ZAP HCW

Site: https://ns1.idgt.me:10000

Generated on Wed, 23 Apr 2025 06:16:41

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	6
Low	5
Informational	12

Alerts

Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	5
CSP: Failure to Define Directive with No Fallback	Medium	5
CSP: Wildcard Directive	Medium	5
CSP: script-src unsafe-eval	Medium	5
CSP: script-src unsafe-inline	Medium	5
CSP: style-src unsafe-inline	Medium	5
Cookie without SameSite Attribute	Low	10
Insufficient Site Isolation Against Spectre Vulnerability	Low	28
Permissions Policy Header Not Set	Low	6
Strict-Transport-Security Header Not Set	Low	18
X-Content-Type-Options Header Missing	Low	13
Authentication Request Identified	Informational	2
Base64 Disclosure	Informational	2
Information Disclosure - Sensitive Information in URL	Informational	2
Modern Web Application	Informational	5
Re-examine Cache-control Directives	Informational	8
Sec-Fetch-Dest Header is Missing	Informational	15
Sec-Fetch-Mode Header is Missing	Informational	15
Sec-Fetch-Site Header is Missing	Informational	15
Sec-Fetch-User Header is Missing	Informational	19

Storable and Cacheable Content	Informational	18
Tech Detected - PWA	Informational	1
User Controllable HTML Element Attribute (Potential XSS)	Informational	3

Alert Detail

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 to a target destination without their knowledge or intent in order to perform an 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://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	<form class="form-signin session_login clearfix" action="/session_login.cgi" method="post" role="form" onsubmit="spinner()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "save" "user"].
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	<form class="form-signin session_login clearfix" action="/session_login.cgi" method="post" role="form" onsubmit="spinner()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "save" "user"].
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	<form class="form-signin session_login clearfix" action="/session_login.cgi" method="post" role="form" onsubmit="spinner()">

Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "save" "user"].
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	<form class="form-signin session_login clearfix" action="/session_login.cgi" method="post" role="form" onsubmit="spinner()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "save" "user"].
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	<form class="form-signin session_login clearfix" action="/session_login.cgi" method="post" role="form" onsubmit="spinner()">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token, _csrfToken] was found in the following HTML form: [Form 1: "pass" "save" "user"].
Instances	5
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.
	https://cheatsheetseries.owasp.org/cheatsheets/Cross-

Reference	Site_Request_Forgery_Prevention_Cheat_Sheet.html https://cwe.mitre.org/data/definitions/352.html
CWE Id	352
WASC Id	9
Plugin Id	10202

Medium	CSP: Failure to Define Directive with No Fallback
Description	The Content Security Policy fails to define one of the directives that has no fallback. Missing /excluding them is the same as allowing anything.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The directive(s): frame-ancestors, form-action is/are among the directives that do not fallback to default-src.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/

	https://github.com/HtmlUnit/htmlunit-csp 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	**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://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, font-src, media-src, object-src, manifest-src
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, font-src, media-src, object-src, manifest-src
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, font-src, media-src, object-src, manifest-src
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, font-src, media-src, object-src, manifest-src
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: style-src, img-src, connect-src, font-src, media-src, object-src,

Info	manifest-src
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp 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	CSP: script-src unsafe-eval
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://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-eval.
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-eval.
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-eval.
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-eval.
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST

Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-eval.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp 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	**CSP: script-src unsafe-inline**
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://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-inline.

URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	script-src includes unsafe-inline.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp 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	**CSP: style-src unsafe-inline**
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://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	style-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	style-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	style-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	

Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	style-src includes unsafe-inline.
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	script-src 'self' 'unsafe-inline' 'unsafe-eval'; frame-src 'self'; child-src 'self'
Other Info	style-src includes unsafe-inline.
Instances	5
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp 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

Low	**Cookie without SameSite Attribute**
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	Set-Cookie: redirect
Other Info	
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	Set-Cookie: testing
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	Set-Cookie: redirect
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	

Evidence	Set-Cookie: testing
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	Set-Cookie: redirect
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	Set-Cookie: testing
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: redirect
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	Set-Cookie: testing
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	Set-Cookie: redirect
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	Set-Cookie: testing
Other Info	
Instances	10
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	[1275](1275)
WASC Id	13

Plugin Id	10054

Low	**Insufficient Site Isolation Against Spectre Vulnerability**
Description	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	

Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOkCnqEu92Fr1Mu51xIIzI.woff2
Method	GET
Attack	
Evidence	

Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmSU5fBBc4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOmCnqEu92Fr1Mu4mxK.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	

URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
Instances	28

Solution	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided. If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Cross-Origin_Resource_Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low	**Permissions Policy Header Not Set**
Description	Permissions Policy Header is an added layer of security that helps to restrict from unauthorized access or usage of browser/client features by web resources. This policy ensures the user privacy by limiting or specifying the features of the browsers can be used by the web resources. Permissions Policy provides a set of standard HTTP headers that allow website owners to limit which features of browsers can be used by the page such as camera, microphone, location, full screen etc.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET

Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
Instances	6
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Permissions-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Permissions-Policy https://developer.chrome.com/blog/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	**Strict-Transport-Security Header Not Set**
Description	HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET

Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?233000009999999999
Method	GET
Attack	
Evidence	

Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOkCnqEu92Fr1Mu51xIIzI.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmSU5fBBc4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOmCnqEu92Fr1Mu4mxK.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other	

Info	
Instances	18
Solution	Ensure that your web server, application server, load balancer, etc. is configured to enforce Strict-Transport-Security.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html 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	**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://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
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://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
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://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
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://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://ns1.idgt.me:10000/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://ns1.idgt.me:10000/service-worker.js
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://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?233000009999999999
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://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?233000009999999999
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://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?233000009999999999
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://ns1.idgt.me:10000/unauthenticated/fonts/KFOkCnqEu92Fr1Mu51xIIzI.woff2
Method	GET
Attack	
Evidence	
Other	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

Info	away from their actual content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
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://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmSU5fBBc4.woff2
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://ns1.idgt.me:10000/unauthenticated/fonts/KFOmCnqEu92Fr1Mu4mxK.woff2
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	13
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	**Authentication Request Identified**
Description	The given request has been identified as an authentication request. The 'Other Info' field contains a set of key=value lines which identify any relevant fields. If the request is in a context which has an Authentication Method set to "Auto-Detect" then this rule will change the authentication to match the request identified.
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	pass
Other Info	userParam=user userValue=VCZLycOB passwordParam=pass referer=https://ns1.idgt.me:10000/

URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	pass
Other Info	userParam=user userValue=ZAP passwordParam=pass referer=https://ns1.idgt.me:10000/sitemap.xml
Instances	2
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	https://www.zaproxy.org/docs/desktop/addons/authentication-helper/auth-req-id/
CWE Id	
WASC Id	
Plugin Id	10111

Informational	Base64 Disclosure
Description	Base64 encoded data was disclosed by the application/web server. Note: in the interests of performance not all base64 strings in the response were analyzed individually, the entire respor should be looked at by the analyst/security team/developer(s).
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?2330000099999999999
Method	GET
Attack	
Evidence	iVBORw0KGgoAAAANSUhEUgAAAAgAAAAICAYAAADED76LAAAANElEQVQYV2NkIAAYiVb /Y6DiM1ANJoyMjGdBbLgJQAX /kU0DKgDLkaQAvxW4HEvQFwCRcxIJK1XznAAAAABJRU5ErkJggg==
Other Info	‰PNG \x001a \x0000\x0000\x0000 IHDR\x0000\x0000\x0000\x0008\x0000\x0000\x0000\x0008\x0008\x0006\x0000\x0000\x0000Ä ‹\x0000\x0000\x00004IDAT\x0018Wcd \x0000\x0018‰Vðÿÿ•c â3P &ŒŒŒgAl¸ @\x0005ÿ ‘M\x0003*\x0000Ë‘¤\x0000¿\x0015¸\x001cKĐ\x0017\x0000‘s\x0012 +Uóœ\x0000\x0000\x0000\x0000IEND®B`,
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?2330000099999999999
Method	GET
Attack	
Evidence	/fonts/KFOkCnqEu92Fr1Mu51xIIzI
Other Info	ýú'¶ÏÊ\x0014é\x0002ž¡.÷akÔË¹×\x0012\x0008Ì
Instances	2
Solution	Manually confirm that the Base64 data does not leak sensitive information, and that the data ca be aggregated/used to exploit other vulnerabilities.
Reference	https://projects.webappsec.org/w/page/13246936/Information%20Leakage
CWE Id	319
WASC Id	13
Plugin Id	10094

Informational	Information Disclosure - Sensitive Information in URL
Description	The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.
URL	https://ns1.idgt.me:10000/session_login.cgi?user=ZAP&pass=ZAP&save=1
Method	GET

Attack	
Evidence	pass
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass pass
URL	https://ns1.idgt.me:10000/session_login.cgi?user=ZAP&pass=ZAP&save=1
Method	GET
Attack	
Evidence	user
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: user user
Instances	2
Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	598
WASC Id	13
Plugin Id	10024

Informational	**Modern Web Application**
Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	<script src="/service-worker.js" type="application/javascript" defer></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	<script src="/service-worker.js" type="application/javascript" defer></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	<script src="/service-worker.js" type="application/javascript" defer></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	<script src="/service-worker.js" type="application/javascript" defer></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	https://ns1.idgt.me:10000/session_login.cgi

Method	POST
Attack	
Evidence	<script src="/service-worker.js" type="application/javascript" defer></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	5
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	[10109](10109)

Informational	Re-examine Cache-control Directives
Description	The cache-control header has not been set properly or is missing, allowing the browser and proxies to cache content. For static assets like css, js, or image files this might be intended, however, the resources should be reviewed to ensure that no sensitive content will be cached.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	public; max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOkCnqEu92Fr1Mu51xIIzI.woff2
Method	GET
Attack	
Evidence	public; max-age=604800

Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Method	GET
Attack	
Evidence	public; max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmSU5fBBc4.woff2
Method	GET
Attack	
Evidence	public; max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOmCnqEu92Fr1Mu4mxK.woff2
Method	GET
Attack	
Evidence	public; max-age=604800
Other Info	
Instances	8
Solution	For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, must-revalidate". If an asset should be cached consider setting the directives "public, max-age, immutable".
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching 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	Sec-Fetch-Dest Header is Missing
Description	Specifies how and where the data would be used. For instance, if the value is audio, then the requested resource must be audio data and not any other type of resource.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	
Other Info	

URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi?user=ZAP&pass=ZAP&save=1
Method	GET

Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
Instances	15
Solution	Ensure that Sec-Fetch-Dest header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Dest
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	**Sec-Fetch-Mode Header is Missing**
Description	Allows to differentiate between requests for navigating between HTML pages and requests for loading resources like images, audio etc.

URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET

Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi?user=ZAP&pass=ZAP&save=1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	

Evidence	
Other Info	
Instances	15
Solution	Ensure that Sec-Fetch-Mode header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Mode
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	**Sec-Fetch-Site Header is Missing**
Description	Specifies the relationship between request initiator's origin and target's origin.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET

Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi?user=ZAP&pass=ZAP&save=1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?233000009999999999
Method	GET
Attack	
Evidence	

Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?233000009999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
Instances	15
Solution	Ensure that Sec-Fetch-Site header is included in request headers.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-Site
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	Sec-Fetch-User Header is Missing
Description	Specifies if a navigation request was initiated by a user.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET
Attack	

Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi?user=ZAP&pass=ZAP&save=1
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	

Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?2330000099999999999
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOkCnqEu92Fr1Mu51xIIzI.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmSU5fBBc4.woff2
Method	GET
Attack	
Evidence	
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOmCnqEu92Fr1Mu4mxK.woff2
Method	GET
Attack	
Evidence	
Other Info	

URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	
Instances	19
Solution	Ensure that Sec-Fetch-User header is included in user initiated requests.
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Sec-Fetch-User
CWE Id	352
WASC Id	9
Plugin Id	90005

Informational	Storable and Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. 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 "shared" 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://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://ns1.idgt.me:10000/images/favicons/webmin/android-chrome-192x192.png
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/apple-touch-icon.png
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-16x16.png
Method	GET
Attack	
Evidence	max-age=604800
Other Info	

URL	https://ns1.idgt.me:10000/images/favicons/webmin/favicon-32x32.png
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/images/favicons/webmin/safari-pinned-tab.svg
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://ns1.idgt.me:10000/manifest-webmin.json
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://ns1.idgt.me:10000/robots.txt
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/service-worker.js
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/sitemap.xml
Method	GET
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
URL	https://ns1.idgt.me:10000/unauthenticated/css/bundle.min.css?2330000099999999
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/fonts-roboto.min.css?2330000099999999
Method	GET

Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/css/palettes/nightrider.min.css?233000009999999999
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOkCnqEu92Fr1Mu51xIIzI.woff2
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmEU9fBBc4.woff2
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOlCnqEu92Fr1MmSU5fBBc4.woff2
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/unauthenticated/fonts/KFOmCnqEu92Fr1Mu4mxK.woff2
Method	GET
Attack	
Evidence	max-age=604800
Other Info	
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	In the absence of an explicitly specified caching lifetime directive in the response, a liberal lifetime heuristic of 1 year was assumed. This is permitted by rfc7234.
Instances	18
	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:

Solution	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://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Informational	Tech Detected - PWA
Description	The following "Miscellaneous" technology was identified: PWA. Described as: Progressive Web Apps (PWAs) are web apps built and enhanced with modern APIs to deliver enhanced capabilities, reliability, and installability while reaching anyone, anywhere, on any device, all with a single codebase.
URL	https://ns1.idgt.me:10000/
Method	GET
Attack	
Evidence	
Other Info	
Instances	1
Solution	
Reference	https://web.dev/progressive-web-apps/
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	User Controllable HTML Element Attribute (Potential XSS)
Description	This check looks at user-supplied input in query string parameters and POST data to identify where certain HTML attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scripting) that will require further review by a security analyst to determine exploitability.
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://ns1.idgt.me:10000 /session_login.cgi appears to include user input in: a(n) [input] tag [value] attribute The user input found was: pass=ZAP The user-controlled value was: zap
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST

Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://ns1.idgt.me:10000/session_login.cgi appears to include user input in: a(n) [input] tag [value] attribute The user input found was: user=VCZLycOB The user-controlled value was: vczlycob
URL	https://ns1.idgt.me:10000/session_login.cgi
Method	POST
Attack	
Evidence	
Other Info	User-controlled HTML attribute values were found. Try injecting special characters to see if XSS might be possible. The page at the following URL: https://ns1.idgt.me:10000/session_login.cgi appears to include user input in: a(n) [input] tag [value] attribute The user input found was: user=ZAP The user-controlled value was: zap
Instances	3
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html
CWE Id	20
WASC Id	20
Plugin Id	10031