ZAP Scanning Report

Sites: https://api.vantagecircle.co.in http://api.vantagecircle.co.in

Generated on Fri, 22 Nov 2024 11:42:50

ZAP Version: 2.15.0

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	7
Low	4
Informational	9
False Positives:	0

Alerts

Name	Risk Level	Number of Instances
Cloud Metadata Potentially Exposed	High	1
Absence of Anti-CSRF Tokens	Medium	2
CSP: Wildcard Directive	Medium	13
CSP: script-src unsafe-inline	Medium	13
CSP: style-src unsafe-inline	Medium	13
Cross-Domain Misconfiguration	Medium	56
Hidden File Found	Medium	4
Vulnerable JS Library	Medium	6
Cookie without SameSite Attribute	Low	7
Cross-Domain JavaScript Source File Inclusion	Low	12
Strict-Transport-Security Header Not Set	Low	10
X-Content-Type-Options Header Missing	Low	47
Authentication Request Identified	Informational	8
Charset Mismatch (Header Versus Meta Content-Type Charset)	Informational	6
Information Disclosure - Sensitive Information in URL	Informational	4
Information Disclosure - Suspicious Comments	Informational	28
Loosely Scoped Cookie	Informational	37
Modern Web Application	Informational	10
Session Management Response Identified	Informational	49
User Agent Fuzzer	Informational	60
User Controllable HTML Element Attribute (Potential XSS)	Informational	33

Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure. All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.

URL	http://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	1
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the $host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/
CWE Id	
WASC Id	
Plugin Id	90034

Medium	**Absence of Anti-CSRF Tokens**
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request 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://api.vantagecircle.co.in/
Method	POST
Parameter	
Attack	
Evidence	<form name="userForm" ng-submit="userForm.$valid && !conf_error && submituserinfo(user)">
Other Info	No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 1: "accepterm" "email" "gender" "mobile" "name" "password" "regularalert" "year"].
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	
Attack	
Evidence	<form name="userForm" ng-submit="userForm.$valid && !conf_error && submituserinfo(user)">
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] was found in the following HTML form: [Form 1: "accepterm" "email" "gender" "mobile" "name" "password" "regularalert" "year"].
Instances	2

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	https://cheatsheetseries.owasp.org/cheatsheets/Cross-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: 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://api.vantagecircle.co.in/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/._darcs
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/.bzr
Method	GET
Parameter	Content-Security-Policy

Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/.hg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'

Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: script-src, style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, object-src, manifest-src, worker-src, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	13
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://api.vantagecircle.co.in/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/._darcs
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/.bzr
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/.hg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/latest/meta-data/

Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	script-src includes unsafe-inline.
Instances	13
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://api.vantagecircle.co.in/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'

Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/._darcs
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/.bzr
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/.hg
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'

Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self' http: https: data: blob: 'unsafe-inline' 'unsafe-eval'
Other Info	style-src includes unsafe-inline.
Instances	13
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	**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://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/._darcs
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/.bzr
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/.hg
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/apple-touch-icon.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/css/ajax-loader.gif

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/css/common/common-home.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/css/images/favicon.ico
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/css/newreg_common.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/css/ui/custom.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/favicon-16x16.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	https://api.vantagecircle.co.in/favicon-32x32.png
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/safari-pinned-tab.svg
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *

Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/site.webmanifest
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/animate.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/circle.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/cms/custom-vc-style.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/cms/new_homepage_v1.css
Method	GET
Parameter	
Attack	

Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/cms/style.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/homepage.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/ie8.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/css/new_styles/vc_custom1.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/cms/custom-vc-script.js
Method	GET
Parameter	

Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/cms/navigation.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/cms/seo-custom-js.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/html5shiv.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/jquery.jcarousel.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/respond.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-aria.min.js
Method	GET

Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-route.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-sanitize.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-recaptcha.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/angular-input-match.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/infinite-scroll.min.js
Method	GET

Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-0.12.0.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-tpls-0.12.0.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/userregister.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/clipboard/clipboard.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/clipboard/ngclipboard.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jquery.cookie.js

Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jquery.lazyload.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jwt-decode.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assetsv2/bootstrap.min.css
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assetsv2/jquery-vantage.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assetsv2/jquery.min.js
Method	GET
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.

URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	
Attack	
Evidence	Access-Control-Allow-Origin: *
Other Info	The CORS misconfiguration on the web server permits cross-domain read requests from arbitrary third party domains, using unauthenticated APIs on this domain. Web browser implementations do not permit arbitrary third parties to read the response from authenticated APIs, however. This reduces the risk somewhat. This misconfiguration could be used by an attacker to access data that is available in an unauthenticated manner, but which uses some other form of security, such as IP address white-listing.
Instances	56
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	**Hidden File Found**
Description	A sensitive file was identified as accessible or available. This may leak administrative, configuration, or credential information which can be leveraged by a malicious individual to further attack the system or conduct social engineering efforts.
URL	http://api.vantagecircle.co.in/._darcs
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 301 Moved Permanently
Other Info	
URL	http://api.vantagecircle.co.in/.bzr
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 301 Moved Permanently
Other Info	
URL	http://api.vantagecircle.co.in/.hg
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 301 Moved Permanently

Other Info	
URL	http://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	HTTP/1.1 301 Moved Permanently
Other Info	
Instances	4
Solution	Consider whether or not the component is actually required in production, if it isn't then disable it. If it is then ensure access to it requires appropriate authentication and authorization, or limit exposure to internal systems or specific source IPs, etc.
Reference	https://blog.hboeck.de/archives/892-Introducing-Snallygaster-a-Tool-to-Scan-for-Secrets-on-Web-Servers.html
CWE Id	538
WASC Id	13
Plugin Id	40035

Medium	**Vulnerable JS Library**
Description	The identified library bootstrap, version 3.3.7 is vulnerable.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/bootstrap.min.js
Method	GET
Parameter	
Attack	
Evidence	* Bootstrap v3.3.7
Other Info	CVE-2018-14041 CVE-2019-8331 CVE-2018-20677 CVE-2018-20676 CVE-2018-14042 CVE-2016-10735 CVE-2024-6484
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-aria.min.js
Method	GET
Parameter	
Attack	
Evidence	/* AngularJS v1.8.0
Other Info	CVE-2023-26116 CVE-2022-25869 CVE-2022-25844 CVE-2024-21490 CVE-2024-8373 CVE-2024-8372 CVE-2023-26117 CVE-2023-26118
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-route.min.js
Method	GET
Parameter	
Attack	
Evidence	/* AngularJS v1.8.0
Other Info	CVE-2023-26116 CVE-2022-25869 CVE-2022-25844 CVE-2024-21490 CVE-2024-8373 CVE-2024-8372 CVE-2023-26117 CVE-2023-26118
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-sanitize.min.js
Method	GET
Parameter	
Attack	
Evidence	/* AngularJS v1.8.0
Other Info	CVE-2023-26116 CVE-2022-25869 CVE-2022-25844 CVE-2024-21490 CVE-2024-8373 CVE-2024-8372 CVE-2023-26117 CVE-2023-26118
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	
Attack	
Evidence	/* AngularJS v1.8.0
Other Info	CVE-2023-26116 CVE-2022-25869 CVE-2022-25844 CVE-2024-21490 CVE-2024-8373 CVE-2024-8372 CVE-2023-26117 CVE-2023-26118
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-0.12.0.min.js

Method	GET
Parameter	
Attack	
Evidence	bootstrap-0.12.0.min.js
Other Info	CVE-2018-14041 CVE-2018-20677 CVE-2018-20676 CVE-2018-14042
Instances	6
Solution	Please upgrade to the latest version of bootstrap.
Reference	https://nvd.nist.gov/vuln/detail/CVE-2024-6484 https://github.com/advisories/GHSA-pj7m-g53m-7638 https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap-sass/CVE-2024-6484.yml https://github.com/twbs/bootstrap/issues/20631 https://github.com/advisories/GHSA-9mvj-f7w8-pvh2 https://github.com/advisories/GHSA-9v3m-8fp8-mj99 https://github.com/twbs/bootstrap/issues/28236 https://github.com/twbs/bootstrap/issues/20184 https://www.herodevs.com/vulnerability-directory/cve-2024-6484 https://github.com/advisories/GHSA-ph58-4vrj-w6hr https://github.com/twbs/bootstrap https://github.com/advisories/GHSA-4p24-vmcr-4gqj https://github.com/rubysec/ruby-advisory-db/blob/master/gems/bootstrap/CVE-2024-6484.yml https://nvd.nist.gov/vuln/detail/CVE-2018-20676
CWE Id	829
WASC Id	
Plugin Id	10003

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://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Uat_Vantagecircle

Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	Set-Cookie: Uat_Vantagecircle
Other Info	
Instances	7
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
WASC Id	13
Plugin Id	10054

Low	**Cross-Domain JavaScript Source File Inclusion**
Description	The page includes one or more script files from a third-party domain.
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	https://accounts.google.com/gsi/client
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client"></script>
Other Info	
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	https://unpkg.com/jwt-decode/build/jwt-decode.js
Attack	
Evidence	<script src="https://unpkg.com/jwt-decode/build/jwt-decode.js"></script>
Other Info	
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit"></script>
Other Info	
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	https://accounts.google.com/gsi/client
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client"></script>
Other Info	

URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	https://unpkg.com/jwt-decode/build/jwt-decode.js
Attack	
Evidence	<script src="https://unpkg.com/jwt-decode/build/jwt-decode.js"></script>
Other Info	
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit"></script>
Other Info	
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	https://accounts.google.com/gsi/client
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client"></script>
Other Info	
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	https://unpkg.com/jwt-decode/build/jwt-decode.js
Attack	
Evidence	<script src="https://unpkg.com/jwt-decode/build/jwt-decode.js"></script>
Other Info	
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit"></script>
Other Info	
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	https://accounts.google.com/gsi/client
Attack	
Evidence	<script src="https://accounts.google.com/gsi/client"></script>
Other Info	
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	https://unpkg.com/jwt-decode/build/jwt-decode.js
Attack	
Evidence	<script src="https://unpkg.com/jwt-decode/build/jwt-decode.js"></script>
Other Info	
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1

Method	POST
Parameter	https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit
Attack	
Evidence	<script type="text/javascript" src="https://www.google.com/recaptcha/api.js?onload=vcRecaptchaApiLoaded&render=explicit"></script>
Other Info	
Instances	12
Solution	Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.
Reference	
CWE Id	829
WASC Id	15
Plugin Id	10017

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://api.vantagecircle.co.in/._darcs
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/.bzr
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/.hg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	

Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/safari-pinned-tab.svg
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	
Instances	10
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://api.vantagecircle.co.in/
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET

Parameter	x-content-type-options
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://api.vantagecircle.co.in/apple-touch-icon.png
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/css/ajax-loader.gif
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/css/common/common-home.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/css/images/favicon.ico
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/css/newreg_common.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/css/ui/custom.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/favicon-16x16.png

Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/favicon-32x32.png
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/safari-pinned-tab.svg
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/site.webmanifest
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/animate.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/circle.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/cms/custom-vc-style.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/cms/new_homepage_v1.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/cms/style.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/homepage.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/ie8.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/css/new_styles/vc_custom1.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/bootstrap.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/cms/custom-vc-script.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/cms/navigation.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/cms/seo-custom-js.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/html5shiv.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/jquery.jcarousel.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/js/respond.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-aria.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-route.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-sanitize.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-recaptcha.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/angular-input-match.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/infinite-scroll.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-0.12.0.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-tpls-0.12.0.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/userregister.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/clipboard/clipboard.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/clipboard/ngclipboard.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jquery.cookie.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jquery.lazyload.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jwt-decode.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assetsv2/bootstrap.min.css
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assetsv2/jquery-vantage.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/themes/dealspoint/assetsv2/jquery.min.js
Method	GET
Parameter	x-content-type-options
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://api.vantagecircle.co.in/
Method	POST
Parameter	x-content-type-options
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	x-content-type-options
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	47
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	email

Attack	
Evidence	password
Other Info	userParam=email userValue=zaproxy@example.com passwordParam=password referer=https://api.vantagecircle.co.in/
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=1 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/ csrfToken=VANTAGECIRCLE_CSRF_TOKEN
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=2 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/ csrfToken=VANTAGECIRCLE_CSRF_TOKEN
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=3 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/ csrfToken=VANTAGECIRCLE_CSRF_TOKEN
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=4 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/ csrfToken=VANTAGECIRCLE_CSRF_TOKEN
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=1 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 csrfToken=VANTAGECIRCLE_CSRF_TOKEN
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=2 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 csrfToken=VANTAGECIRCLE_CSRF_TOKEN

URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	LoginForm[attempt]
Attack	
Evidence	LoginForm[password]
Other Info	userParam=LoginForm[attempt] userValue=3 passwordParam=LoginForm[password] referer=https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 csrfToken=VANTAGECIRCLE_CSRF_TOKEN
Instances	8
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	**Charset Mismatch (Header Versus Meta Content-Type Charset)**
Description	This check identifies responses where the HTTP Content-Type header declares a charset different from the charset defined by the body of the HTML or XML. When there's a charset mismatch between the HTTP header and content body Web browsers can be forced into an undesirable content-sniffing mode to determine the content's correct character set. An attacker could manipulate content on the page to be interpreted in an encoding of their choice. For example, if an attacker can control content at the beginning of the page, they could inject script using UTF-7 encoded text and manipulate some browsers into interpreting that text.
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET

Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	There was a charset mismatch between the HTTP Header and the META content-type encoding declarations: [UTF-8] and [iso-8859-1] do not match.
Instances	6
Solution	Force UTF-8 for all text content in both the HTTP header and meta tags in HTML or encoding declarations in XML.
Reference	https://code.google.com/p/browsersec/wiki/Part2#Character_set_handling_and_detection
CWE Id	436
WASC Id	15
Plugin Id	90011

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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	email
Attack	
Evidence	zaproxy@example.com
Other Info	The URL contains email address(es).
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	password
Attack	
Evidence	password
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass password
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	email
Attack	
Evidence	zaproxy@example.com
Other Info	The URL contains email address(es).
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	password
Attack	
Evidence	password
Other Info	The URL contains potentially sensitive information. The following string was found via the pattern: pass password
Instances	4

Solution	Do not pass sensitive information in URIs.
Reference	
CWE Id	200
WASC Id	13
Plugin Id	10024

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://api.vantagecircle.co.in/themes/dealspoint/assets/js/html5shiv.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "c=d.insertBefore(c.lastChild,d.firstChild);b.hasCSS=!!c}g||t(a,b);return a}var k=l.html5|| {},s=/^<|^(?:button|map|select|textare", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/js/respond.min.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "/*! Respond.js v1.4.2: min/max-width media query polyfill", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-aria.min.js
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "(function(t,l){'use strict';var c="BUTTON A INPUT TEXTAREA SELECT DETAILS SUMMARY".split(" "),m=function(a,e){if(-1!==e.indexOf(", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular-sanitize.min.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: "p=f("accent-height,accumulate,additive,alphabetic,arabic-form,ascent,baseProfile,bbox,begin,by,calcMode,cap-height,class,color,c", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	
Attack	
Evidence	db
Other Info	The following pattern was used: \bDB\b and was detected 10 times, the first in the element starting with: "b[c])return!1;return!0}}else{if(ha(a))return ha(b)?ec(a.getTime(),b.getTime()):!1;if(ab(a))return ab(b)? a.toString()===b.toStri", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	
Attack	
Evidence	debug

Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "b,a)}}var f=wa||/\bEdge\//.test(d.navigator&&d.navigator.userAgent);return{log:e("log"),info:e("info"),warn:e("warn"),error:e("e", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 3 times, the first in the element starting with: "k,h,l) {l&&l();h=h|| {};h.from&&g.css(h.from);h.to&&g.css(h.to);if(h.addClass||h.removeClass)if(k=h.addClass,l=h.removeClass,h=a.g", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-1.8.0/angular.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 7 times, the first in the element starting with: "lc=Me(z);lc("ng",["ngLocale"],["$provide",function(a) {a.provider({$$sanitizeUri:Qe});a.provider("$compile",Zc).directive({a:Re,i", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angular-recaptcha.min.js
Method	GET
Parameter	
Attack	
Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "!function(a){"use strict";a.module("vcRecaptcha",[])}(angular),function(a){"use strict";function b(){throw new Error('You need t", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-0.12.0.min.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "})}var b= {placement:"top",animation:!0,popupDelay:0},c={mouseenter:"mouseleave",click:"click",focus:"blur"},d= {};this.options=fu", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-0.12.0.min.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "angular.module("ui.bootstrap", ["ui.bootstrap.transition","ui.bootstrap.collapse","ui.bootstrap.accordion","ui.bootstrap.alert",""", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-tpls-0.12.0.min.js
Method	GET
Parameter	
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element starting with: "});var m=i.render;i.render=function(){m(),c.page>0&&c.page<=c.totalPages&& (c.pages=h(c.page,c.totalPages))}}}}}]).constant("page", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/ui-bootstrap-tpls-0.12.0.min.js
Method	GET
Parameter	

Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "angular.module("ui.bootstrap", ["ui.bootstrap.tpls","ui.bootstrap.transition","ui.bootstrap.collapse","ui.bootstrap.accordion","u", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/userregister.js
Method	GET
Parameter	
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " $temp.val($(element).text()).select();", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/angularjs/userregister.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 129 times, the first in the element starting with: " $scope.page='user';", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/clipboard/clipboard.min.js
Method	GET
Parameter	
Attack	
Evidence	SELECT
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: "!function(e){if("object"==typeof exports&&"undefined"!=typeof module)module.exports=e();else if("function"==typeof define&&defin", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jquery.lazyload.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " /* Remove image from array so it is not looped next time. */", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assets/scripts/jwt-decode.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in the element starting with: " * The code was extracted from:", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assetsv2/jquery-vantage.min.js
Method	GET
Parameter	
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/themes/dealspoint/assetsv2/jquery.min.js
Method	GET
Parameter	
Attack	
Evidence	username

Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.exports=e.document?t(e,!0):function(", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<!-- <div ", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "<!-- user registration form -->", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<!-- <div ", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "<!-- user registration form -->", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	
Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<!-- <div ", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "<!-- user registration form -->", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	

Attack	
Evidence	Select
Other Info	The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element starting with: "<!-- <div ", see evidence field for the suspicious comment/snippet.
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "<!-- user registration form -->", see evidence field for the suspicious comment/snippet.
Instances	28
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	Loosely Scoped Cookie
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope.The domain scope applied to a cookie determines which domains can access it. For example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=7t5c9vidg4fk6nso3iv3gu75cs
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=b108girva4rus8r6fug61eqqtu
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=crtj6vhra5m5jae56fhadamdq8
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=qk4bdb42hp55rqphe5urcgc56f
URL	https://api.vantagecircle.co.in/
Method	GET

Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=u6t3gsoh3a9kgjmoe92ian821l
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=9q5tpo5cnu8b1nt9mr4tb7s4uq
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=f1c0calovgeg4haibqloabgg1s
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=ndieu2r0ufaabfmrhnunbhfu3b
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=qnjk9nfudqnjb7b81io1s06p8v
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=sfdlefroc0te16u2ulcqah78nu
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=1araipdsst5m2k6kb5l9028u1h
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=2e14i5kr9bli9l1ou5a3olf5os
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	

Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=85rce4o0m4n4vt6kfv4dv091o7
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=abtvmvqbhl47fr4gq5rnatud9f
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=kk5mqq5f4i4d315ml3bafobj7o
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=1gdv5a7rfgo5avgv64vtototrc
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=486prd07qne5sas7lev0rctss9
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=58ra0095cuqk1gek6tqrd0gugu
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=61j0d1sqg4667pkggj4hbem27m
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=jd3j39gfv65hr1k3pi7dsvcg9s
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	

Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=45ruq8hsa23l9k8t4hlkat9ckh
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=jk0doj0inneo6rrl6kfs57vlds
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=ravpl49h9n8aubhk2hob22gsdd
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=tc278q7coqqac69hbgg51fv6cp
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=v2e00m7aag37th87hl3f8giv6o
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=2lb2b0th0ogm45nb28ch24isb7
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=30qr8gcm2bguf439iousml7fpd
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=5t4qo1l9sdj3hmt3usndocbu0s
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=8ss27oi27gvtqqvb859s2h83ua

URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=e337msdtglpblvso41f1h14ed3
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=lv3d9vatstoteuqmkf2brh9tfa
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=0ijcais96k2nl7le0ggita2rlc
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=10qrjne030pdo8evsecvtardkr
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=6ebjhri5ig6r4vomso2te4n8b9
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=88qv0tq1q7s8d9hct9edv1sbt9
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=eq576qs4ss6db4etmmvot5agjl
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	
Other Info	The origin domain used for comparison was: api.vantagecircle.co.in Uat_Vantagecircle=m3qmpgc627u841qb7fp9ng208u
Instances	37

Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Reference	https://tools.ietf.org/html/rfc6265#section-4.1 https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies
CWE Id	565
WASC Id	15
Plugin Id	90033

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://api.vantagecircle.co.in/
Method	GET
Parameter	
Attack	
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	
Attack	
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://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	
Attack	
Evidence	<a class="error">
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://api.vantagecircle.co.in/latest
Method	GET
Parameter	
Attack	
Evidence	<a class="error">
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://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	
Attack	
Evidence	<a class="error">
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://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	
Attack	
Evidence	<a class="error">
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://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	
Attack	
Evidence	<a class="error">
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://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<a class="error">
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://api.vantagecircle.co.in/
Method	POST
Parameter	
Attack	
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	
Attack	
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	10
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

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://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	7t5c9vidg4fk6nso3iv3gu75cs
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	b108girva4rus8r6fug61eqqtu
Other Info	cookie:Uat_Vantagecircle

URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	crtj6vhra5m5jae56fhadamdq8
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	qk4bdb42hp55rqphe5urcgc56f
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	u6t3gsoh3a9kgjmoe92ian821l
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	9q5tpo5cnu8b1nt9mr4tb7s4uq
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	f1c0calovgeg4haibqloabgg1s
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	ndieu2r0ufaabfmrhnunbhfu3b
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	qnjk9nfudqnjb7b81io1s06p8v
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	sfdlefroc0te16u2ulcqah78nu
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest
Method	GET

Parameter	Uat_Vantagecircle
Attack	
Evidence	1araipdsst5m2k6kb5l9028u1h
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	2e14i5kr9bli9l1ou5a3olf5os
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	85rce4o0m4n4vt6kfv4dv091o7
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	abtvmvqbhl47fr4gq5rnatud9f
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	kk5mqq5f4i4d315ml3bafobj7o
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	1gdv5a7rfgo5avgv64vtototrc
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	486prd07qne5sas7lev0rctss9
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	58ra0095cuqk1gek6tqrd0gugu
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Uat_Vantagecircle

Attack	
Evidence	61j0d1sqg4667pkggj4hbem27m
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	jd3j39gfv65hr1k3pi7dsvcg9s
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	45ruq8hsa23l9k8t4hlkat9ckh
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	jk0doj0inneo6rrl6kfs57vlds
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	ravpl49h9n8aubhk2hob22gsdd
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	tc278q7coqqac69hbgg51fv6cp
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	v2e00m7aag37th87hl3f8giv6o
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	2lb2b0th0ogm45nb28ch24isb7
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	

Evidence	30qr8gcm2bguf439iousml7fpd
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	5t4qo1l9sdj3hmt3usndocbu0s
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	8ss27oi27gvtqqvb859s2h83ua
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	e337msdtglpblvso41f1h14ed3
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	lv3d9vatstoteuqmkf2brh9tfa
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	0ijcais96k2nl7le0ggita2rlc
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	10qrjne030pdo8evsecvtardkr
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	6ebjhri5ig6r4vomso2te4n8b9
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	88qv0tq1q7s8d9hct9edv1sbt9
Other Info	cookie:Uat_Vantagecircle

URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	eq576qs4ss6db4etmmvot5agjl
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	m3qmpgc627u841qb7fp9ng208u
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	7t5c9vidg4fk6nso3iv3gu75cs
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	b108girva4rus8r6fug61eqqtu
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	qk4bdb42hp55rqphe5urcgc56f
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	u6t3gsoh3a9kgjmoe92ian821l
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/BitKeeper
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	f1c0calovgeg4haibqloabgg1s
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	kk5mqq5f4i4d315ml3bafobj7o
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/latest/meta-data/
Method	GET

Parameter	Uat_Vantagecircle
Attack	
Evidence	45ruq8hsa23l9k8t4hlkat9ckh
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	8ss27oi27gvtqqvb859s2h83ua
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	e337msdtglpblvso41f1h14ed3
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	0ijcais96k2nl7le0ggita2rlc
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	6ebjhri5ig6r4vomso2te4n8b9
Other Info	cookie:Uat_Vantagecircle
URL	https://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Uat_Vantagecircle
Attack	
Evidence	88qv0tq1q7s8d9hct9edv1sbt9
Other Info	cookie:Uat_Vantagecircle
Instances	49
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	**User Agent Fuzzer**
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data

Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/latest/meta-data
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/robots.txt
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET

Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent

Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	http://api.vantagecircle.co.in/sitemap.xml
Method	GET
Parameter	Header User-Agent
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
Instances	60
Solution	
Reference	https://owasp.org/wstg
CWE Id	
WASC Id	
Plugin Id	10104

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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	day
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: day={{value}} The user-controlled value was: {{value}}
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [div] tag [aria-valuemax] attribute The user input found was: mobile=10 The user-controlled value was: 100
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET

Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [maxlength] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [min] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [ng-maxlength] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	GET
Parameter	month
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: month={{index+1}} The user-controlled value was: {{index+1}}
URL	https://api.vantagecircle.co.in/
Method	POST

Parameter	LoginForm[email]
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: LoginForm[email]=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	LoginForm[otp]
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: LoginForm[otp]=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	LoginForm[password]
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: LoginForm[password]=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=ab2bdc76bf18939eef5e7d9a9e8c5ba87c5f6ef8 The user-controlled value was: ab2bdc76bf18939eef5e7d9a9e8c5ba87c5f6ef8
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=b7203844d788a56259d6aee708280821ef8ff4bb The user-controlled value was: b7203844d788a56259d6aee708280821ef8ff4bb
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=bc9e34ea5879bd2ea6c21c2286d9ca0a0cc57364 The user-controlled value was: bc9e34ea5879bd2ea6c21c2286d9ca0a0cc57364
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=d5aa2a6905ed1c63077375b8803eb50190f74a72 The user-controlled value was: d5aa2a6905ed1c63077375b8803eb50190f74a72
URL	https://api.vantagecircle.co.in/
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/ appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=eb7985e923f19f098670ddc85a6203028c62e349 The user-controlled value was: eb7985e923f19f098670ddc85a6203028c62e349
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	day
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: day={{value}} The user-controlled value was: {{value}}
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	LoginForm[email]
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: LoginForm[email]=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	LoginForm[otp]
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: LoginForm[otp]=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	LoginForm[password]
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: LoginForm[password]=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [div] tag [aria-valuemax] attribute The user input found was: mobile=10 The user-controlled value was: 100
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [maxlength] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [min] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [ng-maxlength] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	mobile
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: mobile=10 The user-controlled value was: 10
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	month
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [option] tag [value] attribute The user input found was: month={{index+1}} The user-controlled value was: {{index+1}}
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	name
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: name=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	password
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: password=ZAP The user-controlled value was: zap
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=ab2bdc76bf18939eef5e7d9a9e8c5ba87c5f6ef8 The user-controlled value was: ab2bdc76bf18939eef5e7d9a9e8c5ba87c5f6ef8
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST

Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=b7203844d788a56259d6aee708280821ef8ff4bb The user-controlled value was: b7203844d788a56259d6aee708280821ef8ff4bb
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=bc9e34ea5879bd2ea6c21c2286d9ca0a0cc57364 The user-controlled value was: bc9e34ea5879bd2ea6c21c2286d9ca0a0cc57364
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=d5aa2a6905ed1c63077375b8803eb50190f74a72 The user-controlled value was: d5aa2a6905ed1c63077375b8803eb50190f74a72
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=e419cf9b2d5e85d29b802b359bb9fb11bba39e3c The user-controlled value was: e419cf9b2d5e85d29b802b359bb9fb11bba39e3c
URL	https://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1
Method	POST
Parameter	VANTAGECIRCLE_CSRF_TOKEN
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://api.vantagecircle.co.in/?agree=on&city=East+Romaineburgh&day=%7B%7Bvalue%7D%7D&email=zaproxy%40example.com&gender=1&mobile=10&month=%7B%7Bindex%2B1%7D%7D&name=ZAP&password=ZAP&regularalert=on&year=1 appears to include user input in: a(n) [input] tag [value] attribute The user input found was: VANTAGECIRCLE_CSRF_TOKEN=eb7985e923f19f098670ddc85a6203028c62e349 The user-controlled value was: eb7985e923f19f098670ddc85a6203028c62e349
Instances	33
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