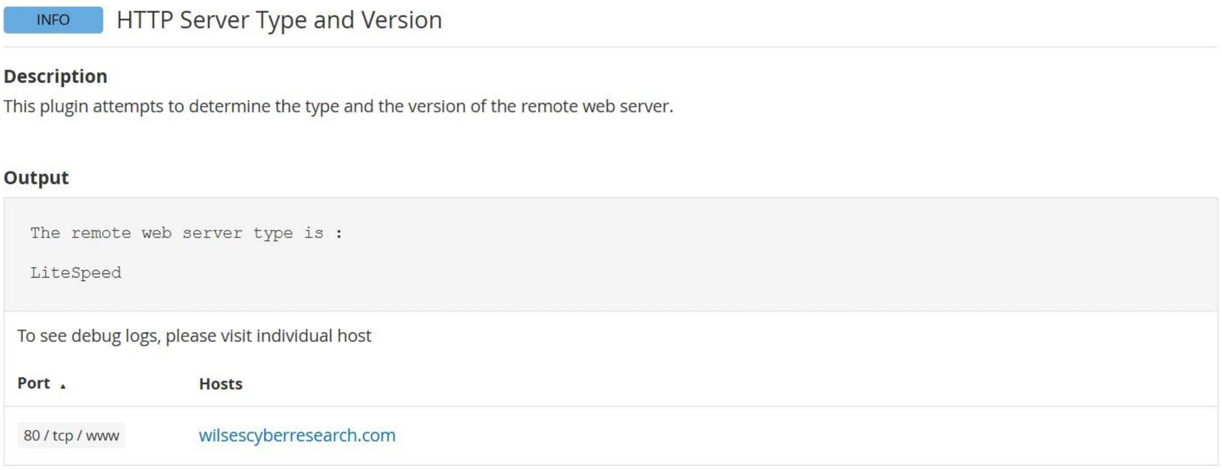
Vulnerability Scan Report of Wiles Cyberresearch.com

Prepared By : Mehrier B. Touhid



INFO 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 :

LiteSpeed
```

To see debug logs, please visit individual host

Port ▴	Hosts
80 / tcp / www	wilsescyberresearch.com

Vulnerability: HTTP Server Type and Version (LiteSpeed)

Severity: Info

Description: Nessus determined that the remote web server is running LiteSpeed, but no version or specific vulnerabilities were identified in this output. This is an informational finding used for asset inventory.

OWASP Top 10 Mapping: A06:2021 – Vulnerable and Outdated Components

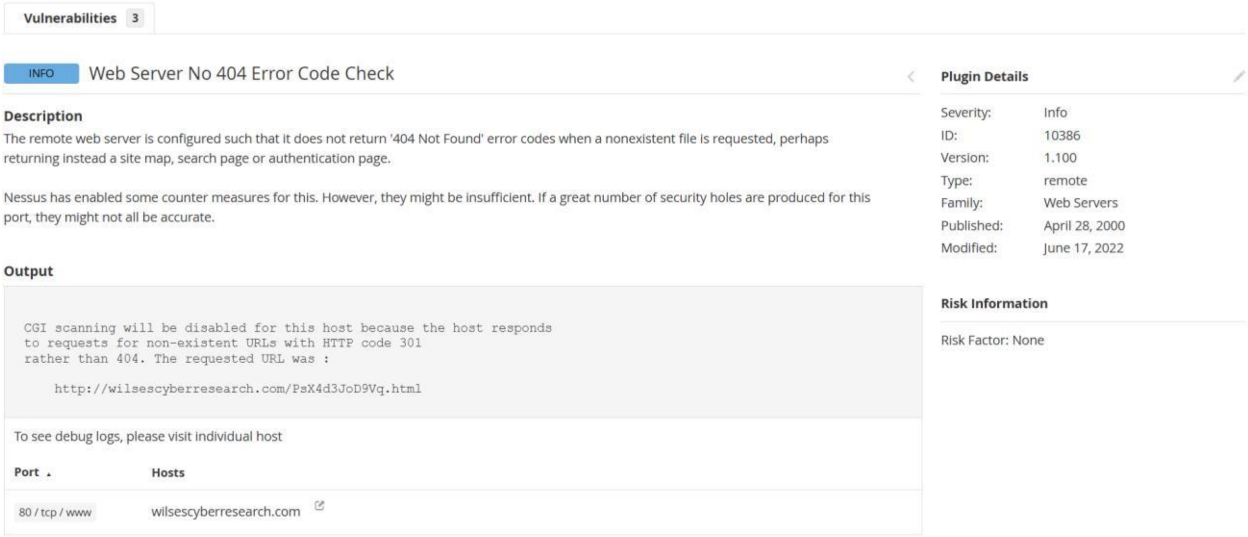
Affected System: Web server at wilsescyberresearch.com, port 80/tcp Evidence: The

plugin output states, “The remote web server type is: LiteSpeed.” Recommendation:

Verify the version of LiteSpeed in use and ensure it is up to date to mitigate risks from known vulnerabilities (e.g., check for LiteSpeed releases and patches on their official website or documentation).

Implement version hiding in the server configuration (e.g., remove or obscure the Server header in HTTP responses) to prevent attackers from identifying the software version.

Regularly audit and update all server software to prevent exploitation of outdated components.



INFO Web Server No 404 Error Code Check

Description

The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page.

Nessus has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate.

Output

```
CGI scanning will be disabled for this host because the host responds
to requests for non-existent URLs with HTTP code 301
rather than 404. The requested URL was :

    http://wilsescyberresearch.com/PsX4d3JoD9Vq.html
```

To see debug logs, please visit individual host

Port ▲	Hosts
80 / tcp / www	wilsescyberresearch.com

Plugin Details

Severity:	Info
ID:	10386
Version:	1.100
Type:	remote
Family:	Web Servers
Published:	April 28, 2000
Modified:	June 17, 2022

Risk Information

Risk Factor: None

Vulnerability: Web Server No 404 Error Code Check

Severity: Info

Description: The web server is configured to return HTTP 301 (Moved Permanently) for non-existent URLs instead of the standard 404 (Not Found) error code, potentially masking issues or complicating vulnerability scans. Nessus notes that scanning may be disabled for this host due to this behavior.

OWASP Top 10 Mapping: A05:2021 – Security Misconfiguration (potential alignment, as this could indicate a misconfiguration impacting security visibility)

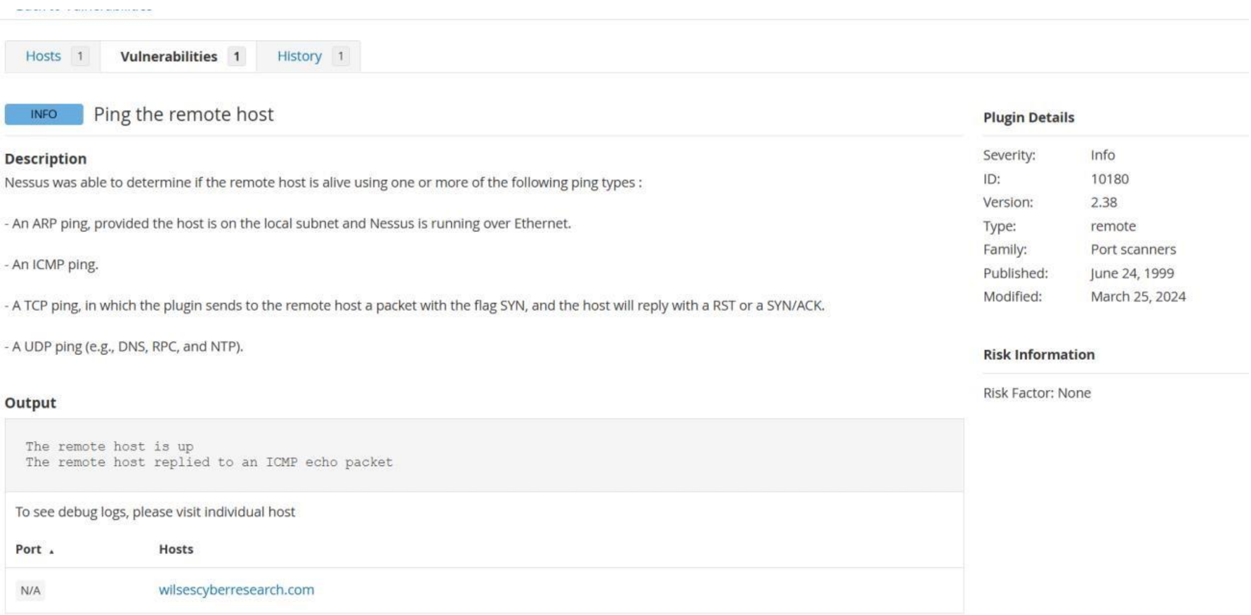
Affected System: Web server at wilsescyberresearch.com, port 80/tcp

Evidence: The output shows, "HTTP scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404." Recommendation:

Configure the web server to return appropriate 404 responses for non-existent resources to improve security scanning accuracy and prevent confusion with legitimate redirects.

Review and standardize HTTP error handling to ensure consistency and alignment with security best practices.

Test the server’s response with tools like curl or Postman to verify proper error code behavior.



Ping the remote host

Description

Nessus was able to determine if the remote host is alive using one or more of the following ping types :

- An ARP ping, provided the host is on the local subnet and Nessus is running over Ethernet.

- An ICMP ping.

- A TCP ping, in which the plugin sends to the remote host a packet with the flag SYN, and the host will reply with a RST or a SYN/ACK.

- A UDP ping (e.g., DNS, RPC, and NTP).

Output

```
The remote host is up
The remote host replied to an ICMP echo packet
```

To see debug logs, please visit individual host

Port ▲	Hosts
N/A	wilsescyberresearch.com

Plugin Details

Severity:	Info
ID:	10180
Version:	2.38
Type:	remote
Family:	Port scanners
Published:	June 24, 1999
Modified:	March 25, 2024

Risk Information

Risk Factor: None

Vulnerability: Ping the Remote Host

Severity: Info

Description: Nessus confirmed the remote host is alive using an ICMP echo packet, indicating the host is responsive. This is an informational finding for network mapping and asset discovery.

OWASP Top 10 Mapping: Not directly applicable (informational only, no specific web application risk)

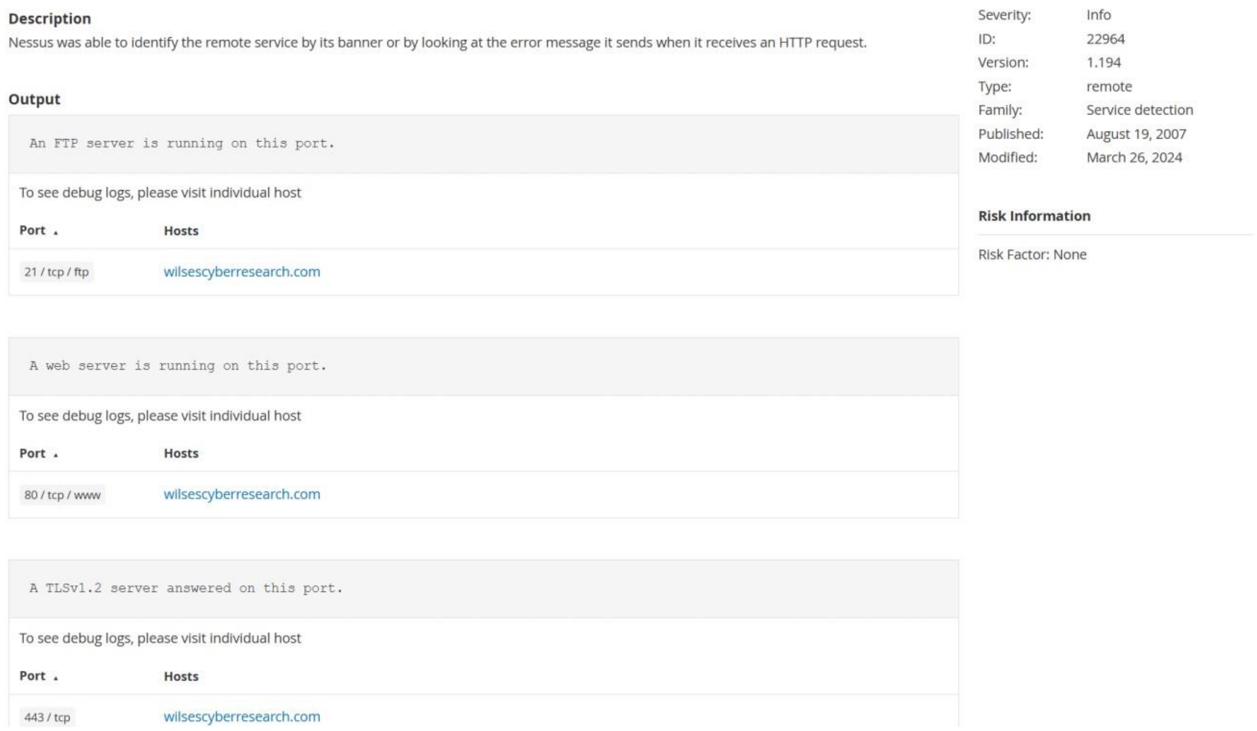
Affected System: wilsescyberresearch.com, no specific port (N/A)

Evidence: The output states, “The remote host is up. The remote host replied to an ICMP echo packet.”

Recommendation:

If ICMP responses are not required for legitimate operations, consider disabling ICMP echo replies on the host or network to reduce visibility to attackers (e.g., configure firewall rules to block ICMP unless necessary).

Regularly monitor network traffic to detect unauthorized pings or scans.



Description

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

Output

```
An FTP server is running on this port.
```

To see debug logs, please visit individual host

Port ▴	Hosts
21 / tcp / ftp	wilsescyberresearch.com

```
A web server is running on this port.
```

To see debug logs, please visit individual host

Port ▴	Hosts
80 / tcp / www	wilsescyberresearch.com

```
A TLSv1.2 server answered on this port.
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / tcp	wilsescyberresearch.com

Severity:	Info
ID:	22964
Version:	1.194
Type:	remote
Family:	Service detection
Published:	August 19, 2007
Modified:	March 26, 2024

Risk Information

Risk Factor: None

Vulnerability: Service Detection (FTP, Web Server, TLSv1.2)

Severity: Info

Description: Nessus identified multiple services running on the host: an FTP server on port 21/tcp, a web server on port 80/tcp, and a TLSv1.2 server on port 443/tcp. These are informational findings for asset inventory and service enumeration.

OWASP Top 10 Mapping: A06:2021 – Vulnerable and Outdated Components (potential alignment, depending on the versions of FTP, web server, or TLS configuration)

Affected System: wilsescyberresearch.com on ports 21/tcp, 80/tcp, and 443/tcp

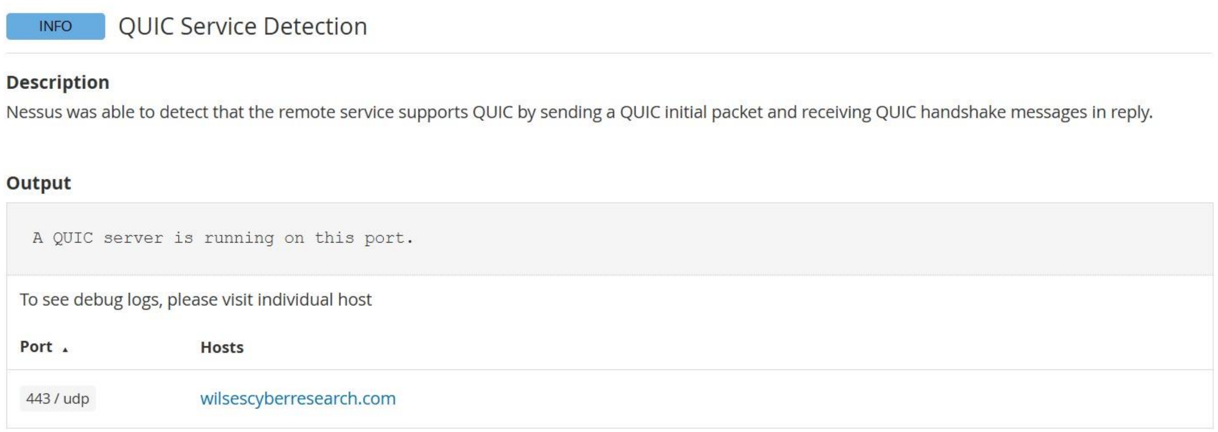
Evidence: The output states: “An FTP server is running on this port,” “A web server is running on this port,” and “A TLSv1.2 server answered on this port.” Recommendation:

Verify the versions of the FTP, web server (LiteSpeed), and TLS implementations, ensuring they are up to date and patched against known vulnerabilities.

Disable TLSv1.2 if not required, and enforce TLS 1.3 for stronger encryption and security (e.g., update LiteSpeed configuration to disable older protocols).

Restrict access to the FTP server to authorized users only, using strong authentication (e.g., SSHbased FTP or SFTP) and firewall rules to limit exposure.

Hide or obscure service banners (FTP, HTTP headers) to reduce information disclosure to attackers.



INFO QUIC Service Detection

Description

Nessus was able to detect that the remote service supports QUIC by sending a QUIC initial packet and receiving QUIC handshake messages in reply.

Output

```
 A QUIC server is running on this port.
```

To see debug logs, please visit individual host

Port ▴	Hosts
443 / udp	wilsescyberresearch.com

Vulnerability: QUIC Service Detection

Severity: Info

Description: Nessus detected that the remote service supports QUIC (Quick UDP Internet Connections) by sending a QUIC initial packet and receiving QUIC handshake messages in reply. This is an informational finding indicating the presence of a QUIC server.

OWASP Top 10 Mapping: A05:2021 – Security Misconfiguration (potential alignment, as QUIC implementation may require proper configuration to avoid exposure or vulnerabilities)

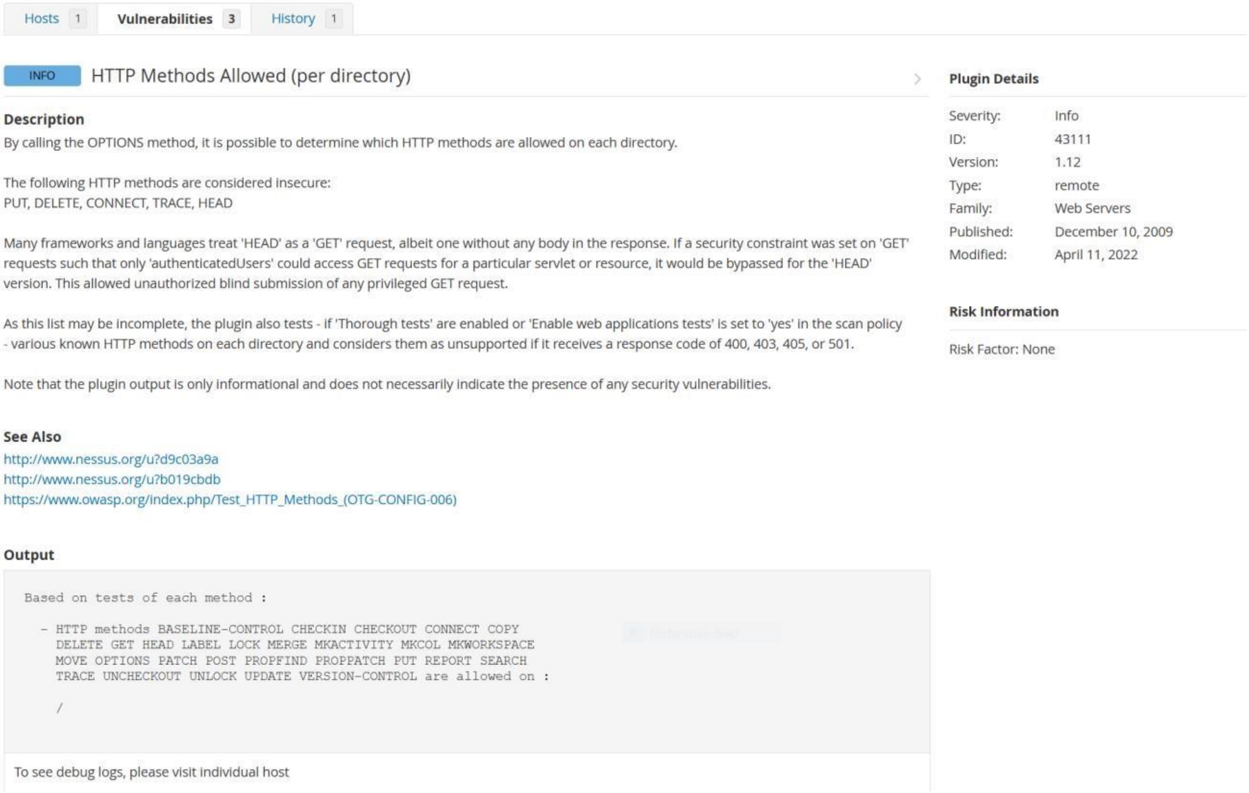
Affected System: Web server at wilsescyberresearch.com, port 443/udp

Evidence: The output states, “A QUIC server is running on this port.” Recommendation:

Verify the QUIC implementation (e.g., in LiteSpeed or another service) and ensure it is configured securely, using the latest protocols and patches.

Monitor QUIC traffic for unusual activity, as QUIC’s encryption can obscure malicious behavior if not properly managed.

Restrict QUIC access to authorized users or networks if not needed for public-facing services, using firewalls or network policies.



HTTP Methods Allowed (per directory)

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)

Output

```
Based on tests of each method :

  - HTTP methods BASELINE-CONTROL CHECKIN CHECKOUT CONNECT COPY
    DELETE GET HEAD LABEL LOCK MERGE MKACTIVITY MKCOL MKWORKSPACE
    MOVE OPTIONS PATCH POST PROPFIND PROPPATCH PUT REPORT SEARCH
    TRACE UNCHECKOUT UNLOCK UPDATE VERSION-CONTROL are allowed on :

    /
```

To see debug logs, please visit individual host

Plugin Details

Severity:	Info
ID:	43111
Version:	1.12
Type:	remote
Family:	Web Servers
Published:	December 10, 2009
Modified:	April 11, 2022

Risk Information

Risk Factor: None

Vulnerability: HTTP Methods Allowed (per directory)

Severity: Info

Description: Nessus identified that the web server allows several HTTP methods (e.g., PUT, DELETE, CONNECT, TRACE, HEAD, and others) on the root directory (/), some of which are considered insecure. This is an informational finding, but it could indicate potential misconfigurations or unnecessary exposure.

OWASP Top 10 Mapping: A05:2021 – Security Misconfiguration (potential alignment, as enabling unnecessary or insecure HTTP methods can increase the attack surface)

Affected System: Web server at wilsescyberresearch.com, port 80/tcp

Evidence: The output lists allowed methods like "PUT, DELETE, CONNECT, TRACE, HEAD" among others, noted as potentially insecure.

Recommendation:

Disable unnecessary or insecure HTTP methods (e.g., PUT, DELETE, CONNECT, TRACE) unless explicitly required for application functionality. Configure the server to restrict methods to only GET, POST, and HEAD where appropriate.

Use server configuration files (e.g., LiteSpeed's httpd.conf or .htaccess for Apache compatibility) to limit allowed methods, such as LimitExcept GET POST for Apache/Nginx-like directives.

Regularly review and audit HTTP method permissions to minimize the attack surface and prevent exploitation (e.g., TRACE for cross-site tracing attack