OWASP ZAP Scan Report

Target: https://diplomasite.northeurope.cloudapp.azure.com/

All scanned sites: https://diplomasite.northeurope.cloudapp.azure.com

Javascript included from: https://cdn.jsdelivr.net https://diplomasite.northeurope.cloudapp.azure.com

Generated on Fri, 16 Jun 2023 03:22:09

ZAP Version: 2.12.0

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	3
Informational	2

Alerts

Name	Risk Level	Number of Instances
Content Security Policy (CSP) Header Not Set	Medium	10
Cookie No HttpOnly Flag	Low	2
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	14
Strict-Transport-Security Header Not Set	Low	13
Re-examine Cache-control Directives	Informational	8
User Controllable HTML Element Attribute (Potential XSS)	Informational	12

Alert Detail

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 certain types of attacks, including 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://diplomasite.northeurope.cloudapp.azure.com/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/+/-/_
Method	GET

Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/events
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues?page=1
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/login/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	
Attack	

Evidence	
Instances	10
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy 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

Low	**Cookie No HttpOnly Flag**
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	GET
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	csrftoken
Attack	
Evidence	Set-Cookie: csrftoken
Instances	2
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

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://diplomasite.northeurope.cloudapp.azure.com/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/+/-/_
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)

URL	https://diplomasite.northeurope.cloudapp.azure.com/events
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues?page=1
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/login/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/show_venue/1
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_csv/
Method	GET

Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_pdf/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_text/
Method	GET
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	
Attack	
Evidence	Apache/2.4.41 (Ubuntu)
Instances	14
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 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://diplomasite.northeurope.cloudapp.azure.com/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/+/-/_
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/events
Method	GET
Parameter	

Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues?page=1
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/login/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_csv/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_pdf/
Method	GET
Parameter	
Attack	
Evidence	

URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_text/
Method	GET
Parameter	
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	
Attack	
Evidence	
Instances	13
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 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

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://diplomasite.northeurope.cloudapp.azure.com/
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/events
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/list_venues?page=1
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user

Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_csv/
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/venue_text/
Method	GET
Parameter	Cache-Control
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	Cache-Control
Attack	
Evidence	
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	**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://diplomasite.northeurope.cloudapp.azure.com/list_venues?page=1
Method	GET
Parameter	page
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	email
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST

Parameter	first_name
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	first_name
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	last_name
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	last_name
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	password1
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	password1
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	password2
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	password2
Attack	
Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	username
Attack	

Evidence	
URL	https://diplomasite.northeurope.cloudapp.azure.com/members/register_user
Method	POST
Parameter	username
Attack	
Evidence	
Instances	12
Solution	Validate all input and sanitize output it before writing to any HTML attributes.
Reference	http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute
CWE Id	20
WASC Id	20
Plugin Id	10031