**fragment1:**

**Command injection vulnerability**

**Debug information exposure**

**Code:**

import os

from flask import Flask, request

app = Flask(\_\_name\_\_)

# curl -X GET "http://localhost:5000/tainted7/touch%20HELLO"

@app.route("/tainted7/<something>")

def test\_sources\_7(something):

os.system(request.remote\_addr)

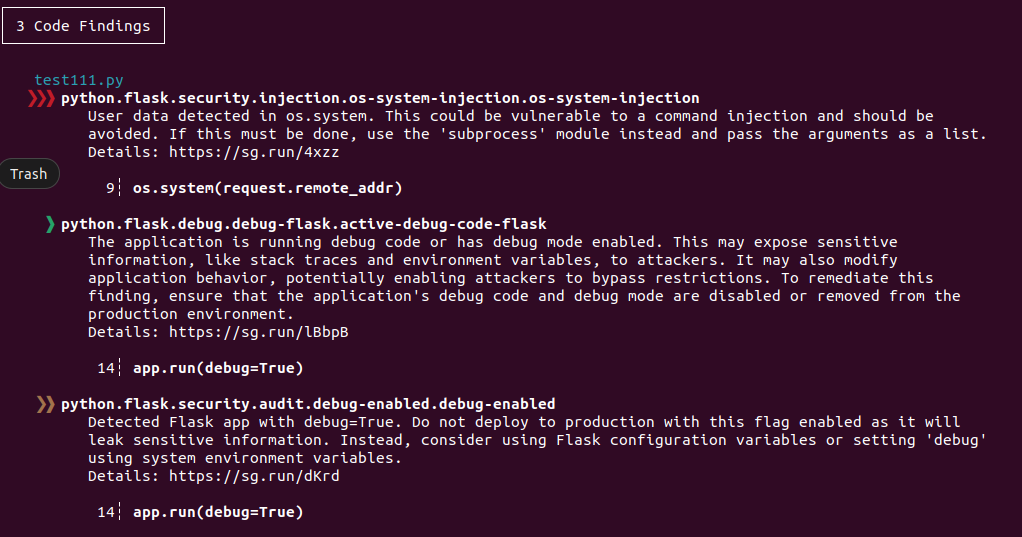
return "foo"

if \_\_name\_\_ == "\_\_main\_\_":

app.run(debug=True)

**Scan result:**

semgrep scan test111.py --config "p/flask"



**fragment2:**

**Command injection vulnerability**

**Code:**

const express = require('express');

const router = express.Router()

const { exec, spawn } = require('child\_process');

router.post('/ping', (req,res) => {

exec(`${req.body.url}`, (error) => {

if (error) {

return res.send('error');

}

res.send('pong')

})

})

router.post('/gzip', (req,res) => {

exec(

'gzip ' + req.query.file\_path,

function (err, data) {

console.log('err: ', err)

console.log('data: ', data);

res.send('done');

});

})

router.get('/run', (req,res) => {

let cmd = req.params.cmd;

runMe(cmd,res)

});

function runMe(cmd,res){

// return spawn(cmd);

const cmdRunning = spawn(cmd, []);

cmdRunning.on('close', (code) => {

res.send(`child process exited with code ${code}`);

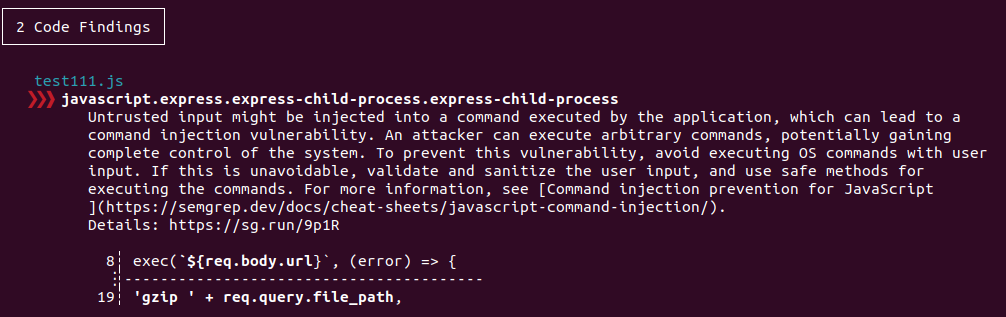
});

}

module.exports = router

**Scan result:**

semgrep scan test111.js --config "p/javascript"



**fragment3:**

**Command injection vulnerability**

**Code:**

<?php include("../common/header.php"); ?>

<!-- from https://pentesterlab.com/exercises/php\_include\_and\_post\_exploitation/course -->

<?php hint("will exec 'whois' with the arg specified in the POST parameter \"domain\""); ?>

<form action="/CMD-4/index.php" method="POST">

<input type="text" name="domain">

</form>

<pre>

<?php

system("whois " . $\_POST["domain"]);

?>

</pre>

**Scan result:**

semgrep scan test111.php --config "p/php"

