Site: https://140.112.36.2

Generated on , 4 5 2026 14:42:13

ZAP Version: 2.17.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	1
Informational	17

Insights

Level	Reason	Site	Description	Statistic
Low	Warning		ZAP warnings logged - see the zap.log file for details	12
	Informational	https://140.112.36.2	Percentage of responses with status code 2xx	75 %
	Informational	https://140.112.36.2	Percentage of responses with status code 3xx	17 %
	Informational	https://140.112.36.2	Percentage of responses with status code 4xx	7 %
	Informational	https://140.112.36.2	Percentage of endpoints with content type application/javascript	6 %
	Informational		Percentage of endpoints with	10 %

		https://140.112.36.2	content type image/jpeg	
	Informational	https://140.112.36.2	Percentage of endpoints with content type image/png	10 %
	Informational	https://140.112.36.2	Percentage of endpoints with content type image/svg+xml	2 %
	Informational	https://140.112.36.2	Percentage of endpoints with content type text/css	4 %
	Informational	https://140.112.36.2	Percentage of endpoints with content type text/html	58 %
	Informational	https://140.112.36.2	Percentage of endpoints with method GET	95 %
	Informational	https://140.112.36.2	Percentage of endpoints with method POST	4 %
	Informational	https://140.112.36.2	Count of total endpoints	254
	Informational	https://140.112.36.2	Percentage of slow responses	71 %

	Risk Level	Number of Instances
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	Systemic
Modern Web Application	Informational	Systemic
Re-examine Cache-control Directives	Informational	Systemic
Session Management Response Identified	Informational	22

Tech Detected - Animate.css	Informational	1
Tech Detected - Bootstrap	Informational	1
Tech Detected - Bootstrap Icons	Informational	1
Tech Detected - HSTS	Informational	1
Tech Detected - Microsoft ASP.NET	Informational	1
Tech Detected - Moment.js	Informational	1
Tech Detected - Nginx	Informational	1
Tech Detected - Parsley.js	Informational	1
Tech Detected - Select2	Informational	1
Tech Detected - Ubuntu	Informational	1
Tech Detected - WOW	Informational	1
Tech Detected - jQuery	Informational	1
Tech Detected - jQuery BlockUI	Informational	1
User Controllable HTML Element Attribute (Potential XSS)	Informational	1

Alert Detail

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://140.112.36.2/AlumniCard
Node Name	https://140.112.36.2/AlumniCard
	GET
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://140.112.36.2/AlumniInfo
Node Name	https://140.112.36.2/AlumniInfo
	GET
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://140.112.36.2/AlumniServe/FindAlumni
Node Name	https://140.112.36.2/AlumniServe/FindAlumni
	GET
Evidence	nginx/1.18.0 (Ubuntu)
Other	

Info	
URL	https://140.112.36.2/robots.txt
Node Name	https://140.112.36.2/robots.txt
	GET
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
URL	https://140.112.36.2/sitemap.xml
Node Name	https://140.112.36.2/sitemap.xml
	GET
Evidence	nginx/1.18.0 (Ubuntu)
Other Info	
Instances	Systemic
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress the "Server" header or provide generic details.
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	497
WASC Id	13
Plugin Id	10036

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://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://140.112.36.2/
Node Name	https://140.112.36.2/
	GET
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://140.112.36.2/AlumniServe/AlumniCardInfo

Node Name	https://140.112.36.2/AlumniServe/AlumniCardInfo
	GET
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://140.112.36.2/News/NewsDetail/NN00000394
Node Name	https://140.112.36.2/News/NewsDetail/NN00000394
	GET
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	https://140.112.36.2/News/NewsDetail/NN00000396
Node Name	https://140.112.36.2/News/NewsDetail/NN00000396
	GET
Evidence	
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
Instances	Systemic
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	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://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	no-cache, no-store
Other Info	
URL	https://140.112.36.2/
Node Name	https://140.112.36.2/
	GET

Evidence	no-cache, no-store
Other Info	
URL	https://140.112.36.2/AlumniServe/AlumniCardInfo
Node Name	https://140.112.36.2/AlumniServe/AlumniCardInfo
	GET
Evidence	no-cache, no-store
Other Info	
URL	https://140.112.36.2/News/NewsDetail/NN00000394
Node Name	https://140.112.36.2/News/NewsDetail/NN00000394
	GET
Evidence	no-cache, no-store
Other Info	
URL	https://140.112.36.2/News/NewsDetail/NN00000396
Node Name	https://140.112.36.2/News/NewsDetail/NN00000396
	GET
Evidence	no-cache, no-store
Other Info	
Instances	Systemic
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/Reference/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/
CWE Id	525
WASC Id	13
Plugin Id	10015

Informational	**Session Management Response Identified**
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	https://140.112.36.2
Node	

Name	https://140.112.36.2
	GET
Evidence	.AspNetCore.Antiforgery.FHLYmWbUJH8
Other Info	cookie:.AspNetCore.Antiforgery.FHLYmWbUJH8
URL	https://140.112.36.2/About/About?LangCode=tw
Node Name	https://140.112.36.2/About/About (LangCode)
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/Activity/ActivityList
Node Name	https://140.112.36.2/Activity/ActivityList
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/AlumniCard
Node Name	https://140.112.36.2/AlumniCard
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/AlumniInfo
Node Name	https://140.112.36.2/AlumniInfo
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/AlumniReunion
Node Name	https://140.112.36.2/AlumniReunion
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other	

Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/AlumniServe/AlumniCardInfo
Node Name	https://140.112.36.2/AlumniServe/AlumniCardInfo
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/AlumniServe/FindAlumni
Node Name	https://140.112.36.2/AlumniServe/FindAlumni
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/AlumniZone/ClassDirectory
Node Name	https://140.112.36.2/AlumniZone/ClassDirectory
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/Communicate/AlumniDynamic
Node Name	https://140.112.36.2/Communicate/AlumniDynamic
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/Communicate/Submission
Node Name	https://140.112.36.2/Communicate/Submission
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/FAQ/FAQList
Node Name	https://140.112.36.2/FAQ/FAQList
	GET

Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/Home/ForgetAua8
Node Name	https://140.112.36.2/Home/ForgetAua8
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000251
Node Name	https://140.112.36.2/News/NewsDetail/NN00000251
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000324
Node Name	https://140.112.36.2/News/NewsDetail/NN00000324
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000333
Node Name	https://140.112.36.2/News/NewsDetail/NN00000333
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000392
Node Name	https://140.112.36.2/News/NewsDetail/NN00000392
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000393

Node Name	https://140.112.36.2/News/NewsDetail/NN00000393
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000394
Node Name	https://140.112.36.2/News/NewsDetail/NN00000394
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/News/NewsDetail/NN00000396
Node Name	https://140.112.36.2/News/NewsDetail/NN00000396
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2/OutstandingAlumni/SelectRegulation
Node Name	https://140.112.36.2/OutstandingAlumni/SelectRegulation
	GET
Evidence	.AspNetCore.Mvc.CookieTempDataProvider
Other Info	cookie:.AspNetCore.Mvc.CookieTempDataProvider
URL	https://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	.AspNetCore.Antiforgery.FHLYmWbUJH8
Other Info	cookie:.AspNetCore.Antiforgery.FHLYmWbUJH8
Instances	22
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/session-mgmt-id/
CWE Id	
WASC Id	
Plugin Id	10112

Informational	Tech Detected - Animate.css
Description	The following "UI frameworks" technology was identified: Animate.css. Described as: Animate.css is a ready-to-use library collection of CSS3 animation effects.
URL	https://140.112.36.2/
Node Name	https://140.112.36.2/
	GET
Evidence	/animate.min.css
Other Info	
Instances	1
Solution	
Reference	https://animate.style
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Bootstrap
Description	The following "UI frameworks" technology was identified: Bootstrap. Described as: Bootstrap is a free and open-source CSS framework directed at responsive, mobile-first front-end web development. It contains CSS and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components.
URL	https://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	<link href="/areas/frontend/css/bootstrap.min.css
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:getbootstrap:bootstrap:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Bootstrap Icons
Description	The following "Font scripts" technology was identified: Bootstrap Icons. Described as: Bootstrap Icons is a growing library of SVG icons that are designed by @mdo and maintained by the Bootstrap Team.

URL	https://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	bootstrap-icons.
Other Info	The following version(s) is/are associated with the identified tech: .
Instances	1
Solution	
Reference	https://icons.getbootstrap.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - HSTS**
Description	The following "Security" technology was identified: HSTS. Described as: HTTP Strict Transport Security (HSTS) informs browsers that the site should only be accessed using HTTPS.
URL	https://140.112.36.2/sitemap.xml
Node Name	https://140.112.36.2/sitemap.xml
	GET
Evidence	Strict-Transport-Security
Other Info	
Instances	1
Solution	
Reference	https://www.rfc-editor.org/rfc/rfc6797#section-6.1
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Microsoft ASP.NET**
Description	The following "Web frameworks" technology was identified: Microsoft ASP.NET. Described as: ASP.NET is an open-source, server-side web-application framework designed for web development to produce dynamic web pages.
URL	https://140.112.36.2/AlumniServe/FindAlumni
Node Name	https://140.112.36.2/AlumniServe/FindAlumni
	GET

Evidence	.AspNetCore
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:microsoft:asp.net:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://www.asp.net
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Moment.js**
Description	The following "JavaScript libraries" technology was identified: Moment.js. Described as: Moment.js is a free and open-source JavaScript library that removes the need to use the native JavaScript Date object directly.
URL	https://140.112.36.2/
Node Name	https://140.112.36.2/
	GET
Evidence	moment.min.js
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:momentjs:moment:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://momentjs.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - Nginx**
Description	The following "Web servers, Reverse proxies" technology was identified: Nginx. Described as: Nginx is a web server that can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache.
URL	https://140.112.36.2/sitemap.xml
Node Name	https://140.112.36.2/sitemap.xml
	GET
Evidence	nginx/1.18.0
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:* The following version(s) is/are associated with the identified tech: 1.18.0
Instances	1

Solution	
Reference	https://nginx.org/en
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Parsley.js
Description	The following "JavaScript libraries" technology was identified: Parsley.js. Described as: Javascript forms validation script.
URL	https://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	parsley.min.js
Other Info	
Instances	1
Solution	
Reference	https://parsleyjs.org
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Select2
Description	The following "JavaScript libraries" technology was identified: Select2. Described as: Select2 is a jQuery based replacement for select boxes. It supports searching, remote data sets, and infinite scrolling of results.
URL	https://140.112.36.2/
Node Name	https://140.112.36.2/
	GET
Evidence	select2.min.js
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:select2:select2:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://select2.org/
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - Ubuntu
Description	The following "Operating systems" technology was identified: Ubuntu. Described as: Ubuntu is a free and open-source operating system on Linux for the enterprise server, desktop, cloud, and IoT.
URL	https://140.112.36.2/AlumniServe/FindAlumni
Node Name	https://140.112.36.2/AlumniServe/FindAlumni
	GET
Evidence	Ubuntu
Other Info	The following CPE is associated with the identified tech: cpe:2.3:o:canonical:ubuntu_linux:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://www.ubuntu.com/server
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - WOW
Description	The following "JavaScript frameworks, Web frameworks, JavaScript graphics" technology was identified: WOW. Described as: Reveal CSS animation as you scroll down a page.
URL	https://140.112.36.2/AlumniServe/AlumniCardInfo
Node Name	https://140.112.36.2/AlumniServe/AlumniCardInfo
	GET
Evidence	wow.min.js
Other Info	
Instances	1
Solution	
Reference	https://www.delac.io/WOW
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	Tech Detected - jQuery
Description	The following "JavaScript libraries" technology was identified: jQuery. Described as:

	jQuery is a JavaScript library which is a free, open-source software designed to simplify HTML DOM tree traversal and manipulation, as well as event handling, CSS animation, and Ajax.
URL	https://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	jquery
Other Info	The following CPE is associated with the identified tech: cpe:2.3:a:jquery:jquery:*:*:*:*:*:*:*:*
Instances	1
Solution	
Reference	https://jquery.com
CWE Id	
WASC Id	13
Plugin Id	10004

Informational	**Tech Detected - jQuery BlockUI**
Description	The following "JavaScript libraries" technology was identified: jQuery BlockUI. Described as: jQuery BlockUI is a plugin that simulates synchronous behavior in AJAX by temporarily blocking user interaction and adding DOM elements that visually indicate restricted activity until the block is removed.
URL	https://140.112.36.2
Node Name	https://140.112.36.2
	GET
Evidence	/jquery.blockUI.js
Other Info	
Instances	1
Solution	
Reference	https://jquery.malsup.com/block
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://140.112.36.2/About/About?LangCode=en
Node Name	https://140.112.36.2/About/About (LangCode)

	GET
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://140.112.36.2/About/About?LangCode=en appears to include user input in: a(n) [html] tag [lang] attribute The user input found was: LangCode=en The user-controlled value was: en
Instances	1
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