Report generated by Nessus™

# our Site webApp deep

Tue, 22 Jun 2021 04:54:21 EDT

**TABLE OF CONTENTS**



## Vulnerabilities by Host

Collapse All | Expand All

## teamnebula.us-east-1.elasticbeanstalk.com

| CRITICAL | HIGH | MEDIUM | LOW | INFO |
|---|---|---|---|---|
| 0 | 1 | 3 | 0 | 12 |

### Scan Information

| | |
|---|---|
| Start time: | Tue Jun 22 04:20:50 2021 |
| End time: | Tue Jun 22 04:54:21 2021 |

### Host Information

| | |
|---|---|
| DNS Name: | teamnebula.us-east-1.elasticbeanstalk.com |
| IP: | 107.20.143.245 |
| OS: | AIX 5.3 |

### Vulnerabilities

**42424 - CGI Generic SQL Injection (blind)** -

#### Synopsis

A CGI application hosted on the remote web server is potentially prone to SQL injection attack.

#### Description

By sending specially crafted parameters to one or more CGI scripts hosted on the remote web server, Nessus was able to get a very different response, which suggests that it may have been able to modify the behavior of the application and directly access the underlying database.

An attacker may be able to exploit this issue to bypass authentication, read confidential data, modify the remote database, or even take control of the remote operating system.

Note that this script is experimental and may be prone to false positives.

#### See Also

http://www.securiteam.com/securityreviews/5DP0N1P76E.html
http://www.nessus.org/u?ed792cf5
http://projects.webappsec.org/w/page/13246963/SQL%20Injection

#### Solution

Modify the affected CGI scripts so that they properly escape arguments.

#### Risk Factor

High

#### CVSS v2.0 Base Score

7.5 (CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P)

#### References

| | |
|---|---|
| XREF | CWE:20 |
| XREF | CWE:77 |

| | |
|---|---|
| XREF | CWE:801 |
| XREF | CWE:810 |
| XREF | CWE:89 |
| XREF | CWE:91 |
| XREF | CWE:203 |
| XREF | CWE:643 |
| XREF | CWE:713 |
| XREF | CWE:722 |
| XREF | CWE:727 |
| XREF | CWE:751 |
| XREF | CWE:928 |
| XREF | CWE:929 |

**Plugin Information**

Published: 2009/11/06, Modified: 2021/01/19

**Plugin Output**

tcp/80/www

```
Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to blind SQL injection :

+ The 'thoughtAuthor' parameter of the /add CGI :

/add [thoughtMessage=519625&thoughtAuthor=zz519625&thoughtAuthor=yy]

-------- output --------
<h1>Share Your Thought!</h1>

<div class="alert alert-error">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Error!</strong> Sorry, The format of your though [...]
-------- vs --------
<h1>Share Your Thought!</h1>

<div class="alert alert-success">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Success!</strong> Thank you for sharing your thought.
------------------------

/add [thoughtMessage=519625&thoughtAuthor=zz519625&thoughtAuthor=yy] {2}

-------- output --------
<h1>Share Your Thought!</h1>

<div class="alert alert-error">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Error!</strong> Sorry, The format of your though [...]
-------- vs --------
<h1>Share Your Thought!</h1>

<div class="alert alert-success">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Success!</strong> Thank you for sharing your thought.
------------------------
```

## 10756 - Apple Mac OS X Find-By-Content .DS_Store Web Directory Listing -

**Synopsis**

It is possible to get the list of files present in the remote directory.

**Description**

It is possible to read a '.DS_Store' file on the remote web server.

This file is created by MacOS X Finder; it is used to remember the icons position on the desktop, among other things, and contains the list of files and directories present in the remote directory.

Note that deleted files may still be present in this .DS_Store file.

**See Also**

https://support.apple.com/en-us/HT1629
https://helpx.adobe.com/dreamweaver/kb/remove-ds-store-files-mac.html
http://www.greci.cc/?p=10

**Solution**

- Configure your web server so as to prevent the download of .DS_Store files
- Mac OS X users should configure their workstation to disable the creation of .DS_Store files on network shares.

**Risk Factor**

Medium

### CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N)

### CVSS v2.0 Temporal Score

3.7 (CVSS2#E:U/RL:OF/RC:C)

### References

| | |
|---|---|
| BID | 3316 |
| BID | 3325 |
| CVE | CVE-2001-1446 |
| XREF | CERT:177243 |

### Plugin Information

Published: 2001/09/14, Modified: 2018/11/15

### Plugin Output

tcp/80/www

```
http://teamnebula.us-east-1.elasticbeanstalk.com/.DS_Store
reveals the following entries:
assets
```

## 46194 - CGI Generic Path Traversal (write test) -

### Synopsis

Arbitrary files may be modified on the remote host.

### Description

The remote web server hosts CGI scripts that fail to adequately sanitize request strings and are affected by directory traversal or local file inclusion vulnerabilities.

By leveraging this issue, an attacker may be able to modify arbitrary files on the web server or execute commands.

Due to the way this flaw is tested, this script is prone to false positives.

### See Also

https://en.wikipedia.org/wiki/Directory_traversal
http://cwe.mitre.org/data/definitions/22.html
http://projects.webappsec.org/w/page/13246952/Path%20Traversal
http://projects.webappsec.org/w/page/13246949/Null%20Byte%20Injection
http://www.nessus.org/u?70f7aa09

### Solution

Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.

### Risk Factor

Medium

### CVSS v2.0 Base Score

6.4 (CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:P)

### References

| | |
|---|---|
| XREF | OWASP:OWASP-AZ-001 |

### Plugin Information

Published: 2010/04/30, Modified: 2021/01/19

### Plugin Output

tcp/80/www

```
Using the POST HTTP method, Nessus found that :

+ The following resources may be vulnerable to directory traversal (write access) :

+ The 'thoughtAuthor' parameter of the /add CGI :
```

```
/add [thoughtMessage=921289&thoughtAuthor=JvUJnyxg../../../../../../../.
./../../windows/system32/config/sam]

-------- output --------
<h1>Share Your Thought!</h1>

<div class="alert alert-success">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Success!</strong> Thank you for sharing your thought.
-------- vs --------
<h1>Share Your Thought!</h1>

<div class="alert alert-error">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Error!</strong> Sorry, The format of your though [...]
------------------------

/add [thoughtMessage=921289&thoughtAuthor=JvUJnyxg../../../../../../../.
./../../windows/system32/config/sam] {2}

-------- output --------
<h1>Share Your Thought!</h1>

<div class="alert alert-success">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Success!</strong> Thank you for sharing your thought.
-------- vs --------
<h1>Share Your Thought!</h1>

<div class="alert alert-error">
<button type="button" class="close" data-dismiss="alert" [...]
<strong>Error!</strong> Sorry, The format of your though [...]
------------------------
```

## 85582 - Web Application Potentially Vulnerable to Clickjacking -

### Synopsis

The remote web server may fail to mitigate a class of web application vulnerabilities.

### Description

The remote web server does not set an X-Frame-Options response header or a Content-Security-Policy 'frame-ancestors' response header in all content responses. This could potentially expose the site to a clickjacking or UI redress attack, in which an attacker can trick a user into clicking an area of the vulnerable page that is different than what the user perceives the page to be. This can result in a user performing fraudulent or malicious transactions.

X-Frame-Options has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors.

Content-Security-Policy (CSP) has been proposed by the W3C Web Application Security Working Group, with increasing support among all major browser vendors, as a way to mitigate clickjacking and other attacks. The 'frame-ancestors' policy directive restricts which sources can embed the protected resource.

Note that while the X-Frame-Options and Content-Security-Policy response headers are not the only mitigations for clickjacking, they are currently the most reliable methods that can be detected through automation. Therefore, this plugin may produce false positives if other mitigation strategies (e.g., frame-busting JavaScript) are deployed or if the page does not perform any security-sensitive transactions.

### See Also

http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking

### Solution

Return the X-Frame-Options or Content-Security-Policy (with the 'frame-ancestors' directive) HTTP header with the page's response.
This prevents the page's content from being rendered by another site when using the frame or iframe HTML tags.

### Risk Factor

Medium

### CVSS v2.0 Base Score

4.3 (CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N)

### References

XREF CWE:693

### Plugin Information

Published: 2015/08/22, Modified: 2017/05/16

### Plugin Output

tcp/80/www

```
The following pages do not use a clickjacking mitigation response header and contain a clickable event :

- http://teamnebula.us-east-1.elasticbeanstalk.com/add
```

### 48204 - Apache HTTP Server Version -

#### Synopsis

It is possible to obtain the version number of the remote Apache HTTP server.

#### Description

The remote host is running the Apache HTTP Server, an open source web server. It was possible to read the version number from the banner.

#### See Also

https://httpd.apache.org/

#### Solution

n/a

#### Risk Factor

None

#### References

XREF IAVT:0001-T-0530

#### Plugin Information

Published: 2010/07/30, Modified: 2020/09/22

#### Plugin Output

tcp/80/www

```
URL : http://teamnebula.us-east-1.elasticbeanstalk.com/
Version : unknown
backported : 0
```

### 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: 2021/01/19

#### 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=12 SP=12 AP=24 SC=0 AC=24
```

```
format string : S=4 SP=4 AP=8 SC=0 AC=8
cross-site scripting (comprehensive test): S=34 SP=34 AP=68 SC=0 AC=68
injectable parameter : S=4 SP=4 AP=8 SC=0 AC=8
arbitrary command execution : S=44 SP=44 AP=88 SC=0 AC=88
local file inclusion : S=8 SP=8 AP=16 SC=0 AC=16
directory traversal : S=58 SP=58 AP=116 SC=0 AC=116
web code injection : S=2 SP=2 AP=4 SC=0 AC=4
blind SQL injection (4 requests) : S=8 SP=8 AP=16 SC=0 AC=16
persistent XSS : S=8 SP=8 AP=16 SC=0 AC=16
directory traversal (write access) : S=4 SP=4 AP=8 SC=0 AC=8
XML injection : S=2 SP=2 AP=4 SC=0 AC=4
blind SQL injection : S=24 SP=24 AP=48 SC=0 AC=48
SQL injection : S=56 SP=56 AP=112 SC=0 AC=112
directory traversal (extended test) : S=102 SP=102 AP=204 SC=0 AC=204
SSI injection : S=6 SP=6 AP=12 SC=0 AC=12
unseen parameters : S=70 SP=70 AP=140 SC=0 AC=140
SQL injection (2nd order) : S=2 SP=2 AP=4 SC=0 AC=4

All tests : S=448 SP=448 AP=896 SC=0 AC=896

Here are the estimated number of requests in miscellaneous modes
for both methods (GET and POST) :
[Single / Some Pairs / All Pairs / Some Combinations / All Combinations]

arbitrary command execution (time based) : S=24 SP=24 AP=48 SC=0 AC=48
format string : S=8 SP=8 AP=16 SC=0 AC=16
cross-site scripting (comprehensive test): S=68 SP=68 AP=136 SC=0 AC=136
injectable parameter : S=8 SP=8 AP=16 SC=0 AC=16
arbitrary command execution : S=88 SP=88 AP=176 SC=0 AC=176
local file inclusion : S=16 SP=16 AP=32 SC=0 AC=32
directory traversal : S=116 SP=116 AP=232 SC=0 AC=232
web code injection : S=4 SP=4 AP=8 SC=0 AC=8
blind SQL injection (4 requests) : S=16 SP=16 AP=32 SC=0 AC=32
persistent XSS : S=16 SP=16 AP=32 SC=0 AC=32
directory traversal (write access) : S=8 SP=8 AP=16 SC=0 AC=16
XML injection : S=4 SP=4 AP=8 SC=0 AC=8
blind SQL injection : S=48 SP=48 AP=96 SC=0 AC=96
SQL injection : S=112 SP=112 AP=224 SC=0 AC=224
directory traversal (extended test) : S=204 SP=204 AP=408 SC=0 AC=408
SSI injection : S=12 SP=12 AP=24 SC=0 AC=24
unseen parameters : S=140 SP=140 AP=280 SC=0 AC=280
SQL injection (2nd order) : S=4 SP=4 AP=8 SC=0 AC=8

All tests : S=896 SP=896 AP=1792 SC=0 AC=1792

Your mode : all_pairs, GET and POST, thorough tests.
Maximum number of requests : 1792
```

### 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: 2019/03/19

**Plugin Output**

tcp/80/www

```
Based on tests of each method :

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

/
/assets
/assets/css

- Invalid/unknown HTTP methods are allowed on :

/
/assets
/assets/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 :

Apache
```

### 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 and HTTP pipelining are 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: 2019/11/22

**Plugin Output**

tcp/80/www

```
Response Code : HTTP/1.1 200 OK

Protocol version : HTTP/1.1
SSL : no
Keep-Alive : yes
Options allowed : (Not implemented)
Headers :

Date: Tue, 22 Jun 2021 08:30:37 GMT
Server: Apache
Cache-Control: no-cache
Keep-Alive: timeout=65, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8

Response Body :

<!DOCTYPE html>
<html lang="en">

<head>
<meta charset="utf-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<title>Your Thoughts</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0">

<link href="assets/css/bootstrap.min.css" rel="stylesheet">
<style>
body {background: url(assets/img/background.png) repeat;}
.hero-unit {background-color: white;}
</style>
<link href="assets/css/bootstrap-responsive.min.css" rel="stylesheet">
<!--[if lt IE 9]><script src="http://html5shim.googlecode.com/svn/trunk/html5.js"></script><![endif]-->
</head>

<body>

<div class="container">

<h1>Your Thoughts</h1>


<p><a href="/add" class="btn"><b class="icon-pencil"></b> Share Your Thought</a></p>

<div class="hero-unit">
<div class="row-fluid">
<blockquote>
<p>c:/Windows/system.ini</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>../../../../../../../../../../../../../../../Windows/system.ini</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>c:\Windows\system.ini</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\Windows\system.ini</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>/etc/passwd</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>../../../../../../../../../../../../../../../etc/passwd</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>c:/</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>/</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>c:\</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
```

```
<p>../../../../../../../../../../../../../../../../</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>WEB-INF/web.xml</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>WEB-INF\web.xml</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>/WEB-INF/web.xml</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>\WEB-INF\web.xml</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>thishouldnotexistandhopefullyitwillnot</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http://www.google.com/</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http://www.google.com:80/</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http://www.google.com</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http://www.google.com/search?q=OWASP%20ZAP</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http://www.google.com:80/search?q=OWASP%20ZAP</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>www.google.com/</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>www.google.com:80/</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>www.google.com</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>www.google.com/search?q=OWASP%20ZAP</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>www.google.com:80/search?q=OWASP%20ZAP</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http://5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>https://5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>http:\\5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
```

```
<blockquote>
<p>https:\\5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>//5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>\\5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>HtTp://5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>HtTpS://5139197254941294801.owasp.org</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>&lt;!--#EXEC cmd=&quot;ls /&quot;--&gt;</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>&quot;&gt;&lt;!--#EXEC cmd=&quot;ls /&quot;--&gt;&lt;</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>&lt;!--#EXEC cmd=&quot;dir \&quot;--&gt;</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>&quot;&gt;&lt;!--#EXEC cmd=&quot;dir \&quot;--&gt;&lt;</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>0W45pz4p</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>0W45pz4p</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>&#039;&quot;&lt;script&gt;alert(1);&lt;/script&gt;</p>
<small>ZAP</small>
</blockquote>
<hr>
<blockquote>
<p>&#039;&quot;
```

## 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://teamnebula.us-east-1.elasticbeanstalk.com/
- http://teamnebula.us-east-1.elasticbeanstalk.com/add
```

### 50345 - Missing or Permissive X-Frame-Options 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 X-Frame-Options response header or does not set one at all.

The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors

**See Also**

https://en.wikipedia.org/wiki/Clickjacking
http://www.nessus.org/u?399b1f56

**Solution**

Set a properly configured X-Frame-Options 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 X-Frame-Options response header or set a permissive policy:

- http://teamnebula.us-east-1.elasticbeanstalk.com/
- http://teamnebula.us-east-1.elasticbeanstalk.com/add
```

### 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: 2021/04/20

**Plugin Output**

tcp/22/ssh

```
Port 22/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: 2021/04/20

#### Plugin Output

tcp/80/www

```
Port 80/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: 2021/06/17

#### Plugin Output

tcp/0

```
Information about this scan :

Nessus version : 8.14.0
Nessus build : 20261
Plugin feed version : 202106220209
```

```
Scanner edition used : Nessus Home
Scanner OS : LINUX
Scanner distribution : debian6-x86-64
Scan type : Normal
Scan name : our Site webApp deep
Scan policy used : Web Application Tests
Scanner IP : 10.0.2.15
Port scanner(s) : nessus_syn_scanner
Port range : default
Ping RTT : 141.766 ms
Thorough tests : yes
Experimental tests : 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 : all_pairs
Web app tests - Try all HTTP methods : yes
Web app tests - Maximum run time : 10 minutes.
Web app tests - Stop at first flaw : param
Max hosts : 30
Max checks : 4
Recv timeout : 5
Backports : None
Allow post-scan editing: Yes
Scan Start Date : 2021/6/22 4:20 EDT
Scan duration : 2002 sec
```

### 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://teamnebula.us-east-1.elasticbeanstalk.com/
- http://teamnebula.us-east-1.elasticbeanstalk.com/add
- http://teamnebula.us-east-1.elasticbeanstalk.com/assets/css/bootstrap-responsive.min.css
- http://teamnebula.us-east-1.elasticbeanstalk.com/assets/css/bootstrap.min.css

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

### 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: 2021/04/20

**Plugin Output**

tcp/80/www

```
Webmirror performed 8 queries in 9s (0.0888 queries per second)

The following CGIs have been discovered :


+ CGI : /add
Methods : POST
Argument : thoughtAuthor
Argument : thoughtMessage
```