Web Application Report

This report includes important security information about your web application.

Security Report

This report was created by HCL AppScan Standard 10.0.6
Scan started: 4/6/2022 2:31:28 PM

Table of Contents

Introduction

This report contains the results of a web application security scan performed by HCL AppScan Standard.

Medium severity issues:	7
Total security issues included in the report:	7
Total security issues discovered in the scan:	96

General Information

Scan file name:	dgqadefence.gov.in
Scan started:	4/6/2022 2:31:28 PM
Test policy:	Application-Only
Test optimization level:	Fastest

Host	dgqadefence.gov.in
Port	443
Operating system:	Unknown
Web server:	Apache
Application server:	Any

Host	dgqadefence.gov.in
Port	80
Operating system:	Unknown
Web server:	Apache
Application server:	Any

Login Settings

Login method: None

Summary

Issue Types 3

TOC

	Issue Type	Number of Issues
M	Email Address Pattern Found	4
M	Missing "Content-Security-Policy" header	1
M	Unnecessary Http Response Headers found in the Application	2

Vulnerable URLs 4

TOC

	URL	Number of Issues
M	http://dgqadefence.gov.in/	2
M	https://dgqadefence.gov.in/	3
M	https://dgqadefence.gov.in/hi	1
M	https://dgqadefence.gov.in/location	1

Fix Recommendations 3

TOC

	Remediation Task	Number of Issues
M	Config your server to use the "Content-Security-Policy" header with secure policies	1
M	Do not allow sensitive information to leak.	2
M	Remove e-mail addresses from the website	4

Security Risks 2

TOC

	Risk	Number of Issues
M	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations	7

M	It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.	1	

Causes 1

TOC

	Cause	Number of Issues
M	Insecure web application programming or configuration	7

WASC Threat Classification

TOC

Threat	Number of Issues
Information Leakage	7

Issues Sorted by Issue Type

M Email Address Pattern Found 4 TOC

Issue 1 of 4 TOC

Email Address Pattern Found

Severity:	Medium
CVSS Score:	0.0
URL:	https://dgqadefence.gov.in/location
Entity:	location (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /location HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://dgqadefence.gov.in/
Connection: keep-alive
Host: dgqadefence.gov.in
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Dest: document


HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-UA-Compatible: IE=edge
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
X-Permitted-Cross-Domain-Policies: none
Vary: Accept-Encoding,User-Agent
X-Generator: Drupal 8 (https://www.drupal.org)
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
```

```
Keep-Alive: timeout=5, max=99
Cache-Control: must-revalidate, no-cache, private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-language: en
X-Drupal-Dynamic-Cache: UNCACHEABLE
Feature-Policy: fullscreen 'none'
X-Drupal-Cache: HIT
Referrer-Policy: no-referrer
Date: Wed, 06 Apr 2022 09:13:28 GMT
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Content-Type: text/html; charset=UTF-8



<!-- THEME DEBUG -->
<!-- THEME HOOK: 'html' -->
<!-- FILE NAME SUGGESTIONS:
   * html--location.html.twig
   x html.html.twig
-->
<!-- BEGIN OUTPUT from 'themes/website/templates/html.html.twig' -->
<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>Location | website</title>
    <meta http-equiv="Content-Security-Policy" content="default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval' http://www.google.com">
    <link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/ajax-progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/align.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/autocomplete-loading.module.css?r8d48t"
/>
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/fieldgroup.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/container-inline.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/clearfix.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/details.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/hidden.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/item-list.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/js.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/nowrap.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/position-container.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="
...
...
...

<p>Address: QAE(WE) A-1, Divyalok Park Society (Ist Floor) Opp Fatehgunj Police Station, Channi Road, Vadodara- 390002<br
/>
Phone: 0265- 2761698<br />
Fax: 0265- 2761698<br />
Telegraphic Address: QUALITYWE, VADORADA.<br />
E-mai: <a href="mailto:qaewevad-navy@nic.in">qaewevad-navy@nic.in</a></p>
...
...
...
<p>Address: SQAE(L&amp;amp;S) 1549, Sec-38 B Chandigarh 160 036<br />
Phone: 0172-2690168<br />
Fax: 0172-2690412<br />
Telegraphic Address:<br />
E-mail: <a href="mailto:sqaelns-dgqa@nic.in">sqaelns-dgqa@nic.in</a></p>
...
...
...
<p>Email: <a href="mailto:exampmle@mail.com" rel="noreferrer" target="_blank">exampmle@mail.com</a></p>
...
...
...
<p><strong>Email:</strong> <a href="mailto:exampmle@mail.com" rel="noreferrer" target="_blank">exampmle@mail.com</a></p>
...
...
...
```

Email Address Pattern Found

Severity:	Medium
CVSS Score:	0.0
URL:	http://dgqadefence.gov.in/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: dgqadefence.gov.in
Upgrade-Insecure-Requests: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US


HTTP/1.1 301 Moved Permanently
Location: https://dgqadefence.gov.in
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
Content-Length: 234
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=99
Cache-Control: max-age=2592000
Strict-Transport-Security: max-age=31536000; includeSubDomains
Feature-Policy: fullscreen 'none'
Date: Wed, 06 Apr 2022 09:13:25 GMT
Expires: Fri, 06 May 2022 09:13:25 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://dgqadefence.gov.in">here</a>.</p>
</body></html>


GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://dgqadefence.gov.in/
Host: dgqadefence.gov.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-UA-Compatible: IE=edge
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
X-Permitted-Cross-Domain-Policies: none
```

```
Vary: Accept-Encoding,User-Agent
X-Generator: Drupal 8 (https://www.drupal.org)
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Cache-Control: must-revalidate, no-cache, private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-language: en
X-Drupal-Dynamic-Cache: MISS
Feature-Policy: fullscreen 'none'
X-Drupal-Cache: HIT
Referrer-Policy: no-referrer
Date: Wed, 06 Apr 2022 09:13:25 GMT
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Content-Type: text/html; charset=UTF-8



<!-- THEME DEBUG -->
<!-- THEME HOOK: 'html' -->
<!-- FILE NAME SUGGESTIONS:
   * html--front.html.twig
   * html--node.html.twig
   x html.html.twig
-->
<!-- BEGIN OUTPUT from 'themes/website/templates/html.html.twig' -->
<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>Home | website</title>
    <meta http-equiv="Content-Security-Policy" content="default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval' http://www.google.com">
    <link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/ajax-progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/align.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/autocomplete-loading.module.css?r8d48t"
/>
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/fieldgroup.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/container-inline.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/clearfix.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/details.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/theme
...
...
...

        <div class="d-inline-block">
                <a href="https://dgqadefence.gov.in/sites/default/files/TPI-Clarification-18-Aug-
2020.pdf">CLARIFICATION ON ELIGIBILITY CRITERIA : REGISTRATION OF TPI FIRMS BY DGQA</a>
                <a href="https://dgqadefence.gov.in/sites/default/files/SOP-on-Green-Channel-Status.pdf">STANDARD
OPERATING PROCEDURE GRANT OF GREEN CHANNEL STATUS TO MANUFACTURERS OF DEFENCE STORES &amp;amp; SPARES </a>
                <span>Suggestion/ Feedback to DGQA can be Mailed at        dgqa-sujhav@gov.in Guidelines For ' RM' Awards
For Excellence in Defence and Aerospace Sector, For Any Query Contact 011-23015445 and 011-23019321</span>
        </div>
 </div>
 </section>
               <section class="quick-links text-center" id="main-content-section">
...
...
...
```

Email Address Pattern Found

Severity:	Medium
CVSS Score:	0.0
URL:	https://dgqadefence.gov.in/hi
Entity:	hi (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
GET /hi HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://dgqadefence.gov.in/
Connection: keep-alive
Host: dgqadefence.gov.in
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US
Sec-Fetch-Dest: document


HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-UA-Compatible: IE=edge
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
X-Permitted-Cross-Domain-Policies: none
Vary: Accept-Encoding,User-Agent
X-Generator: Drupal 8 (https://www.drupal.org)
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=96
Cache-Control: must-revalidate, no-cache, private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-language: hi
X-Drupal-Dynamic-Cache: MISS
Feature-Policy: fullscreen 'none'
X-Drupal-Cache: HIT
Referrer-Policy: no-referrer
Date: Wed, 06 Apr 2022 09:13:26 GMT
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Content-Type: text/html; charset=UTF-8



<!-- THEME DEBUG -->
<!-- THEME HOOK: 'html' -->
<!-- FILE NAME SUGGESTIONS:
   * html--front.html.twig
   * html--node.html.twig
   x html.html.twig
-->
<!-- BEGIN OUTPUT from 'themes/website/templates/html.html.twig' -->
<!DOCTYPE html>
<html lang="hi" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
```

```
<meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>मुख्य पृष्ठ | website</title>
    <meta http-equiv="Content-Security-Policy" content="default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval' http://www.google.com">
    <link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/ajax-progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/align.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/autocomplete-loading.module.css?r8d48t"
/>
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/fieldgroup.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/container-inline.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/clearfix.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/details.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/hidden.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/item-list.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/js.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/nowrap.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/position-container.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/reset-appearance.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/resize.module.css?r8d48t" />
...
...
...

        <div class="d-inline-block">
                <a href="https://dgqadefence.gov.in/sites/default/files/TPI-Clarification-18-Aug-
2020.pdf">CLARIFICATION ON ELIGIBILITY CRITERIA : REGISTRATION OF TPI FIRMS BY DGQA</a>
                <a href="https://dgqadefence.gov.in/sites/default/files/SOP-on-Green-Channel-Status.pdf">STANDARD
OPERATING PROCEDURE GRANT OF GREEN CHANNEL STATUS TO MANUFACTURERS OF DEFENCE STORES &amp;amp; SPARES </a>
                <span>Suggestion/ Feedback to DGQA can be Mailed at        dgqa-sujhav@gov.in Guidelines For ' RM' Awards
For Excellence in Defence and Aerospace Sector, For Any Query Contact 011-23015445 and 011-23019321</span>
        </div>
 </div>
 </section>
                      <section class="quick-links text-center" id="main-content-section">
...
...
...
```

Issue 4 of 4

TOC

Email Address Pattern Found

Severity:	Medium
CVSS Score:	0.0
URL:	https://dgqadefence.gov.in/
Entity:	(Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Remove e-mail addresses from the website

Reasoning: The response contains an e-mail address that may be private.

Test Requests and Responses:

```
POST / HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: https://dgqadefence.gov.in/
Connection: keep-alive
```

```
Host: dgqadefence.gov.in
Upgrade-Insecure-Requests: 1
Sec-Fetch-Mode: navigate
Content-Length: 18
Cache-Control: max-age=0
Origin: null
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Sec-Fetch-User: ?1
Accept-Language: en-US
Sec-Fetch-Dest: document
Content-Type: application/x-www-form-urlencoded

custom_search=1234

HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-UA-Compatible: IE=edge
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
X-Permitted-Cross-Domain-Policies: none
Vary: Accept-Encoding,User-Agent
X-Generator: Drupal 8 (https://www.drupal.org)
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=18
Cache-Control: must-revalidate, no-cache, private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-language: en
Feature-Policy: fullscreen 'none'
Referrer-Policy: no-referrer
Date: Wed, 06 Apr 2022 09:13:47 GMT
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Content-Type: text/html; charset=UTF-8



<!-- THEME DEBUG -->
<!-- THEME HOOK: 'html' -->
<!-- FILE NAME SUGGESTIONS:
   * html--front.html.twig
   * html--node.html.twig
   x html.html.twig
-->
<!-- BEGIN OUTPUT from 'themes/website/templates/html.html.twig' -->
<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>Home | website</title>
    <meta http-equiv="Content-Security-Policy" content="default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval' http://www.google.com">
    <link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/ajax-progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/align.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/autocomplete-loading.module.css?r8d48t"
/>
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/fieldgroup.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/container-inline.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/clearfix.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/details.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/hidden.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/item-list.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/js.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/nowrap.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/position-container.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/reset-appearance.module.css?r8d48t" />
<link rel="stylesheet"
...
...
...
```

```
        <div class="d-inline-block">
                <a href="https://dgqadefence.gov.in/sites/default/files/TPI-Clarification-18-Aug-
2020.pdf">CLARIFICATION ON ELIGIBILITY CRITERIA : REGISTRATION OF TPI FIRMS BY DGQA</a>
                <a href="https://dgqadefence.gov.in/sites/default/files/SOP-on-Green-Channel-Status.pdf">STANDARD
OPERATING PROCEDURE GRANT OF GREEN CHANNEL STATUS TO MANUFACTURERS OF DEFENCE STORES &amp;amp; SPARES </a>
                <span>Suggestion/ Feedback to DGQA can be Mailed at        dgqa-sujhav@gov.in Guidelines For ' RM' Awards
For Excellence in Defence and Aerospace Sector, For Any Query Contact 011-23015445 and 011-23019321</span>
        </div>
 </div>
 </section>
               <section class="quick-links text-center" id="main-content-section">
...
...
...
```

M Missing "Content-Security-Policy" header 1 TOC

Issue 1 of 1 TOC

Missing "Content-Security-Policy" header

Severity:	Medium
CVSS Score:	5.0
URL:	https://dgqadefence.gov.in/
Entity:	dgqadefence.gov.in (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
Cause:	Insecure web application programming or configuration
Fix:	Config your server to use the "Content-Security-Policy" header with secure policies

Reasoning: AppScan detected that the Content-Security-Policy response header is missing or with an insecure policy, which increases exposure to various cross-site injection attacks

Test Requests and Responses:

```
GET /themes/website/js/jquery-2.2.4.min.js?v=1.x HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: dgqadefence.gov.in
Sec-Fetch-Mode: no-cors
Content-Length: 0
Accept: */*
Accept-Language: en-US
Sec-Fetch-Dest: script


HTTP/1.1 200 OK
Last-Modified: Tue, 02 Jan 2018 06:39:50 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
Accept-Ranges: bytes
X-Permitted-Cross-Domain-Policies: none
```

```
Content-Length: 85578
Vary: Accept-Encoding,User-Agent
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=78
Cache-Control: max-age=2678400, private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Feature-Policy: fullscreen 'none'
ETag: "14e4a-561c55d943980"
Date: Wed, 06 Apr 2022 09:01:35 GMT
Referrer-Policy: no-referrer
Expires: Wed, 20 Apr 2022 09:01:35 GMT
Content-Type: application/javascript

/*! jQuery v2.2.4 | (c) jQuery Foundation | jquery.org/license */
!function(a,b){"object"==typeof module&&"object"==typeof module.exports?module.exports=a.document?b(a,!0):function(a)
{if(!a.document)throw new Error("jQuery requires a window with a document");return b(a)}:b(a)}("undefined"!=typeof window?
window:this,function(a,b){var c=[],d=a.document,e=c.slice,f=c.concat,g=c.push,h=c.indexOf,i=
{},j=i.toString,k=i.hasOwnProperty,l={},m="2.2.4",n=function(a,b){return new n.fn.init(a,b)},o=/^[\s\uFEFF\xA0]+|
[\s\uFEFF\xA0]+$/g,p=/^-ms-/,q=/-([\da-z])/gi,r=function(a,b){return b.toUpperCase()};n.fn=n.prototype=
{jquery:m,constructor:n,selector:"",length:0,toArray:function(){return e.call(this)},get:function(a){return null!=a?0>a?
this[a+this.length]:this[a]:e.call(this)},pushStack:function(a){var b=n.merge(this.constructor(),a);return
b.prevObject=this,b.context=this.context,b},each:function(a){return n.each(this,a)},map:function(a){return
this.pushStack(n.map(this,function(b,c){return a.call(b,c,b)}))},slice:function(){return
this.pushStack(e.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){return this.eq(-
1)},eq:function(a){var b=this.length,c=+a+(0>a?b:0);return this.pushStack(c>=0&&b>c?[this[c]]:[])},end:function(){return
this.prevObject||this.constructor()},push:g,sort:c.sort,splice:c.splice},n.extend=n.fn.extend=function(){var
a,b,c,d,e,f,g=arguments[0]||{},h=1,i=arguments.length,j=!1;for("boolean"==typeof g&&(j=g,g=arguments[h]||
{},h++),"object"==typeof g||n.isFunction(g)||(g={}),h===i&&(g=this,h--);i>h;h++)if(null!=(a=arguments[h]))for(b in
a)c=g[b],d=a[b],g!==d&&(j&&d&&(n.isPlainObject(d)||(e=n.isArray(d)))?(e?(e=!1,f=c&&n.isArray(c)?c:
[]):f=c&&n.isPlainObject(c)?c:{},g[b]=n.extend(j,f,d)):void 0!==d&&(g[b]=d));return g},n.extend({expando:"jQuery"+
(m+Math.random()).replace(/\D/g,""),isReady:!0,error:function(a){throw new Error(a)},noop:function()
{},isFunction:function(a){return"function"===n.type(a)},isArray:Array.isArray,isWindow:function(a){return
null!=a&&a===a.window},isNumeric:function(a){var b=a&&a.toString();return!n.isArray(a)&&b-
parseFloat(b)+1>=0},isPlainObject:function(a){var
b;if("object"!==n.type(a)||a.nodeType||n.isWindow(a))return!1;if(a.constructor&&!k.call(a,"constructor")&&!k.call(a.constru
ctor.prototype||{},"isPrototypeOf"))return!1;for(b in a);return void 0===b||k.call(a,b)},isEmptyObject:function(a){var
b;for(b in a)return!1;return!0},type:function(a){return null==a?a+"":"object"==typeof a||"function"==typeof a?
i[j.call(a)]||"object":typeof a},globalEval:function(a){var b,c=eval;a=n.trim(a),a&&(1===a.indexOf("use strict")?
(b=d.createElement("script"),b.text=a,d.head.appendChild(b).parentNode.removeChild(b)):c(a))},camelCase:function(a){return
a.replace(p,"ms-").replace(q,r)},nodeName:function(a,b){return
a.nodeName&&a.nodeName.toLowerCase()===b.toLowerCase()},each:function(a,b){var c,d=0;if(s(a))
{for(c=a.length;c>d;d++)if(b.call(a[d],d,a[d])===!1)break}else for(d in a)if(b.call(a[d],d,a[d])===!1)break;return
a},trim:function(a){return null==a?"":(a+"").replace(o,"")},makeArray:function(a,b){var c=b||[];return null!=a&&
(s(Object(a))?n.merge(c,"string"==typeof a?[a]:a):g.call(c,a)),c},inArray:function(a,b,c){return null==b?-
1:h.call(b,a,c)},merge:function(a,b){for(var c=+b.length,d=0,e=a.length;c>d;d++)a[e++]=b[d];return
a.length=e,a},grep:function(a,b,c){for(var d,e=[],f=0,g=a.length,h=!c;g>f;f++)d=!b(a[f],f),d!==h&&e.push(a[f]);return
e},map:function(a,b,c){var d,e,g=0,h=[];if(s(a))for(d=a.length;d>g;g++)e=b(a[g],g,c),null!=e&&h.push(e);else for(g in
a)e=b(a[g],g,c),null!=e&&h.push(e);return f.apply([],h)},guid:1,proxy:function(a,b){var c,d,f;return"string"==typeof b&&
(c=a[b],b=a,a=c),n.isFunction(a)?(d=e.call(arguments,2),f=function(){return
a.apply(b||this,d.concat(e.call(arguments)))},f.guid=a.guid=a.guid||n.guid++,f):void
0},now:Date.now,support:l}),"function"==typeof Sym
...
...
...
```

M Unnecessary Http Response Headers found in the Application 2 TOC

Issue 1 of 2

TOC

Unnecessary Http Response Headers found in the Application

Severity:	Medium
CVSS Score:	5.0
URL:	http://dgqadefence.gov.in/
Entity:	/ (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Do not allow sensitive information to leak.

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.

Test Requests and Responses:

```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: dgqadefence.gov.in
Upgrade-Insecure-Requests: 1
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US


HTTP/1.1 301 Moved Permanently
Location: https://dgqadefence.gov.in
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
Content-Length: 234
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=99
Cache-Control: max-age=2592000
Strict-Transport-Security: max-age=31536000; includeSubDomains
Feature-Policy: fullscreen 'none'
Date: Wed, 06 Apr 2022 09:13:25 GMT
Expires: Fri, 06 May 2022 09:13:25 GMT
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://dgqadefence.gov.in">here</a>.</p>
</body></html>


GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Referer: http://dgqadefence.gov.in/
Host: dgqadefence.gov.in
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US


HTTP/1.1 200 OK
Transfer-Encoding: chunked
X-UA-Compatible: IE=edge
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
X-Permitted-Cross-Domain-Policies: none
Vary: Accept-Encoding,User-Agent
X-Generator: Drupal 8 (https://www.drupal.org)
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
X-Content-Type-Options: nosniff
Cache-Control: must-revalidate, no-cache, private
```

```
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Content-language: en
X-Drupal-Dynamic-Cache: MISS
Feature-Policy: fullscreen 'none'
X-Drupal-Cache: HIT
Referrer-Policy: no-referrer
Date: Wed, 06 Apr 2022 09:13:25 GMT
Expires: Sun, 19 Nov 1978 05:00:00 GMT
Content-Type: text/html; charset=UTF-8



<!-- THEME DEBUG -->
<!-- THEME HOOK: 'html' -->
<!-- FILE NAME SUGGESTIONS:
   * html--front.html.twig
   * html--node.html.twig
   x html.html.twig
-->
<!-- BEGIN OUTPUT from 'themes/website/templates/html.html.twig' -->
<!DOCTYPE html>
<html lang="en" dir="ltr" prefix="content: http://purl.org/rss/1.0/modules/content/  dc: http://purl.org/dc/terms/  foaf:
http://xmlns.com/foaf/0.1/  og: http://ogp.me/ns#  rdfs: http://www.w3.org/2000/01/rdf-schema#  schema: http://schema.org/
sioc: http://rdfs.org/sioc/ns#  sioct: http://rdfs.org/sioc/types#  skos: http://www.w3.org/2004/02/skos/core#  xsd:
http://www.w3.org/2001/XMLSchema# ">
  <head>
    <meta charset="utf-8" />
<meta name="Generator" content="Drupal 8 (https://www.drupal.org)" />
<meta name="MobileOptimized" content="width" />
<meta name="HandheldFriendly" content="true" />
<meta name="viewport" content="width=device-width, initial-scale=1.0" />

    <title>Home | website</title>
    <meta http-equiv="Content-Security-Policy" content="default-src *; style-src 'self' 'unsafe-inline'; script-src 'self'
'unsafe-inline' 'unsafe-eval' http://www.google.com">
    <link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/ajax-progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/align.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/autocomplete-loading.module.css?r8d48t"
/>
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/fieldgroup.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/container-inline.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/clearfix.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/details.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/hidden.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/item-list.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/js.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/nowrap.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/position-container.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/progress.module.css?r8d48t" />
<link rel="stylesheet" media="all" href="/core/themes/stable/css/system/components/reset-appear
...
...
...
```

Issue 2 of 2

TOC

Unnecessary Http Response Headers found in the Application

Severity:	Medium
CVSS Score:	5.0
URL:	https://dgqadefence.gov.in/
Entity:	select2.min.js (Page)
Risk:	It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Cause:	Insecure web application programming or configuration
Fix:	Do not allow sensitive information to leak.

Reasoning: The response contains unnecessary headers, which may help attackers in planning further attacks.

Test Requests and Responses:

```
GET /themes/website/js/select2.min.js?v=1.x HTTP/1.1
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Connection: keep-alive
Host: dgqadefence.gov.in
Sec-Fetch-Mode: no-cors
Accept: */*
Accept-Language: en-US
Sec-Fetch-Dest: script


HTTP/1.1 200 OK
Last-Modified: Mon, 16 Aug 2021 18:49:04 GMT
Connection: Keep-Alive
X-XSS-Protection: 1; mode=block
Server: Apache
X-Forwarded-Host: dgqadefence.gov.in
Accept-Ranges: bytes
X-Permitted-Cross-Domain-Policies: none
Vary: Accept-Encoding,User-Agent
Content-Length: 70851
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Keep-Alive: timeout=5, max=98
Cache-Control: max-age=2678400, private
Strict-Transport-Security: max-age=31536000; includeSubDomains
Strict-Transport-Security: max-age=31536000; includeSubDomains; preload
Feature-Policy: fullscreen 'none'
ETag: "114c3-5c9b1a7bb0800"
Referrer-Policy: no-referrer
Date: Wed, 06 Apr 2022 09:13:25 GMT
Expires: Wed, 20 Apr 2022 09:13:25 GMT
Content-Type: application/javascript

/*! Select2 4.0.13 | https://github.com/select2/select2/blob/master/LICENSE.md */
!function(n){"function"==typeof define&&define.amd?define(["jquery"],n):"object"==typeof module&&module.exports?
module.exports=function(e,t){return void 0===t&&(t="undefined"!=typeof window?require("jquery"):require("jquery")
(e)),n(t),t}:n(jQuery)}(function(u){var e=function(){if(u&&u.fn&&u.fn.select2&&u.fn.select2.amd)var e=u.fn.select2.amd;var
t,n,r,h,o,s,f,g,m,v,y,_,i,a,b;function w(e,t){return i.call(e,t)}function l(e,t){var
n,r,i,o,s,a,l,c,u,d,p,h=t&&t.split("/"),f=y.map,g=f&&f["*"]||{};if(e){for(s=(e=e.split("/")).length-
1,y.nodeIdCompat&&b.test(e[s])&&(e[s]=e[s].replace(b,"")),"."===e[0].charAt(0)&&h&&(e=h.slice(0,h.length-
1).concat(e)),u=0;u<e.length;u++)if("."===(p=e[u]))e.splice(u,1),--u;else if(".."===p)
{if(0===u||1===u&&".."===e[2]||".."===e[u-1])continue;0<u&&(e.splice(u-1,2),u-=2)}e=e.join("/")}if((h||g)&&f){for(u=
(n=e.split("/")).length;0<u;--u){if(r=n.slice(0,u).join("/"),h)for(d=h.length;0<d;--d)if(i=
(i=f[h.slice(0,d).join("/")])&&i[r]){o=i,a=u;break}if(o)break;!l&&g&&g[r]&&(l=g[r],c=u)}!o&&l&&(o=l,a=c),o&&
(n.splice(0,a,o),e=n.join("/"))}return e}function A(t,n){return function(){var e=a.call(arguments,0);return"string"!=typeof
e[0]&&1===e.length&&e.push(null),s.apply(h,e.concat([t,n]))}}function x(t){return function(e){m[t]=e}}function D(e)
{if(w(v,e)){var t=v[e];delete v[e],_[e]=!0,o.apply(h,t)}if(!w(m,e)&&!w(_,e))throw new Error("No "+e);return m[e]}function
c(e){var t,n=e?e.indexOf("!"):-1;return-1<n&&(t=e.substring(0,n),e=e.substring(n+1,e.length)),[t,e]}function S(e){return e?
c(e):[]}return e&&e.requirejs||(e?n=e:e={},m={},v={},y={},_={},i=Object.prototype.hasOwnProperty,a=
[].slice,b=/\.js$/,f=function(e,t){var n,r,i=c(e),o=i[0],s=t[1];return e=i[1],o&&(n=D(o=l(o,s))),o?e=n&&n.normalize?
n.normalize(e,(r=s,function(e){return l(e,r)})):l(e,s):(o=(i=c(e=l(e,s)))[0],e=i[1],o&&(n=D(o))),{f:o?
o+"!"+e:e,n:e,pr:o,p:n}},g={require:function(e){return A(e)},exports:function(e){var t=m[e];return void 0!==t?t:m[e]=
{}},module:function(e){return{id:e,uri:"",exports:m[e],config:(t=e,function(){return y&&y.config&&y.config[t]||{}})}};var
t},o=function(e,t,n,r){var i,o,s,a,l,c,u,d=[],p=typeof n;if(c=S(r=r||e),"undefined"==p||"function"==p)
{for(t=!t.length&&n.length?["require","exports","module"]:t,l=0;l<t.length;l+=1)if("require"===(o=
(a=f(t[l],c)).f))d[l]=g.require(e);else if("exports"===o)d[l]=g.exports(e),u=!0;else
if("module"===o)i=d[l]=g.module(e);else if(w(m,o)||w(v,o)||w(_,o))d[l]=D(o);else{if(!a.p)throw new Error(e+" missing
"+o);a.p.load(a.n,A(r,!0),x(o),{}),d[l]=m[o]}s=n?n.apply(m[e],d):void 0,e&&(i&&i.exports!==h&&i.exports!==m[e]?
m[e]=i.exports:s===h&&u||(m[e]=s))}else e&&(m[e]=n)},t=n=s=function(e,t,n,r,i){if("string"==typeof e)return g[e]?g[e]
(t):D(f(e,S(t)).f);if(!e.splice){if((y=e).deps&&s(y.deps,y.callback),!t)return;t.splice?(e=t,t=n,n=null):e=h}return
t=t||function(){},"function"==typeof n&&(n=r,r=i),r?o(h,e,t,n):setTimeout(function(){o(h,e,t,n)},4),s},s.config=function(e)
{return s(e)},t._defined=m,(r=function(e,t,n){if("string"!=typeof e)throw new Error("See almond README: incorrect module
build, no module name");t.splice||(n=t,t=[]),w(m,e)||w(v,e)||(v[e]=[e,t,n])}).amd=
{jQuery:!0},e.requirejs=t,e.require=n,e.define=r),e.define("almond",function(){}),e.define("jquery",[],function(){var
e=u||$;return null==e&&console&&console.error&&console.error("Select2: An instance of jQuery or a jQuery-compatible library
was not found. Make sure that you are including jQuery before Select2 on your web page."),e}),e.define("select2/utils",
["jquery"],function(o){var i={};function u(e){var t=e.prototype,n=[];for(var r in t){"function"==typeof
t[r]&&"constructor"!==r&&n.push(r)}return n}i.Extend=function(e,t){var n={}.hasOwnProperty;function r()
{this.constructor=e}for(var i in t)n.call(t,i)&&(e[i]=t[i]);return r.protot
...
...
...
```

How to Fix

Email Address Pattern Found

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
Spambots crawl internet sites, set out to find e-mail addresses in order to build mailing lists for sending unsolicited e-mail (spam).
AppScan detected a response containing one or more e-mail addresses, which may be exploited to send spam mail
Furthermore, the e-mail addresses found may be private and thus should not be accessible to the general public.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Remove any e-mail addresses from the website so that they won't be exploited by malicious users.

CWE:

359

External References:

Definition of Spambot (Wikipedia)

Missing "Content-Security-Policy" header

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web application such as usernames, passwords, machine name and/or sensitive file locations
It is possible to persuade a naive user to supply sensitive information such as username, password, credit card number, social security number etc.
The absence or improper values of CSP can cause the web application being vulnerable to XSS, clickjacking, etc.
The "Content-Security-Policy" header is designed to modify the way browsers render pages, and thus to protect from various cross-site injections, including Cross-Site Scripting. It is important to set the header value correctly, in a way that will not prevent proper operation of the web site. For example, if the header is set to prevent execution of inline JavaScript, the web site must not use inline JavaScript in its pages.
To protect against Cross-Site Scripting, Cross-Frame Scripting and clickjacking, it is important to set the following policies with proper values:
Both of 'default-src' and 'frame-ancestors' policies, *OR* all of 'script-src', 'object-src' and 'frame-ancestors' policies.
For 'default-src', 'script-src' and 'object-src', insecure values such as '*', 'data:', 'unsafe-inline' or 'unsafe-eval' should be avoided.
For 'frame-ancestors', insecure values such as '*' or 'data:' should be avoided.
Please refer the following links for more information.
Please note that “Content-Security-Policy” includes four different tests. A general test that verifies if the "Content-Security-Policy" header is being used and three additional tests that check if "Frame-Ancestors", "Object-Src" and "Script-Src" were configured correctly.

Affected Products:

This issue may affect different types of products

Fix Recommendation:

General

Configure your server to send the "Content-Security-Policy" header.
It is recommended to configure Content-Security-Policy header with secure values for its directives as below:
For 'default-src', 'script-src' and 'object-src', secure values such as 'none', 'self', https://any.example.com.
For 'frame-ancestors', secure values such as 'self', 'none' or https://any.example.com were expected.
"unsafe-inline" and "unsafe-eval" must not be used in any circumstance. Using nonce / hash would be only considered for short-term workaround.
For Apache, see:
http://httpd.apache.org/docs/2.2/mod/mod_headers.html
For IIS, see:
https://technet.microsoft.com/pl-pl/library/cc753133%28v=ws.10%29.aspx
For nginx, see:
http://nginx.org/en/docs/http/ngx_http_headers_module.html

CWE:

1032

External References:

List of some secure Headers
An Introduction to Content Security Policy
MDN web docs - Content-Security-Policy

Unnecessary Http Response Headers found in the Application

TOC

Cause:

Insecure web application programming or configuration

Risk:

It is possible to gather sensitive information about the web server type, version, OS and more.
AppScan detected a Http response header that is unnecessary.
For reasons of security and privacy, The Http response headers like "Server", "X-Powered-By", "X-AspNetMvc-Version" and "X-AspNet-Version" should not appear in web pages.
The "Server" header is a header that is added usually by default whenever a response is sent to the client by the server.
The "X-Powered-By" header is a header that might be added by default whenever a response is sent to the client by the server.
These added header(s) may reveal sensitive information about the internal server software version and type, thus enabling attackers to fingerprint it and attack it with targeted exploits. Moreover, when a new exploit becomes known to the public, the server will most likely get attacked with it.

Affected Products:

This issue may affect different types of products.

Fix Recommendation:

General

Configure your server to remove the default "Server" header from being sent to all outgoing requests.
For IIS, see:
Set IIS response headers
For nginx, see:
Set nginx response headers
For Weblogic, see:
Set Weblogic response headers
For Apache, see:
Set Apache response headers

CWE:

200

External References:

Fingerprinting
Preventing Information Leakage

Application Data

Visited URLs 136

TOC

URL
http://dgqadefence.gov.in/
https://dgqadefence.gov.in/
https://dgqadefence.gov.in/themes/website/js/jquery-2.2.4.min.js?v=1.x
https://dgqadefence.gov.in/themes/website/js/bootstrap.min.js?v=1.x
https://dgqadefence.gov.in/themes/website/js/select2.min.js?v=1.x
https://dgqadefence.gov.in/themes/website/js/owl.carousel.js?v=1.x
https://dgqadefence.gov.in/themes/website/js/mCustomScrollbar.concat.min.js?v=1.x
https://dgqadefence.gov.in/themes/website/js/custom.js?v=1.x
https://dgqadefence.gov.in/themes/website/js/jquery-2.2.4.min.js
https://dgqadefence.gov.in/themes/website/js/bootstrap.min.js
https://dgqadefence.gov.in/themes/website/js/owl.carousel.js
https://dgqadefence.gov.in/themes/website/js/select2.min.js
https://dgqadefence.gov.in/themes/website/js/mCustomScrollbar.concat.min.js
https://dgqadefence.gov.in/core/assets/vendor/jquery-once/jquery.once.min.js?v=2.2.3
https://dgqadefence.gov.in/core/misc/drupalSettingsLoader.js?v=8.9.16
https://dgqadefence.gov.in/themes/website/js/custom.js
https://dgqadefence.gov.in/core/misc/drupal.js?v=8.9.16
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/form-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/jquery-1-7-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery/jquery.min.js?v=3.5.1
https://dgqadefence.gov.in/core/misc/drupal.init.js?v=8.9.16
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/escape-selector-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/labels-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/unique-id-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/data-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/safe-active-element-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/plugin-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/safe-blur-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/keycode-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/disable-selection-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/scroll-parent-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/form-reset-mixin-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/version-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/tabbable-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/checkboxradio-min.js?v=1.12.1

https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/ie-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/focusable-min.js?v=1.12.1
https://dgqadefence.gov.in/core/misc/displace.js?v=8.9.16
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/mouse-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widget-min.js?v=1.12.1
https://dgqadefence.gov.in/core/misc/debounce.js?v=8.9.16
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/controlgroup-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/button-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/draggable-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/position-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/resizable-min.js?v=1.12.1
https://dgqadefence.gov.in/core/assets/vendor/jquery.ui/ui/widgets/dialog-min.js?v=1.12.1
https://dgqadefence.gov.in/core/misc/dialog/dialog.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/dialog/dialog.position.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/dialog/dialog.jquery-ui.js?v=8.9.16
https://dgqadefence.gov.in/modules/external_link_popup/js/dialog.js?v=8.9.16
https://dgqadefence.gov.in/modules/password_encrypt/js/password_encrypt.js?v=8.9.16
https://dgqadefence.gov.in/libraries/CryptoJS/aes.js?v=8.9.16
https://dgqadefence.gov.in/libraries/jquery.cycle/jquery.cycle.all.js?v=3.0.3
https://dgqadefence.gov.in/modules/views_slideshow/modules/views_slideshow_cycle/js/views_slideshow_cycle.js?r8d48t
https://dgqadefence.gov.in/modules/views_slideshow/js/views_slideshow.js?v=8.9.16
https://dgqadefence.gov.in/
https://dgqadefence.gov.in/hi
https://dgqadefence.gov.in/sites/default/files/languages/hi_dyEQOJZVyVr17FM0bx-G4Vd5XDf7sCvyOHVYjHVOsxo.js?r8d48t
https://dgqadefence.gov.in/dgqa-overview
https://dgqadefence.gov.in/dgqa-overview
https://dgqadefence.gov.in/screen-header-access
https://dgqadefence.gov.in/who-is-who
https://dgqadefence.gov.in/who-is-who
https://dgqadefence.gov.in/hi/technical-directorate
https://dgqadefence.gov.in/hi/screen-header-access
https://dgqadefence.gov.in/HPTD
https://dgqadefence.gov.in/core/misc/progress.js?v=8.9.16
https://dgqadefence.gov.in/core/assets/vendor/jquery-form/jquery.form.min.js?v=4.22
https://dgqadefence.gov.in/core/modules/responsive_image/js/responsive_image.ajax.js?v=8.9.16
https://dgqadefence.gov.in/core/modules/views/js/base.js?v=8.9.16
https://dgqadefence.gov.in/core/themes/stable/js/ajax.js?v=8.9.16
https://dgqadefence.gov.in/core/modules/views/js/ajax_view.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/ajax.js?v=8.9.16
https://dgqadefence.gov.in/technical-directorate
https://dgqadefence.gov.in/our-dg
https://dgqadefence.gov.in/hi/vigilance
https://dgqadefence.gov.in/hi/citizen-charter
https://dgqadefence.gov.in/hi/HPTD
https://dgqadefence.gov.in/index.php/hi/our-dg
https://dgqadefence.gov.in/location
https://dgqadefence.gov.in/core/assets/vendor/underscore/underscore-min.js?v=1.13.1
https://dgqadefence.gov.in/core/assets/vendor/backbone/backbone-min.js?v=1.4.0
https://dgqadefence.gov.in/modules/shs/js/shs.js?v=8.9.16

https://dgqadefence.gov.in/modules/shs/js/models/WidgetModel.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/models/ContainerModel.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/models/WidgetItemOptionModel.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/views/ContainerView.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/models/AppModel.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/models/WidgetItemModel.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/views/WidgetView.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/views/WidgetItemView.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/views/AddNewView.js?v=8.9.16
https://dgqadefence.gov.in/modules/shs/js/views/AppView.js?v=8.9.16
https://dgqadefence.gov.in/shs-term-data/shs-nid/location/0
https://dgqadefence.gov.in/location?term_node_tid_depth=All
https://dgqadefence.gov.in/rti
https://dgqadefence.gov.in/green-channel-policy
https://dgqadefence.gov.in/self-certification-status
https://dgqadefence.gov.in/tpi-implementation
https://dgqadefence.gov.in/dtis
https://dgqadefence.gov.in/recruitment
https://dgqadefence.gov.in/index.php/defence-dashboard
https://dgqadefence.gov.in/form/feedback
https://dgqadefence.gov.in/modules/webform/js/webform.element.details.save.js?v=8.9.16
https://dgqadefence.gov.in/modules/webform/js/webform.element.message.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/states.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/form.js?v=8.9.16
https://dgqadefence.gov.in/modules/webform/js/webform.behaviors.js?v=8.9.16
https://dgqadefence.gov.in/modules/webform/js/webform.element.select.js?v=8.9.16
https://dgqadefence.gov.in/modules/webform/js/webform.states.js?v=8.9.16
https://dgqadefence.gov.in/modules/webform/js/webform.form.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/announce.js?v=8.9.16
https://dgqadefence.gov.in/modules/webform/js/webform.element.details.toggle.js?v=8.9.16
https://dgqadefence.gov.in/form/feedback
https://dgqadefence.gov.in/form/feedback/confirmation?token=AdQDVQs73U2OzvKz7HX_Lw67spSmPmS6lCUt7T-n3-s
https://dgqadefence.gov.in/privacy-policy
https://dgqadefence.gov.in/
https://dgqadefence.gov.in/modules/views_slideshow/modules/views_slideshow_cycle/js/views_slideshow_cycle.js?r8d48t
https://dgqadefence.gov.in/libraries/jquery.cycle/jquery.cycle.all.js?v=3.0.3
https://dgqadefence.gov.in/modules/views_slideshow/js/views_slideshow.js?v=8.9.16
https://dgqadefence.gov.in/dtis
https://dgqadefence.gov.in/allotment-of-proof-ranges
https://dgqadefence.gov.in/citizen-charter
https://dgqadefence.gov.in/recruitment
https://dgqadefence.gov.in/core/misc/progress.js?v=8.9.16
https://dgqadefence.gov.in/core/modules/responsive_image/js/responsive_image.ajax.js?v=8.9.16
https://dgqadefence.gov.in/core/themes/stable/js/ajax.js?v=8.9.16
https://dgqadefence.gov.in/core/misc/ajax.js?v=8.9.16
https://dgqadefence.gov.in/core/modules/big_pipe/js/big_pipe.js?v=8.9.16
https://dgqadefence.gov.in/themes/website/js/jquery-2.2.4.min.js
https://dgqadefence.gov.in/themes/website/js/bootstrap.min.js
https://dgqadefence.gov.in/themes/website/js/owl.carousel.js

https://dgqadefence.gov.in/themes/website/js/select2.min.js
https://dgqadefence.gov.in/themes/website/js/mCustomScrollbar.concat.min.js
https://dgqadefence.gov.in/themes/website/js/custom.js

Failed Requests 4

TOC

URL	Reason
https://dgqadefence.gov.in/libraries/json2/json2.js?v=2	Response Status '404' - Not Found
https://dgqadefence.gov.in/libraries/jquery.hoverIntent/jquery.hoverIntent.js?v=1.9	Response Status '404' - Not Found
https://dgqadefence.gov.in/libraries/json2/json2.js?v=2	Response Status '404' - Not Found
https://dgqadefence.gov.in/libraries/jquery.hoverIntent/jquery.hoverIntent.js?v=1.9	Response Status '404' - Not Found