EXPERIMENT 05

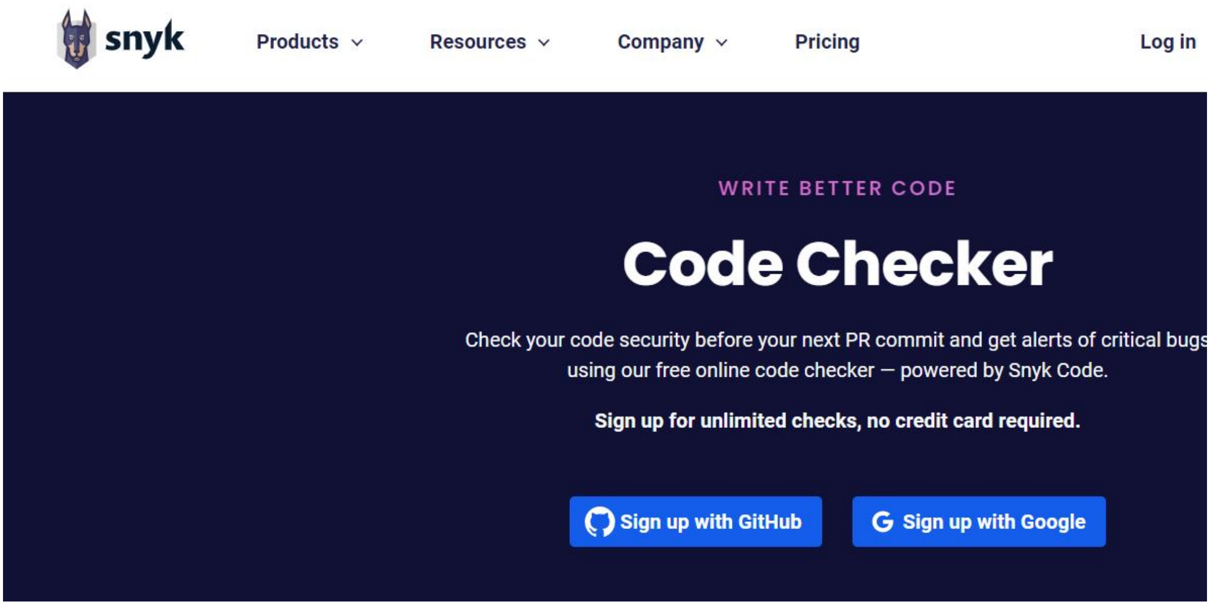
SAST TOOL : SYNK

CODE :

```
import os

import urllib

from flask import Flask, request

from django.db import connection, models

from django.db.models.expressions import RawSQL


app = Flask(__name__)


@app.route("/code-execution")

def code_execution():

    code1 = request.args.get("code1")

    exec("setname('%s')" % code1)

    return a


@app.route("/open-redirect")

def open_redirect():

    redirect_loc = request.args.get('redirect')

    return redirect(redirect_loc)



@app.route("/sqli/<username>")

def show_user(username):

    with connection.cursor() as cursor:

      cursor.execute("SELECT * FROM users WHERE username = '%s'" % username)


if __name__ == '__main__':
```

```
app.run(host='0.0.0.0', port=9000)
```

SOURCE CODE REVIEW USING SYNK

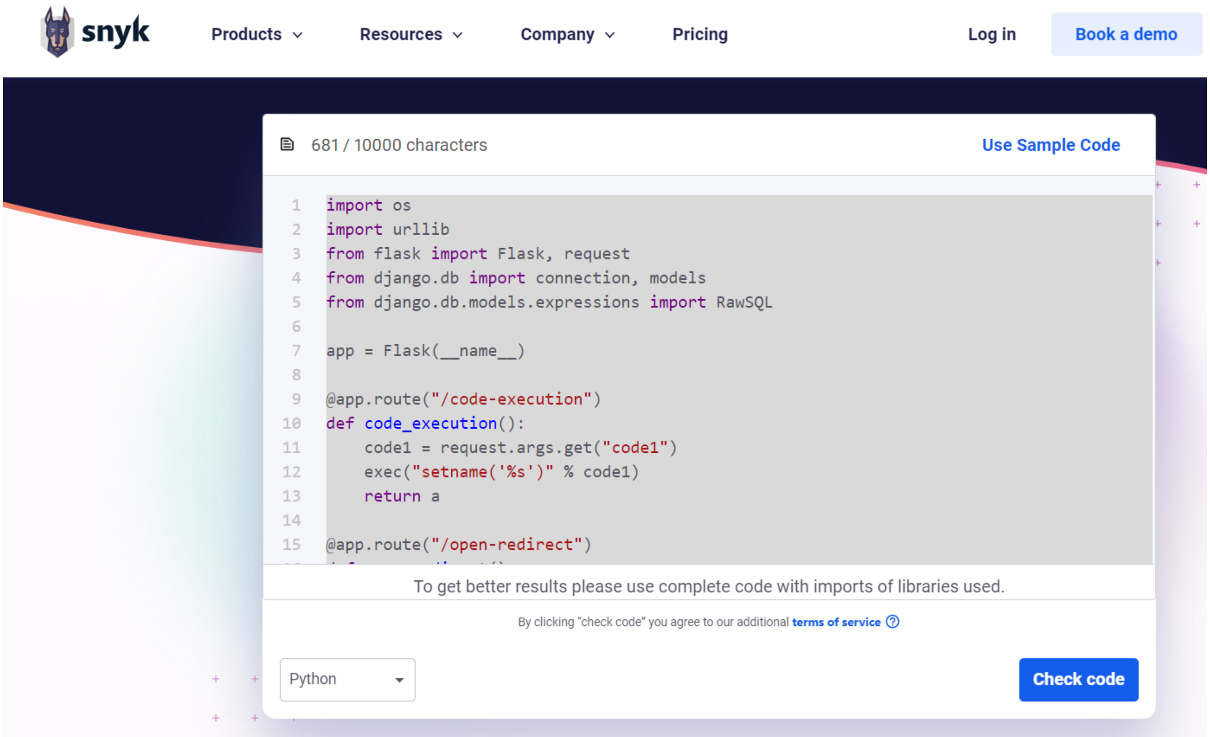


WRITE BETTER CODE

Code Checker

Check your code security before your next PR commit and get alerts of critical bugs using our free online code checker — powered by Snyk Code.

Sign up for unlimited checks, no credit card required.

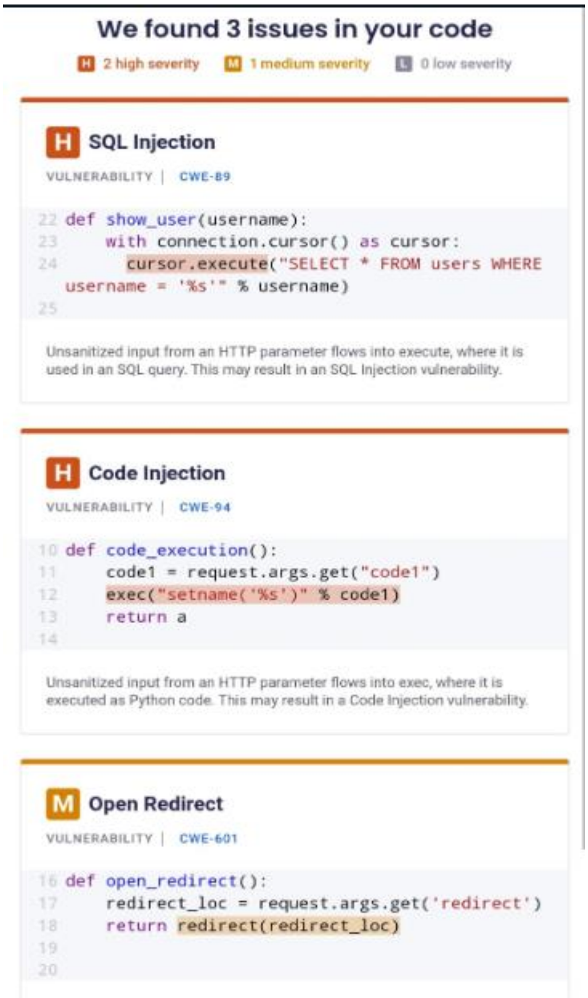


681 / 10000 characters

```python
import os
import urllib
from flask import Flask, request
from django.db import connection, models
from django.db.models.expressions import RawSQL

app = Flask(__name__)

@app.route("/code-execution")
def code_execution():
    code1 = request.args.get("code1")
    exec("setname('%s')" % code1)
    return a

@app.route("/open-redirect")
```

To get better results please use complete code with imports of libraries used.

By clicking "check code" you agree to our additional **terms of service**



We found 3 issues in your code

H 2 high severity M 1 medium severity L 0 low severity

H SQL Injection

VULNERABILITY | CWE-89

```
def show_user(username):
    with connection.cursor() as cursor:
      cursor.execute("SELECT * FROM users WHERE
username = '%s'" % username)

```

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

H Code Injection

VULNERABILITY | CWE-94

```
def code_execution():
    code1 = request.args.get("code1")
    exec("setname('%s')" % code1)
    return a

```

Unsanitized input from an HTTP parameter flows into exec, where it is executed as Python code. This may result in a Code Injection vulnerability.

M Open Redirect

VULNERABILITY | CWE-601

```
def open_redirect():
    redirect_loc = request.args.get('redirect')
    return redirect(redirect_loc)


```