Developer Report

Acunetix Security Audit

05 November 2023

Generated by Acunetix

Scan of toqio.co

Scan details

Scan information	
Start time	05/11/2023, 14:59:21
Start url	https://toqio.co/
Host	toqio.co
Scan time	9 minutes, 0 seconds
Profile	Full Scan
Server information	nginx
Responsive	True
Server OS	Unknown
Server technologies	PHP
Scan status	aborted

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	12
High	0
Medium	1
Low	6
Informational	5

Alerts summary

Development configuration file

Classification	
CVSS3	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N Base Score: 3.1 Attack Vector: Network Attack Complexity: High Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
/wp-content/themes/toqio/package.json	1

Clickjacking: X-Frame-Options header missing

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None

CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-693

Affected items	Variation
Web Server	1

Cookie(s) with missing, inconsistent, or contradictory properties.

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Cookie(s) without HttpOnly flag set

Classification

CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Cookie(s) without Secure flag set

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation

Web Server	1

Documentation file

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-538

Affected items	Variation
/readme.html	1

HTTP Strict Transport Security (HSTS) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None

CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Content Security Policy (CSP) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1

Email address found

Classification

CVSS3	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
/contact/	1
/es/contacto/	1

Subresource Integrity (SRI) not implemented

Classification	
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-16

Affected items	Variation
Web Server	1
/blogs/7-benefits-of-digital-onboarding/	1

Alerts details

Development configuration file

Severity	**Medium**
Reported by module	/Scripts/PerFolder/Development_Files.script

Description

A configuration file (e.g. Vagrantfile, Gemfile, Rakefile, ...) was found in this directory. This file may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all configuration files acessible from internet.

Affected items

/wp-content/themes/toqio/package.json

Details

File info:
package.json => Grunt configuration file. Grunt is a JavaScript task runner.
Pattern found:

```
"dependencies":
```

Request headers

```
GET /wp-content/themes/toqio/package.json HTTP/1.1
Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Clickjacking: X-Frame-Options header missing

Severity	**Low**
Reported by module	/Scripts/PerServer/Clickjacking_X_Frame_Options.script

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return an **X-Frame-Options** header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header.

References

[The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)
[Clickjacking (https://en.wikipedia.org/wiki/Clickjacking)](https://en.wikipedia.org/wiki/Clickjacking)
[OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)](https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
[Frame Buster Buster (https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)](https://stackoverflow.com/questions/958997/frame-buster-buster-buster-code-needed)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Cookie(s) with missing, inconsistent, or contradictory properties.

Severity	**Low**
Reported by module	/RPA/Cookie_Validator.js

Description

At least one of the cookie's properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

Recommendation

Ensure that the cookie configuration complies with the applicable standards.

References

[MDN | Set-Cookie](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie) (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie)
[Securing cookies with cookie prefixes](https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/) (https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/)
[Cookies: HTTP State Management Mechanism](https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05) (https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05)
[SameSite Updates - The Chromium Projects](https://www.chromium.org/updates/same-site) (https://www.chromium.org/updates/same-site)
[draft-west-first-party-cookies-07: Same-site Cookies](https://tools.ietf.org/html/draft-west-first-party-cookies-07) (https://tools.ietf.org/html/draft-west-first-party-cookies-07)

Affected items

Web Server

Verified vulnerability

Details

A cookie was set with the following response header:

```
Set-Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9; path=/
```

This cookie has the following issues:

- **Cookie without SameSite attribute.** When cookies lack the SameSite attribute, Web browsers may apply different and sometimes unexpected defaults. It is therefore recommended to add a SameSite attribute with an appropriate value of either "Strict", "Lax", or "None".

Request headers

```
GET / HTTP/1.1
Referer: https://toqio.co/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Cookie(s) without HttpOnly flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

This cookie does not have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

Recommendation

If possible, you should set the HttpOnly flag for this cookie.

Affected items

Web Server

Verified vulnerability

Details

Set-Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9; path=/

Request headers

```
GET / HTTP/1.1
Referer: https://toqio.co/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Cookie(s) without Secure flag set

Severity	**Low**
Reported by module	/RPA/Cookie_Without_Secure.js

Description

This cookie does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

Recommendation

If possible, you should set the Secure flag for this cookie.

Affected items

Web Server

Verified vulnerability

Details

Set-Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9; path=/

Request headers

```
GET / HTTP/1.1
Referer: https://toqio.co/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Documentation file

Severity	**Low**
Reported by module	/Scripts/PerFolder/Readme_Files.script

Description

A documentation file (e.g. readme.txt, changelog.txt, ...) was found in this directory. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

Recommendation

Remove or restrict access to all documentation file acessible from internet.

Affected items

/readme.html

Verified vulnerability

Details

File contents (first 250 characters):

```
<!DOCTYPE html>
<html lang="en">
<head>
	<meta name="viewport" content="width=device-width" />
	<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
	<title>WordPress &#8250; ReadMe</title>
	<link rel="stylesheet" href="wp-admin/css/ ...
```

Request headers

```
GET /readme.html HTTP/1.1
Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

HTTP Strict Transport Security (HSTS) not implemented

Severity	**Low**
Reported by module	/httpdata/HSTS_not_implemented.js

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

[hstspreload.org (https://hstspreload.org/)](https://hstspreload.org/)
[Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server
Details
Request headers

```
GET / HTTP/1.1
Referer: https://toqio.co/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Content Security Policy (CSP) not implemented

Severity	**Informational**
Reported by module	/httpdata/CSP_not_implemented.js

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

[Content Security Policy (CSP)](https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)(https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
[Implementing Content Security Policy](https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)(https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server

Details

Request headers

```
GET / HTTP/1.1
Referer: https://toqio.co/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Email address found

Severity	**Informational**
Reported by module	/Scripts/PerFolder/Text_Search_Dir.script

Description

One or more email addresses have been found on this page. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

[Anti-spam techniques](https://en.wikipedia.org/wiki/Anti-spam_techniques)(https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

/contact/

Details

Pattern found:

```
press@toq.io
people@toq.io
```

Request headers

```
GET /contact/ HTTP/1.1
Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/es/contacto/

Details

Pattern found:

```
press@toq.io
people@toq.io
```

Request headers

```
GET /es/contacto/ HTTP/1.1
Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

ⓘ Subresource Integrity (SRI) not implemented

Severity	**Informational**
Reported by module	/RPA/SRI_Not_Implemented.js

Description

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
        integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
        crossorigin="anonymous"></script>
```

References

[Subresource Integrity (https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)](https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity)
[SRI Hash Generator (https://www.srihash.org/)](https://www.srihash.org/)

Affected items

Web Server

Details

https://cdn-cookieyes.com/client_data/1ab8fba9db8458622d7a1233/script.js

Request headers

```
GET / HTTP/1.1
Referer: https://toqio.co/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

/blogs/7-benefits-of-digital-onboarding/

Details

//js.hsforms.net/forms/v2.js

Request headers

```
GET /blogs/7-benefits-of-digital-onboarding/ HTTP/1.1
Referer: https://toqio.co/
Cookie: PHPSESSID=667bb63e1e44e080945123c1a98c50a9
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: toqio.co
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/73.0.3683.103 Safari/537.36
Connection: Keep-alive
```

Scanned items (coverage report)

https://toqio.co/
https://toqio.co/HubStyleTokens/
https://toqio.co/HubStyleTokens/static-2.5251
https://toqio.co/I18n/
https://toqio.co/I18n/static-7.1007
https://toqio.co/PatternValidationJS/
https://toqio.co/PatternValidationJS/static-1.382
https://toqio.co/PortalIdParser/
https://toqio.co/PortalIdParser/static-2.169
https://toqio.co/SharedLegalStrings/
https://toqio.co/SharedLegalStrings/static-1.916
https://toqio.co/StyleGuideUI/
https://toqio.co/StyleGuideUI/static-3.360
https://toqio.co/UIComponents/
https://toqio.co/UIComponents/static-3.2202
https://toqio.co/about-us/
https://toqio.co/about-us/talent/
https://toqio.co/blog/
https://toqio.co/blog/newsroom-article/
https://toqio.co/blog/newsroom-article/2021s-hottest-fintech-seed-deals-according-to-investors/
https://toqio.co/blog/newsroom-article/an-uptick-in-damp-lifestyles-the-death-of-influencer-marketing-here-are-some-bold-tech-predictions-for-2023/
https://toqio.co/blog/newsroom-article/baas-is-at-an-inflection-point-here-are-the-changes-we-can-expect/
https://toqio.co/blog/newsroom-article/banking-as-a-service-momentum-to-carry-on-this-year-in-europe/
https://toqio.co/blog/newsroom-article/chris-weller-joins-fintech-saas-platform-toqio-as-commercial-director-for-uk-and-europe/
https://toqio.co/blog/newsroom-article/cracking-the-code-how-the-open-finance-appathon-empowered-api-innovation/
https://toqio.co/blog/newsroom-article/dafna-martin-beltran-joins-toqio-as-head-of-sales-for-new-markets/
https://toqio.co/blog/newsroom-article/exclusive-just-cashflow-partners-with-railsbank-to-launch-business-account/
https://toqio.co/blog/newsroom-article/expansion-spanish-2020-start-up-awards/
https://toqio.co/blog/newsroom-article/fintech-saas-provider-toqio-launches-in-spain-with-plans-to-double-its-spanish-team/
https://toqio.co/blog/newsroom-article/healrworld-partners-with-mastercard-to-launch-first-ever-united-nations-sdg-focused-corporate-debit-card-in-uk/
https://toqio.co/blog/newsroom-article/in-profile-mike-galvin-at-toqio/
https://toqio.co/blog/newsroom-article/meet-toqio-the-digital-finance-platform-and-marketplace/
https://toqio.co/blog/newsroom-article/paysme-eyes-1-million-funding-round-via-globacap/
https://toqio.co/blog/newsroom-article/realizing-the-potential-of-embedded-finance-our-investment-in-toqio/
https://toqio.co/blog/newsroom-article/sdg-corporate-debit-card-launched-by-quartet-of-payments-players/
https://toqio.co/blog/newsroom-article/south-summit/
https://toqio.co/blog/newsroom-article/the-toqio-marketplace-a-thriving-fintech-ecosystem/
https://toqio.co/blog/newsroom-article/toqio-announces-e8m-to-make-it-easier-for-any-business-to-create-financial-products/
https://toqio.co/blog/newsroom-article/toqio-announces-full-pci-dss-certification/
https://toqio.co/blog/newsroom-article/toqio-appoints-alessandro-palma-as-cfo/
https://toqio.co/blog/newsroom-article/toqio-appoints-luis-fernandez-as-new-vice-president-of-customer-success/
https://toqio.co/blog/newsroom-article/toqio-boosts-sales-team-with-new-appointments-as-part-of-growth-plans-for-2022/
https://toqio.co/blog/newsroom-article/toqio-featured-in-the-sunday-times-business-supplement-raconteur/
https://toqio.co/blog/newsroom-article/toqio-hosts-fintech-industry-event-to-inaugurate-new-madrid-offices/
https://toqio.co/blog/newsroom-article/toqio-makes-it-onto-the-startups-100-list-for-2023/
https://toqio.co/blog/newsroom-article/toqio-reveals-remarkable-growth-of-baas-across-europe-in-latest-report/
https://toqio.co/blog/newsroom-article/toqio-secures-e20-million-to-be-the-platform-of-choice-for-building-new-fintech-solutions/
https://toqio.co/blog/newsroom-article/toqio-wins-pay360-award/
https://toqio.co/blog/newsroom-article/uk-saas-platform-toqio-welcomes-michael-pierce-as-vp-of-sales/
https://toqio.co/blog/newsroom-article/view-from-the-top/

https://toqio.co/blog/newsroom-article/what-it-actually-costs-to-build-a-fintech-solution/
https://toqio.co/blog/newsroom-article/worldpay-chief-gabriel-de-montessus-takes-the-chair-at-toqio/
https://toqio.co/blog/newsroom/
https://toqio.co/blog/newsroom/toqio-featured-in-the-sunday-times-business-supplement-raconteur/
https://toqio.co/blogs/
https://toqio.co/blogs/7-benefits-of-digital-onboarding/
https://toqio.co/blogs/a-brief-guide-to-open-banking/
https://toqio.co/blogs/corporate-embedded-finance-the-next-frontier/
https://toqio.co/blogs/embedded-finance-the-future-of-disruptive-banking/
https://toqio.co/blogs/fintech-trends-for-2023/
https://toqio.co/blogs/five-things-to-consider-when-monetizing-your-embedded-finance-solution/
https://toqio.co/blogs/how-digital-banking-empowers-customers/
https://toqio.co/blogs/how-fintech-saas-is-generating-companies-multi-million-dollar-savings/
https://toqio.co/blogs/if-youre-not-compliant-youre-dead-in-the-water/
https://toqio.co/blogs/incumbents-are-making-giant-strides-in-the-baas-landscape/
https://toqio.co/blogs/leveraging-embedded-finance-to-cultivate-enduring-supplier-relationships/
https://toqio.co/blogs/market-secret-embedded-finance-is-redefining-supply-chains/
https://toqio.co/blogs/the-future-of-digital-banking/
https://toqio.co/blogs/the-indispensable-role-of-a-design-system-in-fintech-growth/
https://toqio.co/blogs/the-inevitability-of-fintech-saas/
https://toqio.co/blogs/the-necessity-of-compliance/
https://toqio.co/blogs/the-race-to-hyper-personalisation-its-no-longer-just-about-incumbents-vs-challengers/
https://toqio.co/blogs/the-technology-behind-embedded-finance/
https://toqio.co/blogs/the-top-five-ways-to-leverage-embedded-finance-in-product-distribution/
https://toqio.co/blogs/to-build-or-to-buy-the-10-factors-cios-must-consider/
https://toqio.co/blogs/unlocking-success-the-symbiotic-relationship-between-corporate-embedded-finance-and-hyperfocus/
https://toqio.co/blogs/unlocking-the-potential-of-corporate-embedded-finance-in-franchising/
https://toqio.co/blogs/we-are-diverse-not-just-committed-to-diversity/
https://toqio.co/blogs/what-it-actually-costs-to-build-a-fintech-solution/
https://toqio.co/browserslist-config-hubspot/
https://toqio.co/browserslist-config-hubspot/static-1.77
https://toqio.co/classnames/
https://toqio.co/classnames/static-2.10
https://toqio.co/contact/
https://toqio.co/css2
https://toqio.co/cssUtils/
https://toqio.co/cssUtils/static-1.276
https://toqio.co/csstype/
https://toqio.co/csstype/static-1.8
https://toqio.co/draft
https://toqio.co/emailcheck/
https://toqio.co/emailcheck/v1/
https://toqio.co/emailcheck/v1/form-resubscribe
https://toqio.co/emailcheck/v1/json-ext
https://toqio.co/embedded-viral-link/
https://toqio.co/emoji-regex/
https://toqio.co/emoji-regex/static-1.7
https://toqio.co/enterprise.js
https://toqio.co/enviro/
https://toqio.co/enviro/static-4.176
https://toqio.co/es
https://toqio.co/es/
https://toqio.co/es/camaraderia/
https://toqio.co/es/contacto/
https://toqio.co/es/manifest.json
https://toqio.co/es/politica-de-privacidad/
https://toqio.co/es/solicitar-demo/
https://toqio.co/es/terminos-y-condiciones/
https://toqio.co/es/wp-content/
https://toqio.co/es/wp-content/plugins/
https://toqio.co/es/wp-content/plugins/cookie-law-info/
https://toqio.co/es/wp-content/plugins/cookie-law-info/lite/
https://toqio.co/es/wp-content/plugins/cookie-law-info/lite/frontend/

```
https://toqio.co/es/wp-content/plugins/cookie-law-info/lite/frontend/images/
https://toqio.co/es/wp-content/plugins/cookie-law-info/lite/frontend/js/
https://toqio.co/es/wp-content/plugins/cookie-law-info/lite/frontend/js/script.min.js
https://toqio.co/es/wp-content/themes/
https://toqio.co/es/wp-content/themes/toqio/
https://toqio.co/es/wp-content/themes/toqio/dist/
https://toqio.co/es/wp-content/themes/toqio/dist/css/
https://toqio.co/es/wp-content/themes/toqio/dist/css/slick-styles.min.css
https://toqio.co/es/wp-content/themes/toqio/dist/css/slick-theme.min.css
https://toqio.co/es/wp-content/themes/toqio/dist/css/styles.min.css
https://toqio.co/es/wp-content/themes/toqio/dist/js/
https://toqio.co/es/wp-content/themes/toqio/dist/js/jquery.min.js
https://toqio.co/es/wp-content/themes/toqio/dist/js/scripts.js
https://toqio.co/es/wp-content/themes/toqio/dist/js/slick.min.js
https://toqio.co/es/wp-content/themes/toqio/img/
https://toqio.co/es/wp-content/themes/toqio/img/footer/
https://toqio.co/es/wp-content/themes/toqio/img/icons/
https://toqio.co/es/wp-content/themes/toqio/solent-css.min.css
https://toqio.co/es/wp-content/uploads/
https://toqio.co/es/wp-content/uploads/sites/
https://toqio.co/es/wp-content/uploads/sites/3/
https://toqio.co/es/wp-content/uploads/sites/3/2022/
https://toqio.co/es/wp-content/uploads/sites/3/2022/03/
https://toqio.co/es/wp-content/uploads/sites/3/2022/08/
https://toqio.co/es/wp-includes/
https://toqio.co/es/wp-includes/css/
https://toqio.co/es/wp-includes/css/dist/
https://toqio.co/es/wp-includes/css/dist/block-library/
https://toqio.co/es/wp-includes/css/dist/block-library/style.min.css
https://toqio.co/es/wp-json/
https://toqio.co/es/wp-json/oembed/
https://toqio.co/es/wp-json/oembed/1.0/
https://toqio.co/es/wp-json/oembed/1.0/embed
https://toqio.co/es/wp-json/wp/
https://toqio.co/es/wp-json/wp/v2/
https://toqio.co/es/wp-json/wp/v2/pages/
https://toqio.co/es/wp-json/wp/v2/pages/1409
https://toqio.co/es/wp-json/wp/v2/pages/1532
https://toqio.co/es/xmlrpc.php
https://toqio.co/forms-embed-shared-libs/
https://toqio.co/forms-embed-shared-libs/static-1.263
https://toqio.co/forms-embed-utils-lib/
https://toqio.co/forms-embed-utils-lib/static-1.162
https://toqio.co/forms-embed/
https://toqio.co/forms-embed/static-1.4082
https://toqio.co/forms-utils-lib/
https://toqio.co/forms-utils-lib/static-1.3152
https://toqio.co/hds-components/
https://toqio.co/hds-components/static-1.366
https://toqio.co/hds-tokens/
https://toqio.co/hds-tokens/static-1.129
https://toqio.co/hoist-non-react-statics/
https://toqio.co/hoist-non-react-statics/static-3.9
https://toqio.co/hs-test-utils/
https://toqio.co/hs-test-utils/static-1.1852
https://toqio.co/hub-http-janus/
https://toqio.co/hub-http-janus/static-1.391
https://toqio.co/hub-http-rxjs/
https://toqio.co/hub-http-rxjs/static-1.363
https://toqio.co/hub-http/
https://toqio.co/hub-http/static-1.1039
https://toqio.co/hubspot-url-utils/
https://toqio.co/hubspot-url-utils/static-1.161
https://toqio.co/i18n-data/
```

```
https://toqio.co/i18n-data/static-1.140
https://toqio.co/immutable/
https://toqio.co/immutable/static-2.19
https://toqio.co/index.asp
https://toqio.co/jasmine-runner/
https://toqio.co/jasmine-runner/static-1.411
https://toqio.co/jasmine/
https://toqio.co/jasmine/static-3.135
https://toqio.co/json
https://toqio.co/login.jsp
https://toqio.co/manifest.json
https://toqio.co/metrics-js/
https://toqio.co/metrics-js/static-1.3193
https://toqio.co/newsroom/
https://toqio.co/platform/
https://toqio.co/privacy-policy/
https://toqio.co/privacy-policy/feed/
https://toqio.co/readme.html
https://toqio.co/recaptcha
https://toqio.co/request-a-demo-success/
https://toqio.co/request-a-demo/
https://toqio.co/robots.txt
https://toqio.co/sample-page/
https://toqio.co/sample-page/feed/
https://toqio.co/signup-hubspot
https://toqio.co/sitemap.xml
https://toqio.co/team/
https://toqio.co/terms-of-use/
https://toqio.co/use-cases/
https://toqio.co/wp-admin/
https://toqio.co/wp-content/
https://toqio.co/wp-content/plugins/
https://toqio.co/wp-content/plugins/advanced-custom-fields/
https://toqio.co/wp-content/plugins/advanced-custom-fields/core/
https://toqio.co/wp-content/plugins/advanced-custom-fields/core/actions/
https://toqio.co/wp-content/plugins/advanced-custom-fields/core/actions/export.php
https://toqio.co/wp-content/themes/
https://toqio.co/wp-content/themes/toqio/
https://toqio.co/wp-content/themes/toqio/dist/
https://toqio.co/wp-content/themes/toqio/dist/css/
https://toqio.co/wp-content/themes/toqio/dist/css/fonts/
https://toqio.co/wp-content/themes/toqio/dist/css/slick-theme.css
https://toqio.co/wp-content/themes/toqio/dist/css/slick.css
https://toqio.co/wp-content/themes/toqio/dist/css/styles.min.css
https://toqio.co/wp-content/themes/toqio/dist/js/
https://toqio.co/wp-content/themes/toqio/dist/js/jquery.min.js
https://toqio.co/wp-content/themes/toqio/dist/js/scripts.js
https://toqio.co/wp-content/themes/toqio/dist/js/slick.min.js
https://toqio.co/wp-content/themes/toqio/img/
https://toqio.co/wp-content/themes/toqio/img/footer/
https://toqio.co/wp-content/themes/toqio/img/icons/
https://toqio.co/wp-content/themes/toqio/package.json
https://toqio.co/wp-content/themes/toqio/style.css
https://toqio.co/wp-content/uploads/
https://toqio.co/wp-content/uploads/2021/
https://toqio.co/wp-content/uploads/2021/06/
https://toqio.co/wp-content/uploads/2021/11/
https://toqio.co/wp-content/uploads/2021/12/
https://toqio.co/wp-content/uploads/2022/
https://toqio.co/wp-content/uploads/2022/08/
https://toqio.co/wp-content/uploads/2022/09/
https://toqio.co/wp-content/uploads/2023/
https://toqio.co/wp-content/uploads/2023/05/
https://toqio.co/wp-content/uploads/2023/09/
```

```
https://toqio.co/wp-content/uploads/2023/10/
https://toqio.co/wp-includes/
https://toqio.co/wp-includes/css/
https://toqio.co/wp-includes/css/dist/
https://toqio.co/wp-includes/css/dist/block-library/
https://toqio.co/wp-includes/css/dist/block-library/style.min.css
https://toqio.co/wp-json/
https://toqio.co/wp-json/oembed/
https://toqio.co/wp-json/oembed/1.0/
https://toqio.co/wp-json/oembed/1.0/embed
https://toqio.co/wp-json/wp/
https://toqio.co/wp-json/wp/v2/
https://toqio.co/wp-json/wp/v2/comments
https://toqio.co/wp-json/wp/v2/media
https://toqio.co/wp-json/wp/v2/media/
https://toqio.co/wp-json/wp/v2/media/257
https://toqio.co/wp-json/wp/v2/pages
https://toqio.co/wp-json/wp/v2/pages/
https://toqio.co/wp-json/wp/v2/pages/1024
https://toqio.co/wp-json/wp/v2/pages/1350
https://toqio.co/wp-json/wp/v2/pages/1480
https://toqio.co/wp-json/wp/v2/pages/2
https://toqio.co/wp-json/wp/v2/pages/3
https://toqio.co/wp-json/wp/v2/pages/350
https://toqio.co/wp-json/wp/v2/pages/353
https://toqio.co/wp-json/wp/v2/pages/355
https://toqio.co/wp-json/wp/v2/pages/6
https://toqio.co/wp-json/wp/v2/types/
https://toqio.co/wp-json/wp/v2/types/page
https://toqio.co/wp-sitemap-posts-blogs-1.xml
https://toqio.co/wp-sitemap-posts-case-study-1.xml
https://toqio.co/wp-sitemap-posts-newsroom-article-1.xml
https://toqio.co/wp-sitemap-posts-page-1.xml
https://toqio.co/wp-sitemap-posts-post-1.xml
https://toqio.co/wp-sitemap-posts-team-members-1.xml
https://toqio.co/wp-sitemap-taxonomies-category-1.xml
https://toqio.co/wp-sitemap-taxonomies-post_tag-1.xml
https://toqio.co/wp-sitemap-taxonomies-team-member-type-1.xml
https://toqio.co/wp-sitemap-users-1.xml
https://toqio.co/wp-sitemap.xml
https://toqio.co/xmlrpc.php
```