ZAP Scanning Report

Sites: http://alumni.ths100.in https://alumni.ths100.in

Generated on Wed, 25 Sep 2024 08:47:25

ZAP Version: 2.15.0

ZAP is supported by the Crash Override Open Source Fellowship

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	6
Low	6
Informational	13

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
Absence of Anti-CSRF Tokens	Medium	1
Content Security Policy (CSP) Header Not Set	Medium	4
Hidden File Found	Medium	4
Insecure HTTP Method - PATCH	Medium	1
Missing Anti-clickjacking Header	Medium	3
Sub Resource Integrity Attribute Missing	Medium	3
HTTPS Content Available via HTTP	Low	1
Permissions Policy Header Not Set	Low	4
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	4
Strict-Transport-Security Header Not Set	Low	4
Timestamp Disclosure - Unix	Low	2
X-Content-Type-Options Header Missing	Low	3
Base64 Disclosure	Informational	1
Information Disclosure - Suspicious Comments	Informational	1
Insecure HTTP Method - COPY	Informational	1
Insecure HTTP Method - LOCK	Informational	1
Insecure HTTP Method - MKCOL	Informational	1
Insecure HTTP Method - MOVE	Informational	1
Insecure HTTP Method - PROPFIND	Informational	1
Insecure HTTP Method - PROPPATCH	Informational	1
Insecure HTTP Method - UNLOCK	Informational	1
Modern Web Application	Informational	6

Non-Storable Content	Informational	3
Storable but Non-Cacheable Content	Informational	1
User Agent Fuzzer	Informational	12

Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	https://alumni.ths100.in/latest/meta-data/
Method	GET
Attack	aws.zaproxy.org
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	1
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request t action as the victim. The underlying cause is application functionality using predictable URL/form the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust t cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privile gaining access to the response. The risk of information disclosure is dramatically increased whe for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhC TIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIxC
Method	GET
Attack	

Evidence	<form role="search" method="get" class="search-form" action="https://alumni.ths100.in/">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddleware _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [
Instances	1
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constru For example, use anti-CSRF packages such as the OWASP CSRFGuard. Phase: Implementation Ensure that your application is free of cross-site scripting issues, because most CSRF defenses Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upo Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send that operation. Note that this can be bypassed using XSS. Use the ESAPI Session Management control. This control includes a component for CSRF. Do not use the GET method for any request that triggers a state change. Phase: Implementation Check the HTTP Referer header to see if the request originated from an expected page. This co sending the Referer for privacy reasons.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Chea https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**Content Security Policy (CSP) Header Not Set**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer attacks. These attacks are used for everything from data theft to site defacement or distribution owners to declare approved sources of content that browsers should be allowed to load on that embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	

Other Info	
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhC TIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIxC
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Cont
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Poli https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html https://www.w3.org/TR/CSP/ https://w3c.github.io/webappsec-csp/ https://web.dev/articles/csp https://caniuse.com/#feat=contentsecuritypolicy https://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	**Hidden File Found**
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	https://alumni.ths100.in/._darcs
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://alumni.ths100.in/.bzr
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://alumni.ths100.in/.hg
Method	GET
Attack	

Evidence	HTTP/1.1 200 OK
Other Info	
URL	https://alumni.ths100.in/BitKeeper
Method	GET
Attack	
Evidence	HTTP/1.1 200 OK
Other Info	
Instances	4
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	**Insecure HTTP Method - PATCH**
Description	This method is now most commonly used in REST services, PATCH is used for **modify** capabilities. The PATCH request only needs to contain the changes to the resource, not the complete resource.
URL	https://alumni.ths100.in/dx4msi2b4s
Method	PATCH
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods, for understanding REST operations see http://www.restapitutorial.com/lessons/httpmethods.html
Instances	1
Solution	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200

WASC Id	45
Plugin Id	90028

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
Instances	3
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app. If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
CWE Id	1021
WASC Id	15
Plugin Id	10020

Medium	Sub Resource Integrity Attribute Missing
Description	The integrity attribute is missing on a script or link tag served by an external server. The integrity a malicious content.
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	<link rel="preconnect" href="https://fonts.gstatic.com/" crossorigin>
Other Info	

URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhCTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIxC
Method	GET
Attack	
Evidence	<link rel="profile" href="https://gmpg.org/xfn/11">
Other Info	
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhCTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIxC
Method	GET
Attack	
Evidence	<link rel='stylesheet' id='google-fonts-1-css' href='https://fonts.googleapis.com/css?family=Robo 2C400italic%2C500%2C500italic%2C600%2C600italic%2C700%2C700italic%2C800%2C800it 2C200italic%2C300%2C300italic%2C400%2C400italic%2C500%2C500italic%2C600%2C600it display=swap&ver=6.6.2' media='all' />
Other Info	
Instances	3
Solution	Provide a valid integrity attribute to the tag.
Reference	https://developer.mozilla.org/en/docs/Web/Security/Subresource_Integrity
CWE Id	345
WASC Id	15
Plugin Id	90003

Low	**HTTPS Content Available via HTTP**
Description	Content which was initially accessed via HTTPS (i.e.: using SSL/TLS encryption) is also accessible via HTTP (without encryption).
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	http://alumni.ths100.in/
Other Info	ZAP attempted to connect via: http://alumni.ths100.in/
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to only serve such content via HTTPS. Consider implementing HTTP Strict Transport Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://owasp.org/www-community/Security_Headers http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/html/rfc6797
CWE Id	311
WASC Id	4
Plugin Id	10047

Low	**Permissions Policy Header Not Set**

Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized ensures the user privacy by limiting or specifying the features of the browsers can be used by th that allow website owners to limit which features of browsers can be used by the page such as
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Perm
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy https://developers.google.com/web/updates/2018/06/feature-policy https://scotthelme.co.uk/a-new-security-header-feature-policy/ https://w3c.github.io/webappsec-feature-policy/ https://www.smashingmagazine.com/2018/12/feature-policy/
CWE Id	693
WASC Id	15
Plugin Id	10063

Low	**Server Leaks Version Information via "Server" HTTP Response Header Field**
Description	The web/application server is leaking version information via the "Server" HTTP response head vulnerabilities your web/application server is subject to.
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	imunify360-webshield/1.21

Other Info	
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	imunify360-webshield/1.21
Other Info	
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	imunify360-webshield/1.21
Other Info	
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhCTly8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIxC
Method	GET
Attack	
Evidence	imunify360-webshield/1.21
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress th
Reference	https://httpd.apache.org/docs/current/mod/core.html#servertokens https://learn.microsoft.com/en-us/previous-versions/msp-n-p/ff648552(v=pandp.10) https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	200
WASC Id	13
Plugin Id	10036

Low	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web serv with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IET
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	
Other Info	

URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	
Other Info	
Instances	4
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet https://owasp.org/www-community/Security_Headers https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security https://caniuse.com/stricttransportsecurity https://datatracker.ietf.org/doc/html/rfc6797
CWE Id	319
WASC Id	15
Plugin Id	10035

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	1727242090
Other Info	1727242090, which evaluates to: 2024-09-25 05:28:10.
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhTIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	1727242091
Other Info	1727242091, which evaluates to: 2024-09-25 05:28:11.
Instances	2
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregat
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	200
WASC Id	13

Plugin Id	10096

Low	**X-Content-Type-Options Header Missing**
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	3
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application /web server to not perform MIME-sniffing.
Reference	https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85) https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Base64 Disclosure**
Description	Base64 encoded data was disclosed by the application/web server. Note: in the interests of perf entire response should be looked at by the analyst/security team/developer(s).
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxh0

	TIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	a11yCarouselPaginationBulletMessage
Other Info	k]r ="bpnW1,j\x0007
Instances	1
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data ca
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	200
WASC Id	13
Plugin Id	10094

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matc comments.
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhC TIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIx
Method	GET
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "<scr {"environmentMode":{"edit":false,"wpPreview":false,"isS", see evidence field for the suspicious c
Instances	1
Solution	Remove all comments that return information that may help an attacker and fix any underlying p
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10027

Informational	**Insecure HTTP Method - COPY**
Description	This HTTP method is a WEBDAV method: COPY. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/
Method	COPY
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile.

Solution	2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Insecure HTTP Method - LOCK**
Description	This HTTP method is a WEBDAV method: LOCK. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/
Method	LOCK
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
Solution	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Insecure HTTP Method - MKCOL**

Description	This HTTP method is a WEBDAV method: MKCOL. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/
Method	MKCOL
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
Solution	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Insecure HTTP Method - MOVE**
Description	This HTTP method is a WEBDAV method: MOVE. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/
Method	MOVE
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools.

Solution	3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Insecure HTTP Method - PROPFIND**
Description	This HTTP method is a WEBDAV method: PROPFIND. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/
Method	PROPFIND
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
Solution	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Insecure HTTP Method - PROPPATCH**
Description	This HTTP method is a WEBDAV method: PROPPATCH. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/

Method	PROPPATCH
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
Solution	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques. 5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Insecure HTTP Method - UNLOCK**
Description	This HTTP method is a WEBDAV method: UNLOCK. If this server is not offering any WEBDAV services, these methods should not be available.
URL	https://alumni.ths100.in/
Method	UNLOCK
Attack	
Evidence	response code 200 for insecure HTTP METHOD
Other Info	See the discussion on stackexchange: https://security.stackexchange.com/questions/21413/how-to-exploit-http-methods
Instances	1
Solution	Implement measures to obfuscate or disguise information about the system's platform, web application software technology, backend database version, configurations, and network architecture/topology. This can include: 1. **Platform and Software Diversity:** Use a mix of technologies and platforms to make it harder for attackers to build an accurate profile. 2. **False Information:** Introduce fake or misleading information in system responses to confuse fingerprinting tools. 3. **Response Randomization:** Randomize certain elements in responses to make it difficult for attackers to consistently identify the system. 4. **Firewall Rules:** Implement firewall rules to block or limit the effectiveness of fingerprinting techniques.

	5. **Regular Updates:** Keep software, platforms, and configurations up-to-date to patch known vulnerabilities and prevent accurate identification based on outdated information. There is no one-size-fits-all solution, and a combination of these measures may be most effective.
Reference	https://cwe.mitre.org/data/definitions/205.html
CWE Id	200
WASC Id	45
Plugin Id	90028

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	<script> (function(w){var x=function(){try{return !!w['\x61\x64\x64\x45\x76\x65\x6e\x74\x4c\x69\x ='\x33\x50\x74\x42\x6c\x63\x35\x74\x4a\x41\x5f\x76\x4a\x32\x46\x4d\x4f\x75\x57\x64\x49\x32\x [])+(+!+[]+!![]+!![]+!![]+!![]+!![]+[])+(+!+[]+!![]+!![])+(+![]+[])+(+!+[]+!![]+!![]+!![])+(+!+[]+!![]+!![]+[])+(+! ('\x47\x45\x54','\x2f\x7a\x30\x66\x37\x36\x61\x31\x64\x31\x34\x66\x64\x32\x31\x61\x38\x66\x62 ='\x68\x69\x64\x64\x65\x6e';j['\x74\x79\x70\x65']='\x68\x69\x64\x64\x65\x6e';j['\x76\x61\x6c\x75' ['\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64'](f);f['\x73\x75\x62\x6d\x69\x74']();}},1000);},fals
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	<script> (function(w){var x=function(){try{return !!w['\x61\x64\x64\x45\x76\x65\x6e\x74\x4c\x69\x ='\x32\x45\x74\x4a\x6f\x73\x54\x32\x6b\x6b\x4c\x33\x4b\x67\x6c\x6e\x51\x79\x4e\x44\x72\x5a\ []+!![]+!![])+(+!+[]+!![]+!![]+!![]+[])+(+!+[]+!![]+!![])+(+!+[]+!![]+!![]+!![]+!![]+[])+(+!+[])+(+!+[]+!![]+! ('\x47\x45\x54','\x2f\x7a\x30\x66\x37\x36\x61\x31\x64\x31\x34\x66\x64\x32\x31\x61\x38\x66\x62 ='\x68\x69\x64\x64\x65\x6e';j['\x74\x79\x70\x65']='\x68\x69\x64\x64\x65\x6e';j['\x76\x61\x6c\x75' ['\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64'](f);f['\x73\x75\x62\x6d\x69\x74']();}},1000);},fals
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	<script> (function(w){var x=function(){try{return !!w['\x61\x64\x64\x45\x76\x65\x6e\x74\x4c\x69\x ='\x73\x50\x31\x6d\x55\x44\x70\x72\x31\x44\x6d\x50\x45\x36\x51\x76\x6d\x48\x4a\x47\x54\x55 []+!![])+(+!+[]+!![]+!![]+!![]+!![]+[])+(+!+[]+!![]+!![])+(+![]+[])+(+!+[]+!![]+!![]+!![])+(+!+[]+!![]+!![]+[]) ('\x47\x45\x54','\x2f\x7a\x30\x66\x37\x36\x61\x31\x64\x31\x34\x66\x64\x32\x31\x61\x38\x66\x62 ='\x68\x69\x64\x64\x65\x6e';j['\x74\x79\x70\x65']='\x68\x69\x64\x64\x65\x6e';j['\x76\x61\x6c\x75' ['\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64'](f);f['\x73\x75\x62\x6d\x69\x74']();}},1000);},fals
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
	<script> (function(w){var x=function(){try{return !!w['\x61\x64\x64\x45\x76\x65\x6e\x74\x4c\x69\x ='\x4b\x45\x54\x2d\x4a\x53\x32\x6d\x35\x68\x2d\x5a\x71\x34\x49\x38\x68\x36\x77\x31\x78\x30 o['\x75\x70\x79\x34\x65\x6d\x73\x66\x62\x7a\x30\x37']=+((+!+[]+!![]+!![])+(+!+[]+!![]+!![]+!![]+!![]+

Evidence	['\x58\x4d\x4c\x48\x74\x74\x70\x52\x65\x71\x75\x65\x73\x74']();r['\x6f\x70\x65\x6e']('\x47\x45\x5 ='\x66\x66\x62\x6a\x35\x35\x63\x79\x62\x74\x74\x6f';i['\x74\x79\x70\x65']='\x68\x69\x64\x64\x65 ['\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64'](j);f['\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	
Evidence	<script> (function(w){var x=function(){try{return !!w['\x61\x64\x64\x45\x76\x65\x6e\x74\x4c\x69\x ='\x59\x4b\x73\x5a\x57\x6c\x52\x6d\x69\x66\x78\x5f\x53\x42\x45\x39\x61\x59\x57\x59\x7a\x66 o['\x6d\x6c\x68\x6f\x6e\x74\x6a\x33\x79\x72\x39\x73']=+((+!+[]+!![]+!![])+(+!+[]+!![]+!![]+!![]+!! ['\x6f\x70\x65\x6e']('\x47\x45\x54','\x2f\x7a\x30\x66\x37\x36\x61\x31\x64\x31\x34\x66\x64\x32\x ='\x68\x69\x64\x64\x65\x6e';j['\x74\x79\x70\x65']='\x68\x69\x64\x64\x65\x6e';j['\x76\x61\x6c\x75 ['\x61\x70\x70\x65\x6e\x64\x43\x68\x69\x6c\x64'](f);f['\x73\x75\x62\x6d\x69\x74']();}},1000);},fals
Other Info	No links have been found while there are scripts, which is an indication that this is a modern we
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b0
Method	GET
Attack	
Evidence	HISTORY
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this
Instances	6
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational	**Non-Storable Content**
Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	https://alumni.ths100.in/
Method	GET
Attack	
Evidence	no-store
Other Info	
URL	https://alumni.ths100.in/robots.txt
Method	GET
Attack	
Evidence	no-store
Other Info	
URL	https://alumni.ths100.in/sitemap.xml
Method	GET
Attack	

Evidence	no-store
Other Info	
Instances	3
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable) The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood) The "no-store" cache directive must not appear in the request or response header fields For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives) In addition to the conditions above, at least one of the following conditions must also be satisfied by the response: It must contain an "Expires" header field It must contain a "max-age" response directive For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive It must contain a "Cache Control Extension" that allows it to be cached It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231 http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	**Storable but Non-Cacheable Content**
Description	The response contents are storable by caching components such as proxy servers, but will not l response to similar requests from other users.
URL	https://alumni.ths100.in/z0f76a1d14fd21a8fb5fd0d03e0fdc3d3cedae52f?id=a6105c0a611b41b08f1209506350279e&pdata=2EtJosT2kkL3KglnQyNDrZ91a0s37cU_pxhC TIy8fO8rmm1qNTl1s4hynMtL405A4XlrrMBemSp8IH38u0unfoYtKPkjxfj4PcWo_fvBylhEhcfgDIxC
Method	GET
Attack	
Evidence	no-cache
Other Info	
Instances	1
Solution	
Reference	https://tools.ietf.org/html/rfc7234 https://tools.ietf.org/html/rfc7231

	http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234)
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	

Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	https://alumni.ths100.in/
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	12
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	

Plugin Id	10104