

Sri Lanka Institute of Information Technology



Assignment report 03

IT22357762

Web Security -IE2062

**Web Security – IE2062**

B.Sc. (Hons) in Information

## **Contents**

1	Zabbiz.com .....	3
1.1	Sub- domain list .....	3
1.2	Firewall detection .....	4
1.3	IP scanning .....	5
1.4	Port scanning .....	5
1.5	Nikto scanning .....	6
1.6	SSL scan.....	6
1.7	Burpsuite scanning .....	7
1.8	Netspaker scan .....	8
1.9	Vulnerabilities.....	8
1.9.1	Other vulnerabilities.....	10

# 1 Zabbiz.com

Zabbix is a leading IT monitoring solution company, and its goal is to give businesses the tools they need to make their IT infrastructures work better. They are dedicated to providing a strong, scalable, and adaptable monitoring system, driven by big goals and unwavering determination. Their biggest accomplishment is completely changing tracking technology, giving companies all over the world a powerful tool to make sure their IT operations run smoothly.

## 1.1 Sub- domain list

Tool – amass

Command – amass enum -passive -d zabbix.com

```
(tharu@kali)-[~]
$ amass enum -passive -d zabbix.com
www.zabbix.com
www.www.zabbix.com
assets.zabbix.com
git.zabbix.com
exam.zabbix.com
share.zabbix.com
repo.zabbix.com
support.zabbix.com
zabbix.zabbix.com
zabbix.com
blog.zabbix.com
space.zabbix.com
pms.zabbix.com
cdn.zabbix.com
translate.zabbix.com
www.repo.zabbix.com
www.exam.zabbix.com
www.support.zabbix.com
mail.zabbix.com
www.share.zabbix.com
shop.zabbix.com
link.zabbix.com

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

Sub domain list –


- www.zabbix.com
- www.www.zabbix.com
- assets.zabbix.com
- git.zabbix.com
- exam.zabbix.com
- share.zabbix.com
- repo.zabbix.com
- support.zabbix.com
- zabbix.zabbix.com
- zabbix.com
- blog.zabbix.com

- space.zabbix.com
- pms.zabbix.com
- cdn.zabbix.com
- translate.zabbix.com
- www.repo.zabbix.com
- www.exam.zabbix.com
- www.support.zabbix.com
- mail.zabbix.com
- www.share.zabbix.com
- shop.zabbix.com
- link.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: 172.67.69.4  
Name:   zabbix.com  
Address: 104.26.7.148  
Name:   zabbix.com  
Address: 2606:4700:20::ac43:4504  
Name:   zabbix.com  
Address: 2606:4700:20::681a:794  
Name:   zabbix.com  
Address: 2606:4700:20::681a:694
```

## 1.4 Port scanning

Tool - nmap

Command – `nmap -sV -sC -Pn 192.168.1.1 -A`

```
[~](thorn@kali)-[~]
$ nmap -sV -sC -Pn 192.168.1.1 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-04-04 20:16 +0530
Nmap scan report for 192.168.1.1
Host is up (0.030s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
23/tcp    open  telnet  Huawei Home Gateway telnetd
53/tcp    open  domain  (unknown banner: Version 000)
| dns-nsid:
|_  bind.version: Version 000
|_  fingerprint-strings:
|_    DNSVersionBindReqTCP:
|_      version
|_        bind
|_          Version 000
80/tcp    open  ssl/http
|_  ssl-date: TLS randomness does not represent time
|_  http-title: Site doesn't have a title (text/html).
|_  ssl-cert: Subject: commonName=Huawei Technologies Co., Ltd/stateOrProvinceName=Guangdong/countryName=CN
|_  Not valid before: 2017-09-01T07:57:47
|_  Not valid after: 2027-08-30T07:57:47
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP-V:7.93X1:7904/48time=60EB0538P+x86_64-pc-linux-gnuX(DNSVe
SF:rsionBindReqTCP,46,"00\0x06x85\0x01\0x01\0x01\0x01\0x07version\0
SF:4bind\0x01\0x03\0x0c\0x0c\0x03\0x03\0x0c\0x0c\0x0c\0x0b\0x0bVersion\020000
SF:\xc0\0x0c\0x02\0x03\0x0c\0x02\0x02\0xc0\0xc0");
Service Info: Device: broadband router

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.05 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::681a:794, 2606:4700:20::681a:694, 2606:4700:20::ac43:4504
+ Target IP: 104.26.7.148
+ Target Hostname: zabbix.com
+ Target Port: 80
+ Start Time: 2024-04-04 20:17:47 (GMT+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: UK.
+ /: Cookie abcdefg created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ 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 site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/misusing-content-type-header/
+ /forums/admin/config.php: Uncommon header 'accept-ch' found, with contents: Sec-CH-UA-Bitness, Sec-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-UABitness, UA-Arch, UA-Full-Version, UA-Mobile, UA-Model, UA-Platform-Version, UA-Platform, UA.
+ /forums/admin/config.php: Uncommon header 'origin-agent-cluster' found, with contents: 71.
+ /forums/admin/config.php: Uncommon header 'cf-nitigated' found, with contents: challenge.
+ /forums/admin/config.php: Uncommon header 'cf-chl-out' found, with contents: xLc090xCXlTr5Pph9l10B2zd919q70W0pveqntB357Wrlth8z2B7YxwL8N0zQZ3ox1N0ueqRpmw27u/wFqVpUshhMgZnKCL7Bhfa3MIPftyyA/wu0bF9AKYQCDAFxw910q1/8Ca4C8HmQ==5JMvzXANv0tclMwYb21Q=.
+ /forums/admin/config.php: Uncommon header 'cross-origin-embedder-policy' found, with contents: require-corp.
+ /forum_members.asp?find=322;|alert(9823);function320a();\v420-322: Web Wiz Forums ver. 7.01 and below is vulnerable to Cross Site Scripting (XSS). See: OSVDB-2946
```

## 1.6 SSL scan

Command – sslscan https://www.zabbix.com/

```
(tharu@kali)~$ sslscan https://www.zabbix.com/
Version: 2.1.3-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 104.26.7.148
Testing SSL server www.zabbix.com on port 443 using SNI name www.zabbix.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-ECDSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-GCM-SHA256
Accepted TLSv1.2 128 bits AES128-SHA
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
```

```

Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits AES128-SHA256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits AES256-SHA256

```

#### Server Key Exchange Group(s):

```

TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519

```

#### SSL Certificate:

```

Signature Algorithm: ecdsa-with-SHA384
ECC Curve Name: prime256v1
ECC Key Strength: 128

```

```

Subject: zabbix.com
AltNames: DNS:*.zabbix.com, DNS:zabbix.com
Issuer: E1

```

```

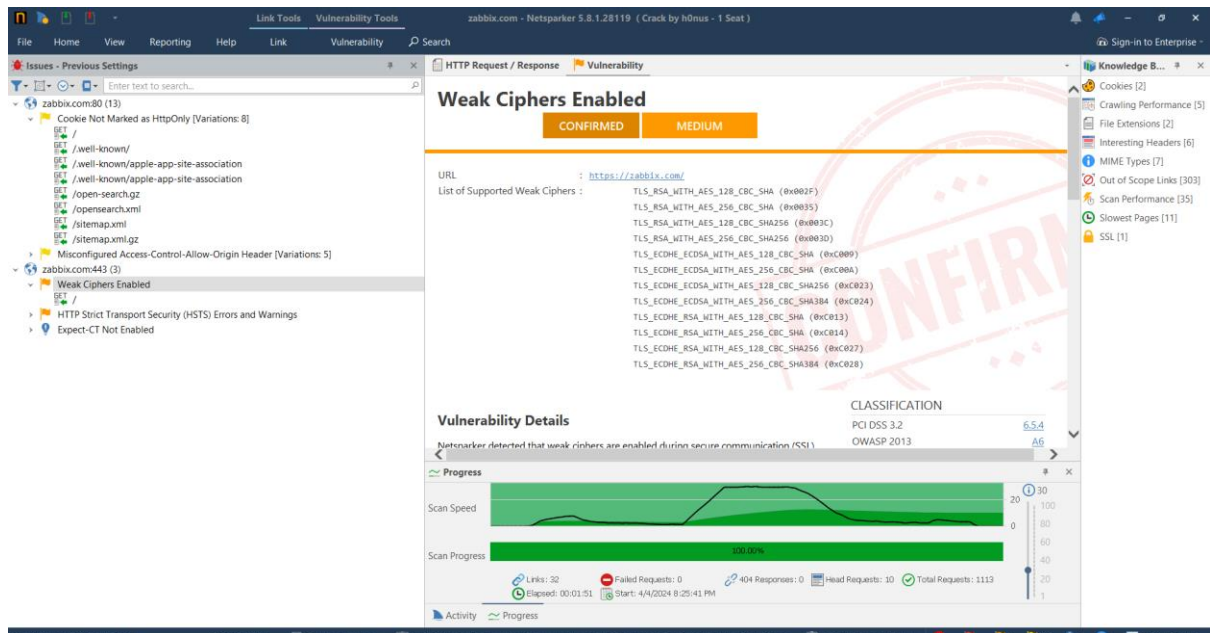
Not valid before: Apr 1 23:11:24 2024 GMT
Not valid after: Jun 30 23:11:23 2024 GMT

```

## 1.7 Burpsuite scanning

The screenshot displays the Burp Suite Professional interface. On the left, the 'Site map' shows a tree structure of scanned URLs, including 'https://analytics.google.com' and 'https://zabbix.com'. The 'Contents' panel in the center lists various resources like '/about', '/aerospace', and '/banking\_and\_finance'. The right panel shows an 'Issues' list with one entry: 'Cacheable HTTPS response'. Below this, the 'Request' and 'Response' tabs are visible, showing the raw HTTP data. The 'Issue description' section explains that browsers can store a local cached copy of content, which could be accessed via HTTPS, potentially exposing sensitive information. The 'Issue remediation' section advises returning caching directives to prevent this.

## 1.8 Netsparker scan



## 1.9 Vulnerabilities

**Vulnerability Title:** Weak Cipher Enabled in SSL Communication

**Vulnerability Description:** The web server for the application is set up to let weak cyphers work during SSL/TLS connection. This means that sensitive data could be vulnerable to attacks that decrypt it. Weak cyphers are cryptographic algorithms that can be hacked, and letting people use them makes the SSL/TLS link less secure. Attackers could use this flaw to decrypt SSL traffic between the server and its visitors, which would let private data slip out.

**Affected Components:** SSL/TLS configuration of the web server.

**Impact Assessment:** Impact of vulnerability includes,

- Decrypt sensitive information.
- Data breaches
- Identity theft
- Financial loss

**Steps to Reproduce:**

1. Open netsparker tool and give the URL to search.
2. In the report weak ciphers are mentioned as a list.
3. If not SSL scan contains ciphers that are used for the site.



## Proof of concept:

### List of Supported Weak Ciphers

- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA (0x002F)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x0035)
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0x003C)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA256 (0x003D)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA (0xC009)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA (0xC00A)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC023)
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC024)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA (0xC013)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0xC014)
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xC027)
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 (0xC028)

```
(tharu@kali)-[~]
$ sslscan https://www.zabbix.com/
Version: 2.1.3-static
OpenSSL 3.0.12 24 Oct 2023

Connected to 104.26.7.148
Testing SSL server www.zabbix.com on port 443 using SNI name www.zabbix.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled

TLS Fallback SCSV:
Server supports TLS Fallback SCSV

TLS renegotiation:
Session renegotiation not supported

TLS Compression:
Compression disabled

Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_AES_256_GCM_SHA384 Curve 25519 DHE 253
Accepted TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 256 bits ECDHE-ECDSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-ECDSA-AES128-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-ECDSA-AES256-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-CHACHA20-POLY1305 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve 25519 DHE 253
```

**Proposed Mitigation or Fix:** In the Apache server modify the SSLCipherSuite directive in the httpd.conf to **SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4**. If it's in Lighttpd change it to **ssl.honor-cipher-order = "enable" ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"**

#### 1.9.1 Other vulnerabilities

1. HTTP Strict Transport Security (HSTS) Errors and Warnings.
2. Misconfigured AccessControl-Allow-Origin Header.
3. Cookie Not Marked as HttpOnly.
4. Expect-CT Not Enabled.