

kirangopisetty



vulnerable-api master

## Code Analysis

[Overview](#) [History](#) [Settings](#)

Created Fri 25th Feb 2022  
Snapshot taken by snyk.io [a few seconds ago](#)

[Retest now](#)

## IMPORTED BY

kiran.gopisetty@gmail.com

## PROJECT OWNER

[Add a project owner](#)

## SCAN COVERAGE

1 Files ( 6% coverage ) [View breakdown](#)



Search...

7 of 7 issues

Group by none Sort by highest severity

# H Cross-site Scripting (XSS)

SNYK CODE | [CWE-79](#)

SCORE


823


```
235         'Command': command,
236         'Output': output
237     }
238 }
239 ...return json.dumps(response, sort_keys=True, indent=2)
```

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

 [ansible/roles/api/files/vAPI.py](#)

17 steps in 1 file

 Ignore

 Full details

# H Cross-site Scripting (XSS)

SNYK CODE | [CWE-79](#)

SCORE


823

```
140     c = conn.cursor()
141     query = "SELECT * FROM users"
142     c.execute(query)
143     users = c.fetchall()
144     return {'response': users}
```

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

 [ansible/roles/api/files/vAPI.py](#)

6 steps in 1 file

 Ignore Full details

## SQL Injection


SNYK CODE | [CWE-89](#) SCORE  
**812**

```
76         # make sure to get most recent token in database, because we arent
77         # removing them...
78         token_query = "SELECT * FROM tokens WHERE userid = '%s' ORDER BY expires DESC" % (user[
79                                                         0])
80         c.execute(token_query)
```

Unsanitized input from *the database flows* into *execute*, where it is used in an SQL query. This may result in an SQL Injection vulnerability.

 [ansible/roles/api/files/vAPI.py](#)

11 steps in 1 file

 Ignore Full details

## Command Injection

SNYK CODE | [CWE-78](#) SCORE  
**812**

```
228     if flag:
229         command = "uptime -" + flag
230     else:
231         command = "uptime"
232     output = os.popen(command).read()
```

Unsanitized input from *an HTTP parameter flows* into *os.popen*, where it is used as a shell command. This may result in a Command Injection vulnerability.

 ansible/roles/api/files/vAPI.py

8 steps in 1 file

 Ignore

 Full details

## insecureHash

SNYK CODE

SCORE  
**573**


```
104         else:
105             # no token exists. create one that expires in 5 minutes
106             expire_stamp = int(time.time() + 300)
107             expire_date = time.ctime(int(expire_stamp))
108             token = hashlib.md5(expire_date).hexdigest()
```

*hashlib.md5* is insecure. Consider changing it to a secure hashing algorithm (e.g. SHA256).

 ansible/roles/api/files/vAPI.py

1 step in 1 file

 Ignore

 Full details

## insecureHash

SNYK CODE

SCORE  
**573**


```
84         # token has expired. create new one that expires 5 minutes
85         # after creation
86         expire_stamp = int(time.time() + 300)
87         expire_date = time.ctime(int(expire_stamp))
88         token = hashlib.md5(expire_date).hexdigest()
```

*hashlib.md5* is insecure. Consider changing it to a secure hashing algorithm (e.g. SHA256).

 [ansible/roles/api/files/vAPI.py](#)

1 step in 1 file

 Ignore

 Full details

## InsecureXmlParser

SNYK CODE

SCORE

562


```
47     if content_type == 'application/xml':
48         try:
49             # LXML is vulnerable to XXE, etree is vulnerable to Billion Laughs
50             # So just have etree try to parse it just to watch it die
51             ET.parse(request.body)
```

*xml.etree.ElementTree.parse* is considered insecure. Use an analog from the defusedxml package.

 [ansible/roles/api/files/vAPI.py](#)

1 step in 1 file

 Ignore

 Full details

