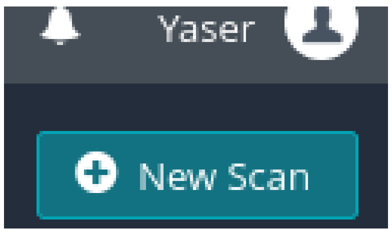
Nessus

Answer the questions below

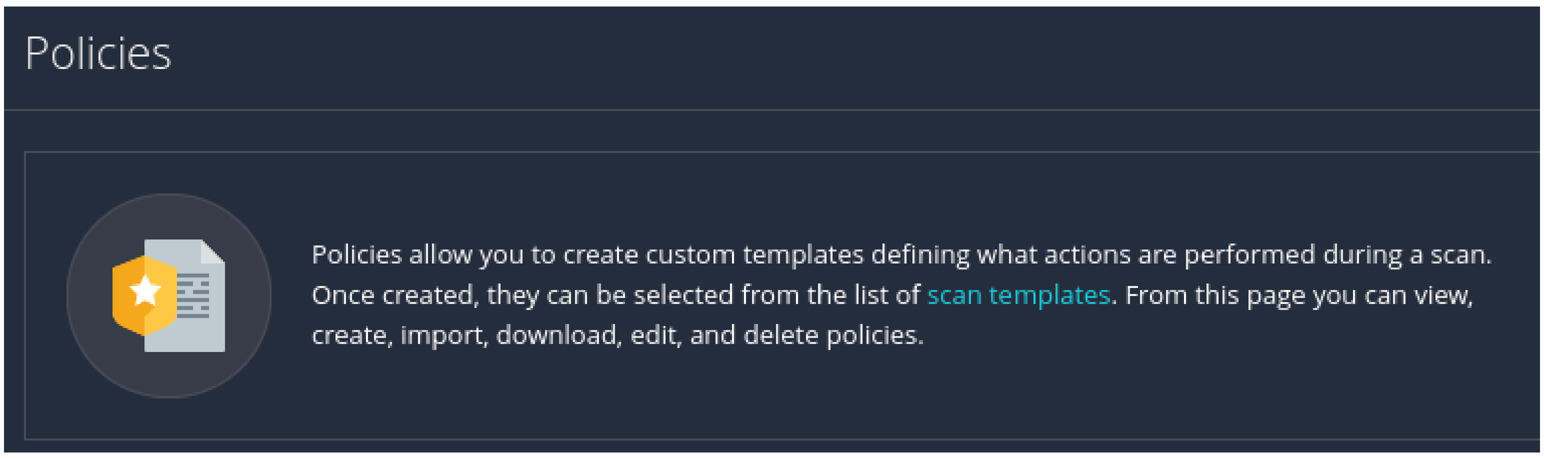
What is the name of the **button** which is used to launch a scan?

New Scan



What side menu option allows us to create **custom templates**?

Policies

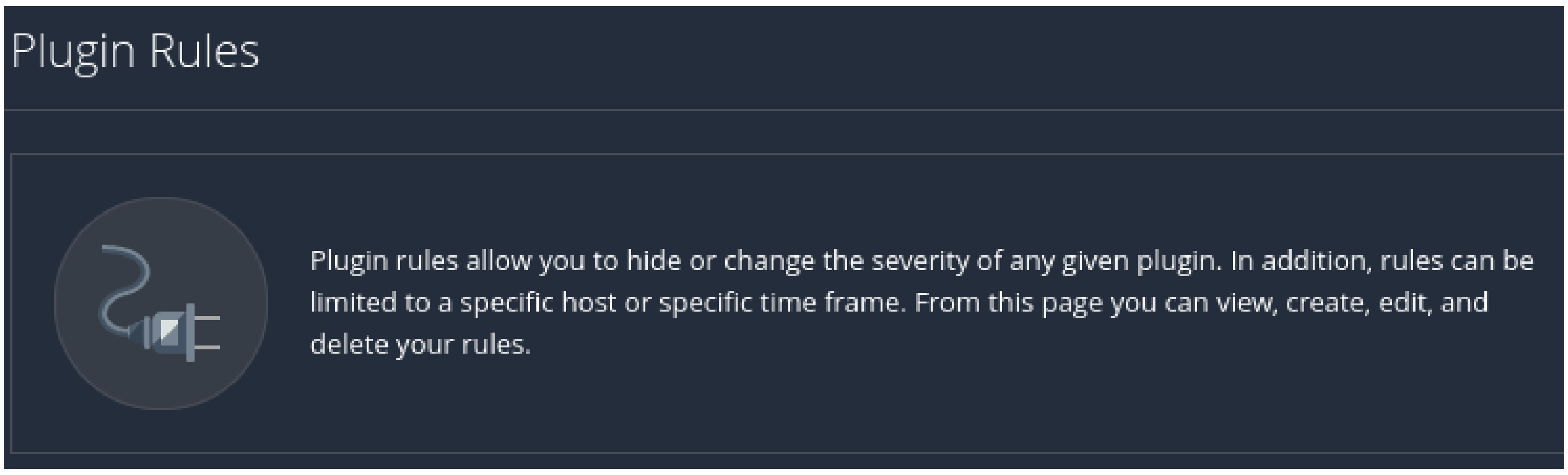


Policies

Policies allow you to create custom templates defining what actions are performed during a scan. Once created, they can be selected from the list of scan templates. From this page you can view, create, import, download, edit, and delete policies.

What menu allows us to change **plugin** properties such as hiding them or changing their severity?

Plugin Rules

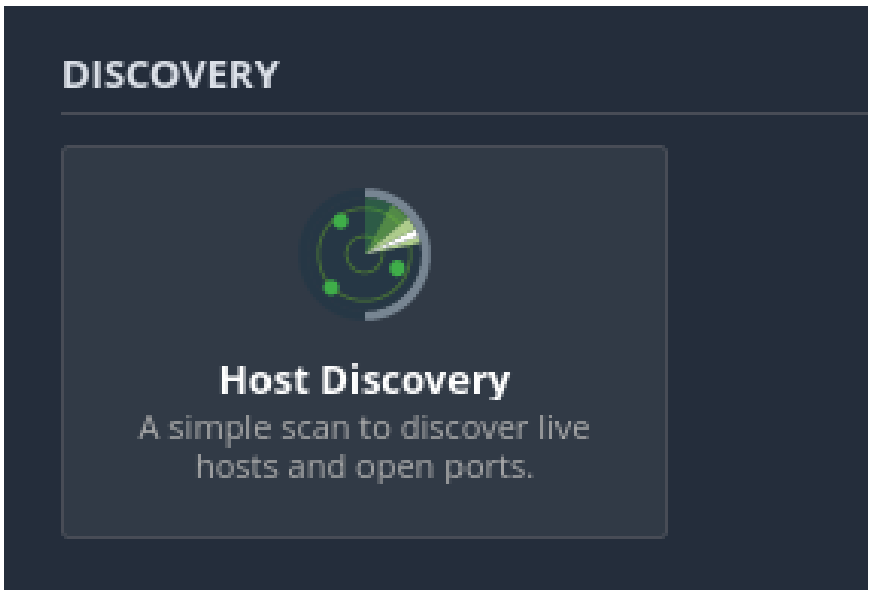


Plugin Rules

Plugin rules allow you to hide or change the severity of any given plugin. In addition, rules can be limited to a specific host or specific time frame. From this page you can view, create, edit, and delete your rules.

In the '**Scan Templates**' section after clicking on '**New Scan**', what scan allows us to see simply what hosts are alive?

Host Discovery



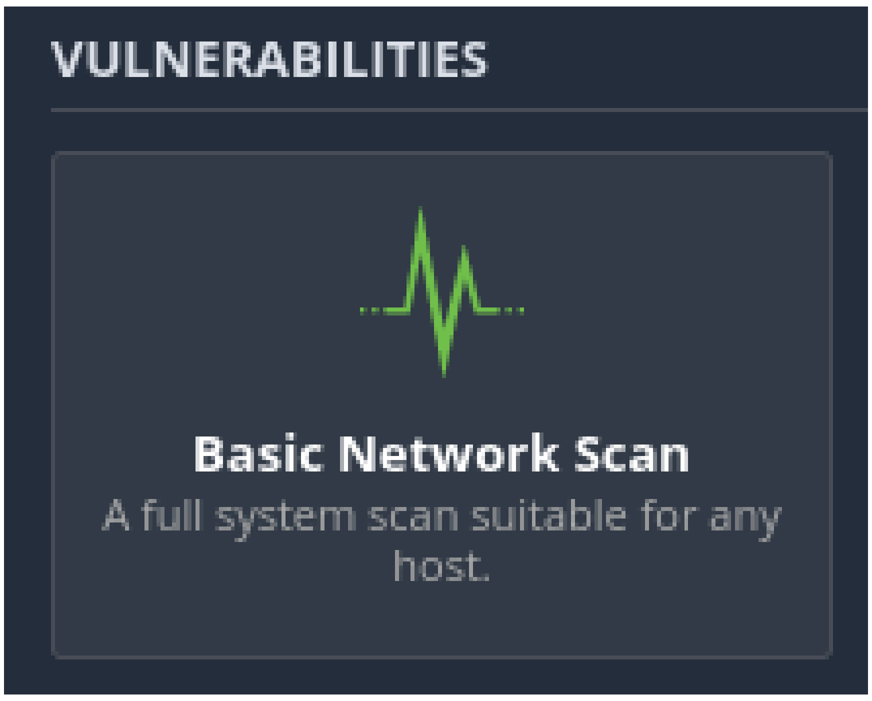
DISCOVERY

Host Discovery

A simple scan to discover live hosts and open ports.

One of the most useful scan types, which is considered to be '**suitable for any host**'?

Basic Network Scan



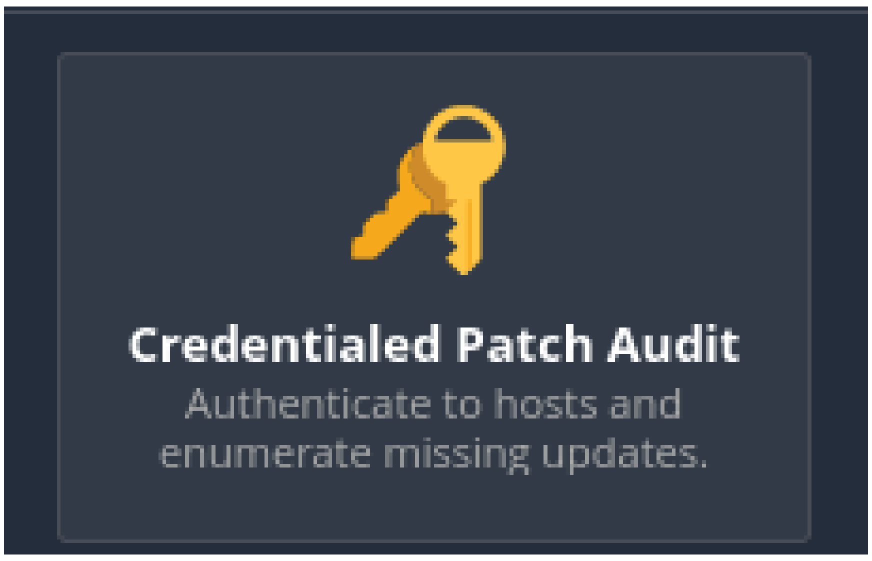
VULNERABILITIES

Basic Network Scan

A full system scan suitable for any host.

What scan allows you to '**Authenticate to hosts and enumerate missing updates**'?

Credentialed Patch Audit

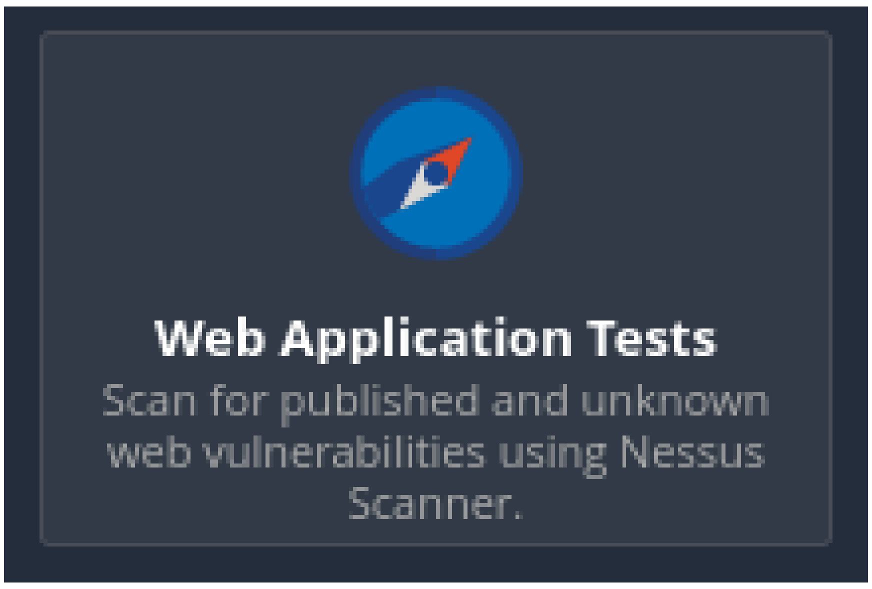


Credentialed Patch Audit

Authenticate to hosts and enumerate missing updates.

What scan is specifically used for scanning **Web Applications**?

Web Application Tests



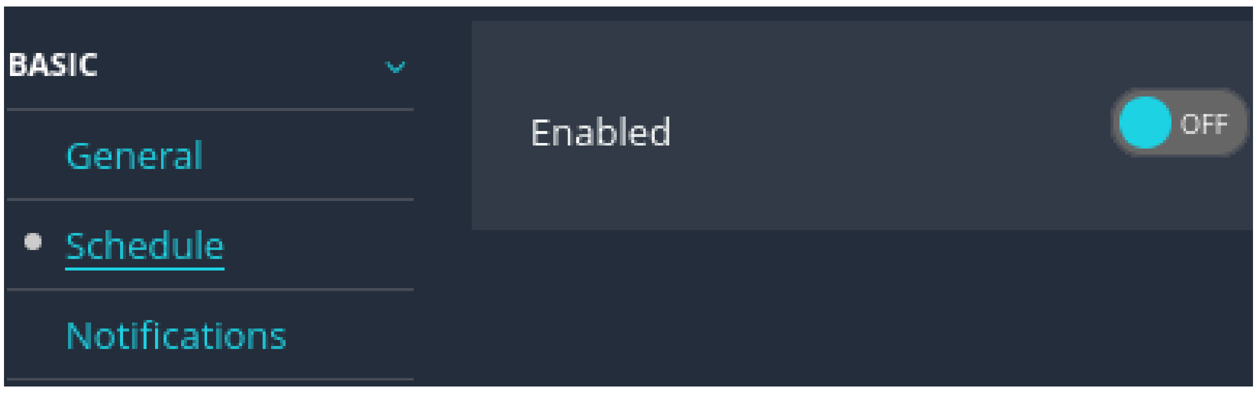
Web Application Tests

Scan for published and unknown web vulnerabilities using Nessus Scanner.

Create a new '**Basic Network Scan**' targeting the deployed VM. What option can we set under '**BASIC**' (on the left) to set a time for this scan to run? This can be very useful when network congestion is an issue.

Schedule

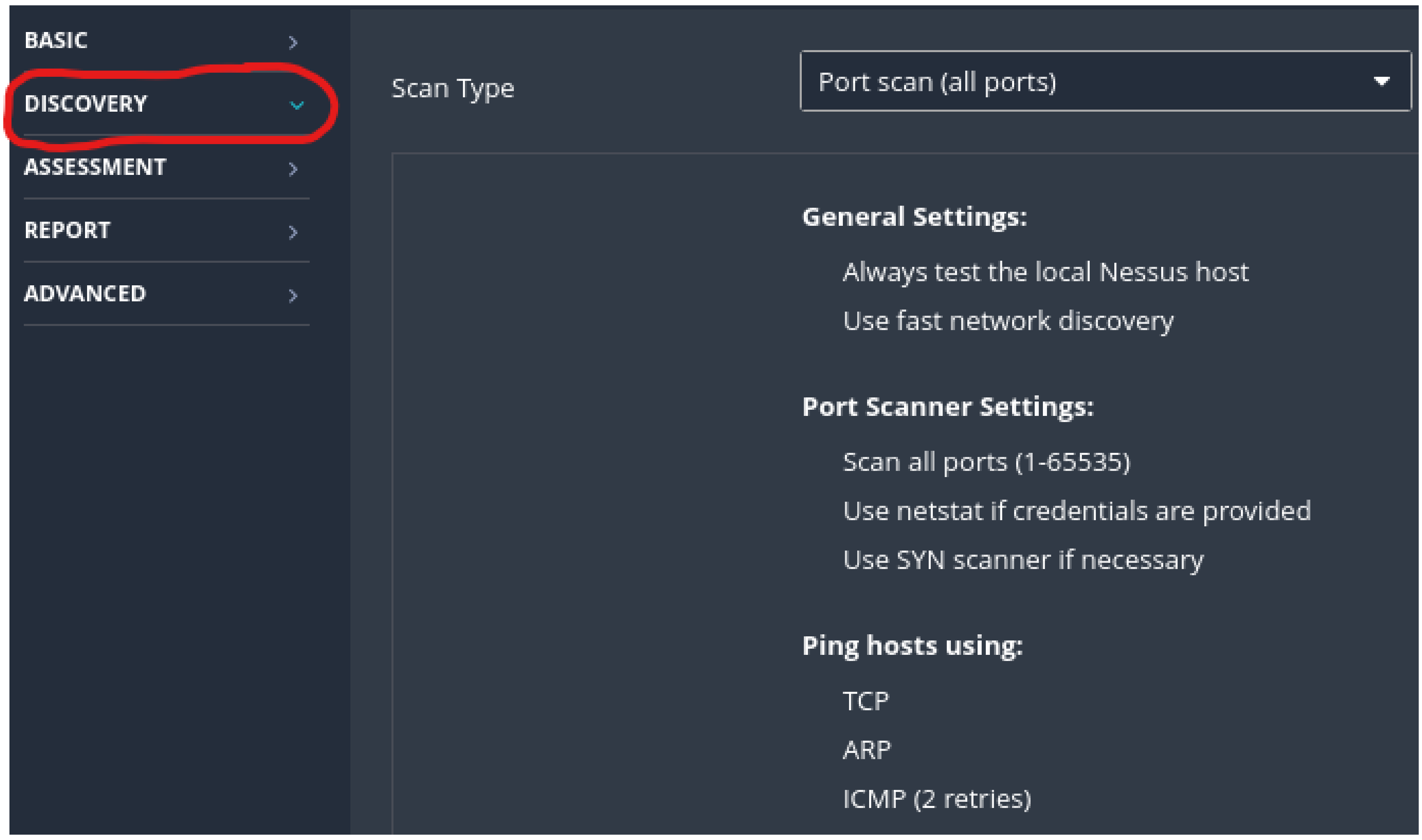
✓ Correct Answer



Enabled OFF

Under '**DISCOVERY**' (on the left) set the '**Scan Type**' to cover ports 1-65535. What is this type called?

Port scan (all ports)



Scan Type: Port scan (all ports)

General Settings:

Always test the local Nessus host

Use fast network discovery

Port Scanner Settings:

Scan all ports (1-65535)

Use netstat if credentials are provided

Use SYN scanner if necessary

Ping hosts using:

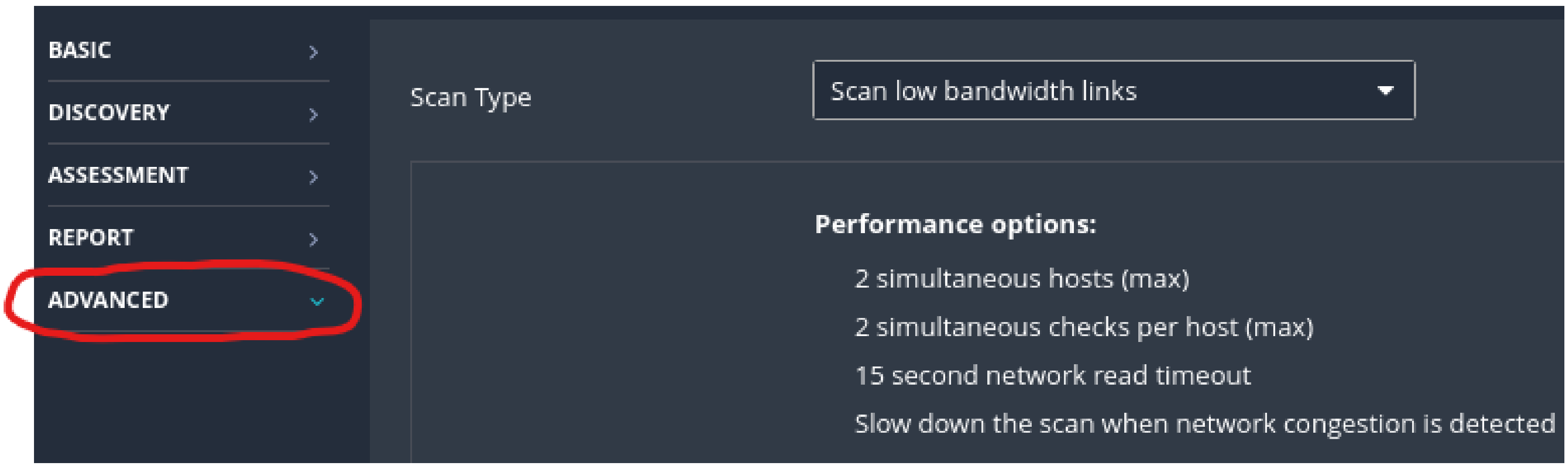
TCP

ARP

ICMP (2 retries)

What '**Scan Type**' can we change to under '**ADVANCED**' for lower bandwidth connection?

Scan low bandwidth links



Scan Type: Scan low bandwidth links

Performance options:

2 simultaneous hosts (max)

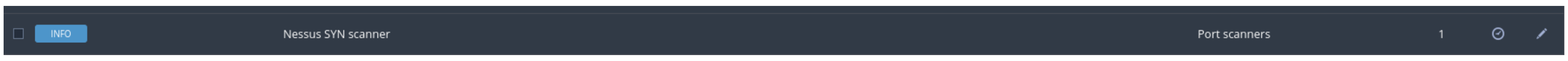
2 simultaneous checks per host (max)

15 second network read timeout

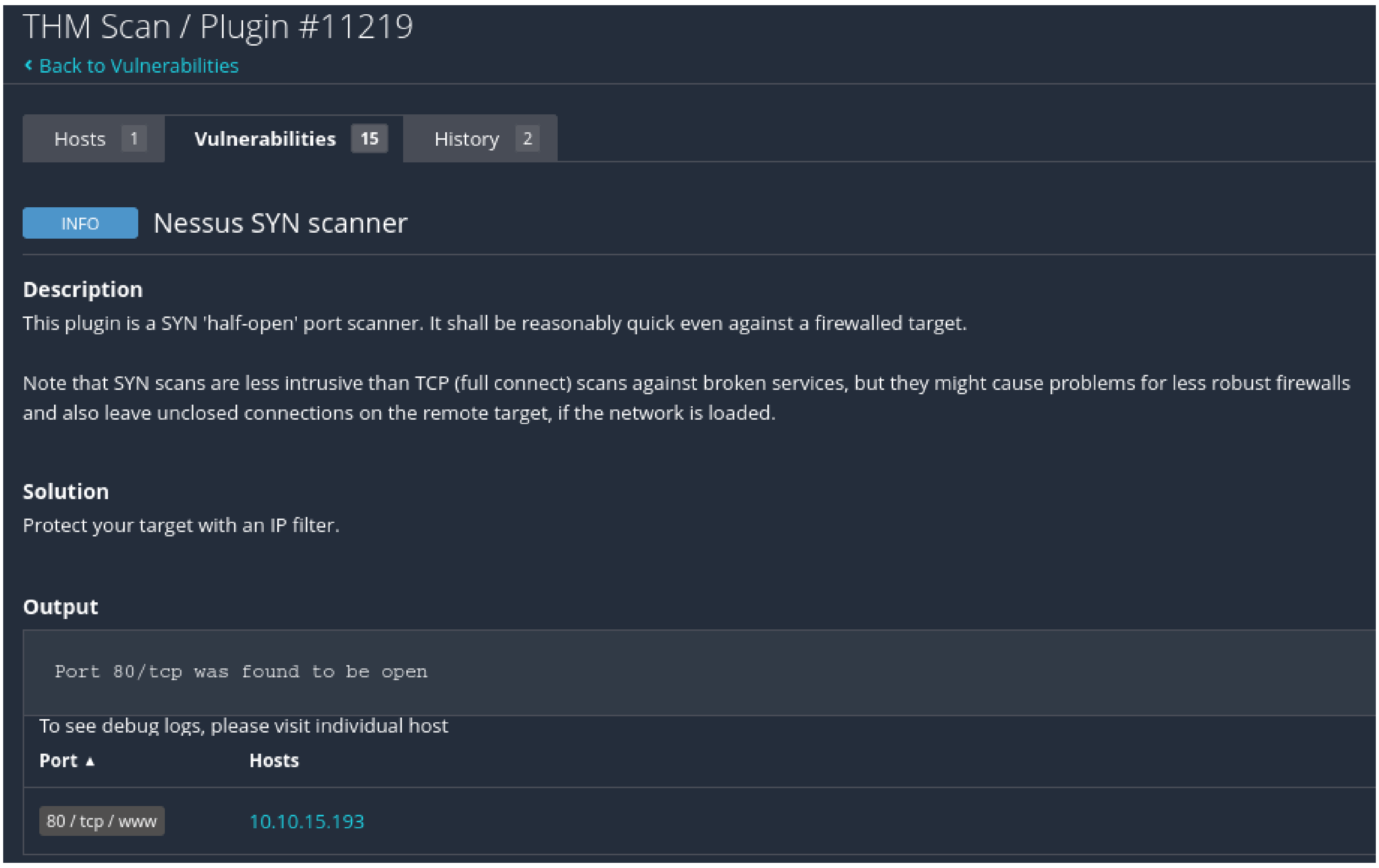
Slow down the scan when network congestion is detected

After the scan completes, which '**Vulnerability**' in the '**Port scanners**' family can we view the details of to see the open ports on this host?

Nessus SYN scanner



□ INFO Nessus SYN scanner Port scanners 1



THM Scan / Plugin #11219

‹ Back to Vulnerabilities

INFO Nessus SYN scanner

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

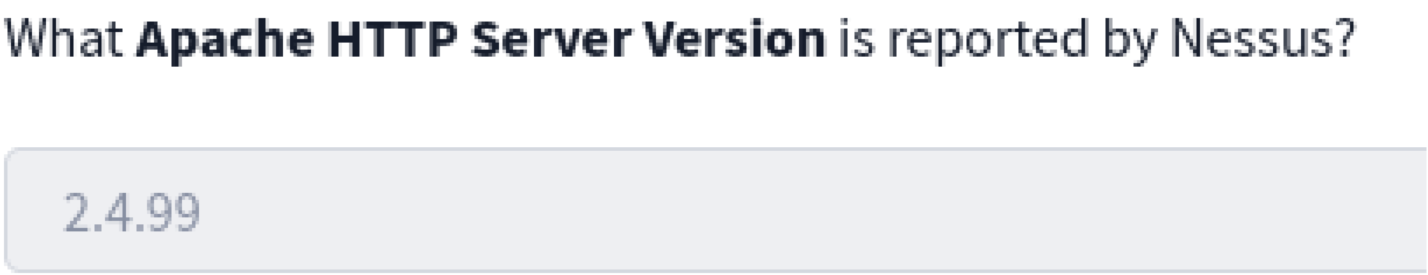
Protect your target with an IP filter.

Output

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

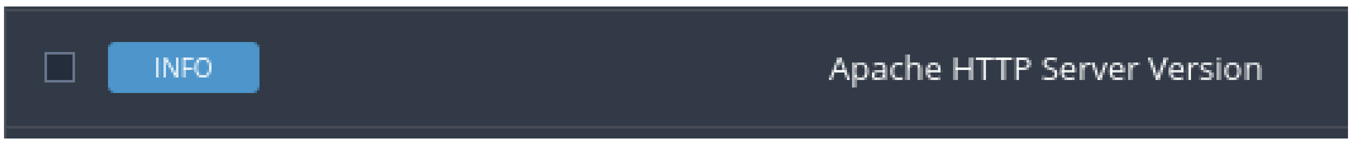
To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.15.193

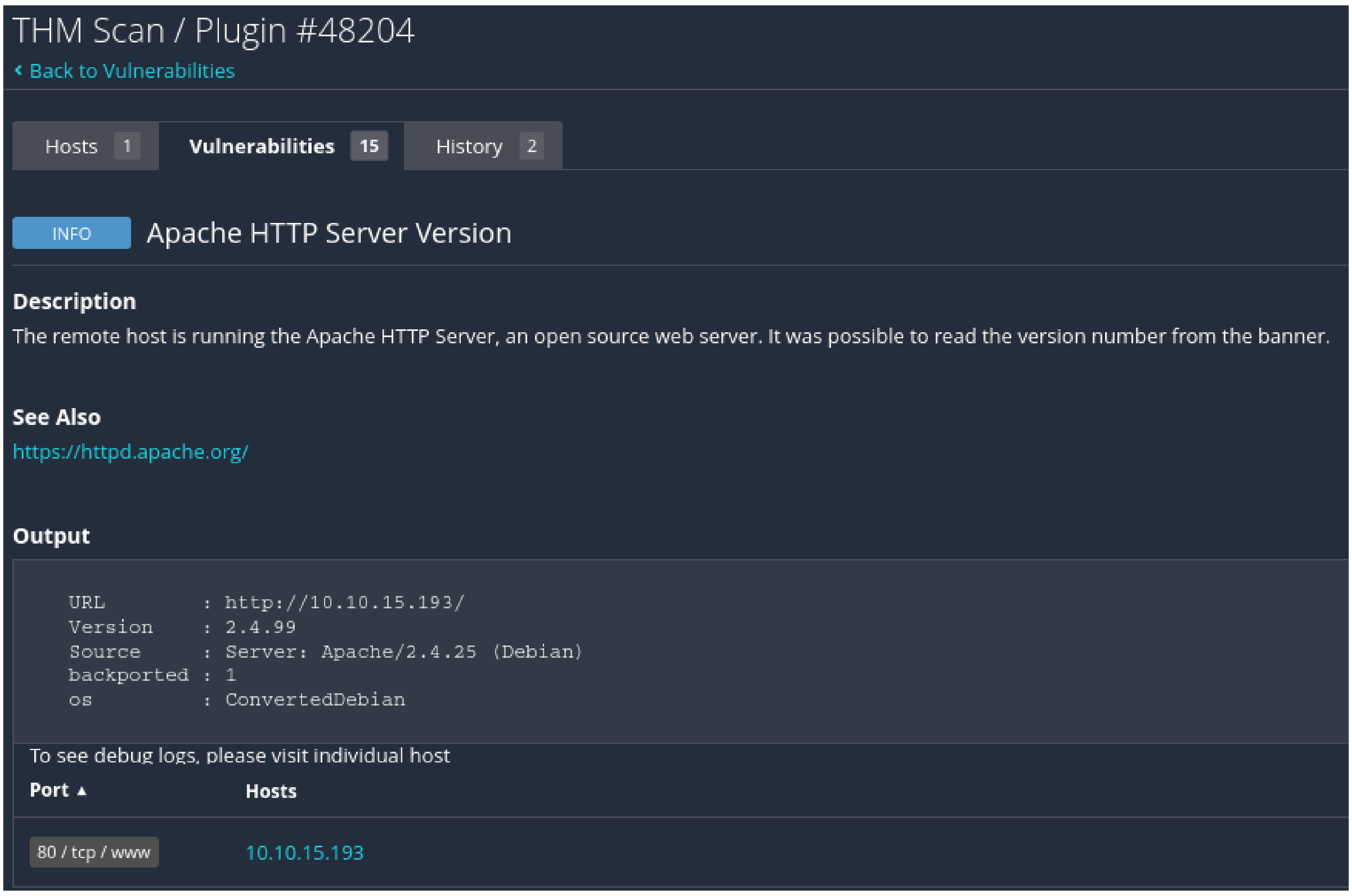


What **Apache HTTP Server Version** is reported by Nessus?

2.4.99



□ INFO Apache HTTP Server Version



THM Scan / Plugin #48204

‹ Back to Vulnerabilities

INFO Apache HTTP Server Version

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/

Output

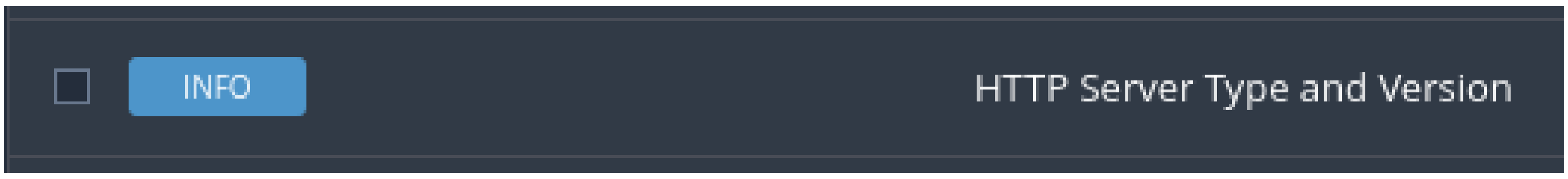
```
  URL        : http://10.10.15.193/
  Version    : 2.4.99
  Source     : Server: Apache/2.4.25 (Debian)
  backported : 1
  os         : ConvertedDebian
```

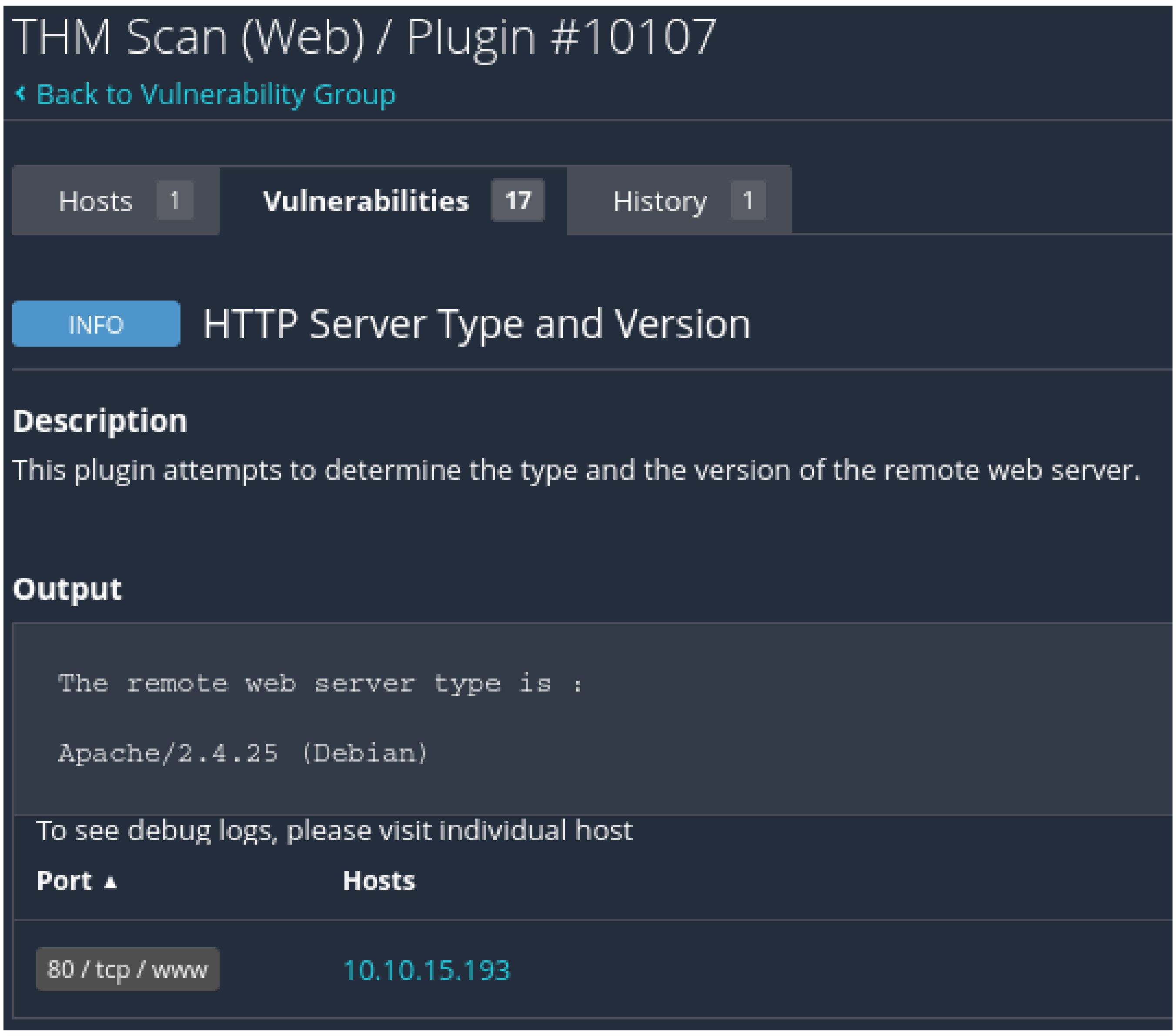
To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.15.193

What is the plugin id of the plugin that determines the HTTP server type and version?

10107





THM Scan (Web) / Plugin #10107

HTTP Server Type and Version

Description

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

Output

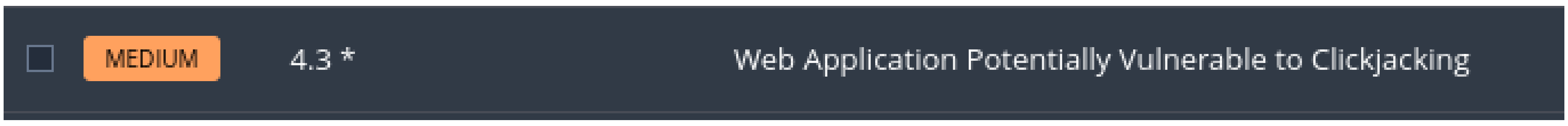
```
The remote web server type is :

Apache/2.4.25 (Debian)
```

To see debug logs, please visit individual host

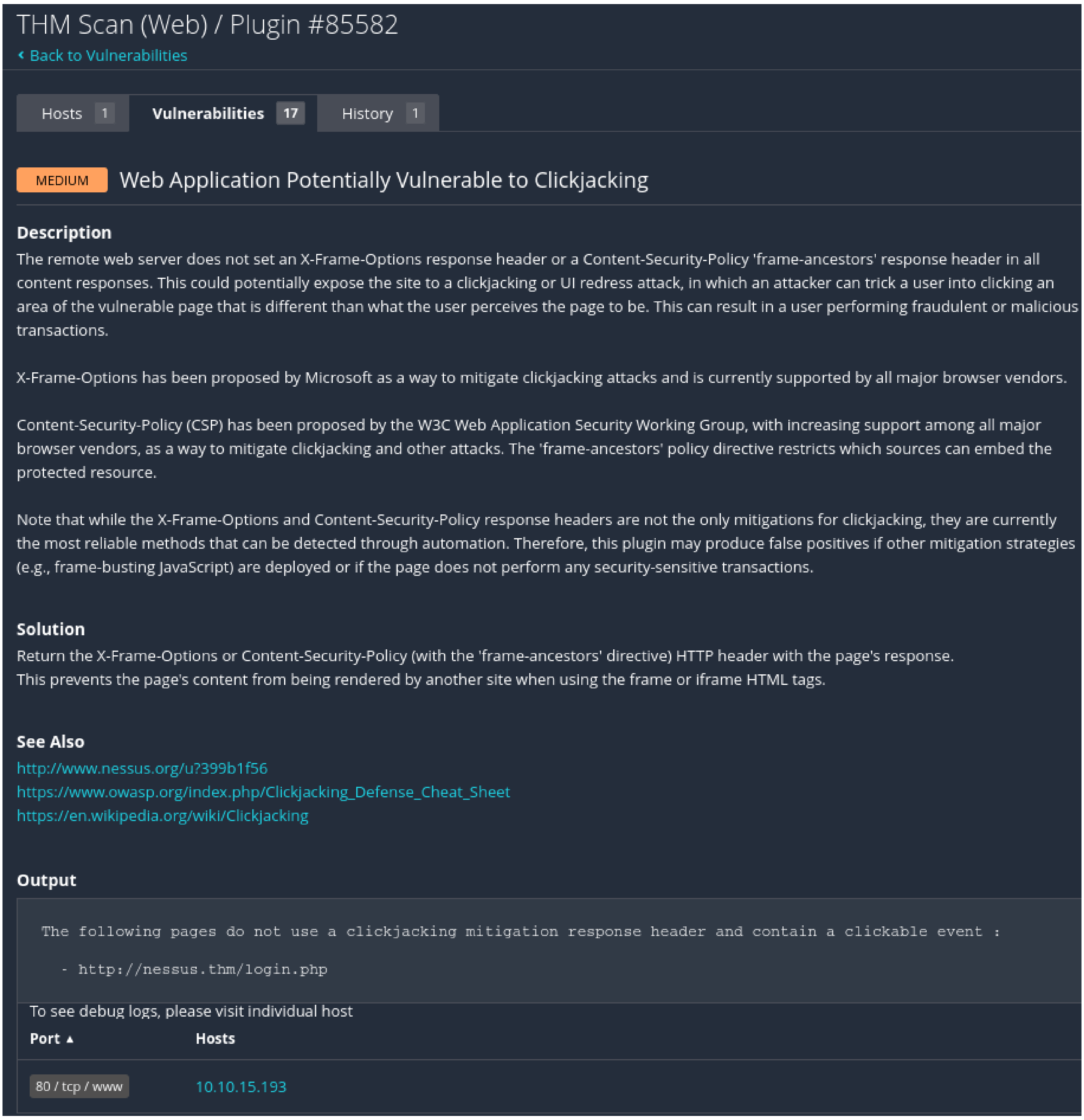
Port ▲	Hosts
80 / tcp / www	10.10.15.193

What authentication page is discovered by the scanner that transmits credentials in cleartext?

login.php



□ MEDIUM 4.3 * Web Application Potentially Vulnerable to Clickjacking



THM Scan (Web) / Plugin #85582

‹ Back to Vulnerabilities

Hosts 1 | **Vulnerabilities 17** | History 1

MEDIUM Web Application Potentially Vulnerable to Clickjacking

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.

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.

See Also

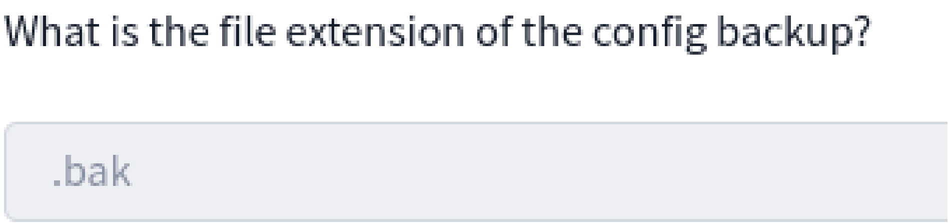
http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking

Output

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

  - http://nessus.thm/login.php
```

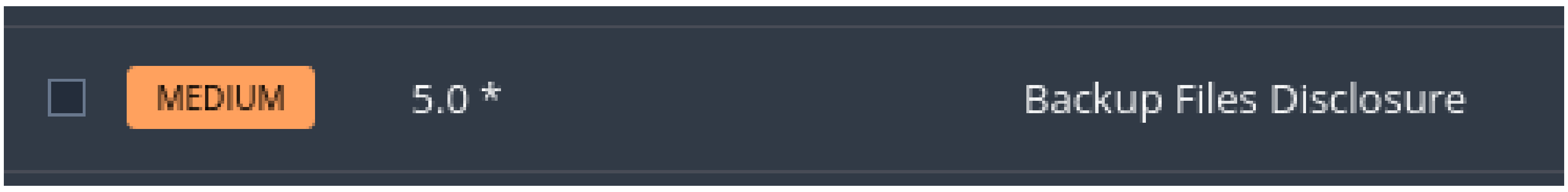
To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.15.193

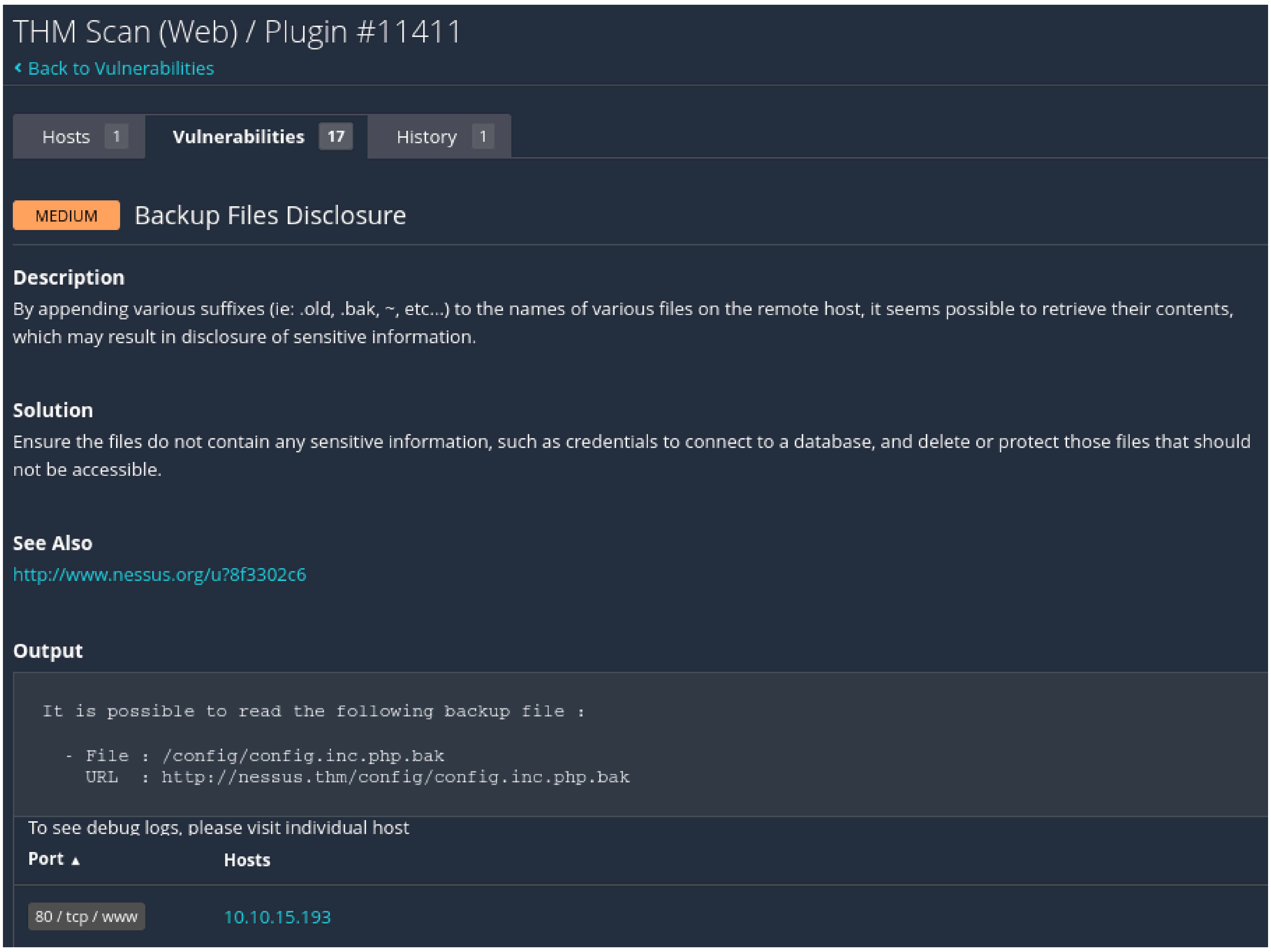


What is the file extension of the config backup?

.bak



☐ MEDIUM 5.0 * Backup Files Disclosure



THM Scan (Web) / Plugin #11411

MEDIUM Backup Files Disclosure

Description

By appending various suffixes (ie: .old, .bak, ~, etc...) to the names of various files on the remote host, it seems possible to retrieve their contents, which may result in disclosure of sensitive information.

Solution

Ensure the files do not contain any sensitive information, such as credentials to connect to a database, and delete or protect those files that should not be accessible.

See Also

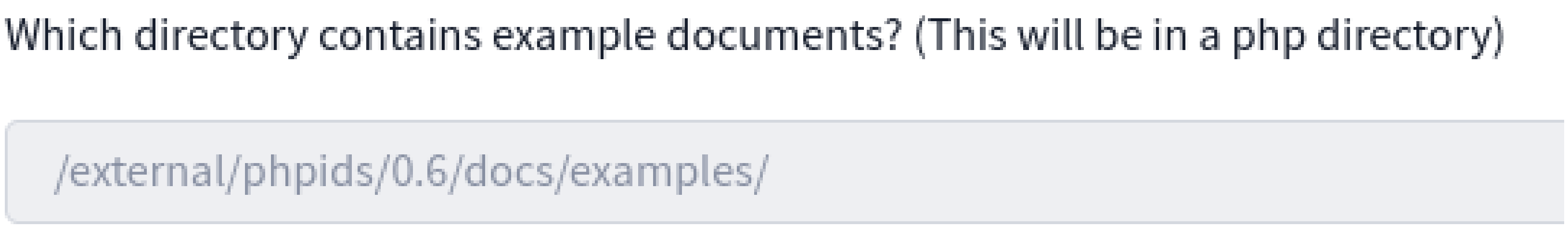
http://www.nessus.org/u?8f3302c6

Output

```
It is possible to read the following backup file :

  - File : /config/config.inc.php.bak
    URL  : http://nessus.thm/config/config.inc.php.bak
```

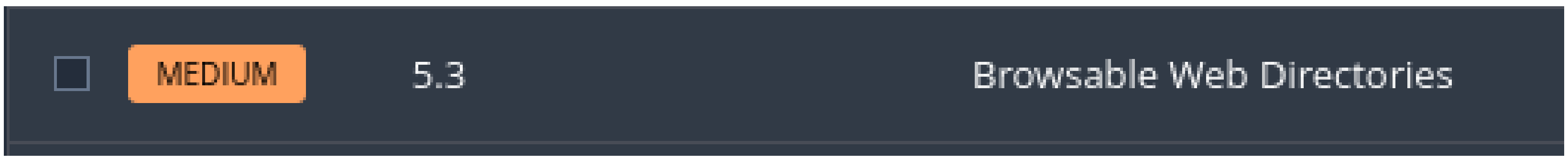
To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.15.193

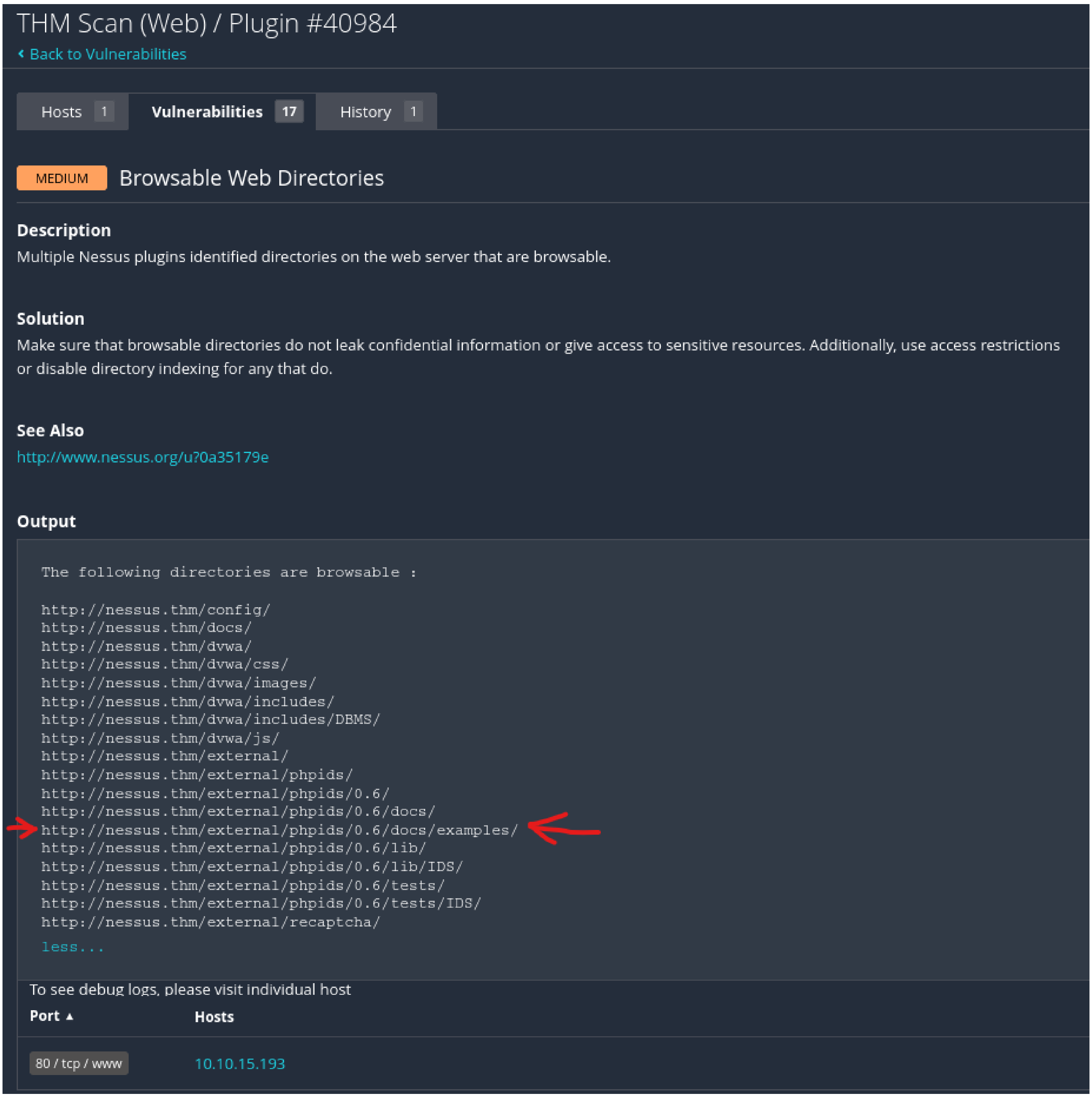


Which directory contains example documents? (This will be in a php directory)

/external/phpids/0.6/docs/examples/



☐ MEDIUM 5.3 Browsable Web Directories



THM Scan (Web) / Plugin #40984

‹ Back to Vulnerabilities

MEDIUM Browsable Web Directories

Description

Multiple Nessus plugins identified directories on the web server that are browsable.

Solution

Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

See Also

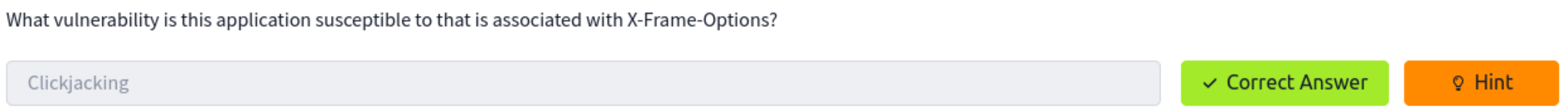
http://www.nessus.org/u?0a35179e

Output

```
The following directories are browsable :

http://nessus.thm/config/
http://nessus.thm/docs/
http://nessus.thm/dvwa/
http://nessus.thm/dvwa/css/
http://nessus.thm/dvwa/images/
http://nessus.thm/dvwa/includes/
http://nessus.thm/dvwa/includes/DBMS/
http://nessus.thm/dvwa/js/
http://nessus.thm/external/
http://nessus.thm/external/phpids/
http://nessus.thm/external/phpids/0.6/
http://nessus.thm/external/phpids/0.6/docs/
http://nessus.thm/external/phpids/0.6/docs/examples/
http://nessus.thm/external/phpids/0.6/lib/
http://nessus.thm/external/phpids/0.6/lib/IDS/
http://nessus.thm/external/phpids/0.6/tests/
http://nessus.thm/external/phpids/0.6/tests/IDS/
http://nessus.thm/external/recaptcha/
less...
```

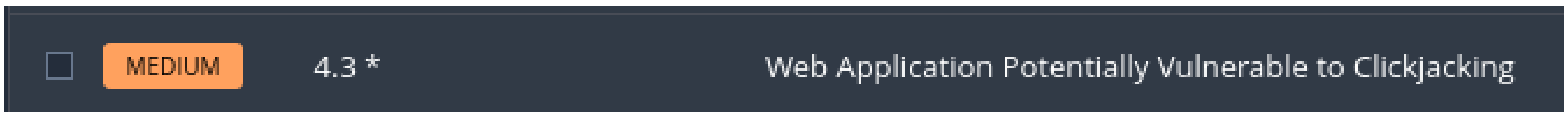
To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.15.193

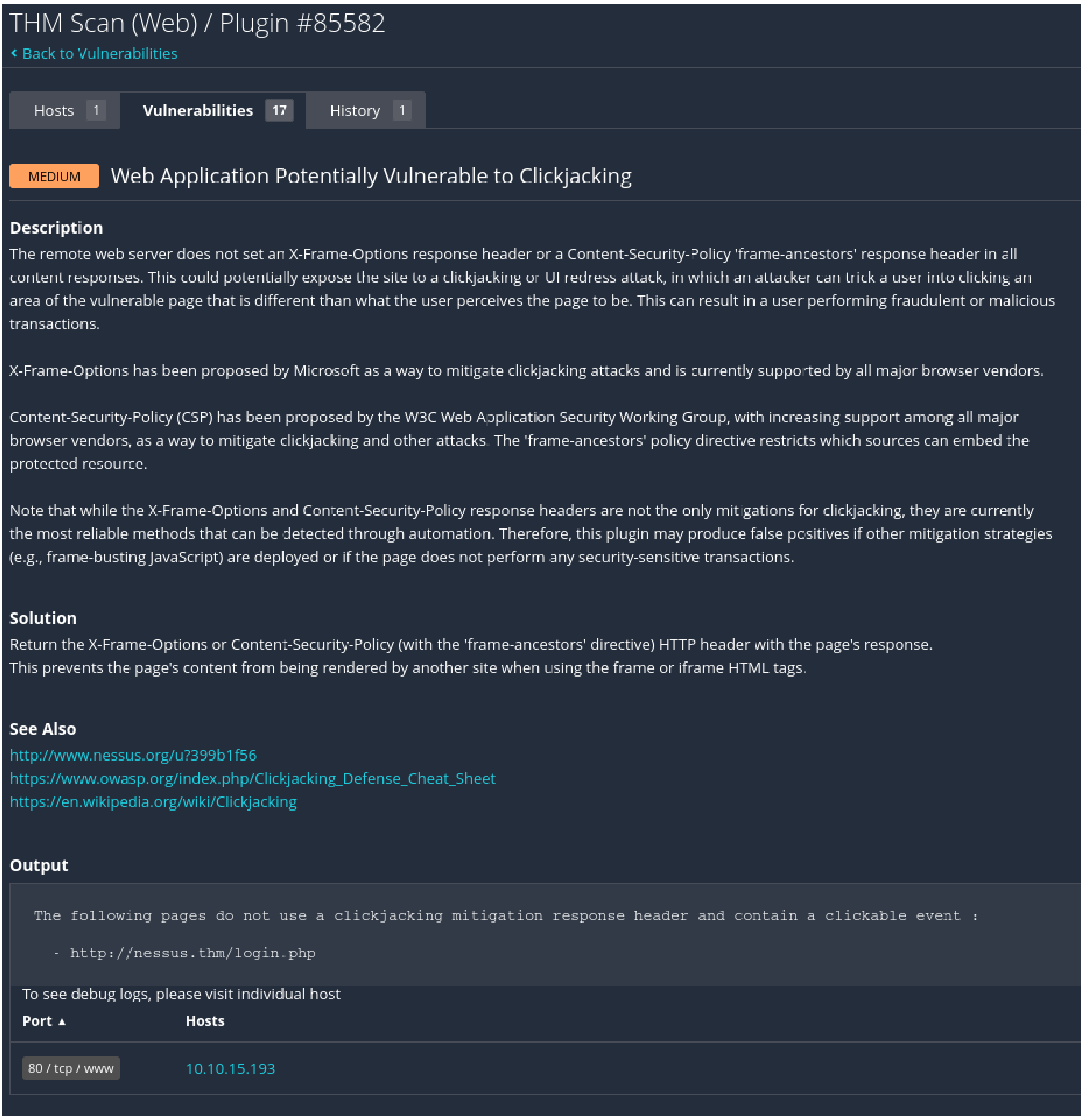


What vulnerability is this application susceptible to that is associated with X-Frame-Options?

Clickjacking



□ MEDIUM 4.3 * Web Application Potentially Vulnerable to Clickjacking



THM Scan (Web) / Plugin #85582

MEDIUM Web Application Potentially Vulnerable to Clickjacking

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.

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.

See Also

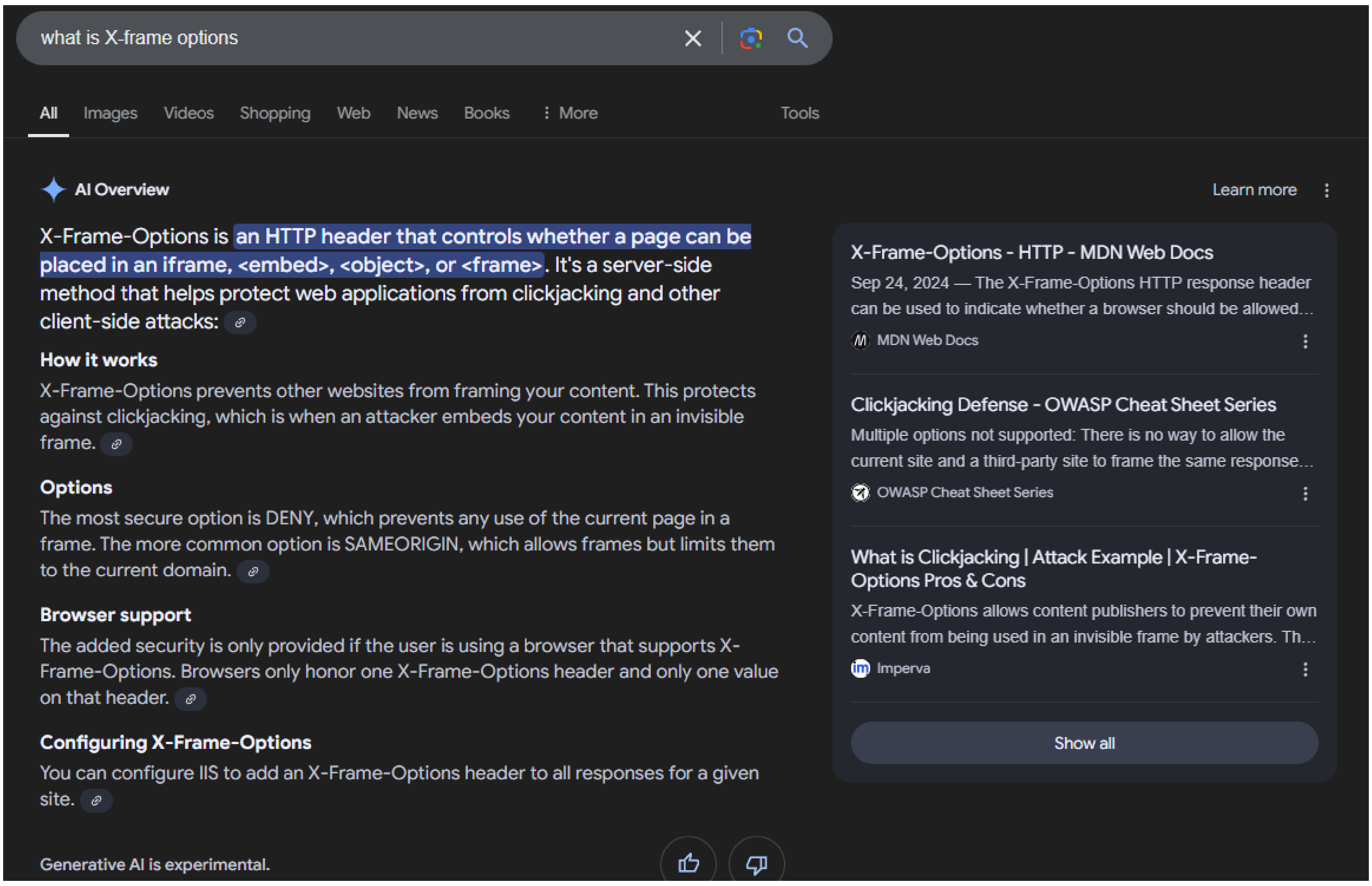
http://www.nessus.org/u?399b1f56
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
https://en.wikipedia.org/wiki/Clickjacking

Output

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

  - http://nessus.thm/login.php
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	10.10.15.193



X-Frame-Options is an HTTP header that controls whether a page can be placed in an iframe, <embed>, <object>, or <frame>. It's a server-side method that helps protect web applications from clickjacking and other client-side attacks:

How it works

X-Frame-Options prevents other websites from framing your content. This protects against clickjacking, which is when an attacker embeds your content in an invisible frame.

Options

The most secure option is DENY, which prevents any use of the current page in a frame. The more common option is SAMEORIGIN, which allows frames but limits them to the current domain.

Browser support

The added security is only provided if the user is using a browser that supports X-Frame-Options. Browsers only honor one X-Frame-Options header and only one value on that header.

Configuring X-Frame-Options

You can configure IIS to add an X-Frame-Options header to all responses for a given site.

Generative AI is experimental.

X-Frame-Options - HTTP - MDN Web Docs
Sep 24, 2024 — The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed…
MDN Web Docs

Clickjacking Defense - OWASP Cheat Sheet Series
Multiple options not supported: There is no way to allow the current site and a third-party site to frame the same response…
OWASP Cheat Sheet Series

What is Clickjacking | Attack Example | X-Frame-Options Pros & Cons
X-Frame-Options allows content publishers to prevent their own content from being used in an invisible frame by attackers. Th…
Imperva