登途维修连锁总部端

Report generated by Tenable Nessus™ Thu, 13 Nov 2025 15:14:22 China Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

dtzb.sihuiyun.com

0	0	0	0	15
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Nov 13 14:54:53 2025
End time:	Thu Nov 13 15:14:22 2025

Host Information

DNS Name:	dtzb.sihuiyun.com
IP:	60.205.106.102
OS:	Microsoft Windows

Vulnerabilities

33817 - CGI Generic Tests Load Estimation (all tests)

Synopsis

Load estimation for web application tests.

Description

This script computes the maximum number of requests that would be done by the generic web tests, depending on miscellaneous options. It does not perform any test by itself.

The results can be used to estimate the duration of these tests, or the complexity of additional manual tests.

Note that the script does not try to compute this duration based on external factors such as the network and web servers loads.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/10/26, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Here are the estimated number of requests in miscellaneous modes
for one method only (GET or POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution (time based) : S=6          SP=6         AP=6         SC=6         AC=6

format string                            : S=2          SP=2         AP=2         SC=2         AC=2

cross-site scripting (comprehensive test): S=4          SP=4         AP=4         SC=4         AC=4

injectable parameter                     : S=2          SP=2         AP=2         SC=2         AC=2

arbitrary command execution              : S=16         SP=16        AP=16        SC=16        AC=16

local file inclusion                     : S=1          SP=1         AP=1         SC=1         AC=1

directory traversal                      : S=25         SP=25        AP=25        SC=25        AC=25

web code injection                       : S=1          SP=1         AP=1         SC=1         AC=1

blind SQL injection (4 requests)         : S=4          SP=4         AP=4         SC=4         AC=4

persistent XSS                           : S=4          SP=4         AP=4         SC=4         AC=4

directory traversal (write access)       : S=2          SP=2         AP=2         SC=2         AC=2

XML injection                            : S=1          SP=1         AP=1         SC=1         AC=1

blind SQL injection                      : S=12         SP=12        AP=12        SC=12        AC=12

SQL injection                            : S=24         SP=24        AP=24        SC=24        AC=24

directory traversal (extended test)      : S=51         SP=51        AP=51        SC=51        AC=51

SSI injection                            : S=3          SP=3         AP=3         SC=3         AC=3

unseen parameters                        : S=35         SP=35        AP=35        SC=35        AC=35

SQL injection (2nd order)              [...]
```

43111 - HTTP Methods Allowed (per directory)

Synopsis

This plugin determines which HTTP methods are allowed on various CGI directories.

Description

By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory.

The following HTTP methods are considered insecure:

PUT, DELETE, CONNECT, TRACE, HEAD

Many frameworks and languages treat 'HEAD' as a 'GET' request, albeit one without any body in the response. If a security constraint was set on 'GET' requests such that only 'authenticatedUsers' could access GET requests for a particular servlet or resource, it would be bypassed for the 'HEAD' version. This allowed unauthorized blind submission of any privileged GET request.

As this list may be incomplete, the plugin also tests - if 'Thorough tests' are enabled or 'Enable web applications tests' is set to 'yes'

in the scan policy - various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501.

Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.

See Also

http://www.nessus.org/u?d9c03a9a

http://www.nessus.org/u?b019cbdb

https://www.owasp.org/index.php/Test_HTTP_Methods_(OTG-CONFIG-006)

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2009/12/10, Modified: 2022/04/11

Plugin Output

tcp/80/www

```
Based on the response to an OPTIONS request :

  - HTTP methods  GET  HEAD  POST  TRACE OPTIONS are allowed on :

    /
    /Resource
    /Resource/Css
    /Resource/css
    /Resource/images
    /Resource/layui
    /Resource/layui/css
    /Service
    /business
    /help
    /logs
    /service
    /system


Based on tests of each method :

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT are allowed on :

    /Resource/css
    /Resource/images
    /Resource/layui
    /Resource/layui/css
    /Service
    /business
    /help
    /logs
    /service
    /system

  - HTTP methods ACL BASELINE-CONTROL BCOPY BDELETE BMOVE BPROPFIND
    BPROPPATCH CHECKIN CHECKOUT DEBUG GET HEAD INDEX LABEL MERGE
    MKACTIVITY MKWORKSPACE NOTIFY OPTIONS ORDERPATCH PATCH POLL POST
    REPORT RPC_IN_DATA RPC_OUT_DATA SEARCH SUBSCRIBE UNCHECKOUT
    UNSUBSCRIBE UPDATE VERSION-CONTROL X-MS-ENUMATTS are allowed on :

    /
    /Resource
    /Resource/Css

  - Invalid/unknown HTTP methods are allowed on :

    /
    /Resource
    /Resource/Css
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/80/www

```
The remote web server type is :

Microsoft-IIS/10.0
```

10107 - HTTP Server Type and Version

Synopsis

A web server is running on the remote host.

Description

This plugin attempts to determine the type and the version of the remote web server.

Solution

n/a

Risk Factor

None

References

XREF	IAVT:0001-T-0931

Plugin Information

Published: 2000/01/04, Modified: 2020/10/30

Plugin Output

tcp/443/www

```
The remote web server type is :

Microsoft-HTTPAPI/2.0
```

24260 - HyperText Transfer Protocol (HTTP) Information

Synopsis

Some information about the remote HTTP configuration can be extracted.

Description

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2007/01/30, Modified: 2024/02/26

Plugin Output

tcp/80/www

```

Response Code : HTTP/1.1 302 Found

Protocol version : HTTP/1.1
HTTP/2 TLS Support: No
HTTP/2 Cleartext Support: No
SSL : no
Keep-Alive : no
Options allowed : OPTIONS, TRACE, GET, HEAD, POST
Headers :

  Cache-Control: private
  Content-Type: text/html; charset=utf-8
  Location: /Login.aspx
  Server: Microsoft-IIS/10.0
  X-AspNet-Version: 4.0.30319
  X-Powered-By: ASP.NET
  X-Frame-Options: SAMEORIGIN
  Access-Control-Allow-Origin: *
  Access-Control-Allow-Methods: GET,POST,OPTIONS
  Access-Control-Allow-Headers: token,action,timestamp,checkcode,x-requested-with,content-type
  Date: Thu, 13 Nov 2025 07:01:04 GMT
  Content-Length: 128

Response Body :

<html><head><title>Object moved</title></head><body>
<h2>Object moved to <a href="/Login.aspx">here</a>.</h2>
```

```
</body></html>
```

91634 - HyperText Transfer Protocol (HTTP) Redirect Information

Synopsis

The remote web server redirects requests to the root directory.

Description

The remote web server issues an HTTP redirect when requesting the root directory of the web server.

This plugin is informational only and does not denote a security problem.

Solution

Analyze the redirect(s) to verify that this is valid operation for your web server and/or application.

Risk Factor

None

Plugin Information

Published: 2016/06/16, Modified: 2025/11/03

Plugin Output

tcp/80/www

```
Request          : http://dtzb.sihuiyun.com/
HTTP response    : HTTP/1.1 302 Found
Redirect to      : http://dtzb.sihuiyun.com/Login.aspx
Redirect type    : 30x redirect

Final page       : http://dtzb.sihuiyun.com/Login.aspx
HTTP response    : HTTP/1.1 200 OK
```

24242 - Microsoft .NET Handlers Enumeration

Synopsis

It is possible to enumerate the remote .NET handlers used by the remote web server.

Description

It is possible to obtain the list of handlers the remote ASP.NET web server supports.

See Also

https://support.microsoft.com/en-us/help/815145

Solution

None

Risk Factor

None

Plugin Information

Published: 2007/01/26, Modified: 2018/11/15

Plugin Output

tcp/80/www

```
The remote extensions are handled by the remote ASP.NET server :

 - .rem
 - .soap
```

50344 - Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header

Synopsis

The remote web server does not take steps to mitigate a class of web application vulnerabilities.

Description

The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all.

The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks.

See Also

http://www.nessus.org/u?55aa8f57

http://www.nessus.org/u?07cc2a06

https://content-security-policy.com/

https://www.w3.org/TR/CSP2/

Solution

Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources.

Risk Factor

None

Plugin Information

Published: 2010/10/26, Modified: 2021/01/19

Plugin Output

tcp/80/www

```
The following pages do not set a Content-Security-Policy frame-ancestors response header or set a
 permissive policy:

   - http://dtzb.sihuiyun.com/Login.aspx
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/80/www

```
Port 80/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/443/www

```
Port 443/tcp was found to be open
```

11219 - Nessus SYN scanner

Synopsis

It is possible to determine which TCP ports are open.

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Risk Factor

None

Plugin Information

Published: 2009/02/04, Modified: 2025/07/14

Plugin Output

tcp/3389/msrdp

```
Port 3389/tcp was found to be open
```

19506 - Nessus Scan Information

Synopsis

This plugin displays information about the Nessus scan.

Description

This plugin displays, for each tested host, information about the scan itself :

- The version of the plugin set.
- The type of scanner (Nessus or Nessus Home).
- The version of the Nessus Engine.
- The port scanner(s) used.
- The port range scanned.
- The ping round trip time
- Whether credentialed or third-party patch management checks are possible.
- Whether the display of superseded patches is enabled
- The date of the scan.
- The duration of the scan.
- The number of hosts scanned in parallel.
- The number of checks done in parallel.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2005/08/26, Modified: 2025/10/29

Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 10.10.1
Nessus build : 20010
Plugin feed version : 202511120339
Scanner edition used : Nessus Home
Scanner OS : WINDOWS
Scanner distribution : win-x86-64
Scan type : Normal
Scan name : #########
Scan policy used : Web Application Tests
Scanner IP : 10.20.30.153
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 21.102 ms
Thorough tests : no
Experimental tests : no
Scan for Unpatched Vulnerabilities : no
Plugin debugging enabled : no
Paranoia level : 1
Report verbosity : 1
Safe checks : yes
Optimize the test : yes
Credentialed checks : no
Patch management checks : None
Display superseded patches : yes (supersedence plugin did not launch)
CGI scanning : enabled
Web application tests : enabled
Web app tests -  Test mode : single
Web app tests -  Try all HTTP methods : no
Web app tests -  Maximum run time : 5 minutes.
Web app tests -  Stop at first flaw : CGI
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing : Yes
Nessus Plugin Signature Checking : Enabled
Audit File Signature Checking : Disabled
Scan Start Date : 2025/11/13 14:55 China Standard Time (UTC +08:00)
Scan duration : 1145 sec
Scan for malware : no
```

91815 - Web Application Sitemap

Synopsis

The remote web server hosts linkable content that can be crawled by Nessus.

Description

The remote web server contains linkable content that can be used to gather information about a target.

See Also

http://www.nessus.org/u?5496c8d9

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2016/06/24, Modified: 2016/06/24

Plugin Output

tcp/80/www

```

The following sitemap was created from crawling linkable content on the target host :

  - http://dtzb.sihuiyun.com/Login.aspx
  - http://dtzb.sihuiyun.com/Resource/Css/ft-carousel.css
  - http://dtzb.sihuiyun.com/Resource/css/css.css
  - http://dtzb.sihuiyun.com/Resource/images/favicon.ico
  - http://dtzb.sihuiyun.com/Resource/layui/css/layui.css
  - http://dtzb.sihuiyun.com/Service/NavigationCss.ashx

Attached is a copy of the sitemap file.
```

11032 - Web Server Directory Enumeration

Synopsis

It is possible to enumerate directories on the web server.

Description

This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not.

See Also

http://projects.webappsec.org/w/page/13246953/Predictable%20Resource%20Location

Solution

n/a

Risk Factor

None

References

XREF	OWASP:OWASP-CM-006

Plugin Information

Published: 2002/06/26, Modified: 2024/06/07

Plugin Output

tcp/80/www

```
The following directories were discovered:
/logs, /help, /service, /system, /business

While this is not, in and of itself, a bug, you should manually inspect
these directories to ensure that they are in compliance with company
security standards
```

10662 - Web mirroring

Synopsis

Nessus can crawl the remote website.

Description

This plugin makes a mirror of the remote website(s) and extracts the list of CGIs that are used by the remote host.

It is suggested that you change the number of pages to mirror in the 'Options' section of the client.

Solution

n/a

Risk Factor

None

Plugin Information

Published: 2001/05/04, Modified: 2025/11/03

Plugin Output

tcp/80/www

```
Webmirror performed 31 queries in 2s (15.0500 queries per second)

The following CGIs have been discovered :


+ CGI : /Resource/images/favicon.ico
  Methods : GET
  Argument :
   Value: 20251113144741


+ CGI : /Service/NavigationCss.ashx
  Methods : GET
  Argument : v
   Value: 20251113144741
```