



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.

Scan Detail

Target	https://ths100.in/
Scan Type	hardend
Start Time	Sep 25, 2024, 8:37:39 AM GMT
Scan Duration	1 hour, 19 minutes
Requests	83137
Average Response Time	59ms
Maximum Response Time	31868ms
Application Build	v24.1.240111130
Authentication Profile	-

0

Critical

0

High

2






Medium

6

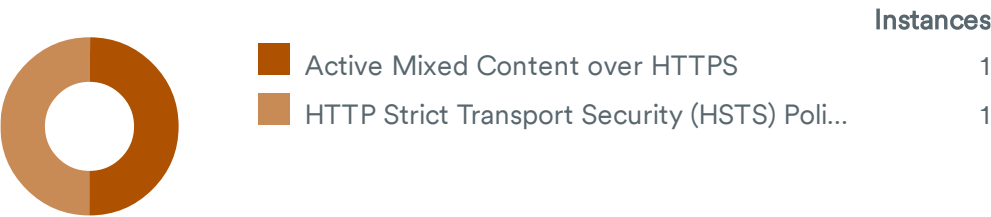
Low

5

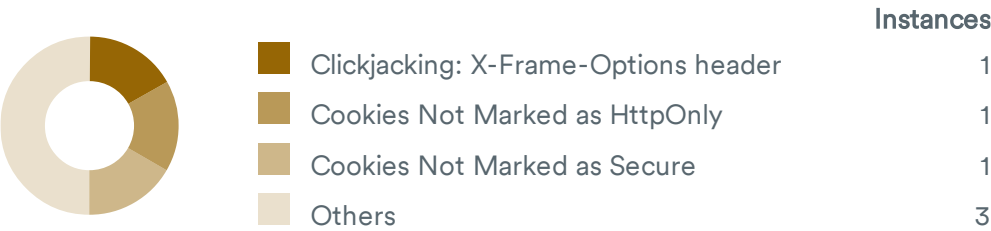
Informational

Severity	Vulnerabilities	Instances
 Critical	0	0
 High	0	0
 Medium	2	2
 Low	5	6
 Informational	5	5
Total	12	13

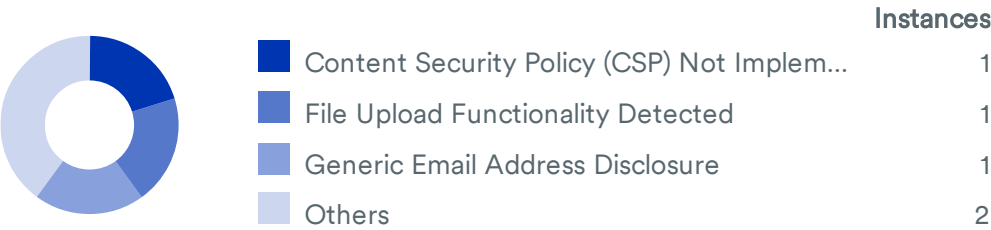
Medium Severity















Low Severity



Informational



Impacts

SEVERITY	IMPACT
 Medium	1 Active Mixed Content over HTTPS
 Medium	1 HTTP Strict Transport Security (HSTS) Policy Not Enabled
 Low	1 Clickjacking: X-Frame-Options header
 Low	1 Cookies Not Marked as HttpOnly
 Low	1 Cookies Not Marked as Secure
 Low	1 Cookies with missing, inconsistent or contradictory properties
 Low	2 Insecure Frame (External)
 Informational	1 Content Security Policy (CSP) Not Implemented
 Informational	1 File Upload Functionality Detected
 Informational	1 Generic Email Address Disclosure
 Informational	1 Permissions-Policy header not implemented
 Informational	1 Web Application Firewall Detected

Active Mixed Content over HTTPS

Active Content is a resource which can run in the context of your page and moreover can alter the entire page. If the HTTPS page includes active content like scripts or stylesheets retrieved through regular, cleartext HTTP, then the connection is only partially encrypted. The unencrypted content is accessible to sniffers.

Impact

A man-in-the-middle attacker can intercept the request for the HTTP content and also rewrite the response to include malicious codes. Malicious active content can steal the user's credentials, acquire sensitive data about the user, or attempt to install malware on the user's system (by leveraging vulnerabilities in the browser or its plugins, for example), and therefore the connection is not safeguarded anymore.

<https://ths100.in/>

The following issues were detected:

- The tag `link` references the resource `http://gmpg.org/xfn/11`

Request

```
GET / HTTP/1.1
Referer: https://ths100.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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive
```

Recommendation

There are two technologies to defense against the mixed content issues: - HTTP Strict Transport Security (HSTS) is a mechanism that enforces secure resource retrieval, even in the face of user mistakes (attempting to access your web site on port 80) and implementation errors (your developers place an insecure link into a secure page) - Content Security Policy (CSP) can be used to block insecure resource retrieval from third-party web sites - Last but not least, you can use "protocol relative URLs" to have the user's browser automatically choose HTTP or HTTPS as appropriate, depending on which protocol the user is connected with. For example: A protocol relative URL to load an style would look like `>link rel="stylesheet" href="//example.com/style.css"<`. Same for scripts `>script type="text/javascript"`

src="//example.com/code.js"<>/script< The browser will automatically add either "http:" or "https:" to the start of the URL, whichever is appropriate.

References

[MDN: Mixed Content](https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content)

https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

[What is mixed content?](https://web.dev/what-is-mixed-content/)

<https://web.dev/what-is-mixed-content/>

[Fixing mixed content](https://web.dev/fixing-mixed-content/)

<https://web.dev/fixing-mixed-content/>

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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 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

<https://ths100.in/>

URLs where HSTS is not enabled:

- <https://ths100.in/>
- <https://ths100.in/9707507>
- <https://ths100.in/wp-json/oembed/1.0/embed>
- <https://ths100.in/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css>
- <https://ths100.in/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css>
- <https://ths100.in/xmlrpc.php>
- <https://ths100.in/wp-includes/js/jquery/ui/core.min.js>
- <https://ths100.in/comments/feed/>
- <https://ths100.in/announcement-and-news/>
- <https://ths100.in/admission/>
- <https://ths100.in/wp-content/plugins/revslider/public/assets/css/rs6.css>
- <https://ths100.in/contact/>
- <https://ths100.in/blog>

- <https://ths100.in/down-memory-lane/>
- <https://ths100.in/wp-includes/js/dist/api-fetch.min.js>
- <https://ths100.in/wp-content/themes/eduma/assets/css/v4-shims.min.css>
- <https://ths100.in/feed/>
- <https://ths100.in/headmaster/>
- <https://ths100.in/our-school/>
- <https://ths100.in/teachers-staffs/>
- <https://ths100.in/wp-json/wp/v2/pages/4524>

Request

```
GET / HTTP/1.1
Referer: https://ths100.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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive
```

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/>

[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>

Clickjacking: X-Frame-Options header

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.

Impact

The impact depends on the affected web application.

<https://ths100.in/>

Paths without secure XFO header:

- <https://ths100.in/>
- <https://ths100.in/9707507>
- <https://ths100.in/wp-json/oembed/1.0/embed>
- <https://ths100.in/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css>
- <https://ths100.in/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css>
- <https://ths100.in/wp-includes/js/jquery/ui/core.min.js>
- <https://ths100.in/xmlrpc.php>
- <https://ths100.in/comments/feed/>
- <https://ths100.in/announcement-and-news/>
- <https://ths100.in/admission/>
- <https://ths100.in/wp-content/plugins/revslider/public/assets/css/rs6.css>
- <https://ths100.in/contact/>
- <https://ths100.in/blog>
- <https://ths100.in/down-memory-lane/>
- <https://ths100.in/wp-includes/js/dist/api-fetch.min.js>
- <https://ths100.in/wp-content/themes/eduma/assets/css/v4-shims.min.css>
- <https://ths100.in/feed/>
- <https://ths100.in/headmaster/>

- <https://ths100.in/our-school/>
- <https://ths100.in/teachers-staffs/>
- <https://ths100.in/wp-json/wp/v2/pages/4524>

Request

GET / HTTP/1.1
Referer: <https://ths100.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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive

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>

Cookies Not Marked as HttpOnly

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.

Impact

Cookies can be accessed by client-side scripts.

<https://ths100.in/>

Verified

Cookies without HttpOnly flag set:

- <https://ths100.in/wp-comments-post.php>

```
Set-Cookie: comment_author_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; path=/
```

- <https://ths100.in/wp-comments-post.php>

```
Set-Cookie: comment_author_email_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; path=/
```

- <https://ths100.in/wp-comments-post.php>

```
Set-Cookie: comment_author_url_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; path=/
```

Request

```
POST /wp-comments-post.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://ths100.in/guardians-of-the-globe-project/
Cookie: wssplashuid=aff28dec62bf4544744fa0c94cad94c30f3d8fbd.1727257240.0
Content-Length: 140
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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive

attachment=&author=1&comment=555&comment_parent=0&comment_post_ID=14086&email=testing%40example.com&submit=Submit&url=http://www.example.com
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies Not Marked as Secure

One or more cookies 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.

<https://ths100.in/>

Verified

Cookies without Secure flag set:

- <https://ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f>

```
Set-Cookie: wssplashuid=084bf393ffae21d9fc183cb2a83c025a74feb4da.1727257197.1;  
Path=/; Domain=ths100.in; Max-Age=3600; HttpOnly; SameSite=Lax
```

- <https://ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f>

```
Set-Cookie: wssplashuid=aff28dec62bf4544744fa0c94cad94c30f3d8fbd.1727257240.0;  
Path=/; Domain=ths100.in; Max-Age=3600; HttpOnly; SameSite=Lax
```

- <https://ths100.in/wp-comments-post.php>

```
Set-Cookie: comment_author_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-  
Sep-2023 09:20:16 GMT; Max-Age=0; path=/  

```

- <https://ths100.in/wp-comments-post.php>

```
Set-Cookie: comment_author_email_18550296b023cec14e4257cfa9551987=%20;  
expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; path=/  

```

- <https://ths100.in/wp-comments-post.php>

Set-Cookie: comment_author_url_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; path=/

Request

```
GET /z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?
id=7fa3b767c460b54a2be4d49030b349c7&pdata=vRfurVL3V_zSdrTQyEywT6KCzcPVYEVzQCoHaayNCtr49Pi70HuvxQpgWH
HPiXqYIrkjdPj0mLIsp_EZbw3xPnny9rYWN-
4NTdezGPwhbUU9TUciDICLD9z3Z8z8vkuRk3MTmG0RUV38uEKllIzAe390aD1bMcOne0rtG-
piKRZdzkZ_Ooqk_g9BuYJlynd8HjclL52Fn05WjsxGor0g=&wsidchk=12962150 HTTP/1.1
Referer: https://ths100.in/9707507
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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive
```

Recommendation

If possible, you should set the Secure flag for these cookies.

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies 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.

<https://ths100.in/>

Verified

List of cookies with missing, inconsistent or contradictory properties:

- <https://ths100.in/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; 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".

- <https://ths100.in/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_email_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; 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".

- <https://ths100.in/wp-comments-post.php>

Cookie was set with:

```
Set-Cookie: comment_author_url_18550296b023cec14e4257cfa9551987=%20; expires=Tue, 26-Sep-2023 09:20:16 GMT; Max-Age=0; 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

POST /wp-comments-post.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://ths100.in/guardians-of-the-globe-project/
Cookie: wssplashuid=aff28dec62bf4544744fa0c94cad94c30f3d8fbd.1727257240.0
Content-Length: 140
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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive

attachment=&author=1&comment=555&comment_parent=0&comment_post_ID=14086&email=testing%40example.com&submit=Submit&url=http://www.example.com

Recommendation

Ensure that the cookies 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>

Insecure Frame (External)

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.

Impact

When a web page uses an insecurely configured iframe to embed another web page, the latter may manipulate the former, and trick its visitors into performing unwanted actions.

<https://ths100.in/>

Verified

An iframe tag references an external resource, and no sandbox attribute is set.

Request

```
GET / HTTP/1.1
Referer: https://ths100.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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive
```

<https://ths100.in/>

Verified

An iframe tag references an external resource, and no sandbox attribute is set.

Request

```
GET / HTTP/1.1
Referer: https://ths100.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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive
```

Recommendation

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.

References

[MDN | iframe: The Inline Frame Element](https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe)

<https://developer.mozilla.org/en-US/docs/Web/HTML/Element/iframe>

[HTML Standard: iframe](https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element)

<https://html.spec.whatwg.org/multipage/iframe-embed-object.html#the-iframe-element>

Content Security Policy (CSP) Not Implemented

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.

<https://ths100.in/>

Paths without CSP header:

- <https://ths100.in/>
- <https://ths100.in/9707507>
- <https://ths100.in/wp-json/oembed/1.0/embed>
- <https://ths100.in/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css>

- <https://ths100.in/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css>
- <https://ths100.in/xmlrpc.php>
- <https://ths100.in/wp-includes/js/jquery/ui/core.min.js>
- <https://ths100.in/comments/feed/>
- <https://ths100.in/announcement-and-news/>
- <https://ths100.in/admission/>
- <https://ths100.in/wp-content/plugins/revslider/public/assets/css/rs6.css>
- <https://ths100.in/contact/>
- <https://ths100.in/blog>
- <https://ths100.in/down-memory-lane/>
- <https://ths100.in/wp-includes/js/dist/api-fetch.min.js>
- <https://ths100.in/wp-content/themes/eduma/assets/css/v4-shims.min.css>
- <https://ths100.in/feed/>
- <https://ths100.in/headmaster/>
- <https://ths100.in/our-school/>
- <https://ths100.in/teachers-staffs/>
- <https://ths100.in/wp-json/wp/v2/pages/4524>

Request

GET / HTTP/1.1

Referer: <https://ths100.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/119.0.0.0 Safari/537.36

Host: ths100.in

Connection: Keep-alive

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/>

File Upload Functionality Detected

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

<https://ths100.in/>

Pages with file upload forms:

- <https://ths100.in/guardians-of-the-globe-project/>

Form name: <empty>

Form action: <https://ths100.in/wp-comments-post.php>

Form method: POST

Form file input: attachment [file]

Request

GET /guardians-of-the-globe-project/ HTTP/1.1

Referer: <https://ths100.in/>

Cookie: wssplashuid=aff28dec62bf4544744fa0c94cad94c30f3d8fbd.1727257240.0

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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

Generic Email Address Disclosure

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.

Impact

Email addresses posted on Web sites may attract spam.

<https://ths100.in/>

Emails found:

- <https://ths100.in/>
tarakeswarschool1925@gmail.com
- <https://ths100.in/9707507>
tarakeswarschool1925@gmail.com
- <https://ths100.in/author/admin24/>
tarakeswarschool1925@gmail.com
- <https://ths100.in/category/event/>
tarakeswarschool1925@gmail.com
- <https://ths100.in/category/uncategorized/>
tarakeswarschool1925@gmail.com
- <https://ths100.in/comments/>
tarakeswarschool1925@gmail.com
- https://ths100.in/plugins/error/confirm/page_follow
tarakeswarschool1925@gmail.com

- <https://ths100.in/gaming/tarakeswarschool1925@gmail.com>
- <https://ths100.in/reel/tarakeswarschool1925@gmail.com>
- <https://ths100.in/author/tarakeswarschool1925@gmail.com>
- <https://ths100.in/plugins/tarakeswarschool1925@gmail.com>
- <https://ths100.in/watch/tarakeswarschool1925@gmail.com>
- <https://ths100.in/wp-includes/css/dist/block-library/tarakeswarschool1925@gmail.com>
- <https://ths100.in/guardians-of-the-globe-project/tarakeswarschool1925@gmail.com>
- <https://ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f/tarakeswarschool1925@gmail.com>

Request

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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive

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

Permissions-Policy header not implemented

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

<https://ths100.in/>

Locations without Permissions-Policy header:

- <https://ths100.in/>
- <https://ths100.in/9707507>
- <https://ths100.in/wp-json/oembed/1.0/embed>
- <https://ths100.in/wp-content/plugins/elementor/assets/lib/swiper/v8/css/swiper.min.css>
- <https://ths100.in/wp-content/plugins/thim-elementor-kit/build/libraries/thim-ekits/css/thim-ekits-icons.min.css>
- <https://ths100.in/xmlrpc.php>
- <https://ths100.in/wp-includes/js/jquery/ui/core.min.js>
- <https://ths100.in/comments/feed/>
- <https://ths100.in/announcement-and-news/>
- <https://ths100.in/admission/>
- <https://ths100.in/wp-content/plugins/revslider/public/assets/css/rs6.css>
- <https://ths100.in/contact/>
- <https://ths100.in/blog>
- <https://ths100.in/down-memory-lane/>
- <https://ths100.in/wp-includes/js/dist/api-fetch.min.js>
- <https://ths100.in/wp-content/themes/eduma/assets/css/v4-shims.min.css>
- <https://ths100.in/feed/>
- <https://ths100.in/headmaster/>
- <https://ths100.in/our-school/>
- <https://ths100.in/teachers-staffs/>
- <https://ths100.in/wp-json/wp/v2/pages/4524>

Request

GET / HTTP/1.1
Referer: <https://ths100.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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive

References

[Permissions-Policy / Feature-Policy \(MDN\)](#)

<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy>

[Permissions Policy \(W3C\)](#)

<https://www.w3.org/TR/permissions-policy-1/>

Web Application Firewall Detected

This server is protected by an IPS (Intrusion Prevention System), IDS (Intrusion Detection System) or an WAF (Web Application Firewall). Acunetix detected this by sending various malicious payloads and detecting changes in the response code, headers and body.

Impact

You may receive incorrect/incomplete results when scanning a server protected by an IPS/IDS/WAF. Also, if the WAF detects a number of attacks coming from the scanner, the IP address can be blocked after a few attempts.

<https://ths100.in/>

Detected Imunify360 from the server header.

Request

```
GET /9707507 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/119.0.0.0 Safari/537.36
Host: ths100.in
Connection: Keep-alive
```

Recommendation

If possible, it's recommended to scan an internal (development) version of the web application where the WAF is not active.

Coverage

https://ths100.in

Inputs

GET __im-PhdUltRu, p, __im-qakxnsFu, id, pdata



%E0%A6%B6%E0%A6%BF%E0%A6%95%E0%A7%8D%E0%A6%B7%E0%A6%BE%E0%A6%99%E0%A7%8D%E0%A6%97%E0%A6%A8%E0%A7%87%E0%A6%B0-%E0%A6%86%E0%A6%99%E0%A6%BF%E0%A6%A8%E0%A6%BE%E0%A6%AF%E0%A6%BC-%E0%A6%A4%E0%A6%BE

#fragments

respond



admission



announcement-and-news



author



admin24



feed



blog



category



event



feed



uncategorized



feed



comments



feed



contact



down-memory-lane



feed



gaming



Inputs

GET



{



Inputs

GET

guardians-of-the-globe-project

#fragments

comment-162

respond

Inputs

GET replytocon, moderation-hash, unapproved

feed

headmaster

history-of-school

list-of-past-headmasters

our-school

plugins

error

confirm

page_follow

Inputs

GET follow_location, iframe_referer, kid_directed_site, plugin, return_params, secure

GET href, width, show_text, appld, height, ret, act, page_id

reel

Inputs

GET

{

Inputs

GET

tarakeswar-the-holy-city-of-heritage

teachers-staffs

watch

Inputs

GET

{

Inputs

GET

wp-admin

 admin-ajax.php

 Inputs

POST action, thim_key, thim_value

 admin.php

 Inputs

GET , page, saved

 wp-content

 plugins

 contact-form-7

 includes

 css

 styles.css

 #fragments

 mask-2

 js

 index.js

 swv

 js

 index.js

 custom-facebook-feed

 assets

 css

 cff-style.min.css

 #fragments

 mask-2

 js

 cff-scripts.js

 dco-comment-attachment

 assets

 dco-comment-attachment.css

 #fragments

 mask-2

 dco-comment-attachment.js

 elementor

assets

css

frontend.min.css

#fragments

mask-2

js

frontend-modules.min.js

frontend.min.js

webpack.runtime.min.js

lib

dialog

dialog.min.js

eicons

css

elementor-icons.min.css

fonts

font-awesome

css

all.css

#fragments

mask-2

share-link

share-link.min.js

swiper

v8

css

swiper.min.css

#fragments

mask-2

swiper.min.js

waypoints

waypoints.min.js

feeds-for-youtube

- css
 - sb-youtube-free.min.css
 - #fragments
 - mask-2

- sb-youtube.min.css
 - #fragments
 - mask-2

- feedzy-rss-feeds
 - css
 - feedzy-rss-feeds.css
 - #fragments
 - mask-2

- img

- instagram-feed
 - css
 - sbi-styles.min.css
 - #fragments
 - mask-2

- revslider
 - public
 - assets
 - assets
 - css
 - rs6.css
 - #fragments
 - mask-2
 - js
 - rbtools.min.js
 - rs6.min.js

- thim-elementor-kit
 - build
 - libraries
 - thim-ekits
 - css

 thim-ekits-icons.min.css

 #fragments

 mask-2

 frontend.css

 #fragments

 mask-2

 frontend.js

 widgets.css

 #fragments

 mask-2

 widgets.js

 widget-google-reviews

 assets

 css

 public-main.css

 #fragments

 mask-2

 js

 public-main.js

 wp-embed-facebook

 inc

 js

 fb.min.js

 templates

 lightbox

 css

 lightbox.css

 #fragments

 mask-2

 js

 lightbox.min.js

 themes

 eduma

- assets
 - css
 - v4-shims.min.css
 - #fragments
 - mask-2

- js
 - main.min.js
 - thim-scripts.min.js

- style.css
 - #fragments
 - mask-2

- uploads
 - 2018
 - 01

- 2019
 - 02

- 2022
 - 11

- 2024
 - 07

- 09
 - hm.webp

- thim-fonts
 - robotoslab

- wp-includes
 - css
 - dist
 - block-library
 - style.min.css

- js
 - dist
 - api-fetch.min.js
 - hooks.min.js

 i18n.min.js

 url.min.js

 jquery

 ui

 core.min.js

 jquery-migrate.min.js

 jquery.min.js

 comment-reply.min.js

 imagesloaded.min.js

 wp-json

 oembed

 1.0

 embed

 Inputs

 GET format, url

 wp

 v2

 categories

 1

 189

 pages

 14353

 14378

 4524

 posts

 14086

 users

 1

 users

 9707507

 Inputs

 GET __im-ftmaQury

 blog

 robots.txt

 wp-comments-post.php

 Inputs

POST attachment, author, comment, comment_parent, comment_post_ID, email, submit, url

POST attachment, author, comment, comment_parent, comment_post_ID, email, submit, url

 xmlrpc.php

 Inputs

GET