ZAP Scanning Report

Sites: https://optimizationguide-pa.googleapis.com https://www.google-analytics.com https://www.googletagmanager.com https://firebaseinstallations.googleapis.com https://firebase.googleapis.com https://content-autofill.googleapis.com https://www.gstatic.com https://accounts.google.com https://cosc-402-group-3-project.web.app

Generated on Sun, 14 May 2023 19:36:05

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	5
Informational	3

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	3
CSP: Wildcard Directive	Medium	2
Content Security Policy (CSP) Header Not Set	Medium	16
Cross-Domain Misconfiguration	Medium	3
Missing Anti-clickjacking Header	Medium	13
Session ID in URL Rewrite	Medium	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	3
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	1
Strict-Transport-Security Header Not Set	Low	17
Timestamp Disclosure - Unix	Low	4
X-Content-Type-Options Header Missing	Low	17
Information Disclosure - Suspicious Comments	Informational	16
Re-examine Cache-control Directives	Informational	16
Retrieved from Cache	Informational	14

Alert Detail

Medium	Absence of Anti-CSRF Tokens
	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 to a target destination without their knowledge or intent in order to perform an

Description	action as the victim. The underlying cause is application functionality using predictable URL /form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. 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 privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	https://cosc-402-group-3-project.web.app/Donate.html
Method	GET
Attack	
Evidence	<form action="/insert_data" method="post" >
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	
Evidence	<form>
URL	https://cosc-402-group-3-project.web.app/signup.html
Method	GET
Attack	
Evidence	<form action="/insert_data" method="post" >
Instances	3
Solution	Phase: Architecture and Design Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid. 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 can be bypassed using attacker-controlled script. Phase: Architecture and Design Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS. Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform 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 could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.
Reference	http://projects.webappsec.org/Cross-Site-Request-Forgery http://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	**CSP: Wildcard Directive**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	https://cosc-402-group-3-project.web.app/insert_data
Method	GET
Attack	
Evidence	default-src 'none'
URL	https://cosc-402-group-3-project.web.app/sitemap.xml
Method	GET
Attack	
Evidence	default-src 'none'
Instances	2
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	http://www.w3.org/TR/CSP2/ http://www.w3.org/TR/CSP/ http://caniuse.com/#search=content+security+policy http://content-security-policy.com/ https://github.com/shapesecurity/salvation https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources
CWE Id	693
WASC Id	15
Plugin Id	10055

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, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP h website owners to declare approved sources of content that browsers should be allowed to load covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such ActiveX, audio and video files.
URL	https://cosc-402-group-3-project.web.app

Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/About%20Us.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/Contact%20Us.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/Donate.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/gettinginvolved.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/index.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/robots.txt
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/signup.html
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION

Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550902&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550915&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZATION_TARGET_SEGMENTATION_CHROME_LOW_US
Method	GET
Attack	
Evidence	
URL	https://firebase.googleapis.com/v1alpha/projects/-/apps/1:40122580647:web:b543922962f5d18
Method	OPTIONS
Attack	
Evidence	
URL	https://firebaseinstallations.googleapis.com/v1/projects/test-6a9b6/installations
Method	OPTIONS
Attack	
Evidence	
Instances	16
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Cont header.
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 http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/
CWE Id	693
WASC Id	15
Plugin Id	10038

Medium	Cross-Domain Misconfiguration
Description	Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *

URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-analytics.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	Access-Control-Allow-Origin: *
Instances	3
Solution	Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance). Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.
Reference	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy
CWE Id	264
WASC Id	14
Plugin Id	10098

Medium	Missing Anti-clickjacking Header
Description	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or to protect against 'ClickJacking' attacks.
URL	https://cosc-402-group-3-project.web.app
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/About%20Us.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/Contact%20Us.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/Donate.html
Method	GET
Attack	
Evidence	

URL	https://cosc-402-group-3-project.web.app/gettinginvolved.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/index.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/signup.html
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550902&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550915&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZATION_TARGET_SEGMENTATION_CHROME_LOW_US
Method	GET
Attack	
Evidence	
Instances	13
Solution	Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP header 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 use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY 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	Session ID in URL Rewrite
Description	URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site referer header. In addition, the session ID might be stored in browser history or server logs.
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-PNKN8DFN6Z&gtm=45je35a0&_p=1212657310&_fid=eqO4fbJy_R0tijO-jK8Ezo&cid=283564146.1684106845&ul=en-us&sr=1920x1080&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.93%7CChromium%3B113.0.5672.93%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=Windows&uapv=15.0.0&uaw=0&ngs=1&_s=1&sid=1684106844&sct=1&seg=0&dl=https%3A%2F%2Fcosc-402-group-3-project.web.app%2F&dt=Food%20Bank%20Homepage&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&ep.origin=firebase
Method	POST
Attack	
Evidence	1684106844
Instances	1
Solution	For secure content, put session ID in a cookie. To be even more secure consider using a combination of cookie and URL rewrite.
Reference	http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html
CWE Id	200
WASC Id	13
Plugin Id	3

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	https://cosc-402-group-3-project.web.app/insert_data
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://cosc-402-group-3-project.web.app/sitemap.xml
Method	GET
Attack	
Evidence	X-Powered-By: Express
URL	https://cosc-402-group-3-project.web.app/insert_data
Method	POST
Attack	
Evidence	X-Powered-By: Express
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html

CWE Id	200
WASC Id	13
Plugin Id	10037

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 header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-PNKN8DFN6Z&gtm=45je35a0&_p=1212657310&_fid=eqO4fbJy_R0tijO-jK8Ezo&cid=283564146.1684106845&ul=en-us&sr=1920x1080&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.93%7CChromium%3B113.0.5672.93%7CNot-A.Brand%3B24.0.0.0&uamb=0&uam=&uap=Windows&uapv=15.0.0&uaw=0&ngs=1&_s=1&sid=1684106844&sct=1&seg=0&dl=https%3A%2F%2Fcosc-402-group-3-project.web.app%2F&dt=Food%20Bank%20Homepage&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&ep.origin=firebase
Method	POST
Attack	
Evidence	Golfe2
Instances	1
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
Reference	http://httpd.apache.org/docs/current/mod/core.html#servertokens http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007 http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.aspx http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html
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://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTEzLjAuNTY3Mi45MxIXCW
Method	GET
Attack	
Evidence	
URL	https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTEzLjAuNTY3Mi45MxJICbTmrF5B_mW2EgUNBu27_xIFDQbtu_8SBQ0G7?alt=proto
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/insert_data
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/robots.txt

Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/sitemap.xml
Method	GET
Attack	
Evidence	
URL	https://firebase.googleapis.com/v1alpha/projects/-/apps/1:40122580647:web:b543922962f5d18
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZA
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550902&target=OPTIMIZA
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550915&target=OPTIMIZA
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZA
Method	GET
Attack	
Evidence	
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-analytics.js
Method	GET
Attack	
Evidence	
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	
URL	https://firebase.googleapis.com/v1alpha/projects/-/apps/1:40122580647:web:b543922962f5d18
Method	OPTIONS
Attack	
Evidence	
URL	https://firebaseinstallations.googleapis.com/v1/projects/test-6a9b6/installations
Method	OPTIONS

Attack	
Evidence	
URL	https://firebaseinstallations.googleapis.com/v1/projects/test-6a9b6/installations
Method	POST
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIe
Method	POST
Attack	
Evidence	
URL	https://www.google-analytics.com/g/collect?v=2&tid=G-PNKN8DFN6Z&gtm=45je35a0&_p=121 us&sr=1920x1080&uaa=x86&uab=64&uafvl=Google%2520Chrome%3B113.0.5672.93%7CChr &uamb=0&uam=&uap=Windows&uapv=15.0.0&uaw=0&ngs=1&_s=1&sid=1684106844&sct=1& 2F&dt=Food%20Bank%20Homepage&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&ep.origin=
Method	POST
Attack	
Evidence	
Instances	17
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 http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security http://caniuse.com/stricttransportsecurity http://tools.ietf.org/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://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
Method	POST
Attack	
Evidence	1679317318
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
Method	POST
Attack	
Evidence	1682959204
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw
Method	POST
Attack	
Evidence	1683550902
URL	https://optimizationguide-pa.googleapis.com/v1:GetModels?key=AIzaSyBOti4mM-6x9WDnZIjIeyEU21OpBXqWBgw

Method	POST
Attack	
Evidence	1683550915
Instances	4
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	http://projects.webappsec.org/w/page/13246936/Information%20Leakage
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 olde Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causi body to be interpreted and displayed as a content type other than the declared content type. Cu and legacy versions of Firefox will use the declared content type (if one is set), rather than perfo
URL	https://cosc-402-group-3-project.web.app
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/About%20Us.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/Contact%20Us.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/Donate.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/gettinginvolved.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/index.html
Method	GET
Attack	

Evidence	
URL	https://cosc-402-group-3-project.web.app/Main.css
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/signup.css
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/signup.html
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZATION_TARGET_LANGUAGE_DETECTION
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550902&target=OPTIMIZATION_TARGET_GEOLOCATION_PERMISSION_PRED
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550915&target=OPTIMIZATION_TARGET_NOTIFICATION_PERMISSION_PREDI
Method	GET
Attack	
Evidence	
URL	https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZATION_TARGET_SEGMENTATION_CHROME_LOW_US
Method	GET
Attack	
Evidence	
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	
Evidence	
URL	https://cosc-402-group-3-project.web.app/insert_data
Method	POST

Attack	
Evidence	
Instances	17
Solution	Ensure that the application/web server sets the Content-Type header appropriately, and that it s 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 MIME-sniffing at all, or that can be directed by the web application/web server to not perform MI
Reference	http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx https://owasp.org/www-community/Security_Headers
CWE Id	693
WASC Id	15
Plugin Id	10021

Informational	**Information Disclosure - Suspicious Comments**
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	https://cosc-402-group-3-project.web.app
Method	GET
Attack	
Evidence	TODO
URL	https://cosc-402-group-3-project.web.app/
Method	GET
Attack	
Evidence	TODO
URL	https://cosc-402-group-3-project.web.app/index.html
Method	GET
Attack	
Evidence	TODO
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	
Evidence	db
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	
Evidence	from
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	
Evidence	query
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	

Evidence	SELECT
URL	https://www.googletagmanager.com/gtag/js?l=dataLayer&id=G-PNKN8DFN6Z
Method	GET
Attack	
Evidence	username
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-analytics.js
Method	GET
Attack	
Evidence	from
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	db
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	from
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	later
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	TODO
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	user
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	where
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	
Evidence	admin
Instances	16
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	200

WASC Id	13
Plugin Id	10027

Informational	**Re-examine Cache-control Directives**
Description	The cache-control header has not been set properly or is missing, allowing the browser and pro intended, however, the resources should be reviewed to ensure that no sensitive content will be
URL	https://content-autofill.googleapis.com/v1/pages/ChRDaHJvbWUvMTEzLjAuNTY3Mi45MxIXCW
Method	GET
Attack	
Evidence	private,max-age=604800
URL	https://content-autofill.googleapis.com/v1/pages /ChRDaHJvbWUvMTEzLjAuNTY3Mi45MxJICbTmrF5B_mW2EgUNBu27_xIFDQbtu_8SBQ0G7 alt=proto
Method	GET
Attack	
Evidence	private,max-age=604800
URL	https://cosc-402-group-3-project.web.app
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/About%20Us.html
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/Contact%20Us.html
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/Donate.html
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/gettinginvolved.html
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/index.html
Method	GET
Attack	

Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	
Evidence	max-age=3600
URL	https://cosc-402-group-3-project.web.app/signup.html
Method	GET
Attack	
Evidence	max-age=3600
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1679317318&target=OPTIMIZA
Method	GET
Attack	
Evidence	public, max-age=86400
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550902&target=OPTIMIZA
Method	GET
Attack	
Evidence	public, max-age=86400
URL	https://optimizationguide-pa.googleapis.com/downloads?name=1683550915&target=OPTIMIZA
Method	GET
Attack	
Evidence	public, max-age=86400
URL	https://optimizationguide-pa.googleapis.com/downloads?name=2202180000&target=OPTIMIZA
Method	GET
Attack	
Evidence	public, max-age=86400
URL	https://cosc-402-group-3-project.web.app/insert_data
Method	POST
Attack	
Evidence	private
Instances	16
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Retrieved from Cache**
Description	The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This

	is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.
URL	https://cosc-402-group-3-project.web.app
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/About%20Us.html
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/Contact%20Us.html
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/Donate.html
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/gettinginvolved.html
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/index.html
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/Main.css
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/robots.txt
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/SignIn.html
Method	GET
Attack	

Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/signup.css
Method	GET
Attack	
Evidence	HIT
URL	https://cosc-402-group-3-project.web.app/signup.html
Method	GET
Attack	
Evidence	HIT
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-analytics.js
Method	GET
Attack	
Evidence	Age: 1586
URL	https://www.gstatic.com/firebasejs/9.21.0/firebase-app.js
Method	GET
Attack	
Evidence	Age: 1586
Instances	14
Solution	Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user: Cache-Control: no-cache, no-store, must-revalidate, private Pragma: no-cache Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
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	
WASC Id	
Plugin Id	10050