Affected Items Report

Security Audit

Robin Roy
robin113x@gmail.com
+91-6201297211

Scan of www.apnacollege.in

Scan details

Scan information	
Start time	2022-07-21T20:23:27.128271+00:00
Start url	https://www.apnacollege.in
Host	www.apnacollege.in
Scan time	374 minutes, 48 seconds
Profile	Full Scan
Responsive	True
Server OS	Unknown
Application build	14.8.220606174

Threat level

Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	11
High	2
Medium	0
Low	5
Informational	4

Affected items

Web Server	
Alert group	**Cross site scripting**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	URI was set to **ö"onmouseover=RXwB(97585)//** The input is reflected inside a tag parameter between double quotes.

```
GET
/home/%F6%22%6F%6E%6D%6F%75%73%65%6F%76%65%72%3D%52%58%77%42%28%39%37%35%38%35%29%2F%2F
HTTP/1.1

Referer: https://www.apnacollege.in/

Cookie: slim_session=8EHh17GLvccnTmGhdPDssDO1NCK8Jr2praVWfQz4

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**Cross site scripting (verified)**
Severity	High
Description	Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
Recommendations	Apply context-dependent encoding and/or validation to user input rendered on a page
Alert variants	
Details	Path Fragment input **/[*]/<s>** was set to **pages%22onmouseover=cHJ7(94292)%22** The input is reflected inside a tag parameter between double quotes.

```
GET /pages%22onmouseover=cHJ7(94292)%22/terms HTTP/1.1

Referer: https://www.apnacollege.in/

Cookie: slim_session=8EHh17GLvccnTmGhdPDssDO1NCK8Jr2praVWfQz4

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**Clickjacking: X-Frame-Options header**
Severity	Low
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 did not return an **X-Frame-Options** header with the value DENY or SAMEORIGIN, 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 untrusted sites.
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	Paths without secure XFO header: • https://www.apnacollege.in/ • https://www.apnacollege.in/payment • https://www.apnacollege.in/liquid/navigationMenu1 • https://www.apnacollege.in/liquid/basicComponentTemplate • https://www.apnacollege.in/error • https://www.apnacollege.in/bundles • https://www.apnacollege.in/liquid/coursecard1-2 • https://www.apnacollege.in/all-courses • https://www.apnacollege.in/home • https://www.apnacollege.in/home-post-login • https://www.apnacollege.in/privacy • https://www.apnacollege.in/refund-policy • https://www.apnacollege.in/terms • https://www.apnacollege.in/cookies • https://www.apnacollege.in/subscriptions • https://www.apnacollege.in/thankyou • https://www.apnacollege.in/faqs • https://www.apnacollege.in/home-old • https://www.apnacollege.in/course/placement-course-java • https://www.apnacollege.in/liquid/{{%20item.linkData.href%20}} • https://www.apnacollege.in/liquid/{{%20subItem.linkData.href%20}}

```
GET / HTTP/1.1

Referer: https://www.apnacollege.in/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**Cookies without HttpOnly flag set (verified)**
Severity	Low
Description	One or more cookies don't 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.
Recommendations	If possible, you should set the HttpOnly flag for these cookies.
Alert variants	

Details	Cookies without HttpOnly flag set:
	• https://www.apnacollege.in/api/users
	`Set-Cookie: lw_tokens=; path=/; expires=Wed, 20-Jul-2022 23:50:3`
	• https://www.apnacollege.in/api/users
	`Set-Cookie: lw_tokens=; path=/; expires=Thu, 21-Jul-2022 02:04:2`

```
GET /api/users HTTP/1.1

Referer: https://www.apnacollege.in/

Cookie: slim_session=8EHh17GLvccnTmGhdPDssDO1NCK8Jr2praVWfQz4

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

/bundles	
Alert group	**Insecure Inline Frame (iframe) (verified)**
Severity	Low
Description	The web page was found to be using an Inline Frame ("iframe") to embed a resource, such as a different web page. The Inline Frame is either configured insecurely, or not as securely as expected. This vulnerability alert is based on the origin of the embedded resource and the iframe's sandbox attribute, which can be used to apply security restrictions as well as exceptions to these restrictions.
Recommendations	Review the iframe's purpose and environment, and use the sandbox attribute to secure the iframe while applying sandbox directives to ease security restrictions if necessary.
Alert variants	
Details	An iframe tag references an external resource, and no sandbox attribute is set.

```
GET /bundles?bundle_id= HTTP/1.1

Referer: https://www.apnacollege.in/

Cookie: slim_session=8EHh17GLvccnTmGhdPDssDO1NCK8Jr2praVWfQz4

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**Sensitive pages could be cached**
Severity	Low

Description	One or more pages contain possible sensitive information (e.g. a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified.
Recommendations	Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header.
Alert variants	
Details	List of pages that could be cached: • https://www.apnacollege.in/payment?cf_phonenumber=555-666-0606&email=sample@email.tst&password=g00dPa$$w0rD&username=WjrfVCgh

```
GET /payment?cf_phonenumber=555-666-
0606&email=sample%40email.tst&password=g00dPa%24%24w0rD&username=WjrfVCgh HTTP/1.1

Referer: https://www.apnacollege.in/payment

Cookie: slim_session=8EHh17GLvccnTmGhdPDssDO1NCK8Jr2praVWfQz4

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**TLS/SSL certificate about to expire**
Severity	Low
Description	One of the TLS/SSL certificates used by your server is about to expire. Once the certificate has expired, most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server. This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.
Recommendations	Contact your Certificate Authority to renew the SSL certificate.
Alert variants	
Details	The TLS/SSL certificate (serial: 04f96d2be13df4a895d87119c5eb9e3582a7) will expire in less than **60** days. The certificate validity period is from **Mon Jun 20 2022 07:20:04 GMT+0000 (Coordinated Universal Time)** to **Sun Sep 18 2022 07:20:03 GMT+0000 (Coordinated Universal Time)** (58 days left)

Web Server

Alert group	Content Security Policy (CSP) not implemented
Severity	Informational

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.

Recommendations	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.
Alert variants	

Details	Paths without CSP header: • https://www.apnacollege.in/ • https://www.apnacollege.in/payment • https://www.apnacollege.in/liquid/navigationMenu1 • https://www.apnacollege.in/liquid/basicComponentTemplate • https://www.apnacollege.in/error • https://www.apnacollege.in/bundles • https://www.apnacollege.in/liquid/coursecard1-2 • https://www.apnacollege.in/all-courses • https://www.apnacollege.in/home • https://www.apnacollege.in/home-post-login • https://www.apnacollege.in/privacy • https://www.apnacollege.in/refund-policy • https://www.apnacollege.in/terms • https://www.apnacollege.in/cookies • https://www.apnacollege.in/subscriptions • https://www.apnacollege.in/thankyou • https://www.apnacollege.in/faqs • https://www.apnacollege.in/home-old • https://www.apnacollege.in/course/placement-course-java • https://www.apnacollege.in/liquid/{{%20item.linkData.href%20}} • https://www.apnacollege.in/liquid/{{%20subItem.linkData.href%20}}

```
GET / HTTP/1.1

Referer: https://www.apnacollege.in/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**Email addresses**
Severity	Informational
Description	One or more email addresses have been found on this website. 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.
Recommendations	Check references for details on how to solve this problem.
Alert variants	

Details	Emails found: • https://www.apnacollege.in/ **hello@apnacollege.in** • https://www.apnacollege.in/payment **hello@apnacollege.in** • https://www.apnacollege.in/error **hello@apnacollege.in** • https://www.apnacollege.in/bundles **hello@apnacollege.in** • https://www.apnacollege.in/all-courses **hello@apnacollege.in** • https://www.apnacollege.in/home **hello@apnacollege.in** • https://www.apnacollege.in/home-post-login **hello@apnacollege.in** • https://www.apnacollege.in/privacy **hello@apnacollege.in** • https://www.apnacollege.in/refund-policy **hello@apnacollege.in** • https://www.apnacollege.in/terms **hello@apnacollege.in** • https://www.apnacollege.in/cookies **hello@apnacollege.in** • https://www.apnacollege.in/subscriptions **hello@apnacollege.in** • https://www.apnacollege.in/thankyou **hello@apnacollege.in** • https://www.apnacollege.in/faqs **hello@apnacollege.in** • https://www.apnacollege.in/home-old **hello@apnacollege.in** • https://www.apnacollege.in/course/placement-course-java **hello@apnacollege.in**

```
GET / HTTP/1.1

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**HTTP Strict Transport Security (HSTS) not following best practices**
Severity	Informational
Description	HTTP Strict Transport Security (HSTS) instructs a web browser to only connect to a web site using HTTPS. It was detected that your web application's HTTP Strict Transport Security (HSTS) implementation is not as strict as is typically advisable.

Recommendations	It is recommended to implement best practices of HTTP Strict Transport Security (HSTS) in your web application. Consult web references for more information.
Alert variants	
Details	URLs where HSTS configuration is not according to best practices: • https://www.apnacollege.in/ - max-age is less that 1 year (31536000); • https://www.apnacollege.in/payment - max-age is less that 1 year (31536000); • https://www.apnacollege.in/liquid/navigationMenu1 - max-age is less that 1 year (31536000); • https://www.apnacollege.in/liquid/basicComponentTemplate - max-age is less that 1 year (31536000); • https://www.apnacollege.in/error - max-age is less that 1 year (31536000); • https://www.apnacollege.in/bundles - max-age is less that 1 year (31536000); • https://www.apnacollege.in/liquid/coursecard1-2 - max-age is less that 1 year (31536000); • https://www.apnacollege.in/all-courses - max-age is less that 1 year (31536000); • https://www.apnacollege.in/home - max-age is less that 1 year (31536000); • https://www.apnacollege.in/home-post-login - max-age is less that 1 year (31536000); • https://www.apnacollege.in/privacy - max-age is less that 1 year (31536000); • https://www.apnacollege.in/refund-policy - max-age is less that 1 year (31536000); • https://www.apnacollege.in/terms - max-age is less that 1 year (31536000); • https://www.apnacollege.in/cookies - max-age is less that 1 year (31536000); • https://www.apnacollege.in/subscriptions - max-age is less that 1 year (31536000); • https://www.apnacollege.in/thankyou - max-age is less that 1 year (31536000); • https://www.apnacollege.in/faqs - max-age is less that 1 year (31536000); • https://www.apnacollege.in/home-old - max-age is less that 1 year (31536000); • https://www.apnacollege.in/course/placement-course-java - max-age is less that 1 year (31536000); • https://www.apnacollege.in/liquid/{{%20item.linkData.href%20}} - max-age is less that 1 year (31536000); • https://www.apnacollege.in/liquid/{{%20subItem.linkData.href%20}} - max-age is less that 1 year (31536000);

```
GET / HTTP/1.1

Referer: https://www.apnacollege.in/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```

Web Server	
Alert group	**Subresource Integrity (SRI) not implemented**
Severity	Informational

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.

Recommendations	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/uxy9rx7HN`
	`crossorigin="anonymous"></script>`

Alert variants	
Details	Pages where SRI is not implemented: • https://www.apnacollege.in/ Script SRC: **https://ajax.googleapis.com/ajax/libs/webfont/1.6.26/webfont.js** • https://www.apnacollege.in/ Script SRC: **https://cdn.mycourse.app/v2.1.9/commonjs/jquery-1.8.0.min.js** • https://www.apnacollege.in/ Script SRC: **https://www.googletagmanager.com/gtag/js?id=G-VPHPY6NJ60** • https://www.apnacollege.in/ Script SRC: **https://d2wy8f7a9ursnm.cloudfront.net/v7/bugsnag.min.js**

```
GET / HTTP/1.1

Referer: https://www.apnacollege.in/

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

Accept-Encoding: gzip,deflate,br

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.4896.127 Safari/537.36

Host: www.apnacollege.in

Connection: Keep-alive
```