only support OpenAPI JSON files

YAML support broken? · Issue #111 · blst-security/cherrybomb

Describe the bug According to #19 yaml support should be there, but I couldn't get it working: An OAS 3.1 file in yaml format raises error: &#gt; cherrybomb --file foo.yaml v1.0.0 Starti...

github.com

blst-security/cherrybomb

#111 YAML support broken?

2 comments

opened on February 1, 2023

Postman

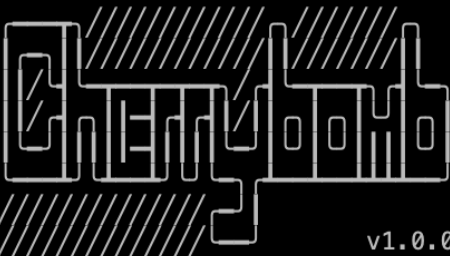
www.postman.com

```
# Install postman2openapi
cargo install postman2openapi --bin --features binary
# Convert Postman Collections Into OpenAPI json format
postman2openapi -f json api.postman_collection.json > api_openapi.json
```

Bash

3. Test Report

ghl@mao:~\$ cherrybomb --file api.json

 v1.0.0

Starting Cherrybomb...
Opening OAS file...
Parsing OAS file...
Running passive scan...
Running active scan...

Check	Severity	Description	Location
AUTH	"Medium"	The API doesn't have authentication defined	swagger root components
DEFAULT RESPONSE	"Low"	No default response defined	swagger path:/api/jsonBlob operation:POST
DEFAULT RESPONSE	"Low"	No default response defined	swagger path:/api/1073089485935493120 operation:GET

Check	Severity	Description	Location
AUTH BY PASS	"High"	The endpoint seems to be not secure "/api/1073089485935493120", with the method : GET	/api/1073089485935493120
SSL ENFORCED	"Medium"	The server does not seem to be using SSL, status code: 200	http://jsonblob.com

标准模式

站点

Contexts

- 默认上下文
- 站点
 - https://jsonblob.com
 - api
 - GET:1073089485935493120
 - POST:jsonBlob({"people":["bill","steve","bob"]})
 - GET:api

导入

Import a WSDL file from local file system

Import a WSDL file from a URL

Import an OpenAPI definition from the local file system

Import an OpenAPI definition from a URL

Import a GraphQL Schema from a File

Import a GraphQL Schema from a URL

Import HAR (HTTP Archive File)

Import a File Containing URLs

Import URLs from Logs or raw Files...

未命名会话 - OWASP ZAP 2.12.0

标准模式

请求 响应

Header: 原始视图 Body: 原始视图

POST https://jsonblob.com/api/jsonBlob HTTP/1.1

Host: jsonblob.com

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:105.0) Gecko/20100101 Firefox/105.0

Pragma: no-cache

Cache-Control: no-cache

Accept: */*

Content-Type: application/json

Content-Length: 33

{"people":["bill","steve","bob"]}

历史 Progress 输出 主动扫描 警告

新扫描 进展: 0: https://jsonblob.com/api 100% 当前扫描: 0 Num Requests: 639 新建告警: 12 导出

Id	Req. Timestamp	Resp. Timestamp	方法	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
5	2023/2/15 下午2:15:31	2023/2/15 下午2:15:31	GET	https://jsonblob.com/api/2102031782314564...	404	Not Found	528 ...	647 字节	105 字节
7	2023/2/15 下午2:15:31	2023/2/15 下午2:15:32	GET	https://jsonblob.com/api	200	OK	892 ...	633 字节	15,047 字节
8	2023/2/15 下午2:15:31	2023/2/15 下午2:15:33	POST	https://jsonblob.com/api/jsonBlob	201	Created	1.34 ...	699 字节	50 字节
9	2023/2/15 下午2:15:33	2023/2/15 下午2:15:33	POST	https://jsonblob.com/api/jsonBlob	201	Created	519 ...	704 字节	95 字节
10	2023/2/15 下午2:15:33	2023/2/15 下午2:15:34	POST	https://jsonblob.com/api/jsonBlob	201	Created	528 ...	704 字节	52 字节
11	2023/2/15 下午2:15:34	2023/2/15 下午2:15:34	POST	https://jsonblob.com/api/jsonBlob	201	Created	518 ...	707 字节	112 字节
12	2023/2/15 下午2:15:34	2023/2/15 下午2:15:35	POST	https://jsonblob.com/api/jsonBlob	201	Created	522 ...	711 字节	40 字节
13	2023/2/15 下午2:15:35	2023/2/15 下午2:15:35	POST	https://jsonblob.com/api/jsonBlob	201	Created	522 ...	698 字节	87 字节
14	2023/2/15 下午2:15:35	2023/2/15 下午2:15:36	POST	https://jsonblob.com/api/jsonBlob	201	Created	523 ...	697 字节	32 字节
15	2023/2/15 下午2:15:36	2023/2/15 下午2:15:36	POST	https://jsonblob.com/api/jsonBlob	201	Created	520 ...	704 字节	30 字节
16	2023/2/15 下午2:15:36	2023/2/15 下午2:15:37	POST	https://jsonblob.com/api/jsonBlob	201	Created	522 ...	706 字节	33 字节
17	2023/2/15 下午2:15:37	2023/2/15 下午2:15:37	POST	https://jsonblob.com/api/jsonBlob	201	Created	523 ...	702 字节	77 字节
18	2023/2/15 下午2:15:37	2023/2/15 下午2:15:38	POST	https://jsonblob.com/api/jsonBlob	201	Created	522 ...	700 字节	44 字节
19	2023/2/15 下午2:15:38	2023/2/15 下午2:15:38	POST	https://jsonblob.com/api/jsonBlob	201	Created	521 ...	704 字节	45 字节

警报 (4)

Strict-Transport-Security Header Not Set (2)

GET: https://jsonblob.com/api/10730894859354

POST: https://jsonblob.com/api/jsonBlob

X-Content-Type-Options Header Missing (2)

GET: https://jsonblob.com/api/10730894859354

POST: https://jsonblob.com/api/jsonBlob

Re-examine Cache-control Directives (2)

GET: https://jsonblob.com/api/10730894859354

POST: https://jsonblob.com/api/jsonBlob

User Agent Fuzzer (12)

GET: https://jsonblob.com/api

GET: https://jsonblob.com/api

GET: https://jsonblob.com/api

GET: https://jsonblob.com/api

GET: https://jsonblob.com/api

GET: https://jsonblob.com/api

Strict-Transport-Security Header Not Set

URL: https://jsonblob.com/api/jsonBlob

风险: Low

信心: High

参数:

攻击:

证据:

CWE ID: 319

WASC ID: 15

根源: 消极的 (10035 - Strict-Transport-Security Header)

Input Vector:

说明: HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

其他信息:

CATS

CATS is a REST API Fuzzer and negative testing tool for OpenAPI endpoints.

Installation via Homebrew

```
brew tap endava/tap
brew install cats
```

Bash

Usage

```
cats --contract=api_openapi.json --server=https://jsonblob.com
```

Bash

github.com

<https://github.com/pnp200/resource/raw/main/cats-report.zip>

Reference

API Security Tools | OWASP Foundation

API Security Tools on the main website for The OWASP Foundation. OWASP is a nonprofit foundation that works to improve the security of software.

[🌐 owasp.org](https://owasp.org)



GitHub - arainho/awesome-api-security: A collection of awesome API Security tools and ...

A collection of awesome API Security tools and resources. The focus goes to open-source tools and resources that benefit all the community. - GitHub - arainho/awesome-api-security: A collection of ...

[🌐 github.com](https://github.com)

arainho/awesome-api-security



A collection of awesome API Security tools and resources. The focus goes to open-source tools and resources that benefit all...

🔗 5 🕒 0 ⭐ 2k 🗨️ 304

