WAS Scan Report

Qualys. Enterprise

Scan Report

18 Apr 2023

Vulnerabilities of all selected scans are consolidated into one report so that you can view their evolution.

Nicholas Teney
naafs3nt

NOAA
1315 East West Highway, Room 3428
silver spring, Maryland 20910
United States of America

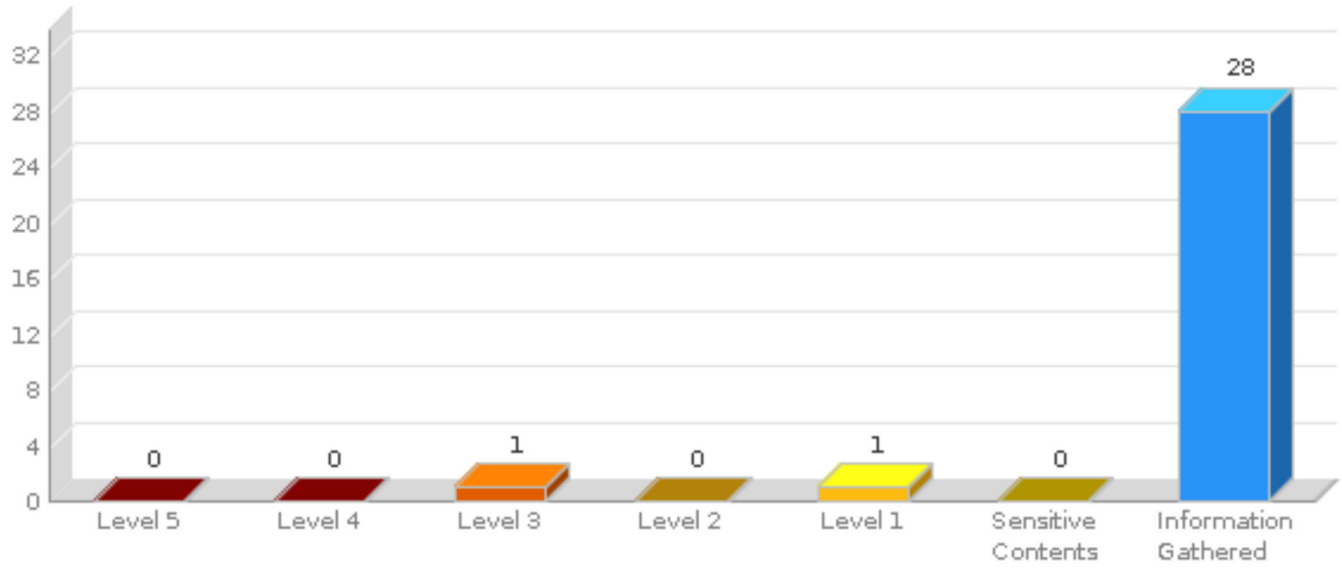
Target and Filters

Scans (1)	**Web Application Vulnerability Scan - PIFSC_4960_picahi.nmfs.local - 2023-04-14**
Web Applications (1)	**PIFSC_4960_picahi.nmfs.local**

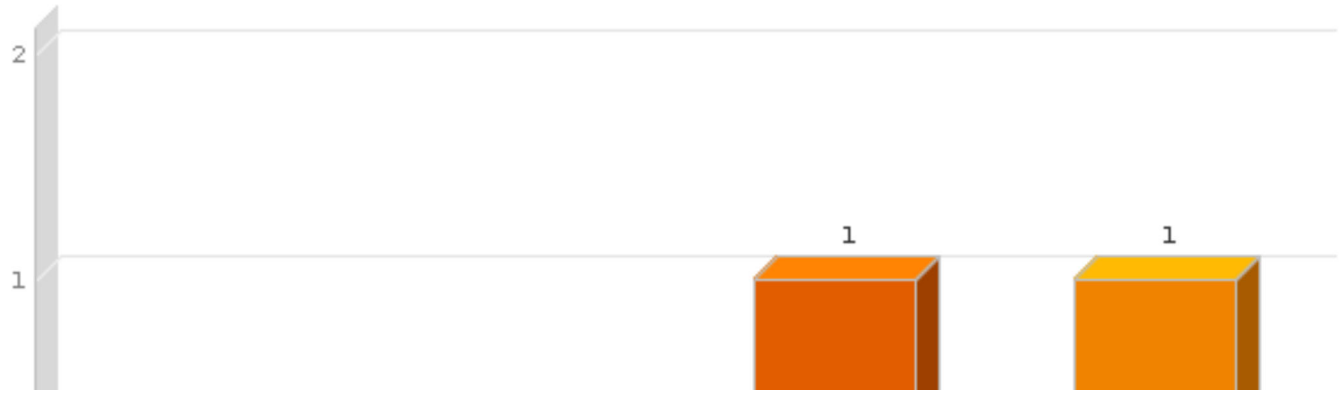
Summary

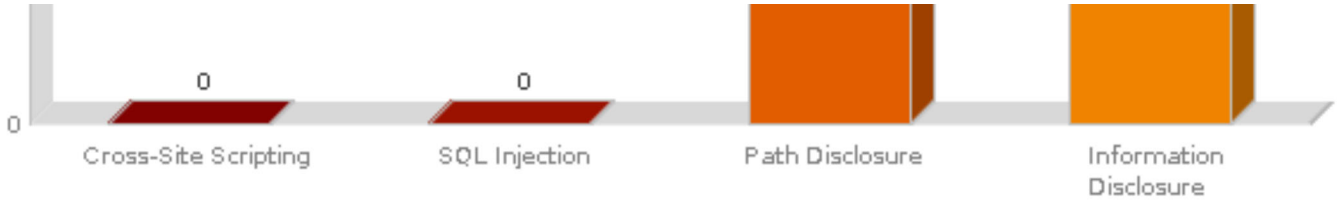
Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
MED	2	0	28

Findings by Severity

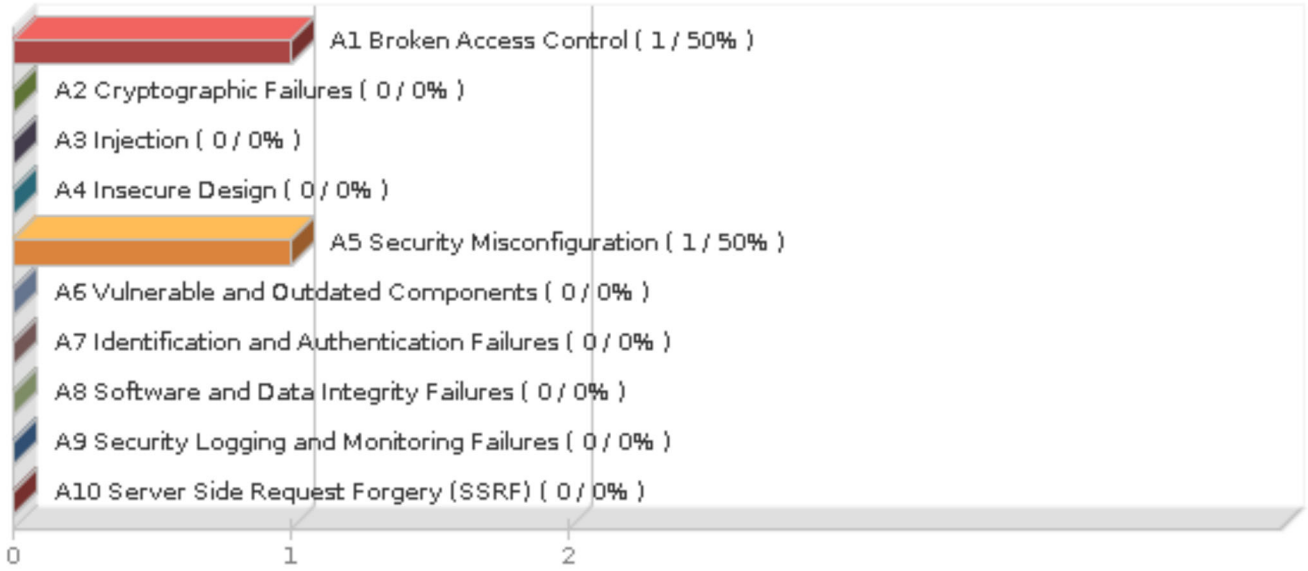


Vulnerabilities by Group





OWASP Top 10 2021 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Web Application Vulnerability Scan - PIFSC_4960_picahi.nmfs.local - 2023-04-14	14 Apr 2023 09:34 GMT-1000	0	0	1	0	1	0	28

Results (30)

Vulnerability (2)

Path Disclosure (1)

150246 Path-relative stylesheet import (PRSSI) vulnerability (1)

150246 Path-relative stylesheet import (PRSSI) vulnerability

URL: https://picahi.nmfs.local/pirri

Finding #	**20706970** (230455657)	**Severity**	Confirmed Vulnerability - Level 1
Unique #	**5aa856a3-a92b-441a-af9f-3a7b4505a8d6**		
Group	Path Disclosure	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-23		
OWASP	A1 Broken Access Control		
WASC	-		
CVSS V3 Base	3.1	**CVSS V3 Temporal** 2.9	**CVSS V3 Attack Vector** Network

Details

Threat

Relative URLs can be dangerous since browser may not determine the correct directory. If the HTML uses path-relative CSS links, it may be susceptible to path-relative stylesheet import (PRSSI) vulnerabilities. This could allow an attacker to take advantage of CSS imports with relative URLs by overwriting their target file.

References:
Evil CSS Injection
Relative Path Overwrite Attack
Research paper: Large-Scale Analysis of Style Injection by Relative Path Overwrite

Impact

An attacker may trick browsers into importing JavaScript or HTML code as a stylesheet. This has been shown to enable a number of different attacks, including cross-site scripting (XSS) and exfiltration of CSRF tokens.

Solution

It is recommended to use absolute URLs for CSS imports. Alternately you can add the HTML "base" tag in the document which defines the base URL or target

location for all the relative URLs.

The vulnerability can also be mitigated by using the following best practices to harden the web pages:

- Set a DOCTYPE which does not allow Quirks mode as explained at https://hsivonen.fi/doctype/
- Set response header X-Frame-Options: deny
- Set response header X-Content-Type-Options: nosniff.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

```
GET https://picahi.nmfs.local/pirri
Referer: https://picahi.nmfs.local/pirri
Host: picahi.nmfs.local
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1
Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
Relative Path CSS Links found:
<link href="./res/css/template.css" rel="stylesheet" type="text/css">
<link href="./res/css/tooltip.css" rel="stylesheet" type="text/css">
<link href="./php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css" rel="stylesheet" type="text/css">
<link href="./res/css/index.css" rel="stylesheet" type="text/css">
```

Information Disclosure (1)

150124 Clickjacking - Framable Page (1)

150124 Clickjacking - Framable Page

URL: https://picahi.nmfs.local/pirri

Finding #	**20706968** (230455656)	**Severity**	Confirmed Vulnerability - Level 3
Unique #	**12b31812-dff5-42fb-bf8f-1017ec64b83c**		
Group	Information Disclosure	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-451		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		
CVSS V3 Base	5.8	**CVSS V3 Temporal** 5.5	**CVSS V3 Attack Vector** Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.
Note: Only 10 pages are reported for this QID similar to 150245 Missing header: X-Frame-Options

Impact

With clickjacking, an attacker can trick a victim user into clicking an invisible frame on the web page, thereby causing the victim to take an action they did not intend to take.

Solution

Clickjacking prevention mechanisms include:
- X-Frame-Options: This HTTP response header can be used to prevent framing of web pages.
- Content-Security-Policy: The 'frame-ancestors' directive can be used to prevent framing of web pages.
- Framekiller JavaScript code designed to prevent a malicious user from framing the page. This method is not recommended due to its unreliability.

See the OWASP Clickjacking Defense Cheat Sheet for more information.
To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.

Payloads

#1 Request

```
GET https://picahi.nmfs.local/pirri
Host: picahi.nmfs.local
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_5) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.1.1
Safari/605.1.15
Accept: */*
```

Click this link to try to reproduce the vulnerability using above payload.Note that clicking this link may not lead to visible results, either because the vulnerability requires context to be previously set (authentication, cookies...) or because the exploitation of the vulnerability does not lead to any visible proof.

#1 Response

```
The URI was framed.
```

Information Gathered (28)

Scan Diagnostics (18)

45017 Operating System Detected (1)

45017 Operating System Detected

Finding #	**9473827** (230455645)	**Severity**	Information Gathered - Level 2
Unique #	**775ab371-62ff-4f6c-a7ff-0ae5ab7fb8e1**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Several different techniques can be used to identify the operating system (OS) running on a host. A short description of these techniques is provided below. The specific technique used to identify the OS on this host is included in the RESULTS section of your report.

1) **TCP/IP Fingerprint**: The operating system of a host can be identified from a remote system using TCP/IP fingerprinting. All underlying operating system TCP/IP stacks have subtle differences that can be seen in their responses to specially-crafted TCP packets. According to the results of this "fingerprinting" technique, the OS version is among those listed below.

Note that if one or more of these subtle differences are modified by a firewall or a packet filtering device between the scanner and the host, the fingerprinting technique may fail. Consequently, the version of the OS may not be detected correctly. If the host is behind a proxy-type firewall, the version of the operating system detected may be that of the firewall instead of the host being scanned.

2) **NetBIOS**: Short for Network Basic Input Output System, an application programming interface (API) that augments the DOS BIOS by adding special functions for local-area networks (LANs). Almost all LANs for PCs are based on the NetBIOS. Some LAN manufacturers have even extended it, adding additional network capabilities. NetBIOS relies on a message format called Server Message Block (SMB).

3) **PHP Info**: PHP is a hypertext pre-processor, an open-source, server-side, HTML-embedded scripting language used to create dynamic Web pages. Under some configurations it is possible to call PHP functions like phpinfo() and obtain operating system information.

4) **SNMP**: The Simple Network Monitoring Protocol is used to monitor hosts, routers, and the networks to which they attach. The SNMP service maintains Management Information Base (MIB), a set of variables (database) that can be fetched by Managers. These include "MIB_II.system.sysDescr" for the operating system.

Impact

Not applicable.

Solution

Not applicable.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	10.18.17.175
Port	-
Result	Linux_2.6 TCP/IP_Fingerprint U6835:443

Info List

Info #1

150018 Connection Error Occurred During Web Application Scan (1)

150018 Connection Error Occurred During Web Application Scan

Finding #	**9473805** (230455628)	**Severity**	Information Gathered - Level 2
Unique #	**c645c91a-b044-4b11-b4c9-1ca53779e47d**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following are some of the possible reasons for the timeouts or connection errors:

1. A disturbance in network connectivity between the scanner and the web application occurred.
2. The web server or application server hosting the application was taken down in the midst of a scan.
3. The web application experienced an overload, possibly due to load generated by the scan.
4. An error occurred in the SSL/TLS handshake (applies to HTTPS web applications only).
5. A security device, such as an IDS/IPS or web application firewall (WAF), began to drop or reject the HTTP connections from the scanner.
6. Very large files like PDFs, videos, etc. are present on the site and caused timeouts when accessed by the scanner.

Impact

Some of the links were not crawled or scanned. Results may be incomplete or incorrect.

Solution

First, confirm that the server was not taken down in the midst of the scan. After that, investigate the root cause by reviewing the listed links and examining web server logs, application server logs, or IDS/IPS/WAF logs. If the errors are caused due to load generated by the scanner then try reducing the scan intensity (this could increase the scan duration). If the errors are due to specific URLs being tested by the scanner or due to specific form data sent by the scanner, then configure exclude lists in the scan configuration as needed to avoid such requests. If timeouts or connection errors are a persistent issue but you want the scan to run to completion, change the Behavior Settings in the option profile to increase the error thresholds or disable the error checks entirely.

Results

```
Total number of unique links that encountered timeout errors: 1
Links with highest number of timeouts:
1 http://picahi.nmfs.local/pirri

Phase wise summary of timeout and connection errors encountered:
ePhaseCrawl : 1 0
```

6 DNS Host Name (1)

6 DNS Host Name

Finding #	**9473826** (230455634)	**Severity**	Information Gathered - Level 1
Unique #	**585f054e-6945-43d1-9863-0aa3dcedafd2**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The fully qualified domain name of this host, if it was obtained from a DNS server, is displayed in the RESULT section.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	-
IP	10.18.17.175
Port	-
Result	#table IP_address Host_name 10.18.17.175 picahi.nmfs.local

38116 SSL Server Information Retrieval (1)

38116 SSL Server Information Retrieval

Finding #	**9473832** (230455653)	**Severity**	Information Gathered - Level 1
Unique #	**d52493af-7f2f-4861-a840-585746fc4e34**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of supported SSL ciphers.

Note: If a cipher is included in this list it means that it was possible to establish a SSL connection using that cipher. There are some web servers setups that allow connections to be established using a LOW grade cipher, only to provide a web page stating that the URL is accessible only through a non-LOW grade cipher. In this case even though LOW grade cipher will be listed here QID 38140 will not be reported.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _ _ _ _ _ _ SSLv3_PROTOCOL_IS_DISABLED _ _ _ _ _ _ TLSv1_PROTOCOL_IS_DISABLED _ _ _ _ _ _ TLSv1.1_PROTOCOL_IS_DISABLED _ _ _ _ _ _ TLSv1.2_PROTOCOL_IS_ENABLED _ _ _ _ _ _ TLSv1.2 COMPRESSION_METHOD None _ _ _ DHE-RSA-AES128-SHA256 DH RSA SHA256 AES(128) MEDIUM DHE-RSA-AES256-SHA256 DH RSA SHA256 AES(256) HIGH AES128-GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH DHE-RSA-AES128-GCM-SHA256 DH RSA AEAD AESGCM(128) MEDIUM DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDIUM ECDHE-RSA-AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM AES256-SHA256 RSA RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_DISABLED _ _ _ _ _

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
DHE-RSA-AES128-SHA256	RSA	AES(128)	MEDIUM	DH	SHA256	TLSv1.2
DHE-RSA-AES256-SHA256	RSA	AES(256)	HIGH	DH	SHA256	TLSv1.2
AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	RSA	AEAD	TLSv1.2
AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	RSA	AEAD	TLSv1.2
DHE-RSA-AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	DH	AEAD	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	DH	AEAD	TLSv1.2
ECDHE-RSA-AES128-SHA256	RSA	AES(128)	MEDIUM	ECDH	SHA256	TLSv1.2
ECDHE-RSA-AES256-SHA384	RSA	AES(256)	HIGH	ECDH	SHA384	TLSv1.2
ECDHE-RSA-AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	ECDH	AEAD	TLSv1.2
ECDHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	ECDH	AEAD	TLSv1.2
AES128-SHA256	RSA	AES(128)	MEDIUM	RSA	SHA256	TLSv1.2
AES256-SHA256	RSA	AES(256)	HIGH	RSA	SHA256	TLSv1.2

38291 SSL Session Caching Information (1)

38291 SSL Session Caching Information

Finding #	**9473829** (230455650)	**Severity**	Information Gathered - Level 1
Unique #	**fb328906-73b5-490e-bbaa-bec33b95dbf0**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		

OWASP	-
WASC	-

Details

Threat

SSL session is a collection of security parameters that are negotiated by the SSL client and server for each SSL connection. SSL session caching is targeted to reduce the overhead of negotiations in recurring SSL connections. SSL sessions can be reused to resume an earlier connection or to establish multiple simultaneous connections. The client suggests an SSL session to be reused by identifying the session with a Session-ID during SSL handshake. If the server finds it appropriate to reuse the session, then they both proceed to secure communication with already known security parameters.

This test determines if SSL session caching is enabled on the host.

Impact

SSL session caching is part of the SSL and TLS protocols and is not a security threat. The result of this test is for informational purposes only.

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	TLSv1.2 session caching is enabled on the target.

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)

38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance

Finding #	**9473831** (230455652)	**Severity**	Information Gathered - Level 1
Unique #	**9fe9ec27-6cfe-46d2-8565-ca4c97e59e63**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL/TLS protocols have different version that can be supported by both the client and the server. This test attempts to send invalid protocol versions to the target in order to find out what is the target's behavior. The results section contains a table that indicates what was the target's response to each of our tests.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods (1)

38704 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Key Exchange Methods

Finding #	**9473833** (230455654)	**Severity**	Information Gathered - Level 1
Unique #	**83ec4f94-7e1d-4a74-8053-7a8abe4ff04b**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of SSL/TLS key exchange methods supported by the server, along with their respective key sizes, strengths and ciphers.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	#table cols="7" CIPHER NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ _ AES256-SHA256 RSA _ 2048 no 110 low AES128-SHA256 RSA _ 2048 no 110 low AES256-GCM-SHA384 RSA _ 2048 no 110 low AES128-GCM-SHA256 RSA _ 2048 no 110 low DHE-RSA-AES256-GCM-SHA384 DHE _ 2048 yes 110 low DHE-RSA-AES128-GCM-SHA256 DHE _ 2048 yes 110 low DHE-RSA-AES256-SHA256 DHE _ 2048 yes 110 low DHE-RSA-AES128-SHA256 DHE _ 2048 yes 110 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE secp256k1 256 yes 128 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE secp256k1 256 yes 128 low ECDHE-RSA-AES256-SHA384 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-SHA384 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-SHA384 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES256-SHA384 ECDHE secp256k1 256 yes 128 low ECDHE-RSA-AES128-SHA256 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-SHA256 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-SHA256 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES128-SHA256 ECDHE secp256k1 256 yes 128 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
RSA		TLSv1.2	2048	no	110	low
RSA		TLSv1.2	2048	no	110	low
RSA		TLSv1.2	2048	no	110	low
RSA		TLSv1.2	2048	no	110	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	2048	yes	110	low
DHE		TLSv1.2	2048	yes	110	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	256	yes	128	low

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Protocol Properties (1)

38706 Secure Sockets Layer/Transport Layer Security (SSL/TLS)

Protocol Properties

Finding #	**9473834** (230455655)	**Severity**	Information Gathered - Level 1
Unique #	**37de33e7-4f24-4d3b-a525-9077fa0ab665**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The following is a list of detected SSL/TLS protocol properties.

Impact

Items include:

- Extended Master Secret: indicates whether the extended_master_secret extension is supported or required by the server. This extension enhances security and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Encrypt Then MAC: indicates whether the encrypt_then_mac extension is supported or required by the server. This extension enhances the security of non-AEAD ciphers and is recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Heartbeat: indicates whether the heartbeat extension is supported. It is not recommended to enable this, except for DTLS. Applicable to TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2
- Truncated HMAC: indicates whether the truncated_hmac extension is supported. This can degrade security and is not recommended. Applicable to TLSv1, TLSv1.1, TLSv1.2, DTLSv1, DTLSv1.2
- Cipher priority: indicates whether client, server or both determine the priority of ciphers. Having the server determine the priority is recommended. Applicable to SSLv3, TLSv1, TLSv1.1, TLSv1.2, TLSv1.3, DTLSv1, DTLSv1.2

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret no Encrypt_Then_MAC no Heartbeat yes Truncated_HMAC no Cipher_priority_controlled_by client OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	no	TLSv1.2
Encrypt Then MAC	no	TLSv1.2
Heartbeat	yes	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	client	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2

42350 TLS Secure Renegotiation Extension Support Information (1)

42350 TLS Secure Renegotiation Extension Support Information

Finding #	**9473830** (230455651)	**Severity**	Information Gathered - Level 1
Unique #	**98c7de6b-6ed2-4a7e-b701-e6f7652dcf78**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Secure Socket Layer (SSL) and Transport Layer Security (TLS) renegotiation are vulnerable to an attack in which the attacker forms a TLS connection with the target server, injects content of his choice, and then splices in a new TLS connection from a client. The server treats the client's initial TLS handshake as a renegotiation and thus believes that the initial data transmitted by the attacker is from the same entity as the subsequent client data. TLS protocol was extended to cryptographically tierenegotiations to the TLS connections they are being performed over. This is referred to as TLS secure renegotiation extension. This detection determines whether the TLS secure renegotiation extension is supported by the server or not.

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

45038 Host Scan Time - Scanner (1)

45038 Host Scan Time - Scanner

Finding #	**9473818** (230455641)	**Severity**	Information Gathered - Level 1
Unique #	**6c31088b-98e9-4043-994b-c5525e5db002**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Host Scan Time is the period of time it takes the scanning engine to perform the vulnerability assessment of a single target host. The Host Scan Time for this host is reported in the Result section below.

The Host Scan Time does not have a direct correlation to the Duration time as displayed in the Report Summary section of a scan results report. The Duration is the period of time it takes the service to perform a scan task. The Duration includes the time it takes the service to scan all hosts, which may involve parallel scanning. It also includes the time it takes for a scanner appliance to pick up the scan task and transfer the results back to the service's Secure Operating Center. Further, when a scan task is distributed across multiple scanners, the Duration includes the time it takes to perform parallel host scanning on all scanners.

Impact

N/A

Solution

N/A

Results

```
Scan duration: 3091 seconds

Start time: Fri, Apr 14 2023, 19:34:05 GMT

End time: Fri, Apr 14 2023, 20:25:36 GMT
```

86002 SSL Certificate - Information (1)

86002 SSL Certificate - Information

Finding #	**9473828** (230455649)	**Severity**	Information Gathered - Level 1
Unique #	**7d602ad1-ee0c-4d03-83cc-e84c36b8944d**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
SSL certificate information is provided in the Results section.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	picahi.nmfs.local
IP	10.18.17.175
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number 45739_(0xb2ab) (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName U.S._Government _organizationalUnitName DoD _organizationalUnitName PKI _commonName DOD_SW_CA-66 (0)SUBJECT_NAME _ countryName US _organizationName U.S._Government _organizationalUnitName DoD _organizationalUnitName PKI _organizationalUnitName DISA _commonName picahi.nmfs.local (0)Valid_From Mar_20_19:31:00_2023_GMT (0)Valid_Till Mar_20_19:31:00_2026_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:ac:11:fc:e5:51:28:7e:ae:1a:cb:9d:06:29:29: (0) _82:b9:a4:df:8a:57:9e:37:a0:be:3e:00:ff:2c:e7: (0) _19:85:6c:c1:be:cf:3d:9f:48:e3:24:f8:0f:9b:86: (0) _1a:4f:82:87:09:27:96:3a:4f:20:da:f2:e3:ef:3c: (0) _e9:bc:6b:c0:68:5c:40:fc:5d:2a:a4:7d:8d:64:91: (0) _f5:5d:8f:f5:52:ff:f7:9d:bc:bd:79:47:a8:13:9f: (0) _7e:1b:c8:38:cc:ab:9f:80:2d:d9:df:68:53:81:b3: (0) _32:9c:66:60:a0:da:ca:b3:58:e0:09:23:03:ff:30: (0) _f9:22:12:8b:42:90:07:56:01:fd:f2:4d:3d:5e:ec: (0) _f2:b7:65:31:14:64:03:bd:1d:f4:a1:c0:97:24:60: (0) _74:7d:7b:16:25:c3:88:df:a4:cb:d9:d1:5c:eb:87: (0) _1a:85:6f:0a:8f:ff:77:5b:f9:67:73:c3:03:5b:c3: (0) _8c:25:c2:b5:3e:64:c3:18:c4:77:37:82:81:9c:5c: (0) _ae:97:5c:7b:b7:ff:b7:bb:cf:e9:67:81:ea:6f:81: (0) _32:f1:95:b8:f5:b3:13:47:51:e5:e1:59:c8:4a:2d: (0) _78:26:66:42:94:01:40:6f:6f:58:43:c7:88:97:d4: (0) _a9:d1:3e:c2:7b:3a:d8:7a:71:8f:f4:83:24:50:c9: (0) _f5:31 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Authority_Key_Identifier _keyid:EB:06:53:98:30:86:9E:DF:5E:8B:0B:A1:26:26:FA:A6:61:0F:B9:94 (0)X509v3_Subject_Key_Identifier _05:12:EE:3D:72:C8:27:29:20:3B:7E:52:A1:86:1E:88:3C:FF:C6:77 (0)Authority_Information_Access _CA_Issuers_-_URI:http://crl.disa.mil /sign/DODSWCA_66.cer (0) _OCSP_-_URI:http://ocsp.disa.mil (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.disa.mil/crl/DODSWCA_66.crl (0)X509v3_Subject_Alternative_Name _DNS:picahi.nmfs.local (0)X509v3_Certificate_Policies _Policy:_2.16.840.1.101.2.1.11.39 (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication,_1.3.6.1.5.5.8.2.2 (0)Signature (256_octets) (0) 09:82:a4:2f:10:0e:58:aa:08:3e:0a:dc:63:8d:2e:57 (0) 87:ed:a5:1f:d4:2e:a9:a8:63:36:3f:fa:6f:ac:1b:19 (0) 5a:2e:ec:38:63:5e:8d:9b:77:70:59:03:b4:2e:57:c8 (0) 22:b9:f7:7c:82:72:9e:7f:a2:ba:25:fd:c0:69:fc:16 (0) bd:27:e6:fd:2e:e2:58:3e:fe:e5:5e:b0:f7:66:09:34 (0) e0:21:08:8e:58:34:f2:ec:36:c8:09:b9:0b:29:fb:34 (0) e3:fa:c5:8c:03:68:8b:a9:4d:04:c8:33:9a:52:cc:f8 (0) f8:d5:c8:7a:e2:b6:71:37:eb:18:41:9c:17:21:83:f0 (0) ba:6c:98:26:c2:71:a3:f4:d8:8d:16:28:5d:b1:5a:1e (0) f9:7f:26:6c:a3:91:cd:58:ca:1b:1e:0f:42:79:1e:cb (0) f5:48:d6:02:60:10:58:9d:ba:1c:45:19:0f:03:17:60 (0) 8d:e4:26:33:6c:65:a6:bd:d4:72:2c:ec:0f:df:c5:43 (0) 89:c3:16:dd:a5:2e:f1:73:37:61:f5:6f:cf:27:e3:a4 (0) e5:a0:dd:7b:76:de:1f:a5:fa:b0:94:d0:a3:d2:5b:4d (0) 11:ac:01:e7:c8:c6:eb:81:da:da:66:b8:6e:27:63:61 (0) 58:34:92:9e:17:cd:e5:64:ff:19:7d:e8:c4:b3:96:22

Info List

Info #1

Certificate Fingerprint:2030E0434FF89E8F0D7543D14E51B2A9E9F0E60C6456AF70C1E7A49EA07504C9

150009 Links Crawled (1)

150009 Links Crawled

Finding #	**9473823** (230455646)	**Severity**	Information Gathered - Level 1
Unique #	**b9dfb94e-4036-45d6-b13f-9ea2457c9746**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
The list of unique links crawled and HTML forms submitted by the scanner appear in the Results section. This list may contain fewer links than the maximum threshold defined.

NOTE: This list also includes:
- All the unique links that are reported in QID 150140 (Redundant links/URL paths crawled and not crawled)
- All the forms reported in QID 150152 (Forms Crawled)
- All the forms in QID 150115 (Authentication Form Found)
- Certain requests from QID 150172 (Requests Crawled)

Impact
N/A

Solution
N/A

Results

```
Duration of crawl phase (seconds): 394.00
Number of links: 21
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://picahi.nmfs.local/
https://picahi.nmfs.local/php-shared-library/
https://picahi.nmfs.local/php-shared-library/css/
https://picahi.nmfs.local/php-shared-library/css/smoothness/
https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css
https://picahi.nmfs.local/php-shared-library/js/
https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js
https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js
https://picahi.nmfs.local/pirri
https://picahi.nmfs.local/res/
https://picahi.nmfs.local/res/css/
https://picahi.nmfs.local/res/css/index.css
https://picahi.nmfs.local/res/css/template.css
https://picahi.nmfs.local/res/css/tooltip.css
https://picahi.nmfs.local/res/js/
https://picahi.nmfs.local/res/js/RIA_tooltips.js
https://picahi.nmfs.local/res/js/index.js
https://picahi.nmfs.local/res/js/template.js
https://picahi.nmfs.local/res/js/tooltip.js
https://picahi.nmfs.local/view_all_projects.php
https://picahi.nmfs.local/view_all_resources.php
```

150020 Links Rejected By Crawl Scope or Exclusion List (1)

150020 Links Rejected By Crawl Scope or Exclusion List

Finding #	**9473812** (230455635)	**Severity**	Information Gathered - Level 1
Unique #	**6f4a0bf6-3521-4301-92f8-498eefd09171**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

One or more links were not crawled because of an explicit rule to exclude them. This also occurs if a link is malformed.

Exclude list and Include list entries can cause links to be rejected. If a scan is limited to a specific starting directory, then links outside that directory will neither be crawled or tested.

Links that contain a host name or IP address different from the target application are considered external links and not crawled by default; those types of links are not listed here. This often happens when the scope of a scan is limited to the directory of the starting URL. The scope can be changed in the Web Application Record.

During the test phase, some path-based tests may be rejected if the scan is limited to the directory of the starting URL and the test would fall outside that directory. In these cases, the number of rejected links may be too high to list in the Results section.

Impact

Links listed here were neither crawled or tested by the Web application scanning engine.

Solution

A link might have been intentionally matched by a exclude or include list entry. Verify that no links in this list were unintentionally rejected.

Results

```
Links not permitted:
(This list includes links from QIDs: 150010,150041,150143,150170)

IP based excluded links:
```

150021 Scan Diagnostics (1)

150021 Scan Diagnostics

Finding #	**9473813** (230455636)	**Severity**	Information Gathered - Level 1
Unique #	**cdd83005-8c61-4eec-be36-97e5d0abcc4b**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

This check provides various details of the scan's performance and behavior. In some cases, this check can be used to identify problems that the scanner encountered when crawling the target Web application.

Impact

The scan diagnostics data provides technical details about the crawler's performance and behavior. This information does not necessarily imply problems with the Web application.

Solution

No action is required.

Results

```
Loaded 1 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://picahi.nmfs.local/pirri fetched. Status code:200, Content-Type:text/html, load time:3
milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 46 seconds. Completed 70 requests of 70 estimated
requests (100%). All tests completed.
Batch #0 CMSDetection: estimated time < 1 minute (1 tests, 1 inputs)
[CMSDetection phase] : No potential CMS found using Blind Elephant algorithm. Aborting the CMS Detection phase
CMSDetection: 1 vulnsigs tests, completed 56 requests, 24 seconds. Completed 56 requests of 56 estimated requests (100%).
All tests completed.
Collected 21 links overall in 0 hours 6 minutes duration.
Batch #0 BannersVersionReporting: estimated time < 1 minute (1 tests, 1 inputs)
BannersVersionReporting: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 estimated requests
(0%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 13) + directories:(9
x 9) + paths:(0 x 22) = total (81)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 22 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 81 requests, 22 seconds. Completed 81 requests of 81
estimated requests (100%). All tests completed.
Batch #0 WS enumeration: estimated time < 10 minutes (11 tests, 21 inputs)
WS enumeration: 11 vulnsigs tests, completed 101 requests, 23 seconds. Completed 101 requests of 231 estimated requests
(43.7229%). All tests completed.
Batch #4 WebCgiOob: estimated time < 30 minutes (116 tests, 1 inputs)
Batch #4 WebCgiOob: 116 vulnsigs tests, completed 666 requests, 154 seconds. Completed 666 requests of 2816 estimated
requests (23.6506%). All tests completed.
No XML requests found. Skipping XXE tests.
Batch #4 DOM XSS exploitation: estimated time < 1 minute (4 tests, 0 inputs)
Batch #4 DOM XSS exploitation: 4 vulnsigs tests, completed 0 requests, 1 seconds. No tests to execute.
Batch #4 HTTP call manipulation: estimated time < 1 minute (38 tests, 0 inputs)
Batch #4 HTTP call manipulation: 38 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Open Redirect analysis: estimated time < 1 minute (2 tests, 0 inputs)
Batch #4 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 2 seconds. No tests to execute.
CSRF tests will not be launched because the scan is not successfully authenticated.
Batch #4 File Inclusion analysis: estimated time < 1 minute (1 tests, 21 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 21 estimated
requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 0 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #4 Header manipulation: estimated time < 30 minutes (47 tests, 21 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 1323 requests, 314 seconds. Completed 1323 requests of 2730
estimated requests (48.4615%). XSS optimization removed 609 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 21 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 21 requests, 7 seconds. Completed 21 requests of 21 estimated
requests (100%). All tests completed.
Batch #4 shell shock detector(form): estimated time < 1 minute (1 tests, 0 inputs)
Batch #4 shell shock detector(form): 1 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Login Brute Force manipulation estimated time: no tests enabled
Login Brute Force manipulation estimated time: no tests enabled
Cookies Without Consent no tests enabled.
Batch #5 HTTP Time Bandit: estimated time < 1 minute (1 tests, 10 inputs)
Batch #5 HTTP Time Bandit: 1 vulnsigs tests, completed 200 requests, 94 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 13) + directories:(4
x 9) + paths:(11 x 22) = total (278)
Batch #5 Path XSS manipulation: estimated time < 10 minutes (15 tests, 22 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 277 requests, 64 seconds. Completed 277 requests of 278
estimated requests (99.6403%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 13) + directories:(1
x 9) + paths:(0 x 22) = total (9)
Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 22 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 7 requests, 2 seconds. Completed 7 requests of 9 estimated
requests (77.7778%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 12) + files:(0 x 13) +
directories:(16 x 9) + paths:(0 x 22) = total (144)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 22 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 64 requests, 1440 seconds. Completed 64 requests of
144 estimated requests (44.4444%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(4 x 12) + files:(18 x 13) +
directories:(146 x 9) + paths:(18 x 22) = total (1992)
Batch #5 Path manipulation: estimated time < 10 minutes (186 tests, 22 inputs)
```

```
Batch #5 Path manipulation: 186 vulnsigs tests, completed 1596 requests, 355 seconds. Completed 1596 requests of 1992
estimated requests (80.1205%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 1 hour (288 tests, 1 inputs)
Batch #5 WebCgiGeneric: 288 vulnsigs tests, completed 383 requests, 90 seconds. Completed 383 requests of 7920 estimated
requests (4.83586%). All tests completed.
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 0 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 5 seconds. No tests to execute.
Duration of Crawl Time: 394.00 (seconds)
Duration of Test Phase: 2693.00 (seconds)
Total Scan Time: 3087.00 (seconds)

Total requests made: 4891
Average server response time: 0.47 seconds

Average browser load time: 0.48 seconds
```

150152 Forms Crawled (1)

150152 Forms Crawled

Finding #	**9473815** (230455638)	**Severity**	Information Gathered - Level 1
Unique #	**4419093f-ac43-4d5c-b5c9-bbf92a541b68**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Results section lists the unique forms that were identified and submitted by the scanner. The forms listed in this QID do not include authentication forms (i.e. login forms), which are reported separately under QID 150115.

The scanner does a redundancy check on forms by inspecting the form fields. Forms determined to be the redundant based on identical form fields will not be tested. If desired, you can enable 'Include form action URI in form uniqueness calculation' in the WAS option profile to have the scanner also consider the form's action attribute in the redundancy check.

NOTE: Any regular expression specified under 'Redundant Links' are not applied to forms. Forms (unique or redundant) are not reported under QID 150140.

Impact

N/A

Solution

N/A

Results

```
Total internal forms seen (this count includes duplicate forms): 0

Crawled forms (Total: 0)
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115
```

150247 Web Server and Technologies Detected (1)

150247 Web Server and Technologies Detected

Finding #	**9473810** (230455633)	**Severity**	Information Gathered - Level 1
Unique #	**d5c907d0-eb3a-44c5-92bf-52e594b85f85**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-200		
OWASP	-		
WASC	-		

Details

Threat

Information disclosure is an application weakness in revealing sensitive data, such as technical details of the system or environment.

This check reports the various technologies used by the web application based on the information available in different components of the Request-Response.

Impact

An attacker may use sensitive data to exploit the target web application, its hosting network, or its users.

Solution

Ensure that your web servers do not reveal any sensitive information about your technology stack and system details

Please review the issues reported below:

Results

```
Number of technologies detected: 2
Technology name: Apache
Matched Components:
header match:
Server:Apache
Matched links: reporting only first 3 links
https://picahi.nmfs.local/
https://picahi.nmfs.local/pirri
https://picahi.nmfs.local/res/js/tooltip.js

Technology name: PHP
Technology version: PHP 8.1.17
Matched Components:
header match:
X-Powered-By:PHP/8.1.17
Matched links: reporting only first 3 links
https://picahi.nmfs.local/pirri
```

150528 Server Returns HTTP 4XX Error Code During Scanning (1)

150528 Server Returns HTTP 4XX Error Code During Scanning

Finding #	**9473808** (230455631)	**Severity**	Information Gathered - Level 1
Unique #	**240ff3bb-9288-4fd6-8810-713aba9b2f21**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

During the WAS scan, links with HTTP 4xx response code were observed and these are listed in the Results section. The HTTP 4xx message indicates a client error. The list of supported 4xx response code are as below:

400 - Bad Request
401 - Unauthorized
403 - Forbidden
404 - Not Found
405 - Method Not Allowed
407 - Proxy Authentication Required
408 - Request Timeout
413 - Payload Too Large
414 - URI Too Long

Impact

The presence of a HTTP 4xx error during the crawl phase indicates that some problem exists on the website that will be encountered during normal usage of the Web application. Note WAS depends on responses to detect many vulnerabilities if the link does not respond with an expected response then any vulnerabilities present on such links may not be detected.

Solution

Review each link to determine why the client encountered an error while requesting the link. Additionally review and investigate the results of QID 150042 which lists 5xx errors, QID 150019 which lists unexpected response codes and QID 150097 which lists a potential blocked request.

Results

```
Number of links with 4xx response code: 20
(Only first 50 such links are listed)
```

```
403 https://picahi.nmfs.local/
404 https://picahi.nmfs.local/php-shared-library/
404 https://picahi.nmfs.local/php-shared-library/css/
404 https://picahi.nmfs.local/php-shared-library/css/smoothness/
404 https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css
404 https://picahi.nmfs.local/php-shared-library/js/
404 https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js
404 https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js
404 https://picahi.nmfs.local/res/
404 https://picahi.nmfs.local/res/css/
404 https://picahi.nmfs.local/res/css/index.css
404 https://picahi.nmfs.local/res/css/template.css
404 https://picahi.nmfs.local/res/css/tooltip.css
404 https://picahi.nmfs.local/res/js/
404 https://picahi.nmfs.local/res/js/RIA_tooltips.js
404 https://picahi.nmfs.local/res/js/index.js
404 https://picahi.nmfs.local/res/js/template.js
404 https://picahi.nmfs.local/res/js/tooltip.js
404 https://picahi.nmfs.local/view_all_projects.php
404 https://picahi.nmfs.local/view_all_resources.php
```

150546 First Link Crawled Response Code Information (1)

150546 First Link Crawled Response Code Information

Finding #	**9473819** (230455642)	**Severity**	Information Gathered - Level 1
Unique #	**f0ef2efc-234a-4482-85ec-3732ee2d0d4d**		
Group	Scan Diagnostics	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The Web server returned the following information from where the Web application scanning engine initiated. Information reported includes First Link Crawled, response Code, response Header, and response Body (first 500 characters). The first link crawled is the "Web Application URL (or Swagger file URL)" set in the Web Application profile.

Impact

An erroneous response might be indicative of a problem in the Web server, or the scan configuration.

Solution

Review the information to check if this is in line with the expected scan configuration. Refer to the output of QIDs 150009, 150019, 150021, 150042 and 150528 (if present) for additional details.

Results

```
Base URI: https://picahi.nmfs.local/pirri
Response Code: 200
Response Header:
Date: Fri, 14 Apr 2023 19:34:53 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=
(self),payment=()
X-Powered-By: PHP/8.1.17
X-Frame-Options: ALLOW-FROM https://ahi.pifsc.gov/
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'unsafe-inline' 'unsafe-eval' 'self' *.pifsc.gov; script-src 'unsafe-inline'
'unsafe-eval' 'self' *.pifsc.gov; img-src 'self' https://picgitlab.nmfs.local https://secure.gravatar.com;
append: frame-ancestors *fisheries.noaa.gov *nmfs.local *pifsc.gov
Access-Control-Allow-Origin: https://ahi.pifsc.gov
Content-Type: text/html;charset=utf-8
Content-Length: 4820
Connection: close

Response Body:
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" lang="en"><head><script type="text/javascript" src="./php-
shared-library/js/jquery-1.7.2.min.js"></script><script type="text/javascript" src="./php-shared-library/js/jquery-
ui-1.12.1.min.js"></script><script type="text/javascript">var app_instance = 'test';</script><script
type="text/javascript" src="./res/js/template.js"></script><script type="text/javascript" src="./res/js/index.js">
</script><script type="text/javascript" src="./res/js/t
...
```

Security Weaknesses (10)

150086 Server accepts unnecessarily large POST request body (1)

150086 Server accepts unnecessarily large POST request body

Finding #	**9473809** (230455632)	**Severity**	Information Gathered - Level 3
Unique #	**9c80f8ab-1daa-4abe-81c8-1f7c802da1a1**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-130, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The scanner successfully sent a POST request with content type of application/x-www-form-urlencoded and 65536 bytes length random text data. Accepting request bodies with unnecessarily large size could help attacker to use less connections to achieve Layer 7 DDoS of web server. More information can be found at the here

Impact

Potentially could result in a successful application-layer DDoS attack.

Solution

Limit the size of the request body to each form's requirements. For example, a search form with 256-char search field should not accept more than 1KB value. Server-specific details can be found here.

Results

```
Server responded 200 to unnecessarily large random request body(over 64 KB) for URL https://picahi.nmfs.local/pirri,
significantly increasing attacker's chances to prolong slow HTTP POST attack.
```

150210 Information Disclosure via Response Header (1)

150210 Information Disclosure via Response Header

Finding #	**9473806** (230455629)	**Severity**	Information Gathered - Level 3
Unique #	**6daf8cdf-9640-4609-8cbb-34fd2ddfcc11**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-16, CWE-201		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

HTTP response headers like 'Server', 'X-Powered-By', 'X-AspNetVersion', 'X-AspNetMvcVersion' could disclose information about the platform and technologies used by the website. The HTTP response include one or more such headers.

Impact

The headers can potentially be used by attackers for fingerprinting and launching attacks specific to the technologies and versions used by the web application. These response headers are not necessary for production sites and should be disabled.

Solution

Disable such response headers, remove them from the response, or make sure that the header value does not contain information which could be used to fingerprint the server-side components of the web application.

Results

```
One or more response headers disclosing information about the application platform were present on the following pages:
(Only first 50 such pages are reported)

GET https://picahi.nmfs.local/pirri response code: 200
X-Powered-By: PHP/8.1.17
```

150202 Missing header: X-Content-Type-Options (1)

150202 Missing header: X-Content-Type-Options

Finding #	**9473821** (230455644)	**Severity**	Information Gathered - Level 2
Unique #	**6447f799-47fa-4f51-9488-ee41e691a772**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-Content-Type-Options response header is not present. WAS reports missing X-Content-Type-Options header on each crawled link for both static and

dynamic responses. The scanner performs the check not only on 200 responses but 4xx and 5xx responses as well. It's also possible the QID will be reported on directory-level links.

Impact

All web browsers employ a content-sniffing algorithm that inspects the contents of HTTP responses and also occasionally overrides the MIME type provided by the server. If X-Content-Type-Options header is not present, browsers can potentially be tricked into treating non-HTML response as HTML. An attacker can then potentially leverage the functionality to perform a cross-site scripting (XSS) attack. This specific case is known as a Content-Sniffing XSS (CS-XSS) attack.

Solution

It is recommended to disable browser content sniffing by adding the X-Content-Type-Options header to the HTTP response with a value of 'nosniff'. Also, ensure that the 'Content-Type' header is set correctly on responses.

Results

```
X-Content-Type-Options: Header missing
Response headers on link: GET https://picahi.nmfs.local/ response code: 403
Date: Fri, 14 Apr 2023 19:35:59 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://picahi.nmfs.local/ response code: 403
GET https://picahi.nmfs.local/res/js/tooltip.js response code: 404
GET https://picahi.nmfs.local/view_all_projects.php response code: 404
GET https://picahi.nmfs.local/res/css/index.css response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css response code: 404
GET https://picahi.nmfs.local/view_all_resources.php response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js response code: 404
GET https://picahi.nmfs.local/res/js/RIA_tooltips.js response code: 404
GET https://picahi.nmfs.local/res/css/template.css response code: 404
GET https://picahi.nmfs.local/res/css/tooltip.css response code: 404
GET https://picahi.nmfs.local/res/js/template.js response code: 404
GET https://picahi.nmfs.local/res/js/index.js response code: 404
GET https://picahi.nmfs.local/res/js/ response code: 404
GET https://picahi.nmfs.local/res/ response code: 404
GET https://picahi.nmfs.local/res/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/ response code: 404
```

150206 Content-Security-Policy Not Implemented (1)

150206 Content-Security-Policy Not Implemented

Finding #	**9473824** (230455647)	**Severity**	Information Gathered - Level 2
Unique #	**ecb5088f-c597-4de2-bb1d-67463d85b0f1**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

No Content-Security-Policy (CSP) is specified for the page. WAS checks for the missing CSP on all static and dynamic pages. It checks for CSP in the response headers (Content-Security-Policy, X-Content-Security-Policy or X-Webkit-CSP) and in response body (http-equiv="Content-Security-Policy" meta tag).

HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security it's important to set appropriate CSP policies on 4xx and 5xx responses as well.

Impact

Content-Security Policy is a defense mechanism that can significantly reduce the risk and impact of XSS attacks in modern browsers. The CSP specification provides a set of content restrictions for web resources and a mechanism for transmitting the policy from a server to a client where the policy is enforced. When a Content Security Policy is specified, a number of default behaviors in user agents are changed; specifically inline content and JavaScript eval constructs are not interpreted without additional directives. In short, CSP allows you to create a whitelist of sources of the trusted content. The CSP policy instructs the browser to only render resources from those whitelisted sources. Even though an attacker can find a security vulnerability in the application through which to inject script, the script won't match the whitelisted sources defined in the CSP policy, and therefore will not be executed.

The absence of Content Security Policy in the response will allow the attacker to exploit vulnerabilities as the protection provided by the browser is not at all leveraged by the Web application. If secure CSP configuration is not implemented, browsers will not be able to block content-injection attacks such as Cross-Site Scripting and Clickjacking.

Solution

Appropriate CSP policies help prevent content-injection attacks such as cross-site scripting (XSS) and clickjacking. It's recommended to add secure CSP policies as a part of a defense-in-depth approach for securing web applications.

References:
- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- https://developers.google.com/web/fundamentals/security/csp/

Results

```
Content-Security-Policy: Header missing
Response headers on link: GET https://picahi.nmfs.local/ response code: 403
Date: Fri, 14 Apr 2023 19:35:59 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://picahi.nmfs.local/ response code: 403
GET https://picahi.nmfs.local/res/js/tooltip.js response code: 404
GET https://picahi.nmfs.local/view_all_projects.php response code: 404
GET https://picahi.nmfs.local/res/css/index.css response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css response code: 404
GET https://picahi.nmfs.local/view_all_resources.php response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js response code: 404
GET https://picahi.nmfs.local/res/js/RIA_tooltips.js response code: 404
GET https://picahi.nmfs.local/res/css/template.css response code: 404
GET https://picahi.nmfs.local/res/css/tooltip.css response code: 404
GET https://picahi.nmfs.local/res/js/template.js response code: 404
GET https://picahi.nmfs.local/res/js/index.js response code: 404
GET https://picahi.nmfs.local/res/js/ response code: 404
GET https://picahi.nmfs.local/res/ response code: 404
GET https://picahi.nmfs.local/res/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/ response code: 404
```

150208 Missing header: Referrer-Policy (1)

150208 Missing header: Referrer-Policy

Finding #	**9473807** (230455630)	**Severity**	Information Gathered - Level 2
Unique #	**4b7f4ba5-1236-43e3-853e-16aaf46916cd**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat
No Referrer Policy is specified for the link. WAS checks for the missing Referrer Policy on all static and dynamic pages. It checks for one of the following Referrer Policy in the response headers:

1) no-referrer
2) no-referrer-when-downgrade
3) same-origin
4) origin
5) origin-when-cross-origin
6) strict-origin
7) strict-origin-when-cross-origin

If the Referrer Policy header is not found , WAS checks in response body for meta tag containing tag name as "referrer" and one of the above Referrer Policy.

Impact
The Referrer-Policy header controls how much referrer information is sent to a site when navigating to it. Absence of Referrer-Policy header can lead to leakage of sensitive information via the referrer header.

Solution
Referrer Policy header improves security by ensuring websites don't leak sensitive information via the referrer header. It's recommended to add secure Referrer Policies as a part of a defense-in-depth approach.

References:
- https://www.w3.org/TR/referrer-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Results

```
Referrer-Policy: Header missing
Response headers on link: GET https://picahi.nmfs.local/ response code: 403
Date: Fri, 14 Apr 2023 19:35:59 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://picahi.nmfs.local/ response code: 403
GET https://picahi.nmfs.local/res/js/tooltip.js response code: 404
GET https://picahi.nmfs.local/view_all_projects.php response code: 404
GET https://picahi.nmfs.local/res/css/index.css response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css response code: 404
GET https://picahi.nmfs.local/view_all_resources.php response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js response code: 404
GET https://picahi.nmfs.local/res/js/RIA_tooltips.js response code: 404
GET https://picahi.nmfs.local/res/css/template.css response code: 404
GET https://picahi.nmfs.local/res/css/tooltip.css response code: 404
GET https://picahi.nmfs.local/res/js/template.js response code: 404
GET https://picahi.nmfs.local/res/js/index.js response code: 404
GET https://picahi.nmfs.local/res/js/ response code: 404
GET https://picahi.nmfs.local/res/ response code: 404
GET https://picahi.nmfs.local/res/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/ response code: 404
```

150248 Missing header: Permissions-Policy (1)

150248 Missing header: Permissions-Policy

Finding #	**9473816** (230455639)	**Severity**	Information Gathered - Level 2
Unique #	**9db5db86-8021-4bf3-920d-641f4b6b2e55**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-284		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

The Permissions-Policy response header is not present.

Impact

Permissions-Policy allows web developers to selectively enable, disable, or modify the behavior of some of the browser features and APIs within their application.

A user agent has a set of supported features(Policy Controlled Features), which is the set of features which it allows to be controlled through policies.

Not defining policy for unused and risky policy controlled features may leave application vulnerable.

Solution

It is recommended to define policy for policy controlled features to make application more secure.

References:
Permissions-Policy W3C Working Draft
Policy Controlled Features

Results

```
Permissions-Policy: Header missing
Response headers on link: GET https://picahi.nmfs.local/ response code: 403
Date: Fri, 14 Apr 2023 19:35:59 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1

Header missing on the following link(s):
(Only first 50 such pages are listed)
```

```
GET https://picahi.nmfs.local/ response code: 403
GET https://picahi.nmfs.local/res/js/tooltip.js response code: 404
GET https://picahi.nmfs.local/view_all_projects.php response code: 404
GET https://picahi.nmfs.local/res/css/index.css response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css response code: 404
GET https://picahi.nmfs.local/view_all_resources.php response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js response code: 404
GET https://picahi.nmfs.local/res/js/RIA_tooltips.js response code: 404
GET https://picahi.nmfs.local/res/css/template.css response code: 404
GET https://picahi.nmfs.local/res/css/tooltip.css response code: 404
GET https://picahi.nmfs.local/res/js/template.js response code: 404
GET https://picahi.nmfs.local/res/js/index.js response code: 404
GET https://picahi.nmfs.local/res/js/ response code: 404
GET https://picahi.nmfs.local/res/ response code: 404
GET https://picahi.nmfs.local/res/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/ response code: 404
```

150262 Missing header: Feature-Policy (1)

150262 Missing header: Feature-Policy

Finding #	**9473820** (230455643)	**Severity**	Information Gathered - Level 2
Unique #	**31abc964-b65b-4e85-9aa4-64c7e906b6d3**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Feature-Policy response header is not present.

Impact

Feature Policy allows web developers to selectively enable, disable, and modify the behavior of certain APIs and web features such as "geolocation","camera", "usb", "fullscreen", "animations" etc in the browser.

These policies restrict what APIs the site can access or modify the browser's default behavior for certain features.

Solution

It is recommended to set the Feature-Policy header to selectively enable, disable, and modify the behavior of certain APIs and web features.

References:
- https://www.w3.org/TR/feature-policy/
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Results

```
Feature-Policy: Header missing
Response headers on link: GET https://picahi.nmfs.local/ response code: 403
Date: Fri, 14 Apr 2023 19:35:59 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://picahi.nmfs.local/ response code: 403
GET https://picahi.nmfs.local/res/js/tooltip.js response code: 404
GET https://picahi.nmfs.local/view_all_projects.php response code: 404
GET https://picahi.nmfs.local/res/css/index.css response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css response code: 404
GET https://picahi.nmfs.local/view_all_resources.php response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js response code: 404
GET https://picahi.nmfs.local/res/js/RIA_tooltips.js response code: 404
GET https://picahi.nmfs.local/res/css/template.css response code: 404
GET https://picahi.nmfs.local/res/css/tooltip.css response code: 404
GET https://picahi.nmfs.local/res/js/template.js response code: 404
GET https://picahi.nmfs.local/res/js/index.js response code: 404
GET https://picahi.nmfs.local/res/js/ response code: 404
GET https://picahi.nmfs.local/res/ response code: 404
GET https://picahi.nmfs.local/res/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/ response code: 404
```

```
GET https://picahi.nmfs.local/php-shared-library/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/ response code: 404
```

150126 Links With High Resource Consumption (1)

150126 Links With High Resource Consumption

Finding #	**9473817** (230455640)	**Severity**	Information Gathered - Level 1
Unique #	**13827c8d-ec9b-4a9a-a393-a17bc56d63fb**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The list of links with lowest bytes/sec which are assumed to be resources with highest resource consumption. The links in the list have slower transfer times speeds to an average resource on the server. This may indicate that the links are more CPU or DB intensive than majority of links.

The latency of the network and file size have no effect on calculations.

Impact

The links with high resource consumption could be used to perform DOS on the server by just performing GET Flooding. Attackers could more easily take the server down if there are huge resource hogs on it, performing less request.

Solution

Find the root cause of resources slow download speed.

If the cause is a real CPU strain or complex DB queries performed, there may be a need for re-engineering of the web application or defense measures should be in place. Examples of defense against DOS that is targeted towards high resource consumption links are Load Balancers and Rate Limiters.

Results

```
473.000000 bytes/sec https://picahi.nmfs.local/res/js/tooltip.js
476.400000 bytes/sec https://picahi.nmfs.local/php-shared-library/
483.400000 bytes/sec https://picahi.nmfs.local/res/js/index.js
492.800000 bytes/sec https://picahi.nmfs.local/res/js/
503.200000 bytes/sec https://picahi.nmfs.local/view_all_projects.php
519.300000 bytes/sec https://picahi.nmfs.local/res/js/RIA_tooltips.js
543.400000 bytes/sec https://picahi.nmfs.local/res/js/template.js
585.400000 bytes/sec https://picahi.nmfs.local/php-shared-library/css/smoothness/
590.700000 bytes/sec https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js
637.000000 bytes/sec https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css
```

150204 Missing header: X-XSS-Protection (1)

150204 Missing header: X-XSS-Protection

Finding #	**9473825** (230455648)	**Severity**	Information Gathered - Level 1
Unique #	**f58fac48-3361-4e67-899a-d226ab6ab2f4**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The X-XSS-Protection response header is not present.

Impact

The X-XSS-Protection response header provides a layer of protection against reflected cross-site scripting (XSS) attacks by instructing browsers to abort rendering a page in which a reflected XSS attack has been detected. This is a best-effort second line of defense measure which helps prevent an attacker from using evasion techniques to avoid the neutralization mechanisms that the filters use by default. When configured appropriately, browser-level XSS filters can provide additional layers of defense against web application attacks.

Note that HTTP 4xx and 5xx responses can also be susceptible to attacks such as XSS. For better security the X-XSS-Protection header should be set on 4xx and 5xx responses as well.

Solution

It is recommend to set X-XSS-Protection header with value set to '1; mode=block' on all the relevant responses to activate browser's XSS filter.

NOTE: The X-XSS-Protection header is not supported by all browsers. Google Chrome and Safari are some of the browsers which support it, Firefox on the other hand does not support the header. X-XSS-Protection header does not guarantee a complete protection against XSS. For better protection against XSS attacks, the web application should use secure coding principles. Also, consider leveraging the Content-Security-Policy (CSP) header, which is supported by all browsers.

Using X-XSS-Protection could have unintended side effects, please understand the implications carefully before using it.

References:
- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-XSS-Protection
- https://blog.innerht.ml/the-misunderstood-x-xss-protection/
- https://www.mbsd.jp/blog/20160407.html
- https://www.chromium.org/developers/design-documents/xss-auditor

Results

```
X-Xss-Protection: Header missing
Response headers on link: GET https://picahi.nmfs.local/ response code: 403
Date: Fri, 14 Apr 2023 19:35:59 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
Content-Length: 202
Connection: close
Content-Type: text/html; charset=iso-8859-1

Header missing on the following link(s):
(Only first 50 such pages are listed)

GET https://picahi.nmfs.local/ response code: 403
GET https://picahi.nmfs.local/res/js/tooltip.js response code: 404
GET https://picahi.nmfs.local/view_all_projects.php response code: 404
GET https://picahi.nmfs.local/res/css/index.css response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/jquery-ui-1.12.1.min.css response code: 404
GET https://picahi.nmfs.local/view_all_resources.php response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-1.7.2.min.js response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/jquery-ui-1.12.1.min.js response code: 404
GET https://picahi.nmfs.local/res/js/RIA_tooltips.js response code: 404
GET https://picahi.nmfs.local/res/css/template.css response code: 404
GET https://picahi.nmfs.local/res/css/tooltip.css response code: 404
GET https://picahi.nmfs.local/res/js/template.js response code: 404
GET https://picahi.nmfs.local/res/js/index.js response code: 404
GET https://picahi.nmfs.local/res/js/ response code: 404
GET https://picahi.nmfs.local/res/ response code: 404
GET https://picahi.nmfs.local/res/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/smoothness/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/css/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/ response code: 404
GET https://picahi.nmfs.local/php-shared-library/js/ response code: 404
```

150245 Missing header: X-Frame-Options (1)

150245 Missing header: X-Frame-Options

Finding #	**9473814** (230455637)	**Severity**	Information Gathered - Level 1
Unique #	**01937780-4b81-4977-89ba-62b82e90745d**		
Group	Security Weaknesses	**Detection Date**	14 Apr 2023 09:34 GMT-1000
CWE	CWE-693		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat
The X-Frame-Options header is not set in the HTTP response, meaning the page can potentially be loaded into an attacker-controlled frame. This could lead to clickjacking, where an attacker adds an invisible layer on top of the legitimate page to trick users into clicking on a malicious link or taking a harmful action.

Impact
Without an X-Frame-Options response header, clickjacking may be possible. However, if the application properly uses the Content-Security-Policy "frame-ancestors" directive, then modern web browsers would stop the page from being framed and prevent clickjacking.

Solution
The X-Frame-Options allows three values: DENY, SAMEORIGIN and ALLOW-FROM. It is recommended to use DENY, which prevents all domains from framing the page or SAMEORIGIN, which allows framing only by the same site. DENY and SAMEORGIN are supported by all browsers. Using ALLOW-FROM is not recommended because not all browsers support it.

Note: To avoid a common X-Frame-Options implementation mistake, see https://blog.qualys.com/securitylabs/2015/10/20/clickjacking-a-common-implementation-mistake-that-can-put-your-websites-in-danger.

Results

```
X-Frame-Options header is missing or not set to DENY or SAMEORIGIN for the following pages:
(Only first 10 such pages are reported)

GET https://picahi.nmfs.local/pirri
Response code: 200
```

```
Response headers:
Date: Fri, 14 Apr 2023 19:34:53 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubDomains
X-Content-Type-Options: nosniff
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: geolocation=(),midi=(),sync-xhr=(),microphone=(),camera=(),magnetometer=(),gyroscope=(),fullscreen=
(self),payment=()
X-Powered-By: PHP/8.1.17
X-Frame-Options: ALLOW-FROM https://ahi.pifsc.gov/
X-XSS-Protection: 1; mode=block
Content-Security-Policy: default-src 'unsafe-inline' 'unsafe-eval' 'self' *.pifsc.gov; script-src 'unsafe-inline'
'unsafe-eval' 'self' *.pifsc.gov; img-src 'self' https://picgitlab.nmfs.local https://secure.gravatar.com;
append: frame-ancestors *fisheries.noaa.gov *nmfs.local *pifsc.gov
Access-Control-Allow-Origin: https://ahi.pifsc.gov
Content-Type: text/html;charset=utf-8
Content-Length: 4820
Connection: close
```

Appendix

- **Scan Details**
  - **Web Application Vulnerability Scan - PIFSC_4960_picahi.nmfs.local - 2023-04-14**
- **Option Profile Details**
- **Web Application Details: PIFSC_4960_picahi.nmfs.local**
- **Severity Levels**