

# Scan of karamozesh.github.io

## Scan details



Scan information	
Start time	2023-07-10T20:10:47.027274+03:30
Start url	https://karamozesh.github.io/
Host	karamozesh.github.io
Scan time	5 minutes, 35 seconds
Profile	Full Scan
Server information	GitHub.com
Responsive	True
Server OS	Unknown

## Threat level

### Acunetix Threat Level 1

One or more low-severity type vulnerabilities have been discovered by the scanner.

## Alerts distribution

Total alerts found	7
 High	0
 Medium	0
 Low	3
 Informational	4

## Affected items

Web Server	
Alert group	Clickjacking: CSP frame-ancestors missing
Severity	Low
Description	<p>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.</p> <p>The server didn't return a <b>frame-ancestors</b> directive in the Content-Security-Policy header which means that this website could be at risk of a clickjacking attack. The frame-ancestors directives can be used to indicate whether or not a browser should be allowed to render a page inside a frame. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.</p>
Recommendations	Configure your web server to include a CSP header with frame-ancestors directive and an X-Frame-Options header. Consult Web references for more information about the possible values for this header.
Alert variants	
Details	<p>Paths without CSP frame-ancestors:</p> <ul style="list-style-type: none"> <li>• <a href="https://karamozesh.github.io/assets/">https://karamozesh.github.io/assets/</a></li> <li>• <a href="https://karamozesh.github.io/resume-creating-app/base-information">https://karamozesh.github.io/resume-creating-app/base-information</a></li> <li>• <a href="https://karamozesh.github.io/skill/javascript">https://karamozesh.github.io/skill/javascript</a></li> <li>• <a href="https://karamozesh.github.io/login">https://karamozesh.github.io/login</a></li> <li>• <a href="https://karamozesh.github.io/resume-creating">https://karamozesh.github.io/resume-creating</a></li> <li>• <a href="https://karamozesh.github.io/talent-survey/disk">https://karamozesh.github.io/talent-survey/disk</a></li> <li>• <a href="https://karamozesh.github.io/register">https://karamozesh.github.io/register</a></li> <li>• <a href="https://karamozesh.github.io/resume-training">https://karamozesh.github.io/resume-training</a></li> <li>• <a href="https://karamozesh.github.io/skill">https://karamozesh.github.io/skill</a></li> <li>• <a href="https://karamozesh.github.io/talent-survey">https://karamozesh.github.io/talent-survey</a></li> <li>• <a href="https://karamozesh.github.io/talent-survey/haland">https://karamozesh.github.io/talent-survey/haland</a></li> <li>• <a href="https://karamozesh.github.io/moshavere-request">https://karamozesh.github.io/moshavere-request</a></li> <li>• <a href="https://karamozesh.github.io/talent-survey/mbti">https://karamozesh.github.io/talent-survey/mbti</a></li> <li>• <a href="https://karamozesh.github.io/skill/">https://karamozesh.github.io/skill/</a></li> <li>• <a href="https://karamozesh.github.io/resume-creating-app/">https://karamozesh.github.io/resume-creating-app/</a></li> <li>• <a href="https://karamozesh.github.io/talent-survey/">https://karamozesh.github.io/talent-survey/</a></li> </ul>

GET /assets/ HTTP/1.1

Referer: https://karamozesh.github.io/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: karamozesh.github.io

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive

Web Server
------------

Alert group	Clickjacking: X-Frame-Options header missing
-------------	--

Severity	Low
----------	-----

Description	<p>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.</p> <p>The server didn't return an <b>X-Frame-Options</b> 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.</p>
-------------	--

Recommendations	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.
-----------------	--

Alert variants	
----------------	--

Details	
---------	--

GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: karamozesh.github.io

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive

Web Server
------------

Alert group	Possible virtual host found
-------------	-----------------------------

Severity	Low
----------	-----

Description	<p>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.</p> <p>This web server is responding differently when the Host header is manipulated and various common virtual hosts are tested. This could indicate there is a Virtual Host present.</p>
Recommendations	Consult the virtual host configuration and check if this virtual host should be publicly accessible.
Alert variants	
Details	<p>Virtual host: <b>test</b> Response:</p> <pre>&lt;html&gt;  &lt;head&gt;&lt;title&gt;301 Moved Permanently&lt;/title&gt;&lt;/head&gt;  &lt;body&gt;  &lt;center&gt;&lt;h1&gt;301 Moved Permanently&lt;/h1&gt;&lt;/center&gt;  &lt;hr&gt;&lt;center&gt;nginx&lt;/center&gt;  &lt;/body&gt;  &lt;/html&gt;</pre>

<b>Web Server</b>	
<b>Alert group</b>	<b>Content Security Policy (CSP) not implemented</b>
Severity	Informational
Description	<p>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.</p> <p>Content Security Policy (CSP) can be implemented by adding a <b>Content-Security-Policy</b> 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:</p> <pre>Content-Security-Policy:      default-src 'self';      script-src 'self' https://code.jquery.com;</pre> <p>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.</p>

Recommendations	It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the <b>Content-Security-Policy</b> HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.
Alert variants	
Details	<p>Paths without CSP header:</p> <ul style="list-style-type: none"> <li>• <a href="https://karamozesh.github.io/">https://karamozesh.github.io/</a></li> <li>• <a href="https://karamozesh.github.io/index.html">https://karamozesh.github.io/index.html</a></li> <li>• <a href="https://karamozesh.github.io/index">https://karamozesh.github.io/index</a></li> </ul>
<pre>GET / HTTP/1.1  Referer: https://karamozesh.github.io/  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8  Accept-Encoding: gzip,deflate  Host: karamozesh.github.io  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36  Connection: Keep-alive</pre>	

<b>Web Server</b>	
<b>Alert group</b>	<b>HTTP Strict Transport Security (HSTS) Best Practices</b>
Severity	Informational
Description	HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessible using HTTPS. It was detected that your web application doesn't implement best practices of HTTP Strict Transport Security (HSTS).
Recommendations	It's recommended to implement best practices of HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information
Alert variants	
Details	No includeSubDomains directive

```

GET / HTTP/1.1

Referer: https://karamozesh.github.io/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Encoding: gzip,deflate

Host: karamozesh.github.io

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive

```

<b>Web Server</b>	
<b>Alert group</b>	<b>Insecure Referrer Policy</b>
<b>Severity</b>	Informational
<b>Description</b>	Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.
<b>Recommendations</b>	Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value
<b>Alert variants</b>	
<b>Details</b>	<p>URLs where Referrer Policy configuration is insecure:</p> <ul style="list-style-type: none"> <li>• <a href="https://karamozesh.github.io/">https://karamozesh.github.io/</a></li> <li>• <a href="https://karamozesh.github.io/assets/">https://karamozesh.github.io/assets/</a></li> <li>• <a href="https://karamozesh.github.io/index.html">https://karamozesh.github.io/index.html</a></li> <li>• <a href="https://karamozesh.github.io/resume-creating-app/base-information">https://karamozesh.github.io/resume-creating-app/base-information</a></li> <li>• <a href="https://karamozesh.github.io/skill/javaScript">https://karamozesh.github.io/skill/javaScript</a></li> <li>• <a href="https://karamozesh.github.io/login">https://karamozesh.github.io/login</a></li> <li>• <a href="https://karamozesh.github.io/resume-creating">https://karamozesh.github.io/resume-creating</a></li> <li>• <a href="https://karamozesh.github.io/talent-survey/disk">https://karamozesh.github.io/talent-survey/disk</a></li> <li>• <a href="https://karamozesh.github.io/register">https://karamozesh.github.io/register</a></li> </ul>

GET / HTTP/1.1

Referer: https://karamozesh.github.io/

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: karamozesh.github.io

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive

<b>Web Server</b>	
-------------------	--

<b>Alert group</b>	<b>Reverse proxy detected</b>
--------------------	-------------------------------

<b>Severity</b>	Informational
-----------------	---------------

<b>Description</b>	This server uses a reverse proxy, a load balancer or a CDN (Content Delivery Network) or it's hosted in a cloud provider. Acunetix detected this by sending various payloads and detecting changes in headers and body.
--------------------	---

<b>Recommendations</b>	None
------------------------	------

<b>Alert variants</b>	
-----------------------	--

<b>Details</b>	Detected reverse proxy: Fastly
----------------	--------------------------------

GET / HTTP/1.1

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Accept-Encoding: gzip,deflate

Host: karamozesh.github.io

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36

Connection: Keep-alive

## Scanned items (coverage report)

---

<https://karamozesh.github.io/>  
<https://karamozesh.github.io/assets/>  
<https://karamozesh.github.io/assets/index.49866857.js>  
<https://karamozesh.github.io/assets/index.cf804f97.css>  
<https://karamozesh.github.io/index>  
<https://karamozesh.github.io/index.html>  
<https://karamozesh.github.io/login>  
<https://karamozesh.github.io/moshavere-request>  
<https://karamozesh.github.io/register>  
<https://karamozesh.github.io/resume-creating>  
<https://karamozesh.github.io/resume-creating-app/>  
<https://karamozesh.github.io/resume-creating-app/base-information>  
<https://karamozesh.github.io/resume-training>  
<https://karamozesh.github.io/skill>  
<https://karamozesh.github.io/skill/>  
<https://karamozesh.github.io/skill/javascript>  
<https://karamozesh.github.io/talent-survey>  
<https://karamozesh.github.io/talent-survey/>  
<https://karamozesh.github.io/talent-survey/disk>  
<https://karamozesh.github.io/talent-survey/haland>  
<https://karamozesh.github.io/talent-survey/mbti>