



Web Application Report18 Jul 2024

Each targeted web application is listed with the total number of detected vulnerabilities and sensitive content.

Hector DeJesus  
devem3hd

Develom  
  
Portland, Oregon 97239  
United States of America

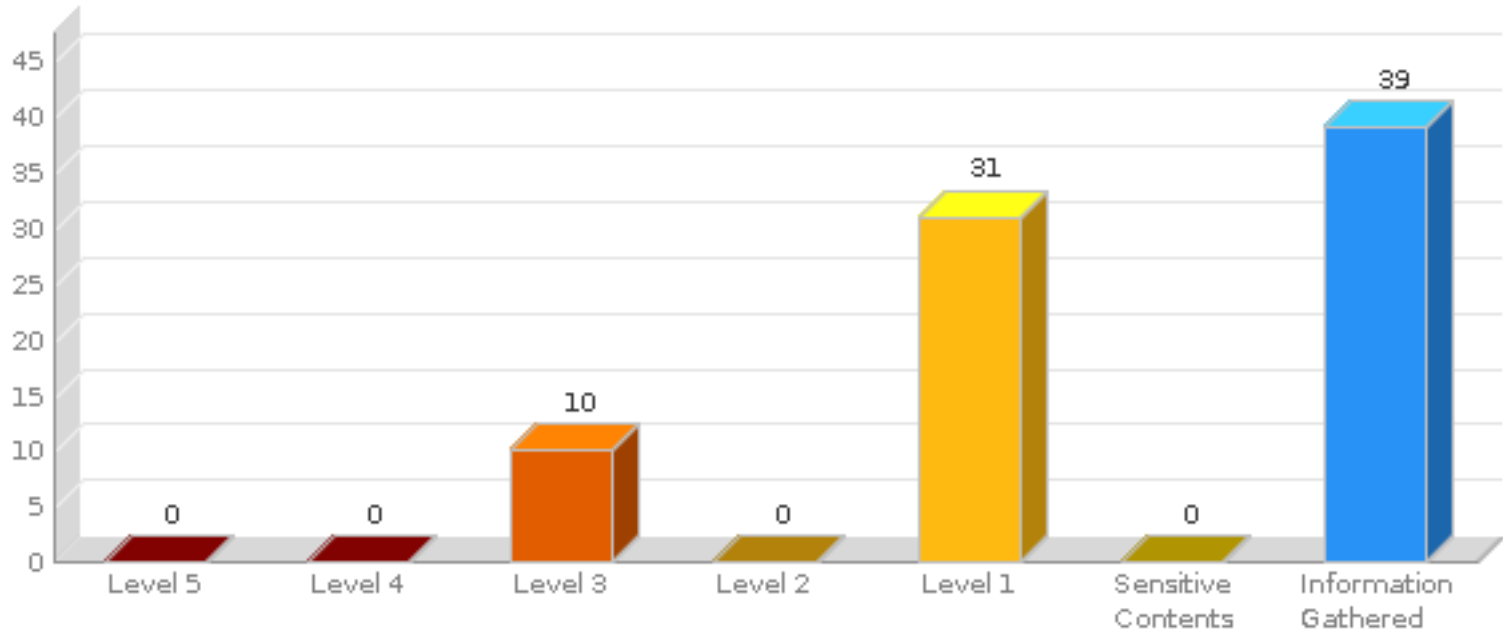
Target and Filters

Web Applications (1)	Develom
Status	New, Active, Re-Opened
Detection Source	Qualys, Burp, Bugcrowd

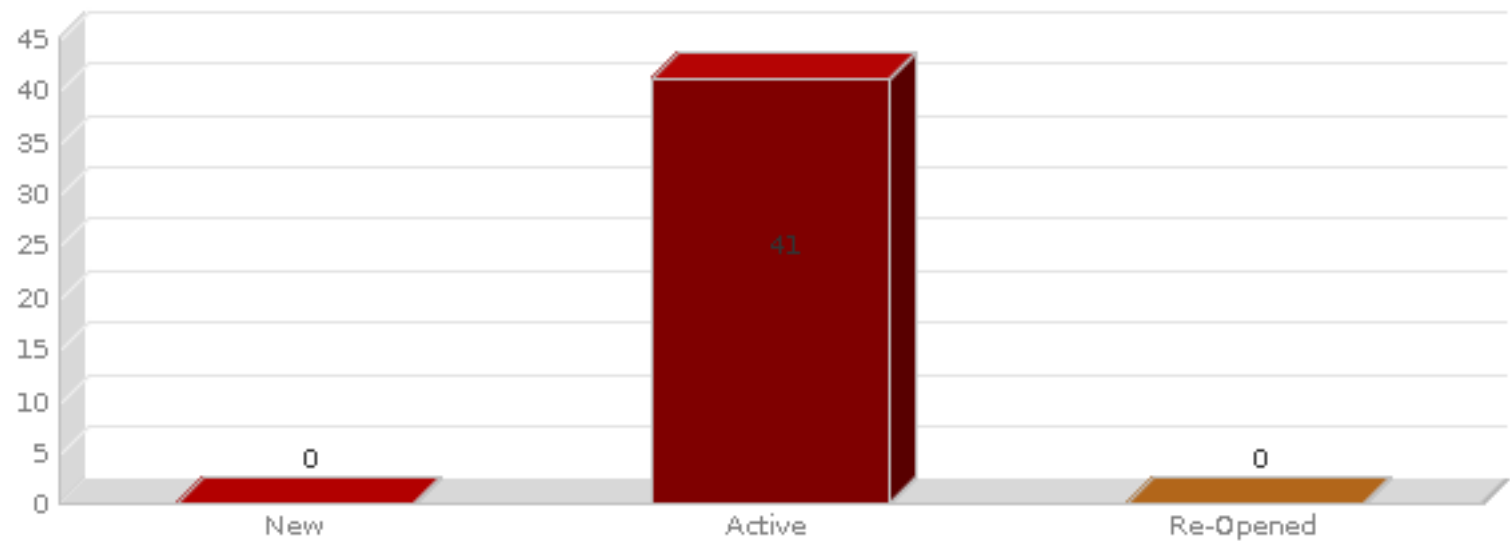
Summary

Security Risk	Web Applications	Vulnerabilities	Sensitive Contents	Information Gathered
MED	1	41	0	39

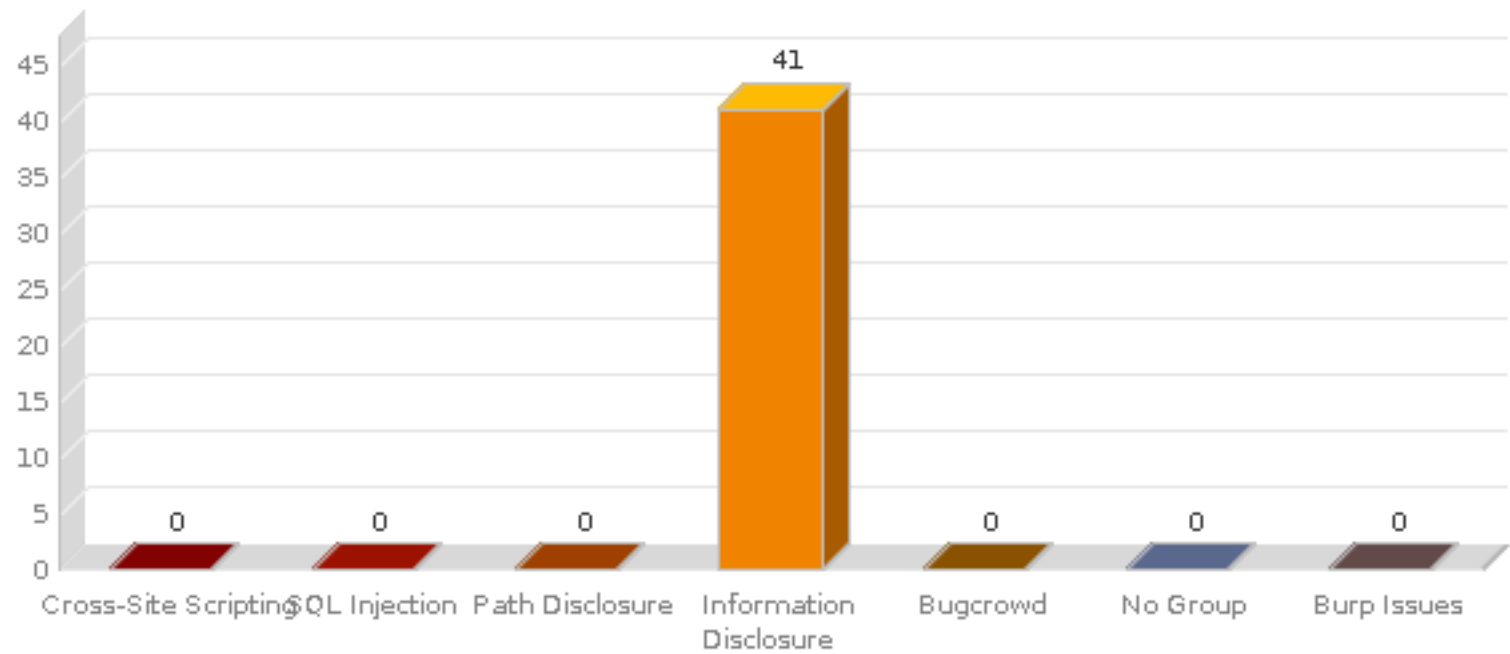
Findings by Severity



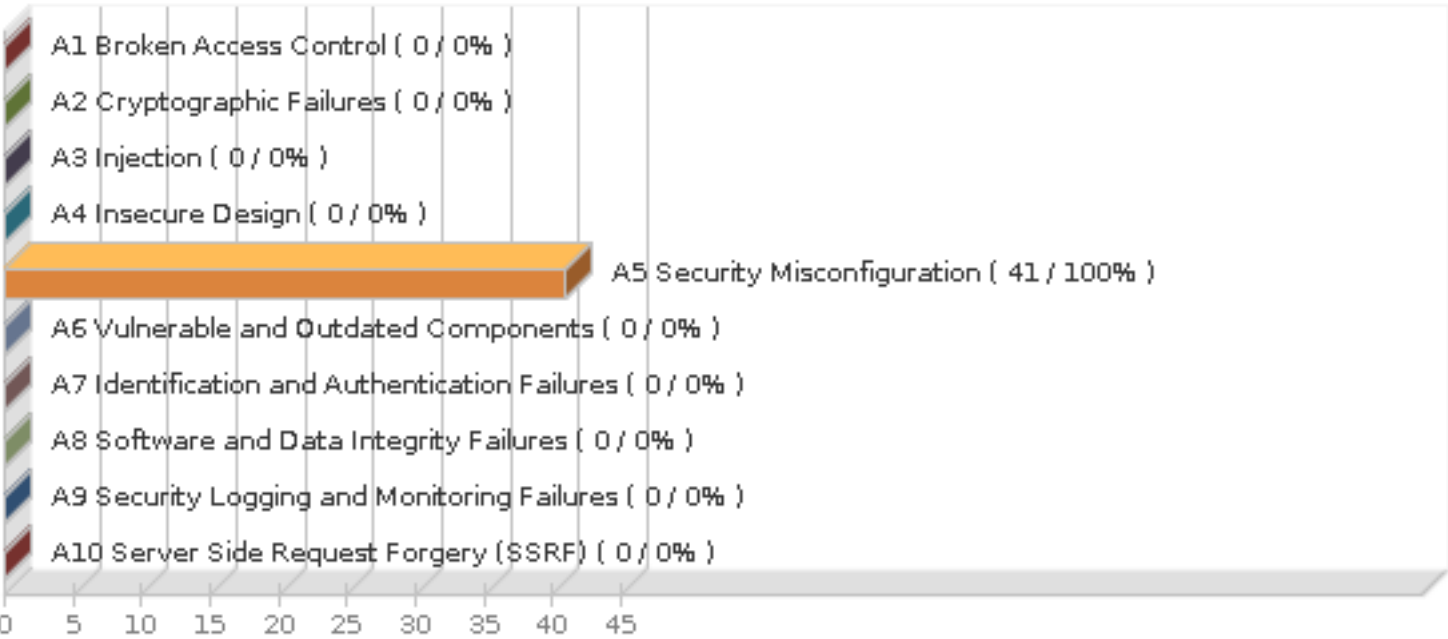
Vulnerabilities by Status



Vulnerabilities by Group



OWASP Top 10 2021 Vulnerabilities



Web Application	Level 5	Level 4	Level 3	Level 2	Level 1	Sensitive Contents	Information Gathered
Develom	0	0	10	0	31	0	39

Results(80)

Vulnerability (41)

Information Disclosure (41)

150124 Clickjacking - Framable Page (10)

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/

Finding #	27264768	Severity	Confirmed Vulnerability - Level 3
Unique #	a173881b-14d1-4300-95c2-f9889b51613c		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

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

Payloads

#1 Request

GET https://www.develom.com/  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/articles

Finding #	27264828	Severity	Confirmed Vulnerability - Level 3
Unique #	bcfab825-3148-4885-9cc5-69fe75224650		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/articles  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/articles/clggsudoa0008xl0upm0wtbq2

Finding #	27264850	Severity	Confirmed Vulnerability - Level 3
Unique #	4e2d52dd-4643-4427-bf79-c547a74bb08c		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/articles/clggsudoa0008x10upm0wtbq2  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/articles/clj7q6qea0004y00uy6syet33

Finding #	27264840	Severity	Confirmed Vulnerability - Level 3
Unique #	d42d075d-0611-450d-a6de-22d4c10e9e37		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/articles/clj7q6qea0004y00uy6syet33  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence

Finding #	27264766	Severity	Confirmed Vulnerability - Level 3
Unique #	d217d762-b3bb-4a8e-9f7d-cb9a570ad0fe		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads



#1 Request

GET https://www.develom.com/articles/what-are-the-top-10-approaches-a-fortune-500-mu st-follow-when-using-artificial-intelligence

Host: www.develom.com

User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36

Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/contact

Finding #	27264776	Severity	Confirmed Vulnerability - Level 3
Unique #	f1f1be84-3e2c-4cbc-85b8-6525db97a598		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.

Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

See the [OWASP Clickjacking Defense Cheat Sheet](#) for more information.

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/contact  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/products

Finding #	27264836	Severity	Confirmed Vulnerability - Level 3
Unique #	6c66de41-004e-4495-859d-a3358897506c		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/products  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/use-cases

Finding #	27264822	Severity	Confirmed Vulnerability - Level 3
Unique #	dd9012ba-9d3c-43d6-be65-c305dbfc422a		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/use-cases  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/videos

Finding #	27264816	Severity	Confirmed Vulnerability - Level 3
Unique #	c8a9ac37-dda8-4747-850d-00deb70fd7e7		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150124 Clickjacking - Framable Page

Develom

Active

URL: https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp

Finding #	27264790	Severity	Confirmed Vulnerability - Level 3
Unique #	8ca241b3-53cb-48c5-9ae3-87cee7b5a84c		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-451	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-15 APPLICATION MISCONFIGURATION	Times Detected	2
CVSS V3 Base	5.8	CVSS V3 Temporal	5.2
		CVSS V3 Attack Vector	Network

Details

Threat

The web page can be framed. This means that clickjacking attacks against users are possible.  
Note: For both 150245 and 150124 only 10 pages are reported and only responses with status code 200 ok are tested and reported

Impact

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

Solution

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

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

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The URI was framed.

150146 Passive Mixed Content Vulnerability (31)

150146 Passive Mixed Content Vulnerability

DevelomActive

URL: https://www.develom.com/about-us

Finding #	27264802	Severity	Confirmed Vulnerability - Level 1
Unique #	3f9ae64a-1da7-4ead-be61-a2f28f0afacc		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/about-us  
Referer: https://www.develom.com/  
Cookie: entityId=clmuy18fn000e1b4511u2vch6; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/about-us was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/57f3f693-2c87-411d-958a-1939972adea9

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/articles

Finding #	27264830	Severity	Confirmed Vulnerability - Level 1
Unique #	6c9b1740-823a-4324-ab23-dee388d80d0e		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/articles  
Referer: https://www.develom.com/  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/articles was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/f99e0c02-0d51-48ad-9798-42ebc999c3d5

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/articles/clggsudoa0008xl0upm0wtbq2

Finding #	27264852	Severity	Confirmed Vulnerability - Level 1
Unique #	ea14de62-ee05-4ca3-8498-15ff8979f434		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal	3
		CVSS V3 Attack Vector	Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads



#1 Request

GET https://www.develom.com/articles/clggsudoa0008xl0upm0wtbq2  
Referer: https://www.develom.com/  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/articles/clggsudoa0008xl0upm0wtbq2 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/d81c6047-122f-490c-9f58-eeadb145bb74

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/articles/clj7qnnyr000cy00u04icighu

Finding #	27264806	Severity	Confirmed Vulnerability - Level 1
Unique #	e232dcf0-5689-4bbb-8857-f927747bd822		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal	3
		CVSS V3 Attack Vector	Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/articles

Payloads

#1 Request

GET https://www.develom.com/articles/clj7qnnyr000cy00u04icighu  
Referer: https://www.develom.com/  
Cookie: entityId=from-healthcare-to-finance-real-life-ai-use-cases-that-inspire; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/articles/clj7qnnyr000cy00u04icighu was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/89a0ba2f-90de-4a0d-acac-8b95eb54245c

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/articles/clj7qx5td000my00uqwm5wtlk

Finding #	27264780	Severity	Confirmed Vulnerability - Level 1
Unique #	4bc38ae6-6ba0-4352-a332-267c0cf52430		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/articles

Payloads

#1 Request

GET https://www.develom.com/articles/clj7qx5td000my00uqwm5wtlk  
Referer: https://www.develom.com/  
Cookie: entityId=unlocking-success-ai-readiness-for-genai-are-you-ready; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/articles/clj7qx5td000my00uqwm5wtlk was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/72c83409-2bfd-473d-aadd-8d70cea65663

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/articles/clj7r43ye000wy00uvzgvyd7

Finding #	27264844	Severity	Confirmed Vulnerability - Level 1
Unique #	a694516a-208c-4429-9342-843ae828dd12		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/articles

Payloads

#1 Request

GET https://www.develom.com/articles/clj7r43ye000wy00uvzgvyd7  
Referer: https://www.develom.com/  
Cookie: entityId=revolutionizing-customer-service-how-chatbots-are-changing-the-game; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/articles/clj7r43ye000wy00uvzgvyd7 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/0bffb0d-a3ba-4891-9381-cfa6323e106d

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/contact

Finding #	27264778	Severity	Confirmed Vulnerability - Level 1
Unique #	bedfd769-4133-4e91-8660-0332cc2fe17c		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/contact  
Referer: https://www.develom.com/  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/contact was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/18daf226-b2d4-4e0c-b24f-12abd96e2122

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/contact?firstName=John%26lastName=John%26email=was@qualys.com%26phone=8000000000%26timeZone=Africa%26Abidjan%26subject=1%26message=1

Finding #	27264842	Severity	Confirmed Vulnerability - Level 1
Unique #	694a7506-2b71-4159-81b3-221ecebb2609		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal	3
		CVSS V3 Attack Vector	Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

<https://www.develom.com/>

Payloads

#1 Request

GET https://www.develom.com/contact?firstName=John&lastName=John&email=was@q ualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&m essage=1  
Referer: https://www.develom.com/  
Cookie: entityId=clggsudoa0008xl0upm0wtbq2; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*  
Content-Length: 112

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

#1 Response

The page at https://www.develom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/180f56fc-714f-4b48-9426-6b5f48ef856f

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/privacy

Finding #	27264834	Severity	Confirmed Vulnerability - Level 1
Unique #	0859db5b-a457-4311-9a53-d3939325520b		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

**Threat**  
Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

**Impact**  
The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

**Solution**  
The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

<https://www.develom.com/>

Payloads

#1 Request

GET https://www.develom.com/privacy  
Referer: https://www.develom.com/  
Cookie: entityId=clog0nmcb0000ye44vyj7j6vz; entity=videos;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/privacy was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/7d6a6729-71cc-437f-ae7-37373fa8ed67

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products

Finding #	27264838	Severity	Confirmed Vulnerability - Level 1
Unique #	f4ac8a91-a599-4a9d-846e-7560bc8cf95a		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/products  
Referer: https://www.develom.com/  
Cookie: entityId=clggsudoa0008xl0upm0wtbq2; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/d833e7be-b68f-4dc2-b05e-8b60555f811e

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmux1i7500041b45ojawf83q

Finding #	27264808	Severity	Confirmed Vulnerability - Level 1
Unique #	6b18c907-f240-4877-9e9e-37befb1138f7		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads



#1 Request

GET https://www.develom.com/products/clmux1i7500041b45ojawf83q  
Referer: https://www.develom.com/  
Cookie: entityId=clmv8ns9x0006us4ttfhr3hik; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmux1i7500041b45ojawf83q was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/e68dc9e6-8de2-436a-b963-fe6d1b18d097

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmuxwfy00071b45fz70lz2a

Finding #	27264804	Severity	Confirmed Vulnerability - Level 1
Unique #	169816a8-c34a-4d56-9349-5e21f71ef088		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmuxwlfy00071b45fz70lz2a  
Referer: https://www.develom.com/  
Cookie: entityId=clmuy18fn000e1b4511u2vch6; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmuxwlfy00071b45fz70lz2a was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/907e794f-592c-40f2-a8b5-b0a369f15c37

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmuy83lh000c1b454sixbm0w

Finding #	27264810	Severity	Confirmed Vulnerability - Level 1
Unique #	af3ac8bb-cf18-4c75-8805-ceb4f3acd708		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmuy83lh000c1b454sixbm0w  
Referer: https://www.develom.com/  
Cookie: entityId=revolutionizing-customer-service-how-chatbots-are-changing-the-game; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmuy83lh000c1b454sixbm0w was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/213b3a42-ec99-4ab8-9eb2-82a195ae9b5b

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmuy8fn000e1b451u2vch6

Finding #	27264800	Severity	Confirmed Vulnerability - Level 1
Unique #	509848a3-81e0-400e-9319-f230cabb7f0		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmuy18fn000e1b4511u2vch6  
Referer: https://www.develom.com/  
Cookie: entityId=clmv9544r000cus4t5g598d78; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmuy18fn000e1b4511u2vch6 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/29f66b62-432d-451a-8ef4-223a9178ccc8

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmuz5qml000h1b45qtdz2lk9

Finding #	27264846	Severity	Confirmed Vulnerability - Level 1
Unique #	6138fe02-a447-45be-bae6-351e01daf8fc		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack Vector Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmuz5qml000h1b45qtdz2lk9  
Referer: https://www.develom.com/  
Cookie: entityId=clmv85ero0002us4tb5kuozjw; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmuz5qml000h1b45qtdz2lk9 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/91ef00b7-2b9b-4ff2-8c98-6dfcbd8619c2

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv85ero0002us4tb5kuozjw

Finding #	27264782	Severity	Confirmed Vulnerability - Level 1
Unique #	c19ff4d6-eb19-4a2c-a6b3-8745ca3ad07c		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmv85ero0002us4tb5kuzjw  
Referer: https://www.develom.com/  
Cookie: entityId=clj7qx5td000my00uqwm5wtlk; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv85ero0002us4tb5kuzjw was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/560571f6-908a-4903-9094-6fa168be6c84

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv8ns9x0006us4ttfhr3hik

Finding #	27264784	Severity	Confirmed Vulnerability - Level 1
Unique #	d81736a1-c99e-4102-adb9-7df0d8d36d63		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmv8ns9x0006us4ttfhr3hik  
Referer: https://www.develom.com/  
Cookie: entityId=cllx766m40001zl2qx31jooud; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv8ns9x0006us4ttfhr3hik was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/a98f210d-31bc-4903-9ace-706f12500809

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv8ujvf0007us4ttuu4a5zo

Finding #	27264796	Severity	Confirmed Vulnerability - Level 1
Unique #	3b257d76-8e70-4a5c-9fe3-56eb49ba2597		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmv8ujvf0007us4ttuu4a5zo  
Referer: https://www.develom.com/  
Cookie: entityId=clmuy18fn000e1b4511u2vch6; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv8ujvf0007us4ttuu4a5zo was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/26b9ccf8-f054-40d6-bdae-f148629e71b9

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv8vrct0009us4t7diurr9l

Finding #	27264788	Severity	Confirmed Vulnerability - Level 1
Unique #	8e1e77ff-e8ea-45bd-8998-06e044f3d56d		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads



#1 Request

GET https://www.develom.com/products/clmv8vrct0009us4t7diurr9l  
Referer: https://www.develom.com/  
Cookie: entityId=clmv8ns9x0006us4ttfhr3hik; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv8vrct0009us4t7diurr9l was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/e7370ad7-d4b7-4893-a201-4662a4fbab0d

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv90exx000aus4tjpfsevri

Finding #	27264820	Severity	Confirmed Vulnerability - Level 1
Unique #	550658eb-d574-4ff3-ab90-6c84c53fe6ce		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmv90exx000aus4tjpfsevri  
Referer: https://www.develom.com/  
Cookie: entityId=ai-just-got-more-amazing-discover-openai-s-latest-user-friendly-innovations; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv90exx000aus4tjpfsevri was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/2f03a3a1-29df-4412-b7a9-a65f19863593

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv91j6j000bus4tbsu30gy3

Finding #	27264826	Severity	Confirmed Vulnerability - Level 1
Unique #	a117dd7a-37ec-409e-b6de-54d776b45650		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack Vector Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmv91j6j000bus4tbsu30gy3  
Referer: https://www.develom.com/  
Cookie: entityId=clmux1i7500041b45ojawf83q; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv91j6j000bus4tbsu30gy3 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/555d30ad-4143-4cde-a0ce-a5e263d0502b

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/products/clmv9544r000cus4t5g598d78

Finding #	27264770	Severity	Confirmed Vulnerability - Level 1
Unique #	3fbb9f2f-f217-4126-b79f-0a22c92fe9ae		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/products

Payloads

#1 Request

GET https://www.develom.com/products/clmv9544r000cus4t5g598d78  
Referer: https://www.develom.com/  
Cookie: entityId=clmv85ero0002us4tb5kuozjw; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/products/clmv9544r000cus4t5g598d78 was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/e6a30f3e-0fef-473f-b197-3eafb50c1f50

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/terms

Finding #	27264814	Severity	Confirmed Vulnerability - Level 1
Unique #	552979a9-5d45-418e-86b2-eade5ac870f0		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack Vector Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/terms  
Referer: https://www.develom.com/  
Cookie: entityId=clmv90exx000aus4tjpfsevri; entity=products;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/terms was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/88e02d9c-1885-4e21-800c-9cbd39530056

150146 Passive Mixed Content Vulnerability

Develop

Active

URL: https://www.develom.com/use-cases

Finding #	27264824	Severity	Confirmed Vulnerability - Level 1
Unique #	3fae4712-6777-4980-8f3a-b337c581c9a6		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/use-cases  
Referer: https://www.develom.com/  
Cookie: entityId=clggsudoa0008xl0upm0wtbq2; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/use-cases was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/1a864c4e-8369-4fe2-aea4-03ce445b59c6

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/videos

Finding #	27264818	Severity	Confirmed Vulnerability - Level 1
Unique #	7bb53f04-fce8-4f93-a404-6fddb11b6e95		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos  
Referer: https://www.develom.com/  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/videos was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/3eebe3dd-4d07-44eb-a867-b704365841a5

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/videos/clj7rv3ax000yy00u0qzsta2h

Finding #	27264794	Severity	Confirmed Vulnerability - Level 1
Unique #	9983e870-5f74-478f-bdca-09cc32a74aac		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal	3
		CVSS V3 Attack Vector	Network

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos/clj7rv3ax000yy00u0qzsta2h  
Referer: https://www.develom.com/  
Cookie: entityId=clog0nmcb0000ye44vyj7j6vz; entity=videos;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/videos/clj7rv3ax000yy00u0qzsta2h was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/c7242b8c-a99f-44b3-96c1-b28dcdae021f

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/videos/clnvzzq2z0002t6440a247c7g

Finding #	27264832	Severity	Confirmed Vulnerability - Level 1
Unique #	ea75f584-b265-4bf5-b5c3-2ac52c549eae		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads



#1 Request

GET https://www.develom.com/videos/clnvzzq2z0002t6440a247c7g  
Referer: https://www.develom.com/  
Cookie: entityId=clo1rphds0003xq4awxl4qvpp; entity=videos;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/videos/clnvzzq2z0002t6440a247c7g was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/95ca4909-9408-40cd-844e-e82fefaa66b8

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/videos/clnyph7xn0000ts45l2pnq07m

Finding #	27264812	Severity	Confirmed Vulnerability - Level 1
Unique #	fec5c64b-1567-4f14-a2ea-64de165b3cd3		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos/clnyph7xn0000ts45l2pnq07m  
Referer: https://www.develom.com/  
Cookie: entityId=clj7rv3ax000yy00u0qzsta2h; entity=videos;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/videos/clnyph7xn0000ts45l2pnq07m was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/6616eb1f-9c79-40e0-bad7-c8822c3ff581

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp

Finding #	27264792	Severity	Confirmed Vulnerability - Level 1
Unique #	d45d4fde-d24c-4d71-99db-c9b68da400ae		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp  
Referer: https://www.develom.com/  
Cookie: entityId=clj7q6qea0004y00uy6syet33; entity=articles;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/b92c8fe2-b223-4f00-a569-5d7d51919492

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/videos/clog0nmcb0000ye44vyj7j6vz

Finding #	27264798	Severity	Confirmed Vulnerability - Level 1
Unique #	1440cde4-ad7c-413e-a1d4-00fdcbbc989d		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/

Payloads

#1 Request

GET https://www.develom.com/videos/clog0nmcb0000ye44vyj7j6vz  
Referer: https://www.develom.com/  
Cookie: entityId=clnvzzq2z0002t6440a247c7g; entity=videos;  
Host: www.develom.com  
User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36  
Accept: \*/\*

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

#1 Response

The page at https://www.develom.com/videos/clog0nmcb0000ye44vyj7j6vz was loaded over HTTPS, but following requested an insecure resource.  
Miscellaneous  
blob:https://www.develom.com/97c5e93b-70ba-4dcd-9ecb-8d93051fc7b4

150146 Passive Mixed Content Vulnerability

Develom

Active

URL: https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721327129039

Finding #	27264786	Severity	Confirmed Vulnerability - Level 1
Unique #	eb530c1f-06b6-4bbc-a78b-abc1791dfb5a		
Group	Information Disclosure	First Time Detected	18 Jul 2024 11:23 GMT-0800
CWE	CWE-319	Last Time Detected	18 Jul 2024 12:48 GMT-0800
OWASP	A5 Security Misconfiguration	Last Time Tested	18 Jul 2024 12:48 GMT-0800
WASC	WASC-4 INSUFFICIENT TRANSPORT LAYER PROTECTION	Times Detected	2
CVSS V3 Base	3.1	CVSS V3 Temporal3	CVSS V3 Attack VectorNetwork

Details

Threat

Passive mixed content vulnerability has been discovered while loading the web page. In mixed-content web applications, the web page is delivered to the browser over secure channel but additional content is delivered over non secure channel. We classify the mixed content into Passive mixed content with reference to Mozilla Firefox browser behavior. Passive mixed-content Vulnerability is reported if any of the following content are discovered when loading the web page to be delivered over non secure channel. Images, Audio, Video

Impact

The non secure channels(HTTP) is not encrypted and hence vulnerable to sniffing attacks. These non secure channels can be exploited to gain access to wide set of capabilities such as forging requests, stealing cookies or DOM data leakage.

Solution

The solution to mixed content vulnerability is simply load sub-resources of web page over HTTPS. Apart from loading sub-resource over HTTPS, it can mitigated using following two options: 1. HTTP Strict Transport Security (HSTS) 2. Content Security Policy (CSP)

Detection Information

Parameter	No param has been required for detecting the information.
Authentication	In order to detect this vulnerability, no authentication has been required.
Access Path	Here is the path followed by the scanner to reach the exploitable URL:

https://www.develom.com/  
https://www.develom.com/?email=was@qualys.com

Payloads

#1 Request

GET https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721327104116

Referer: https://www.develop.com/

Cookie: entityId=clog0nmc0000ye44vyj7j6vz; entity=videos;

Host: www.develop.com

User-Agent: Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.177 Safari/537.36

Accept: \*/\*

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

#1 Response

The page at https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721327104116 was loaded over HTTPS, but following requested an insecure resource.

Miscellaneous

blob:https://www.develop.com/ee758774-8dd2-4269-bf8e-d07f63e6ec6a

Information Gathered (39)

Information Disclosure (1)

150319 Weak Cookies in Use (1)

150319 Weak Cookies in Use

Develop

Finding #	12630738	Severity	Information Gathered - Level 2
Unique #	102cbd8f-6aca-4a04-ae01-7746701432e3		
Group	Information Disclosure		
CWE	CWE-6	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	A4 Insecure Design		
WASC	-		

Details

Threat

Cookies are used to track HTTP sessions. Both session and non-session cookies could be persistent cookies in those cases it is important to verify the complexity of the cookie values.

Detection: WAS scan evaluates cookie length, analyzes for common cookie parameters not limited to PHPSESSID, ASP.NET\_SessionId, JSESSIONID, sessionId, etc.

Impact

With weak cookie values, sessions can be predictable. Such cookies can be used by attacker and impersonate as a legitimate user to steal information or carry out some malicious operations.

Solution

Review cookies reported, all session cookies should have strong length, combination of alpha-number characters.

Use cryptographically secure pseudorandom number generator (CSPRNG) with a size of at least 128 bits and ensure that each sessionId is unique.

Verify non-session cookie values are strong, randomize as applicable.

Results

Weak cookies detected: 1

entity=articles with issuing URI: https://www.develop.com/contact, reason: Cookie value alphabetic only

Scan Diagnostics (26)

150018 Connection Error Occurred During Web Application Scan (1)

Develop

150018 Connection Error Occurred During Web Application Scan

Finding #	12630720	Severity	Information Gathered - Level 2
Unique #	46a13b38-4668-4b6d-8c35-843c10ec5551		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

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

Impact

Some of the resources were not accessible. Results may be incomplete or incorrect.

Solution

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

Results

Total number of unique links that encountered connection errors: 2  
Links with highest number of connection errors:  
1 https://www.develop.com/fonts/Gordita-Bold.ttf  
1 https://www.develop.com/fonts/Gordita-Regular.ttf

Phase wise summary of timeout and connection errors encountered:  
ePhaseCrawl : 0 2

150375 PII Fields Found (1)

Develop

150375 PII Fields Found

Finding #	12630734	Severity	Information Gathered - Level 2
Unique #	1b2999ba-6f7d-4a71-a672-f29dc0950434		
Group	Scan Diagnostics		
CWE	CWE-359	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	A2 Cryptographic Failures		
WASC	WASC-13 INFORMATION LEAKAGE		

Details

Threat

Personally Identifiable Information(PII) is found on the form(s) on the Web Application.

Impact

Improper handling of the PII can lead to loss of reputation for the organization and the individuals whose personal information is stored. Attackers can use this information for more focused attacks in the future.

Solution

Please review all the PII fields below in the report and if required, PII should be obtained by lawful and fair means.

Results

Parent URI: https://www.develom.com/

PII fields Found:  
Email

Parent URI: https://www.develom.com/contact

PII fields Found:  
Email  
Phone

150009 Links Crawled (1)

150009 Links Crawled

Develom

Finding #	12630744	Severity	Information Gathered - Level 1
Unique #	afae6876-f9df-4288-921c-a4568a61ec4e		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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

# WAS Web Application Report

Duration of crawl phase (seconds): 1763.00  
Number of links: 62  
(This number excludes form requests and links re-requested during authentication.)

https://www.develom.com/  
https://www.develom.com/?email=was@qualys.com  
https://www.develom.com/about-us  
https://www.develom.com/articles  
https://www.develom.com/articles/ai-just-got-more-amazing-discover-openai-s-latest-user-friendly-innovations  
https://www.develom.com/articles/clggsudoa0008xl0upm0wtbq2  
https://www.develom.com/articles/clj7q6qa0004y00uy6syet33  
https://www.develom.com/articles/clj7qnnyr000cy00u04icighu  
https://www.develom.com/articles/clj7qx5td000my00uqwm5wtlk  
https://www.develom.com/articles/clj7r43ye000wy00uvzgvvyd7  
https://www.develom.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds  
https://www.develom.com/articles/from-healthcare-to-finance-real-life-ai-use-cases-that-inspire  
https://www.develom.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses  
https://www.develom.com/articles/revolutionizing-customer-service-how-chatbots-are-changing-the-game  
https://www.develom.com/articles/unlocking-success-ai-readiness-for-genai-are-you-ready  
https://www.develom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence  
https://www.develom.com/contact  
https://www.develom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1  
https://www.develom.com/favicon.ico  
https://www.develom.com/hero\_banner/Hero\_banner\_1728.webp  
https://www.develom.com/legal/privacy  
https://www.develom.com/logo\_gradient.svg  
https://www.develom.com/privacy  
https://www.develom.com/products  
https://www.develom.com/products/cllx766m40001zl2qx3ljooud  
https://www.develom.com/products/clmux1i7500041b45ojawf83q  
https://www.develom.com/products/clmuxwlfy00071b45fz70lz2a  
https://www.develom.com/products/clmuy83lh000c1b454sixbm0w  
https://www.develom.com/products/clmuy18fn000e1b451lu2vch6  
https://www.develom.com/products/clmuz5qml000h1b45qtdz2lk9  
https://www.develom.com/products/clmv85ero0002us4tb5kuozjw  
https://www.develom.com/products/clmv8ns9x0006us4ttfhr3hik  
https://www.develom.com/products/clmv8ujvf0007us4ttuu4a5zo  
https://www.develom.com/products/clmv8vrct0009us4t7diurr9l  
https://www.develom.com/products/clmv90exx000aus4tjpfsevri  
https://www.develom.com/products/clmv9lj6j000bus4tbsu30gy3  
https://www.develom.com/products/clmv9544r000cus4t5g598d78  
https://www.develom.com/terms  
https://www.develom.com/use-cases  
https://www.develom.com/use-cases/clnbyne4900001c4r7wx1fx0r  
https://www.develom.com/use-cases/clncmoho400091c4rs0w1nwi8  
https://www.develom.com/use-cases/clncoc8nv000a1c4rmwz7t3ou  
https://www.develom.com/use-cases/clncovabx000b1c4roqzdbp8e  
https://www.develom.com/use-cases/clncpafk3000c1c4rswlxy179  
https://www.develom.com/videos  
https://www.develom.com/videos/clj7rv3ax000yy00u0qzsta2h  
https://www.develom.com/videos/clnvzzq2z0002t6440a247c7g  
https://www.develom.com/videos/clnyph7xn0000ts45l2pnq07m  
https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp  
https://www.develom.com/videos/clog0nmcb0000ye44vyj7j6vz  
https://www.develom.com/~partytown/  
https://www.develom.com/~partytown/%7BS(  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331724174  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331739362  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331759497  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331778695  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331780446  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331787348  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331789548  
https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331796107  
http://www.develom.com/  
http://www.develom.com/favicon.ico

 150010 External Links Discovered (1)

 150010 External Links Discovered

Develom

Finding #	12630742	Severity	Information Gathered - Level 1
Unique #	13e2db30-8d3e-430a-8069-6eefb382e3dd		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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: 75  
https://d116fk6v375eub.cloudfront.net/velom-chatbot-training-E72KgQKOLt5qW07nK8z7.mp4  
https://privacy.apple.com/  
https://develom-media-assets.s3.us-east-2.amazonaws.com/0da7f6a4-38cb-40d7-984b-1fd0edf8cf38.png?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=3b696383effb973b2d138ccd32d1b0f8f7790fd1b7b4e877d3e631017ddaf333&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/0da7f6a4-38cb-40d7-984b-1fd0edf8cf38.png?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=2f70c54d7f7b456c838fc45293ce6773aa2e65b0e9150368994fa2c29ff68ddc&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/2ce2c478-ec7c-43d0-a0ac-0eb4d1635a2e.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=29d351387817f2ff7d3fa872450657831931dc630cabd6711b3154e9980a3a5f&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/2ce2c478-ec7c-43d0-a0ac-0eb4d1635a2e.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=fbdb64d54edceb789f412fc2237bc2f2f7b77c27d131eb2d4068537a5ebbd0ce3&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66adb9ea-eaaa-4bc4-92fc-b2fd4f7e62e0.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=63788a459986115ebbd00daa9c7384753294fe5ab4caec176da0d19270821d7&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66adb9ea-eaaa-4bc4-92fc-b2fd4f7e62e0.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=65397dd2bfa4c5a90bce92bccc20097fed41d1758379ca05d966b5e168ab0&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66c57819-3dab-432e-8264-f90d2fdee87.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=b92cba437f691d5793808b006660da0b15f7719986c2189d243258a96deabce&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/83133546-081b-4d04-b173-51b674746d26.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=65406af7d1717690623b09ceff4e99ec78b59dd6797edb2f59d321262e994270&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/bb34dd0f-8d5b-4627-a8e5-9d23f1e379b.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=96b9d894ec30341152dfbebd2312dbdb7c26d74d79869286f6e8d8917e228c1b&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/83133546-081b-4d04-b173-51b674746d26.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=c2a0202448fa6ece08fe85b4b3de1dc5b8306876adcd8af4110d1772e7822ca0&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/bb34dd0f-8d5b-4627-a8e5-9d23f1e379b.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=aff36d9235119768490bdfb8101f4935a8cd93908b7b7e31d26bb8d3a6883d9d&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/bf1898a8-9f90-4c7e-84f8-ca3614aef6f0f.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=e0bac8bd80fd48731723095f0964d4d4d4e7ad7f7c49530dc70561720b504fe9&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/bf1898a8-9f90-4c7e-84f8-ca3614aef6f0f.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=fef47fef906e024d68f15c4b16b4620c7d71bbae5254969158b4270ca65b750&X-Amz-SignedHeaders=host&x-id=GetObject  
https://github.com/develom-dev  
https://www.google.com/js/t/G9IHigwxVH3Mn3WnChzJeeVNQhz-kZ0Q5G-GviBI-tL.js  
https://static.doubleclick.net/instream/ad\_status.js  
https://www.linkedin.com/company/develom-ai  
https://fonts.gstatic.com/s/montserrat/v26/JTUQjIg1\_i6t8kCHKm459WxRyS7m.woff2  
https://fonts.gstatic.com/s/montserrat/v26/JTUSjIg1\_i6t8kCHKm459Wlhwy.woff2  
https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBc4.woff2  
https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2  
https://fonts.googleapis.com/  
https://fonts.googleapis.com/css?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap  
https://fonts.googleapis.com/css?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap  
https://develom.com/contact  
https://develom.com/legal/cookies.html  
https://develom.com/team  
https://www.gstatic.com/cv/js/sender/v1/cast\_sender.js  
https://www.gstatic.com/eureka/clank/102/cast\_sender.js  
https://chat.openai.com/c/420c784d-de42-4ad6-929f-ad28b734ef38

# WAS Web Application Report

https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK  
https://googleads.g.doubleclick.net/pagead/id  
https://www.youtube.com/@develom\_ai/  
https://www.youtube.com/api/stats/at?ns=yt&el=embedded&cpn=33eMa4viKM1EATfB&ver=2&cmt=0&fs=0&rt=7.214&euri=https%3A%2F%2Fwww.develop.com%2F&lact=8808&cl=653065649&mos=0&volume=100&abr=Chrome&abrver=102.0.5005.177&c=WEB\_EMBEDDED\_PLAYER&cver=1.20240715.01.00&cplayer=UNIPLAYER&cos=X11&cplatfor

https://www.youtube.com/api/stats/at?ns=yt&el=embedded&cpn=5HCWmx\_eb0T-FA5u&ver=2&cmt=0&fs=0&rt=8.597&euri=https%3A%2F%2Fwww.develop.com%2F&lact=9385&cl=652668211&mos=0&volume=100&abr=Chrome&abrver=102.0.5005.177&c=WEB\_EMBEDDED\_PLAYER&cver=1.20240715.01.00&cplayer=UNIPLAYER&cos=X11&cplatfor

https://www.youtube.com/api/stats/at?ns=yt&el=embedded&cpn=AVQzFw8opWHfN-Te&ver=2&cmt=0&fs=0&rt=7.394&euri=https%3A%2F%2Fwww.develop.com%2F&lact=8366&cl=652668211&mos=0&volume=100&abr=Chrome&abrver=102.0.5005.177&c=WEB\_EMBEDDED\_PLAYER&cver=1.20240715.01.00&cplayer=UNIPLAYER&cos=X11&cplatfor

HahZM  
https://www.youtube.com/api/stats/at?ns=yt&el=embedded&cpn=CtLeIKiWUduzbBBA&ver=2&cmt=0&fs=0&rt=6.69&euri=https%3A%2F%2Fwww.develop.com%2F&lact=7483&cl=652668211&mos=0&volume=100&abr=Chrome&abrver=102.0.5005.177&c=WEB\_EMBEDDED\_PLAYER&cver=1.20240715.01.00&cplayer=UNIPLAYER&cos=X11&cplatfor

https://www.youtube.com/api/stats/at?ns=yt&el=embedded&cpn=Plt3G8MXUeTm2Kq1&ver=2&cmt=0&fs=0&rt=7.007&euri=https%3A%2F%2Fwww.develop.com%2F&lact=7891&cl=652668211&mos=0&volume=100&abr=Chrome&abrver=102.0.5005.177&c=WEB\_EMBEDDED\_PLAYER&cver=1.20240715.01.00&cplayer=UNIPLAYER&cos=X11&cplatfor

HahZM  
https://www.youtube.com/api/stats/at?ns=yt&el=embedded&cpn=kxi4NC0NZIxExQ2t&ver=2&cmt=0&fs=0&rt=8.1&euri=https%3A%2F%2Fwww.develop.com%2F&lact=9474&cl=652668211&mos=0&volume=100&abr=Chrome&abrver=102.0.5005.177&c=WEB\_EMBEDDED\_PLAYER&cver=1.20240715.01.00&cplayer=UNIPLAYER&cos=X11&cplatfor

https://www.youtube.com/embed/5p248y0a30E%22t=15s  
https://www.youtube.com/embed/5p248y0a30E&t=15s  
https://www.youtube.com/embed/ZXiruGOCn9s  
https://www.youtube.com/embed/tAGQY9\_2Heo  
https://www.youtube.com/embed/w5nEf-HahZM  
https://www.youtube.com/generate\_204?0Riagc  
https://www.youtube.com/generate\_204?7D5h8A  
https://www.youtube.com/generate\_204?HWRM7A  
https://www.youtube.com/generate\_204?i0bnqw  
https://www.youtube.com/generate\_204?kDVnbg  
https://www.youtube.com/generate\_204?zWf80g  
https://www.youtube.com/s/player/8eff86d5/player\_ias.vflset/en\_US/base.js  
https://www.youtube.com/s/player/8eff86d5/player\_ias.vflset/en\_US/embed.js  
https://www.youtube.com/s/player/8eff86d5/player\_ias.vflset/en\_US/remote.js  
https://www.youtube.com/s/player/8eff86d5/www-embed-player.vflset/www-embed-player.js  
https://www.youtube.com/s/player/8eff86d5/www-player.css  
https://www.youtube.com/s/player/d60b0ef9/player\_ias.vflset/en\_US/base.js  
https://www.youtube.com/s/player/d60b0ef9/player\_ias.vflset/en\_US/embed.js  
https://www.youtube.com/s/player/d60b0ef9/player\_ias.vflset/en\_US/remote.js  
https://www.youtube.com/s/player/d60b0ef9/www-embed-player.vflset/www-embed-player.js  
https://www.youtube.com/s/player/d60b0ef9/www-player.css  
https://www.youtube.com/youtu.be/v1/log\_event?alt=json&key=AlzaSyAO\_FJ2SlqU8Q4STEHLGCilw\_Y9\_11qcW8  
https://yt3.ggpht.com/7WZa4nYXdIFzNHaTL5u9sxfD8o55KS2h-tPSwxSbFZGN8\_MB8lnWCC2A1Jbju132oDvQaLLoOg=s68-c-k-c0x00ffffff-no-rj  
https://yt3.ggpht.com/HHjrQZrBhfkugOkjzUJoWr1pteqnTro55ww253giS7A77VgkFeSZEWu0WFFUkzY2lf3vjzwhw=s68-c-k-c0x00ffffff-no-rj  
https://yt3.ggpht.com/QnXaC\_YmVgrih83IPHmS\_37TOJquPQm4ESeop\_PTYvatdS6pJa4ynQ57K9NtD6xV9n41h7to6Bw=s68-c-k-c0x00ffffff-no-rj  
https://www.instagram.com/develom\_ai/  
https://play.google.com/log?format=json&hasfast=true&authuser=0  
https://i.ytimg.com/vi/ZXiruGOCn9s/maxresdefault.jpg  
https://i.ytimg.com/vi/tAGQY9\_2Heo/maxresdefault.jpg  
https://i.ytimg.com/vi/w5nEf-HahZM/maxresdefault.jpg  
https://twitter.com/Develom\_AI  
https://jnn-pa.googleapis.com/\$rpc/google.internal.waa.v1.Waa/Create  
https://jnn-pa.googleapis.com/\$rpc/google.internal.waa.v1.Waa/GenerateIT

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

150020 Links Rejected By Crawl Scope or Exclusion List

Develom

Finding #	12630723	Severity	Information Gathered - Level 1
Unique #	17044207-b21c-465c-b9e9-ab6bd3ca3491		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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://d116fk6v375eub.cloudfront.net/velom-chatbot-training-E72KgQKOLt5qW07nK8z7.mp4  
https://privacy.apple.com/  
https://develom-media-assets.s3.us-east-2.amazonaws.com/0da7f6a4-38cb-40d7-984b-1fd0edf8cf38.png?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=3b696383effb973b2d138ccd32d1b0f8f7790fd1b7b4e877d3e631017ddaf333&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/0da7f6a4-38cb-40d7-984b-1fd0edf8cf38.png?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=2f70c54d7f7b456c838fc45293ce6773aa2e65b0e9150368994fa2c29ff68ddc&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/2ce2c478-ec7c-43d0-a0ac-0eb4d1635a2e.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=29d35138781f2ff7d3fa872450657831931dc630cabd6711b3154e9980a3a5f&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/2ce2c478-ec7c-43d0-a0ac-0eb4d1635a2e.webp?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=fbd64d54edceb789f412fc2237bc2f2f7b77c27d131eb2d4068537a5ebbd0ce3&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66adb9ea-eaaa-4bc4-92fc-b2fd4f7e62e0.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=63788459986115ebbd00daaa9c7384753294fe5ab4caec176da0d19270821d7&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66adb9ea-eaaa-4bc4-92fc-b2fd4f7e62e0.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=65397dd2bfac4c5a90bcee92bccd20097fed41d1758379ca05d966b5e168ab0&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66c57819-3dab-432e-8264-f90d2fdeeb87.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T194156Z&X-Amz-Expires=3600&X-Amz-Signature=b92cba437f691dd5793808b006660da0b15f7719986c2189d243258a96deabce&X-Amz-SignedHeaders=host&x-id=GetObject  
https://develom-media-assets.s3.us-east-2.amazonaws.com/66c57819-3dab-432e-8264-f90d2fdeeb87.jpg?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Content-Sha256=UNSIGNED-PAYLOAD&X-Amz-Credential=AKIATMJ2TEB2KXCDU3CV%2F20240718%2Fus-east-2%2Fs3%2Faws4\_request&X-Amz-Date=20240718T195255Z&X-Amz-Expires=3600&X-Amz-Signature=65406af7d1717690623b09ceff4e99ee78b59dd6797edb2f59d321262e994270&X-Amz-SignedHeaders=host&x-id=GetObject

IP based excluded links:

150021 Scan Diagnostics (1)		Development	
150021 Scan Diagnostics			
Finding #	12630724	Severity	Information Gathered - Level 1
Unique #	3bd3bf6a-0825-4f28-9aee-9f79a202a645		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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://www.develom.com/ fetched. Status code:200, Content-Type:text/html, load time:9 milliseconds.  
Batch #0 VirtualHostDiscovery: estimated time < 30 minutes (70 tests, 0 inputs)  
VirtualHostDiscovery: 70 vulnsigs tests, completed 69 requests, 11 seconds. Completed 69 requests of 70 estimated requests (98.5714%). All tests completed.  
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, 6 seconds. Completed 56 requests of 56 estimated requests (100%). All tests completed.  
Collected 186 links overall in 0 hours 29 minutes duration.  
Cookies Without Consent no tests enabled.  
Duration of Crawl Time: 1763.00 (seconds)  
Total Scan Time: 1763.00 (seconds)

Total requests made: 317  
Average server response time: 5.24 seconds

Average browser load time: 9.91 seconds

150028 Cookies Collected (1)

150028 Cookies Collected

Develom

Finding #	12630727	Severity	Information Gathered - Level 1
Unique #	7e801c26-5776-4344-9185-00a9bcc78086		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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: 3  
entity=articles; expires=Fri, 18-Jul-2025 19:43:18 GMT; domain=www.develop.com; path=/ First set at URL: https://www.develop.com/contact  
entityId=clggsudoa0008x10upm0wtbq2; expires=Fri, 18-Jul-2025 19:43:18 GMT; domain=www.develop.com; path=/ First set at URL: https://www.develop.com/contact  
NID=516=CA2REObNiPB9LJwvela1gOq9nBM0k4UcTd8sELfxVmkBo8b4SsKA2v1tAkcl\_iNYQliHakAXTl\_T8KMdN\_Rlk6XkniJ1eDEk8XDqU9AZaYDUuzxitQSwj6DNyfKPdfQ6R9iEh8fMdA7y  
cpoIS-XTUbS87KS2Pc; secure; HttpOnly; expires=Fri, 17-Jan-2025 19:44:00 GMT; domain=.google.com; path=/ First set at URL: https://www.develop.com/videos/clo1rphds0003xq4awxl4qvpp

150054 Email Addresses Collected (1)

150054 Email Addresses Collected Develop

Finding #	12630733	Severity	Information Gathered - Level 1
Unique #	720444a3-e8ec-4198-97d9-e73354bb0aa5		
Group	Scan Diagnostics		
CWE	CWE-359	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

The email addresses listed in the Results section were collected from the returned HTML content during the crawl phase.

Impact

Email addresses may help a malicious user with brute force and phishing attacks.

Solution

Review the email list to see if they are all email addresses you want to expose.

Results

Number of emails: 7  
info@edustatmentor.com first seen at https://www.develop.com/products/clmv90exx000aus4tjpfsevri  
info@retailriskadvisor.com first seen at https://www.develop.com/products/clmv8ujvf0007us4ttuu4a5zo  
privacy@develop.com first seen at https://www.develop.com/contact  
support@autoregnavigator.com first seen at https://www.develop.com/products/clmv91j6j000bus4tbsu30gy3  
support@energycomplybot.com first seen at https://www.develop.com/products/clmv8vrct0009us4t7diurr9l  
support@healthguardbot.com first seen at https://www.develop.com/products/clmv8ns9x0006us4ttfhr3hik  
support@pharmawiseguide.com first seen at https://www.develop.com/products/clmv9544r000cus4t5g598d78

150104 Form Contains Email Address Field (1)

150104 Form Contains Email Address Field Develop

Finding #	12630730	Severity	Information Gathered - Level 1
Unique #	10a01260-7c5f-4c4a-a46c-6f95c36a190b		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

The HTML form contains a field that collects an email address.

Impact

In some web apps, forms that collect email addresses also generate messages to back-end systems whenever the form is submitted. If no rate limiting or

# WAS Web Application Report

CAPTCHA is applied to form submissions, then vulnerability tests against this form may produce a significant amount of messages. If too many messages are generated, then it may produce a Denial of Service situation.

### Solution

Review the form to determine if it produces an email message each time it is submitted. If so, consider excluding this form from being tested or disable the messaging during the web application scan. Forms that generate messages can be abused by malicious users to create Denial of Service attacks. Apply rate limiting to the form in order to throttle the number of times it may be submitted by a user or by an IP address; or apply a CAPTCHA to it to reduce the chance of automated tools being used against the form.

### Results

https://www.develom.com/  
https://www.develom.com/contact

## 150152 Forms Crawled (1)

### 150152 Forms Crawled

Develom

Finding #	12630726	Severity	Information Gathered - Level 1
Unique #	ebfed16b-ec1e-4647-b911-4adc9d7d7fb3		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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): 45

Crawled forms (Total: 2)  
NOTE: This does not include authentication forms. Authentication forms are reported separately in QID 150115  
Form #:1 Action URI:https://www.develom.com/ (found at: https://www.develom.com/)  
Form Fields: email

Form #:2 Action URI:https://www.develom.com/contact (found at: https://www.develom.com/contact)  
Form Fields: firstName, lastName, email, phone, timeZone, subject, message

NOTE: Forms with exactly the same form fields were considered identical even if they had different action URI. Only one such form is crawled, the other forms with exactly the same form fields are considered duplicate and are not crawled. If they are different forms and each of them should be crawled then change the scan settings accordingly.

The following forms were not crawled as their fields matched Form #1 above:  
Form Action URI: https://www.develom.com/videos



Form Action URI: https://www.develop.com/articles  
Form Action URI: https://www.develop.com/products  
Form Action URI: https://www.develop.com/use-cases  
Form Action URI: https://www.develop.com/contact  
Form Action URI: https://www.develop.com/articles/clggsudoa0008x10upm0wtbq2  
Form Action URI: https://www.develop.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence  
Form Action URI: https://www.develop.com/videos/clo1rphds0003xq4awxl4qvpp  
Form Action URI: https://www.develop.com/articles/clj7q6qea0004y00uy6syet33  
Form Action URI: https://www.develop.com/videos/clj7rv3ax000yy00u0qzsta2h  
Form Action URI: https://www.develop.com/videos/clnvzzq2z0002t6440a247c7g  
Form Action URI: https://www.develop.com/videos/clog0nmcb0000ye44vyj7j6vz  
Form Action URI: https://www.develop.com/videos/clnyph7xn0000ts45l2pnq07m  
Form Action URI: https://www.develop.com/terms  
Form Action URI: https://www.develop.com/privacy  
Form Action URI: https://www.develop.com/about-us  
Form Action URI: https://www.develop.com/articles/clj7r43ye000wy00uvzgvvyd7  
Form Action URI: https://www.develop.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses  
Form Action URI: https://www.develop.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds  
Form Action URI: https://www.develop.com/articles/from-healthcare-to-finance-real-life-ai-use-cases-that-inspire  
Form Action URI: https://www.develop.com/articles/ai-just-got-more-amazing-discover-openai-s-latest-user-friendly-innovations  
Form Action URI: https://www.develop.com/articles/clj7qx5td000my00uqwm5wtlk  
Form Action URI: https://www.develop.com/articles/unlocking-success-ai-readiness-for-genai-are-you-ready  
Form Action URI: https://www.develop.com/articles/revolutionizing-customer-service-how-chatbots-are-changing-the-game  
Form Action URI: https://www.develop.com/articles/clj7qnnyr000cy00u04icighu  
Form Action URI: https://www.develop.com/products/clmv85ero0002us4tb5kuozjw  
Form Action URI: https://www.develop.com/products/clmv90exx000aus4tjpfsevr  
Form Action URI: https://www.develop.com/products/clmuxwlfy00071b45fz70lz2a  
Form Action URI: https://www.develop.com/products/clmuy18fn000e1b45l1u2vch6  
Form Action URI: https://www.develop.com/products/clmv8ujvf0007us4ttuu4a5zo  
Form Action URI: https://www.develop.com/products/clmv8vrct0009us4t7diurr9l  
Form Action URI: https://www.develop.com/products/clmv9544r000cus4t5g598d78  
Form Action URI: https://www.develop.com/products/clmux1i7500041b45ojawf83q  
Form Action URI: https://www.develop.com/products/clmuy83lh000c1b454sixbm0w  
Form Action URI: https://www.develop.com/products/cllx766m40001zl2qx3ljooud  
Form Action URI: https://www.develop.com/products/clmv91j6j000bus4tbsu30gy3  
Form Action URI: https://www.develop.com/products/clmuz5qml000h1b45qtdz2lk9  
Form Action URI: https://www.develop.com/products/clmv8ns9x0006us4ttfhr3hik  
Form Action URI: https://www.develop.com/use-cases/clncoc8nv000a1c4rmwz7t3ou  
Form Action URI: https://www.develop.com/use-cases/clncmo400091c4rs0w1nwi8  
Form Action URI: https://www.develop.com/use-cases/clncpafk3000c1c4rswlxy179  
Form Action URI: https://www.develop.com/use-cases/clnbyne4900001c4r7wx1fx0r  
Form Action URI: https://www.develop.com/use-cases/clncovabx000b1c4roqzdbp8e

150176 In-scope JavaScript Libraries Detected (1)			
150176 In-scope JavaScript Libraries Detected		Develom	
Finding #	12630732	Severity	Information Gathered - Level 1
Unique #	475620c7-f974-4014-8ac4-baf53266ca5e		
Group	Scan Diagnostics		
CWE	CWE-200	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details
---------

Threat

WAS will report "in-scope" JavaScript libraries discovered by the scanner during crawling and are provided in the Results section. In-scope means, links that are considered to be "in-scope" per the configuration set up for the Web Application. The discovered libraries are reported only once, based on the page on which they were first detected.

Each library is reported along with other information such as the URL of page on which it was first found, the version, and the URL of the .js file.

Impact

When including third-party JavaScript libraries, the application must effectively trust those libraries added. Without sufficient protection mechanisms, the functionality may be malicious in nature (i.e. either by coming from an untrusted source, being spoofed, or being modified in transit from a trusted source).

Solution

Use digital signatures or similar mechanisms to verify the software or data is from the expected source and has not been altered. Ensure libraries and dependencies, are consuming trusted repositories. If you have a higher risk profile, consider hosting an internal known-good repository that's vetted.

Results

Number of unique JS libraries: 1  
Javascript library : METAGeneratorReports  
Version : Astro v3.4.3  
Found on the following page(only first page is reported):  
<https://www.develom.com/>

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

Develom

150528 Server Returns HTTP 4XX Error Code During Scanning

Finding #	12630722	Severity	Information Gathered - Level 1
Unique #	36a9df0a-91dd-499b-92d9-13c12d44ccbd		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

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

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

Impact

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

Solution

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

Results

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

404 <https://www.develom.com/favicon.ico>  
404 <https://www.develom.com/legal/privacy>  
404 <https://www.develom.com/~partytown/>  
404 [150546 First Link Crawled Response Code Information \(1\)](https://www.develom.com/~partytown/%7BS(</a></p></div><div data-bbox=)



150546 First Link Crawled Response Code Information

Developm

Finding #	12630728	Severity	Information Gathered - Level 1
Unique #	358e1554-19be-4b5d-af87-80994eefc8af		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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://www.developom.com/  
Response Code: 200  
Response Header:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::9btb7-1721331733156-f5f97b74a366

Response Body:  
<!DOCTYPE html><html lang="en" class="bg-background"><head><!-- Google tag (gtag.js) --><script type="text/partytown-x" async="" src="https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK"></script><script type="text/partytown-x">window.dataLayer = window.dataLayer || [];  
function gtag() {  
dataLayer.push(arguments);  
}  
gtag("js", new Date());  
  
gtag("config", "G-8TXQH76GDK");  
</script><meta charset="UTF-8"><meta name="viewport" content="width=device-width"><meta name="google-site  
...

150621 List of JavaScript Links (1)

150621 List of JavaScript Links

Developm

Finding #	12630731	Severity	Information Gathered - Level 1
Unique #	9dfd5fa3-c8be-4ed0-b6cd-561db821fd66		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

This QID reports all the JavaScript links that are in-scope of this scan.

Impact

JavaScript links may pose security risks such as XSS, CSRF.

Solution

Verify JavaScript links are intentional and required for your web application.  
Review any third party scripts that are hosted on your local server instead of using CDN.  
Update all the JavaScript libraries with latest version as applicable.

Results

JavaScript Links were found while crawling.  
Total Number of Links: 32  
https://www.developom.com/\_astro/ChatBubble.03a86e9a.js  
https://www.developom.com/\_astro/DevelopomApolloProvider.0fe78ec8.js  
https://www.developom.com/\_astro/Footer.979b54a3.js  
https://www.developom.com/\_astro/GradientComponent.b189efbc.js  
https://www.developom.com/\_astro/HeroBannerLandingPage.82365e97.js  
https://www.developom.com/\_astro/NavBar.be2d4950.js  
https://www.developom.com/\_astro/axios.8a9713b4.js  
https://www.developom.com/\_astro/client.e04c411a.js  
https://www.developom.com/\_astro/clsx.m.1229b3e0.js  
https://www.developom.com/\_astro/index.0f268f1b.js  
https://www.developom.com/\_astro/index.c30e9e06.js  
https://www.developom.com/\_astro/jsx-runtime.4e6dfa6a.js  
https://www.developom.com/\_astro/keyboard.be908299.js  
https://www.developom.com/\_astro/transition.0053f6cc.js  
https://www.developom.com/\_astro/NavBar.9431a621.js  
https://www.developom.com/\_astro/PlayCircleIcon.5bf2f150.js  
https://www.developom.com/\_astro/ShareModal.ca6fd24c.js  
https://www.developom.com/\_astro/Videos.45a29a33.js  
https://www.developom.com/\_astro/ArticleCard.0b0e5248.js  
https://www.developom.com/\_astro/Articles.f9fd8fa3.js  
https://www.developom.com/\_astro/index.ce4c6bf6.js  
https://www.developom.com/\_astro/Products.e5a84468.js  
https://www.developom.com/\_astro/UseCases.434a4839.js  
https://www.developom.com/\_astro/Contact.3b412af9.js  
https://www.developom.com/\_astro/KeyStoneRenderer.4ef45748.js  
https://www.developom.com/\_astro/KeyStoneRenderer.1c4393eb.js  
https://www.developom.com/\_astro/\_urlId\_.8ef2d33c.fca56edb.js  
https://www.developom.com/\_astro/Video.fac7eacf.js  
https://www.developom.com/\_astro/Terms.4fea6ce4.js  
https://www.developom.com/\_astro/Privacy.1273b1f4.js  
https://www.developom.com/\_astro/About\_Us.118cbc02.js  
https://www.developom.com/.

38116 SSL Server Information Retrieval (1)

38116 SSL Server Information Retrieval

Development

Finding #	12630752	Severity	Information Gathered - Level 1
Unique #	4e76f2f1-b0a7-468a-a7b8-1ff61c99363a		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

# WAS Web Application Report

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	76.76.21.142
IP	76.76.21.142
Port	443
Result	#table cols="6" CIPHER KEY-EXCHANGE AUTHENTICATION MAC ENCRYPTION(KEY-STRENGTH) GRADE SSLv2_PROTOCOL_IS_DISABLED _____ SSLv3_PROTOCOL_IS_DISABLED _____ TLSv1_PROTOCOL_IS_DISABLED _____ TLSv1.1_PROTOCOL_IS_DISABLED _____ TLSv1.2_PROTOCOL_IS_ENABLED _____ TLSv1.2_COMPRESSION_METHOD None _____ DHE-RSA-AES256-GCM-SHA384 DH RSA AEAD AESGCM(256) HIGH 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_DISABLED _____

## Info List

### Info #1

## Ciphers

Name	Auth	Encryption	Grade	Key Exchange	Mac	Protocol
DHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	DH	AEAD	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(128)	MEDIUM	ECDH	AEAD	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	RSA	AESGCM(256)	HIGH	ECDH	AEAD	TLSv1.2
DHE-RSA-AES256-GCM-SHA384	RSA	CHACHA20/POLY1305(256)	HIGH	ECDH	AEAD	TLSv1.2

38291 SSL Session Caching Information (1)

38291 SSL Session Caching Information

Developm

Finding #

12630749

Severity

Information Gathered - Level 1

# WAS Web Application Report

Unique #	3034f16f-6cf4-4789-8919-751b8541ab1a		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	TLSv1.2 session caching is enabled on the target.

## Info List

### Info #1

<div><div></div><div></div></div>	<b>38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance (1)</b>			
<div><div></div><div></div></div>	38597 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Invalid Protocol Version Tolerance			Development
Finding #	12630751		Severity	Information Gathered - Level 1
Unique #	644e04ae-a3aa-46c0-9348-17b8af7967f6			
Group	Scan Diagnostics			
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800	
OWASP	-			
WASC	-			

## Details

### Threat

# WAS Web Application Report

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	76.76.21.142
IP	76.76.21.142
Port	443
Result	#table cols=2 my_version target_version 0304 rejected 0399 rejected 0400 rejected 0499 rejected

## Info List

### Info #1

38600 SSL Certificate will expire within next six months (1)			
38600 SSL Certificate will expire within next six months			Developm
Finding #	12630756	Severity	Information Gathered - Level 1
Unique #	abfcbb7d-82cc-4516-97c2-f4df44292b4f		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	Certificate #0 CN=www.developm.com The certificate will expire within six months: Oct 1 22:26:49 2024 GMT Certificate #0 CN=no-sni.vercel-infra.com The certifi will expire within six months: Sep 29 11:35:32 2024 GMT

Info List

Info #1

Certificate Fingerprint:71EE0C85570CA6338642BC3213F87B70298E935D0538041C7C808B1F01171A7A

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

Developm

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

Finding #	12630753	Severity	Information Gathered - Level 1
Unique #	3f5f1181-a97f-4ea8-b3ca-1b0046c155f8		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	#table cols="6" NAME GROUP KEY-SIZE FORWARD-SECRET CLASSICAL-STRENGTH QUANTUM-STRENGTH TLSv1.2 _ _ _ _ _ DHE _ 2048 yes 110 low ECDHE x25519 256 yes 128 low ECDHE secp384r1 384 yes 192 low ECDHE secp256r1 256 yes 128 low ECDHE secp521r1 521 yes 260 low

Info List

Info #1

Kexs

Kex	Group	Protocol	Key Size		Classical	Quantum
DHE		TLSv1.2	2048	yes	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

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

Develop

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

Finding #	12630754	Severity	Information Gathered - Level 1
Unique #	d4a681b3-9ff2-460c-a419-6452d9a4c79a		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	#table cols="2" NAME STATUS TLSv1.2 _ Extended_Master_Secret yes Heartbeat no Cipher_priority_controlled_by server OCSP_stapling yes 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	yes	TLSv1.2
SCT extension	no	TLSv1.2

38717 Secure Sockets Layer (SSL) Certificate Online Certificate Status Protocol (OCSP) Information (1)

Develop

38717 Secure Sockets Layer (SSL) Certificate  
Online Certificate Status Protocol (OCSP) Information

Finding #	12630757	Severity	Information Gathered - Level 1
Unique #	bfbbd463-878d-46cb-a977-4d0a96d2c048		
Group	<a href="#">Scan Diagnostics</a>		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	-		
WASC	-		

Details

Threat

OCSP (Online Certificate Status Protocol) is a protocol to determine the status of an SSL certificate, specifically whether a certificate has been revoked by the issuing certificate authority. SSL servers can provide the OCSP status of their certificate as part of the SSL/TLS handshake. This information is referred to as "Status Request" or "OCSP Stapling".

Impact

N/A

Solution

N/A

SSL Data

Flags	-
Protocol	tcp
Virtual Host	76.76.21.142
IP	76.76.21.142
Port	443



Result

Certificate #0 CN=www.develop.com OCSF status: good Certificate #0 CN=no-sni.vercel-infra.com OCSF status: good

Info List

Info #1

Certificate Fingerprint:71EE0C85570CA6338642BC3213F87B70298E935D0538041C7C808B1F01171A7A

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

Develop

38718 Secure Sockets Layer (SSL) Certificate Transparency Information

Finding #	12630758	Severity	Information Gathered - Level 1
Unique #	da2317c8-0128-4c36-86c9-aa61dd7df8b6		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	#table cols="6" Source Validated Name URL ID Time Certificate #0 _ CN=www.develop.com _ _ Certificate no (unknown) (unknown) 3f174b4fd7224758941d651c84be0d12ed90377f1f856aebc1bf2885ecf8646e Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 1998107109f0d6522e3080d29e3f64bb836e28ccf90f528eedf4a3f16b4ca Thu_01_Jan_1970_12:00:00_AM_GMT Certificate #0 _ CN=no-sni.vercel-infra.com _ _ Certificate no (unknown) (unknown) 1998107109f0d6522e3080d29e3f64bb836e28ccf90f528eedf4a3f16b4ca Thu_01_Jan_1970_12:00:00_AM_GMT Certificate no (unknown) (unknown) 48b0e36bdaa647340fe56a02fa9d30eb1c5201cb56dd2c81d9bbbfbab39d88473 Thu_01_Jan_1970_12:00:00_AM_GMT

Info List

Info #1

Certificate Fingerprint:71EE0C85570CA6338642BC3213F87B70298E935D0538041C7C808B1F01171A7A

42350 TLS Secure Renegotiation Extension Support Information (1)

42350 TLS Secure Renegotiation Extension Support Information

Develop

Finding #	12630750	Severity	Information Gathered - Level 1
Unique #	6735ea9c-695d-4327-be62-8d10651cb924		
Group	<a href="#">Scan Diagnostics</a>		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	TLS Secure Renegotiation Extension Status: supported.

Info List

Info #1

45038 Host Scan Time - Scanner (1)

45038 Host Scan Time - Scanner

Develop

Finding #	12630759	Severity	Information Gathered - Level 1
Unique #	d7e641f5-4f38-4332-954e-2cf511e8dd8a		

# WAS Web Application Report

Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	www.develom.com
IP	76.76.21.142
Port	-
Result	Scan duration: 1872 seconds Start time: Thu Jul 18 19:40:54 UTC 2024 End time: Thu Jul 18 20:12:06 UTC 2024

## Info List

### Info #1

6 DNS Host Name (1)			
6 DNS Host Name			Develom
Finding #	12630748	Severity	Information Gathered - Level 1
Unique #	103cee93-ccc4-4825-a1a0-fbda54d91d6e		
Group	Scan Diagnostics		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	-
Result	#table IP_address Host_name 76.76.21.142 No_registered_hostname

Info List

Info #1

86002 SSL Certificate - Information (1)		
86002 SSL Certificate - Information		Develop
Finding #	12630755	Severity
Unique #	9e432f7e-c65a-4016-aa09-5328c3421bc1	Information Gathered - Level 1
Group	Scan Diagnostics	
CWE	-	Detection Date
OWASP	-	18 Jul 2024 12:41 GMT-0800
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	76.76.21.142
IP	76.76.21.142
Port	443
Result	#table cols="2" NAME VALUE (0)CERTIFICATE_0 _ (0)Version 3_(0x2) (0)Serial_Number _04:6a:51:9f:c0:99:f4:dc:6c:14:3a:3e:31:00:e7:76:7c:42_ (0)Signature_Algorithm sha256WithRSAEncryption (0)ISSUER_NAME _ countryName US _organizationName Let's_Encrypt _commonName R10

(0)SUBJECT\_NAME \_commonName www.develop.com (0)Valid\_From Jul\_3\_22:26:50\_2024\_GMT (0)Valid\_Till Oct\_1\_22:26:49\_2024\_GMT (0)Public\_Key\_Algorithm rsaEncryption (0)RSA\_Public\_Key (2048\_bit) (0)\_RSA\_Public-Key: (2048\_bit) (0)\_Modulus: (0)\_00:e0:25:8c:86:ef:5c:8c:0d:0c:b9:1e:91:b2:5f: (0)\_d4:83:f4:48:f0:f2:cf:21:9a:9c:d2:04:0c:12:88: (0)\_62:3f:f5:4b:1a:e7:2c:f2:ae:90:6d:0d:b1:16:f4: (0)\_9e:56:7a:88:b6:d6:60:4b:24:7a:ca:4e:02:22:ed:49: (0)\_37:d4:e7:74:18:f0:c1:32:96:61:d0:1a:e7:0e:ef: (0)\_1f:a0:44:63:62:33:fc:70:da:d9:34:fb:53:9e:6e: (0)\_47:8d:98:f3:0b:03:4a:29:ea:9a:73:ea:51:11:9f: (0)\_87:73:73:f5:a1:40:2b:38:09:d4:c0:d9:52:e5:39: (0)\_ab:a3:3a:9d:61:71:ff:95:22:12:9d:9c:18:30:fd: (0)\_1d:da:76:cb:f0:89:8e:30:54:d0:80:2b:c4:1c:9a: (0)\_49:37:b7:3b:25:7c:e5:3d:bc:b6:8c:21:81:2a:05: (0)\_50:84:a9:9c:18:5a:26:5d:13:a3:a6:fd:1e:11:2e: (0)\_4b:d1:d2:54:34:a1:f6:10:1b:c6:05:29:24:e0:03: (0)\_87:27:9d:fc:66:7b:ed:72:17:0e:4c:b6:d4:96:5f: (0)\_b9:18:03:47:a8:08:3c:ba:49:9f:a2:c9:79:25:b4: (0)\_5a:e6:03:05:89:9b:db:19:fd:e9:fb:f7:53:47:f3: (0)\_7d:77:e8:f3:da:4a:1f:12:b2:af:f9:17:1a:77:a5: (0)\_61:71 (0)\_Exponent: 65537\_(0x10001) (0)X509v3\_EXTENSIONS (0)X509v3\_Key\_Usage critical (0)\_Digital\_Signature\_Key\_Encipherment (0)X509v3\_Extended\_Key\_Usage\_TLS\_Web\_Server\_Authentication,\_TLS\_Web\_Client\_Authentication (0)X509v3\_Basic\_Constraints critical (0)\_CA:FALSE (0)X509v3\_Subject\_Key\_Identifier\_68:8E:80:FE:74:45:61:26:98:B8:8D:44:C3:01:7D:F7:EB:79:6A:DB (0)X509v3\_Authority\_Key\_Identifier\_keyid:BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8 (0)Authority\_Information\_Access\_OCSP\_-\_URI:http://r10.o.lencr.org (0)\_CA\_Issuers\_-\_URI:http://r10.i.lencr.org/ (0)X509v3\_Subject\_Alternative\_Name\_DNS:www.develop.com (0)X509v3\_Certificate\_Policies\_Policy: 2.23.140.1.2.1 (0)CT\_Precertificate\_SCTs\_Signed\_Certificate\_Timestamp: (0)\_Version:\_v1\_(0x0) (0)\_Log\_ID:\_3F:17:4B:4F:D7:22:57:58:94:1D:65:1C:84:BE:0D:12: (0)\_ED:90:37:7F:1F:85:6A:EB:C1:BF:28:85:EC:F8:64:6E (0)\_Timestamp:\_Jul\_3\_23:26:50.769\_2024\_GMT (0)\_Extensions:\_none (0)\_Signature:\_ecdsa-with-SHA256 (0)\_30:44:02:20:05:E8:3D:0A:B8:0C:40:C3:AB:65:CC:66:BC: (0)\_6B:F8:F0:16:AB:3F:33:8C:BA:BB:D4:75:E6:C5:EB:86: (0)\_32:B2:9D:F1:02:20:19:A3:B4:5E:88:67:95:0E:DD:C1: (0)\_4E:65:55:5A:BD:E7:61:3D:AB:7B:E1:62:31:B5:B4:0F: (0)\_4E:D4:33:8A:B7:51 (0)\_Signed\_Certificate\_Timestamp: (0)\_Version:\_v1\_(0x0) (0)\_Log\_ID:\_19:98:10:71:09:F0:D6:52:2E:30:80:D2:9E:3F:64:BB: (0)\_83:6E:28:CF:F9:0F:52:8E:EE:DF:CE:4A:3F:16:B4:CA (0)\_Timestamp:\_Jul\_3\_23:26:50.782\_2024\_GMT (0)\_Extensions:\_none (0)\_Signature:\_ecdsa-with-SHA256 (0)\_30:45:02:21:00:B3:E3:E7:C0:64:CA:CC:B8:75:51:A9: (0)\_5B:B3:D7:03:10:82:FB:CC:39:56:1B:C0:48:7C:39:0B: (0)\_A4:90:D7:53:4E:02:20:69:70:00:A9:72:46:D2:C8: (0)\_30:61:89:E6:7C:84:BF:96:18:28:FF:46:49:22:71:78: (0)\_9A:09:AB:E4:96:29:E8 (0)Signature (256\_octets) (0)\_2a:eb:bd:a7:70:8d:9c:b2:eb:f4:39:b5:8b:ba:95:b3 (0)\_5a:dc:53:80:47:8d:c7:bf:be:ee:6f:73:c7:59:33:ca (0)\_c8:cd:c8:99:4c:d1:c6:6b:15:8e:d5:49:24:f2:b0:02 (0)\_f4:c4:43:f3:cf:3a:8c:f3:01:37:50:3e:7d:d0:17:0f (0)\_8c:ec:07:60:d4:26:b1:83:7b:1a:9c:23:43:14:4e:17 (0)\_fd:dc:a4:2c:90:d1:07:80:53:ec:e8:6d:ee:be:9a:33 (0)\_5a:40:9d:bd:a7:8d:8b:c7:3e:c3:96:77:3e:b5:65:f0 (0)\_c0:d6:0a:15:14:a7:32:98:ea:76:3c:36:f2:f2:85:08 (0)\_ed:d9:58:f9:57:33:d6:a0:49:0c:5d:e5:72:cf:05:be (0)\_de:a2:1f:45:44:07:39:01:c4:00:94:25:8a:6a:fc:18 (0)\_db:15:87:1e:84:9e:ee:10:2c:89:e3:46:c8:e8:68:37 (0)\_f5:84:17:5d:81:5f:df:9e:0c:68:ec:ac:02:d1:d9:7b:bc (0)\_8b:e7:dd:94:48:01:32:69:92:d1:3f:5a:ae:21:61:c4 (0)\_3f:d4:51:d7:61:5b:c8:1d:8d:f6:dd:2f:24:a9:90:f8 (0)\_5c:fa:bd:b1:b5:dd:94:d4:4e:6a:3d:90:43:bf:4a:ec (0)\_fb:f7:40:7e:ed:b1:63:48:0b:d1:d5:34:0a:38:2e:88 (1)CERTIFICATE\_1 (1)Version 3\_(0x2) (1)Serial\_Number\_4b:a8:52:93:f7:9a:2f:a2:73:06:4b:a8:04:8d:75:d0 (1)Signature\_Algorithm sha256WithRSAEncryption (1)ISSUER\_NAME \_countryName US \_organizationName Internet\_Security\_Research\_Group \_commonName ISRG\_Root\_X1 (1)SUBJECT\_NAME \_countryName US \_organizationName Let's\_Encrypt \_commonName R10 (1)Valid\_From Mar\_13\_00:00:00\_2024\_GMT (1)Valid\_Till Mar\_12\_23:59:59\_2027\_GMT (1)Public\_Key\_Algorithm rsaEncryption (1)RSA\_Public\_Key (2048\_bit) (1)\_RSA\_Public-Key: (2048\_bit) (1)\_Modulus: (1)\_00:c5:57:e5:e6:c4:54:12:ed:b4:47:fe:c9:27:58: (1)\_76:46:50:28:8c:1d:3b:88:df:05:9d:d5:b5:18:29: (1)\_bd:dd:b5:5a:bf:f4:f6:ce:a3:be:af:00:21:4b:62: (1)\_5a:5a:3c:01:2f:c5:58:03:f6:89:ff:8e:11:43:eb: (1)\_c1:b5:e0:14:07:96:8f:6f:1f:d7:e7:ba:81:39:09: (1)\_75:65:b7:c2:af:18:5b:37:26:28:e7:a3:f4:07:2b: (1)\_6d:1a:ff:ab:58:bc:95:ae:40:ff:e9:cb:57:c4:b5: (1)\_5b:7f:78:0d:18:61:bc:17:e7:54:c6:bb:49:91:cd: (1)\_6e:18:d1:80:85:ee:a6:65:36:bc:74:ea:bc:50:4c: (1)\_ea:fc:21:f3:38:16:93:4a:ba:b0:3d:6b:38:06:cd: (1)\_16:12:7a:ca:52:75:c8:ad:76:b2:c2:9c:5d:98:45: (1)\_5c:6f:61:7b:c6:2d:ec:3c:13:52:86:01:d9:57:e6: (1)\_38:1c:df:8d:b5:1f:92:91:9a:e7:4a:1c:cc:45:a8: (1)\_72:55:f0:b0:e6:a3:07:ec:fd:a7:1b:66:9e:3f:48: (1)\_8b:71:84:71:58:c9:3a:fa:ef:5e:f2:5b:44:2b:3c: (1)\_74:e7:8f:b2:47:c1:07:6a:cd:9a:b7:0d:96:f7:12: (1)\_81:26:51:54:0a:ec:61:f6:f7:f5:e2:f2:8a:c8:95: (1)\_0d:8d (1)\_Exponent: 65537\_(0x10001) (1)X509v3\_EXTENSIONS (1)X509v3\_Key\_Usage critical (1)\_Digital\_Signature,\_Certificate\_Sign,\_CRL\_Sign (1)X509v3\_Extended\_Key\_Usage\_TLS\_Web\_Server\_Authentication,\_TLS\_Web\_Client\_Authentication (1)X509v3\_Basic\_Constraints critical (1)\_CA:TRUE,\_pathlen:0 (1)X509v3\_Subject\_Key\_Identifier\_BB:BC:C3:47:A5:E4:BC:A9:C6:C3:A4:72:0C:10:8D:A2:35:E1:C8:E8 (1)X509v3\_Authority\_Key\_Identifier\_keyid:79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E (1)Authority\_Information\_Access\_CA\_Issuers\_-\_URI:http://x1.i.lencr.org/ (1)X509v3\_Certificate\_Policies\_Policy: 2.23.140.1.2.1 (1)X509v3\_CRL\_Distribution\_Points (1)\_Full\_Name: (1)\_URI:http://x1.c.lencr.org/ (1)Signature (512\_octets (1)\_92:b1:e7:41:37:eb:79:9d:81:e6:cd:e2:25:e1:3a:20 (1)\_e9:90:44:95:a3:81:5c:cf:c3:5d:fd:bd:a0:70:d5:b1 (1)\_96:28:22:0b:d2:f2:28:cf:0c:e7:d4:e6:43:8c:24:22 (1)\_1d:c1:42:92:d1:09:af:9f:4b:f4:c8:70:4f:20:16:b1 (1)\_5a:dd:01:f6:1f:f8:1f:61:6b:14:27:b0:72:8d:63:ae (1)\_ee:e2:ce:4b:cf:37:d2:bb:a3:d4:cd:e7:ad:50:ad:bd (1)\_bf:e3:ec:3e:62:36:70:59:31:a7:e8:8d:dd:ea:62:e2 (1)\_12:ae:f5:9c:d4:3d:2c:0c:aa:d0:9c:79:be:ea:3d:5c (1)\_44:6e:96:31:63:5a:7d:d6:7e:4f:24:a0:4b:05:7f:5e (1)\_6f:d2:d4:ea:5f:33:4b:13:d6:57:b6:ca:de:51:b8:5d (1)\_a3:09:82:74:fd:c7:78:9e:b3:b9:ac:16:da:4a:2b:96 (1)\_c3:b6:8b:62:8f:9f:74:19:a2:9e:03:de:e9:6f:9b:b0 (1)\_0f:d2:a0:5a:f6:85:5c:2:04:b7:c8:d5:4e:32:c4:bf (1)\_04:5d:bc:29:f6:f7:81:8f:0c:5d:3c:53:c9:40:90:8b (1)\_fb:b6:08:65:b9:a4:21:d5:09:e5:13:84:84:37:82:ce (1)\_10:28:fc76:c2:06:25:7a:46:52:cd:4a:53:72:a4:27 (1)\_3f:62:70:ac:be:69:48:00:fb:67:0f:db:5b:a1:e8:a7 (1)\_03:21:2d:d7:c9:f6:99:42:39:83:43:df:77:04:12:08 (1)\_1f:25:d6:ba:c9:19:54:18:88:a5:c5:8e:e1:1a:99:93 (1)\_79:6b:ec:1c:f9:31:40:b0:cc:32:00:df:9f:5e:e7:b4 (1)\_92:ab:90:82:91:8d:0d:e0:1e:95:ba:59:3b:2e:4b:5f (1)\_c2:b7:46:35:52:39:06:c0:bd:aa:ac:52:c1:22:a4:d4 (1)\_97:99:f7:0c:a0:21:a7:a1:6c:71:47:16:17:01:68:c0 (1)\_ba:a6:26:65:04:7c:b3:ae:c9:e7:94:55:c2:6f:9b:3c (1)\_1c:a9:f9:2e:c5:20:1a:f0:76:e0:be:ec:18:d6:4f:d8 (1)\_25:bf:76:11:e8:bfe:6:21:0f:e8:8e:cc:b5:b6:a7:5d (1)\_b8:f7:9f:41:cf:61:22:46:6a:83:b6:68:97:2e:7c:ea (1)\_4e:95:db:23:eb:2e:c8:b2:28:84:a4:60:e9:49:f4:44 (1)\_2e:3b:f9:ca:62:57:01:e2:5d:90:16:f9:c9:cf:7a:23 (1)\_48:8e:a6:d5:81:72:f1:28:fa:5d:ce:fb:ed:4e:73:8f (1)\_94:2e:d2:41:94:98:99:db:a7:af:70:5f:f5:be:fb:02 (1)\_20:bf:66:27:6c:b4:af:75:12:0b:2b:3e:ce:03:9e #table cols="2" NAME VALUE (0)CERTIFICATE\_0 (0)Version 3\_(0x2) (1)Serial\_Number\_0c:42:41:4e:e9:87:9a:40:16:50:86:c9:4f:d9:88:c4:b4:21 (1)Signature\_Algorithm sha256WithRSAEncryption (0)ISSUER\_NAME \_countryName US \_organizationName Let's\_Encrypt \_commonName R11 (0)SUBJECT\_NAME \_commonName no-sni.vercel-infra.com (0)Valid\_From Jul\_1\_11:35:33\_2024\_GMT (0)Valid\_Till Sep\_29\_11:35:32\_2024\_GMT (0)Public\_Key\_Algorithm rsaEncryption (0)RSA\_Public\_Key (2048\_bit) (0)\_RSA\_Public-Key: (2048\_bit) (0)\_Modulus: (0)\_00:c1:5c:fb:c5:fb:25:7a:bc:5c:ef:9b:cc:68:45: (0)\_92:7d:ab:82:ba:99:19:f6:b1:eb:c6:6f:7b:95: (0)\_bd:b1:3a:c5:99:1d:dd:a3:24:60:9b:d1:2a:cf:c2: (0)\_bf:95:e7:c3:41:91:7f:d4:26:67:af:46:e4:04:0c: (0)\_2c:81:d7:5f:00:ff:4f:cf:b5:eb:2d:47:75:39:04: (0)\_00:0b:e4:67:35:a8:7a:46:55:46:fe:66:71:7d:37: (0)\_02:92:db:a6:8f:4c:62:b1:06:30:38:33:22:81:0a: (0)\_f4:65:29:ee:96:b6:65:e3:b9:80:ad:9c:e5:42:d7: (0)\_98:3a:d9:45:3a:e7:3d:f1:ef:fd:f5:08:da:ae:c1: (0)\_69:bd:a3:24:b0:31:bf:6c:e2:77:34:38:50:ef:f8: (0)\_5d:54:19:3b:67:43:75:3c:ff:b4:7a:71: (0)\_6d:d3:8d:c3:61:26:e3:03:f9:ed:0d:d3:79:27:8d: (0)\_12:40:dd:d8:15:a0:85:06:92:db:05:a3:e2:46:4c: (0)\_c6:98:fd:4b:68:1f:45:e0:c1:94:85:57:33:b4:99: (0)\_c1:83:fc:e4:63:09:38:84:1d:6e:c7:12:40:54:d0: (0)\_8d:4a:f9:f4:26:5f:0f:86:17:44:4a:1c:05:af:f6: (0)\_ee:03:a9:42:a3:0f:4f:8f:54:81:d4:ab:cd:9d:8b: (0)\_13:7b (0)\_Exponent: 65537\_(0x10001) (0)X509v3\_EXTENSIONS (0)X509v3\_Key\_Usage critical (0)\_Digital\_Signature,\_Key\_Encipherment (0)X509v3\_Extended\_Key\_Usage\_TLS\_Web\_Server\_Authentication,\_TLS\_Web\_Client\_Authentication (0)X509v3\_Basic\_Constraints critical (0)\_CA:FALSE (0)X509v3\_Subject\_Key\_Identifier\_93:B8:6B:A9:64:4A:2E:68:C8:2B:37:AC:A0:3C:6B:5F:C6:A7:73:01 (0)X509v3\_Authority\_Key\_Identifier\_keyid:C5:CF:46:A4:EA:F4:C3:C0:7A:6C:95:C4:2D:B0:5E:92:2F:26:E3:B9 (0)Authority\_Information\_Access\_OCSP\_-\_URI:http://r11.o.lencr.org/ (0)\_CA\_Issuers\_-\_URI:http://r11.i.lencr.org/ (0)X509v3\_Subject\_Alternative\_Name\_DNS:no-sni.vercel-infra.com (0)X509v3\_Certificate\_Policies\_Policy: 2.23.140.1.2.1 (0)CT\_Precertificate\_SCTs\_Signed\_Certificate\_Timestamp: (0)\_Version:\_v1\_(0x0) (0)\_Log\_ID:\_19:98:10:71:09:F0:D6:52:2E:30:80:D2:9E:3F:64:BB: (0)\_83:6f28:CF:F9:0F:52:8E:EE:DF:CE:4A:3F:16:B4:CA (0)\_Timestamp:\_Jul\_1\_12:35:33.763\_2024\_GMT (0)\_Extensions:\_none (0)\_Signature:\_ecdsa-with-SHA256 (0)\_30:45:02:21:00:81:A2:8E:09:08:18:FA:92:AB:22:74: (0)\_C2:EB:FF:3C:32:96:C7:AE:17:3D:E1:D9:74:B7:48:9F: (0)\_64:56:7F:77:C1:02:20:1E:7F:85:FC:28:2D:60:92:B5: (0)\_7D:4B:1E:47:CE:49:66:57:AB:03:B2:C8:D3:E2:66:9E: (0)\_25:66:0b:58:7C:35:69 (0)\_Signed\_Certificate\_Timestamp: (0)\_Version:\_v1\_(0x0) (0)\_Log\_ID:\_48:B0:E3:6B:DA:A6:47:34:0F:E5:6A:02:FA:9D:30:B6: (0)\_1C:52:01:CB:56:DD:3C:81:D9:BB:FB:AB:39:D8:84:73 (0)\_Timestamp:\_Jul\_1\_12:35:33.763\_2024\_GMT (0)\_Extensions:\_none (0)\_Signature:\_ecdsa-with-SHA256 (0)\_30:45:02:20:05:7E:4D:45:48:C8:9D:7C:1D:79:98:87: (0)\_63:CA:A0:C6:EF:46:B8:12:14:09:5E:A2:ED:C6:0A:F3: (0)\_30:BF:CB:DF:02:21:00:AE:0F:DA:2B:DC:22:FC:5E:EC: (0)\_7F:71:0D:BA:94:AF:25:B9:56:04:A5:07:3D:65:D6:7D: (0)\_A9:DB:D6:76:A9:99:8B (0)Signature (256\_octets) (0)\_7a:a2:7d:b7:6f:a3:5d:ae:63:3a:1d:bd:bf:3:89:99 (0)\_83:30:29:88:f6:d2:829:60:5c:19:4e:51:f8:67:dc (0)\_f2:a0:5c:4b:d2:f0:e1:5b:28:82:86:f4:07:fe:4b:d2 (0)\_65:7d:ba:95:26:e7:95:44:f2:23:bc:0b:43:32:8f:44 (0)\_33:6d:26:4f:4c:b4:f7:a9:12:c3:89:80:b2:0c:3d:f7 (0)\_64:b8:22:6f:76:63:62:79:5b:3c:57:62:4f:b4:ed:31 (0)\_37:b4:2a:c7:cb:03:a6:e1:0f:2d:91:5a:bd:18:cc:f4 (0)\_51:c8:30:dd:d1:ed:22a:ae:78:67:3f:c7:a0:1a:08 (0)\_59:08:d7:0d:c0:b7:ef:02:26:ce:78:5b:03:47:2f:cc (0)\_39:70:1b:a4:2d:36:40:c2:1e:17:f4:10:6b:e2:8d:7e:3 (0)\_bb:c9:bf:df:26:24:ae:99:54:05:86:a3:9e:c5:c6:dd (0)\_9c:e8:d2:5d:39:08:2f:9a:0e:bb:6d:51:e9:a7:d7:17 (0)\_90:2c:5d:ca:36:41:bd:aa:9d:a5:c3:94:9e:00:92:f2 (0)\_94:92:04:ed:9e:5b:b8:14:ec:c3:75:af:a4:e9:14:f8 (0)\_46:03:e4:e8:1c:d9:4e:09:32:b3:15:5a:33:e6:c9:48 (0)\_ec:31:58:d4:67:ae:af:bd:6f:5a:41:a1:5f:6d:2d:26 (1)CERTIFICATE\_1\_1 (1)Version 3\_(0x2) (1)Serial\_Number\_8a:7d:3e:13:d6:2f:30:ef:23:86:bd:29:07:6b:34:f8 (1)Signature\_Algorithm sha256WithRSAEncryption (1)ISSUER\_NAME \_countryName US \_organizationName Internet\_Security\_Research\_Group \_commonName ISRG\_Root\_X1 (1)SUBJECT\_NAME \_countryName US \_organizationName Let's\_Encrypt \_commonName R11 (1)Valid\_From Mar\_13\_00:00:00\_2024\_GMT (1)Valid\_Till Mar\_12\_23:59:59\_2027\_GMT (1)Public\_Key\_Algorithm rsaEncryption (1)RSA\_Public\_Key (2048\_bit) (1)\_RSA\_Public-Key: (2048\_bit) (1)\_Modulus: (1)\_00:ba:87:bc:5c:1b:00:39:cb:ca:

0a:cd:d4:67:10: (1) \_f9:01:3c:a5:4e:a5:61:cb:26:ca:52:fb:15:01:b7: (1) \_b9:28:f5:28:1e:ed:27:b3:24:18:39:67:09:0c:08: (1) \_ec:e0:3a:b0:3b:77:0e:bd:f3:e5:39:54:41:0c:4e: (1) \_ae:41:d6:99:74:de:51:db:ef:7b:ff:58:bd:a8:b7: (1) \_13:f6:de:31:d5:f2:72:c9:72:6a:0b:83:74:95:9c: (1) \_46:00:64:14:99:f3:b1:d9:22:d9:cd:a8:92:aa:1c: (1) \_26:7a:3f:fe:ef:58:05:7b:08:95:81:db:71:0f:8e: (1) \_fb:e3:31:09:bb:09:be:50:4d:5f:8f:91:76:3d:5a: (1) \_9d:9e:83:f2:e9:c4:66:b3:e1:06:66:43:48:18:80: (1) \_65:a0:37:18:9a:9b:84:32:97:b1:b2:bd:c4:f8:15: (1) \_00:9d:27:88:fb:e2:63:17:96:6c:9b:27:67:4b:c4: (1) \_db:28:5e:69:c2:79:f0:49:5c:e0:24:50:e1:c4:bc: (1) \_a1:05:ac:7b:40:6d:00:b4:c2:41:3f:a7:58:b8:2f: (1) \_c5:5c:9b:a5:bb:09:9e:f1:fe:eb:b0:85:39:fd:a8: (1) \_0a:ef:45:c4:78:eb:65:2a:c2:cf:5f:3c:de:e3:5c: (1) \_4d:1b:f7:0b:27:2b:aa:0b:42:77:53:4f:79:6a:1d: (1) \_87:d9 (1) \_Exponent:\_65537\_(0x10001) (1)X509v3\_EXTENSIONS \_ (1)X509v3\_Key\_Usage critical (1)\_Digital\_Signature,\_Certificate\_Sign,\_CRL\_Sign (1)X509v3\_Extended\_Key\_Usage \_TLS\_Web\_Client\_Authentication,\_TLS\_Web\_Server\_Authentication (1)X509v3\_Basic\_Constraints critical (1)\_CA:TRUE,\_pathlen:0 (1)X509v3\_Subject\_Key\_Identifier \_C5:CF:46:A4:EA:F4:C3:C0:7A:6C:95:C4:2D:B0:5E:92:2F:26:E3:B9 (1)X509v3\_Authority\_Key\_Identifier \_keyid: 79:B4:59:E6:7B:B6:E5:E4:01:73:80:08:88:C8:1A:58:F6:E9:9B:6E (1)Authority\_Information\_Access \_CA\_Issuers - \_URI:http://x1.i.lencr.org/ (1)X509v3\_Certificate\_Policies \_Policy: \_2.23.140.1.2.1 (1)X509v3\_CRL\_Distribution\_Points (1)\_Full\_Name: (1)\_URI:http://x1.c.lencr.org/ (1)Signature (512\_octet) (1) 4e:e2:89:5d:0a:03:1c:90:38:d0:f5:1f:f9:71:5c:f8 (1) c3:8f:b2:37:88:7a:6f:b0:25:1f:ed:be:b7:d8:86:06 (1) 8e:e9:09:84:cd:72:bf:81:f3:fc:ca:cf:53:48:ed:bd (1) f6:69:42:d4:a5:11:3e:35:c8:13:b2:92:1d:05:5f:ea (1) 2e:d4:d8:f8:49:c3:ad:f5:99:96:9c:ef:26:d8:e1:b4 (1) 24:0b:48:20:4d:fc:d3:54:b4:a9:c6:21:c8:e1:36:1b (1) ff:77:64:29:17:b9:f0:4b:ef:5d:ea:cd:79:d0:bf:90 (1) bf:be:23:b2:90:da:4a:a9:48:31:74:a9:44:0b:e1:e2 (1) f6:2d:83:71:a4:75:7b:d2:94:c1:05:19:46:1c:b9:8f (1) f3:c4:74:48:25:2a:0d:e5:f5:db:43:e2:db:93:9b:b9 (1) 19:b4:1f:2f:df:6a:0e:8f:31:d3:63:0f:bb:29:dc:dd (1) 66:2c:3f:b0:1b:67:51:f8:41:3c:e4:4d:b9:ac:b8:a4 (1) 9c:66:63:f5:ab:85:23:1d:cc:53:b6:ab:71:ae:dc:c5 (1) 01:71:da:36:ee:0a:18:2a:32:fd:09:31:7c:8f:6:73 (1) e7:9c:9c:b5:4a:15:6a:77:82:5a:cf:da:8d:45:fe:1f (1) 2a:64:05:30:3e:73:c2:c6:0c:b9:d6:3b:63:4a:ab:46 (1) 03:fe:99:c0:46:40:27:60:63:df:50:3a:07:47:d8:15 (1) 4a:9f:ea:47:1f:99:5a:08:62:0c:b6:6c:33:08:4d:d7 (1) 38:ed:48:2d:2e:05:68:ae:80:5d:ef:4c:dc:d8:20:41 (1) 5f:68:f1:bb:5a:cd:e3:0e:b0:0c:31:87:9b:43:de:49 (1) 43:e1:c8:04:3f:d1:3c:1b:87:45:30:69:a8:a9:72:0e (1) 79:12:1c:31:d8:3e:23:57:dd:a7:4f:a0:f0:1c:81:d1 (1) 77:1f:6f:d6:d2:b9:a8:b3:03:16:81:39:4b:9f:55:ae (1) d2:6a:e4:b3:bf:ea:a5:d5:9f:4b:a3:c9:d6:3b:72:f3 (1) 4a:f6:54:ab:0c:f3:8f:70:80:df:6e:35:ca:75:a1 (1) 54:e4:2f:bc:6e:17:c9:1a:a5:37:b5:a2:9a:ba:ec:f4 (1) c0:75:46:4f:77:a8:e8:59:56:91:66:2d:6e:de:29:81 (1) d6:a6:97:05:5e:64:45:b2:c:ce:ea:64:42:44:b0:c3 (1) 4f:ad:f0:b4:dc:03:ca:99:9b:09:82:95:82:0d:63:8a (1) 66:f9:19:72:f8:d5:b9:89:10:e2:89:98:09:35:f9:a2 (1) 1c:be:92:73:23:74:e9:9d:1f:d7 4a:9a:84:58:10 (1) c2:f3:a7:e2:35:ec:7e:3b:45:ce:30:46:52:6b:c0:c0


Info List

Info #1

Certificate Fingerprint:591E9CE6C863D3A079E9FABE1478C7339A26B21269DDE795211361024AE31A44

Security Weaknesses (12)

 150261 Subresource Integrity (SRI) Not Implemented (1)

 150261 Subresource Integrity (SRI) Not Implemented

Develop

Finding #	12630741	Severity	Information Gathered - Level 3
Unique #	4d5697c7-99a8-4ef9-a371-12a5e1cf5e1d		
Group	Security Weaknesses		
CWE	CWE-693	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	A1 Broken Access Control		
WASC	-		

Details

Threat

The integrity attribute is missing in script and/or link elements. Subresource Integrity (SRI) is a standard browser security feature that verifies the value of the integrity attribute in

Impact

Absence of SRI checks means it is impossible to verify that the third-party resources are delivered without any unexpected manipulation.

Solution

All script and link elements that load external content should include the integrity attribute to ensure that the content is trustworthy.

More information:  
[Subresource Integrity article by Mozilla](#)  
[OWASP Third-Party JavaScript Management Cheat Sheet](#)

Results

# WAS Web Application Report

Externally loaded Javascript and CSS resources without integrity checks:

Parent link : <https://www.developom.com/>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/?email=was@qualys.com>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/videos>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/articles>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/products>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/use-cases>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/contact>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/articles/clggsudoa0008xl0upm0wtbq2>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/articles/clj7q6qea0004y00uy6syet33>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/videos/clo1rphds0003xq4awxl4qvpp>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/videos/clj7rv3ax000yy00u0qzsta2h>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/videos/clnvzzq2z0002t6440a247c7g>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/videos/clog0nmcb0000ye44vyj7j6vz>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/videos/clnyph7xn0000ts45l2pnq07m>  
Found following resource links without integrity checks (only first 10 links are reported)  
<https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap>  
<https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK>

Parent link : <https://www.developom.com/terms>  
Found following resource links without integrity checks (only first 10 links are reported)



https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap  
https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK

Parent link : https://www.develom.com/privacy  
Found following resource links without integrity checks (only first 10 links are reported)  
https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap  
https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK

Parent link : https://www.develom.com/about-us  
Found following resource links without integrity checks (only first 10 links are reported)  
https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap  
https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK

Parent link : https://www.develom.com/?email=was@qualys.com  
Found following resource links without integrity checks (only first 10 links are reported)  
https://fonts.googleapis.com/css2?family=Montserrat:ital,wght@0,100;0,200;0,300;0,400;0,500;0,600;0,700;0,800;0,900;1,100;1,200;1,300;1,400;1,500;1,600;1,700;1,800;1,900&display=swap  
https://www.googletagmanager.com/gtag/js?id=G-8TXQH76GDK  
Please check there may be more pages with subresource links without integrity checks.

150202 Missing header: X-Content-Type-Options (1)				Development
150202 Missing header: X-Content-Type-Options				
Finding #	12630743	Severity	Information Gathered - Level 2	
Unique #	960d74d9-840d-4fcf-8a6c-b4834757ada7			
Group	Security Weaknesses			
CWE	CWE-16, CWE-1032	Detection Date	18 Jul 2024 12:41 GMT-0800	
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://www.develom.com/ response code: 200  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::9b7b7-1721331733156-f5f97b74a366  
  
Header missing on the following link(s):  
(Only first 50 such pages are listed)  
  
GET https://www.develom.com/ response code: 200  
GET https://www.develom.com/?email=was@qualys.com response code: 200  
GET https://www.develom.com/logo\_gradient.svg response code: 200  
GET https://www.develom.com/\_astro/about-us.5894b19d.css response code: 200  
GET https://www.develom.com/\_astro/team.2544d23c.css response code: 200



GET https://www.develop.com/videos response code: 200  
GET https://www.develop.com/articles response code: 200  
GET https://www.develop.com/products response code: 200  
GET https://www.develop.com/use-cases response code: 200  
GET https://www.develop.com/contact response code: 200  
GET https://www.develop.com/articles/clggsudoa0008xl0upm0wtbq2 response code: 200  
GET https://www.develop.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 response code: 200  
GET https://www.develop.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence response code: 200  
GET https://www.develop.com/articles/clj7q6qea0004y00uy6syet33 response code: 200  
GET https://www.develop.com/videos/clo1rphds0003xq4awxl4qvpp response code: 200  
GET https://www.develop.com/videos/clj7rv3ax000yy00u0qzsta2h response code: 200  
GET https://www.develop.com/videos/clnvzzq2z0002t6440a247c7g response code: 200  
GET https://www.develop.com/videos/clog0nmc0000ye44vyj7j6vz response code: 200  
GET https://www.develop.com/videos/clnyph7xn0000ts45l2pnq07m response code: 200  
GET https://www.develop.com/~partytown/ response code: 404  
GET https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721331739362 response code: 200  
GET https://www.develop.com/terms response code: 200  
GET https://www.develop.com/privacy response code: 200  
GET https://www.develop.com/\_astro/ChatBubble.03a86e9a.js response code: 200  
GET https://www.develop.com/about-us response code: 200  
GET https://www.develop.com/\_astro/DevelopApolloProvider.0fe78ec8.js response code: 200  
GET https://www.develop.com/\_astro/Footer.979b54a3.js response code: 200  
GET https://www.develop.com/\_astro/GradientComponent.b189efbc.js response code: 200  
GET https://www.develop.com/\_astro/HeroBannerLandingPage.82365e97.js response code: 200  
GET https://www.develop.com/\_astro/NavBar.be2d4950.js response code: 200  
GET https://www.develop.com/\_astro/axios.8a9713b4.js response code: 200  
GET https://www.develop.com/\_astro/client.e04c411a.js response code: 200  
GET https://www.develop.com/\_astro/clsx.m.1229b3e0.js response code: 200  
GET https://www.develop.com/\_astro/index.0f268f1b.js response code: 200  
GET https://www.develop.com/\_astro/index.c30e9e06.js response code: 200  
GET https://www.develop.com/\_astro/jsx-runtime.4e6dfa6a.js response code: 200  
GET https://www.develop.com/\_astro/keyboard.be908299.js response code: 200  
GET https://www.develop.com/\_astro/transition.0053f6cc.js response code: 200  
GET https://www.develop.com/hero\_banner/Hero\_banner\_1728.webp response code: 200  
GET https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721331724174 response code: 200  
GET https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721331759497 response code: 200  
GET https://www.develop.com/favicon.ico response code: 404  
GET https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721331778695 response code: 200  
GET https://www.develop.com/\_astro/NavBar.9431a621.js response code: 200  
GET https://www.develop.com/\_astro/PlayCircleIcon.5bf2f150.js response code: 200  
GET https://www.develop.com/\_astro/ShareModal.ca6fd24c.js response code: 200  
GET https://www.develop.com/\_astro/Videos.45a29a33.js response code: 200  
GET https://www.develop.com/articles/clj7r43ye000wy00uvzgvyd7 response code: 200  
GET https://www.develop.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses response code: 200  
GET https://www.develop.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds response code: 200

150206 Content-Security-Policy Not Implemented (1)



150206 Content-Security-Policy Not Implemented

Develop

Finding #	12630746	Severity	Information Gathered - Level 2
Unique #	7581c242-ba6c-4fa0-82a1-1337c17cf3cd		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	Detection Date	18 Jul 2024 12:41 GMT-0800
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

# WAS Web Application Report

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://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://www.developom.com/ response code: 200  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfol::iad1::9btb7-1721331733156-f5f97b74a366

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

GET https://www.developom.com/ response code: 200  
GET https://www.developom.com/?email=was@qualys.com response code: 200  
GET https://www.developom.com/logo\_gradient.svg response code: 200  
GET https://www.developom.com/\_astro/about-us.5894b19d.css response code: 200  
GET https://www.developom.com/\_astro/team.2544d23c.css response code: 200  
GET https://www.developom.com/videos response code: 200  
GET https://www.developom.com/articles response code: 200  
GET https://www.developom.com/products response code: 200  
GET https://www.developom.com/use-cases response code: 200  
GET https://www.developom.com/contact response code: 200  
GET https://www.developom.com/articles/clggsudoa0008x10upm0wtbq2 response code: 200  
GET https://www.developom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 response code: 200  
GET https://www.developom.com/articles/clj7r3ax000yy00u0qzsta2h response code: 200  
GET https://www.developom.com/articles/clj7q6qea0004y00uy6syet33 response code: 200  
GET https://www.developom.com/videos/clo1rphds0003xq4awxl4qvpp response code: 200  
GET https://www.developom.com/videos/clj7rv3ax000yy00u0qzsta2h response code: 200  
GET https://www.developom.com/videos/clnvzzq2z0002t6440a247c7g response code: 200  
GET https://www.developom.com/videos/clog0nmc0000ye44vyj7j6vz response code: 200  
GET https://www.developom.com/videos/clnyph7xn0000ts45l2pnq07m response code: 200  
GET https://www.developom.com/~partytown/ response code: 404  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331739362 response code: 200  
GET https://www.developom.com/terms response code: 200  
GET https://www.developom.com/privacy response code: 200  
GET https://www.developom.com/\_astro/ChatBubble.03a86e9a.js response code: 200  
GET https://www.developom.com/about-us response code: 200  
GET https://www.developom.com/\_astro/DevelopomApolloProvider.0fe78ec8.js response code: 200  
GET https://www.developom.com/\_astro/Footer.979b54a3.js response code: 200  
GET https://www.developom.com/\_astro/GradientComponent.b189efbc.js response code: 200  
GET https://www.developom.com/\_astro/HeroBannerLandingPage.82365e97.js response code: 200  
GET https://www.developom.com/\_astro/NavBar.be2d4950.js response code: 200  
GET https://www.developom.com/\_astro/axios.8a9713b4.js response code: 200  
GET https://www.developom.com/\_astro/client.e04c411a.js response code: 200  
GET https://www.developom.com/\_astro/clsx.m.1229b3e0.js response code: 200  
GET https://www.developom.com/\_astro/index.0f268f1b.js response code: 200  
GET https://www.developom.com/\_astro/index.c30e9e06.js response code: 200  
GET https://www.developom.com/\_astro/jsx-runtime.4e6dfa6a.js response code: 200  
GET https://www.developom.com/\_astro/keyboard.be908299.js response code: 200  
GET https://www.developom.com/\_astro/transition.0053f6cc.js response code: 200  
GET https://www.developom.com/hero\_banner/Hero\_banner\_1728.webp response code: 200  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331724174 response code: 200  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331759497 response code: 200  
GET https://www.developom.com/favicon.ico response code: 404  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331778695 response code: 200

GET https://www.developom.com/\_astro/NavBar.9431a621.js response code: 200  
GET https://www.developom.com/\_astro/PlayCircleIcon.5bf2f150.js response code: 200  
GET https://www.developom.com/\_astro/ShareModal.ca6fd24c.js response code: 200  
GET https://www.developom.com/\_astro/Videos.45a29a33.js response code: 200  
GET https://www.developom.com/articles/clj7r43ye000wy00uvzgvyd7 response code: 200  
GET https://www.developom.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses response code: 200  
GET https://www.developom.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds response code: 200

150208 Missing header: Referrer-Policy (1)

150208 Missing header: Referrer-Policy

Developom

Finding #	12630721	Severity	Information Gathered - Level 2
Unique #	6d7f4706-7764-4e7e-b502-194f861f8a11		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	Detection Date	18 Jul 2024 12:41 GMT-0800
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://www.developom.com/ response code: 200  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::9btb7-1721331733156-f5f97b74a366

# WAS Web Application Report

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

GET https://www.develom.com/ response code: 200  
GET https://www.develom.com/?email=was@qualys.com response code: 200  
GET https://www.develom.com/logo\_gradient.svg response code: 200  
GET https://www.develom.com/\_astro/about-us.5894b19d.css response code: 200  
GET https://www.develom.com/\_astro/team.2544d23c.css response code: 200  
GET https://www.develom.com/videos response code: 200  
GET https://www.develom.com/articles response code: 200  
GET https://www.develom.com/products response code: 200  
GET https://www.develom.com/use-cases response code: 200  
GET https://www.develom.com/contact response code: 200  
GET https://www.develom.com/articles/clggsudoa0008xl0upm0wtbq2 response code: 200  
GET https://www.develom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 response code: 200  
GET https://www.develom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence response code: 200  
GET https://www.develom.com/articles/clj7q6qea0004y00uy6syet33 response code: 200  
GET https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp response code: 200  
GET https://www.develom.com/videos/clj7rv3ax000yy00u0qzsta2h response code: 200  
GET https://www.develom.com/videos/clnvzzq2z0002t6440a247c7g response code: 200  
GET https://www.develom.com/videos/clog0nmcb0000ye44vyj7j6vz response code: 200  
GET https://www.develom.com/videos/clnyph7xn0000ts45l2pnq07m response code: 200  
GET https://www.develom.com/~partytown/ response code: 404  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331739362 response code: 200  
GET https://www.develom.com/terms response code: 200  
GET https://www.develom.com/privacy response code: 200  
GET https://www.develom.com/\_astro/ChatBubble.03a86e9a.js response code: 200  
GET https://www.develom.com/about-us response code: 200  
GET https://www.develom.com/\_astro/DevelomApolloProvider.0fe78ec8.js response code: 200  
GET https://www.develom.com/\_astro/Footer.979b54a3.js response code: 200  
GET https://www.develom.com/\_astro/GradientComponent.b189efbc.js response code: 200  
GET https://www.develom.com/\_astro/HeroBannerLandingPage.82365e97.js response code: 200  
GET https://www.develom.com/\_astro/NavBar.be2d4950.js response code: 200  
GET https://www.develom.com/\_astro/axios.8a9713b4.js response code: 200  
GET https://www.develom.com/\_astro/client.e04c411a.js response code: 200  
GET https://www.develom.com/\_astro/clsx.m.1229b3e0.js response code: 200  
GET https://www.develom.com/\_astro/index.0f268f1b.js response code: 200  
GET https://www.develom.com/\_astro/index.c30e9e06.js response code: 200  
GET https://www.develom.com/\_astro/jsx-runtime.4e6dfa6a.js response code: 200  
GET https://www.develom.com/\_astro/keyboard.be908299.js response code: 200  
GET https://www.develom.com/\_astro/transition.0053f6cc.js response code: 200  
GET https://www.develom.com/hero\_banner/Hero\_banner\_1728.webp response code: 200  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331724174 response code: 200  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331759497 response code: 200  
GET https://www.develom.com/favicon.ico response code: 404  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331778695 response code: 200  
GET https://www.develom.com/\_astro/NavBar.9431a621.js response code: 200  
GET https://www.develom.com/\_astro/PlayCircleIcon.5bf2f150.js response code: 200  
GET https://www.develom.com/\_astro/ShareModal.ca6fd24c.js response code: 200  
GET https://www.develom.com/\_astro/Videos.45a29a33.js response code: 200  
GET https://www.develom.com/articles/clj7r43ye000wy00uvzgvyd7 response code: 200  
GET https://www.develom.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses response code: 200  
GET https://www.develom.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds response code: 200

## 150248 Missing header: Permissions-Policy (1)

### 150248 Missing header: Permissions-Policy Develom

Finding #	12630736	Severity	Information Gathered - Level 2
Unique #	327d47e0-df8d-4565-8d83-b6bdfad82afe		
Group	Security Weaknesses		
CWE	CWE-284	Detection Date	18 Jul 2024 12:41 GMT-0800
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://www.developom.com/ response code: 200  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::9btb7-1721331733156-f5f97b74a366

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

GET https://www.developom.com/ response code: 200  
GET https://www.developom.com/?email=was@qualys.com response code: 200  
GET https://www.developom.com/logo\_gradient.svg response code: 200  
GET https://www.developom.com/\_astro/about-us.5894b19d.css response code: 200  
GET https://www.developom.com/\_astro/team.2544d23c.css response code: 200  
GET https://www.developom.com/videos response code: 200  
GET https://www.developom.com/articles response code: 200  
GET https://www.developom.com/products response code: 200  
GET https://www.developom.com/use-cases response code: 200  
GET https://www.developom.com/contact response code: 200  
GET https://www.developom.com/articles/clggsudoa0008xl0upm0wtbq2 response code: 200  
GET https://www.developom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 response code: 200  
GET https://www.developom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence response code: 200  
GET https://www.developom.com/articles/clj7q6qea0004y00uy6syet33 response code: 200  
GET https://www.developom.com/videos/clo1rphds0003xq4awxl4qvpp response code: 200  
GET https://www.developom.com/videos/clj7rv3ax000yy00u0qzsta2h response code: 200  
GET https://www.developom.com/videos/clnvzzq2z0002t6440a247c7g response code: 200  
GET https://www.developom.com/videos/clog0nmcb0000ye44vyj7j6vz response code: 200  
GET https://www.developom.com/videos/clnyph7xn0000ts45l2pnq07m response code: 200  
GET https://www.developom.com/~partytown/ response code: 404  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331739362 response code: 200  
GET https://www.developom.com/terms response code: 200  
GET https://www.developom.com/privacy response code: 200  
GET https://www.developom.com/\_astro/ChatBubble.03a86e9a.js response code: 200  
GET https://www.developom.com/about-us response code: 200  
GET https://www.developom.com/\_astro/DevelopomApolloProvider.0fe78ec8.js response code: 200  
GET https://www.developom.com/\_astro/Footer.979b54a3.js response code: 200  
GET https://www.developom.com/\_astro/GradientComponent.b189efbc.js response code: 200  
GET https://www.developom.com/\_astro/HeroBannerLandingPage.82365e97.js response code: 200  
GET https://www.developom.com/\_astro/NavBar.be2d4950.js response code: 200  
GET https://www.developom.com/\_astro/axios.8a9713b4.js response code: 200  
GET https://www.developom.com/\_astro/client.e04c411a.js response code: 200  
GET https://www.developom.com/\_astro/clsx.m.1229b3e0.js response code: 200  
GET https://www.developom.com/\_astro/index.0f268f1b.js response code: 200  
GET https://www.developom.com/\_astro/index.c30e9e06.js response code: 200  
GET https://www.developom.com/\_astro/jsx-runtime.4e6dfa6a.js response code: 200  
GET https://www.developom.com/\_astro/keyboard.be908299.js response code: 200  
GET https://www.developom.com/\_astro/transition.0053f6cc.js response code: 200  
GET https://www.developom.com/hero\_banner/Hero\_banner\_1728.webp response code: 200  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331724174 response code: 200  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331759497 response code: 200  
GET https://www.developom.com/favicon.ico response code: 404  
GET https://www.developom.com/~partytown/partytown-sandbox-sw.html?1721331778695 response code: 200  
GET https://www.developom.com/\_astro/NavBar.9431a621.js response code: 200  
GET https://www.developom.com/\_astro/PlayCircleIcon.5bf2f150.js response code: 200

GET https://www.develop.com/\_astro/ShareModal.ca6fd24c.js response code: 200  
GET https://www.develop.com/\_astro/Videos.45a29a33.js response code: 200  
GET https://www.develop.com/articles/clj7r43ye000wy00uvzgvyd7 response code: 200  
GET https://www.develop.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses response code: 200  
GET https://www.develop.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds response code: 200

150249 Misconfigured Header: Cache-Control (1)

150249 Misconfigured Header: Cache-Control

Develop

Finding #	12630737	Severity	Information Gathered - Level 2
Unique #	8e391c08-51fe-459a-978b-a6e4a2ce2ea0		
Group	Security Weaknesses		
CWE	CWE-525	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

**Threat**  
Cache-Control header present but directives may not configured to adequately safeguard sensitive information.

For Example:  
Cache-Control directive set to public.

max-age value is greater than 86400.

**Impact**  
If directive is set to public, the resource can be stored by any cache.

If max-age value is greater than 86400 for sensitive information may lead to information leakage.

**Solution**  
Please check that resources with sensitive information are not configured with Cache-Control public directive.

Also please make sure that max-age directive value set properly to not cache sensitive information for longer period than needed.

References:  
[Mozilla Documentation Cache-Control](#)

Results

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develop.com/ response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develop.com/?email=was@qualys.com response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develop.com/logo\_gradient.svg response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develop.com/\_astro/about-us.5894b19d.css response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develop.com/\_astro/team.2544d23c.css response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develop.com/videos response code: 200



# WAS Web Application Report

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/articles response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/products response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/use-cases response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/contact response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/articles/clggsudoa0008xl0upm0wtbq2 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/contact?  
firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence  
response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/articles/clj7q6qea0004y00uy6syet33 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/videos/clo1rphds0003xq4awxl4qvpp response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/videos/clj7rv3ax000yy00u0qzsta2h response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/videos/clnvzzq2z0002t6440a247c7g response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/videos/clog0nmcb0000ye44vyj7j6vz response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/videos/clnyph7xn0000ts4512pnq07m response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/~partytown/ response code: 404

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/terms response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/privacy response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/ChatBubble.03a86e9a.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/about-us response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/DevelopApolloProvider.0fe78ec8.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/Footer.979b54a3.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/GradientComponent.b189efbc.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/HeroBannerLandingPage.82365e97.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/NavBar.be2d4950.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/axios.8a9713b4.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/client.e04c411a.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/clsx.m.1229b3e0.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.developom.com/\_astro/index.0f268f1b.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.

# WAS Web Application Report

Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/index.c30e9e06.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/jsx-runtime.4e6dfa6a.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/keyboard.be908299.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/transition.0053f6cc.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/hero\_banner/Hero\_banner\_1728.webp response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/favicon.ico response code: 404

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/NavBar.9431a621.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/PlayCircleIcon.5bf2f150.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/ShareModal.ca6fd24c.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/\_astro/Videos.45a29a33.js response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/clj7r43ye000wy00uvzgvvyd7 response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/ai-just-got-more-amazing-discover-openai-s-latest-user-friendly-innovations response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/from-healthcare-to-finance-real-life-ai-use-cases-that-inspire response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/clj7qx5td000my00uqwm5wtlk response code: 200

Cache-Control: Header misconfigured. Cache-Control public directive found.  
Cache-Control:public, max-age=0, must-revalidate on the link: GET https://www.develom.com/articles/unlocking-success-ai-readiness-for-genai-are-you-ready response code: 200

150101 Third-party Cookies Collected (1)

150101 Third-party Cookies Collected

Develom

Finding #	12630729	Severity	Information Gathered - Level 1
Unique #	a98cc4c1-72da-47e2-aa60-934600b38969		
Group	Security Weaknesses		
CWE	-	Detection Date	18 Jul 2024 12:41 GMT-0800
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

NID=516=CA2REObNiPB9LJwvela1gOq9nBM0k4UcTd8sELfxVmkBo8b4SsKA2v1tAkcl\_iNYQliHakAXTL\_T8KMdN\_Rlk6XkniJ1eDEk8XDqU9AZaYDUuzxitQSwj6DNyfKPdfQ6R9iEh8fMdA7y  
cpo1S-XTUbS87KS2Pc; secure; HttpOnly; expires=Fri, 17-Jan-2025 19:44:00 GMT; domain=.google.com; path=/ First set at URL: https://www.develop.com/videos/clo1rphds0003xq4awxl4qvpp

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured (1)

Develop

150135 HTTP Strict Transport Security (HSTS) header missing or misconfigured

Finding #	12630740	Severity	Information Gathered - Level 1
Unique #	039a4aa3-626f-4408-8533-ba4eb50445b8		
Group	Security Weaknesses		
CWE	CWE-523	Detection Date	18 Jul 2024 12:41 GMT-0800
OWASP	A5 Security Misconfiguration		
WASC	-		

Details

Threat

HTTP Strict Transport Security (HSTS) header was found to be missing or misconfigured. The HSTS header instructs browsers that all subsequent connections to the website, for a configurable amount of time, should be performed over a secure (HTTPS) connection only. Additionally, it instructs browsers that users should not be permitted to bypass SSL/TLS certificate errors, in the event of an expired or otherwise untrusted certificate for example.

Impact

If HSTS header is not set, users are potentially vulnerable to man-in-the-middle (MITM) attacks, SSL stripping, and passive eavesdropper attacks.

Solution

For information about how to implement the HSTS header properly, refer to the [OWASP HTTP Strict Transport Security Cheat Sheet](#).

Results

Strict Transport Security header missing for  
<https://www.develop.com/~partytown/partytown-sandbox-sw.html?1721331724174>

150142 Virtual Host Discovered (1)

Develop

150142 Virtual Host Discovered

Finding #	12630745	Severity	Information Gathered - Level 1
Unique #	643df05d-7097-400f-9f0b-ce204ebde569		
Group	Security Weaknesses		
CWE	CWE-200	Detection Date	18 Jul 2024 12:41 GMT-0800
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: HTTP Response code  
Virtual Host: qa.developom.com  
URI: https://www.developom.com/

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

150204 Missing header: X-XSS-Protection

Developom

Finding #	12630747	Severity	Information Gathered - Level 1
Unique #	d8480046-19c2-4e13-b45a-78d5b718c08c		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	Detection Date	18 Jul 2024 12:41 GMT-0800
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://www.develom.com/ response code: 200  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfol::iad1::9btb7-1721331733156-f5f97b74a366

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

GET https://www.develom.com/ response code: 200  
GET https://www.develom.com/?email=was@qualys.com response code: 200  
GET https://www.develom.com/videos response code: 200  
GET https://www.develom.com/articles response code: 200  
GET https://www.develom.com/products response code: 200  
GET https://www.develom.com/use-cases response code: 200  
GET https://www.develom.com/contact response code: 200  
GET https://www.develom.com/articles/clggsudoa0008x10upm0wtbq2 response code: 200  
GET https://www.develom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1 response code: 200  
GET https://www.develom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence response code: 200  
GET https://www.develom.com/articles/clj7q6qea0004y00uy6syet33 response code: 200  
GET https://www.develom.com/videos/clo1rphds0003xq4awxl4qvpp response code: 200  
GET https://www.develom.com/videos/clj7rv3ax000yy00u0qzsta2h response code: 200  
GET https://www.develom.com/videos/clnvzzq2z0002t6440a247c7g response code: 200  
GET https://www.develom.com/videos/clog0nmcb0000ye44vyj7j6vz response code: 200  
GET https://www.develom.com/videos/clnyph7xn0000ts45l2pnq07m response code: 200  
GET https://www.develom.com/~partytown/ response code: 404  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331739362 response code: 200  
GET https://www.develom.com/terms response code: 200  
GET https://www.develom.com/privacy response code: 200  
GET https://www.develom.com/about-us response code: 200  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331724174 response code: 200  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331759497 response code: 200  
GET https://www.develom.com/favicon.ico response code: 404  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331778695 response code: 200  
GET https://www.develom.com/articles/clj7r43ye000wy00uvzgvyd7 response code: 200  
GET https://www.develom.com/articles/gpt-4-vision-top-ten-use-cases-for-businesses response code: 200  
GET https://www.develom.com/articles/dueling-ai-chatbots-witness-the-battle-of-artificial-intelligence-minds response code: 200  
GET https://www.develom.com/articles/ai-just-got-more-amazing-discover-openai-s-latest-user-friendly-innovations response code: 200  
GET https://www.develom.com/articles/from-healthcare-to-finance-real-life-ai-use-cases-that-inspire response code: 200  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331780446 response code: 200  
GET https://www.develom.com/articles/clj7qx5td000my00uqwm5wtlk response code: 200  
GET https://www.develom.com/articles/unlocking-success-ai-readiness-for-genai-are-you-ready response code: 200  
GET https://www.develom.com/articles/revolutionizing-customer-service-how-chatbots-are-changing-the-game response code: 200  
GET https://www.develom.com/articles/clj7qnnyr000cy00u04icighu response code: 200  
GET https://www.develom.com/products/clmv85ero0002us4tb5kuozjw response code: 200  
GET https://www.develom.com/products/clmv90exx000aus4tjpfsevri response code: 200  
GET https://www.develom.com/products/clmuxwlfy00071b45fz70lz2a response code: 200  
GET https://www.develom.com/products/clmuy18fn000e1b4511u2vch6 response code: 200  
GET https://www.develom.com/products/clmv8ujvf0007us4ttuu4a5zo response code: 200  
GET https://www.develom.com/products/clmv8vrct0009us4t7diurr9l response code: 200  
GET https://www.develom.com/products/clmv9544r000cus4t5g598d78 response code: 200  
GET https://www.develom.com/products/clmux1i7500041b45ojawf83q response code: 200  
GET https://www.develom.com/products/clmuy83lh000c1b454sixbm0w response code: 200  
GET https://www.develom.com/products/cllx766m40001zl2qx31jooud response code: 200  
GET https://www.develom.com/products/clmv91j6j000bus4tbsu30gy3 response code: 200  
GET https://www.develom.com/products/clmv8ns9x0006us4ttfhr3hik response code: 200  
GET https://www.develom.com/products/clmuz5qml000h1b45qtdz2lk9 response code: 200  
GET https://www.develom.com/~partytown/partytown-sandbox-sw.html?1721331787348 response code: 200  
GET https://www.develom.com/use-cases/clncmoho400091c4rs0w1nwi8 response code: 200

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

150245 Missing header: X-Frame-Options

Develom

Finding #	12630735	Severity	Information Gathered - Level 1
Unique #	30f030ab-a1a1-4f6e-864a-ba3a0c2c25e8		
Group	Security Weaknesses		
CWE	CWE-693	Detection Date	18 Jul 2024 12:41 GMT-0800

# WAS Web Application Report

OWASP

A5 Security Misconfiguration

WASC

WASC-15 APPLICATION MISCONFIGURATION

## Details

### Threat

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

Note: Only responses with status code 200 ok are tested and reported for 150245 and 150124

### Impact

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

### Solution

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

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

## Results

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

GET https://www.develom.com/  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:13 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::9btb7-1721331733156-f5f97b74a366

GET https://www.develom.com/?email=was@qualys.com  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:31 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::f25dc-1721331751758-f2dc32b9f36f

GET https://www.develom.com/articles  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:59 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::jtzjd-1721331779178-af2503aa053e

GET https://www.develom.com/articles/clggsudoa0008x10upm0wtbq2  
Response code: 200  
Response headers:

# WAS Web Application Report

age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:43:18 GMT  
server: Vercel  
set-cookie: entity=articles; Path=/; Expires=Fri, 18 Jul 2025 19:43:18 GMT  
set-cookie: entity=articles; expires=Fri, 18-Jul-2025 19:43:18 GMT; domain=www.developom.com; path=/  
set-cookie: entityId=clggsudoa0008xl0upm0wtbq2; expires=Fri, 18-Jul-2025 19:43:18 GMT; domain=www.developom.com; path=/  
entityId=clggsudoa0008xl0upm0wtbq2; Path=/; Expires=Fri, 18 Jul 2025 19: 43:18 GMT  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::2zb7n-1721331798160-2f5cb09b95c3

GET https://www.developom.com/articles/what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:43:23 GMT  
server: Vercel  
set-cookie: entity=articles; Path=/; Expires=Fri, 18 Jul 2025 19:43:23 GMT  
set-cookie: entity=articles; expires=Fri, 18-Jul-2025 19:43:36 GMT; domain=www.developom.com; path=/  
set-cookie: entityId=clj7q6qea0004y00uy6syet33; expires=Fri, 18-Jul-2025 19:43:36 GMT; domain=www.developom.com; path=/  
entityId=what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence; Path=/; Expires=Fri, 18 Jul 2025 19: 43:23 GMT  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::wrxj7-1721331803182-021425a974b0

GET https://www.developom.com/contact  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:43:14 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::jdttt-1721331794156-dcf073431f34

GET https://www.developom.com/contact?firstName=John&lastName=John&email=was@qualys.com&phone=8000000000&timeZone=Africa%2FAbidjan&subject=1&message=1  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:43:26 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::zxxtr-1721331806457-c71798d9c538  
Set-Cookie: entity=articles; expires=Fri, 18-Jul-2025 19:43:23 GMT; domain=www.developom.com; path=/  
Set-Cookie: entityId=what-are-the-top-10-approaches-a-fortune-500-must-follow-when-using-artificial-intelligence; expires=Fri, 18-Jul-2025 19:43:23 GMT; domain=www.developom.com; path=/

GET https://www.developom.com/products  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:43:06 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::s428v-1721331786156-0b5cea97a954

GET https://www.developom.com/use-cases  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:43:09 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::fcj8b-1721331789157-c6aff9f11269

# WAS Web Application Report

GET https://www.develop.com/videos  
Response code: 200  
Response headers:  
age: 0  
cache-control: public, max-age=0, must-revalidate  
content-encoding: br  
content-type: text/html  
date: Thu, 18 Jul 2024 19:42:57 GMT  
server: Vercel  
strict-transport-security: max-age=63072000  
x-vercel-cache: MISS  
x-vercel-id: sfo1::iad1::h6gf7-1721331777157-6be68a0e0ef8

## 150277 Cookie without SameSite attribute (1)

	150277 Cookie without SameSite attribute	Develop	
Finding #	12630725	Severity	Information Gathered - Level 1
Unique #	96b05500-a7b1-40a1-828c-53680435830b		
Group	Security Weaknesses		
CWE	CWE-16, CWE-1032	Detection Date	18 Jul 2024 12:41 GMT-0800
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  
entity=articles; expires=Fri Jul 18 19:43:18 2025; path=/; domain=www.develop.com; max-age=31534353 | First set at URL: https://www.develop.com/contact  
entityId=clggsudoa0008xl0upm0wtbq2; expires=Fri Jul 18 19:43:18 2025; path=/; domain=www.develop.com; max-age=31534353 | First set at URL: https://www.develop.com/contact  
  
NID=516=CA2REObNiPB9LJwvela1gOq9nBM0k4UcTd8sELfxVmkBo8b4SsKA2v1tAkcl\_iNYQiHAKAXTI\_T8KMdN\_Rlk6XkniJ1eDEk8XDqU9AZaYDUuzxitQSwj6DNyfKPDfQ6R9iEh8fMda7y  
cpo1S-XTUbS87KS2Pc; expires=Fri Jan 17 19:44:00 2025; path=/; domain=.google.com; max-age=15809595; secure; httponly | First set at URL: https://www.develop.com/videos/  
clo1rphds0003xq4awx14qvpp

Appendix

Web Application Details  
Develom

Name	Develom
ID	674852198
URL	https://www.develom.com
Owner	Hector DeJesus (devem3hd)
Scope	Limit to URL hostname
Tags	platform, vulnerability-management
Custom Attributes	-