



report

26 Nov 2024

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

PingYen Chou
tawan_pc

Chinatrust Life Insurance
Taipei
Taipei, None 115
Taiwan

Target and Filters

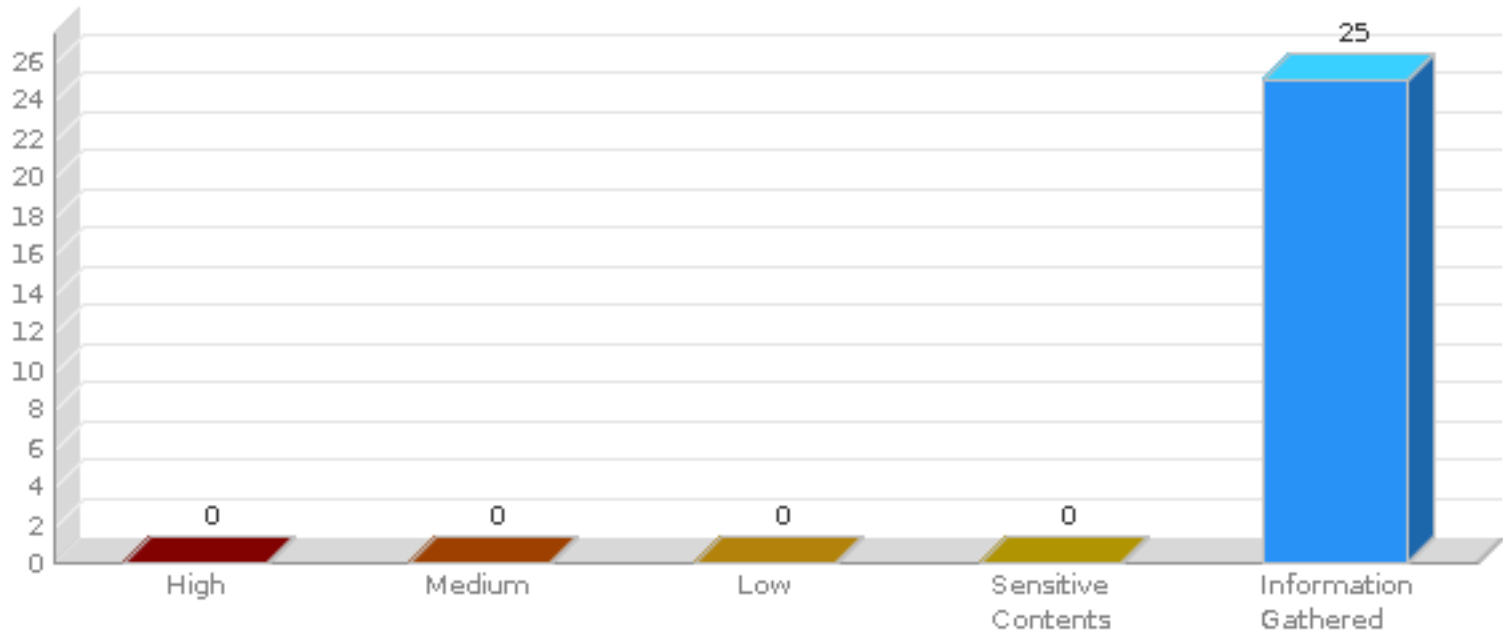
Scans (1)
Web Applications (1)

RCIS_Web Application Vulnerability Scan - Nov 26, 2024 Slice #1
RCIS_BATCH(DEV)

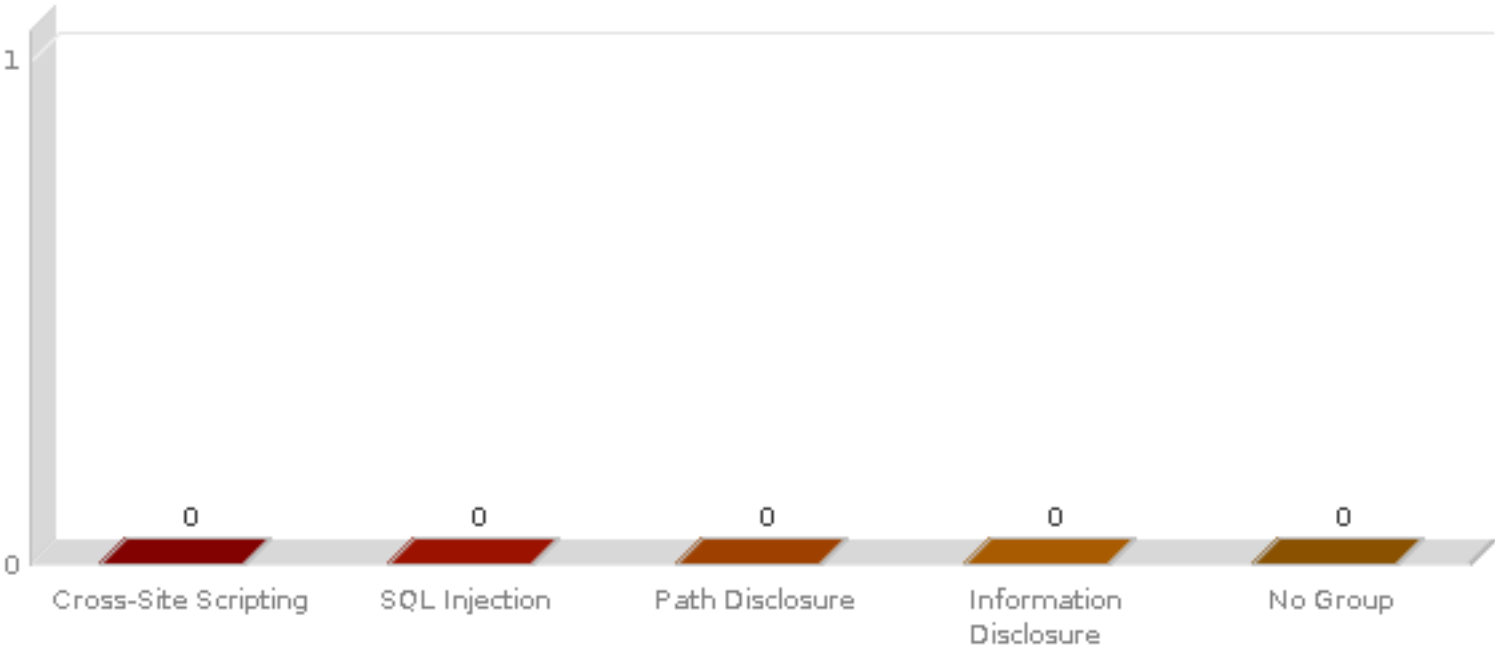
Summary

Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
-	0	0	25

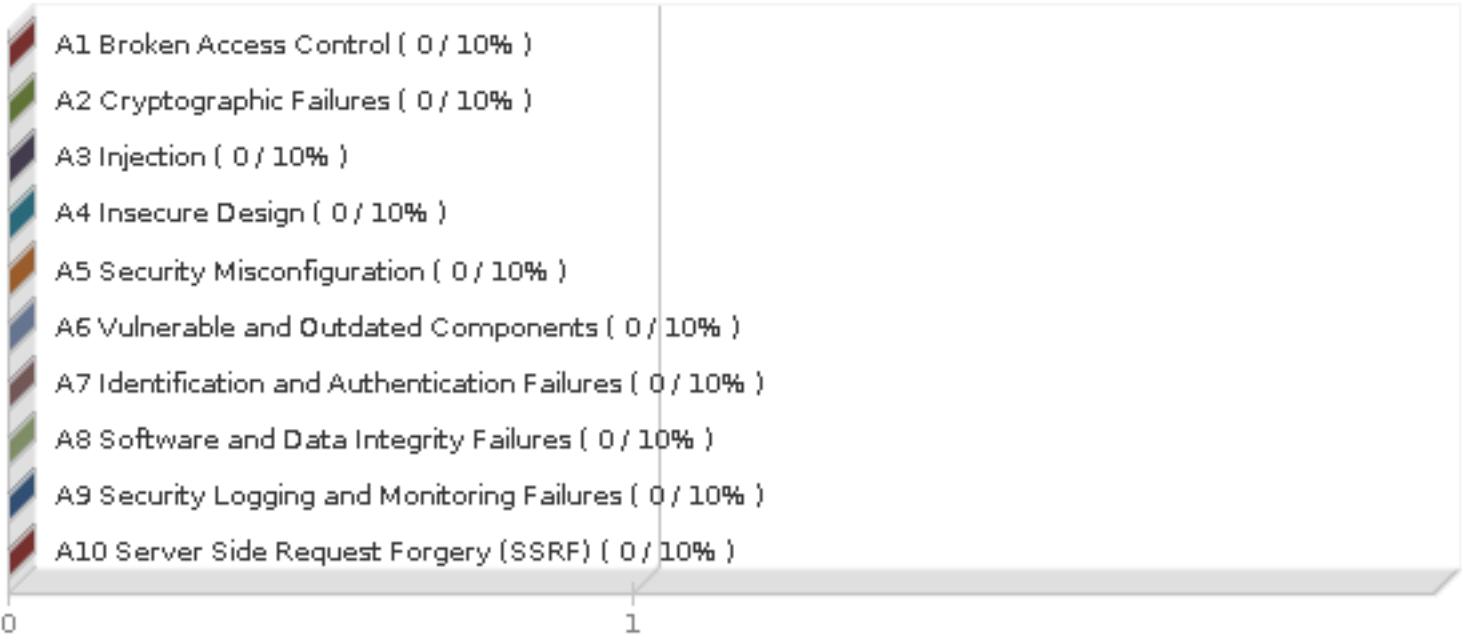
Findings by Severity



Vulnerabilities by Group



OWASP Top 10 2021 Vulnerabilities



Scan	Date	High	Medium	Low	Sensitive Contents	Information Gathered
RCIS_Web Application Vulnerability Scan - Nov 26, 2024 Slice #1	26 Nov 2024 09:31 GMT +0800	0	0	0	0	25

Results(25)

Information Gathered (25)

Scan Diagnostics (19)

INFO 150042 Server Returns HTTP 5XX Error Code During Scanning (1)

INFO 150042 Server Returns HTTP 5XX Error Code During Scanning

Finding #	15241984(990664759)	Severity	Information Gathered - Level 3
Unique #	f0d97eee-434e-4b4c-bf13-54695a3cf5c9		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
CWE	CWE-209, CWE-550		
OWASP	A5 Security Misconfiguration		
WASC	WASC-14 SERVER MISCONFIGURATION		

Details

Threat

During the WAS scan, links or end points with HTTP 5xx response code were observed and these are listed in the Results section. The HTTP 5xx message indicates a server error. The list of supported 5xx response code are as below:

- 500 - Internal Server Error
- 501 - Not Implemented
- 502 - Bad Gateway
- 503 - Service Unavailable
- 504 - Gateway Timeout
- 505 - HTTP Version Not Supported

Impact

The presence of a HTTP 5xx 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 expected response is not received then vulnerabilities present on such links or end points may not be detected.

Solution

Review each link to determine why the server encountered an error when responding to the link. Review and investigate the results of QID 150528 which lists 4xx errors and QID 150019 which lists unexpected response codes.

Results

https://10.1.242.13/

INFO 45017 Operating System Detected (1)

INFO 45017 Operating System Detected

Finding #	15241986(990664761)	Severity	Information Gathered - Level 2
Unique #	41233eff-11bc-4fbc-8b02-fa77961a1e65		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
Port	-
Result	EulerOS/_Ubuntu/_Fedora/_Tiny_Core_Linux/_Linux_3.x/_IBM/_FortiSOAR/_F5_Networks_Big-IP TCP/IP_Fingerprint M5933:7322::443

Info List

Info #1

INFO 6 DNS Host Name (1)

INFO 6 DNS Host Name

Finding #	15241976(990664751)	Severity	Information Gathered - Level 1
Unique #	7b02268d-6f98-4cda-9d01-519d5c169058		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
Port	-
Result	#table IP_address Host_name 10.1.242.13 No_registered_hostname

INFO 38116 SSL Server Information Retrieval (1)

INFO 38116 SSL Server Information Retrieval

Finding #	15241994(990664770)	Severity	Information Gathered - Level 1
Unique #	92ed364f-9214-49a4-81e2-5a84fd5f864f		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
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 _ _ _ _ AES128-SHA RSA RSA SHA1 AES(128) MEDIUM AES25 RSA RSA SHA1 AES(256) HIGH CAMELLIA128-SHA RSA RSA SHA1 Camellia(128) MEDIUM CAMELLIA256-SHA RSA RSA SHA1 Camellia(256) HIGH AES128-GCM-SHA256 RSA RSA AEAD AESGCM(128) MEDIUM AES256-GCM-SHA384 RSA RSA AEAD AESGCM(256) HIGH CAMELLIA128-SHA256 f RSA SHA256 Camellia(128) MEDIUM CAMELLIA256-SHA256 RSA RSA SHA256 Camellia(256) HIGH ECDHE-RSA-AES128-SHA ECDH RSA SHA1 AES MEDIUM ECDHE-RSA-AES256-SHA ECDH RSA SHA1 AES(256) HIGH ECDHE-RSA-AES128-SHA256 ECDH RSA SHA256 AES(128) MEDIUM ECDHE- AES256-SHA384 ECDH RSA SHA384 AES(256) HIGH ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AE GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CAMELLIA128-SHA256 ECDH RSA SHA256 Camellia(128) MEDIUM ECDHE-RSA- CAMELLIA256-SHA384 ECDH RSA SHA384 Camellia(256) HIGH AES128-CCM RSA RSA AEAD AESCCM(128) MEDIUM AES256-CCM RSA RSA AEAD AESCCM(256) HIGH AES128-CCM-8 RSA RSA AEAD AESCCM8(128) MEDIUM AES256-CCM-8 RSA RSA AEAD AESCCM8(256) HIGH ECDHE-RSA- CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH AES128-SHA256 RSA RSA SHA256 AES(128) MEDIUM AES256-SHA256 I RSA SHA256 AES(256) HIGH TLSv1.3_PROTOCOL_IS_DISABLED _ _ _ _ _

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
AES128-SHA	RSA	AES(128)	MEDIUM	RSA	SHA1	TLSv1.2
AES256-SHA	RSA	AES(256)	HIGH	RSA	SHA1	TLSv1.2
CAMELLIA128-SHA	RSA	Camellia(128)	MEDIUM	RSA	SHA1	TLSv1.2
CAMELLIA256-SHA	RSA	Camellia(256)	HIGH	RSA	SHA1	TLSv1.2
AES128-GCM-SHA256	RSA	AESGCM(128)	MEDIUM	RSA	AEAD	TLSv1.2
AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	RSA	AEAD	TLSv1.2
CAMELLIA128-SHA256	RSA	Camellia(128)	MEDIUM	RSA	SHA256	TLSv1.2
CAMELLIA256-SHA256	RSA	Camellia(256)	HIGH	RSA	SHA256	TLSv1.2
ECDHE-RSA-AES128-SHA	RSA	AES(128)	MEDIUM	ECDH	SHA1	TLSv1.2
ECDHE-RSA-AES256-SHA	RSA	AES(256)	HIGH	ECDH	SHA1	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
ECDHE-RSA-CAMELLIA128-SHA256	RSA	Camellia(128)	MEDIUM	ECDH	SHA256	TLSv1.2
ECDHE-RSA-CAMELLIA256-SHA384	RSA	Camellia(256)	HIGH	ECDH	SHA384	TLSv1.2
AES128-CCM	RSA	AESCCM(128)	MEDIUM	RSA	AEAD	TLSv1.2
AES256-CCM	RSA	AESCCM(256)	HIGH	RSA	AEAD	TLSv1.2

Info List

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
AES128-CCM-8	RSA	AESCCM8(128)	MEDIUM	RSA	AEAD	TLSv1.2
AES256-CCM-8	RSA	AESCCM8(256)	HIGH	RSA	AEAD	TLSv1.2
ECDHE-RSA-CHACHA20-POLY1305	RSA	CHACHA20/POLY1305(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

INFO 38291 SSL Session Caching Information (1)

INFO 38291 SSL Session Caching Information

Finding #	15241991(990664767)	Severity	Information Gathered - Level 1
Unique #	0a2c6c80-b155-4592-87e8-2208a6755480		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
Port	443
Result	TLSv1.2 session caching is enabled on the target.

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

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

Finding #	15241993(990664769)	Severity	Information Gathered - Level 1
Unique #	55acd33d-5e46-4ad8-aecf-9c78c79d629e		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

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

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

Finding #	15241995(990664771)	Severity	Information Gathered - Level 1
Unique #	71004709-7ae0-43a8-8aab-2287e04399f9		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
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-CCM-8 RSA _ 2048 no 110 low AES128-CCM-8 RSA _ 2048 no 110 low AES256-CCM RSA _ 2048 no 110 low AES128-CCM RSA _ 2048 no 110 low CAMELLIA256-SHA256 RSA _ 2048 no 110 low AES256-GCM-SHA384 RSA _ 2048 no 110 low AES128-GCM-SHA256 RSA _ 2048 no 110 low CAMELLIA256-SHA RSA _ 2048 no 110 low CAMELLIA128-SHA RSA _ 2048 no 110 low AES256-SHA RSA _ 2048 no 110 low AES128-SHA RSA _ 2048 no 110 low CAMELLIA128-SHA256 RSA _ 2048 no 110 low ECDHE-RSA-AES256-GCM-SHA384 ECDHE x25519 256 yes 128 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-CHACHA20-POLY1305 ECDHE x25519 256 yes 128 low ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-CHACHA20-POLY1305 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES128-GCM-SHA256 ECDHE x25519 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-AES256-SHA384 ECDHE x25519 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-CAMELLIA256-SHA384 ECDHE x25519 256 yes 128 low ECDHE-RSA-CAMELLIA256-SHA384 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-CAMELLIA256-SHA384 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-CAMELLIA256-SHA384 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES128-SHA256 ECDHE x25519 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-CAMELLIA128-SHA256 ECDHE x25519 256 yes 128 low ECDHE-RSA-CAMELLIA128-SHA256 ECDHE secp384r1 384 yes 192 low ECDHE-RSA-CAMELLIA128-SHA256 ECDHE secp256r1 256 yes 128 low ECDHE-RSA-CAMELLIA128-SHA256 ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES256-SHA ECDHE x25519 256 yes 128 low ECDHE-RSA-AES256-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES256-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES256-SHA ECDHE secp521r1 521 yes 260 low ECDHE-RSA-AES128-SHA ECDHE x25519 256 yes 128 low ECDHE-RSA-AES128-SHA ECDHE secp384r1 384 yes 192 low ECDHE-RSA-AES128-SHA ECDHE secp256r1 256 yes 128 low ECDHE-RSA-AES128-SHA ECDHE secp521r1 521 yes 260 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
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
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
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
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	
ECDHE	TLSv1.2	384	yes	192	low	

Info List

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
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

Info List

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
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

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

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

Finding #	15241996(990664772)	Severity	Information Gathered - Level 1
Unique #	befbcd07-c445-4b30-93e8-4acb1f388da6		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Encrypt_Then_MAC yes Heartbeat no 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	yes	TLSv1.2
Encrypt Then MAC	yes	TLSv1.2
Heartbeat	no	TLSv1.2
Truncated HMAC	no	TLSv1.2
Cipher priority controlled by	client	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2

INFO 42350 TLS Secure Renegotiation Extension Support Information (1)

INFO 42350 TLS Secure Renegotiation Extension Support Information

Finding #	15241992(990664768)	Severity	Information Gathered - Level 1
Unique #	7733c86b-d086-480e-aa9e-b029da911e96		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

INFO 45038 Host Scan Time - Scanner (1)

INFO 45038 Host Scan Time - Scanner

Finding #	15241981(990664756)	Severity	Information Gathered - Level 1
Unique #	f7d11858-80e6-4d13-acb1-5fc2ca96b8a3		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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: 1128 seconds

Start time: Tue, Nov 26 2024, 01:31:42 GMT

End time: Tue, Nov 26 2024, 01:50:30 GMT

INFO 86002 SSL Certificate - Information (1)

INFO 86002 SSL Certificate - Information

Finding #	15241990(990664766)	Severity	Information Gathered - Level 1
Unique #	720dc9db-3357-4882-9812-57d4978061d8		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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	10.1.242.13
IP	10.1.242.13
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _08:b4:4f:ba:19:44:db:b7:04:29:f6:36:52:65:7e:ff:c3:a0:c1:4e_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName TW _stateOrProvinceName Taiwan _localityName Taipei _organizationName GOYOURLIFE_INC. _organizationalUnitName RD _commonName reference.map8.zone _emailAddress service@goyourlife.com (0)SUBJECT_NAME _ countryName TW _stateOrProvinceName Taiwan _localityName Taipei _organizationName GOYOURLIFE_INC. _organizationalUnit RD _commonName reference.map8.zone _emailAddress service@goyourlife.com (0)Valid_From Nov_11_13:56:32_2021_GMT (0)Valid_Till Nov_11_13:56:32_2022_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0)_RSA_Public-Key: (2048_bit) (0)_Modulus: (0)_00:c7:f0:b0:ff:24:1a:bc:6a:9c:1d:87:2a:90:6b: (0)_f8:29:8e:85:aa:c0:9c:cb:0b:0c:a9:cf:ef:55:56: (0)_06:6a:8d:3b:c8:c9:1e:5d:b5:d7:03:cd:1b:e2:23: (0)_e0 38:42:cc:cd:bd:ba:9c:46:b3:53:fc:26:11: (0)_66:59:19:fd:42:ed:23:7b:61:6b:c9:03:29:36:08: (0)_74:44:af:a4:a6:a1:3f:70:f0:55:91:a4:62:46:ad: (0)_45:71:d2:bc:e1:39:d8:68:18:b2:aa:24:4b:a9:76: (0)_90:76:1e:30:7f:f3:85:58:85:e2:2c:ad:f9:2a:22: (0)_63:56:18:19:ac:54:2b:33:bb:ae:d7:4c:c7:e2:5e: (0)_31:5f:cd:15:3f:47:e0:cb:c0:77:58:0c:ee:19:1c: (0)_a3:f4:bd:7e:8b:09:f4:6b:68:4b:e3:c7:c5:9d:45: (0)_8d:0b:5a:2a:c0:34:fd:8f:40:4f:e4:a1:df:bc:d7: (0)_d5: 6d:e4:ad:ad:ae:12:7f:07:34:79:1e:30:6d: (0)_35:ed:fe:e2:33:16:c8:20:e7:0e:60:cf:f5:d5:b8: (0)_ae:30:06:ee:3a:1a:96:67:c7:b8:bd:f0:24:51:54: (0)_f4:0c:6d: 5a:40:a6:1a:65:fd:fd:a4:c1:01: (0)_34:d0:b8:9c:b2:7e:44:28:88:9c:39:72:43:51:95: (0)_2f:bf (0)_Exponent: 65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Subject_Key_Identifier 1A:B0:2E:03:5C:58:EE:F1:23:20:F4:F9:0D:E1:D4:B6:57:94:74:77 (0)X509v3_Authority_Key_Identifier _keyid:1A:B0:2E: 58:EE:F1:23:20:F4:F9:0D:E1:D4:B6:57:94:74:77 (0)X509v3_Basic_Constraints critical (0)_CA:TRUE (0)Signature (256_octets) (0) 21:61:9a:e5:20:fd: 26:91:23:ba:f7:b5:a4:8d:a8:4a (0) 48:d6:65:c8:52:8a:96:c1:06:3e:c4:eb:e5:0f:02:58 (0) b9:f5:87:c4:ba:37:84:51:1b:21:c5:39:0b:3b:11:8f (0) 07:07:23:2f:c7:ed:a0:52:38:e1:6c:3b:e5:bb:8e:da (0) 4b:8b:2c:c6:1b:7c:2e:76:30:66:1e:0a:1e:35:48:5e (0) 68:07:8f:85:26:2c:30:ee:74:11:9e:7d:db:bd:48:d1 42:66:54:12:dd:86:46:36:32:a3:51:8f:77:f9:09:57 (0) 18:50:d3:10:a0:82:38:15:c0:f1:b4:48:9b:89:b5:0a (0) 4b:3d:2c:da:91:e4:a7:0b:4d:c8:f9:4f:65:73:a7:0c (0) 95:0b:cc:9b:93:4c:ba:ce:1e:c9:9a:e7:54:09:34:60 (0) 5b:28:d7:f4:bc:13:89:5a:a4:d2:8f:95:59:1b:ca:a8 (0) 8f:44:1a:fc:22:d8:9d:f8:85:c6:29:41:95:e7:43:51 (0) 38:e3:a1:3a:94:1a:92:87:2a:ad:45:80:a3:b7 (0) 40:e2:6e:ed:d4:ef:ce:d4:b3:d5:84:a6:37:ca:3d:a2 (0) ae:4b:b5:76:49:5e:46:cf:f5:cd:d0:ab:6c:cd:d7:3a (0) 0c:5 8f:2d:72:ac:fa:72:b2:29:33:66:c9:5c:59

Info List

Info #1

Certificate Fingerprint:9F8218AA37B0D91C10172BB789C2795BFA58B0F6DBEA5A15F8F1BE4CD7371D48

INFO 150009 Links Crawled (1)

INFO 150009 Links Crawled

Finding #	15241987(990664762)	Severity	Information Gathered - Level 1
Unique #	ec9de2c7-3696-40e0-a1eb-060ac4d54d19		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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): 280.00
Number of links: 1
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://10.1.242.13/

INFO 150010 External Links Discovered (1)

INFO 150010 External Links Discovered

Finding #	15241983(990664758)	Severity	Information Gathered - Level 1
Unique #	01766d87-ab7d-4261-bb47-fd22dc159651		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

External links discovered during the scan are listed in the Results section. These links were out of scope for the scan and were not crawled.

Impact

N/A

Solution

N/A

Results

Number of links: 1
https://rcisuat.taiwanlife.com/

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

INFO 150020 Links Rejected By Crawl Scope or Exclusion List

Finding #	15241977(990664752)	Severity	Information Gathered - Level 1
Unique #	f47317e1-e5c2-4ae9-887e-04f0c1d2771b		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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)

External links discovered:
https://rcisuat.taiwanlife.com/./

IP based excluded links:

INFO 150021 Scan Diagnostics (1)

INFO 150021 Scan Diagnostics

Finding #	15241978(990664753)	Severity	Information Gathered - Level 1
Unique #	099459af-ef1d-4d9e-a1b9-93a356f332ac		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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 0 exclude list entries.
Loaded 0 allow list entries.
HTML form authentication unavailable, no WEBAPP entry found
Target web application page https://10.1.242.13/ fetched. Status code:502, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 1 minute (0 tests, 0 inputs)
VirtualHostDiscovery: 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #0 SameSiteScripting: estimated time < 1 minute (0 tests, 0 inputs)
SameSiteScripting: 0 vulnsigs tests, completed 0 requests, 0 seconds. No tests to execute.
Batch #0 CMSDetection: estimated time < 10 minutes (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, 169 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.
Collected 1 links overall in 0 hours 4 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.
WS Directory Path manipulation no tests enabled.
Batch #0 WS enumeration: estimated time < 1 minute (11 tests, 1 inputs)
WS enumeration: 11 vulnsigs tests, completed 11 requests, 6 seconds. Completed 11 requests of 11 estimated requests (100%). All tests completed.
Batch #4 WebCgiOob: estimated time < 10 minutes (157 tests, 1 inputs)
Batch #4 WebCgiOob: 157 vulnsigs tests, completed 134 requests, 83 seconds. Completed 134 requests of 196 estimated requests (68.3673%). All tests completed.
Insufficient Authentication token validation no tests enabled.
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, 3 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, 1 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 1 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 < 10 minutes (47 tests, 1 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 121 requests, 74 seconds. Completed 121 requests of 130 estimated requests (93.0769%). XSS optimization removed 58 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 1 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 1 requests, 3 seconds. Completed 1 requests of 1 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 0 requests, 0 seconds. No tests to execute.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(4 x 1) + paths:(11 x 1) = total (15)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 1 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 14 requests, 6 seconds. Completed 14 requests of 15 estimated requests (93.3333%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(1 x 1) + paths:(0 x 1) = total (1)

WAS Scan Report

Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 1 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 1 requests, 3 seconds. Completed 1 requests of 1 estimated requests (100%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 0) + files:(0 x 0) + directories:(16 x 1) + paths:(0 x 1) = total (16)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 1 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 16 requests, 40 seconds. Completed 16 requests of 16 estimated requests (100%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(1 x 0) + files:(8 x 0) + directories:(65 x 1) + paths:(11 x 1) = total (76)
Batch #5 Path manipulation: estimated time < 1 minute (85 tests, 1 inputs)
Batch #5 Path manipulation: 85 vulnsigs tests, completed 70 requests, 28 seconds. Completed 70 requests of 76 estimated requests (92.1053%). All tests completed.
Batch #5 WebCgiHrs: estimated time < 1 minute (1 tests, 1 inputs)
Batch #5 WebCgiHrs: 1 vulnsigs tests, completed 3 requests, 9 seconds. Completed 3 requests of 2 estimated requests (150%). All tests completed.
Batch #5 WebCgiGeneric: estimated time < 30 minutes (847 tests, 1 inputs)
Batch #5 WebCgiGeneric: 847 vulnsigs tests, completed 780 requests, 461 seconds. Completed 780 requests of 1251 estimated requests (62.3501%). 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: 280.00 (seconds)
Duration of Test Phase: 845.00 (seconds)
Total Scan Time: 1125.00 (seconds)

Total requests made: 1229
Average server response time: 2.92 seconds

Average browser load time: 2.93 seconds

INFO

150152 Forms Crawled (1)

INFO

150152 Forms Crawled

Finding #	15241979(990664754)	Severity	Information Gathered - Level 1
Unique #	c990ef31-2ead-4643-93c9-97e59480a738		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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

INFO

150247 Web Server and Technologies Detected (1)

INFO 150247 Web Server and Technologies Detected

Finding #	15241975(990664750)	Severity	Information Gathered - Level 1
Unique #	a758524d-c67e-4649-9160-5812649c6f90		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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: 1
Technology name: OpenResty
Technology version: OpenResty 1.15.8.2
Matched Components:
header match:
Server:openresty/1.15.8.2
Matched links: reporting only first 3 links
https://10.1.242.13/

INFO 150546 First Link Crawled Response Code Information (1)

INFO 150546 First Link Crawled Response Code Information

Finding #	15241982(990664757)	Severity	Information Gathered - Level 1
Unique #	110000d7-7518-48ce-98c9-e2861bc3c6ab		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/
Response Code: 502
Response Header:
Server: openresty/1.15.8.2
Date: Tue, 26 Nov 2024 01:32:35 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

Response Body:
<html><head><title>502 Bad Gateway</title></head>
<body>
<center><h1>502 Bad Gateway</h1></center>
<hr><center>openresty/1.15.8.2</center>

</body></html>

INFO 150845 Business logic abuse potential due to presence of external domains detected (1)

INFO 150845 Business logic abuse potential due to presence of external domains detected

Finding #	15712606(990664765)	Severity	Information Gathered - Level 1
Unique #	34fbf9b2-bd95-4539-afc4-c81389fe411c		
Group	Scan Diagnostics	Detection Date	26 Nov 2024 09:31 GMT+0800
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

External domains detected in the application. Using external domains in an application introduces risk by potentially exposing the application to external threats and dependencies, which can be exploited for malicious purposes such as data exfiltration, phishing, or compromise of application integrity. These vulnerabilities arise from inadequate validation, reliance on unsecured external services, and the application's failure to enforce strict security controls over external interactions.

Impact

N/A

Solution

Audit external domains accessed by your application. If possible launch scans against those.

Results

External domains could be involved in potential business logic abuse.
rcisuat.taiwanlife.com

Security Weaknesses (6)

INFO 150210 Information Disclosure via Response Header (1)

INFO 150210 Information Disclosure via Response Header

Finding #	15241973(990664748)	Severity	Information Gathered - Level 3
Unique #	d45c151b-33cd-4553-9f60-824d4688b6ce		
Group	Security Weaknesses	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/ response code: 502
Server: openresty/1.15.8.2

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

INFO 150202 Missing header: X-Content-Type-Options

Finding #	15241985(990664760)	Severity	Information Gathered - Level 2
Unique #	9dcf007f-5b21-4774-9654-63ad30892c18		
Group	Security Weaknesses	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/ response code: 502
Server: openresty/1.15.8.2
Date: Tue, 26 Nov 2024 01:32:35 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

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

GET https://10.1.242.13/ response code: 502

INFO 150206 Content-Security-Policy Not Implemented (1)

INFO 150206 Content-Security-Policy Not Implemented

Finding #	15241988(990664763)	Severity	Information Gathered - Level 2
Unique #	5cb85b86-73d8-43fe-b180-1e26fea78fc4		
Group	Security Weaknesses	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/ response code: 502
Server: openresty/1.15.8.2
Date: Tue, 26 Nov 2024 01:32:35 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

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

GET https://10.1.242.13/ response code: 502

INFO 150208 Missing header: Referrer-Policy (1)

INFO 150208 Missing header: Referrer-Policy

Finding #	15241974(990664749)	Severity	Information Gathered - Level 2
Unique #	4032f92d-485c-4080-8ea2-551f97959aa9		
Group	Security Weaknesses	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/ response code: 502
Server: openresty/1.15.8.2
Date: Tue, 26 Nov 2024 01:32:35 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

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

GET https://10.1.242.13/ response code: 502

INFO 150248 Missing header: Permissions-Policy (1)

INFO 150248 Missing header: Permissions-Policy

Finding #	15241980(990664755)	Severity	Information Gathered - Level 2
Unique #	208a73d7-1d20-4ae6-ad5e-28fde9c2bf58		
Group	Security Weaknesses	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/ response code: 502
Server: openresty/1.15.8.2
Date: Tue, 26 Nov 2024 01:32:35 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

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

GET https://10.1.242.13/ response code: 502

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

INFO 150204 Missing header: X-XSS-Protection

Finding #	15241989(990664764)	Severity	Information Gathered - Level 1
Unique #	6c98679b-7ea2-4422-b93b-afd3149468a8		
Group	Security Weaknesses	Detection Date	26 Nov 2024 09:31 GMT+0800
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://10.1.242.13/ response code: 502
Server: openresty/1.15.8.2
Date: Tue, 26 Nov 2024 01:32:35 GMT
Content-Type: text/html
Content-Length: 163
Connection: keep-alive
Strict-Transport-Security: max-age=31536000; includeSubDomains

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

GET https://10.1.242.13/ response code: 502

Appendix

Scan Details

RCIS_Web Application Vulnerability Scan - Nov 26, 2024 Slice #1	
Reference	was/1732584648927.68037539.1
Date	26 Nov 2024 09:31 GMT+0800
Mode	On-Demand
Progressive Scanning	Disabled
Type	Vulnerability
Authentication	None
Scanner Appliance	HQ0LUX246 (IP: 10.1.119.2, Scanner: 14.3.10-1, WAS: 9.8.64-1, Signatures: 2.6.198-2)
Profile	twlife
DNS Override	-
Duration	00:18:48
Status	Finished
Authentication Status	None

Option Profile Details

Form Submission	BOTH
Form Crawl Scope	Do not include form action URI in uniqueness calculation
Maximum links to test in scope	600
User Agent	-
Request Parameter Set	Initial Parameters
Document Type	Ignore common binary files
Enhanced Crawling	Disabled
SmartScan	Enabled
SmartScan Depth	10
Timeout Error Threshold	300
Unexpected Error Threshold	600
Performance Settings	Pre-defined
Scan Intensity	High
Bruteforce Option	Disabled
Detection Scope	Custom Search Lists
Include additional XSS payloads	No
Inclusion Search List Names	-
Exclusion Search List Names	SSL certificates verify, twlife : exclude list
Inclusion Search List QIDs	-
Exclusion Search List QIDs	38167, 38169, 38170, 38171, 38172, 38176, 38173, 38685, 38174, 151040, 150263, 150004, 150476
Credit Card Numbers Search	Off
Social Security Numbers (US) Search	Off

Web Application Details: RCIS_BATCH(DEV)

Name	RCIS_BATCH(DEV)
ID	1288134972

WAS Scan Report

URL	https://10.1.242.13/
Owner	oliver kuo (ctbcf_ik)
Scope	Limit to URL hostname
Tags	Taiwanlife, dev
Custom Attributes	-

Severity Levels Confirmed Vulnerabilities

Vulnerabilities (QIDs) are design flaws, programming errors, or mis-configurations that make your web application and web application platform susceptible to malicious attacks. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information to a complete compromise of the web application and/or the web application platform. Even if the web application isn't fully compromised, an exploited vulnerability could still lead to the web application being used to launch attacks against users of the site.

<div><div></div><div></div><div></div><div></div><div></div></div>	Minimal	Basic information disclosure (e.g. web server type, programming language) might enable intruders to discover other vulnerabilities, but lack of this information does not make the vulnerability harder to find.
<div><div></div><div></div><div></div><div></div><div></div></div>	Medium	Intruders may be able to collect sensitive information about the application platform, such as the precise version of software used. With this information, intruders can easily exploit known vulnerabilities specific to software versions. Other types of sensitive information might disclose a few lines of source code or hidden directories.
<div><div></div><div></div><div></div><div></div><div></div></div>	Serious	Vulnerabilities at this level typically disclose security-related information that could result in misuse or an exploit. Examples include source code disclosure or transmitting authentication credentials over non-encrypted channels.
<div><div></div><div></div><div></div><div></div><div></div></div>	Critical	Intruders can exploit the vulnerability to gain highly sensitive content or affect other users of the web application. Examples include certain types of cross-site scripting and SQL injection attacks.
<div><div></div><div></div><div></div><div></div><div></div></div>	Urgent	Intruders can exploit the vulnerability to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture.

Potential Vulnerabilities

Potential Vulnerabilities indicate that the scanner observed a weakness or error that is commonly used to attack a web application, and the scanner was unable to confirm if the weakness or error could be exploited. Where possible, the QID's description and results section include information and hints for following-up with manual analysis. For example, the exploitability of a QID may be influenced by characteristics that the scanner cannot confirm, such as the web application's network architecture, or the test to confirm exploitability requires more intrusive testing than the scanner is designed to conduct.




<div><div></div><div></div><div></div><div></div><div></div></div>	Minimal	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example in this scenario, information such as web server type, programming language, passwords or file path references can be disclosed.
<div><div></div><div></div><div></div><div></div><div></div></div>	Medium	Presence of this vulnerability is indicative of basic information disclosure (e.g. web server type, programming language) and might enable intruders to discover other vulnerabilities. For example version of software or session data can be disclosed, which could be used to exploit.
<div><div></div><div></div><div></div><div></div><div></div></div>	Serious	Presence of this vulnerability might give access to security-related information to intruders who are bound to misuse or exploit. Examples of what could happen if this vulnerability was exploited include bringing down the server or causing hindrance to the regular service.
<div><div></div><div></div><div></div><div></div><div></div></div>	Critical	Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.
<div><div></div><div></div><div></div><div></div><div></div></div>	Urgent	Presence of this vulnerability might enable intruders to compromise the web application's data store, obtain information from other users' accounts, or obtain command execution on a host in the web application's architecture. For example in this scenario, the web application users can potentially be targeted if the application is exploited.

Sensitive Content

Sensitive content may be detected based on known patterns (credit card numbers, social security numbers) or custom patterns (strings, regular expressions), depending on the option profile used. Intruders may gain access to sensitive content that could result in misuse or other exploits.

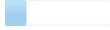


<div><div></div><div></div><div></div><div></div><div></div></div>
--

WAS Scan Report

	Minimal	Sensitive content was found in the web server response. During our scan of the site form(s) were found with field(s) for credit card number or social security number. This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.
	Medium	Sensitive content was found in the web server response. Specifically our service found a certain sensitive content pattern (defined in the option profile). This information disclosure could result in a confidentiality breach and could be a target for intruders. For this reason we recommend caution.
	Serious	Sensitive content was found in the web server response - a valid social security number or credit card information. This information disclosure could result in a confidentiality breach, and it gives intruders access to valid sensitive content that could be misused.

Information Gathered

Information Gathered issues (QIDs) include visible information about the web application's platform, code, or architecture. It may also include information about users of the web application.

	Minimal	Intruders may be able to retrieve sensitive information related to the web application platform.
	Medium	Intruders may be able to retrieve sensitive information related to internal functionality or business logic of the web application.
	Serious	Intruders may be able to detect highly sensitive data, such as personally identifiable information (PII) about other users of the web application.