WAS Scan Report

Qualys. Express

Scan Report

22 Aug 2025

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

Sravan Kumar Medishetty
vctry3sm

Victory Live
3060 Peachtree Road Northwest 3060 Peachtree Rd Suite 1625, Atlanta, GA 30305
hyderabad, Andhra Pradesh 500098
India

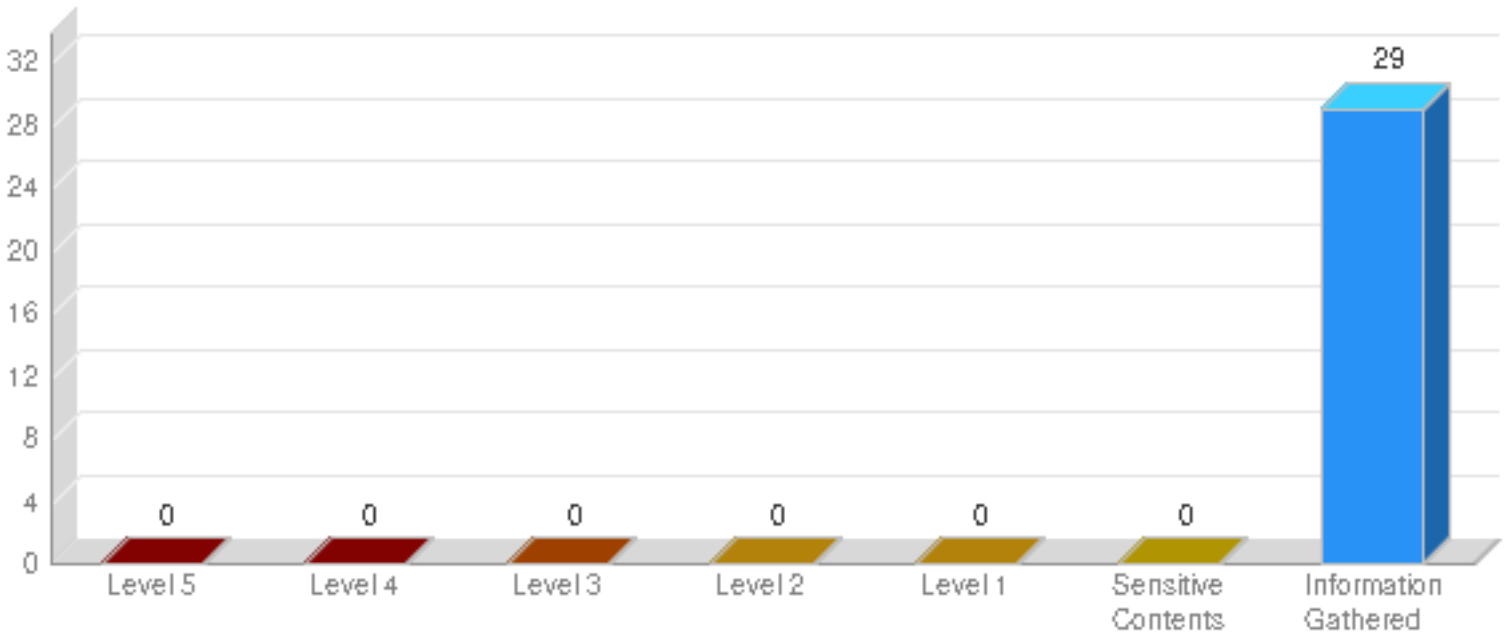
Target and Filters

Scans (1)	VL - Aug 22, 2025
Web Applications (1)	VL

Summary

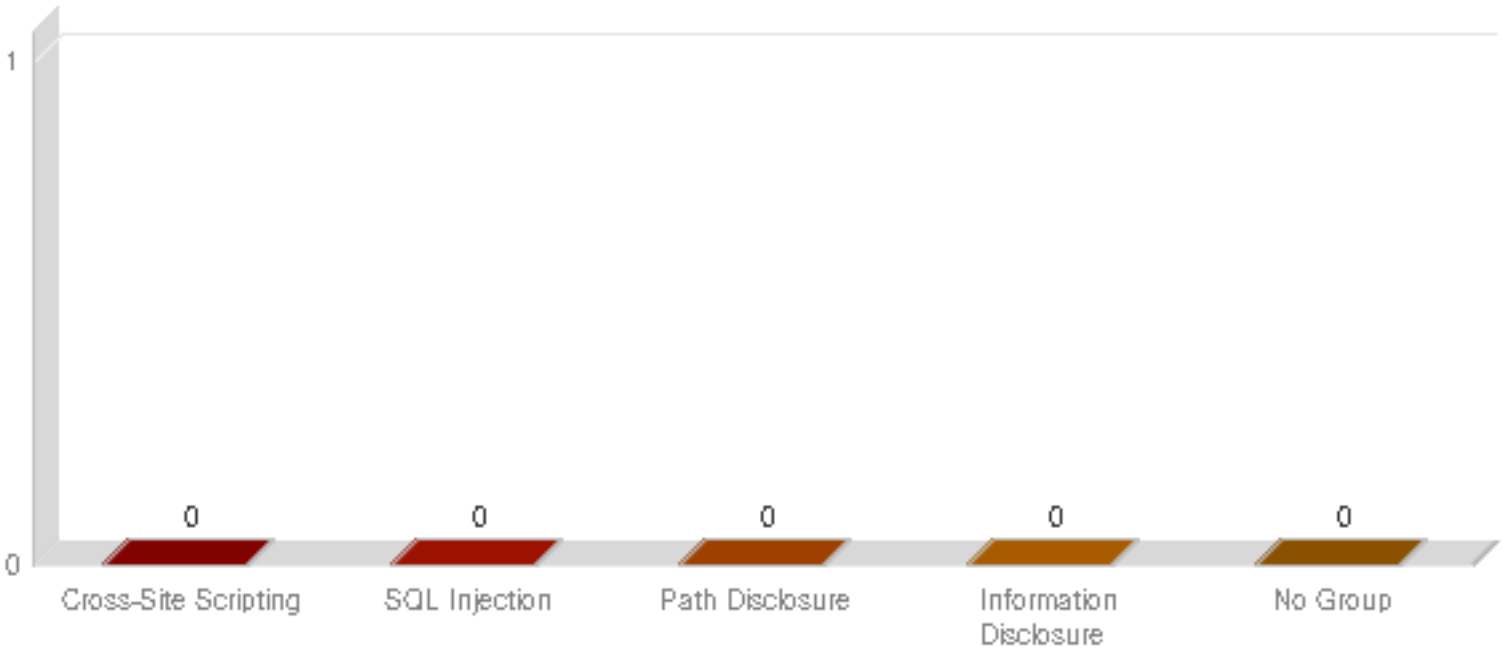
Security Risk	Vulnerabilities	Sensitive Contents	Information Gathered
-	0	0	29

Findings by Severity

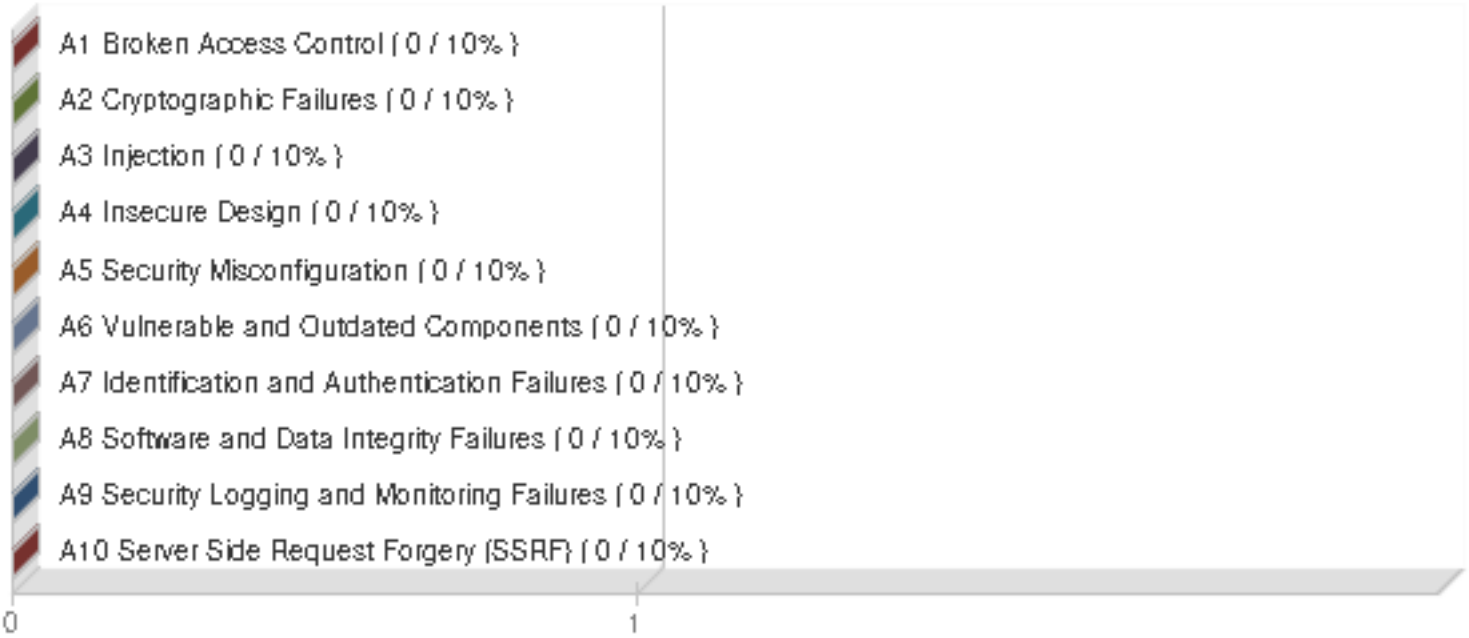


WAS Scan Report

Vulnerabilities by Group



OWASP Top 10 2021 Vulnerabilities



Scan	Date	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
VL - Aug 22, 2025	22 Aug 2025 21:02 GMT +0630	0	0	0	0	0	0	29

WAS Scan Report

Results(29)

Information Gathered (29)

Information Disclosure (1)

150228 Subdomains Found During Crawling (1)

150228 Subdomains Found During Crawling

Finding #	**16653934**(375112106)	Severity	Information Gathered - Level 1
Unique #	**ff50efe1-c6e9-45b7-871b-db6a193e9c5b**		
Group	Information Disclosure	Detection Date	22 Aug 2025 21:02 GMT+0630
CWE	-		
OWASP	-		
WASC	-		

Details

Threat
Sub-domains are reported under this section.

Impact
N/A

Solution
N/A

Results

Number of subdomain links: 1
https://login.victorylive.com

Scan Diagnostics (20)

150067 Links Discovered During User-Agent and Mobile Site Checks (1)

WAS Scan Report

150067 Links Discovered During User-Agent and Mobile Site Checks

Finding #	**16653933**(375112105)	**Severity**	Information Gathered - Level 3
Unique #	**0f46da1e-d09d-40c4-989b-59f08fdeed0f**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Links were discovered via requests using an alternate User-Agent or guessed based on common mobile device URI patterns. The scanner attempts to determine if the Web application changes its behavior when accessed by mobile devices. These checks are based on modifying the User-Agent, changing the domain name, and appending common directories.

The extra links discovered by the Web application scanner during User-Agent manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures irrespective of browser platform, type or version used to access the application. If the Web application fails to apply security controls to alternate representations of the site, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

No specific vulnerability has been discovered that requires action to be taken. These links are provided to ensure that a review of the web application includes all possible access points.

Results

Unique content discovered during User-Agent and common mobile device specific subdomains and paths manipulation:

Detected based on: Unique redirect URI
User-Agent: Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_1_2 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7D11 Safari/528.16
URI: http://one.victorylive.com/mobile
Redirect URI(307): https://one.victorylive.com/mobile

Detected based on: Unique redirect URI
User-Agent: Opera/9.80 (IPhone; Opera Mini/5.0.019802/886; U; en) Presto/2.4.15
URI: http://one.victorylive.com/mobile
Redirect URI(307): https://one.victorylive.com/mobile

6 DNS Host Name (1)

WAS Scan Report

6 DNS Host Name

Finding #	**16653943**(375112115)	**Severity**	Information Gathered - Level 1
Unique #	**205fe61b-b0cf-4402-b0be-60e06d315430**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	-
Virtual Host	104.46.117.181
IP	104.46.117.181
Port	-
Result	#table IP_address Host_name 104.46.117.181 one.victorylive.com 104.46.117.181 No_registered_hostname

Info List

Info #1

38116 SSL Server Information Retrieval (1)

WAS Scan Report

38116 SSL Server Information Retrieval

Finding #	**16653950**(375112122)	**Severity**	Information Gathered - Level 1
Unique #	**758264fd-87cd-4cf9-a96d-78d813d7abba**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
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 _ _ _ ECDHE-RSA-AES128-GCM-SHA256 ECDH RSA AEAD AESGCM(128) MEDIUM ECDHE-RSA-AES256-GCM-SHA384 ECDH RSA AEAD AESGCM(256) HIGH ECDHE-RSA-CHACHA20-POLY1305 ECDH RSA AEAD CHACHA20/POLY1305(256) HIGH TLSv1.3_PROTOCOL_IS_ENABLED _ _ _ _ _ TLS13-AES-128-GCM-SHA256 N/A N/A AEAD AESGCM(128) MEDIUM TLS13-AES-256-GCM-SHA384 N/A N/A AEAD AESGCM(256) HIGH TLS13-CHACHA20-POLY1305-SHA256 N/A N/A AEAD CHACHA20/POLY1305(256)

Info List

Info #1

Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
TLS13-AES-128-GCM-SHA256	N/A	AESGCM(128)	MEDIUM	N/A	AEAD	TLSv1.3
TLS13-AES-256-GCM-SHA384	N/A	AESGCM(256)	HIGH	N/A	AEAD	TLSv1.3
TLS13-CHACHA20-POLY1305-SHA256	N/A	CHACHA20/POLY1305(256)	HIGH	N/A	AEAD	TLSv1.3

38291 SSL Session Caching Information (1)

WAS Scan Report

38291 SSL Session Caching Information

Finding #	**16653944**(375112116)	**Severity**	Information Gathered - Level 1
Unique #	**890b8b29-6df9-49c2-a497-4480585f4ecd**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
Port	443
Result	TLSv1.2 session caching is enabled on the target. TLSv1.3 session caching is enabled on the target.

Info List

Info #1

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

WAS Scan Report

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

Finding #	**16653949**(375112121)	**Severity**	Information Gathered - Level 1
Unique #	**13df7c1f-71e0-4eeb-80a9-a7211f5d3d27**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
Port	443
Result	#table cols=2 my_version target_version 0304 0303 0399 0303 0400 0303 0499 0303

Info List

Info #1

38600 SSL Certificate will expire within next six months (1)

WAS Scan Report

38600 SSL Certificate will expire within next six months

Finding #	**16653946**(375112118)	**Severity**	Information Gathered - Level 1
Unique #	**4610da49-cfe1-4ee1-a4f4-8ccd7588efe0**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

Certificates are used for authentication purposes in different protocols such as SSL/TLS. Each certificate has a validity period outside of which it is supposed to be considered invalid. This QID is reported to inform that a certificate will expire within next six months. The advance notice can be helpful since obtaining a certificate can take some time.

Impact

Expired certificates can cause connection disruptions or compromise the integrity and privacy of the connections being protected by the certificates.

Solution

Contact the certificate authority that signed your certificate to arrange for a renewal.

SSL Data

Flags	-
Protocol	tcp
Virtual Host	104.46.117.181
IP	104.46.117.181
Port	443
Result	Certificate #0 CN=*.victorylive.com The certificate will expire within six months: Nov 20 13:57:49 2025 GMT

Info List

Info #1

Certificate Fingerprint:2D9736FE6985D62BD37BF224B7B052FD85BBA981845DA2B408FE999809DBC857

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

WAS Scan Report

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

Finding #	**16653951**(375112123)	**Severity**	Information Gathered - Level 1
Unique #	**1fcb6641-7ec9-4e01-bfc1-76545391f11e**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
Port	443
Result	#table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ ECDHE x25519 256 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes 260 low ECDHE secp384r1 384 yes 192 low TLSv1 _ _ _ ECDHE x25519 256 yes 128 low ECDHE secp256r1 256 yes 128 low ECDHE x448 448 yes 224 low ECDHE secp521r1 521 yes 260 low ECDHE secp384r1 384 yes 192 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size	Fwd Sec	Classical	Quantam
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	256	yes	128	low
ECDHE		TLSv1.2	448	yes	224	low
ECDHE		TLSv1.2	521	yes	260	low
ECDHE		TLSv1.2	384	yes	192	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	256	yes	128	low
ECDHE		TLSv1.3	448	yes	224	low
ECDHE		TLSv1.3	521	yes	260	low
ECDHE		TLSv1.3	384	yes	192	low

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

WAS Scan Report

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

Finding #	**16653952**(375112124)	**Severity**	Information Gathered - Level 1
Unique #	**1fdd033f-3261-427f-a90b-3df99c73a12c**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Heartbeat no Cipher_priority_controlled_by server OCSP_stapling no SCT_extens TLSv1.3 _ Heartbeat no Cipher_priority_controlled_by server OCSP_stapling no SCT_extension no

Info List

Info #1

Props

Name	Value	Protocol
Extended Master Secret	yes	TLSv1.2
Heartbeat	no	TLSv1.2
Cipher priority controlled by	server	TLSv1.2
OCSP stapling	no	TLSv1.2
SCT extension	no	TLSv1.2
Heartbeat	no	TLSv1.3
Cipher priority controlled by	server	TLSv1.3
OCSP stapling	no	TLSv1.3
SCT extension	no	TLSv1.3

38718 Secure Sockets Layer (SSL) Certificate Transparency Information (1)

WAS Scan Report

38718 Secure Sockets Layer (SSL) Certificate Transparency Information

Finding #	**16653947**(375112119)	**Severity**	Information Gathered - Level 1
Unique #	**8d52aae2-83dc-4b95-9002-ff8ca03e7653**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

SSL Certificate Transparency is an industry effort to improve visibility into the process of how certificate authorities issue certificates. It is designed to allow the owners of domain names to find all certificates that have been issued for their domains, and which certificate authorities have issued them. This is done by requiring certificate authorities to publish all issued certificates in public logs. TLS servers can then provide cryptographic evidence to TLS clients that the server certificate has been registered in public logs, thus providing some degree of confidence that the certificate is legitimate. Such cryptographic evidence is referred to as an "SCT Log Proof".

The information below lists all validated SCT Log Proofs for server certificates along with information about the public log, where available.

Impact
N/A

Solution
N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	104.46.117.181
IP	104.46.117.181
Port	443
Result	#table cols="6" Source Validated Name URL ID Time Certificate_#0 _ CN=*.victorylive.com _ _ _ Certificate no (unknown) (unknown) 12f14e34bd53724c840619c38f3f7a13f8e7b56287889c6d300584ebe586263a Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 7d591e12e1782a7b1c61677c5efdf8d0875c14a04e959eb9032fd90e8c2e79b8 Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) ccfb0f6a85710965fe959b53cee9b27c22e9855c0d978db6a97e54c0fe4c0db0 Thu_01_Jan_1970_12:00:00_AM_GMT

Info List

Info #1

Certificate Fingerprint:2D9736FE6985D62BD37BF224B7B052FD85BBA981845DA2B408FE999809DBC857

42350 TLS Secure Renegotiation Extension Support Information (1)

WAS Scan Report

42350 TLS Secure Renegotiation Extension Support Information

Finding #	**16653948**(375112120)	**Severity**	Information Gathered - Level 1
Unique #	**09b860a7-062b-4678-a710-880516a963dd**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

Info List

Info #1

45038 Host Scan Time - Scanner (1)

WAS Scan Report

45038 Host Scan Time - Scanner

Finding #	**16653953**(375112125)	**Severity**	Information Gathered - Level 1
Unique #	**c92b5af6-aad2-4adf-953f-a811332a9a44**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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

SSL Data

Flags	-
Protocol	-
Virtual Host	one.victorylive.com
IP	104.46.117.181
Port	-
Result	Scan duration: 1161 seconds Start time: Fri Aug 22 15:32:03 UTC 2025 End time: Fri Aug 22 15:51:24 UTC 2025

Info List

Info #1

86002 SSL Certificate - Information (1)

WAS Scan Report

86002 SSL Certificate - Information

Finding #	**16653945**(375112117)	**Severity**	Information Gathered - Level 1
Unique #	**3697d1d4-ae05-4968-ada9-f046dc818184**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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	104.46.117.181
IP	104.46.117.181
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _22:ce:69:ff:3e:1b:0e:7a_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _stateOrProvinceName Arizona _localityName Scottsdale _organizationName "GoDaddy.com,_Inc." _organizationalUnitName http://certs.godaddy.com/repository/ _commonName Go_Daddy_Secure_Certificate_Authority_-_G2 (0)SUBJECT_NAME _ commonName *.victorylive.com (0)Valid_From Nov_20_13:57:49_2024_GMT (0)Valid_Till Nov_20_13:57:49_2025_GMT (0)Public_Key_Algorithm rsaEncryption (0)RSA_Public_Key (2048_bit) (0) _RSA_Public-Key:_(2048_bit) (0) _Modulus: (0) _00:a6:93:24:2e: 05:ba:c9:ca:eb:d0:15:76:64:85: (0) _c8:52:a3:97:44:d3:ca:ce:d9:00:c6:bd:4f:1e:e6: (0) _a4:e3:36:fa:c5:9e:7e:a6:a6:67:e7:b0:86:fc:40: (0) _42:48:24:41:59:69:e8:ec:41:19:9f:89:60:48:17: (0) _bc:31:fe:ad:da:49:e8:e6:76:ea:bd:b8:7a:21:a8: (0) _60:0b:48:2b:88:f3:af:3e:dd:60:50:76:f2:51:a5: (0) _a7:49:55:24:0f:9e:b6:d1:d5:77:33:e4:92:76:2b: (0) _1b:4c:5f:f2:fb:c6:8e:25:31:ec:f5:50:49:6a:b9: (0) _12:10:a9:3e:50:6f:1b:50:d5:b5:91:b1:a1:89:87: (0) _4e:cb:bb:07:29:88:11:78:3c:67:1d:2d:3d:ef:dd: (0) _1f:4b:7b:54:4b:58:5f:0b:4b:c9:6a:a5:e4:6e:2a: (0) _a6:fc:fe:d5:a8:71:e5:bd:7d:bb:0d:64:1e:4d:8d: (0) _07:d7:f2:61:fb:6b:b0:76:70:c0:60:53:58:58:80: (0) _ab:71:d6:12:22:a4:7e:56:9f:1a:35:d6:d2:ea:4f: (0) _9f:36:43:0b:d5:2e:5b:d1:8d:40:ed:fc:4b:fb:5a: (0) _49:87:00:29:d8:56:87:d1:31:86:ed:79:b2:06:f4: (0) _6e:a5:58:cc:ac:e5:46:ec:37:1b:45:56:14:e3:e5: (0) _7e:a3 (0) _Exponent:_65537_(0x10001) (0)X509v3_EXTENSIONS _ (0)X509v3_Basic_Constraints critical (0) _CA:FALSE (0)X509v3_Extended_Key_Usage _TLS_Web_Server_Authentication,_TLS_Web_Client_Authentication (0)X509v3_Key_Usage critical (0) _Digital_Signature,_Key_Encipherment (0)X509v3_CRL_Distribution_Points (0) _Full_Name: (0) _URI:http://crl.godaddy.com/gdig2s1-33502.crl (0)X509v3_Certificate_Policies _Policy:_2.16.840.1.114413.1.7.23.1 (0) _CPS:_http://certificates.godaddy.com/repository/ (0) _Policy:_2.23.140.1.2.1 (0)Authority_Information_Access _OCS _URI:http://ocsp.godaddy.com/ (0) _CA_Issuers_-_URI:http://certificates.godaddy.com/repository/gdig2.crt (0)X509v3_Authority_Key_Identifier _keyid:40:C2: 27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE (0)X509v3_Subject_Alternative_Name _DNS:*.victorylive.com,_DNS:victorylive.com (0)X509v3_Subject_Key_Identifier _E7:ED:9A:A0:2D:8A:30:3F:BF:AB:26:07:5B:BE:FA:CC:FC:DA:2F:F0 (0)CT_Precertificate_SCTs _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_12:F1:4E:34:BD:53:72:4C:84:06:19:C3:8F:3F:7A:13: (0) _F8:E7:B5:62:87:88:9C:6D 30:05:84:EB:E5:86:26:3A (0) _Timestamp_:_Nov_20_13:57:50.455_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:46:02:21:00:B3:17:89:7A:BF:DB:35:C0:FD:8E:E8: (0) _CB:46:7E:1F:D7:B2:B1:94:A9:2A:1E:1E:84:5B:74:FE: (0) _BD:90:22:43:0F:02:21:00:A5:5F: 84:57:F7:7F:AF:97: (0) _62:32:C9:1F:A5:9E:08:EE:AE:EE:BA:86:66:E6:F6:9A: (0) _A3:AD:35:1C:3E:9E:75:84 (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_7D:59:1E:12:E1:78:2A:7B:1C:61:67:7C:5E:FD:F8:D0: (0) _87:5C:14:A0:4E:95:9E:B9:03:2F:D9:0E:8C:2E:79:B8 (0) _Timestamp_:_Nov_20_13:57:50.712_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:70:63:3A:B9:3C: 16:23:AC:D6:89:1A:1B: (0) _83:E2:2B:EB:6D:36:D8:94:0A:68:2F:1D:19:A2:2F:48: (0) _7A:03:62:93:02:20:09:F2:D1:64:CB:25:16:B5:1E:A7: (0) _DD:D4:9C:EA:E3:B3:70:BF:E5:31:0E:17:34:C5:6C:20: (0) _B3:75:92:CF:F7:BD (0) _Signed_Certificate_Timestamp: (0) _Version_:_v1_(0x0) (0) _Log_ID_:_CC:FB:0F:6A:85:71:09:65:FE:95:9B:53:CE:E9:B2:7C: (0) _22:E9:85:5C:0D:97:8D:B6:A9:7E:54:C0:FE:4C:0D:B0 (0) _Timestamp_:_Nov_20_13:57:53.824_2024_GMT (0) _Extensions:_none (0) _Signature_:_ecdsa-with-SHA256 (0) _30:44:02:20:4F:C5:DE:19:AE: 66:F1:D2:1E:E9:63:46: (0) _73:08:67:F6:EA:24:8C:3B:DC:40:93:FC:B3:16:B2:A8: (0) _BD:86:11:54:02:20:4A:37:7E:B6:32:53:3C:D0:D9:3A: (0) _35:EA:3F: 89:10:56:5E:47:37:A2:BE:71:3F:3A:76:46: (0) _E4:7A:67:33:90:DE (0)Signature (256_octets) (0) 31:9f:d5:93:c7:a7:d2:a6:50:a0:30:16:e3:e8:93:dc (0) 54:f6:b 46:cb:45:99:5a:86:54:b1:e3:7a:40:c4 (0) 63:d0:8b:65:2f:b8:d6:60:40:ed:82:06:9f:f7:69:f6 (0) a7:2a:45:ea:ce:3f:a9:86:79:63:7b:c0:e4:04:f6:7c (0) f7:0b:d2:08:87:d9:8a:95:ab:4a:73:ca:55:bb:ae:21 (0) 59:94:e5:4c:25:8e:85:f9:04:67:15:83:f6:30:de:92 (0) 72:f1:8a:f1:ce:53:c2:18:97:d6:4b:00:87:47:af:14 (0) e 20:d1:5c:54:bc:12:c4:c6:a5:00:fe:66:e8:4c (0) e6:8c:0c:a0:13:57:d7:61:d6:db:fe:fd:fc:fd:d2:ba (0) d1:3c:c9:66:03:58:f3:29:41:40:86:c5:09:d1:e9:b1 (0) 35:1a: 11:f2:51:ed:e9:21:82:7b:74:3c:3d:c6:68:92 (0) d7:94:94:11:c5:50:91:87:b2:93:f9:9d:6a:fd:23:b6 (0) 79:d6:f2:fd:32:c5:dd:8b:28:51:92:93:3e:7d:6d:81 (0) 5e: 26:fc:c8:ea:fe:d7:85:a0:33:ee:25:a2:59:60:93 (0) 43:7b:d8:7b:18:60:13:a7:bb:5c:fd:7e:aa:05:6c:3d (0) 8d:4a:a6:e6:03:9d:b4:00:f8:1f:f7:18:97:c2:42:e9 (1)CERTIFICATE_1 _ (1)Version 3_(0x2) (1)Serial_Number 7_(0x7) (1)Signature_Algorithm sha256WithRSAEncryption (1)ISSUER_NAME _ countryName U _stateOrProvinceName Arizona _localityName Scottsdale _organizationName "GoDaddy.com,_Inc." _commonName Go_Daddy_Root_Certificate_Authority_

WAS Scan Report

(1)SUBJECT_NAME _ countryName US _stateOrProvinceName Arizona _localityName Scottsdale _organizationName "GoDaddy.com,_Inc." _organizationalUnitName http://certs.godaddy.com/repository/ _commonName Go_Daddy_Secure_Certificate_Authority_-_G2 (1)Valid_From May_3_07:00:00_2011_GMT (1)Valid_Till May_3_07:00:00_2031_GMT (1)Public_Key_Algorithm rsaEncryption (1)RSA_Public_Key (2048_bit) (1) _RSA_P Key:_(2048_bit) (1) _Modulus: (1) _00:b9:e0:cb:10:d4:af:76:bd:d4:93:62:eb:30:64: (1) _b8:81:08:6c:c3:04:d9:62:17:8e:2f:ff:3e:65:cf: (1) _8f:ce:62:e6:3c:52:1 16:45:4b:55:ab:78:6b: (1) _63:83:62:90:ce:0f:69:6c:99:c8:1a:14:8b:4c:cc: (1) _45:33:ea:88:dc:9e:a3:af:2b:fe:80:61:9d:79:57: (1) _c4:cf:2e:f4:3f:30:3c:5d:47:f 16:bc:c3:37: (1) _96:41:51:8e:11:4b:54:f8:28:be:d0:8c:be:f0:30: (1) _38:1e:f3:b0:26:f8:66:47:63:6d:de:71:26:47:8f: (1) _38:47:53:d1:46:1d:b4:e3:dc:00:ea: 45:ac:bd:bc: (1) _71:d9:aa:6f:00:db:db:cd:30:3a:79:4f:5f:4c:47: (1) _f8:1d:ef:5b:c2:c4:9d:60:3b:b1:b2:43:91:d8:a4: (1) _33:4e:ea:b3:d6:27:4f:ad: 25:8a:a5:c6:f4:d5:d0: (1) _a6:ae:74:05:64:57:88:b5:44:55:d4:2d:2a:3a:3e: (1) _f8:b8:bd:e9:32:0a:02:94:64:c4:16:3a:50:f1:4a: (1) _ae:e7:79:33:af:0c:20:07:7 04:39:c2:69: (1) _02:6c:63:52:fa:77:c1:1b:c8:74:87:c8:b9:93:18: (1) _50:54:35:4b:69:4e:bc:3b:d3:49:2e:1f:dc:c1:d2: (1) _52:fb (1) _Exponent:_65537_(0x100 (1)X509v3_EXTENSIONS _ (1)X509v3_Basic_Constraints critical (1) _CA:TRUE (1)X509v3_Key_Usage critical (1) _Certificate_Sign,_CRL_Sign (1)X509v3_Subject_Key_Identifier _40:C2:BD:27:8E:CC:34:83:30:A2:33:D7:FB:6C:B3:F0:B4:2C:80:CE (1)X509v3_Authority_Key_Identifier _keyid:3A:9A: 85:07:10:67:28:B6:EF:F6:BD:05:41:6E:20:C1:94:DA:0F:DE (1)Authority_Information_Access _OCSP_-_URI:http://ocsp.godaddy.com/ (1)X509v3_CRL_Distribution_Points (1) _Full_Name: (1) _URI:http://crl.godaddy.com/gdroot-g2.crl (1)X509v3_Certificate_Policies _Policy:_X509v3_Any_P (1) _CPS:_https://certs.godaddy.com/repository/ (1)Signature (256_octets) (1) 08:7e:6c:93:10:c8:38:b8:96:a9:90:4b:ff:a1:5f:4f (1) 04:ef:6c:3e:9c: 88:06:c9:50:8f:a6:73:f7:57:31:1b (1) be:bc:e4:2f:db:f8:ba:d3:5b:e0:b4:e7:e6:79:62:0e (1) 0c:a2:d7:6a:63:73:31:b5:f5:a8:48:a4:3b:08:2d:a2 (1) 5d:90:d7:b4:7 11:56:30:c4:b6:44:9d:7b:2c (1) 9d:e5:5e:e6:ef:0c:61:aa:bf:e4:2a:1b:ee:84:9e:b8 (1) 83:7d:c1:43:ce:44:a7:13:70:0d:91:1f:f4:c8:13:ad (1) 83:60:d9:d8:72:a8:73:24:1e:b5:ac:22:0e:ca:17:89 (1) 62:58:44:1b:ab:89:25:01:00:0f:cd:c4:1b:62:db:51 (1) b4:d3:0f:51:2a:9b:f4:bc:73:fc:76:ce:36:a4:cd:d9 (1 d8:2c:ea:ae:9b:f5:2a:b2:90:d1:4d:75:18:8a:3f:8a (1) 41:90:23:7d:5b:4b:fe:a4:03:58:9b:46:b2:c3:60:60 (1) 83:f8:7d:50:41:ce:c2:a1:90:c3:bb:ef:02:2f:d2:15 (1) 44:15:d9:0a:ae:a7:8a:33:ed:b1:2d:76:36:26 (1) dc:04:eb:9f:f7:61:1f:15:dc:87:6f:ee:46:96:28:ad (1) a1:26:7d:0a:09:a7:2e:04:a3:8d:bc:f8:bc:04:30:01 (2)CERTIFICATE_2 _ (2)Version 3_(0x2) (2)Serial_Number 1828629_(0x1be715) (2)Signature_Algorithm sha256WithRSAEncryption (2)ISSUER_NAME _ countryName US _organizationName "The_Go_Daddy_Group,_Inc." _organizationalUnitName Go_Daddy_Class_2_Certification_Authority (2)SUBJECT_NA countryName US _stateOrProvinceName Arizona _localityName Scottsdale _organizationName "GoDaddy.com,_Inc." _commonName Go_Daddy_Root_Certificate_Authority_-_G2 (2)Valid_From Jan_1_07:00:00_2014_GMT (2)Valid_Till May_30_07:00:00_2031_GMT (2)Public_Key_Algorith rsaEncryption (2)RSA_Public_Key (2048_bit) (2) _RSA_Public-Key:_(2048_bit) (2) _Modulus: (2) _00:bf:71:62:08:f1:fa:59:34:f7:1b:c9:18:a3:f7: (2) _80:49:58:e9:22:83:13:a6:c5:20:43:01:3b:84:f1: (2) _e6:85:49:9f:27:ea:f6:84:1b:4e:a0:b4:db:70:98: (2) _c7:32:01:b1:05:3e:07:4e:ee:f4:fa:4f:2f:59:30: (2) _22:e7:ab:19:56:6b:e2:80:07:fc:f3:16:75:80:39: (2) _51:7b:e5:f9:35:b6:74:4e:a9:8d:82:13:e4:b6:3f: (2) _a9:03:83:fa:a2:be:8a:15:6a:7f:de:0b:c3:b6:19: (2) _14:05:ca:ea:c3:a8:04:94:3b:46:7c:32:0d:f3:00: (2) _66:22:c8:8d:69:6d:36:8c:11:18:b7:d3:b2:1c:60: (2) _b4:38:fa:02:8c:ce:d3:dd:46:07:de:0a:3e:eb:5d: (2) _7c:c8:7c:fb:b0:2b:53:a4:92:62:69:51:25:05:61: (2) _1a:44:81:8c:2c:a9:43:96:23:df:ac:3a:81:9a:0e: (2) _29:c5:1c:a9:e9:5d:1e:b6:9e:9e:30:0a:39:ce:f1: (2) _88:80:fb:4b:5d:cc:32:ec:85:62:43:25:34:02:56: (2) _27:01:91:b4:3b:70:2a:3f:6e:b1:e8:9c:88:01:7d: (2) _9f:d4:f9:db:53:6d:60:9d:bf:2c:e7:58:ab:b8:5f: (2) _46:fc:ce:c4:1b:03:3c:09:eb:49:31:5c:69:46:b3: (2) _e0:47 (2) _Exponent:_65537_(0x10001) (2)X509v3_EXTENSIONS _ (2)X509v3_Basic_Constraints criti _CA:TRUE (2)X509v3_Key_Usage critical (2) _Certificate_Sign,_CRL_Sign (2)X509v3_Subject_Key_Identifier _3A:9A:85:07:10:67:28:B6:EF:F6:BD:05:41:6 20:C1:94:DA:0F:DE (2)X509v3_Authority_Key_Identifier _keyid:D2:C4:B0:D2:91:D4:4C:11:71:B3:61:CB:3D:A1:FE:DD:A8:6A:D4:E3 (2)Authority_Information_Access _OCSP_-_URI:http://ocsp.godaddy.com/ (2)X509v3_CRL_Distribution_Points (2) _Full_Name: (2) _URI:http://crl.godaddy. gdroot.crl (2)X509v3_Certificate_Policies _Policy:_X509v3_Any_Policy (2) _CPS:_https://certs.godaddy.com/repository/ (2)Signature (256_octets) (2) 59:0b 92:86:11:a7:24:7b:ed:5b:31:cf:1d:1f (2) 6c:70:c5:b8:6e:be:4e:bb:f6:be:97:50:e1:30:7f:ba (2) 28:5c:62:94:c2:e3:7e:33:f7:fb:42:76:85:db:95:1c (2) 8c:22:58:75 88:65:67:39:0a:16:09:c5:a0:38 (2) 97:a4:c5:23:93:3f:b4:18:a6:01:06:44:91:e3:a7:69 (2) 27:b4:5a:25:7f:3a:b7:32:cd:dd:84:ff:2a:38:29:33 (2) a4:dd: 67:b2:85:fe:a1:88:20:1c:50:89:c8:dc:2a:f6 (2) 42:03:37:4c:e6:88:df:d5:af:24:f2:b1:c3:df:cc:b5 (2) ec:e0:99:5e:b7:49:54:20:3c:94:18:0c:c7:1c:52:18 (2) 49:a4:6d:e1:b3:58:0b:c9:d8:ec:d9:ae:1c:32:8e:28 (2) 70:0d:e2:fe:a6:17:9e:84:0f:bd:57:70:b3:5a:e9:1f (2) a0:86:53:bb:ef:7c:ff:69:0b:e0:48:c3:b7:93:0b:c8 (2) 54:c4:ac:5d:14:67:37:6c:ca:a5:2f:31:08:37:aa (2) 6e:6f:8c:bc:9b:e2:57:5d:24:81:af:97:97:9c:84:ad (2) 6c:ac:37:4c:66:f3:61:91:11:20:e4:be:30:9f:7a:a4 (2) 29:09:b0:e1:34:5f:64:77:18:40:51:df:8c:30:a6:af (3)CERTIFICATE_3 _ (3)Version 3_(0x2) (3)Serial_Number 0_(0x0) (3)Signature_Algorithm sha1WithRSAEncryption (3)ISSUER_NAME _ countryName US _organizationName "The_Go_Daddy_Group,_Inc." _organizationalUnitName Go_Daddy_Class_2_Certification_Authority (3)SUBJECT_NAME _ countryName US _organizationName "The_Go_Daddy_Group,_Inc." _organizationalUni Go_Daddy_Class_2_Certification_Authority (3)Valid_From Jun_29_17:06:20_2004_GMT (3)Valid_Till Jun_29_17:06:20_2034_GMT (3)Public_Key_Algorith rsaEncryption (3)RSA_Public_Key (2048_bit) (3) _RSA_Public-Key:_(2048_bit) (3) _Modulus: (3) _00:de:9d:d7:ea:57:18:49:a1:5b:eb:d7:5f:48:86: (3) _ea:be:dd:ff:e4:ef:67:1c:f4:65:68:b3:57:71:a0: (3) _5e:77:bb:ed:9b:49:e9:70:80:3d:56:18:63:08:6f: (3) _da:f2:cc:d0:3f:7f:02:54:22:54:10:d8:b2:81:d4: (3) _c0: 4b:7f:c7:77:c3:3e:78:ab:1a:03:b5:20: (3) _6b:2f:6a:2b:b1:c5:88:7e:c4:bb:1e:b0:c1:d8:45: (3) _27:6f:aa:37:58:f7:87:26:d7:d8:2d:f6:a9:17:b7: (3) _1f: 72:36:4e:a6:17:3f:65:98:92:db:2a:6e:5d:a2: (3) _fe:88:e0:0b:de:7f:e5:8d:15:e1:eb:cb:3a:d5:e2: (3) _12:a2:13:2d:d8:8e:af:5f:12:3d:a0:08:05:08:b6: (3) _5c:a5:65:38:04:45:99:1e:a3:60:60:74:c5:41:a5: (3) _72:62:1b:62:c5:1f:6f:5f:1a:42:be:02:51:65:a8: (3) _ae:23:18:6a:fc:78:03:a9:4d:7f:80:c3:fa:ab:5a: (3) _fc:a1:40:a4:ca:19:16:fe:b2:c8:ef:5e:73:0d:ee: (3) _77:bd:9a:f6:79:98:bc:b1:07:67:a2:15:0d:dd:a0: (3) _58:c6:44:7b:0a:3e:62:28:5f:ba:41:07:53:58:cf: (3) _1 38:74:c5:f8:ff:b5:69:90:8f:84:74:ea:97: (3) _1b:af (3) _Exponent:_3_(0x3) (3)X509v3_EXTENSIONS _ (3)X509v3_Subject_Key_Identifier _D2:C4:B0:D2:91: 11:71:B3:61:CB:3D:A1:FE:DD:A8:6A:D4:E3 (3)X509v3_Authority_Key_Identifier _keyid:D2:C4:B0:D2:91:D4:4C:11:71:B3:61:CB:3D:A1:FE:DD:A8:6A:D4:E3 _DirName:/C=US/O=The_Go_Daddy_Group,_Inc./OU=Go_Daddy_Class_2_Certification_Authority (3) _serial:00 (3)X509v3_Basic_Constraints _CA:TRUE (3)Signature (256_octets) (3) 32:4b:f3:b2:ca:3e:91:fc:12:c6:a1:07:8c:8e:77:a0 (3) 33:06:14:5c:90:1e:18:f7:08:a6:3d:0a:19:f9:87:80 (3) 11:6e:69:e4:96:17:30: 34:91:63:72:38:ee:cc:1c (3) 01:a3:1d:94:28:a4:31:f6:7a:c4:54:d7:f6:e5:31:58 (3) 03:a2:cc:ce:62:db:94:45:73:b5:bf:45:c9:24:b5:d5 (3) 82:02:ad: 23:79:69:8d:b8:b6:4d:ce:cf:4c:ca:33:23 (3) e8:1c:88:aa:9d:8b:41:6e:16:c9:20:e5:89:9e:cd:3b (3) da:70:f7:7e:99:26:20:14:54:25:ab:6e:73:85:e6:9b (3) 21:9d: 82:0e:a8:f8:c2:0c:fa:10:1e:6c:96:ef (3) 87:0d:c4:0f:61:8b:ad:ee:83:2b:95:f8:8e:92:84:72 (3) 39:eb:20:ea:83:ed:83:cd:97:6e:08:bc:eb:4e:26:b6 (3) 73:2b:e4:d3:f6:4c:fe:26:71:e2:61:11:74:4a:ff:57 (3) 1a:87:0f:75:48:2e:cf:51:69:17:a0:02:12:61:95:d5 (3) d1:40:b2:10:4c:ee:c4:ac:10:43:a6:a5:9e:0a:d5:95 (3) 0d:cf:88:82:c5:32:0c:e4:2b:9f:45:e6:0d:9f (3) 28:9c:b1:b9:2a:5a:57:ad:37:0f:af:1d:7f:db:bd:9f

Info List

Info #1

Certificate Fingerprint:C3846BF24B9E93CA64274C0EC67C1ECC5E024FFCACD2D74019350E81FE546AE4

150009 Links Crawled (1)

WAS Scan Report

150009 Links Crawled

Finding #	**16653939**(375112111)	**Severity**	Information Gathered - Level 1
Unique #	**ece1c454-d967-43c2-a686-aa94b982fd03**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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): 152.00
Number of links: 5
(This number excludes form requests, ajax links (included in QID 150148) and links re-requested during authentication.)

https://one.victorylive.com/
https://one.victorylive.com/.
https://one.victorylive.com/favicon.ico
http://one.victorylive.com/
http://one.victorylive.com/favicon.ico

150010 External Links Discovered (1)

WAS Scan Report

150010 External Links Discovered

Finding #	**16653937**(375112109)	**Severity**	Information Gathered - Level 1
Unique #	**0eb3dddf-3971-4dd7-94d8-314f30a96aba**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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: 12

https://login.victorylive.com/VL-logo-login.png

https://login.victorylive.com/account/login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3DOIDC-ServicesMembersSite%26redirect_uri%3Dhttps%253A%252F%252Fone.victorylive.com%252Fsignin-oidc%26response_mode%3Dform_post%26response_type%3Did_token%26scope%3Dopenid%2520profile%26state%3DOpenIdConnect.AuthenticationProperties%253DsUcCRw-oI0N7_vwhl2idMah6Dw7TSDTb3vlLCS78LRTxU5hZXQmr4olM4rmO3VPCz50CVS1YUv9KEWJs9ulqNUTv2NGQliSNWnjQEumxfiksXZtpOgzMc7e-mB6pPCAxQ_JwP2WfX32f2n-yYy1nz6EaBukg1GsZuiv_Km564Jom5ikDQXoPApAuOrwqPkd1GZbikyAGEGULz0u5wiQ3f_qgq3w%26nonce%3D638914735862475549.ZmYzZGY3ZWItZmI1MS00Yzg5LWIzNTktMTZhNGQ4MGE5MmIwOWJmMWY1OWMtNWMzMS00YmU3LWFiZmUtNTU3NjNjZjdhNWVj%26x-client-SKU%3DID_NET461%26x-client-ver%3D5.3.0.0

https://login.victorylive.com/connect/authorize?client_id=OIDC-ServicesMembersSite&redirect_uri=https%3A%2F%2Fone.victorylive.com%2Fsignin-oidc&response_mode=form_post&response_type=id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3D-VAoUVofqxBAUdCotvEPE9tiDVM-l6X5IXdT9HFnnt8eExbWRcQ1Q5XRlil8K2LOgYFJfjSUnqk9xZB0TSxGc0SzW_7AegXwrZ9euVngztcdEWPHRV_M1OhXlpYrCy-x_6oZM84EV_pB_5BXWboqlJ2P5Z3p6jIFEoOsiMq6LU7402gDz4vrNEPfeNWWW8DFy4quX4GUyzt56EwLahJ9GMYsgkI&nonce=638914736051477120.MGIzMWZmZGMtZjc2Yy00ZTk3LWFmclient-SKU=ID_NET461&x-client-ver=5.3.0.0

https://login.victorylive.com/connect/authorize?client_id=OIDC-ServicesMembersSite&redirect_uri=https%3A%2F%2Fone.victorylive.com%2Fsignin-oidc&response_mode=form_post&response_type=id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3DsUcCRw-oI0N7_vwhl2idMah6Dw7TSDTb3vlLCS78LRTxU5hZXQmr4olM4rmO3VPCz50CVS1YUv9KEWJs9ulqNUTv2NGQliSNWnjQEumxfiksXZtpOgzMc7e-mB6pPCAxQ_JwP2WfX32f2n-yYy1nz6EaBukg1GsZuiv_Km564Jom5ikDQXoPApAuOrwqPkd1GZbikyAGEGULz0u5wiQ3f_qgq3w&nonce=638914735862475549.ZmYzZGY3ZWItZmI1MS00Yzg5LWIzNTktMTZhNGQ4MGE5Iclient-SKU=ID_NET461&x-client-ver=5.3.0.0

https://login.victorylive.com/css/site.css

https://login.victorylive.com/favicon.ico

https://login.victorylive.com/img/social/facebook_icon.png

https://login.victorylive.com/img/social/instagram_icon.png

https://login.victorylive.com/img/social/linkedin_icon.png

https://login.victorylive.com/img/social/twitter_icon.png

https://login.victorylive.com/lib/bootstrap/css/bootstrap.css

https://login.victorylive.com/lib/font-awesome-4.7.0/css/font-awesome.min.css

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

WAS Scan Report

150020 Links Rejected By Crawl Scope or Exclusion List

Finding #	**16653927**(375112099)	**Severity**	Information Gathered - Level 1
Unique #	**5bf49fcc-8c5f-4ddb-8896-4e4b7ca41c87**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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://login.victorylive.com/VL-logo-login.png
https://login.victorylive.com/account/login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3DOIDC-ServicesMembersSite%26redirect_uri%3Dhttps%253A%252F%252Fone.victorylive.com%252Fsignin-oidc%26response_mode%3Dform_post%26response_type%3Did_token%26scope%3Dopenid%2520profile%26state%3DOpenIdConnect.AuthenticationProperties%253DsUcCRw-oI0N7_vwhl2idMah6Dw7TSDTb3vlLCS78LRTxU5hZXQmr4olM4rmO3VPCz50CVS1YUv9KEWJs9ulqNUTv2NGQliSNWnjQEumxfiksXZtpOgzMc7e-mB6pPCAxQ_JwP2WfX32f2n-yYy1nz6EaBukg1GsZuiv_Km564Jom5ikDQXoPApAuOrwqPkd1GZbikyAGEGULz0u5wiQ3f_qgq3w%26nonce%3D638914735862475549.ZmYzZGY3ZWItZmI1MS00Yzg5LWIzNTktMTZhNGQ4MGE5MmIwOWJmMWY1OWMtNWMzMS00YmU3LWFiZmUtNTU3NjNjZjdhNWVj%26x-client-SKU%3DID_NET461%26x-client-ver%3D5.3.0.0
https://login.victorylive.com/connect/authorize?client_id=OIDC-ServicesMembersSite&redirect_uri=https%3A%2F%2Fone.victorylive.com%2Fsignin-oidc&response_mode=form_post&response_type=id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3D-VAoUVofqxBAUdCotvEPE9tiDVM-l6X5IXdT9HFnnt8eExbWRcQ1Q5XRlil8K2LOgYFJfjSUnqk9xZB0TSxGc0SzW_7AegXwrZ9euVngztcdEWPHRV_M1OhXlpYrCy-x_6oZM84EV_pB_5BXWboqlJ2P5Z3p6jIFEoOsiMq6LU7402gDz4vrNEPfeNWWW8DFy4quX4GUyzt56EwLahJ9GMYsgkI&nonce=638914736051477120.MGIzMWZmZGMtZjc2Yy00ZTk3LWFmclient-SKU=ID_NET461&x-client-ver=5.3.0.0
https://login.victorylive.com/connect/authorize?client_id=OIDC-ServicesMembersSite&redirect_uri=https%3A%2F%2Fone.victorylive.com%2Fsignin-oidc&response_mode=form_post&response_type=id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3DsUcCRw-oI0N7_vwhl2idMah6Dw7TSDTb3vlLCS78LRTxU5hZXQmr4olM4rmO3VPCz50CVS1YUv9KEWJs9ulqNUTv2NGQliSNWnjQEumxfiksXZtpOgzMc7e-mB6pPCAxQ_JwP2WfX32f2n-yYy1nz6EaBukg1GsZuiv_Km564Jom5ikDQXoPApAuOrwqPkd1GZbikyAGEGULz0u5wiQ3f_qgq3w&nonce=638914735862475549.ZmYzZGY3ZWItZmI1MS00Yzg5LWIzNTktMTZhNGQ4MGE5lclient-SKU=ID_NET461&x-client-ver=5.3.0.0
https://login.victorylive.com/css/site.css
https://login.victorylive.com/favicon.ico
https://login.victorylive.com/img/social/facebook_icon.png
https://login.victorylive.com/img/social/instagram_icon.png
https://login.victorylive.com/img/social/linkedin_icon.png
https://login.victorylive.com/img/social/twitter_icon.png

IP based excluded links:
Links rejected during the test phase not reported due to volume of links.

WAS Scan Report

150021 Scan Diagnostics (1)

WAS Scan Report

150021 Scan Diagnostics

Finding #	**16653928**(375112100)	**Severity**	Information Gathered - Level 1
Unique #	**4248dd27-fe59-4fef-9159-231e842076ae**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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 http://one.victorylive.com/ fetched. Status code:307, Content-Type:text/html, load time:1 milliseconds.
Batch #0 VirtualHostDiscovery: estimated time < 10 minutes (70 tests, 0 inputs)
VirtualHostDiscovery: 70 vulnsigs tests, completed 70 requests, 4 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 59 requests, 3 seconds. Completed 59 requests of 59 estimated requests (100%). All tests completed.
Batch #0 ApiSec spec files detection: estimated time < 1 minute (1 tests, 1 inputs)
ApiSec spec files detection: 1 vulnsigs tests, completed 0 requests, 16 seconds. No tests to execute.
Collected 7 links overall in 0 hours 2 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 2) + files:(0 x 2) + directories:(9 x 3) + paths:(0 x 5) = total (27)
Batch #0 WS Directory Path manipulation: estimated time < 1 minute (9 tests, 5 inputs)
WS Directory Path manipulation: 9 vulnsigs tests, completed 18 requests, 0 seconds. Completed 18 requests of 27 estimated requests (66.6667%). All tests completed.
Batch #0 WS enumeration: estimated time < 1 minute (11 tests, 5 inputs)
WS enumeration: 11 vulnsigs tests, completed 25 requests, 1 seconds. Completed 25 requests of 55 estimated requests (45.4545%). All tests completed.
Batch #4 WebCgiOob: estimated time < 1 minute (167 tests, 1 inputs)
Batch #4 WebCgiOob: 167 vulnsigs tests, completed 500 requests, 12 seconds. Completed 500 requests of 740 estimated requests (67.5676%). 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, 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, 5 inputs)
Batch #4 File Inclusion analysis: 1 vulnsigs tests, completed 0 requests, 0 seconds. Completed 0 requests of 5 estimated requests (0%). All tests completed.
Batch #4 Cookie manipulation: estimated time < 1 minute (47 tests, 3 inputs)
Batch #4 Cookie manipulation: 47 vulnsigs tests, completed 108 requests, 2 seconds. Completed 108 requests of 108 estimated requests (100%). XSS optimization removed 116 links. All tests completed.
Batch #4 Header manipulation: estimated time < 1 minute (47 tests, 4 inputs)
Batch #4 Header manipulation: 47 vulnsigs tests, completed 726 requests, 15 seconds. Completed 726 requests of 520 estimated requests (139.615%). XSS optimization removed 232 links. All tests completed.
Batch #4 shell shock detector: estimated time < 1 minute (1 tests, 4 inputs)
Batch #4 shell shock detector: 1 vulnsigs tests, completed 6 requests, 0 seconds. Completed 6 requests of 4 estimated requests (150%). 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.
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 2) + files:(0 x 2) + directories:(4 x 3) + paths:(11 x 5) = total (67)
Batch #5 Path XSS manipulation: estimated time < 1 minute (15 tests, 5 inputs)
Batch #5 Path XSS manipulation: 15 vulnsigs tests, completed 61 requests, 1 seconds. Completed 61 requests of 67 estimated requests (91.0448%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(1 x 3) + paths:(0 x 5) = total (3)

Batch #5 Tomcat Vuln manipulation: estimated time < 1 minute (1 tests, 5 inputs)
Batch #5 Tomcat Vuln manipulation: 1 vulnsigs tests, completed 2 requests, 1 seconds. Completed 2 requests of 3 estimated requests (66.6667%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(0 x 2) + files:(0 x 2) + directories:(16 x 3) + paths:(0 x 5) = total (48)
Batch #5 Time based path manipulation: estimated time < 1 minute (16 tests, 5 inputs)
Batch #5 Time based path manipulation: 16 vulnsigs tests, completed 64 requests, 660 seconds. Completed 64 requests of 48 estimated requests (133.333%). All tests completed.
Path manipulation: Estimated requests (payloads x links): files with extension:(1 x 2) + files:(12 x 2) + directories:(145 x 3) + paths:(14 x 5) = total (531)
Batch #5 Path manipulation: estimated time < 1 minute (172 tests, 5 inputs)
Batch #5 Path manipulation: 172 vulnsigs tests, completed 354 requests, 8 seconds. Completed 354 requests of 531 estimated requests (66.6667%). All tests completed.
WebCgiHrsTests: no test enabled
Batch #5 WebCgiGeneric: estimated time < 10 minutes (1547 tests, 1 inputs)
Batch #5 WebCgiGeneric: 1547 vulnsigs tests, completed 1764 requests, 47 seconds. Completed 1764 requests of 4000 estimated requests (44.1%). All tests completed.
WebCgiTimebasedTests: no test enabled
Batch #5 Open Redirect analysis: estimated time < 1 minute (2 tests, 0 inputs)
Batch #5 Open Redirect analysis: 2 vulnsigs tests, completed 0 requests, 4 seconds. No tests to execute.
Duration of Crawl Time: 152.00 (seconds)
Duration of Test Phase: 896.00 (seconds)
Total Scan Time: 1048.00 (seconds)

Total requests made: 4572
Average server response time: 0.07 seconds

Average browser load time: 0.07 seconds

150028 Cookies Collected (1)

WAS Scan Report

150028 Cookies Collected

Finding #	**16653931**(375112103)	**Severity**	Information Gathered - Level 1
Unique #	**e4f934d0-96f3-424d-b7e5-1747dd05f46c**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	-		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were set by the web application during the crawl phase.

Impact

Cookies may potentially contain sensitive information about the user.

Note: Long scan duration can occur if a web application sets a large number of cookies (e.g., 25 cookies or more) and QIDs 150002, 150046, 150047, and 150048 are enabled.

Solution

Review cookie values to ensure they do not include sensitive information. If scan duration is excessive due to a large number of cookies, consider excluding QIDs 150002, 150046, 150047, and 150048.

Results

Total cookies: 4
.AspNetCore.Antiforgery.yomrRab43ow=CfDJ8KUL8yHJ9f5CkxfIXFzjoi4q0jQjsFrIJVBTrleYW8rGjTaLjNNthvXq3IogZ3_lNlE-0XcGxoQfmPKrAy5iHVSDhv4uuCbh6MF8-NuB5vL-jMXtP4uxu1YJWiXzR0hp4vJmcf8LL_0ngaPys76u8tc; HttpOnly; SameSite=Strict; domain=login.victorylive.com; path=/ First set at URL: https://login.victorylive.com/account/login?ReturnUrl=%2Fconnect%2Fauthorize%2Fcallback%3Fclient_id%3DOIDC-ServicesMembersSite%26redirect_uri%3Dhttps%253A%252F%252Fone.victorylive.com%252Fsignin-oidc%26response_mode%3Dform_post%26response_type%3Did_token%26scope%3Dopenid%2520profile%26state%3DOpenIdConnect.AuthenticationProperties%253DsUcCRw-oI0N7_vwhl2idMah6Dw7TSDTb3vlLCS78LRTxU5hZXQmr4olM4rmO3VPCz50CVS1YUv9KEWJs9ulqNUTv2NGQliSNWnjQEumxfiksXZtpOgzMc7e-mB6pPCAxQ_JwP2WfX32f2n-yYy1nz6EaBukg1GsZuiv_Km564Jom5ikDQXoPApAuOrwqPkd1GZbikyAGEGULz0u5wiQ3f_qgq3w%26nonce%3D6389147358624755 49.ZmYzZGY3ZWItZmI1MS00Yzg5LWIzNTktMTZhNGQ4MGE5MmIwOWJmMWY1OWMtNWMzMS00YmU3LWFiZmUtNTU3NjNjZjdhNWVj%26x-client-SKU%3DID_NET461%26x-client-ver%3D5.3.0.0

OpenIdConnect.nonce.ffO0cjs5O91k5F8SMSKrWYS49nONEzHKnzXoPqHVbX4%3D=cEZUYi1nd1RrQThSSE1QMU5TcjhIQmV0NXhTYW82REE0MFp3TE5KREFwb3FhZmlqTy1zdGtYYW9wb3
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:06 GMT; domain=one.victorylive.com; path=/ First set at URL: https://one.victorylive.com/
OpenIdConnect.nonce.iK5BccTj6Y0bns%2BrWkrTbBAjOkyt6E4e9RYDf%2BJRnp4%3D=NW1sdldHb0hJbVRlaGRkcUpJQnR5OEtiSjNOZ2JBNnVMRWNXc3RsaFlQdGxHNVZGVWcwdDhvWUltV214cG5jVkI2TXA5bnotaXVjT0d6alp2OGp4YXN3aXJlcGlPSDdSV3NK
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:18 GMT; domain=one.victorylive.com; path=/ First set at URL: https://one.victorylive.com/
OpenIdConnect.nonce.f2Kar%2Fo8YIjRJpn%2F7%2F7%2BshZ%2B0kadX%2B90zlc5DVs6m%2F4%3D=ODR0cHVFRDFtNHp1QzFQNlhfUGhaemMxajNPUktkaVctdkVvdU9mWjhmZVpfNXhER2dEVS1pYzIwdXlzWjR1ZVU4YlJVRGhBdTM3eEdrcnJraWxueTFDNnk2ZUkzMzVHV0JJWI
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:26 GMT; domain=one.victorylive.com; path=/ First set at URL: https://one.victorylive.com/

150516 Web Application External URL Redirection (1)

WAS Scan Report

150516 Web Application External URL Redirection

Finding #	**16653935**(375112107)	**Severity**	Information Gathered - Level 1
Unique #	**62a1d440-e834-4cb0-998a-a0c59853e450**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	CWE-601		
OWASP	-		
WASC	-		

Details

Threat

External redirected links were discovered during the scan and are listed in the Results section.

Impact

Attackers can use external redirects without validation to redirect a user to a malicious URL. For example, if the trusted application is https://X.X.X.TrustQualys/test?url=qualys.com, the user is navigating to https://X.X.X.TrustQualys, and it is a trusted domain. However, there is an invalidated redirect, and the attacker can manipulate the redirection. The attacker can use this link https://X.X.X.TrustQualys/test?url=X.X.XReallyBadApp.com (for this example, ReallyBadApp is used, savvy malicious attackers will use more legitimate looking values) where the customer may be redirected to an external entity X.X.XReallyBadApp.com. This unintended redirect may lead to fishing or malware. Since the user was redirected from a trusted application, the user may be more willing to provide information.

Solution

As a standard avoid using external redirects and forwards in the application when possible. As a standard, avoid external redirects and forwards in the application when possible. Applications often are designed to redirect the user within the application and trusted external URLs. If a redirect parameter is used, ensure that the supplied value is valid and filtered based on trusted URLs. Setting up a whitelist would be most applicable to this technique. Reference: Unvalidated_Redirects_and_Forwards_Cheat_Sheet

Results

External Redirect URLs:
https://one.victorylive.com/ Redirects to
https://login.victorylive.com/connect/authorize?client_id=OIDC-ServicesMembersSite&redirect_uri=https%3A%2F%2Fone.victorylive.com%2Fsignin-oidc&response_mode=form_post&response_type=id_token&scope=openid%20profile&state=OpenIdConnect.AuthenticationProperties%3D-VAoUVofqxBAUdCotvEPE9tiDVM-l6X5IXdT9HFnnt8eExbWRcQ1Q5XRlil8K2LOgYFJfjSUnqk9xZB0TSxGc0SzW_7AegXwrZ9euVngztcdEWPHRV_M1OhXlpYrCy-x_6oZM84EV_pB_5BXWboqlJ2P5Z3p6jIFEoOsiMq6LU7402gDz4vrNEPfeNWWW8DFy4quX4GUyzt56EwLahJ9GMYsgkI&nonce=638914736051477120.MGIzMWZmZGMtZjc2Yy00ZTk3LWFm client-SKU=ID_NET461&x-client-ver=5.3.0.0

150546 First Link Crawled Response Code Information (1)

WAS Scan Report

150546 First Link Crawled Response Code Information

Finding #	**16653932**(375112104)	**Severity**	Information Gathered - Level 1
Unique #	**08090a21-1ec3-4b1d-abf5-28498e60a5fe**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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: http://one.victorylive.com/
Response Code: 307
Response Header:
Cross-Origin-Resource-Policy: Cross-Origin
Location: https://one.victorylive.com/
Non-Authoritative-Reason: HSTS

Response Body:
<html><head></head><body></body></html>

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

WAS Scan Report

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

Finding #	**16653942**(375112114)	**Severity**	Information Gathered - Level 1
Unique #	**714d5a2c-7231-495f-969f-cbec22203cb2**		
Group	Scan Diagnostics	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	-		
OWASP	A4 Insecure Design		
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.
login.victorylive.com

Security Weaknesses (8)

150210 Information Disclosure via Response Header (1)

WAS Scan Report

150210 Information Disclosure via Response Header

Finding #	**16653925**(375112097)	**Severity**	Information Gathered - Level 3
Unique #	**25dd2aee-17a3-4631-8e39-f294cfae2112**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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://one.victorylive.com/ response code: 302
server: AutoProcessor/1.0

GET https://one.victorylive.com/favicon.ico response code: 200
server: AutoProcessor/1.0

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

WAS Scan Report

150202 Missing header: X-Content-Type-Options

Finding #	**16653938**(375112110)	**Severity**	Information Gathered - Level 2
Unique #	**84f91d0a-a447-4e18-a608-e798a236b79c**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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://one.victorylive.com/favicon.ico response code: 200
accept-ranges: bytes
content-length: 1150
content-type: image/x-icon
date: Fri, 22 Aug 2025 15:33:38 GMT
etag: "0a9f395ec11dc1:0"
last-modified: Wed, 20 Aug 2025 16:07:54 GMT
server: AutoProcessor/1.0
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: DENY
x-servedby: ui02
Set-Cookie:
OpenIdConnect.nonce.ffO0cjs5O91k5F8SMSKrWYS49nONEzHKnzXoPqHVbX4%3D=cEZUYi1nd1RrQThSSE1QMU5TcjhIQmV0NXhTYW82REE0MFp3TE5KREFwb3FhZmlqTy1zdGtYYW9wb
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:07 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.iK5BccTj6Y0bns%2BrWkrTbBAjOkyt6E4e9RYDf
%2BJRnp4%3D=NW1sdldHb0hJbVRlaGRkcUpJQnR5OEtiSjNOZ2JBNnVMRWNXc3RsaFlQdGxHNVZGVWcwdDhvWUltV214cG5jVkI2TXA5bnotaXVjT0d6alp2OGp4YXN3aXJlcGlPSDdSV3NK
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:18 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.f2Kar%2Fo8YIjRJpn%2F7%2F7%2BshZ%2B0kadX%2B90zlc5DVs6m
%2F4%3D=ODR0cHVFRDFtNHp1QzFQNlhfUGhaemMxajNPUktkaVctdkVvdU9mWjhmZVpfNXhER2dEVS1pYzIwdXlzWjR1ZVU4YlJVRGhBdTM3eEdrcnJraWxueTFDNnk2ZUkzMzVHV0JJWI
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:26 GMT; domain=one.victorylive.com; path=/

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

GET https://one.victorylive.com/favicon.ico response code: 200

150206 Content-Security-Policy Not Implemented (1)

WAS Scan Report

150206 Content-Security-Policy Not Implemented

Finding #	**16653941**(375112113)	**Severity**	Information Gathered - Level 2
Unique #	**4b9d4ec0-31b9-4ecd-aae6-83d43bff5c25**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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://one.victorylive.com/favicon.ico response code: 200
accept-ranges: bytes
content-length: 1150
content-type: image/x-icon
date: Fri, 22 Aug 2025 15:33:38 GMT
etag: "0a9f395ec11dc1:0"
last-modified: Wed, 20 Aug 2025 16:07:54 GMT
server: AutoProcessor/1.0
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: DENY
x-servedby: ui02
Set-Cookie:
OpenIdConnect.nonce.ffO0cjs5O91k5F8SMSKrWYS49nONEzHKnzXoPqHVbX4%3D=cEZUYi1nd1RrQThSSE1QMU5TcjhIQmV0NXhTYW82REE0MFp3TE5KREFwb3FhZmlqTy1zdGtYYW9wb
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:07 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.iK5BccTj6Y0bns%2BrWkrTbBAjOkyt6E4e9RYDf
%2BJRnp4%3D=NW1sdldHb0hJbVRlaGRkcUpJQnR5OEtiSjNOZ2JBNnVMRWNXc3RsaFlQdGxHNVZGVWcwdDhvWUltV214cG5jVkI2TXA5bnotaXVjT0d6alp2OGp4YXN3aXJlcGlPSDdSV3NK
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:18 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.f2Kar%2Fo8YIjRJpn%2F7%2F7%2BshZ%2B0kadX%2B90zlc5DVs6m
%2F4%3D=ODR0cHVFRDFtNHp1QzFQNlhfUGhaemMxajNPUktkaVctdkVvdU9mWjhmZVpfNXhER2dEVS1pYzIwdXlzWjR1ZVU4YlJVRGhBdTM3eEdrcnJraWxueTFDNnk2ZUkzMzVHV0JJWI
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:26 GMT; domain=one.victorylive.com; path=/

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

WAS Scan Report

GET https://one.victorylive.com/favicon.ico response code: 200

150208 Missing header: Referrer-Policy (1)

WAS Scan Report

150208 Missing header: Referrer-Policy

Finding #	**16653926**(375112098)	**Severity**	Information Gathered - Level 2
Unique #	**af83c254-6018-4a1b-a43e-3182b7b55fb6**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	WASC-15 APPLICATION MISCONFIGURATION		

Details

Threat

The Referrer Policy header is used to control the flow of information from the source to the destination when a link is clicked. During the scan checks are done for the presence of the Referrer Policy on all static and dynamic pages. One of the following values for Referrer Policy in the response headers was found to be missing:

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, the response body is checked for a meta tag containing the tag name as "referrer" and one of the above Referrer Policy. Missing referrer header is reported for links with the following response codes - 2XX, 4xx, and 5xx. Links that report a response code of 3xx will not be tested for presence of this header.

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://one.victorylive.com/favicon.ico response code: 200
accept-ranges: bytes
content-length: 1150
content-type: image/x-icon
date: Fri, 22 Aug 2025 15:33:38 GMT
etag: "0a9f395ec11dc1:0"
last-modified: Wed, 20 Aug 2025 16:07:54 GMT
server: AutoProcessor/1.0
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: DENY
x-servedby: ui02
Set-Cookie:
OpenIdConnect.nonce.ffO0cjs5O91k5F8SMSKrWYS49nONEzHKnzXoPqHVbX4%3D=cEZUYi1nd1RrQThSSE1QMU5TcjhIQmV0NXhTYW82REE0MFp3TE5KREFwb3FhZmlqTy1zdGtYYW9wb
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:07 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.iK5BccTj6Y0bns%2BrWkrTbBAjOkyt6E4e9RYDf
%2BJRnp4%3D=NW1sdldHb0hJbVRlaGRkcUpJQnR5OEtiSjNOZ2JBNnVMRWNXc3RsaFlQdGxHNVZGVWcwdDhvWUltV214cG5jVkI2TXA5bnotaXVjT0d6alp2OGp4YXN3aXJlcGlPSDdSV3NK
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:18 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.f2Kar%2Fo8YIjRJpn%2F7%2F7%2BshZ%2B0kadX%2B90zlc5DVs6m
%2F4%3D=ODR0cHVFRDFtNHp1QzFQNlhfUGhaemMxajNPUktkaVctdkVvdU9mWjhmZVpfNXhER2dEVS1pYzIwdXlzWjR1ZVU4YlJVRGhBdTM3eEdrcnJraWxueTFDNnk2ZUkzMzVHV0JJWI
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:26 GMT; domain=one.victorylive.com; path=/

WAS Scan Report

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

GET https://one.victorylive.com/favicon.ico response code: 200

150248 Missing header: Permissions-Policy (1)

WAS Scan Report

150248 Missing header: Permissions-Policy

Finding #	**16653930**(375112102)	**Severity**	Information Gathered - Level 2
Unique #	**c022d99b-34ca-41d9-ad30-748a795ca8c7**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
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://one.victorylive.com/favicon.ico response code: 200
accept-ranges: bytes
content-length: 1150
content-type: image/x-icon
date: Fri, 22 Aug 2025 15:33:38 GMT
etag: "0a9f395ec11dc1:0"
last-modified: Wed, 20 Aug 2025 16:07:54 GMT
server: AutoProcessor/1.0
strict-transport-security: max-age=31536000; includeSubDomains; preload
x-frame-options: DENY
x-servedby: ui02
Set-Cookie:
OpenIdConnect.nonce.ffO0cjs5O91k5F8SMSKrWYS49nONEzHKnzXoPqHVbX4%3D=cEZUYi1nd1RrQThSSE1QMU5TcjhIQmV0NXhTYW82REE0MFp3TE5KREFwb3FhZmlqTy1zdGtYYW9wb
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:07 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.iK5BccTj6Y0bns%2BrWkrTbBAjOkyt6E4e9RYDf
%2BJRnp4%3D=NW1sdldHb0hJbVRlaGRkcUpJQnR5OEtiSjNOZ2JBNnVMRWNXc3RsaFlQdGxHNVZGVWcwdDhvWUltV214cG5jVkI2TXA5bnotaXVjT0d6alp2OGp4YXN3aXJlcGlPSDdSV3NK
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:18 GMT; domain=one.victorylive.com; path=/
Set-Cookie: OpenIdConnect.nonce.f2Kar%2Fo8YIjRJpn%2F7%2F7%2BshZ%2B0kadX%2B90zlc5DVs6m
%2F4%3D=ODR0cHVFRDFtNHp1QzFQNlhfUGhaemMxajNPUktkaVctdkVvdU9mWjhmZVpfNXhER2dEVS1pYzIwdXlzWjR1ZVU4YlJVRGhBdTM3eEdrcnJraWxueTFDNnk2ZUkzMzVHV0JJWI
secure; HttpOnly; expires=Fri, 22-Aug-2025 15:48:26 GMT; domain=one.victorylive.com; path=/

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

GET https://one.victorylive.com/favicon.ico response code: 200

150101 Third-party Cookies Collected (1)

WAS Scan Report

150101 Third-party Cookies Collected

Finding #	**16653936**(375112108)	**Severity**	Information Gathered - Level 1
Unique #	**596a9b14-7d4a-40fe-bbdc-878ca663a6c7**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	CWE-830		
OWASP	-		
WASC	-		

Details

Threat

The cookies listed in the Results section were received from third-party web application(s) during the crawl phase.

Impact

Cookies may contain sensitive information about the user. Cookies sent via HTTP may be sniffed.

Solution

Review cookie values to ensure that sensitive information such as passwords are not present within them.

Results

Total cookies: 1
.AspNetCore.Antiforgery.yomrRab43ow=CfDJ8KUL8yHJ9f5CkxfIXFzjoi4q0jQjsFrIJVBTrleYW8rGjTaLjNNthvXq3IogZ3_lNlE-0XcGxoQfmPKrAy5iHVSDhv4uuCbh6MF8-NuB5vL-jMXtP4uxu1YJWiXzR0hp4vJmcf8LL_0ngaPys76u8tc; HttpOnly; domain=login.victorylive.com; path=/ First set at URL: http://one.victorylive.com/

150142 Virtual Host Discovered (1)

WAS Scan Report

150142 Virtual Host Discovered

Finding #	**16653940**(375112112)	**Severity**	Information Gathered - Level 1
Unique #	**c9b3866e-b7b9-459f-b32d-33507b34f9df**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	CWE-200		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

Web server is responding differently when the HOST header is manipulated and various common virtual hosts are tested. This could indicate the presence of Virtual Host. Virtual hosting is a method for hosting multiple domain names (with separate handling of each name) on a single server (or pool of servers). This allows one server to share its resources, such as memory and processor cycles, without requiring all services provided to use the same host name. The extra virtual hosts discovered by the Web application scanner during HOST header manipulation are provided in the Results section.

Impact

The Web application should apply consistent security measures. If the Web application fails to apply security controls to other domains hosted on the same server, then it may be exposed to vulnerabilities like cross-site scripting, SQL injection, or authorization-based attacks.

Solution

Consult the virtual host configuration and check if this virtual host should be publicly accessible.

Results

Virtual host discovered:

Detected based on: Unique redirect URI
Virtual Host: www.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://www.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: stage.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://stage.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: m.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://m.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: test.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://test.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: secure.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://secure.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: mail.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://mail.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: demo.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://demo.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: dev.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://dev.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: portal.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://portal.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: webmail.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://webmail.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: staging.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://staging.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: app.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://app.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: shop.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://shop.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: qa.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://qa.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: apps.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://apps.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: admin.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://admin.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: login.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://login.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: online.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://online.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: mobile.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://mobile.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: store.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://store.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: blog.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://blog.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: beta.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://beta.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: api.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://api.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: extranet.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://extranet.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: web.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://web.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: intranet.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://intranet.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: services.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://services.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: support.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://support.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: connect.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://connect.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: email.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://email.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: remote.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://remote.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: images.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://images.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: orders.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://orders.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: merchant.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://merchant.one.victorylive.com/

Detected based on: Unique redirect URI
Virtual Host: retail.one.victorylive.com
URI: http://one.victorylive.com/
Redirect URI(302): https://retail.one.victorylive.com/

150277 Cookie without SameSite attribute (1)

WAS Scan Report

150277 Cookie without SameSite attribute

Finding #	**16653929**(375112101)	**Severity**	Information Gathered - Level 1
Unique #	**ad16f56d-d473-4234-99ae-b01185cc59ff**		
Group	Security Weaknesses	**Detection Date**	22 Aug 2025 21:02 GMT+0630
CWE	CWE-16, CWE-1032		
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat
The cookies listed in the Results section are missing the SameSite attribute.

Impact
The SameSite cookie attribute is an effective countermeasure against cross-site request forgery (CSRF) attacks. Note that a missing SameSite attribute does not mean the web application is automatically vulnerable to CSRF. The scanner will report QID 150071 if a CSRF vulnerability is detected.

Solution
Consider adding the SameSite attribute to the cookie(s) listed.

More information:
DZone article
OWASP CSRF Prevention Cheat Sheet

Results

Total cookies: 3
OpenIdConnect.nonce.f2Kar%2Fo8YIjRJpn%2F7%2F7%2BshZ%2B0kadX%2B90zlc5DVs6m
%2F4%3D=ODR0cHVFRDFtNHp1QzFQNlhfUGhaemMxajNPUktkaVctdkVvdU9mWjhmZVpfNXhER2dEVS1pYzIwdXlzWjR1ZVU4YlJVRGhBdTM3eEdrcnJraWxueTFDNnk2ZUkzMzVHV0JJWI
expires=Fri Aug 22 15:48:26 2025; path=/; domain=one.victorylive.com; max-age=810; secure; httponly | First set at URL: https://one.victorylive.com/

OpenIdConnect.nonce.ffO0cjs5O91k5F8SMSKrWYS49nONEzHKnzXoPqHVbX4%3D=cEZUYi1nd1RrQThSSE1QMU5TcjhIQmV0NXhTYW82REE0MFp3TE5KREFwb3FhZmlqTy1zdGtYYW9wb
expires=Fri Aug 22 15:48:06 2025; path=/; domain=one.victorylive.com; max-age=790; secure; httponly | First set at URL: https://one.victorylive.com/
OpenIdConnect.nonce.iK5BccTj6Y0bns%2BrWkrTbBAjOkyt6E4e9RYDf
%2BJRnp4%3D=NW1sdldHb0hJbVRlaGRkcUpJQnR5OEtiSjNOZ2JBNnVMRWNXc3RsaFlQdGxHNVZGVWcwdDhvWUltV214cG5jVkI2TXA5bnotaXVjT0d6alp2OGp4YXN3aXJlcGlPSDdSV3NK
expires=Fri Aug 22 15:48:18 2025; path=/; domain=one.victorylive.com; max-age=802; secure; httponly | First set at URL: https://one.victorylive.com/

WAS Scan Report

Appendix

Scan Details

VL - Aug 22, 2025

Reference	was/1755876648411.23176460
Date	22 Aug 2025 21:02 GMT+0630
Mode	On-Demand
Progressive Scanning	Enabled
Progression Number	1
Type	Vulnerability
Authentication	None
Scanner Appliance	External (IP: 139.87.104.123, Scanner: 0.6.680b2-1, WAS: 10.10.3-1, Signatures: 2.6.400-3)
Profile	hackthissite.org-test
DNS Override	-
Duration	00:19:24
Status	Finished
Authentication Status	None

Option Profile Details

Form Submission	BOTH
Form Crawl Scope	Include form action URI in uniqueness calculation
Maximum links to test in scope	1000
User Agent	-
Request Parameter Set	Initial Parameters
Document Type	Ignore common binary files
Enhanced Crawling	Disabled
SmartScan	Enabled
SmartScan Depth	5
Timeout Error Threshold	100
Unexpected Error Threshold	300
Performance Settings	Pre-defined
Scan Intensity	Low
Bruteforce Option	Minimal
Detection Scope	Core
Include additional XSS payloads	No
Credit Card Numbers Search	Off
Social Security Numbers (US) Search	Off

Web Application Details: VL

Name	VL
ID	941863138
URL	http://one.victorylive.com
Owner	Sravan Kumar Medishetty (vctry3sm)
Scope	Limit to URL hostname

WAS Scan Report

Tags	-
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.

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.**
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.**
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.**
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.**
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.

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.**
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.**
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.**
Critical	**Presence of this vulnerability might give intruders the ability to gain highly sensitive content or affect other users of the web application.**
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.

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 infomation 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.