ATTACK DEFENSE

by PentesterAcademy

Name	Prog Pilot: Statically Scanning PHP Code
URL	https://www.attackdefense.com/challengedetails?cid=2159
Type	DevSecOps Basics: Static Application Security Testing

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Challenge Description

The ProgPilot tool is used to find vulnerabilities in PHP applications.

A Kali CLI machine (kali-cli) is provided to the user with Progpilot installed on it. The source code for three sample applications is provided in the home directory of the root user.

Objective: Use the progpilot utility to find vulnerabilities in the applications!

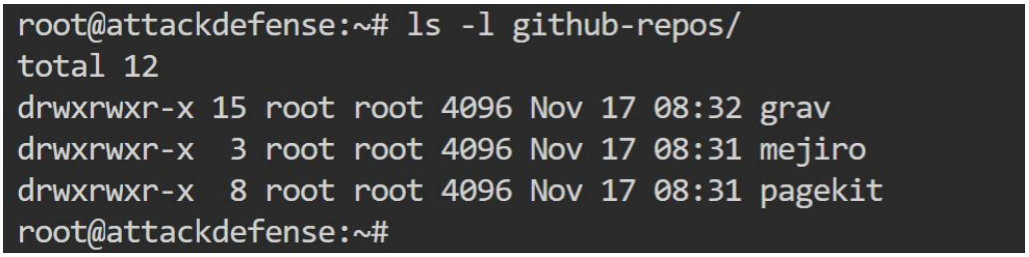
Instructions:

- The source code of applications is provided at /root/github-repos

Solution

Step 1: Check the provided applications.

Command: ls -l github-repos



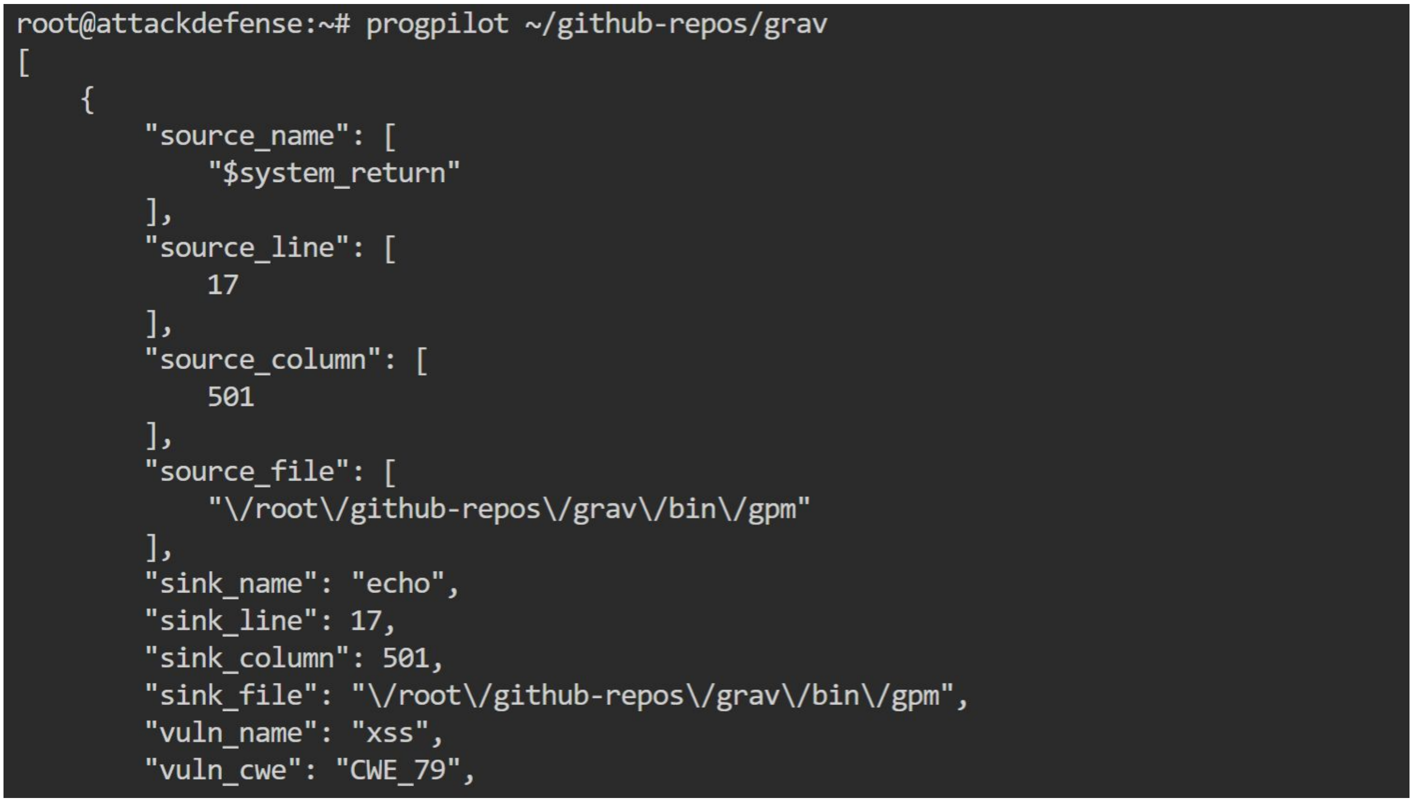
```
root@attackdefense:~# ls -l github-repos/
total 12
drwxrwxr-x 15 root root 4096 Nov 17 08:32 grav
drwxrwxr-x  3 root root 4096 Nov 17 08:31 mejiro
drwxrwxr-x  8 root root 4096 Nov 17 08:31 pagekit
root@attackdefense:~#
```

We will take one example at a time and run the tool on that.

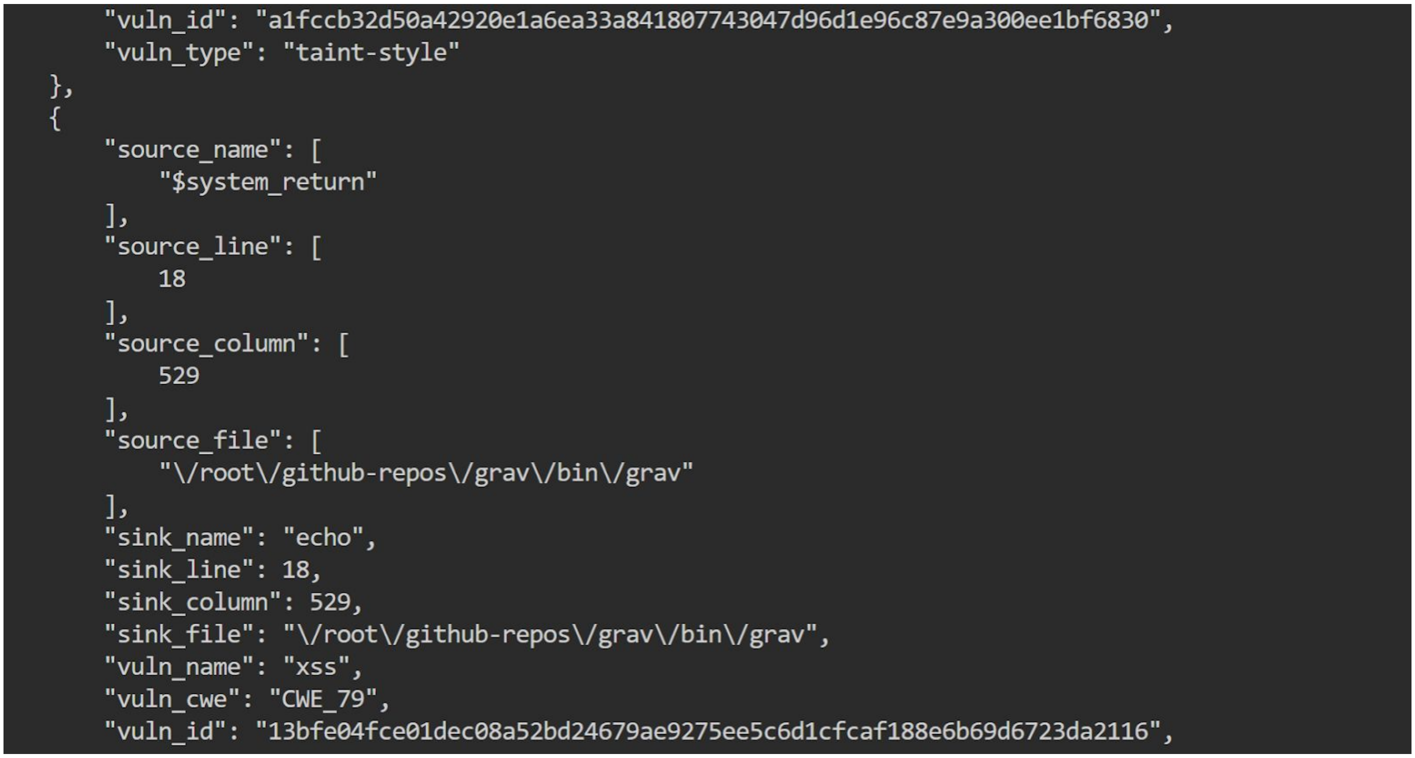
Example 1: grav

Step 1: Run the progpilot tool on the grav project directory.

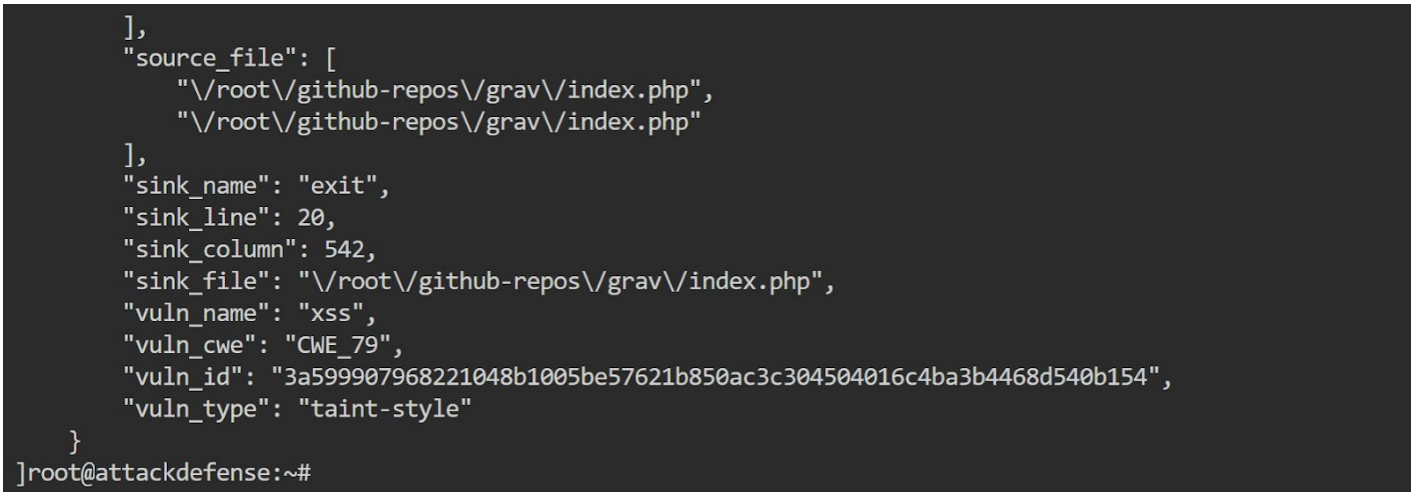
Command: progpilot ~/github-repos/grav



```
root@attackdefense:~# progpilot ~/github-repos/grav
[
    {
        "source_name": [
            "$system_return"
        ],
        "source_line": [
            17
        ],
        "source_column": [
            501
        ],
        "source_file": [
            "\/root\/github-repos\/grav\/bin\/gpm"
        ],
        "sink_name": "echo",
        "sink_line": 17,
        "sink_column": 501,
        "sink_file": "\/root\/github-repos\/grav\/bin\/gpm",
        "vuln_name": "xss",
        "vuln_cwe": "CWE_79",
```



```
        "vuln_id": "a1fccb32d50a42920e1a6ea33a841807743047d96d1e96c87e9a300ee1bf6830",
        "vuln_type": "taint-style"
    },
    {
        "source_name": [
            "$system_return"
        ],
        "source_line": [
            18
        ],
        "source_column": [
            529
        ],
        "source_file": [
            "\/root\/github-repos\/grav\/bin\/grav"
        ],
        "sink_name": "echo",
        "sink_line": 18,
        "sink_column": 529,
        "sink_file": "\/root\/github-repos\/grav\/bin\/grav",
        "vuln_name": "xss",
        "vuln_cwe": "CWE_79",
        "vuln_id": "13bfe04fce01dec08a52bd24679ae9275ee5c6d1cfcaf188e6b69d6723da2116",
```



```
        ],
        "source_file": [
            "\/root\/github-repos\/grav\/index.php",
            "\/root\/github-repos\/grav\/index.php"
        ],
        "sink_name": "exit",
        "sink_line": 20,
        "sink_column": 542,
        "sink_file": "\/root\/github-repos\/grav\/index.php",
        "vuln_name": "xss",
        "vuln_cwe": "CWE_79",
        "vuln_id": "3a599907968221048b1005be57621b850ac3c304504016c4ba3b4468d540b154",
        "vuln_type": "taint-style"
    }
]root@attackdefense:~#
```

The tool has identified Cross-site scripting in multiple sections.

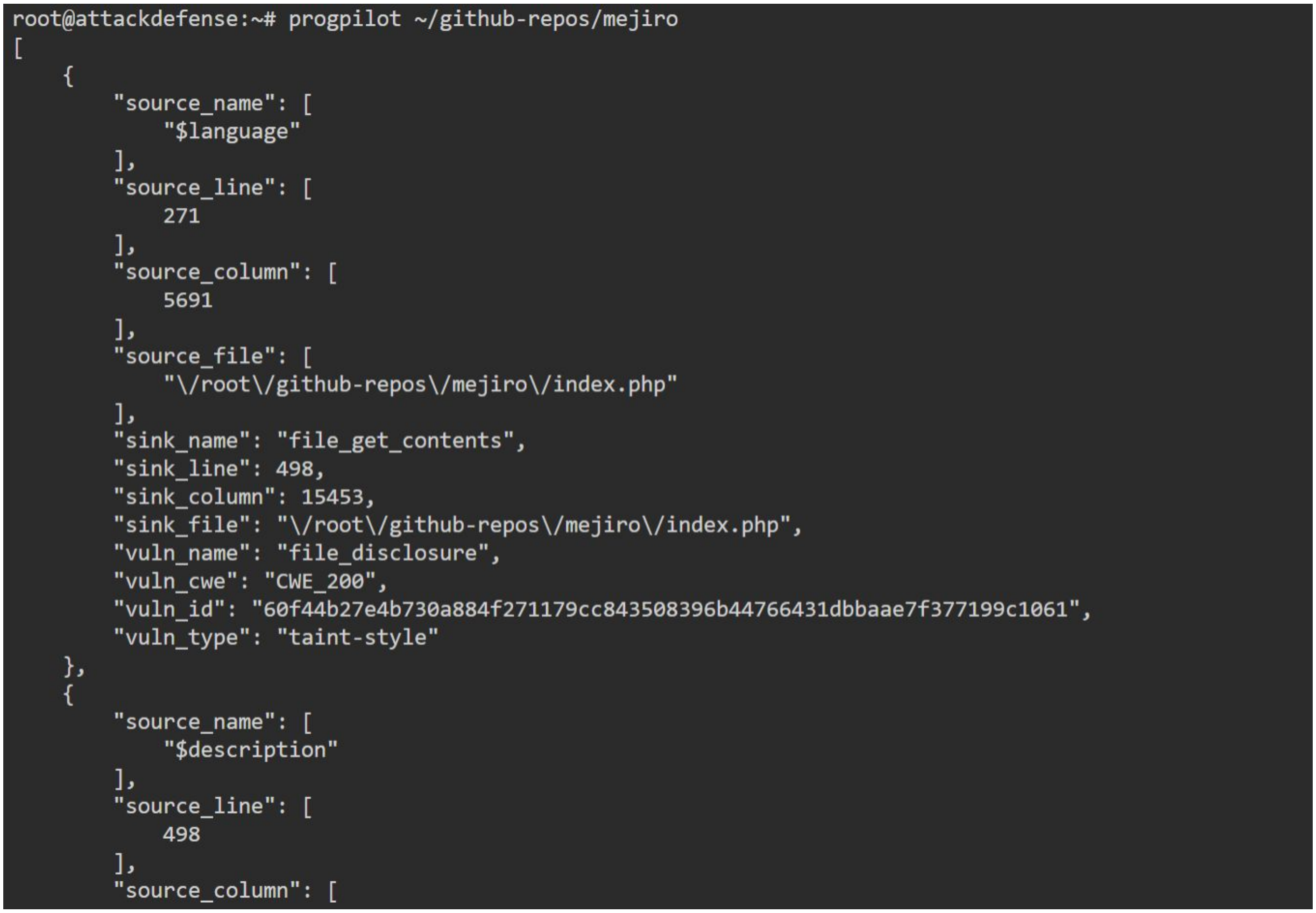
Issues Identified:

- Cross-Site Scripting (CWE-79)

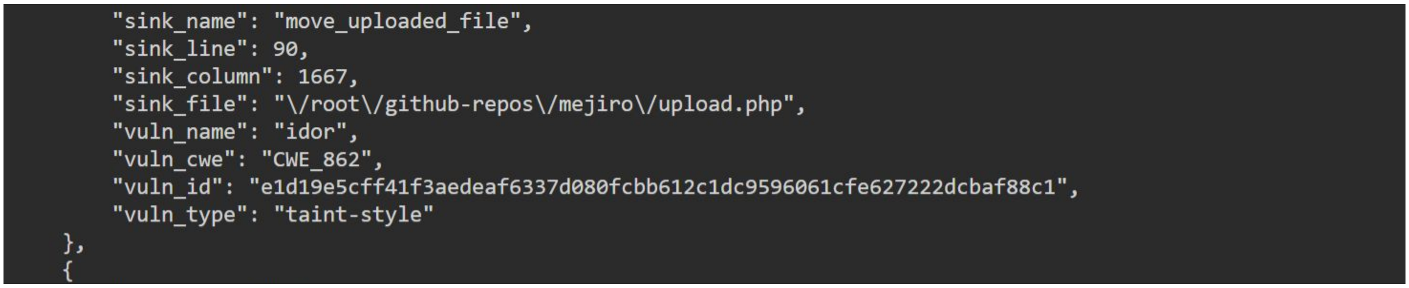
Example 2: mejiro

Step 1: Run the progpilot tool on the mejiro project directory.

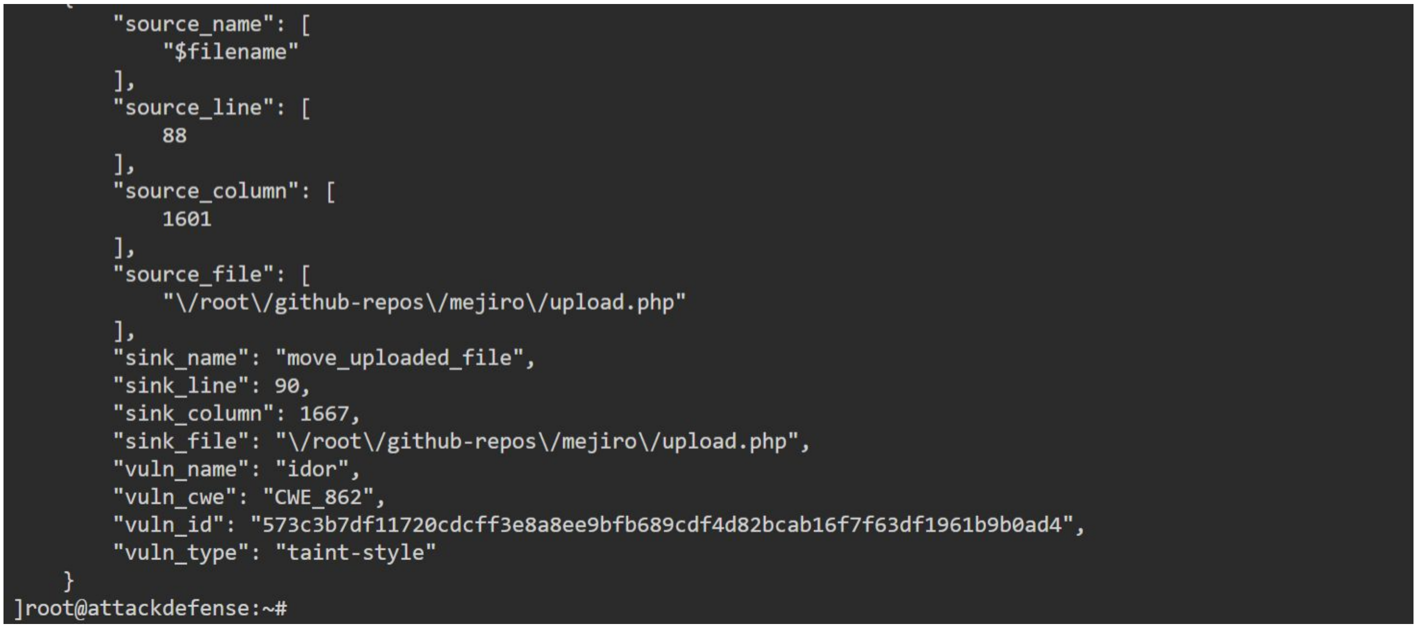
Command: progpilot ~/github-repos/mejiro



```
root@attackdefense:~# progpilot ~/github-repos/mejiro
[
    {
        "source_name": [
            "$language"
        ],
        "source_line": [
            271
        ],
        "source_column": [
            5691
        ],
        "source_file": [
            "\/root\/github-repos\/mejiro\/index.php"
        ],
        "sink_name": "file_get_contents",
        "sink_line": 498,
        "sink_column": 15453,
        "sink_file": "\/root\/github-repos\/mejiro\/index.php",
        "vuln_name": "file_disclosure",
        "vuln_cwe": "CWE_200",
        "vuln_id": "60f44b27e4b730a884f271179cc843508396b44766431dbbaae7f377199c1061",
        "vuln_type": "taint-style"
    },
    {
        "source_name": [
            "$description"
        ],
        "source_line": [
            498
        ],
        "source_column": [
```



```
        "sink_name": "move_uploaded_file",
        "sink_line": 90,
        "sink_column": 1667,
        "sink_file": "\/root\/github-repos\/mejiro\/upload.php",
        "vuln_name": "idor",
        "vuln_cwe": "CWE_862",
        "vuln_id": "e1d19e5cff41f3aedeaf6337d080fcbb612c1dc9596061cfe627222dcbaf88c1",
        "vuln_type": "taint-style"
    },
    {
```



```
        "source_name": [
            "$filename"
        ],
        "source_line": [
            88
        ],
        "source_column": [
            1601
        ],
        "source_file": [
            "\/root\/github-repos\/mejiro\/upload.php"
        ],
        "sink_name": "move_uploaded_file",
        "sink_line": 90,
        "sink_column": 1667,
        "sink_file": "\/root\/github-repos\/mejiro\/upload.php",
        "vuln_name": "idor",
        "vuln_cwe": "CWE_862",
        "vuln_id": "573c3b7df11720cdcff3e8a8ee9bfb689cdf4d82bcab16f7f63df1961b9b0ad4",
        "vuln_type": "taint-style"
    }
]root@attackdefense:~#
```

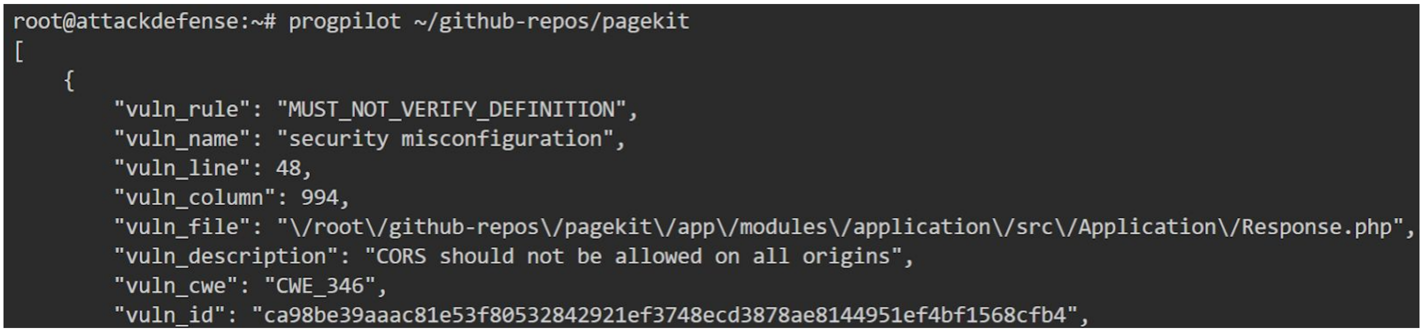
Issues Detected

- File disclosure (CWE-200)
- Insecure direct object references (CWE-862)
- cookie setted without secure or httponly flags (CWE-1004)
- Cross-Site Scripting (CWE-79)

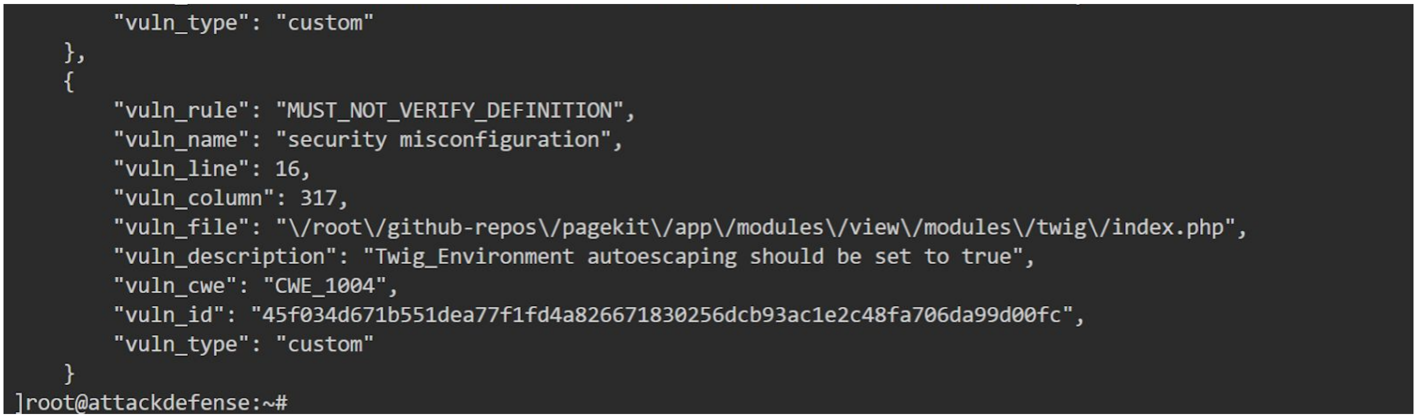
Example 3: Pagekit

Step 1: Run the progpilot tool on the pagekit project directory.

Command: progpilot ~/github-repos/pagekit



```
root@attackdefense:~# progpilot ~/github-repos/pagekit
[
    {
        "vuln_rule": "MUST_NOT_VERIFY_DEFINITION",
        "vuln_name": "security misconfiguration",
        "vuln_line": 48,
        "vuln_column": 994,
        "vuln_file": "\/root\/github-repos\/pagekit\/app\/modules\/application\/src\/Application\/Response.php",
        "vuln_description": "CORS should not be allowed on all origins",
        "vuln_cwe": "CWE_346",
        "vuln_id": "ca98be39aaac81e53f80532842921ef3748ecd3878ae8144951ef4bf1568cfb4",
```



```
        "vuln_type": "custom"
    },
    {
        "vuln_rule": "MUST_NOT_VERIFY_DEFINITION",
        "vuln_name": "security misconfiguration",
        "vuln_line": 16,
        "vuln_column": 317,
        "vuln_file": "\/root\/github-repos\/pagekit\/app\/modules\/view\/modules\/twig\/index.php",
        "vuln_description": "Twig_Environment autoescaping should be set to true",
        "vuln_cwe": "CWE_1004",
        "vuln_id": "45f034d671b551dea77f1fd4a826671830256dcb93ac1e2c48fa706da99d00fc",
        "vuln_type": "custom"
    }
]root@attackdefense:~#
```

Issues Detected

- CORS should not be allowed on all origins (CWE-346)
- Twig_Environment autoescaping should be set to true (CWE-1004)

Learnings

Perform Static Code Analysis using the Progpilot tool.

References:

- Mejiro (https://github.com/dmpop/mejiro.git)
- PageKit (https://github.com/pagekit/pagekit.git)
- Grav (https://github.com/getgrav/grav.git)