Sri Lanka Institute of Information Technology

Assignment report 05

IT22357762

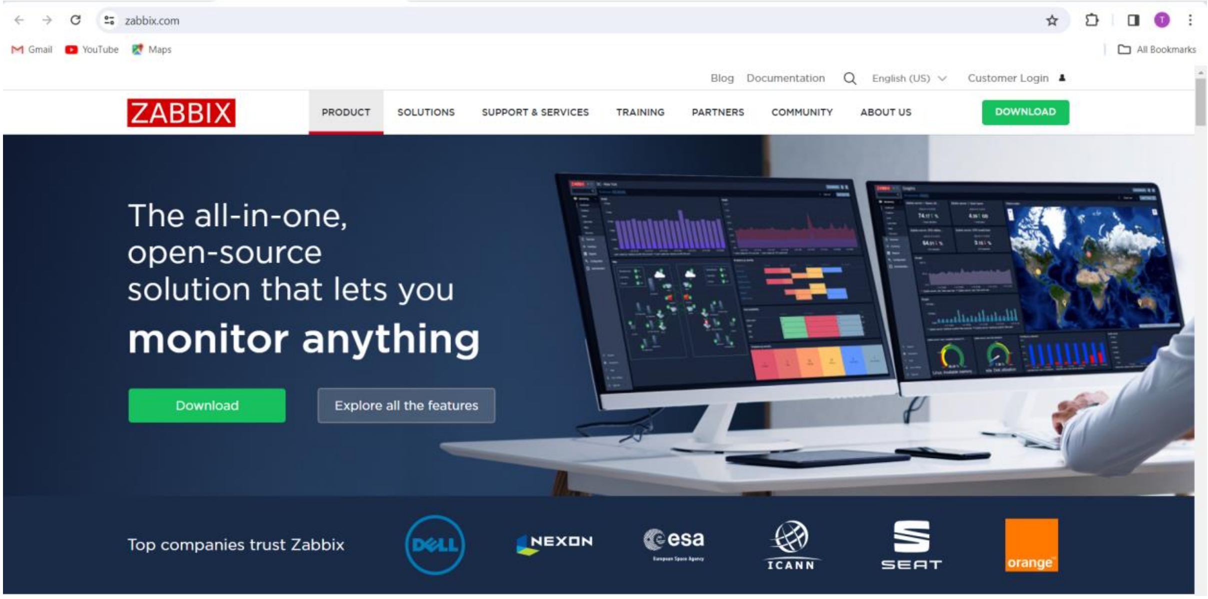
Web Security -IE2062

Web Security – IE2062

B.Sc. (Hons) in Information

Contents

1 Zabbix.com



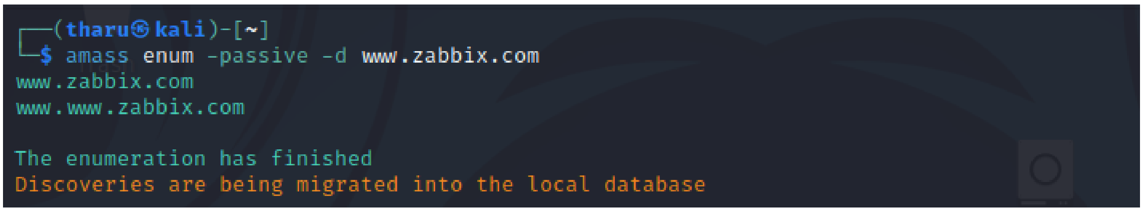
The all-in-one, open-source solution that lets you monitor anything

Top companies trust Zabbix

1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d zabbix.com



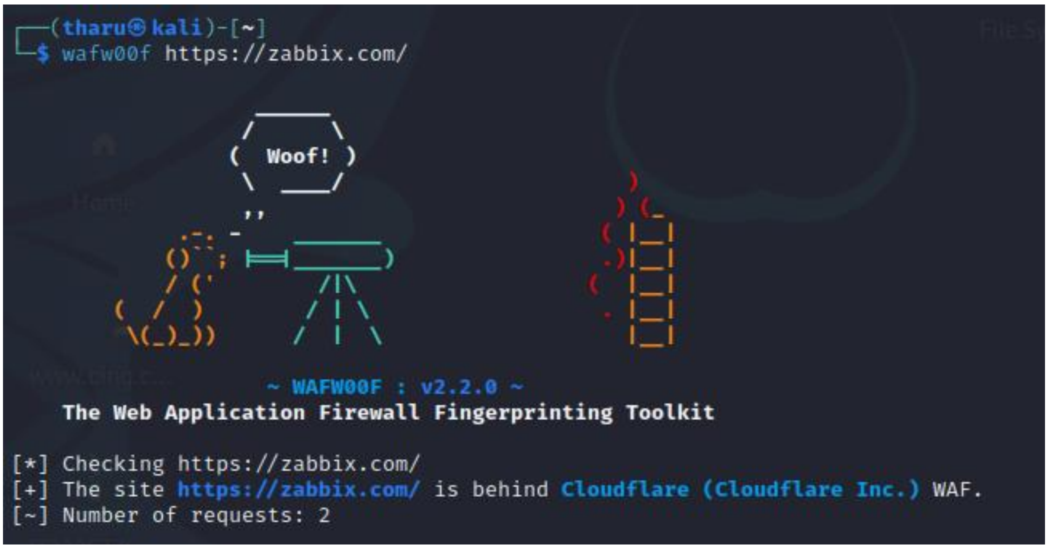
```
┌──(tharu㉿kali)-[~]
└─$ amass enum -passive -d www.zabbix.com
www.zabbix.com
www.www.zabbix.com

The enumeration has finished
Discoveries are being migrated into the local database
```

Sub domain list –

- www.zabbix.com
- www.www.zabbix.com

1.2 Firewall detection

Command – wafw00f https://zabbix.com /

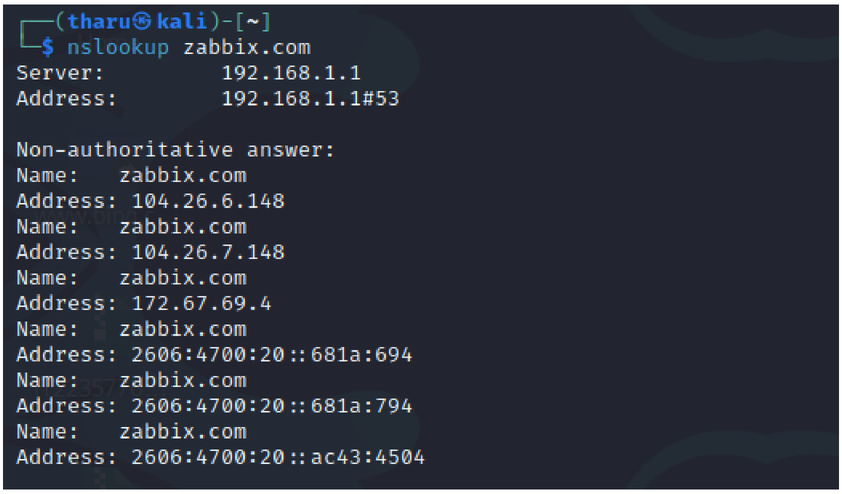


```
┌──(tharu㉿kali)-[~]
└─$ wafw00f https://zabbix.com/

                ~ WAFW00F : v2.2.0 ~
    The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://zabbix.com/
[+] The site https://zabbix.com/ is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

1.3 IP scanning

Tool – nslookup

Command – nslookup zabbix.com

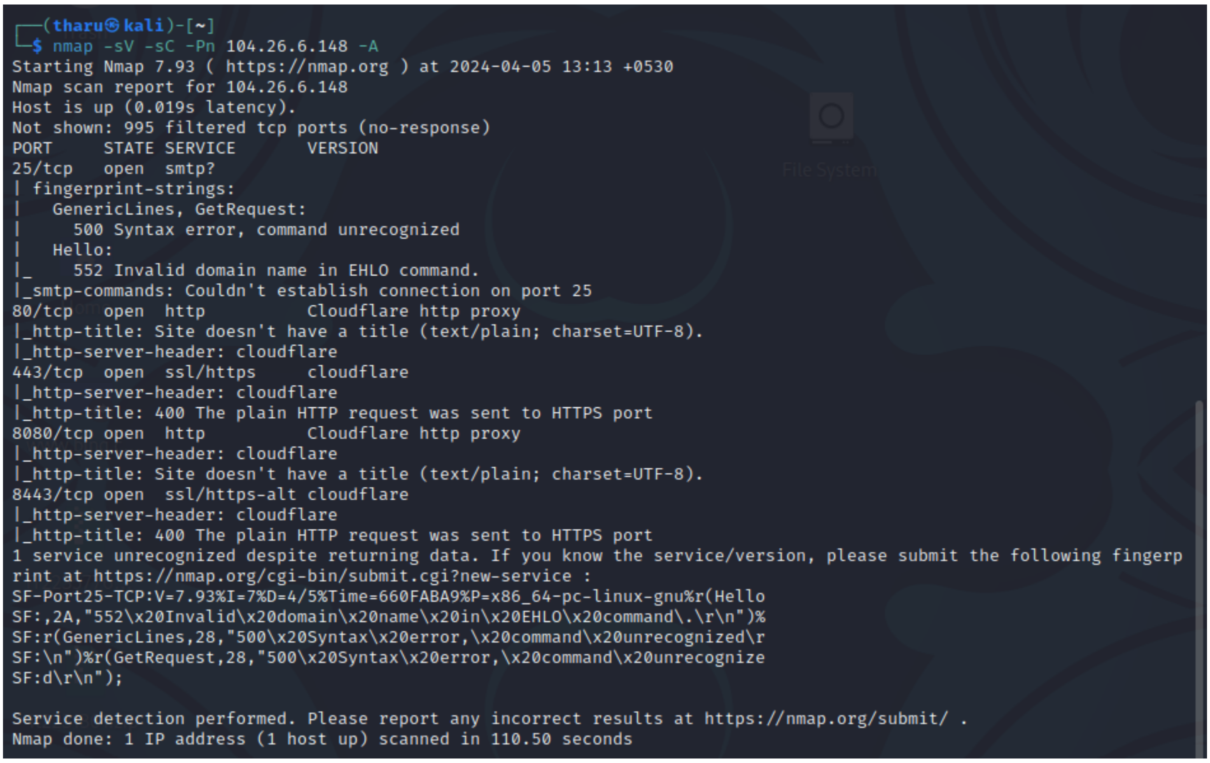


```
┌──(tharu㉿kali)-[~]
└─$ nslookup zabbix.com
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
Name:   zabbix.com
Address: 104.26.6.148
Name:   zabbix.com
Address: 104.26.7.148
Name:   zabbix.com
Address: 172.67.69.4
Name:   zabbix.com
Address: 2606:4700:20::681a:694
Name:   zabbix.com
Address: 2606:4700:20::681a:794
Name:   zabbix.com
Address: 2606:4700:20::ac43:4504
```

1.4 Port scanning

Tool - nmap

Command – nmap -sV -sC -Pn 104.26.6.148 -A

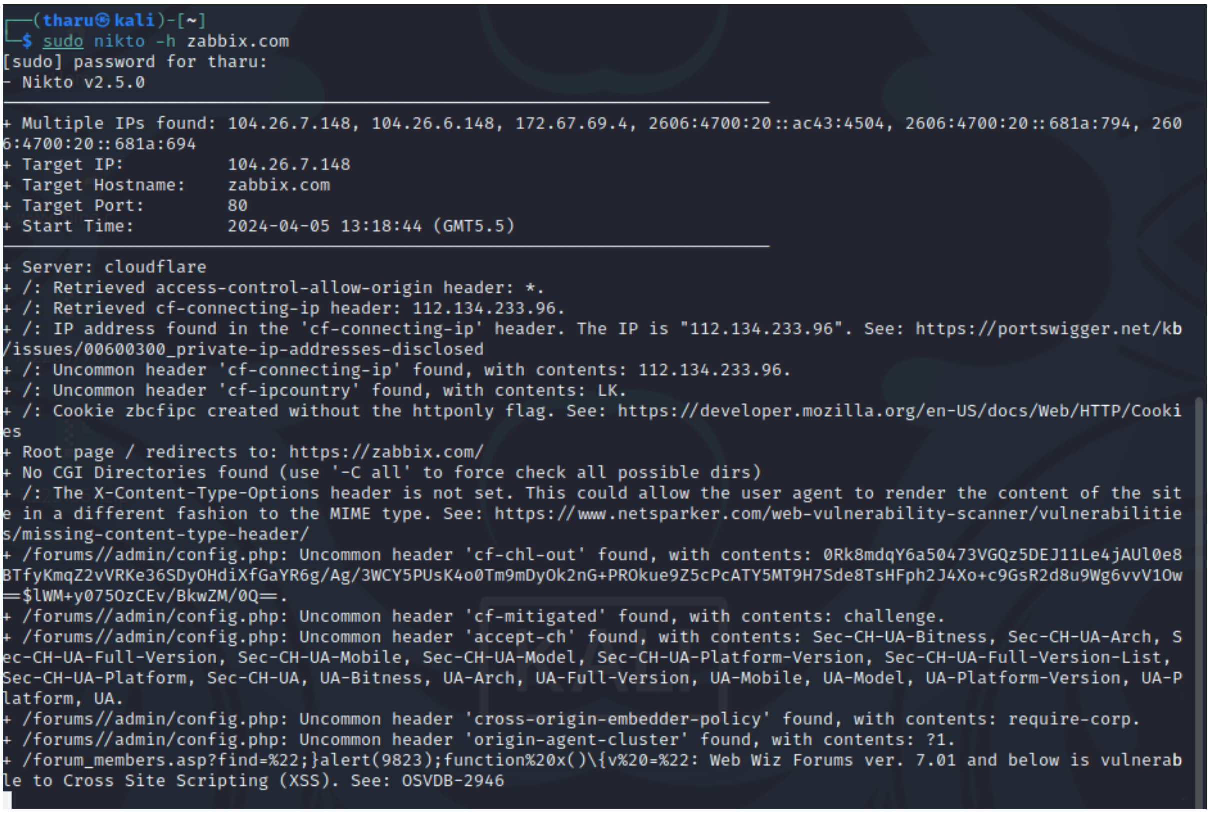


```
┌──(tharu㉿kali)-[~]
└─$ nmap -sV -sC -Pn 104.26.6.148 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-05 13:13 +0530
Nmap scan report for 104.26.6.148
Host is up (0.019s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp?
| fingerprint-strings:
|   GenericLines, GetRequest:
|     500 Syntax error, command unrecognized
|   Hello:
|_    552 Invalid domain name in EHLO command.
|_smtp-commands: Couldn't establish connection on port 25
80/tcp   open  http          Cloudflare http proxy
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http-server-header: cloudflare
443/tcp  open  ssl/https     cloudflare
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
8080/tcp open  http          Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
8443/tcp open  ssl/https-alt cloudflare
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerp
rint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port25-TCP:V=7.93%I=7%D=4/5%Time=660FABA9%P=x86_64-pc-linux-gnu%r(Hello
SF:,2A,"552\x20Invalid\x20domain\x20name\x20in\x20EHLO\x20command\.\r\n")%
SF:r(GenericLines,28,"500\x20Syntax\x20error,\x20command\x20unrecognized\r
SF:\n")%r(GetRequest,28,"500\x20Syntax\x20error,\x20command\x20unrecognize
SF:d\r\n");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.50 seconds
```

1.5 Nikto scanning

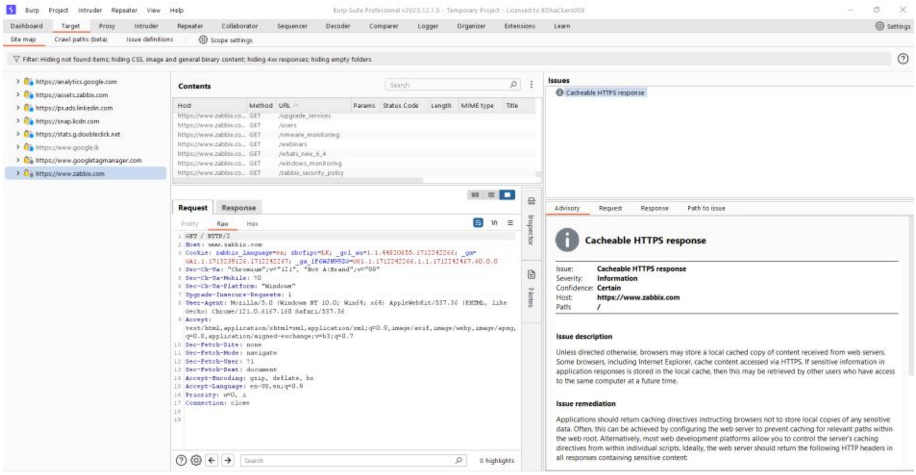
Tool – Nikto

Command - sudo nikto -h zabbix.com



```
┌──(tharu㉿kali)-[~]
└─$ sudo nikto -h zabbix.com
[sudo] password for tharu:
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 104.26.7.148, 104.26.6.148, 172.67.69.4, 2606:4700:20::ac43:4504, 2606:4700:20::681a:794, 260
6:4700:20::681a:694
+ Target IP:          104.26.7.148
+ Target Hostname:    zabbix.com
+ Target Port:        80
+ Start Time:         2024-04-05 13:18:44 (GMT5.5)
---------------------------------------------------------------------------
+ Server: cloudflare
+ /: Retrieved access-control-allow-origin header: *.
+ /: Retrieved cf-connecting-ip header: 112.134.233.96.
+ /: IP address found in the 'cf-connecting-ip' header. The IP is "112.134.233.96". See: https://portswigger.net/kb
/issues/00600300_private-ip-addresses-disclosed
+ /: Uncommon header 'cf-connecting-ip' found, with contents: 112.134.233.96.
+ /: Uncommon header 'cf-ipcountry' found, with contents: LK.
+ /: Cookie zbcfipc created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cooki
es
+ Root page / redirects to: https://zabbix.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the sit
e in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilitie
s/missing-content-type-header/
+ /forums//admin/config.php: Uncommon header 'cf-chl-out' found, with contents: 0Rk8mdqY6a50473VGQz5DEJ11Le4jAUl0e8
BTfyKmqZ2vVRKe36SDyOHdiXfGaYR6g/Ag/3WCY5PUsK4o0Tm9mDyOk2nG+PROkue9Z5cPcATY5MT9H7Sde8TsHFph2J4Xo+c9GsR2d8u9Wg6vvV1Ow
==$lWM+y075OzCEv/BkwZM/0Q==.
+ /forums//admin/config.php: Uncommon header 'cf-mitigated' found, with contents: challenge.
+ /forums//admin/config.php: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Bitness, Sec-CH-UA-Arch, S
ec-CH-UA-Full-Version, Sec-CH-UA-Mobile, Sec-CH-UA-Model, Sec-CH-UA-Platform-Version, Sec-CH-UA-Full-Version-List,
Sec-CH-UA-Platform, Sec-CH-UA, UA-Bitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-P
latform, UA.
+ /forums//admin/config.php: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
+ /forums//admin/config.php: Uncommon header 'origin-agent-cluster' found, with contents: ?1.
+ /forum_members.asp?find=%22;}alert(9823);function%20x()\{v%20=%22: Web Wiz Forums ver. 7.01 and below is vulnerab
le to Cross Site Scripting (XSS). See: OSVDB-2946
```

1.6 Burpsuite scanning



Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

- https://analytics.google.com
- https://assets.zabbix.com
- https://px.ads.linkedin.com
- https://snap.licdn.com
- https://stats.g.doubleclick.net
- https://www.google.lk
- https://www.googletagmanager.com
- https://www.zabbix.com

Host	Method	URL	Params	Status Code	Length	MIME type	Title
https://www.zabbix.co...	GET	/upgrade_services					
https://www.zabbix.co...	GET	/users					
https://www.zabbix.co...	GET	/vmware_monitoring					
https://www.zabbix.co...	GET	/webinars					
https://www.zabbix.co...	GET	/whats_new_6_4					
https://www.zabbix.co...	GET	/windows_monitoring					
https://www.zabbix.co...	GET	/zabbix_security_policy					

```
GET / HTTP/2
Host: www.zabbix.com
Cookie: zabbix_language=en; zbcfipc=LK; _gcl_au=1.1.44820655.1712242266; _ga=
GA1.1.1713239126.1712242267; _ga_1P6WJN99ZG=GS1.1.1712242266.1.1.1712242467.60.0.0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,
q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close


```

Issues

- Cacheable HTTPS response

Cacheable HTTPS response

Issue: **Cacheable HTTPS response**
Severity: **Information**
Confidence: **Certain**
Host: **https://www.zabbix.com**
Path: **/**

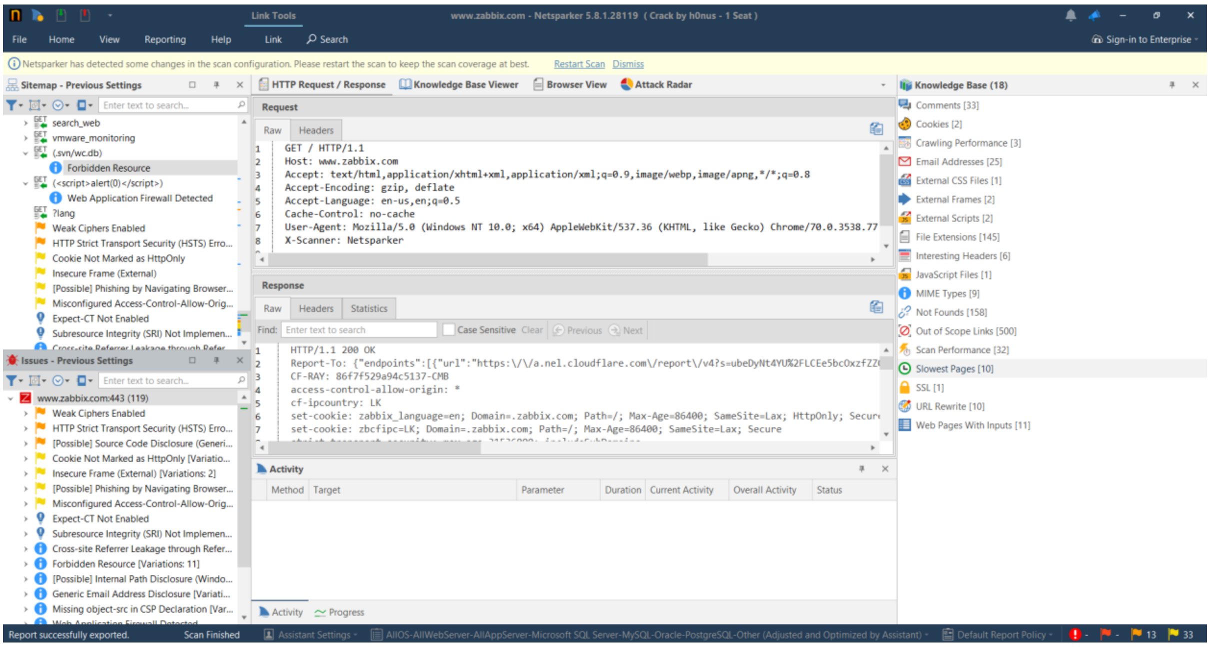
Issue description

Unless directed otherwise, browsers may store a local cached copy of content received from web servers. Some browsers, including Internet Explorer, cache content accessed via HTTPS. If sensitive information in application responses is stored in the local cache, then this may be retrieved by other users who have access to the same computer at a future time.

Issue remediation

Applications should return caching directives instructing browsers not to store local copies of any sensitive data. Often, this can be achieved by configuring the web server to prevent caching for relevant paths within the web root. Alternatively, most web development platforms allow you to control the server's caching directives from within individual scripts. Ideally, the web server should return the following HTTP headers in all responses containing sensitive content:

1.7 Netspaker scan



Link Tools
www.zabbix.com - Netsparker 5.8.1.28119 (Crack by h0nus - 1 Seat)
File
Home
View
Reporting
Help
Link
Search
Sign-in to Enterprise
Netsparker has detected some changes in the scan configuration. Please restart the scan to keep the scan coverage at best.
Restart Scan
Dismiss
Sitemap - Previous Settings
Enter text to search...
search_web
vmware_monitoring
(.svn/wc.db)
Forbidden Resource
(<script>alert(0)</script>)
Web Application Firewall Detected
?lang
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) Erro...
Cookie Not Marked as HttpOnly
Insecure Frame (External)
[Possible] Phishing by Navigating Browser...
Misconfigured Access-Control-Allow-Orig...
Expect-CT Not Enabled
Subresource Integrity (SRI) Not Implemen...
Issues - Previous Settings
Enter text to search...
www.zabbix.com:443 (119)
Weak Ciphers Enabled
HTTP Strict Transport Security (HSTS) Erro...
[Possible] Source Code Disclosure (Generi...
Cookie Not Marked as HttpOnly [Variatio...
Insecure Frame (External) [Variations: 2]
[Possible] Phishing by Navigating Browser...
Misconfigured Access-Control-Allow-Orig...
Expect-CT Not Enabled
Subresource Integrity (SRI) Not Implemen...
Cross-site Referrer Leakage through Refer...
Forbidden Resource [Variations: 11]
[Possible] Internal Path Disclosure (Windo...
Generic Email Address Disclosure [Variati...
Missing object-src in CSP Declaration [Var...
HTTP Request / Response
Knowledge Base Viewer
Browser View
Attack Radar
Request
Raw
Headers
Response
Raw
Headers
Statistics
Find:
Enter text to search
Case Sensitive
Clear
Previous
Next
Activity
Method
Target
Parameter
Duration
Current Activity
Overall Activity
Status
Activity
Progress
Knowledge Base (18)
Comments [33]
Cookies [2]
Crawling Performance [3]
Email Addresses [25]
External CSS Files [1]
External Frames [2]
External Scripts [2]
File Extensions [145]
Interesting Headers [6]
JavaScript Files [1]
MIME Types [9]
Not Founds [158]
Out of Scope Links [500]
Scan Performance [32]
Slowest Pages [10]
SSL [1]
URL Rewrite [10]
Web Pages With Inputs [11]
Report successfully exported.
Scan Finished
Assistant Settings
AllOS-AllWebServer-AllAppServer-Microsoft SQL Server-MySQL-Oracle-PostgreSQL-Other (Adjusted and Optimized by Assistant)
Default Report Policy
13
33

```
GET / HTTP/1.1
Host: www.zabbix.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.77
X-Scanner: Netsparker
```

```
HTTP/1.1 200 OK
Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=ubeDyNt4YU%2FLCEe5bcOxzfZZ
CF-RAY: 86f7f529a94c5137-CMB
access-control-allow-origin: *
cf-ipcountry: LK
set-cookie: zabbix_language=en; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; HttpOnly; Secure
set-cookie: zbcfipc=LK; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; Secure
```

1.8 Vulnerabilities

Vulnerability Title: Missing preload directive in HTTP Strict Transport Security (HSTS) configuration.

Vulnerability Description: Enabling the preload directive in the HTTP Strict Transport Security (HSTS) configuration allows browsers to automatically preload the site's HSTS policy. Without this directive, the browser might not properly enforce HSTS on the site, which could potentially expose it to downgrade attacks or other security risks.

Affected Components: https://zabbix.com/

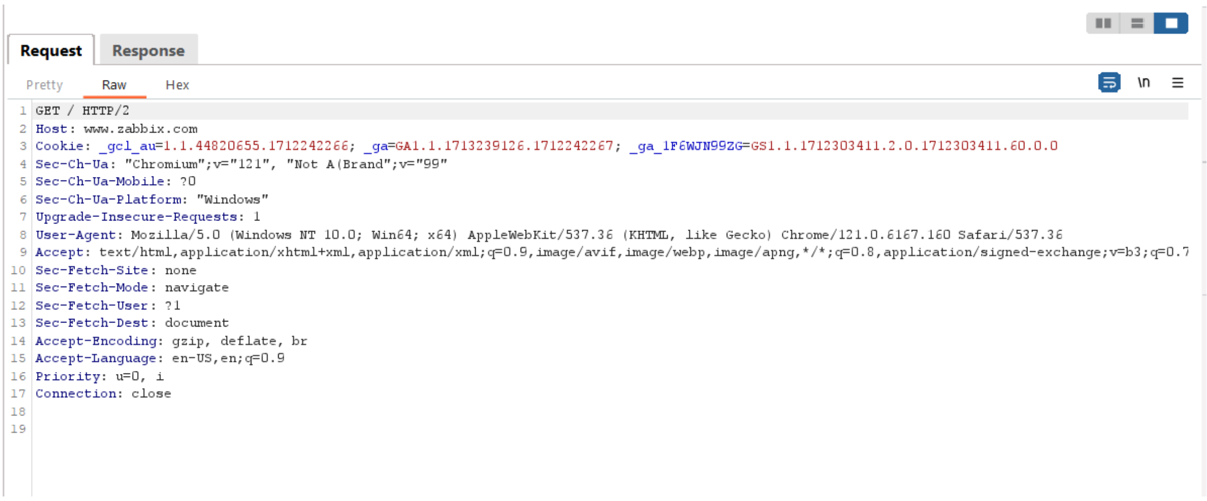
Impact Assessment: Impact of vulnerability includes,

- Increased Risk of SSL/TLS Downgrade Attacks
- Exposure to Man-in-the-Middle Attacks
- Potential Legal and Financial Consequences

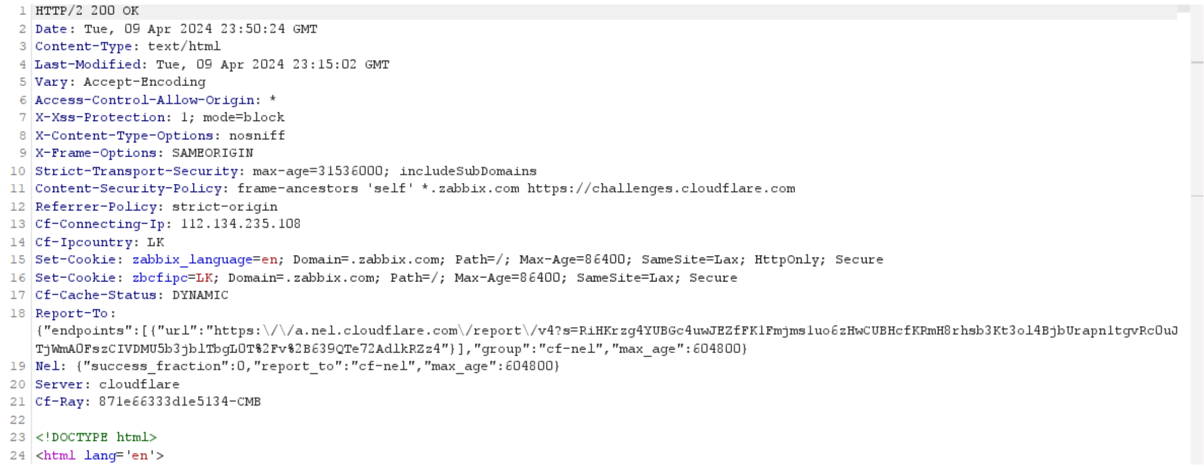
Steps to Reproduce:

1. Inspect the website's HSTS header or configuration.
2. Look for the absence of the preload directive.

Proof of concept:



```
GET / HTTP/2
Host: www.zabbix.com
Cookie: _gcl_au=1.1.44820655.1712242266; _ga=GA1.1.1713239126.1712242267; _ga_1F6WJN99ZG=GS1.1.1712303411.2.0.1712303411.60.0.0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.160 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close


```



```
HTTP/2 200 OK
Date: Tue, 09 Apr 2024 23:50:24 GMT
Content-Type: text/html
Last-Modified: Tue, 09 Apr 2024 23:15:02 GMT
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
X-Xss-Protection: 1; mode=block
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: frame-ancestors 'self' *.zabbix.com https://challenges.cloudflare.com
Referrer-Policy: strict-origin
Cf-Connecting-Ip: 112.134.235.108
Cf-Ipcountry: LK
Set-Cookie: zabbix_language=en; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; HttpOnly; Secure
Set-Cookie: zbcfipc=LK; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; Secure
Cf-Cache-Status: DYNAMIC
Report-To:
{"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v4?s=RiHKrzg4YUBGc4uwJEZfFK1Fmjms1uo6zHwCUBHcfKRmH8rhsb3Kt3o14BjbUrapn1tgvRc0uJ
TjWmA0FszCIVDMU5b3jb1TbgL0T%2Fv%2B639QTe72Ad1kRZz4"}],"group":"cf-nel","max_age":604800}
Nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
Server: cloudflare
Cf-Ray: 871e66333d1e5134-CMB

<!DOCTYPE html>
<html lang='en'>
```

Proposed Mitigation or Fix: Include the domain in the HSTS preload list

1.8.1 Other vulnerabilities

1. Weak Ciphers Enabled.
2. Cookie Not Marked as HttpOnly.
3. Misconfigured Access-Control-Allow-Origin Header.
4. Expect-CT Not Enabled.