

Sri Lanka Institute of Information Technology



Specialized in Cyber Security

Year 2, Semester 2

IE2062 – Web Security

Bug Bounty – Report 05

Student ID No.	Name
IT23136106	D.M.M. Pasindu Supushmika

Table of Contents

- 01. [Website Overview](#)
- 02. [Step 01: Gather Information](#)
 - a. [Subdomain Discovery](#)
 - i. [Sublist3r](#)
 - ii. [Subfinder](#)
 - b. [Live Subdomains](#)
 - c. [IP Discovery](#)
 - d. [Open Ports](#)
 - e. [Used Technologies](#)
- 03. [Step 02: Scanning and Vulnerability Identification](#)
 - a. [Identify Potential Vulnerabilities](#)
 - b. [Application Error Disclosure](#)
- 04. [Step 03: Exploitation and Validation](#)
- 05. [Step 04: Mitigation / Fix](#)

1. Website Overview

[Dynatrace | Understand your business like never before](#)

HackerOne Link: [Dynatrace](#) | [Bug Bounty Program Policy](#) | [HackerOne](#)

Security page
Program guidelines
Scope
Hacktivity
Thanks
Updates
Collaborators

Program highlights

Platform Standards
Fully compliant with Platform Standards.

Top Response Efficiency
This program's response efficiency is above 90%.

Managed by HackerOne
Collaboration Enabled
Includes Retesting

🕒
2 days, 3 hours
Average time to first response

📄
3 days, 1 hour
Average time to triage

💰
1 week, 1 day
Average time to bounty

💰
1 week, 4 days
Average time from submission to bounty

📅
2 weeks, 1 day
Average time to resolution

Rewards summary

Last updated on January 8, 2024. [View changes](#)

Each severity lists the 90-day average bounty and the percentage of total resolved reports, if applicable.

Asset	Low	Medium	High	Critical

Dynatrace
<https://dynatrace.com>
Application Performance, Real-User / Cloud Monitoring Solution [SaaS based]
Bug Bounty Program launched in Jan 2024

- Response efficiency: 90%

[Submit report](#)

Rewards

Severity	Rewards
Low	\$100-\$250 Avg. bounty \$192 39.19% submissions
Medium	\$250-\$750 Avg. bounty \$850 34.43% submissions
High	\$500-\$2,500

Platform
Solutions
Resources
Company
Pricing
Support
Login
[Free trial](#)

Understand your business like never before

Transform complexity into your greatest asset with the leader in AI-powered observability.

[Explore Playground](#)
[Request a demo](#)

Step 01: Gather Information.

a. Sub-domain Discovery

i. Sublist3r: [sublist3r_dynatrace_results.txt](#)

Tool : Sublist3r

Code : python3 sublist3r.py -d dynatrace.com -o sublist3r_dynatrace_results.txt

Explanation:

python3 sublist3r.py - Run the script using python

-d dynatrace.com - Target domain

-o sublist3r_dynatrace_results.txt – Output file where the result is saved

```
[-] Enumerating subdomains now for dynatrace.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
Process DNSdumpster-8:
Traceback (most recent call last):
  File "/usr/lib/python3.13/multiprocessing/process.py", line 313, in _bootstrap
    self.run()
    ~~~~~^
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 268, in run
    domain_list = self.enumerate()
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 647, in enumerate
    token = self.get_csrf_token(resp)
  File "/home/kali/Desktop/Sublist3r/sublist3r.py", line 641, in get_csrf_token
    token = csrf_regex.findall(resp)[0]
    ~~~~~^
IndexError: list index out of range
[!] Error: Virustotal probably now is blocking our requests
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Saving results to file: sublist3r_dynatrace_results.txt
[-] Total Unique Subdomains Found: 654
www.dynatrace.com
AT1i-ISE-01.dynatrace.com
AT1i-ISE-02.dynatrace.com
a.dynatrace.com
access-approval.dynatrace.com
account.dynatrace.com
www.account.dynatrace.com
ace-tools.dynatrace.com
api.ace-tools.dynatrace.com
internal.ace-tools.dynatrace.com
api.internal.ace-tools.dynatrace.com
siem-prod.internal.ace-tools.dynatrace.com
sso-access.admin-portal.dynatrace.com
ajax.dynatrace.com
amplify.dynatrace.com
```

Activate W
Go to Settings

www.dynatrace.com
AT1i-ISE-01.dynatrace.com
AT1i-ISE-02.dynatrace.com
a.dynatrace.com
access-approval.dynatrace.com
account.dynatrace.com
www.account.dynatrace.com
ace-tools.dynatrace.com
api.ace-tools.dynatrace.com
internal.ace-tools.dynatrace.com
api.internal.ace-tools.dynatrace.com
siem-prod.internal.ace-tools.dynatrace.com
sso-access.admin-portal.dynatrace.com
ajax.dynatrace.com
amplify.dynatrace.com
answers.dynatrace.com
www.answers.dynatrace.com
apac-sbc.dynatrace.com
www.apac-sbc.dynatrace.com
api.dynatrace.com
apm-confluence.dynatrace.com
apmblog.dynatrace.com
apmu.dynatrace.com
www.apmu.dynatrace.com
apmu-dev.dynatrace.com
www.apmu-dev.dynatrace.com
apmu-vlabs.dynatrace.com
www.apmu-vlabs.dynatrace.com
apmwiki.dynatrace.com
applicationperformance.dynatrace.com
appmon-webservice.dynatrace.com
apps.dynatrace.com
apeks-prod1-us-east-1.apps.dynatrace.com
apeks-prod2-eu-west-1.apps.dynatrace.com
assets.dynatrace.com
assistant.dynatrace.com
www.assistant.dynatrace.com
bi.assistant.dynatrace.com
autodiscover.dynatrace.com
awarenesstraining.dynatrace.com
jobs.barcelona.dynatrace.com
barista.dynatrace.com
benchmarks.dynatrace.com
gdn-kban-test.bf.dynatrace.com
kbannach-test.bf.dynatrace.com
bi.dynatrace.com
tableau.bi.dynatrace.com
emea.tableau.bi.dynatrace.com
emeap.tableau.bi.dynatrace.com
noram.tableau.bi.dynatrace.com
noramp.tableau.bi.dynatrace.com
pub.tableau.bi.dynatrace.com
biemea.dynatrace.com
bitsight.dynatrace.com
blog.dynatrace.com
book.dynatrace.com

ii. Subfinder: [subfinder result dynatrace.txt](#)**Tool** : Subfinder**Code** : subfinder -d Dynatrace.com -o subfinder_result_dynatrace.txt**Explanation:***subfinder* - run subfinder too*-d dynatrace.com* - Mention the target website*-o subfinder_result.txt* – Mention the output file

```

Home
Subfinder
projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for dynatrace.com
saas-gateway.spine.internal.dynatrace.com
mgmt.plsrv.prod4.dtp.internal.dynatrace.com
bf50616tne.bf.dynatrace.com
testing.v2.keybroker.spine.internal.dynatrace.com
uss.noram.insights.dynatrace.com
bf08379irm.bf.dynatrace.com
bf73521gdg.bf.dynatrace.com
ssprsetup.dynatrace.com
srv.grail.prod6.dtp.internal.dynatrace.com
bf71615ufy.bf.dynatrace.com
iam-gateway.spine.internal.dynatrace.com
mobilecontent.dynatrace.com
www.staging-defect.dynatrace.com
bf44553uhf.bf.dynatrace.com
bf19629get.bf.dynatrace.com
bf41316fic.bf.dynatrace.com
careers.dynatrace.com
token.dynatrace.com
cxblog.dynatrace.com
mxr.dynatrace.com
bf04098hbb.bf.dynatrace.com
bf45614mfj.bf.dynatrace.com
bf52325khw.bf.dynatrace.com
mgmt.grail.prod13.dtp.internal.dynatrace.com
dev-lwfusion-search-nv-zk.ocs.dynatrace.com
bf08581rsl.bf.dynatrace.com
bf27853irn.bf.dynatrace.com
bf44680uzd.bf.dynatrace.com
bf18264pgn.bf.dynatrace.com
lima-autoprov.spine.internal.dynatrace.com
zendesk.dynatrace.com
bf09668xdm.bf.dynatrace.com
bf54607cnw.bf.dynatrace.com
search.dynatrace.com
jamfadcs.dynatrace.com
bf36631rar.bf.dynatrace.com
applicationperformance.dynatrace.com
jobs.dynatrace.com
us-east-1.token.dynatrace.com
bf00533cik.bf.dynatrace.com
bf04658cjb.bf.dynatrace.com
bf17610ysy.bf.dynatrace.com
bf46250qfs.bf.dynatrace.com

```

Activate Win
Go to Settings to

saas-gateway.spine.internal.dynatrace.com
mgmt.plsrv.prod4.dtp.internal.dynatrace.com
bf50616tne.bf.dynatrace.com
testing.v2.keybroker.spine.internal.dynatrace.com
uss.noram.insights.dynatrace.com
bf08379irm.bf.dynatrace.com
bf73521gdg.bf.dynatrace.com
ssprsetup.dynatrace.com
srv.grail.prod6.dtp.internal.dynatrace.com
bf71615ufy.bf.dynatrace.com
iam-gateway.spine.internal.dynatrace.com
mobilecontent.dynatrace.com
www.staging-defect.dynatrace.com
bf44553uhf.bf.dynatrace.com
bf19629get.bf.dynatrace.com
bf41316fic.bf.dynatrace.com
careers.dynatrace.com
token.dynatrace.com
cxblog.dynatrace.com
mxr.dynatrace.com
bf04098hbb.bf.dynatrace.com
bf45614mfj.bf.dynatrace.com
bf52325khw.bf.dynatrace.com
mgmt.grail.prod13.dtp.internal.dynatrace.com
dev-lwfusion-search-nv-zk.ocs.dynatrace.com
bf08581rsl.bf.dynatrace.com
bf27853irn.bf.dynatrace.com
bf44680uzd.bf.dynatrace.com
bf18264pgn.bf.dynatrace.com
lima-autoprov.spine.internal.dynatrace.com
zendesk.dynatrace.com
bf09668xdm.bf.dynatrace.com
bf54607cnw.bf.dynatrace.com
search.dynatrace.com
jamfadcs.dynatrace.com
bf36631rar.bf.dynatrace.com
applicationperformance.dynatrace.com
jobs.dynatrace.com
us-east-1.token.dynatrace.com
bf00533cik.bf.dynatrace.com
bf04658cjb.bf.dynatrace.com
bf17610ysy.bf.dynatrace.com
bf46250qfs.bf.dynatrace.com
hub-api.spine.internal.dynatrace.com
srv.apigw.prod5.dtp.dynatrace.com
umsbcar06.dynatrace.com
api.dynatrace.com
bf81540srt.bf.dynatrace.com
easytravel.demo.dynatrace.com
benchmarks.dynatrace.com
files.dynatrace.com
siem-prod.internal.ace-tools.dynatrace.com

`-o livesub_results.txt` – mention the file which should write the output

```
~/Desktop/dynatrace)
$ curl -s https://api.dynatrace.com/web_results.txt | \
jq -r '.urls | map(select(.url | contains("https://"))) | sort_by(.url)'
[{"url": "https://api.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.insights.dynatrace.com/x", "status": 200, "method": "GET"}, {"url": "https://ajax.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.myaccount.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.sso-beta.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://answers.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://access-approval.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://apmblog.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.sso.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://amplify.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.ace-tools.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://applicationperformance.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://apmu.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.university.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.mobileagent.downloads.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://admin.myaccount.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://a.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.devops-services.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://account.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://arm.cxapps.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://ace-tools.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://artemis-search.spine.internal.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://artemis-api.spine.internal.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://artemis-support.spine.internal.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://artemis.spine.internal.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://assets.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://assets.cloud.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://attachments.one.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://aws.cloud.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://api.careers.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://awarenesstraining.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://barista.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://apply.careers.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://benchmarks.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://auto-response-manager.cxapps.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf00539hsb.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf01006zdw.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf01632wee.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf00533cik.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf01010lrr.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf01739bkp.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf01002bli.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf02779stq.bf.dynatrace.com", "status": 200, "method": "GET"}, {"url": "https://bf02606zwy.bf.dynatrace.com", "status": 200, "method": "GET"}]
```


<https://api.dynatrace.com>
<https://api.insights.dynatrace.com>
<https://ajax.dynatrace.com>
<https://api.myaccount.dynatrace.com>
<https://api.sso-beta.dynatrace.com>
<https://answers.dynatrace.com>
<https://access-approval.dynatrace.com>
<https://apmblog.dynatrace.com>
<https://api.sso.dynatrace.com>
<https://amplify.dynatrace.com>
<https://api.ace-tools.dynatrace.com>
<https://applicationperformance.dynatrace.com>
<https://apmu.dynatrace.com>
<https://api.university.dynatrace.com>
<https://api.mobileagent.downloads.dynatrace.com>
<https://admin.myaccount.dynatrace.com>
<https://a.dynatrace.com>
<https://api.devops-services.dynatrace.com>
<https://account.dynatrace.com>
<https://arm.cxapps.dynatrace.com>
<https://ace-tools.dynatrace.com>
<https://artemis-search.spine.internal.dynatrace.com>
<https://artemis-api.spine.internal.dynatrace.com>
<https://artemis-support.spine.internal.dynatrace.com>
<https://artemis.spine.internal.dynatrace.com>
<https://assets.dynatrace.com>
<https://assets.cloud.dynatrace.com>
<https://attachments.one.dynatrace.com>
<https://aws.cloud.dynatrace.com>
<https://api.careers.dynatrace.com>
<https://awarenesstraining.dynatrace.com>
<https://barista.dynatrace.com>
<https://apply.careers.dynatrace.com>
<https://benchmarks.dynatrace.com>
<https://auto-response-manager.cxapps.dynatrace.com>
<https://bf00539hsb.bf.dynatrace.com>
<https://bf01006zdw.bf.dynatrace.com>
<https://bf01632wee.bf.dynatrace.com>
<https://bf00533cik.bf.dynatrace.com>
<https://bf01010lrr.bf.dynatrace.com>
<https://bf01739bkip.bf.dynatrace.com>
<https://bf01002bli.bf.dynatrace.com>
<https://bf02779stq.bf.dynatrace.com>
<https://bf02606zwy.bf.dynatrace.com>
<https://bf01868vpr.bf.dynatrace.com>
<https://bf02182chf.bf.dynatrace.com>
<https://bf02275nvn.bf.dynatrace.com>
<https://bf03334wlw.bf.dynatrace.com>
<https://bf03331hna.bf.dynatrace.com>
<https://bf02454vkj.bf.dynatrace.com>
<https://au.step.dynatrace.com>
<https://bf03069gjb.bf.dynatrace.com>
<https://bf03260rex.bf.dynatrace.com>
<https://bf03979hmm.bf.dynatrace.com>
<https://bf04011nr.bf.dynatrace.com>
<https://bf03584esi.bf.dynatrace.com>
<https://bf04658cjb.bf.dynatrace.com>
<https://bf04098hbb.bf.dynatrace.com>

c. IP Discovery

Tool: nslookup: [nslookup_result.txt](#)

Code: since we have a file with subdomains, to find IP addresses using “nslookup” we need to make a loop until all the IPs of all the subdomains are found.

```
while read sub; do
    echo "Looking up: $sub" >> nslookup_result.txt
    nslookup "$sub" | awk '/^Name:|^Address:/' >> nslookup_result.txt
    echo "-----" >> nslookup_result.txt
done < livesub_results.txt
```

Explanation:

While read sub; do - start of the loop

Echo “Looking up: \$sub”>>ips.txt - print message “Looking up: subdomain” into the file “ips.txt”

nslookup “\$sub” | awk ‘/^Name:|^Address:/' >> ips.txt - run the nslookup command

echo “-----” >> ips.txt - separate one subdomain details from another

done < livesub_results.txt - End the loop and continue until the lines in the livesub_results.txt

```
(kali@kali)-[~/Desktop/dynatrace]
$ ./nslookup_script.sh
(kali@kali)-[~/Desktop/dynatrace]
$ cat nslookup_result.txt
Looking up: https://api.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.insights.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://ajax.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.myaccount.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.sso-beta.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://answers.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://access-approval.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://apmblog.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.sso.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://amplify.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.ace-tools.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://applicationperformance.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://apmu.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.university.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://api.mobileagent.downloads.dynatrace.com
Address: 192.168.0.1#53

Looking up: https://admin.myaccount.dynatrace.com
Address: 192.168.0.1#53
```

IP list:

Looking up: <https://api.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.insights.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://ajax.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.myaccount.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.sso-beta.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://answers.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://access-approval.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://apmblog.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.sso.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://amplify.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.ace-tools.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://applicationperformance.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://apmu.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.university.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://api.mobileagent.downloads.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://admin.myaccount.dynatrace.com>

Address: 192.168.0.1#53

Looking up: <https://a.dynatrace.com>

Address: 192.168.0.1#53

d. Open Ports

Tool: nmap: [nmap_result.txt](#)

Code: nmap -sV -A -v -O dynatrace.com -oN nmap_results.txt

Explanation:

- nmap - start the tool
- sV - Service and version detection
- A - OS detection, version detection, script scanning
- v - increase verbosity level
- O - Os detection
- dynatrace.com - target website
- oN nmap_results.txt - result in an output text file

```
(kali㉿kali)-[~/Desktop/dynatrace]
$ nmap -sV -A -v -O dynatrace.com -oN nmap_result.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-27 16:53 +0530
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:53
Completed NSE at 16:53, 0.00s elapsed
Initiating NSE at 16:53
Completed NSE at 16:53, 0.00s elapsed
Initiating NSE at 16:53
Completed NSE at 16:53, 0.00s elapsed
Initiating Ping Scan at 16:53
Scanning dynatrace.com (13.215.198.151) [4 ports]
Completed Ping Scan at 16:53, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:53
Completed Parallel DNS resolution of 1 host. at 16:53, 0.10s elapsed
Initiating SYN Stealth Scan at 16:53
Scanning dynatrace.com (13.215.198.151) [1000 ports]
Discovered open port 443/tcp on 13.215.198.151
Discovered open port 25/tcp on 13.215.198.151
Discovered open port 80/tcp on 13.215.198.151
Completed SYN Stealth Scan at 16:53, 5.88s elapsed (1000 total ports)
Initiating Service scan at 16:53
Scanning 3 services on dynatrace.com (13.215.198.151)
Completed Service scan at 16:53, 5.01s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against dynatrace.com (13.215.198.151)
Retrying OS detection (try #2) against dynatrace.com (13.215.198.151)
Initiating Traceroute at 16:53
Completed Traceroute at 16:53, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 16:53
Completed Parallel DNS resolution of 1 host. at 16:53, 0.06s elapsed
NSE: Script scanning 13.215.198.151.
Initiating NSE at 16:53
Completed NSE at 16:54, 18.57s elapsed
Initiating NSE at 16:54
Completed NSE at 16:54, 32.70s elapsed
Initiating NSE at 16:54
Completed NSE at 16:54, 0.01s elapsed
Nmap scan report for dynatrace.com (13.215.198.151)
Host is up (0.0088s latency).
Other addresses for dynatrace.com (not scanned): 18.138.187.28
rDNS record for 13.215.198.151: ec2-13-215-198-151.ap-southeast-1.compute.amazonaws.com
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
25/tcp    open  tcpwrapped
|_smtp-commands: SMTP EHLO dynatrace.com: failed to receive data: connection closed
80/tcp    open  tcpwrapped
443/tcp   open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: AT&T BGW210 voice gateway (95%), Oracle Virtualbox Slirp NAT bridge (93%), QEMU user mode net
work gateway (92%), ZyXEL Prestige 2602R-D1A ADSL router (ZyNOS 3.40) (92%), Allied Telesyn AT-AR410 router (90%), G
NU Hurd 0.3 (89%), Cisco 1812, 3640, or 3700 router (IOS 12.4) (89%), Cisco Catalyst 3560 or 6500-series switch (IOS
12.1 - 12.2) (89%), Kodak ESP C310 printer (88%), Kodak ESP 5210 printer (88%),
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

e. Used Technologies

Tool: whatweb - [whatweb results.txt](#)

Code: whatweb -v dynatrace.com > whatweb_result.txt

Explanation:

whatweb - start whatweb tool

-v - verbose

dynatrace.com - target website

> *whatweb_result.txt* - file with the output

```
(kali@kali)~[~/Desktop/dynatrace]
$ whatweb -v dynatrace.com --o whatweb_results.txt
WhatWeb report for http://dynatrace.com
Status      : 301 Moved Permanently
Title       : 301 Moved Permanently
IP          : 18.138.187.28
Country     : UNITED STATES, US

Summary     : HTTPServer[nginx], nginx, RedirectLocation[https://www.dynatrace.com/]

Detected Plugins:
[ HTTPServer ]
  HTTP server header string. This plugin also attempts to
  identify the operating system from the server header.

  String      : nginx (from server string)

[ RedirectLocation ]
  HTTP Server string location. used with http-status 301 and
  302

  String      : https://www.dynatrace.com/ (from location)

[ nginx ]
  Nginx (Engine-X) is a free, open-source, high-performance
  HTTP server and reverse proxy, as well as an IMAP/POP3
  proxy server.

  Website     : http://nginx.net/

HTTP Headers:
  HTTP/1.1 301 Moved Permanently
  Content-Type: text/html
  Date: Sun, 27 Apr 2025 11:21:24 GMT
  Location: https://www.dynatrace.com/
  Server: nginx
  Content-Length: 162
  Connection: Close

WhatWeb report for https://www.dynatrace.com/
Status      : 200 OK
Title       : Dynatrace | Understand your business like never before
IP          : 108.159.61.115
Country     : UNITED STATES, US

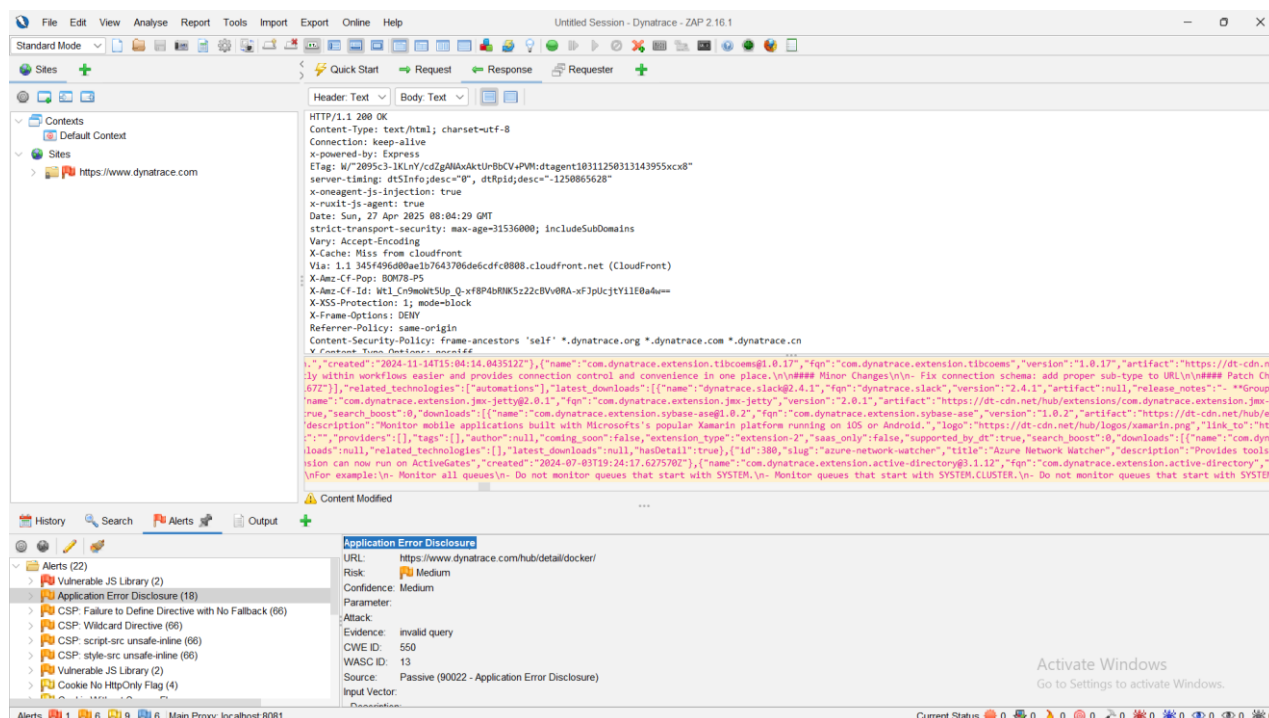
Summary     : Email[sales@dynatrace.com], Frame, HTML5, HTTPServer[AmazonS3], Open-Graph-Protocol[1221150274658460],
PoweredBy[groundbreaking], Script[application/ld+json,module,speculationrules,text/plain], Strict-Transport-Securit
y[max-age=31536000; includeSubDomains], UncommonHeaders[x-amz-server-side-encryption,x-amz-version-id,x-amz-cf-pop,
x-amz-cf-id,referrer-policy,content-security-policy,x-content-type-options], Via-Proxy[1.1 853b5be3b78b835fb7185ce9
```


3. Step 02: Scanning and vulnerability identification

a. Identify Potential Vulnerabilities

Tool : OWASP ZAP

Vulnerability : Application Error Disclosure



Application Error Disclosure:

URL: <https://www.dynatrace.com/hub/detail/docker/>

Risk: Medium

Confidential: Medium

Parameter:

Attack:

Evidence: invalid query

CWE ID: 550

WASC ID: 13

Source: Passive (90022 - Application Error Disclosure)

Input Vector:

- Description: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.
- Other Info:
- Solution: Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.
- Reference: <https://openwall.info/wiki/john/sample-hashes>
- Alert Tags:
 - WSTG-v42-ERRH-02: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/02-Testing_for_Stack_Traces
 - WSTG-v42-ERRH-01: https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/08-Testing_for_Error_Handling/01-Testing_For_Improper_Error_Handling
 - OWASP_2021_A05: https://owasp.org/Top10/A05_2021-Security_Misconfiguration/
 - CWE-550: <https://cwe.mitre.org/data/definitions/550.html>
 - OWASP_2017_A06: https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration.html

b. Application Error Disclosure

Application Error Disclosure occurs when a web application displays detailed error messages to users, revealing sensitive information such as server paths, database details, software versions, or even stack traces. These disclosures can give attackers valuable insight into the internal workings of the system, helping them craft targeted attacks like SQL injection, command injection, or remote code execution.

Cause of Application Error Disclosure in website:

- Displaying verbose error messages directly to users in production environments
- Lack of proper error handling or exception management
- Misconfigured servers or frameworks that expose detailed debugging information
- Not sanitizing error outputs that include internal variables or code snippets
- Enabling detailed error reporting settings (like `display_errors` in PHP) in production
- Trusting third-party libraries that might expose errors without proper wrapping

Propositions to Mitigation or Fix:

- Display Generic Error Messages: Always show users a simple, non-technical error message like "An unexpected error occurred."
- Log Detailed Errors Internally: Send full stack traces and debugging information to secure server-side logs only
- Configure Servers for Production: Disable verbose error reporting and debug modes in production environments
- Implement Centralized Error Handling: Use global exception handlers that sanitize and control all error outputs
- Perform Regular Code Reviews: Check for unhandled exceptions or debug outputs before deploying code
- Audit Third-party Libraries: Ensure that external components and frameworks do not leak sensitive errors
- Conduct Security Testing: Perform vulnerability assessments to check for accidental error disclosures

```
GET https://www.dynatrace.com/hub/detail/docker/ HTTP/1.1
host: www.dynatrace.com
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
referer: https://www.dynatrace.com/solutions/application-monitoring/
Cookie: dtCookie=v 4 srv 4 sn CF337F750353286DD817F6E6FFADCCF perc 100000 ol 0 mul 1 app-3A4a0edc0481e5e72 1 app-3A366f9fc79607e4b1 1 rcs-3Accs 0
```

```

HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
Connection: keep-alive
x-powered-by: Express
ETag: W/"2095c3-1KlnY/cdZgANAxAktUrbBcV+PVM:dtagent10311250313143955cxc8"
server-timing: dtSinfo;desc="0", dtRpid;desc="-1250865628"
x-oneagent-js-injection: true
x-puxit-js-agent: true
Date: Sun, 27 Apr 2025 08:04:29 GMT
strict-transport-security: max-age=31536000; includeSubDomains
Vary: Accept-Encoding
X-Cache: Miss from cloudfront
Via: 1.1 345f496d0ae1b7643706de6cdfc0888.cloudfront.net (CloudFront)
X-Amz-Cf-Pop: BOM78-P5
X-Amz-Cf-Id: Wt1_Cn9moWt5Up_Q-xF8P4bRHK5z22cBVv0RA-xFJpUcjtY1lE0a4w==
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
Referrer-Policy: same-origin
Content-Security-Policy: frame-ancestors 'self' *.dynatrace.org *.dynatrace.com *.dynatrace.cn
X-Content-Type-Options: nosniff
Vary: Origin
content-length: 2136438
{"name":"com.dynatrace.extension.tibcoems@1.0.17","fqn":"com.dynatrace.extension.tibcoems","version":"1.0.17","artifact":"https://dt-cdn.net/hub/workflows easier and provides connection control and convenience in one place.\n\nMinor Changes\n\n- Fix connection schema: add proper sub-type to URL\n\nPatch Ch 672"],"related_technologies":[{"name":"dynatrace.slack@2.4.1","fqn":"dynatrace.slack","version":"2.4.1","artifact":null,"release_notes":"- * Group name":"com.dynatrace.extension.jmx-jetty@2.0.1","fqn":"com.dynatrace.extension.jmx-jetty","version":"2.0.1","artifact":"https://dt-cdn.net/hub/extensions/com.dynatrace.extension.jmx-jetty","search_boost":0,"downloads":[{"name":"com.dynatrace.extension.sybase-ase@1.0.2","fqn":"com.dynatrace.extension.sybase-ase","version":"1.0.2","artifact":"https://dt-cdn.net/hub/e description":"Monitor mobile applications built with Microsoft's popular Xamarin platform running on iOS or Android.","logo":"https://dt-cdn.net/hub/logos/xamarin.png","link_to":"ht :","providers":[{"tags":[""],"author":null,"coming_soon":false,"extension_type":"extension-2","saas_only":false,"supported_by_dt":true,"search_boost":0,"downloads":[{"name":"com.dyn loads":null,"related_technologies":[{"latest_downloads":null,"hasDetail":true},"id":380,"slug":"azure-network-watcher","title":"Azure Network Watcher","description":"Provides tools ison can run on ActiveGate","created":"2024-07-03T19:24:17.627570Z"},"name":"com.dynatrace.extension.active-directory@3.1.12","fqn":"com.dynatrace.extension.active-directory"," nFor example:\n- Monitor all queues\n- Do not monitor queues that start with SYSTEM.\n- Monitor queues that start with SYSTEM.CLUSTER.\n- Do not monitor queues that start with SYSTEM hours\n\n- 5a61660: Adjust process data query to fetch the latest CPU and memory values correctly\n\n- f6377b4: Remove chart group tab from network device preview\n\n- 38a40ce: Fix 1 count\n\n- 1.7.0\n\nMinor Changes\n\n- 67cc591: Use the availability state to check if a process is active\n\n- 546e5c7: Introduce an important property in the header and a char osoft365.connector@1.5.0","fqn":"dynatrace.microsoft365.connector","version":"1.5.0","artifact":null,"release_notes":"- Removed message truncation after 5000 characters","created":"2 p.shortlink/linux-hub","providers":[{"tags":["cloud","infrastructure","linux","server-monitoring"],"author":null,"coming_soon":false,"extension_type":null,"saas_only":false,"sup filtering monitoring entities","created":"2024-02-26T11:42:12.971559Z"},"name":"com.dynatrace.extension.hyperv@2.0.10","fqn":"com.dynatrace.extension.hyperv","version":"2.0.10","sa "eol","file monitoring","folder monitoring","governance","job monitoring","port scan","reporting","SSL certification monitoring","topology","vulnerabilities"],"author":"11","coming s :["aks","azure kubernetes service","cloud","container","serverless"],"author":null,"coming_soon":false,"extension_type":null,"saas_only":false,"supported_by_dt":true,"search_boost"}]}

```

5. Step 04: Mitigation / Fix

Immediate Mitigation Actions:

1. Replace raw errors with generic messages.
2. Disable debug mode in production.
3. Configure web servers to show user-friendly pages.

Long Term Prevention:

1. Static analysis using SonarQube/GitHub CodeQL to detect debug mode in code.
2. Use security headers to block MIME-based leaks