


Snyk dependencies vulnerability check



ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help

marsupialseven@...

csec1 > Projects > csec1/MyTeam\_Testcode

Code Analysis

Overview History Settings

Created Sat 22nd Mar 2025 | Snapshot for commit 2699475 taken by snyk.io 2 minutes ago | Retest now

IMPORTED BY

M marsupialseven@gmail.com

PROJECT OWNER

+ Add a project owner

ENVIRONMENT

+ Add a value

BUSINESS CRITICALITY

+ Add a value

LIFECYCLE

+ Add a value

ANALYSIS SUMMARY

2 analyzed files (29%) Repo breakdown

Issues 2

SEVERITY

High 0

Medium 2

Low 0

PRIORITY SCORE

Scored between 0 - 1000

STATUS

Open 2

Ignored 0

LANGUAGES

Python 2

VULNERABILITY TYPES

Debug Mode Enabled 1

Search

2 of 2 issues

Debug Mode Enabled

SNYK CODE | CWE-489

SCORE 600

13 | response = requests.get('https://httpbin.org/get') # Simple GET request for testing

14 | return f"Hello, world! Here is your request data: {response.json()}"

15 |

16 | if \_\_name\_\_ == '\_\_main\_\_':

17 | app.run(debug=True)

Running the application in debug mode (debug flag is set to True in run) is a security risk if the application is accessible by untrusted parties.

project1/src/snyk\_vulnerable\_app.py

2 steps in 1 file

Ignore Full details

csec1 > Projects > csec1/MyTeam\_Testcode

Code Analysis

Overview History Settings

Search

SEVERITY

High 0

Medium 2

Low 0

PRIORITY SCORE

Scored between 0 - 1000

STATUS

Open 2

Ignored 0

LANGUAGES

Python 2

VULNERABILITY TYPES

Debug Mode Enabled 1

2 of 2 issues

Debug Mode Enabled

SNYK CODE | CWE-489

SCORE 600

13 | response = requests.get('https://httpbin.org/get') # Simple GET request for testing

14 | return f"Hello, world! Here is your request data: {response.json()}"

15 |

16 | if \_\_name\_\_ == '\_\_main\_\_':


17 | app.run(debug=True)

Running the application in debug mode (debug flag is set to True in run) is a security risk if the application is accessible by untrusted parties.

project1/src/snyk\_vulnerable\_app.py

2 steps in 1 file

Ignore Full details



ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help

marsupialseven@...

csec1 > Projects > csec1/MyTeam\_Testcode main

Open on GitHub

Code Analysis

Overview History Settings

LANGUAGES

Python

2

VULNERABILITY TYPES

Debug Mode Enabled

1

Cross-site Scripting (XSS)

1

M

Cross-site Scripting (XSS)

SNYK CODE | CWE-79

SCORE  
600

```
11 @app.route('/')
12 def home():
13     response = requests.get('https://httpbin.org/get') # Simple GET request for testing
14     return f"Hello, world! Here is your request data: {response.json()}"
```

Unsanitized input from **data from a remote resource** flows into **the return value of home**, where it is used to render an HTML page returned to the user. This may result in a Cross-Site Scripting attack (XSS).


project1/src/snyk\_vulnerable\_app.py

4 steps in 1 file

Learn about this type of vulnerability and how to fix it

Ignore

Full details



ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help


marsupialseven@...

Security is a team sport

Invite your team members to view and fix the vulnerabilities across your projects



Copy invite link

Top pending tasks


Project	Fixable Issues	Actions
 csec1/MyTeam_Testcode	1 C 6 H 12 M 0 L	<div>Fix vulnerabilities</div>

Showing 1-1 of 1

Top vulnerable projects

Project	Tested	Issues	Actions
 csec1/MyTeam_Testcode:project1/src/requirements.txt	8 minutes ago	1 C 6 H 12 M 0 L	<div>Fix vulnerabilities</div>
 csec1/MyTeam_Testcode	9 minutes ago	0 C 0 H 2 M 0 L	

Showing 1-2 of 2

snyk

ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help

marsupialseven@...

csec1 > Project > Open a Fix PR

# Open a Fix PR


csec1/MyTeam\_Testcode:project1/src/requirements.txt


[Back to project](#)

## Issues with a fix

An upgrade is available to fix these issues:

- ☐ **H** Information Exposure in flask
- ☐ **H** CRLF injection in urllib3
- ☐ **H** Improper Certificate Validation in urllib3
- ☐ **H** Information Exposure Through Sent Data in urllib3
- ☐ **M** Resource Exhaustion in idna
- ☐ **M** Information Exposure in requests
- ☐ **M** Always-Incorrect Control Flow Implementation in requests
- ☐ **C** Information Exposure in requests
- ☐ **H** HTTP Header Injection in urllib3
- ☐ **H** Remote Code Execution (RCE) in werkzeug
- ☐ **M** Regular Expression Denial of Service (ReDoS) in urllib3



snyk

ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates


Help

marsupialseven@...

csec1 > Project > Open a Fix PR

- ☐ **M** Resource Exhaustion in idna
- ☐ **M** Information Exposure in requests
- ☐ **M** Always-Incorrect Control Flow Implementation in requests
- ☐ **C** Information Exposure in requests
- ☐ **H** HTTP Header Injection in urllib3
- ☐ **H** Remote Code Execution (RCE) in werkzeug
- ☐ **M** Regular Expression Denial of Service (ReDoS) in urllib3
- ☐ **M** Information Exposure Through Sent Data in urllib3
- ☒ **M** Information Exposure Through Sent Data in urllib3
- ☐ **M** Improper Removal of Sensitive Information Before Storage or Transfer in urllib3
- ☐ **M** Authentication Bypass in urllib3
- ☐ **M** Inefficient Algorithmic Complexity in werkzeug
- ☐ **M** Directory Traversal in werkzeug
- ☐ **M** Allocation of Resources Without Limits or Throttling in werkzeug
- ☐ **M** Infinite loop in zipp

Open a PR with upgrades and patches to address the selected issues.



ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help

marsupialseven@...

csec1 > Projects > csec1/MyTeam\_Testcode

Open on GitHub

project1/src/requirements.txt

OverviewHistorySettings

Created Sat 22nd Mar 2025 | Snapshot taken by snyk.io 9 minutes ago | Retest now

IMPORTED BY

Marsupialseven@gmail.com

PROJECT OWNER

Add a project owner

PYTHON

Python 3.7.4

ENVIRONMENT

Add a value

BUSINESS CRITICALITY

Add a value

LIFECYCLE

Add a value

Issues19FixesDependencies14

SEVERITY

19 of 19 issues

Sort by highest priority score

Critical1

High6

Medium12

Low0

NEW

Did you know...

You can reduce the backlog of existing vulnerabilities at a manageable pace with prioritized fix pull requests - enable for your GitHub integration.

Fix these vulnerabilities

ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help

marsupialseven@...

csec1 > Projects > csec1/MyTeam\_Testcode

Open on GitHub

project1/src/requirements.txt

OverviewHistorySettings

SEVERITY

19 of 19 issues

Sort by highest priority score

Critical1

High6

Medium12

Low0

NEW

Did you know...

You can reduce the backlog of existing vulnerabilities at a manageable pace with prioritized fix pull requests - enable for your GitHub integration.

Fix these vulnerabilities

C

requests - Information Exposure

VULNERABILITY | \*\*\*

Introduced through

requests@2.18.4

Fixed in

requests@2.20

Exploit maturity

PROOF OF CONCEPT

Scored between 0 - 1000

811

FIXED IN AVAILABLE

Yes19

No0

COMPUTED FIXABILITY

Fixable19

Partially fixable0

Ignore

Fix this vulnerability

ORGANIZATION

csec1

Dashboard

Projects

Integrations

Members

Settings

Product updates

Help

marsupialseven@...

csec1 > Projects > csec1/MyTeam\_Testcode

Open on GitHub

project1/src/requirements.txt

OverviewHistorySettings

PRIORITY SCORE

Scored between 0 - 1000

"FIXED IN" AVAILABLE

Yes19

No0

COMPUTED FIXABILITY

Fixable19

Partially fixable0

No supported fix0

EXPLOIT MATURITY

Mature1

Proof of concept3

No known exploit15

No data0

C

requests - Information Exposure

VULNERABILITY | \*\*\*

SCORE811

Introduced throughrequests@2.18.4

Fixed inrequests@2.20

Show more detail

Exploit maturity

PROOF OF CONCEPT

Ignore

Fix this vulnerability

H

urllib3 - CRLF injection

VULNERABILITY | CWE-93 | CVE-2019-11236 | CVSS 7.3 | HIGH | SNYK-PYTHON-URLLIB3-174323

SCORE794

Introduced throughrequests@2.18.4

Fixed inurllib3@1.24.3

Show more detail

Exploit maturity

MATURE

Learn about this type of vulnerability

csec1 > Projects > csec1/MyTeam\_Testcode

Open on GitHub

project1/src/requirements.txt

OverviewHistorySettings

No supported fix0

EXPLOIT MATURITY

Mature1

Proof of concept3

No known exploit15

No data0

STATUS

Open19

Patched0

Ignored0

H

urllib3 - CRLF injection

VULNERABILITY | CWE-93 | CVE-2019-11236 | CVSS 7.3 | HIGH | SNYK-PYTHON-URLLIB3-174323

SCORE794

Introduced throughrequests@2.18.4

Fixed inurllib3@1.24.3

Show more detail

Exploit maturity

MATURE

Ignore

Fix this vulnerability

M

zipp - Infinite loop

VULNERABILITY | CWE-835 | CVE-2024-5569 | CVSS 6.9 | MEDIUM | SNYK-PYTHON-ZIPP-7430899

SCORE666

Introduced throughflask@1.0.2

Fixed inzipp@3.19.1

Show more detail

Exploit maturity

PROOF OF CONCEPT

# [Snyk] Security upgrade requests from 2.18.4 to 2.20 #1

🔗 Open

csec1 wants to merge 1 commit into `main` from `snyk-fix-4e637611a89d809f6aaf63943b6c2498`

💬 Conversation0

📄 Commits1

📋 Checks0

📄 Files changed1

+1-1🇩🇪🇬🇧🇪🇪



csec1 commented now



Developer loved, security trusted

Reviewers

No reviews

Still in progress? Learn about draft PRs

🔗 Open

[Snyk] Security upgrade requests from 2.18.4 to 2.20 #1

csec1 wants to merge 1 commit into `main` from `snyk-fix-4e637611a89d809f...`



Developer loved, security trusted

Snyk has created this PR to fix 1 vulnerabilities in the pip dependencies of this project.

Snyk changed the following file(s):

- project1/src/requirements.txt

### Important

- Check the changes in this PR to ensure they won't cause issues with your project.
- Max score is 1000. Note that the real score may have changed

No reviews

Still in progress? Learn about draft PRs

Assignees

csec1

Labels

None yet

Projects

None yet

Milestone

No milestone

 Open

[Snyk] Security upgrade requests from 2.18.4 to 2.20 #1

csec1 wants to merge 1 commit into [main](#) from [snyk-fix-4e637611a89d809f...](#) 



### Some checks were not successful

1 failing, 1 successful checks

1 failing check ▾



SonarQube Scan / Run SonarQube analysis (...)



1 successful check ▾



security/snyk (csec1) — 1 security test has pas...



### No conflicts with base branch

Merging can be performed automatically.

Merge pull request ▾

You can also merge this with the command line.

[View command line instructions.](#)

