# ZAP Scanning Report

**Sites: https://db7hsdc8829us.cloudfront.net https://c.clarity.ms https://fonts.gstatic.com https://www.linkedin.com https://p.easyinsights.in https://www.facebook.com https://b.clarity.ms https://d24vv731hdkcnd.cloudfront.net https://www.gstatic.com https://eu1.clevertap-prod.com https://px.ads.linkedin.com https://googleads.g.doubleclick.net https://s3-eu-west-1.amazonaws.com https://bat.bing.com https://www.google.com https://connect.facebook.net https://www.clarity.ms https://d2r1yp2w7bby2u.cloudfront.net https://a.quora.com https://snap.licdn.com https://www.google-analytics.com https://q.quora.com https://script.hotjar.com https://www.google.co.in https://stats.g.doubleclick.net https://analytics.google.com https://static.hotjar.com https://d1jnx9ba8s6j9r.cloudfront.net https://www.googletagmanager.com https://www.edureka.co https://edureka.co**

**Generated on Fri, 19 Apr 2024 23:35:12**

**ZAP Version: 2.14.0**

### Summary of Alerts

| Risk Level | Number of Alerts |
|---|---|
| High | 2 |
| Medium | 9 |
| Low | 10 |
| Informational | 8 |

### Alerts

| Name | Risk Level | Number of Instances |
|---|---|---|
| Open Redirect | High | 1 |
| PII Disclosure | High | 1 |
| Absence of Anti-CSRF Tokens | Medium | 9 |
| CSP: Wildcard Directive | Medium | 8 |
| CSP: script-src unsafe-eval | Medium | 3 |
| CSP: script-src unsafe-inline | Medium | 5 |
| CSP: style-src unsafe-inline | Medium | 8 |
| Cross-Domain Misconfiguration | Medium | 28 |
| Missing Anti-clickjacking Header | Medium | 3 |
| Session ID in URL Rewrite | Medium | 6 |
| Vulnerable JS Library | Medium | 1 |
| CSP: Notices | Low | 3 |

| | | |
|---|---|---|
| Cookie No HttpOnly Flag | Low | 26 |
| Cookie Without Secure Flag | Low | 15 |
| Cookie with SameSite Attribute None | Low | 14 |
| Cookie without SameSite Attribute | Low | 15 |
| Cross-Domain JavaScript Source File Inclusion | Low | 8 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Low | 17 |
| Strict-Transport-Security Header Not Set | Low | 33 |
| Timestamp Disclosure - Unix | Low | 89 |
| X-Content-Type-Options Header Missing | Low | 38 |
| Content-Type Header Missing | Informational | 2 |
| Information Disclosure - Suspicious Comments | Informational | 75 |
| Loosely Scoped Cookie | Informational | 6 |
| Modern Web Application | Informational | 6 |
| Re-examine Cache-control Directives | Informational | 6 |
| Retrieved from Cache | Informational | 17 |
| Session Management Response Identified | Informational | 38 |
| User Controllable HTML Element Attribute (Potential XSS) | Informational | 43 |

## Alert Detail

| High | Open Redirect |
|---|---|
| Description | Open redirects are one of the OWASP 2010 Top Ten vulnerabilities. This check looks at user-supplied input in query string parameters and POST data to identify where open redirects might be possible. Open redirects occur when an application allows user-supplied input (e.g. http://nottrusted.com) to control an offsite redirect. This is generally a pretty accurate way to find where 301 or 302 redirects could be exploited by spammers or phishing attacks.<br><br>For example an attacker could supply a user with the following link: http://example.com /example.php?url=http://malicious.example.com. |
| URL | https://www.linkedin.com/px/li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com%2Fcollect%3Fv%3D2%26fmt%3Djs%26pid%3D180467%26time%3D1713549421165%26li_adsId%3Dc179cf8a-4c6d-4b63-bd84-34747184b4db%26url%3Dhttps%253A%252F%252Fwww.edureka.co%252F%26cookiesTest%3Dtrue%26liSync%3Dtrue |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | The 301 or 302 response to a request for the following URL appeared to contain user input in the location header: https://www.linkedin.com/px/li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com%2Fcollect%3Fv%3D2%26fmt%3Djs%26pid%3D180467%26time%3D1713549421165%26li_adsId%3Dc179cf8a-4c6d-4b63-bd84-34747184b4db%26url%3Dhttps%253A%252F%252Fwww.edureka.co%252F%26cookiesTest%3Dtrue%26liSync%3Dtrue The user input found was: redirect=https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c179cf8a-4c6d-4b63-bd84-34747184b4db&url=https%3A%2F%2Fwww.edureka.co%2F&cookiesTest=true&liSync=true The context was: https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c179cf8a-4c6d-4b63-bd84-34747184b4db&url=https%3A%2F%2Fwww.edureka.co%2F&cookiesTest=true&liSync=true |
| Instances | 1 |
| | |

| | |
|---|---|
| Solution | To avoid the open redirect vulnerability, parameters of the application script/program must be validated before sending 302 HTTP code (redirect) to the client browser. Implement safe redirect functionality that only redirects to relative URI's, or a list of trusted domains |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets<br>/Unvalidated_Redirects_and_Forwards_Cheat_Sheet.html<br>https://cwe.mitre.org/data/definitions/601.html |
| CWE Id | 601 |
| WASC Id | 38 |
| Plugin Id | 10028 |

| **High** | **PII Disclosure** |
|---|---|
| Description | The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/icomoon_20210212.woff |
| Method | GET |
| Attack | |
| Evidence | 5467423261461023 |
| Other Info | Credit Card Type detected: Mastercard Bank Identification Number: 546742 Brand: MASTERCARD Category: Issuer: NATIONAL CITY BANK, KENTUCKY |
| Instances | 1 |
| Solution | Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application. |
| Reference | |
| CWE Id | 359 |
| WASC Id | 13 |
| Plugin Id | 10062 |

| **Medium** | **Absence of Anti-CSRF Tokens** |
|---|---|
| Description | No Anti-CSRF tokens were found in a HTML submission form.<br><br>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.<br><br>CSRF attacks are effective in a number of situations, including:<br><br>* The victim has an active session on the target site.<br><br>* The victim is authenticated via HTTP auth on the target site.<br><br>* The victim is on the same local network as the target site.<br><br>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://www.edureka.co/ |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | <form class="sup_frm signup-new-form" method="post" action="/users/apiSaveUser" data-formslug="signupform"> |
| 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: "category_id" "clp_version" "hidden-signup-code" "offer_id" "sg_popup_email" "sg_popup_phone_no" "slug" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form class="sup_frm sign_up_twoflow signup-new-passwd" method="post" action="/users/signup"> |
| 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 2: "category_id" "clp_version" "data[User][coursename]" "hidden-signup-email" "hidden-signup-mobile" "hiddenname" "hiddenpassword" "is_amb_exist" "offer_id" "pageurl_signup_flow_form" "signup_password" "slug" "update_passwd" "videoclick_sup_flow" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form class="sup_frm tr_signin_form signin-new-form" action="/users/signin" method="post" > |
| 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 3: "clp_version" "coursename_signup_new_login_1" "offer_id" "si_popup_email" "si_popup_passwd" "signin_pageurl_new" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form id="forgotpasswordForm" class="sup_frm"> |
| 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 4: "clp_version" "data[User][coursename]" "data[User][pageurl]" "forgot_email_new" "offer_id" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form class="sup_frm" id="resetcode_new" autocomplete="off"> |
| 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 5: "otpfield_new" "password" "reset_email_in" "verificationfield_new" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form method="post" class="new-duq-form" data-formslug="duqform" data-context="desktop"> |
| | No known Anti-CSRF token [anticsrf, CSRFToken, __RequestVerificationToken, |

| | |
|---|---|
| Other Info | csrfmiddlewaretoken, authenticity_token, OWASP_CSRFTOKEN, anoncsrf, csrf_token, _csrf, _csrfSecret, __csrf_magic, CSRF, _token, _csrf_token] was found in the following HTML form: [Form 6: "data[Feedback][code]" "data[Feedback][email]" "data[Feedback][phone_no]" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form method="post" class="ga_call exit_popup_form"> |
| 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 7: "email" "phone_no" ]. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <form method="post" class="new-duq-form" data-context="mobile" data-formslug="duqform" > |
| 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 8: "data[Feedback][code]" "data[Feedback][email]" "data[Feedback][phone_no]" "data[Feedback][position]" ]. |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | <form id="top_banner_form"> |
| 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: "code" "context" "course_id" "top_banner_email" "top_banner_mobile" ]. |
| Instances | 9 |
| Solution | Phase: Architecture and Design<br><br>Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.<br><br>For example, use anti-CSRF packages such as the OWASP CSRFGuard.<br><br>Phase: Implementation<br><br>Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.<br><br>Phase: Architecture and Design<br><br>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).<br><br>Note that this can be bypassed using XSS.<br><br>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.<br><br>Note that this can be bypassed using XSS. |

| | |
|---|---|
| | Use the ESAPI Session Management control.<br><br>This control includes a component for CSRF.<br><br>Do not use the GET method for any request that triggers a state change.<br><br>Phase: Implementation<br><br>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<br>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 cer attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. The used for everything from data theft to site defacement or distribution of malware. CSP provides HTTP headers that allow website owners to declare approved sources of content that browsers to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and en such as Java applets, ActiveX, audio and video files. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnj https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove img-src, frame-ancestors, font-src, form-action The directive(s): frame-ancestors, form-action ar directives that do not fallback to default-src, missing/excluding them is the same as allowing any |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnj |

| | |
|---|---|
| Evidence | https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove img-src, frame-ancestors, font-src, form-action The directive(s): frame-ancestors, form-action ar directives that do not fallback to default-src, missing/excluding them is the same as allowing any |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-UkKnEIxN7fhNqXSM1HvoEw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, wo action The directive(s): frame-ancestors, form-action are among the directives that do not fallba missing/excluding them is the same as allowing anything. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ 0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_ &size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-8iqwp031_OTtxXhTFdYIbg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-e 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, wo action The directive(s): frame-ancestors, form-action are among the directives that do not fallba missing/excluding them is the same as allowing anything. |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-0Oj_RjVB_1vXHma-81gbCQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove style-src, img-src, connect-src, frame-src, frame-ancestors, font-src, media-src, manifest-src, wo action The directive(s): frame-ancestors, form-action are among the directives that do not fallba missing/excluding them is the same as allowing anything. |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea |

| | |
|---|---|
| Evidence | amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnj<br>https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co<br>razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results<br>https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com<br>https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*<br>https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https<br>com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl<br>https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry<br>https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg<br>bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo<br>gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol<br>admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z<br>zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g<br>com;font-src data: * blob; img-src data: * blob; |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove<br>img-src, frame-ancestors, font-src, form-action The directive(s): frame-ancestors, form-action ar<br>directives that do not fallback to default-src, missing/excluding them is the same as allowing any |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://<br>paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr<br>indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http<br>oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht<br>ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea<br>amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnj<br>https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co<br>razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results<br>https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com<br>https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*<br>https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https<br>com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl<br>https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry<br>https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg<br>bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo<br>gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol<br>admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z<br>zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g<br>com;font-src data: * blob; img-src data: * blob; |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove<br>img-src, frame-ancestors, font-src, form-action The directive(s): frame-ancestors, form-action ar<br>directives that do not fallback to default-src, missing/excluding them is the same as allowing any |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://<br>paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr<br>indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http<br>oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht<br>ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea<br>amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnj<br>https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co<br>razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results<br>https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com<br>https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*<br>https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https<br>com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl<br>https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry<br>https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg<br>bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo<br>gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol<br>admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z |

| | |
|---|---|
| | zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | The following directives either allow wildcard sources (or ancestors), are not defined, or are ove img-src, frame-ancestors, font-src, form-action The directive(s): frame-ancestors, form-action ar directives that do not fallback to default-src, missing/excluding them is the same as allowing any |
| Instances | 8 |
| Solution | Ensure that your web server, application server, load balancer, etc. is properly configured to set Security-Policy header. |
| Reference | http://www.w3.org/TR/CSP2/<br>http://www.w3.org/TR/CSP/<br>http://caniuse.com/#search=content+security+policy<br>http://content-security-policy.com/<br>https://github.com/shapesecurity/salvation<br>https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10055 |

| Medium | CSP: script-src unsafe-eval |
|---|---|
| Description | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. The used for everything from data theft to site defacement or distribution of malware. CSP provides HTTP headers that allow website owners to declare approved sources of content that browsers to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and en such as Java applets, ActiveX, audio and video files. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-UkKnEIxN7fhNqXSM1HvoEw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | script-src includes unsafe-eval. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_&size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-8iqwp031_OTtxXhTFdYIbg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-e 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | script-src includes unsafe-eval. |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-0Oj_RjVB_1vXHma-81gbCQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | script-src includes unsafe-eval. |
| Instances | 3 |
| | |

| | |
|---|---|
| Solution | Ensure that your web server, application server, load balancer, etc. is properly configured to set Security-Policy header. |
| Reference | http://www.w3.org/TR/CSP2/<br>http://www.w3.org/TR/CSP/<br>http://caniuse.com/#search=content+security+policy<br>http://content-security-policy.com/<br>https://github.com/shapesecurity/salvation<br>https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet |
| 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://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://*.paytm.in wss://*.paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayments.com https://*.indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co https://cdn.linkedin.oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com https://www.clarity.ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.reachclk.com https://*.amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs.cloudflare.com https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.com https://*.razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results.affilitrace.com https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*.linkedin.com https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https://static.clevertap.com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cloudfront.net https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvryqq.cloudfront.net https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg.com https://*.bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.taboola.com https://*.gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algolianet.com https://*.admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.zoho.com https://*.zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.googleoptimize.com;font-src data: * blob; img-src data: * blob; |
| Other Info | script-src includes unsafe-inline. |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://*.paytm.in wss://*.paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayments.com https://*.indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co https://cdn.linkedin.oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com https://www.clarity.ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.reachclk.com https://*.amazonaws.com https://*.googleapis.com |

| | |
|---|---|
| Evidence | https://*.google.com https://fast.wistia.net https://cdnjs.cloudflare.com https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.com https://*.razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results.affilitrace.com https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*.linkedin.com https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https://static.clevertap.com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cloudfront.net https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvryqq.cloudfront.net https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg.com https://*.bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.taboola.com https://*.gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algolianet.com https://*.admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.zoho.com https://*.zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.googleoptimize.com;font-src data: * blob; img-src data: * blob; |
| Other Info | script-src includes unsafe-inline. |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://*.paytm.in wss://*.paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayments.com https://*.indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co https://cdn.linkedin.oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com https://www.clarity.ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.reachclk.com https://*.amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs.cloudflare.com https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.com https://*.razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results.affilitrace.com https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*.linkedin.com https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https://static.clevertap.com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cloudfront.net https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvryqq.cloudfront.net https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg.com https://*.bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.taboola.com https://*.gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algolianet.com https://*.admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.zoho.com https://*.zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.googleoptimize.com;font-src data: * blob; img-src data: * blob; |
| Other Info | script-src includes unsafe-inline. |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://*.paytm.in wss://*.paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayments.com https://*.indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co https://cdn.linkedin.oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com https://www.clarity.ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.reachclk.com https://*.amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs.cloudflare.com https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.com https://*.razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com |

| | |
|---|---|
| Evidence | https://results.affilitrace.com https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*.linkedin.com https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https://static.clevertap.com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cloudfront.net https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvryqq.cloudfront.net https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg.com https://*.bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.taboola.com https://*.gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algolianet.com https://*.admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.zoho.com https://*.zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.googleoptimize.com;font-src data: * blob; img-src data: * blob; |
| Other Info | script-src includes unsafe-inline. |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https://*.paytm.in wss://*.paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayments.com https://*.indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co https://cdn.linkedin.oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com https://www.clarity.ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.reachclk.com https://*.amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs.cloudflare.com https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.com https://*.razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results.affilitrace.com https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://*.linkedin.com https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https://static.clevertap.com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cloudfront.net https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvryqq.cloudfront.net https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg.com https://*.bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.taboola.com https://*.gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algolianet.com https://*.admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.zoho.com https://*.zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.googleoptimize.com;font-src data: * blob; img-src data: * blob; |
| Other Info | script-src includes unsafe-inline. |
| Instances | 5 |
| Solution | Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header. |
| Reference | http://www.w3.org/TR/CSP2/<br>http://www.w3.org/TR/CSP/<br>http://caniuse.com/#search=content+security+policy<br>http://content-security-policy.com/<br>https://github.com/shapesecurity/salvation<br>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 cer attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. The used for everything from data theft to site defacement or distribution of malware. CSP provides HTTP headers that allow website owners to declare approved sources of content that browsers to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and en such as Java applets, ActiveX, audio and video files. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | script-src 'nonce-UkKnEIxN7fhNqXSM1HvoEw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ 0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_ &size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-8iqwp031_OTtxXhTFdYIbg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-e 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm- &k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-0Oj_RjVB_1vXHma-81gbCQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co |

| | |
|---|---|
| Evidence | razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | style-src includes unsafe-inline. |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | default-src 'unsafe-inline' 'self' 'unsafe-eval' https://*.edureka.co https://www.google.co.in https:// paytm.in https://*.paytm.com wss://*.paytm.com https://*.paytmpayments.com wss://*.paytmpayr indoleads.com https://*.linksynergy.com https://p.easyinsights.in https://api-corp.edureka.co http oribi.io/ https://*.doubleclick.net https://learningcenter.edureka.co https://*.clevertap-prod.com ht ms https://*.clarity.ms https://s3-eu-west-1.amazonaws.com/static.wizrocket.com https://clk1.rea amazonaws.com https://*.googleapis.com https://*.google.com https://fast.wistia.net https://cdnjs https://*.jquery.com https://*.bootstrapcdn.com https://*.vizury.com https://*.googleadservices.co razorpay.com https://*.paypal.com https://mbsy.co https://www.paypalobjects.com https://results https://*.freshdesk.com https://*.twitter.com https://*.ytimg.com https://fonts.googleapis.com https://d36mpcpuzc4ztk.cloudfront.net https://www.youtube.com https://*.facebook.com https://* https://www.googletagmanager.com https://bat.bing.com https://www.google-analytics.com https com https://wzrkt.com https://connect.facebook.net https://*.twimg.com https://d1jnx9ba8s6j9r.cl https://duyseoho78lqc.cloudfront.net https://d30aa6afk7qd1v.cloudfront.net https://dop9av6nvry https://d25qem54r5kbml.cloudfront.net https://d2r1yp2w7bby2u.cloudfront.net https://*.crazyegg bizographics.com https://*.quora.com https://*.useproof.com https://snap.licdn.com https://*.tabo gstatic.com https://*.emjcd.com https://matomo.easyinsights.ai https://*.algolia.net https://*.algol admitad.com wss://*.hotjar.com https://*.hotjar.com https://*.hotjar.io https://*.algolia.io https://*.z zohostatic.com https://*.zohopublic.com wss://*.zohopublic.com https://*.zohocdn.com https://*.g com;font-src data: * blob; img-src data: * blob; |
| Other Info | style-src includes unsafe-inline. |
| Instances | 8 |
| Solution | Ensure that your web server, application server, load balancer, etc. is properly configured to set Security-Policy header. |
| Reference | http://www.w3.org/TR/CSP2/<br>http://www.w3.org/TR/CSP/<br>http://caniuse.com/#search=content+security+policy<br>http://content-security-policy.com/<br>https://github.com/shapesecurity/salvation<br>https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet |
| 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) m |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20Edureka&kw=e-learning,%20online%20training,%20online%20course,%20Android%20trainir |

| | |
|---|---|
| | 20data,%20hadoop,%20learn,%20Data%20Science,%20Business%20Analytics,%20Cloud%20<br>20training,%20devops,%20tableau,%20python,%20blockchain&p=https%3A%2F%2Fwww.edu<br>2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra<br>on this domain. Web browser implementations do not permit arbitrary third parties to read the re<br>reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t<br>which uses some other form of security, such as IP address white-listing. |
| URL | https://connect.facebook.net/en_US/sdk.js |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra<br>on this domain. Web browser implementations do not permit arbitrary third parties to read the re<br>reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t<br>which uses some other form of security, such as IP address white-listing. |
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra<br>on this domain. Web browser implementations do not permit arbitrary third parties to read the re<br>reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t<br>which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css-cache/cache-autoload-home_optimized-a81a5d6113f9 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra<br>on this domain. Web browser implementations do not permit arbitrary third parties to read the re<br>reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t<br>which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans3.woff |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra<br>on this domain. Web browser implementations do not permit arbitrary third parties to read the re<br>reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t<br>which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans5.woff |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra<br>on this domain. Web browser implementations do not permit arbitrary third parties to read the re<br>reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t |

| | |
|---|---|
| | which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans7.woff |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/cssver.1713530642/css/edurekanew/fonts/home_second_ |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/cssver.1713530642/css/edurekanew/HomeOptimized/hom |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/home_ico_new_12_5_20.woff |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/icomoon_20210212.woff |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/Edureka_V_W_logo.webp |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |

| | |
|---|---|
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/pcpdevops_logo.webp |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/clevertap/edureka-clever |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/HomeOptimized/discove |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc4.woff2 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| | |

| | |
|---|---|
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://static.hotjar.com/c/hotjar-1826269.js?sv=6 |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.clarity.ms/s/0.7.31/clarity.js |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.edureka.co/clevertap_sw.js |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | Access-Control-Allow-Origin: * |
| Other Info | The CORS misconfiguration on the web server permits cross-domain read requests from arbitra on this domain. Web browser implementations do not permit arbitrary third parties to read the re reduces the risk somewhat. This misconfiguration could be used by an attacker to access data t which uses some other form of security, such as IP address white-listing. |
| Instances | 28 |
| Solution | Ensure that sensitive data is not available in an unauthenticated manner (using IP address whit<br><br>Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner. |
| Reference | https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy |
| CWE Id | 264 |
| WASC Id | 14 |
| Plugin Id | 10098 |

| **Medium** | **Missing Anti-clickjacking Header** |
|---|---|
| Description | The response does not include either Content-Security-Policy with 'frame-ancestors' directive or to protect against 'ClickJacking' attacks. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| | |

| | |
|---|---|
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ 0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_ &size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm- &k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| Instances | 3 |
| Solution | Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP header them is set on all web pages returned by your site/app.<br><br>If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DEN consider implementing Content Security Policy's "frame-ancestors" directive. |
| Reference | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options |
| CWE Id | 1021 |
| WASC Id | 15 |
| Plugin Id | 10020 |

| **Medium** | **Session ID in URL Rewrite** |
|---|---|
| Description | URL rewrite is used to track user session ID. The session ID may be disclosed via cross-site ref stored in browser history or server logs. |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5- d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20Edureka&kw=e-learning,%20online%20training,%20online%20course,%20Android%20trainin 20data,%20hadoop,%20learn,%20Data%20Science,%20Business%20Analytics,%20Cloud%20 20training,%20devops,%20tableau,%20python,%20blockchain&p=https%3A%2F%2Fwww.edu 2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | 393ddff0fe7611eea398d53bdab27b47 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G- 0TQ83VTDLH&gtm=45je44h0v883337477z877750292za200&_p=1713549403247&_gaz=1&gc 1713549408&ul=en-us&sr=1753x944&pscdl=noapi&_s=1&sid=1713549427&sct=1&seg=0&dl= 2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20%7 20Edureka&en=page_view&_fv=2&_ss=2&_c=1&tfd=27884 |
| Method | POST |
| | |

| | |
|---|---|
| Attack | |
| Evidence | 1713549427 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za200&_p=1713549403247&_gaz=1&gcd=13l3l3l3l1713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=1&sid=1713549407&sctco%2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20Edureka&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&tfd=8260 |
| Method | POST |
| Attack | |
| Evidence | 1713549407 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za200&_p=1713549403247&gcd=13l3l3l3l1&npa=0us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=3&sid=1713549407&sct=1&seg=0&dl=https%Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&ecourse_id=100&ep.course_type=No%20Course&ep.category=No%20Course&ep.website_action=Drop_Us_Query_Prompt_Opened_Automatic&ep.timestamp=Fri%2C%2019%20GMT&_et=2945&tfd=54402 |
| Method | POST |
| Attack | |
| Evidence | 1713549407 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za200&_p=1713549403247&gcd=13l3l3l3l1&npa=0us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&sid=1713549407&sct=1&seg=0&dl=https%3A%20Online%20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&_s=2& |
| Method | POST |
| Attack | |
| Evidence | 1713549407 |
| Other Info | |
| URL | https://p.easyinsights.in/ga4/vnri56u349gnw03ir0i4u6hngrg039ir03jf390r/g/collect?v=2&tid=G-XWKD9DJ015&gtm=45je44h0v9101910922z877750292za200&_p=1713549403247&gcd=13l31713549408&ul=en-us&sr=1753x944&_fplc=0&pscdl=noapi&_s=1&sid=1713549424&sct=1&se2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20%eiuid=&tfd=24324 |
| Method | POST |
| Attack | |
| Evidence | 1713549424 |
| Other Info | |
| Instances | 6 |
| Solution | For secure content, put session ID in a cookie. To be even more secure consider using a combi |
| Reference | http://seclists.org/lists/webappsec/2002/Oct-Dec/0111.html |
| CWE Id | 200 |
| WASC Id | 13 |
| | |

| | |
|---|---|
| Plugin Id | 3 |

| Medium | Vulnerable JS Library |
|---|---|
| Description | The identified library jquery, version 1.11.2 is vulnerable. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551608580a5bc38b4c11d.js |
| Method | GET |
| Attack | |
| Evidence | /*! jQuery v1.11.2 |
| Other Info | CVE-2020-11023 CVE-2020-11022 CVE-2015-9251 CVE-2019-11358 CVE-2020-23064 |
| Instances | 1 |
| Solution | Please upgrade to the latest version of jquery. |
| Reference | https://github.com/jquery/jquery/issues/2432<br>http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/<br>http://research.insecurelabs.org/jquery/test/<br>https://blog.jquery.com/2019/04/10/jquery-3-4-0-released/<br>https://nvd.nist.gov/vuln/detail/CVE-2019-11358<br>https://nvd.nist.gov/vuln/detail/CVE-2015-9251<br>https://github.com/jquery/jquery/commit/753d591aea698e57d6db58c9f722cd0808619b1b<br>https://bugs.jquery.com/ticket/11974<br>https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/<br>https://github.com/jquery/jquery.com/issues/162 |
| CWE Id | 829 |
| WASC Id | |
| Plugin Id | 10003 |

| Low | CSP: Notices |
|---|---|
| Description | Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate cer attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. The used for everything from data theft to site defacement or distribution of malware. CSP provides HTTP headers that allow website owners to declare approved sources of content that browsers to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and en such as Java applets, ActiveX, audio and video files. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-UkKnEIxN7fhNqXSM1HvoEw' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | Warnings: The report-uri directive has been deprecated in favor of the new report-to directive |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_&size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-8iqwp031_OTtxXhTFdYIbg' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe-e 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | Warnings: The report-uri directive has been deprecated in favor of the new report-to directive |
| | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm- |

| | |
|---|---|
| URL | &k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | script-src 'nonce-0Oj_RjVB_1vXHma-81gbCQ' 'unsafe-inline' 'strict-dynamic' https: http: 'unsafe 'none';base-uri 'self';report-uri https://csp.withgoogle.com/csp/recaptcha/1 |
| Other Info | Warnings: The report-uri directive has been deprecated in favor of the new report-to directive |
| Instances | 3 |
| Solution | Ensure that your web server, application server, load balancer, etc. is properly configured to set Security-Policy header. |
| Reference | http://www.w3.org/TR/CSP2/<br>http://www.w3.org/TR/CSP/<br>http://caniuse.com/#search=content+security+policy<br>http://content-security-policy.com/<br>https://github.com/shapesecurity/salvation<br>https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variet |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10055 |

| **Low** | **Cookie No HttpOnly Flag** |
|---|---|
| Description | A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed and can be transmitted to another site. If this is a session cookie then session hijacking may be |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20online%20course,%20Android%20training,%20%20edureka,%20online%20course,big%20da 20Computing,%20development,%20online%20training,%20devops,%20tableau,%20python,%2 2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: MR |
| Other Info | |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20online%20course,%20Android%20training,%20%20edureka,%20online%20course,big%20da 20Computing,%20development,%20online%20training,%20devops,%20tableau,%20python,%2 2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: MUID |
| Other Info | |
| URL | https://googleads.g.doubleclick.net/pagead/viewthroughconversion/965688462/?random=1713549421289&cv=11&fst=1713549421289&bg=ffffff&guid=ON&async=1&gtm=45be 3A%2F%2Fwww.edureka.co%2F&hn=www.googleadservices.com&frm=0&tiba=Instructor-Led% 20Edureka&npa=0&pscdl=noapi&auid=243454040.1713549409&fdr=QA&rfmt=3&fmt=4 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: test_cookie |

| | |
|---|---|
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bcookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: li_sugr |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: lidc |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: AnalyticsSyncHistory |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bcookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: li_sugr |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: UserMatchHistory |

| | |
|---|---|
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bcookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: li_sugr |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: _aIpjT6rhLb |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: _utm_wb_term |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[currencyprefrence] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[landingpage] |
| | |

| | |
|---|---|
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[preference_country] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[timezoneprefrence] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[Visited] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: f_l_i_s_p |
| Other Info | |
| URL | https://www.edureka.co/clevertap_sw.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |

| | |
|---|---|
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| Instances | 26 |
| Solution | Ensure that the HttpOnly flag is set for all cookies. |
| Reference | https://owasp.org/www-community/HttpOnly |
| CWE Id | 1004 |
| WASC Id | 13 |
| Plugin Id | 10010 |

| **Low** | **Cookie Without Secure Flag** |
|---|---|
| Description | A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: _aIpjT6rhLb |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: _utm_wb_term |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: brain4ce_n |
| | |

| | |
|---|---|
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[currencyprefrence] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[landingpage] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[preference_country] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[timezoneprefrence] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[Visited] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: f_l_i_s_p |
| Other Info | |
| URL | https://www.edureka.co/clevertap_sw.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |

| | |
|---|---|
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| Instances | 15 |
| Solution | Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information. |
| Reference | 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 |
| CWE Id | 614 |
| WASC Id | 13 |
| Plugin Id | 10011 |

| **Low** | **Cookie with SameSite Attribute None** |
|---|---|
| Description | A cookie has been set with its SameSite attribute set to "none", which means that the cookie ca measure to cross-site request forgery, cross-site script inclusion, and timing attacks. |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20online%20course,%20Android%20training,%20%20edureka,%20online%20course,big%20da 20Computing,%20development,%20online%20training,%20devops,%20tableau,%20python,%2 2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: MR |
| Other | |

| | |
|---|---|
| Info | |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024%20online%20course,%20Android%20training,%20%20edureka,%20online%20course,big%20da%20Computing,%20development,%20online%20training,%20devops,%20tableau,%20python,%2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: MUID |
| Other Info | |
| URL | https://googleads.g.doubleclick.net/pagead/viewthroughconversion/965688462/?random=1713549421289&cv=11&fst=1713549421289&bg=ffffff&guid=ON&async=1&gtm=45be3A%2F%2Fwww.edureka.co%2F&hn=www.googleadservices.com&frm=0&tiba=Instructor-Led%20Edureka&npa=0&pscdl=noapi&auid=243454040.1713549409&fdr=QA&rfmt=3&fmt=4 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: test_cookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bcookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: li_sugr |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: lidc |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c12F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: AnalyticsSyncHistory |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c12F&cookiesTest=true |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bcookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: li_sugr |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: UserMatchHistory |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bcookie |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: li_sugr |
| Other Info | |
| URL | https://www.clarity.ms/tag/bu6mlgzzxv |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CLID |
| Other Info | |
| URL | https://www.linkedin.com/px/li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com%2Fcollect 3Dc179cf8a-4c6d-4b63-bd84-34747184b4db%26url%3Dhttps%253A%252F%252Fwww.edurek |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: bscookie |
| Other Info | |

| | |
|---|---|
| Instances | 14 |
| 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** | **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://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: _aIpjT6rhLb |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: _utm_wb_term |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: brain4ce_n |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[currencyprefrence] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[landingpage] |

| | |
|---|---|
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[preference_country] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[timezoneprefrence] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: CakeCookie[Visited] |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | Set-Cookie: f_l_i_s_p |
| Other Info | |
| URL | https://www.edureka.co/clevertap_sw.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |

| | |
|---|---|
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| Instances | 15 |
| 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://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <script src="https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551608580a5bc38b4c11d.js" type="text/javascript"></script> |
| Other Info | |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | <script async src="https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW"></script> |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| Evidence | <script type="text/javascript" src="https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCv/recaptcha__en.js" nonce="UkKnEIxN7fhNqXSM1HvoEw"> </script> |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_&size=compact&cb=v7l0sv7mkvwv |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | <script type="text/javascript" src="https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCv /recaptcha__en.js" nonce="8iqwp031_OTtxXhTFdYIbg"> </script> |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | <script type="text/javascript" src="https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCv /recaptcha__en.js" nonce="0Oj_RjVB_1vXHma-81gbCQ"> </script> |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | <script type="text/javascript" src="https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edu /edureka-clevertap-events.js"></script> |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | <script type="text/javascript" src="https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edu /HomeOptimized/discovert_op_categories.js"> |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | <script src="https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit" /script> |
| Other Info | |
| Instances | 8 |
| Solution | Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be c users of the application. |
| Reference | |
| CWE Id | 829 |
| WASC Id | 15 |
| Plugin Id | 10017 |

| **Low** | **Server Leaks Version Information via "Server" HTTP Response Header Field** |
|---|---|
| Description | The web/application server is leaking version information via the "Server" HTTP response head attackers identifying other vulnerabilities your web/application server is subject to. |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/clevertap.min.js |
| Method | GET |
| | |

| | |
|---|---|
| Attack | |
| Evidence | AmazonS3 |
| Other Info | |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/localforage.min.js |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| Other Info | |
| URL | https://edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | awselb/2.0 |
| Other Info | |
| URL | https://s3-eu-west-1.amazonaws.com/static.wizrocket.com/js/sw_webpush.js |
| Method | GET |
| Attack | |
| Evidence | AmazonS3 |
| Other Info | |
| URL | https://www.google-analytics.com/analytics.js |
| Method | GET |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-0TQ83VTDLH&gtm=45je44h0v883337477z877750292za200&_p=1713549403247&_gaz=1&gc 1713549408&ul=en-us&sr=1753x944&pscdl=noapi&_s=1&sid=1713549427&sct=1&seg=0&dl= 2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20%7 20Edureka&en=page_view&_fv=2&_ss=2&_c=1&tfd=27884 |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za200&_p=1713549403247&_gaz=1&gcd=13l3l3l3l 1713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=1&sid=1713549407&sct edureka.co%2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20S 20Edureka&en=page_view&_fv=1&_nsi=1&_ss=1&_ee=1&tfd=8260 |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other | |

| | |
|---|---|
| Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za200&_p=1713549403247&gcd=13l3l3l3l1&npa=01713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=3&sid=1713549407&sctedureka.co%2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20S20Edureka&en=initiate_generate_lead&_ee=1&epn.course_id=100&ep.course_type=No%20Cowebsite_action=Drop_Us_Query_Prompt_Opened_Automatic&ep.timestamp=Fri%2C%2019%220GMT&_et=2945&tfd=54402 |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za200&_p=1713549403247&gcd=13l3l3l3l1&npa=01713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&sid=1713549407&sct=1&se2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20% |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://b.clarity.ms/collect |
| Method | POST |
| Attack | |
| Evidence | nginx/1.18.0 (Ubuntu) |
| Other Info | |
| URL | https://p.easyinsights.in/ga4/vnri56u349gnw03ir0i4u6hngrg039ir03jf390r/g/collect?v=2&tid=G-XWKD9DJ015&gtm=45je44h0v9101910922z877750292za200&_p=1713549403247&gcd=13l31713549408&ul=en-us&sr=1753x944&_fplc=0&pscdl=noapi&_s=1&sid=1713549424&sct=1&se2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20Support%20%20Edureka&en=page_view&_fv=1&_ss=1&ep.eiuid=&tfd=24324 |
| Method | POST |
| Attack | |
| Evidence | nginx/1.20.2 |
| Other Info | |
| URL | https://stats.g.doubleclick.net/g/collect?v=2&tid=G-0TQ83VTDLH&cid=1883432736.1713549408&gtm=45je44h0v883337477z877750292za200&aip=1&dma=0&gcd=13l3l3l3l1&np |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://stats.g.doubleclick.net/g/collect?v=2&tid=G-6JVFN5CRMW&cid=1883432736.1713549408&gtm=45je44h0v893889588za200&aip=1&dma=0&gcd=13l3l3l3l1&npa=0 |
| Method | POST |
| Attack | |
| | |

| | |
|---|---|
| Evidence | Golfe2 |
| Other Info | |
| URL | https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j101&tid=UA-108517196-1&c 1713549408&jid=106012479&gjid=767128232&_gid=1292194650.1713549421&_u=YADAAEA |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://stats.g.doubleclick.net/j/collect?t=dc&aip=1&_r=3&v=1&_v=j101&tid=UA-33865789-2&ci 1713549408&jid=515432050&gjid=108533144&_gid=1292194650.1713549421&_u=YADAAEA |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1815402468&t=pageview&_s=1&dl 2F&ul=en-us&de=UTF-8&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetir bit&sr=1753x944&vp=1280x702&je=0&_u=YADAAEABAAAAACAEK~&jid=106012479&gjid=76 1713549408&tid=UA-108517196-1&_gid=1292194650. 1713549421&_r=1&_slc=1&gtm=45He44h0n81MQVFZMQv77750292za200&cd3=2024-04-19T 3A30&cd4=1713549408988.itl5e6og&gcd=13l3l3l3l1&dma=0&cd2=1883432736.1713549408&z |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| URL | https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1815402468&t=pageview&_s=1&dl 2F&ul=en-us&de=UTF-8&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetir bit&sr=1753x944&vp=1280x702&je=0&_u=YADAAEABAAAAACAEK~&jid=515432050&gjid=10 1713549408&tid=UA-33865789-2&_gid=1292194650.1713549421&_r=1&_slc=1&cd1=false&cd |
| Method | POST |
| Attack | |
| Evidence | Golfe2 |
| Other Info | |
| Instances | 17 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to suppress th |
| Reference | http://httpd.apache.org/docs/current/mod/core.html#servertokens<br>http://msdn.microsoft.com/en-us/library/ff648552.aspx#ht_urlscan_007<br>http://blogs.msdn.com/b/varunm/archive/2013/04/23/remove-unwanted-http-response-headers.a<br>http://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10036 |

| **Low** | **Strict-Transport-Security Header Not Set** |
|---|---|
| Description | HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web serv only secure HTTPS connections (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards |

| | |
|---|---|
| URL | https://a.quora.com/qevents.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/clevertap.min.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/localforage.min.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc4.woff2 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://googleads.g.doubleclick.net/pagead/viewthroughconversion/965688462/?random=1713549421289&cv=11&fst=1713549421289&bg=ffffff&guid=ON&async=1&gtm=45be3A%2F%2Fwww.edureka.co%2F&hn=www.googleadservices.com&frm=0&tiba=Instructor-Led%20Edureka&npa=0&pscdl=noapi&auid=243454040.1713549409&fdr=QA&rfmt=3&fmt=4 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |

| | |
|---|---|
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://s3-eu-west-1.amazonaws.com/static.wizrocket.com/js/sw_webpush.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://snap.licdn.com/li.lms-analytics/insight.min.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.clarity.ms/s/0.7.31/clarity.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.clarity.ms/tag/bu6mlgzzxv |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/js/bg/IsHUla7t4cK5kOAb6cwcBiPQ5HnUjMTZuq5wUJJd2UM.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api.js?onload=onloadCallback&render=explicit&_=17135494 |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api.js?render=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSe cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ cY2JYCwHSTck0_qm-&size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&k=6L |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google.com/recaptcha/api2/webworker.js?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm- |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/styles__ltr.css |
| | |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-0TQ83VTDLH&gtm=45je44h0v883337477z877750292za200&_p=1713549403247&_gaz=1&gc us&sr=1753x944&pscdl=noapi&_s=1&sid=1713549427&sct=1&seg=0&dl=https%3A%2F%2Fw 20Support%20%7C%20Edureka&en=page_view&_fv=2&_ss=2&_c=1&tfd=27884 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za 1713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=1&sid=1713549407&sct 20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&en=page_view&_ |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za 1713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=3&sid=1713549407&sct 20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&en=initiate_gener 20Course&ep.website_action=Drop_Us_Query_Prompt_Opened_Automatic&ep.timestamp=Fri |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za 1713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&sid=1713549407&sct=1&se 20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&_s=2&tfd=32417 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://b.clarity.ms/collect |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://p.easyinsights.in/ga4/vnri56u349gnw03ir0i4u6hngrg039ir03jf390r/g/collect?v=2&tid=G-XWKD9DJ015&gtm=45je44h0v9101910922z877750292za200&_p=1713549403247&gcd=13l3 us&sr=1753x944&_fplc=0&pscdl=noapi&_s=1&sid=1713549424&sct=1&seg=0&dl=https%3A% 20Lifetime%20Support%20%7C%20Edureka&en=page_view&_fv=1&_ss=1&ep.eiuid=&tfd=243 |

| | |
|---|---|
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://px.ads.linkedin.com/wa/ |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://stats.g.doubleclick.net/g/collect?v=2&tid=G-0TQ83VTDLH&cid=1883432736.171354940 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://stats.g.doubleclick.net/g/collect?v=2&tid=G-6JVFN5CRMW&cid=1883432736.171354946 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1815402468&t=pageview&_s=1&dl 20Online%20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&sd=24- bit&sr=1753x944&vp=1280x702&je=0&_u=YADAAEABAAAAACAEK~&jid=106012479&gjid=76 1713549421&_r=1&_slc=1&gtm=45He44h0n81MQVFZMQv77750292za200&cd3=2024-04-19T itl5e6og&gcd=13l3l3l3l1&dma=0&cd2=1883432736.1713549408&z=1335808386 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.google-analytics.com/j/collect?v=1&_v=j101&a=1815402468&t=pageview&_s=1&dl 20Online%20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&sd=24- bit&sr=1753x944&vp=1280x702&je=0&_u=YADAAEABAAAAACAEK~&jid=515432050&gjid=10 1713549421&_r=1&_slc=1&cd1=false&cd2=false&z=983792749 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| Instances | 33 |
| Solution | Ensure that your web server, application server, load balancer, etc. is configured to enforce Stri |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet https://owasp.org/www-community/Security_Headers |

| | |
|---|---|
| | http://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security<br>http://caniuse.com/stricttransportsecurity<br>http://tools.ietf.org/html/rfc6797 |
| CWE Id | 319 |
| WASC Id | 15 |
| Plugin Id | 10035 |

| **Low** | **Timestamp Disclosure - Unix** |
|---|---|
| Description | A timestamp was disclosed by the application/web server - Unix |
| URL | https://a.quora.com/qevents.js |
| Method | GET |
| Attack | |
| Evidence | 1549556828 |
| Other Info | 1549556828, which evaluates to: 2019-02-07 21:57:08 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1426881987 |
| Other Info | 1426881987, which evaluates to: 2015-03-21 01:36:27 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1508970993 |
| Other Info | 1508970993, which evaluates to: 2017-10-26 04:06:33 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1537002063 |
| Other Info | 1537002063, which evaluates to: 2018-09-15 14:31:03 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1541459225 |
| Other Info | 1541459225, which evaluates to: 2018-11-06 04:37:05 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1555081692 |
| Other Info | 1555081692, which evaluates to: 2019-04-12 20:38:12 |

| | |
|---|---|
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1695183700 |
| Other Info | 1695183700, which evaluates to: 2023-09-20 09:51:40 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1747873779 |
| Other Info | 1747873779, which evaluates to: 2025-05-22 05:59:39 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1779033703 |
| Other Info | 1779033703, which evaluates to: 2026-05-17 21:31:43 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1899447441 |
| Other Info | 1899447441, which evaluates to: 2030-03-11 13:47:21 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1925078388 |
| Other Info | 1925078388, which evaluates to: 2031-01-02 05:29:48 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1955562222 |
| Other Info | 1955562222, which evaluates to: 2031-12-21 01:13:42 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 1986661051 |
| Other Info | 1986661051, which evaluates to: 2032-12-14 23:47:31 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | 1996064986 |
| Other Info | 1996064986, which evaluates to: 2033-04-02 19:59:46 |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | 2024104815 |
| Other Info | 2024104815, which evaluates to: 2034-02-21 08:50:15 |
| URL | https://connect.facebook.net/en_US/sdk.js |
| Method | GET |
| Attack | |
| Evidence | 1713549427 |
| Other Info | 1713549427, which evaluates to: 2024-04-19 23:27:07 |
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | 1713549432 |
| Other Info | 1713549432, which evaluates to: 2024-04-19 23:27:12 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=page&d=N4IglgJiBcIGwFYAsBaAWgaTSgHAualA<br>3D&rn=3&i=1713549420&sn=0&gc=eb8591842ee94266ab421b428fd9eefe&tries=1&useIP=fals |
| Method | GET |
| Attack | |
| Evidence | 1713549432 |
| Other Info | 1713549432, which evaluates to: 2024-04-19 23:27:12 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=ping&d=N4IglgJiBcIGwFYAsBaAWgaTSgHAualAN<br>2BgdiBcIC0DuBeFIA0ICW06IHUAbACwDMBBAUQEkBhC1TEAEwgBcBnOABixZK8sANzgAm |
| Method | GET |
| Attack | |
| Evidence | 1713549432 |
| Other Info | 1713549432, which evaluates to: 2024-04-19 23:27:12 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=ping&d=N4IglgJiBcIGwFYAsBaAWgaTSgHAualAN<br>2BgdiBcIC0DuBeFIA0ICW06IHUAbACwDMBBAUQEkBhC1TEAEwgBcBnOABixZK8sANzgAm |
| Method | GET |
| Attack | |
| Evidence | 1713549542 |
| Other Info | 1713549542, which evaluates to: 2024-04-19 23:29:02 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIoCcD2AzAlgGzgGiTS1 |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | 1713549427 |
| Other Info | 1713549427, which evaluates to: 2024-04-19 23:27:07 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI<br>2BOCoeGgCsBgC0AFoA0nExWpEacUIA5h4wAEapRmpaBnowMEYlGhqEuSVqtXpatPxGZbR<br>2BgdiBcIC0DuBeFIA0ICW06IHUAbACwDMBBAUQEkBhC1TEAEwgBcBnOABixZK8sANzgAm |
| Method | GET |
| Attack | |
| Evidence | 1713549432 |
| Other Info | 1713549432, which evaluates to: 2024-04-19 23:27:12 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI<br>2BOCoeGgCsBgC0AFoA0nExWpEacUIA5h4wAEapRmpaBnowMEYlGhqEuSVqtXpatPxGZbR<br>2BgdiBcIC0DuBeFIA0ICW06IHUAbACwDMBBAUQEkBhC1TEAEwgBcBnOABixZK8sANzgAm |
| Method | GET |
| Attack | |
| Evidence | 1713549463 |
| Other Info | 1713549463, which evaluates to: 2024-04-19 23:27:43 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI<br>3D&rn=4&i=1713549420&sn=0&gc=eb8591842ee94266ab421b428fd9eefe&tries=1&useIP=fals |
| Method | GET |
| Attack | |
| Evidence | 1713549432 |
| Other Info | 1713549432, which evaluates to: 2024-04-19 23:27:12 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI<br>2BgDCAIlAsuTFLMRQCAAMOCyMG9s4YFJmCADaALq7jMen8Jf%2B%2FkAAA&rn=2&i=171 |
| Method | GET |
| Attack | |
| Evidence | 1658131456 |
| Other Info | 1658131456, which evaluates to: 2022-07-18 13:34:16 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI<br>2BgDCAIlAsuTFLMRQCAAMOCyMG9s4YFJmCADaALq7jMen8Jf%2B%2FkAAA&rn=2&i=171 |
| Method | GET |
| Attack | |
| Evidence | 1687254908 |
| Other Info | 1687254908, which evaluates to: 2023-06-20 15:25:08 |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI<br>2BgDCAIlAsuTFLMRQCAAMOCyMG9s4YFJmCADaALq7jMen8Jf%2B%2FkAAA&rn=2&i=171 |
| Method | GET |
| Attack | |
| Evidence | 1713549432 |
| Other | |

| | |
|---|---|
| Info | 1713549432, which evaluates to: 2024-04-19 23:27:12 |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | 1713549427 |
| Other Info | 1713549427, which evaluates to: 2024-04-19 23:27:07 |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | 1713635827 |
| Other Info | 1713635827, which evaluates to: 2024-04-20 23:27:07 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1416354905 |
| Other Info | 1416354905, which evaluates to: 2014-11-19 05:25:05 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1444681467 |
| Other Info | 1444681467, which evaluates to: 2015-10-13 01:54:27 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1473231341 |
| Other Info | 1473231341, which evaluates to: 2016-09-07 12:25:41 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1502002290 |
| Other Info | 1502002290, which evaluates to: 2017-08-06 12:21:30 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1518500249 |
| Other Info | 1518500249, which evaluates to: 2018-02-13 11:07:29 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | 1530992060 |
| Other Info | 1530992060, which evaluates to: 2018-07-08 01:04:20 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1560198380 |
| Other Info | 1560198380, which evaluates to: 2019-06-11 01:56:20 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1700485571 |
| Other Info | 1700485571, which evaluates to: 2023-11-20 18:36:11 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1732584193 |
| Other Info | 1732584193, which evaluates to: 2024-11-26 06:53:13 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1732584194 |
| Other Info | 1732584194, which evaluates to: 2024-11-26 06:53:14 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1735328473 |
| Other Info | 1735328473, which evaluates to: 2024-12-28 01:11:13 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1770035416 |
| Other Info | 1770035416, which evaluates to: 2026-02-02 18:00:16 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| | |

| | |
|---|---|
| Attack | |
| Evidence | 1804603682 |
| Other Info | 1804603682, which evaluates to: 2027-03-09 20:18:02 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1839030562 |
| Other Info | 1839030562, which evaluates to: 2028-04-11 07:19:22 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1859775393 |
| Other Info | 1859775393, which evaluates to: 2028-12-07 09:46:33 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1873313359 |
| Other Info | 1873313359, which evaluates to: 2029-05-13 02:19:19 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1894986606 |
| Other Info | 1894986606, which evaluates to: 2030-01-18 22:40:06 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1926607734 |
| Other Info | 1926607734, which evaluates to: 2031-01-19 22:18:54 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1958414417 |
| Other Info | 1958414417, which evaluates to: 2032-01-23 01:30:17 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 1990404162 |

| | |
|---|---|
| Other Info | 1990404162, which evaluates to: 2033-01-27 07:32:42 |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | 2022574463 |
| Other Info | 2022574463, which evaluates to: 2034-02-03 15:44:23 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1683047075 |
| Other Info | 1683047075, which evaluates to: 2023-05-02 22:34:35 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1686041834 |
| Other Info | 1686041834, which evaluates to: 2023-06-06 14:27:14 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1689336232 |
| Other Info | 1689336232, which evaluates to: 2023-07-14 17:33:52 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1692173549 |
| Other Info | 1692173549, which evaluates to: 2023-08-16 13:42:29 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1692617996 |
| Other Info | 1692617996, which evaluates to: 2023-08-21 17:09:56 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1694011023 |
| Other Info | 1694011023, which evaluates to: 2023-09-06 20:07:03 |

| | |
|---|---|
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1694763745 |
| Other Info | 1694763745, which evaluates to: 2023-09-15 13:12:25 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1697611963 |
| Other Info | 1697611963, which evaluates to: 2023-10-18 12:22:43 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1697614569 |
| Other Info | 1697614569, which evaluates to: 2023-10-18 13:06:09 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1698997684 |
| Other Info | 1698997684, which evaluates to: 2023-11-03 13:18:04 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1702385750 |
| Other Info | 1702385750, which evaluates to: 2023-12-12 18:25:50 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1704262959 |
| Other Info | 1704262959, which evaluates to: 2024-01-03 11:52:39 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1708522282 |
| Other Info | 1708522282, which evaluates to: 2024-02-21 19:01:22 |
| URL | https://www.edureka.co/ |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | 1709715474 |
| Other Info | 1709715474, which evaluates to: 2024-03-06 14:27:54 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1712043987 |
| Other Info | 1712043987, which evaluates to: 2024-04-02 13:16:27 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1712154633 |
| Other Info | 1712154633, which evaluates to: 2024-04-03 20:00:33 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1713442415 |
| Other Info | 1713442415, which evaluates to: 2024-04-18 17:43:35 |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | 1713530642 |
| Other Info | 1713530642, which evaluates to: 2024-04-19 18:14:02 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1426881987 |
| Other Info | 1426881987, which evaluates to: 2015-03-21 01:36:27 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1508970993 |
| Other Info | 1508970993, which evaluates to: 2017-10-26 04:06:33 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| | |

| | |
|---|---|
| Evidence | 1518500249 |
| Other Info | 1518500249, which evaluates to: 2018-02-13 11:07:29 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1537002063 |
| Other Info | 1537002063, which evaluates to: 2018-09-15 14:31:03 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1541459225 |
| Other Info | 1541459225, which evaluates to: 2018-11-06 04:37:05 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1555081692 |
| Other Info | 1555081692, which evaluates to: 2019-04-12 20:38:12 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1695183700 |
| Other Info | 1695183700, which evaluates to: 2023-09-20 09:51:40 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1732584193 |
| Other Info | 1732584193, which evaluates to: 2024-11-26 06:53:13 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1747873779 |
| Other Info | 1747873779, which evaluates to: 2025-05-22 05:59:39 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1779033703 |
| Other | |

| | |
|---|---|
| Info | 1779033703, which evaluates to: 2026-05-17 21:31:43 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1859775393 |
| Other Info | 1859775393, which evaluates to: 2028-12-07 09:46:33 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1899447441 |
| Other Info | 1899447441, which evaluates to: 2030-03-11 13:47:21 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1925078388 |
| Other Info | 1925078388, which evaluates to: 2031-01-02 05:29:48 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1955562222 |
| Other Info | 1955562222, which evaluates to: 2031-12-21 01:13:42 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1986661051 |
| Other Info | 1986661051, which evaluates to: 2032-12-14 23:47:31 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 1996064986 |
| Other Info | 1996064986, which evaluates to: 2033-04-02 19:59:46 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | 2000000000 |
| Other Info | 2000000000, which evaluates to: 2033-05-18 09:03:20 |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | 2024104815 |
| Other Info | 2024104815, which evaluates to: 2034-02-21 08:50:15 |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | 1713530642 |
| Other Info | 1713530642, which evaluates to: 2024-04-19 18:14:02 |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | 1713530642 |
| Other Info | 1713530642, which evaluates to: 2024-04-19 18:14:02 |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | 1713549418 |
| Other Info | 1713549418, which evaluates to: 2024-04-19 23:26:58 |
| Instances | 89 |
| Solution | Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregat |
| Reference | http://projects.webappsec.org/w/page/13246936/Information%20Leakage |
| CWE Id | 200 |
| WASC Id | 13 |
| Plugin Id | 10096 |

| **Low** | **X-Content-Type-Options Header Missing** |
|---|---|
| Description | The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows old set), rather than performing MIME-sniffing. |
| URL | https://a.quora.com/qevents.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still aff |
| URL | https://bat.bing.com/bat.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still aff |

| | |
|---|---|
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css-cache/cache-autoload-home_optimized-a81a5d6113f9 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans3.woff |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans5.woff |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans7.woff |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/cssver.1713530642/css/edurekanew/fonts/home_second_ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/cssver.1713530642/css/edurekanew/HomeOptimized/hom |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/home_ico_new_12_5_20.woff |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/icomoon_20210212.woff |
| | |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/Edureka_V_W_logo.webp |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/pcpdevops_logo.webp |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/clevertap/edureka-clever |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/HomeOptimized/discove |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/clevertap.min.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/localforage.min.js |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=page&d=N4IglgJiBcIGwFYAsBaAWgaTSgHAuaIA 3D&rn=3&i=1713549420&sn=0&gc=eb8591842ee94266ab421b428fd9eefe&tries=1&useIP=fals |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=ping&d=N4IglgJiBcIGwFYAsBaAWgaTSgHAuaIAN 2BgdiBcIC0DuBeFIA0ICW06IHUAbACwDMBBAUQEkBhC1TEAEwgBcBnOABixZK8sANzgAm |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIoCcD2AzAlgGzgGiTS1 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI 2BOCoeGgCsBgC0AFoA0nExWpEacUIA5h4wAEapRmpaBnowMEYlGhqEuSVqtXpatPxGZbR 2BgdiBcIC0DuBeFIA0ICW06IHUAbACwDMBBAUQEkBhC1TEAEwgBcBnOABixZK8sANzgAm |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI 3D&rn=4&i=1713549420&sn=0&gc=eb8591842ee94266ab421b428fd9eefe&tries=1&useIP=fals |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://eu1.clevertap-prod.com/a?t=96&type=push&d=N4IgLgngDgpiBcIYDcYDswgDROWAcgI 2BgDCAIIAsuTFLMRQCAAMOCyMG9s4YFJmCADaALq7jMen8Jf%2B%2FkAAA&rn=2&i=1713 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://s3-eu-west-1.amazonaws.com/static.wizrocket.com/js/sw_webpush.js |
| | |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.clarity.ms/s/0.7.31/clarity.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.clarity.ms/tag/bu6mlgzzxv |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.edureka.co/clevertap_sw.js |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://p.easyinsights.in/ga4/vnri56u349gnw03ir0i4u6hngrg039ir03jf390r/g/collect?v=2&tid=G-X 20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&en=page_view&_ |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| Evidence | |

| | |
|---|---|
| Other Info | This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affe |
| Instances | 38 |
| Solution | Ensure that the application/web server sets the Content-Type header appropriately, and that it s<br><br>If possible, ensure that the end user uses a standards-compliant and modern web browser that |
| Reference | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx<br>https://owasp.org/www-community/Security_Headers |
| CWE Id | 693 |
| WASC Id | 15 |
| Plugin Id | 10021 |

| **Informational** | **Content-Type Header Missing** |
|---|---|
| Description | The Content-Type header was either missing or empty. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/Edureka_V_W_logo.webp |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/pcpdevops_logo.webp |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | |
| Instances | 2 |
| Solution | Ensure each page is setting the specific and appropriate content-type value for the content being delivered. |
| Reference | http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx |
| CWE Id | 345 |
| WASC Id | 12 |
| Plugin Id | 10019 |

| **Informational** | **Information Disclosure - Suspicious Comments** |
|---|---|
| Description | The response appears to contain suspicious comments which may help an attacker. Note: Matc |
| URL | https://a.quora.com/qevents.js |
| Method | GET |
| Attack | |
| Evidence | bug |
| Other Info | The following pattern was used: \bBUG\b and was detected in the element starting with: ""use s<br>n=t.b[r],i=e[0]^n[0],", see evidence field for the suspicious comment/snippet. |
| URL | https://a.quora.com/qevents.js |
| Method | GET |
| Attack | |
| Evidence | later |
| | |

| | |
|---|---|
| Other Info | The following pattern was used: \bLATER\b and was detected in the element starting with: "opti |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected in the element starting with: "(functior performance.now&&a.performa", see evidence field for the suspicious comment/snippet. |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | debug |
| Other Info | The following pattern was used: \bDEBUG\b and was detected in the element starting with: "fbq SignalsEventValidation":2,"SignalsFBEve", see evidence field for the suspicious comment/snipp |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | FROM |
| Other Info | The following pattern was used: \bFROM\b and was detected 2 times, the first in the element sta OUT OF OR IN", see evidence field for the suspicious comment/snippet. |
| URL | https://connect.facebook.net/en_US/fbevents.js |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected in the element starting with: "(fur performance&&a.performance.now&&a.performa", see evidence field for the suspicious comme |
| URL | https://connect.facebook.net/en_US/sdk.js |
| Method | GET |
| Attack | |
| Evidence | FROM |
| Other Info | The following pattern was used: \bFROM\b and was detected in the element starting with: " * IN see evidence field for the suspicious comment/snippet. |
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | bug |
| Other Info | The following pattern was used: \bBUG\b and was detected in the element starting with: "__d("js b=typeof i==="fun", see evidence field for the suspicious comment/snippet. |
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | DEBUG |
| Other Info | The following pattern was used: \bDEBUG\b and was detected 5 times, the first in the element s WARNING:1,ERROR:0};c=function(a,b,c){for(var d=argum", see evidence field for the suspiciou |

| | |
|---|---|
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | FROM |
| Other Info | The following pattern was used: \bFROM\b and was detected 15 times, the first in the element s OUT OF OR IN", see evidence field for the suspicious comment/snippet. |
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 5 times, the first in the element s ([^\\\\/?#@]*@)?(\\[[A-Fa-f0-9:.]+\\]|[^\\/?#:]*)(:", see evidence field for the suspicious comment/s |
| URL | https://connect.facebook.net/en_US/sdk.js?hash=a77c8961ad24e42bf593507fc95cbed9 |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected 2 times, the first in the element sta Runtime"],(function(a,b,c,d,e,f,g){var h=Object.", see evidence field for the suspicious comment/ |
| URL | https://connect.facebook.net/signals/config/674497915940609?v=2.9.154&r=stable&domain=ww co&hme=c3a545c63044e8e9102d4f32d84a1137594d024f28e801d670bc76dc5c075575&ex_m 2C51%2C158%2C161%2C172%2C168%2C169%2C171%2C28%2C94%2C50%2C73%2C170 2C17%2C33%2C38%2C1%2C41%2C62%2C63%2C64%2C68%2C88%2C16%2C13%2C90% 2C27%2C10%2C11%2C12%2C5%2C6%2C24%2C21%2C22%2C54%2C59%2C61%2C71%2 2C81%2C53%2C79%2C32%2C70%2C0%2C89%2C31%2C78%2C83%2C45%2C44%2C82% 2C43%2C75%2C65%2C104%2C57%2C56%2C30%2C92%2C55%2C52%2C47%2C74%2C69 |
| Method | GET |
| Attack | |
| Evidence | FROM |
| Other Info | The following pattern was used: \bFROM\b and was detected 2 times, the first in the element sta OUT OF OR IN", see evidence field for the suspicious comment/snippet. |
| URL | https://connect.facebook.net/signals/config/674497915940609?v=2.9.154&r=stable&domain=ww co&hme=c3a545c63044e8e9102d4f32d84a1137594d024f28e801d670bc76dc5c075575&ex_m 2C51%2C158%2C161%2C172%2C168%2C169%2C171%2C28%2C94%2C50%2C73%2C170 2C17%2C33%2C38%2C1%2C41%2C62%2C63%2C64%2C68%2C88%2C16%2C13%2C90% 2C27%2C10%2C11%2C12%2C5%2C6%2C24%2C21%2C22%2C54%2C59%2C61%2C71%2 2C81%2C53%2C79%2C32%2C70%2C0%2C89%2C31%2C78%2C83%2C45%2C44%2C82% 2C43%2C75%2C65%2C104%2C57%2C56%2C30%2C92%2C55%2C52%2C47%2C74%2C69 |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 3 times, the first in the element s getFbeventsModules("SignalsFBEventsURLUti", see evidence field for the suspicious comment |
| URL | https://connect.facebook.net/signals/config/674497915940609?v=2.9.154&r=stable&domain=ww co&hme=c3a545c63044e8e9102d4f32d84a1137594d024f28e801d670bc76dc5c075575&ex_m 2C51%2C158%2C161%2C172%2C168%2C169%2C171%2C28%2C94%2C50%2C73%2C170 2C17%2C33%2C38%2C1%2C41%2C62%2C63%2C64%2C68%2C88%2C16%2C13%2C90% 2C27%2C10%2C11%2C12%2C5%2C6%2C24%2C21%2C22%2C54%2C59%2C61%2C71%2 2C81%2C53%2C79%2C32%2C70%2C0%2C89%2C31%2C78%2C83%2C45%2C44%2C82% 2C43%2C75%2C65%2C104%2C57%2C56%2C30%2C92%2C55%2C52%2C47%2C74%2C69 |
| Method | GET |
| | |

| | |
|---|---|
| Attack | |
| Evidence | select |
| Other Info | The following pattern was used: \bSELECT\b and was detected in the element starting with: "ret getFbeventsModules("SignalsFBEventsFeatur", see evidence field for the suspicious comment/ |
| URL | https://connect.facebook.net/signals/config/674497915940609?v=2.9.154&r=stable&domain=w co&hme=c3a545c63044e8e9102d4f32d84a1137594d024f28e801d670bc76dc5c075575&ex_m 2C51%2C158%2C161%2C172%2C168%2C169%2C171%2C28%2C94%2C50%2C73%2C17 2C17%2C33%2C38%2C1%2C41%2C62%2C63%2C64%2C68%2C88%2C16%2C13%2C90% 2C27%2C10%2C11%2C12%2C5%2C6%2C24%2C21%2C22%2C54%2C59%2C61%2C71%2 2C81%2C53%2C79%2C32%2C70%2C0%2C89%2C31%2C78%2C83%2C45%2C44%2C82% 2C43%2C75%2C65%2C104%2C57%2C56%2C30%2C92%2C55%2C52%2C47%2C74%2C69 |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "retur assign\|\|function(a){for(var b=1;b<ar", see evidence field for the suspicious comment/snippet. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 2 times, the first in the element startir exports=a.document?b(a,!0):function(a){if(!a.docu", see evidence field for the suspicious comme |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 14 times, the first in the element exports=t():"function"==typeof define&&define.amd?def", see evidence field for the suspicious c |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | select |
| Other Info | The following pattern was used: \bSELECT\b and was detected 5 times, the first in the element (function(A){var t,e,i,n;function s(t,e){var i", see evidence field for the suspicious comment/snipp |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | User |
| Other Info | The following pattern was used: \bUSER\b and was detected 13 times, the first in the element s new-passwd'));var status=(response.status=='error')?", see evidence field for the suspicious cor |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/js-cache/cache-autoload-home_optimized-2fa348bf861551 |
| Method | GET |
| Attack | |
| Evidence | username |
| Other Info | The following pattern was used: \bUSERNAME\b and was detected in the element starting with: this.easing=e\|\|"swing",this.options=", see evidence field for the suspicious comment/snippet. |
| | |

| | |
|---|---|
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/clevertap/edureka-clever |
| Method | GET |
| Attack | |
| Evidence | From |
| Other Info | The following pattern was used: \bFROM\b and was detected 4 times, the first in the element sta field for the suspicious comment/snippet. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/clevertap/edureka-clever |
| Method | GET |
| Attack | |
| Evidence | Query |
| Other Info | The following pattern was used: \bQUERY\b and was detected in the element starting with: "var comment/snippet. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/clevertap/edureka-clever |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected 3 times, the first in the element sta suspicious comment/snippet. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/jsver.1713530642/js/edurekanew/clevertap/edureka-clever |
| Method | GET |
| Attack | |
| Evidence | userName |
| Other Info | The following pattern was used: \bUSERNAME\b and was detected 4 times, the first in the elem /snippet. |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/clevertap.min.js |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "!func ==typeof define&&define.amd?def", see evidence field for the suspicious comment/snippet. |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/localforage.min.js |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected in the element starting with: "!function ("function"==typeof define&&defin", see evidence field for the suspicious comment/snippet. |
| URL | https://googleads.g.doubleclick.net/pagead/viewthroughconversion/965688462/?random=1713549421289&cv=11&fst=1713549421289&bg=ffffff&guid=ON&async=1&gtm=45be3A%2F%2Fwww.edureka.co%2F&hn=www.googleadservices.com&frm=0&tiba=Instructor-Led%20Edureka&npa=0&pscdl=noapi&auid=243454040.1713549409&fdr=QA&rfmt=3&fmt=4 |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "(func Identifier: Apache-2.0 */ va", see evidence field for the suspicious comment/snippet. |

| | |
|---|---|
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | XXX |
| Other Info | The following pattern was used: \bXXX\b and was detected in the element starting with: "!functio ({IDENTIFY_USER:"ident", see evidence field for the suspicious comment/snippet. |
| URL | https://snap.licdn.com/li.lms-analytics/insight.min.js |
| Method | GET |
| Attack | |
| Evidence | select |
| Other Info | The following pattern was used: \bSELECT\b and was detected in the element starting with: "!fu enumerable:!0,configurable:!0,writab", see evidence field for the suspicious comment/snippet. |
| URL | https://static.hotjar.com/c/hotjar-1826269.js?sv=6 |
| Method | GET |
| Attack | |
| Evidence | debug |
| Other Info | The following pattern was used: \bDEBUG\b and was detected in the element starting with: "!fur Symbol.iterator?function(t){return t", see evidence field for the suspicious comment/snippet. |
| URL | https://www.clarity.ms/s/0.7.31/clarity.js |
| Method | GET |
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected in the element starting with: "!fu qa},get stop(){return Fa}", see evidence field for the suspicious comment/snippet. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected in the element starting with: "<sc "https://www.edurek", see evidence field for the suspicious comment/snippet. |
| URL | https://www.google-analytics.com/analytics.js |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 5 times, the first in the element startir *Task$/.test(a)&&J(92)}function mf(a,b){if(a)", see evidence field for the suspicious comment/sn |
| URL | https://www.google-analytics.com/analytics.js |
| Method | GET |
| Attack | |
| Evidence | debug |
| Other Info | The following pattern was used: \bDEBUG\b and was detected in the element starting with: "fun ("gtm_debug"))&&(b=2);!b&&D(M.referr", see evidence field for the suspicious comment/snippet |
| URL | https://www.google-analytics.com/analytics.js |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 5 times, the first in the element s a=a.hostname.replace(N,"").toLowerCase();c&&(c=", see evidence field for the suspicious comm |
| URL | https://www.google.com/js/bg/IsHUla7t4cK5kOAb6cwcBiPQ5HnUjMTZuq5wUJJd2UM.js |
| Method | GET |
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected in the element starting with: "'va g<<x:g>>>x)}catch(f){throw f;}},Y0=f", see evidence field for the suspicious comment/snippet. |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 13 times, the first in the element start (this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | from |
| Other Info | The following pattern was used: \bFROM\b and was detected 3 times, the first in the element sta return a},fh=function(a,b){var c=b.preHit;if(c){", see evidence field for the suspicious comment/sr |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 11 times, the first in the element case "path":a.pathname||a.hostname||ib("TAGGING",", see evidence field for the suspicious cor |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element ("");else b=bc.test(a)?a:void 0;return b};var e", see evidence field for the suspicious comment/sr |
| URL | https://www.googletagmanager.com/gtag/destination?id=AW-965688462&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&" ("auto"!==e||b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| | |

| | |
|---|---|
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 12 times, the first in the element start (this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | from |
| Other Info | The following pattern was used: \bFROM\b and was detected 4 times, the first in the element sta return a},fh=function(a,b){var c=b.preHit;if(c){", see evidence field for the suspicious comment/s |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 15 times, the first in the element vtp_dmaDefault":"DENIED","tag_id":111},{"function":"_", see evidence field for the suspicious co |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element ("");else b=bc.test(a)?a:void 0;return b};var e", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&" ("auto"!==e||b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-0TQ83VTDLH&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | username |
| Other Info | The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the elem replace",[7,[15,"u"],"\\$1"]]]],[50,"w",[46,"bk", see evidence field for the suspicious comment/snip |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 13 times, the first in the element start (this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | from |
| Other | The following pattern was used: \bFROM\b and was detected 4 times, the first in the element sta |

| | |
|---|---|
| Info | return a},fh=function(a,b){var c=b.preHit;if(c){", see evidence field for the suspicious comment/s |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 15 times, the first in the element vtp_isManualEnabled":false,"vtp_isEnabled":true", see evidence field for the suspicious comme |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element ("");else b=bc.test(a)?a:void 0;return b};var e", see evidence field for the suspicious comment/s |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&" ("auto"!==e||b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-6JVFN5CRMW |
| Method | GET |
| Attack | |
| Evidence | username |
| Other Info | The following pattern was used: \bUSERNAME\b and was detected 3 times, the first in the elem replace",[7,[15,"u"],"\\$1"]]]],[50,"w",[46,"bk", see evidence field for the suspicious comment/snip |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 13 times, the first in the element start (this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | from |
| Other Info | The following pattern was used: \bFROM\b and was detected 4 times, the first in the element st return a},fh=function(a,b){var c=b.preHit;if(c){", see evidence field for the suspicious comment/s |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 15 times, the first in the element CSS_SELECTOR","vtp_manualEmailEnabled":false,"vtp_firstNa", see evidence field for the sus |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element ("");else b=bc.test(a)?a:void 0;return b};var e", see evidence field for the suspicious comment/sr |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&" ("auto"!==e||b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet. |
| URL | https://www.googletagmanager.com/gtag/js?id=G-XWKD9DJ015&l=dataLayer&cx=c |
| Method | GET |
| Attack | |
| Evidence | username |
| Other Info | The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the elem function RG(a,b){}RG.H="internal.mergeRemoteConfig";fu", see evidence field for the suspiciou |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 14 times, the first in the element start (this.m,Array.prototype.slice.call(arguments)", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | debug |
| Other Info | The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element s [{"key":"gtag","read":true,"write":true,"execute":true}", see evidence field for the suspicious comr |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | from |
| Other Info | The following pattern was used: \bFROM\b and was detected 3 times, the first in the element sta return Promise.resolve(a);try{var b=Oh(a);retu", see evidence field for the suspicious comment/s |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | QUERY |
| Other Info | The following pattern was used: \bQUERY\b and was detected 17 times, the first in the element (function(){var b=2;return function(a){a.set(\"", see evidence field for the suspicious comment/sn |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| | |

| | |
|---|---|
| Attack | |
| Evidence | SELECT |
| Other Info | The following pattern was used: \bSELECT\b and was detected 2 times, the first in the element ("");else b=bc.test(a)?a:void 0;return b};var e", see evidence field for the suspicious comment/sr |
| URL | https://www.googletagmanager.com/gtm.js?id=GTM-MQVFZMQ |
| Method | GET |
| Attack | |
| Evidence | user |
| Other Info | The following pattern was used: \bUSER\b and was detected in the element starting with: "e&&" ("auto"!==e\|\|b.vtp_allowAutoDataSou", see evidence field for the suspicious comment/snippet. |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | db |
| Other Info | The following pattern was used: \bDB\b and was detected 45 times, the first in the element start =M&&(l[12](56,B,c,v),"number"===typeof M?(l=v[P", see evidence field for the suspicious comm |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | from |
| Other Info | The following pattern was used: \bFROM\b and was detected 15 times, the first in the element s (X).reverse().some(B),1==(E>>C[1]&7))&&(iy.call(", see evidence field for the suspicious comm |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | later |
| Other Info | The following pattern was used: \bLATER\b and was detected in the element starting with: "'Try doscaptcha-header")+B[2]+l[33](h[", see evidence field for the suspicious comment/snippet. |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | query |
| Other Info | The following pattern was used: \bQUERY\b and was detected 2 times, the first in the element s ==E&&(this[a[2]]=M,this[a[0]]=X,this.W=v,this.", see evidence field for the suspicious comment/s |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | select |
| Other Info | The following pattern was used: \bSELECT\b and was detected 29 times, the first in the elemen break a;case M:h=v?"check":"uncheck";break a;case 32:h", see evidence field for the suspicious |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | user |

| | |
|---|---|
| Other Info | The following pattern was used: \bUSER\b and was detected 6 times, the first in the element sta allow-storage-access-by-user-activation"]),X);", see evidence field for the suspicious comment/s |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | username |
| Other Info | The following pattern was used: \bUSERNAME\b and was detected 2 times, the first in the elem (4,55,l[36].bind(null,2)),function(E){return d[13].ca", see evidence field for the suspicious comme |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | TODO |
| Other Info | The following pattern was used: \bTODO\b and was detected in the element starting with: "<scri =w[u]||", see evidence field for the suspicious comment/snippet. |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | select |
| Other Info | The following pattern was used: \bSELECT\b and was detected in the element starting with: "<s clp_banner_offer_expire = '04/20/20", see evidence field for the suspicious comment/snippet. |
| Instances | 75 |
| Solution | Remove all comments that return information that may help an attacker and fix any underlying p |
| 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.Th cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a p access the cookie. Loosely scoped cookies are common in mega-applications like google.com a domain by the browser. However, cookies scoped to a parent-level domain may be transmitted |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20online%20course,%20Android%20training,%20%20edureka,%20online%20course,big%20da 20Computing,%20development,%20online%20training,%20devops,%20tableau,%20python,%2 2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | The origin domain used for comparison was: bat.bing.com MUID=07F6CCED066C6CFC30E9D |
| URL | https://googleads.g.doubleclick.net/pagead/viewthroughconversion/965688462/?random=1713549421289&cv=11&fst=1713549421289&bg=ffffff&guid=ON&async=1&gtm=45be 3A%2F%2Fwww.edureka.co%2F&hn=www.googleadservices.com&frm=0&tiba=Instructor-Led% 20Edureka&npa=0&pscdl=noapi&auid=243454040.1713549409&fdr=QA&rfmt=3&fmt=4 |
| Method | GET |
| | |

| | |
|---|---|
| Attack | |
| Evidence | |
| Other Info | The origin domain used for comparison was: googleads.g.doubleclick.net test_cookie=CheckFo |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | The origin domain used for comparison was: px.ads.linkedin.com li_sugr=e0475219-6a09-417f-<br>s=O:r=O:a=O:p=O:g=3033:u=1:x=1:i=1713549427:t=1713635827:v=2:sig=AQGqCoN26Xs8ew |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1<br>2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | The origin domain used for comparison was: px.ads.linkedin.com li_sugr=e0475219-6a09-417f-<br>UserMatchHistory=AQK5Fsihhbt7wQAAAY73gVRrn_h_d0ul4sFOBueXg2DlYYk0VXijJmGczF8<br>AnalyticsSyncHistory=AQJkiECfjw0LZgAAAY73gVRrtWbxiJn4ZdO418tU-w9QCjR7H9oCdfrGqk<br>5e1931b483bf |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1<br>2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | The origin domain used for comparison was: px.ads.linkedin.com li_sugr=e0475219-6a09-417f- |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | The origin domain used for comparison was: www.edureka.co _aIpjT6rhLb=false brain4ce_n=jn |
| Instances | 6 |
| Solution | Always scope cookies to a FQDN (Fully Qualified Domain Name). |
| Reference | https://tools.ietf.org/html/rfc6265#section-4.1<br>https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Tes<br>http://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 Spider may well be more effective than the standard one. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | <a aria-label="logo" class="trackButton" data-button-name="Edureka" data-button-location="Firs data-button-type="Static" href="/" target="_self"> <img style="min-height: 10px;" class="" src=" https://d1jnx9ba8s6j9r.cloudfront.net/imgver.1713530642/img/Edureka_V_W_logo.webp" alt="lo |
| Other Info | Links have been found with a target of '_self' - this is often used by modern frameworks to force |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c &hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |
| Method | GET |
| Attack | |
| Evidence | <script nonce="UkKnEIxN7fhNqXSM1HvoEw" type="text/javascript">window['__recaptcha_api'] google.com/recaptcha/api2/';</script> |
| Other Info | No links have been found while there are scripts, which is an indication that this is a modern we |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ 0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_ &size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | <script nonce="8iqwp031_OTtxXhTFdYIbg" type="text/javascript">window['__recaptcha_api'] = google.com/recaptcha/api2/';</script> |
| Other Info | No links have been found while there are scripts, which is an indication that this is a modern we |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | <script nonce="0Oj_RjVB_1vXHma-81gbCQ" type="text/javascript">window['__recaptcha_api'] google.com/recaptcha/api2/';</script> |
| Other Info | No links have been found while there are scripts, which is an indication that this is a modern we |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | <script type="text/javascript"> // load script after pageload : TODO (function(w,d,t,r,u){var f,n,i;w f=function(){var o={ti:"4065243"};o.q=w[u],w[u]=new UET(o),w[u].push("pageLoad")},n=d.create n.async=1,n.onload=n.onreadystatechange=function(){var s=this.readyState;s&&s!=="loaded"& (f(),n.onload=n.onreadystatechange=null)},i=d.getElementsByTagName(t)[0],i.parentNode.inser (window,document,"script","//bat.bing.com/bat.js","uetq"); </script> |
| Other Info | No links have been found while there are scripts, which is an indication that this is a modern we |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | <script> var onloadCallback = function() { grecaptcha.render('g-recaptcha', { 'sitekey' : '6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj' }); }; </script> |
| Other Info | No links have been found while there are scripts, which is an indication that this is a modern we |
| Instances | 6 |
| Solution | This is an informational alert and so no changes are required. |

| | |
|---|---|
| Reference | |
| CWE Id | |
| WASC Id | |
| Plugin Id | 10109 |

| **Informational** | **Re-examine Cache-control Directives** |
|---|---|
| Description | The cache-control header has not been set properly or is missing, allowing the browser and pro like css, js, or image files this might be intended, however, the resources should be reviewed to cached. |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | s-maxage=100;max-age=0 |
| Other Info | |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | private, max-age=0 |
| Other Info | |
| URL | https://p.easyinsights.in/ga4/vnri56u349gnw03ir0i4u6hngrg039ir03jf390r/g/collect?v=2&tid=G-XWKD9DJ015&gtm=45je44h0v9101910922z877750292za200&_p=1713549403247&gcd=13l3 1713549408&ul=en-us&sr=1753x944&_fplc=0&pscdl=noapi&_s=1&sid=1713549424&sct=1&se edureka.co%2F&dt=Instructor-Led%20Online%20Training%20with%2024X7%20Lifetime%20S 20Edureka&en=page_view&_fv=1&_ss=1&ep.eiuid=&tfd=24324 |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | private, max-age=0 |
| Other Info | |
| URL | https://www.edureka.co/lazyload/loadHomePageOfferBanner |
| Method | POST |
| Attack | |
| Evidence | private, max-age=0 |
| Other Info | |
| URL | https://www.edureka.co/users/tokens |
| Method | POST |
| Attack | |
| | |

| | |
|---|---|
| Evidence | private, max-age=0 |
| Other Info | |
| Instances | 6 |
| Solution | For secure content, ensure the cache-control HTTP header is set with "no-cache, no-store, mus cached consider setting the directives "public, max-age, immutable". |
| Reference | https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Cache-Control https://grayduck.mn/2021/09/13/cache-control-recommendations/ |
| CWE Id | 525 |
| WASC Id | 13 |
| Plugin Id | 10015 |

| **Informational** | **Retrieved from Cache** |
|---|---|
| Description | The content was retrieved from a shared cache. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance. |
| URL | https://a.quora.com/qevents.js |
| Method | GET |
| Attack | |
| Evidence | Age: 57549 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans3.woff |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans5.woff |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/css/fonts/opensans7.woff |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/cssver.1713530642/css/edurekanew/fonts /home_second_fold_ico_3_6_20.woff |
| Method | GET |

| | |
|---|---|
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/home_ico_new_12_5_20.woff |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://d1jnx9ba8s6j9r.cloudfront.net/fonts/icomoon_20210212.woff |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://d2r1yp2w7bby2u.cloudfront.net/js/clevertap.min.js |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://fonts.gstatic.com/s/roboto/v18/KFOlCnqEu92Fr1MmEU9fBBc4.woff2 |
| Method | GET |
| Attack | |
| Evidence | Age: 396103 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxK.woff2 |
| Method | GET |
| Attack | |
| Evidence | Age: 148437 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://script.hotjar.com/modules.9c3b50ddbc74247d2ae3.js |
| Method | GET |
| Attack | |
| Evidence | Hit from cloudfront |
| Other Info | |
| URL | https://www.google-analytics.com/analytics.js |
| Method | GET |
| Attack | |
| Evidence | Age: 3717 |

| | |
|---|---|
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://www.google-analytics.com/analytics.js |
| Method | GET |
| Attack | |
| Evidence | Age: 3718 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://www.google.com/js/bg/IsHUla7t4cK5kOAb6cwcBiPQ5HnUjMTZuq5wUJJd2UM.js |
| Method | GET |
| Attack | |
| Evidence | Age: 216695 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | Age: 388447 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/recaptcha__en.js |
| Method | GET |
| Attack | |
| Evidence | Age: 388453 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| URL | https://www.gstatic.com/recaptcha/releases/rz4DvU-cY2JYCwHSTck0_qm-/styles__ltr.css |
| Method | GET |
| Attack | |
| Evidence | Age: 567136 |
| Other Info | The presence of the 'Age' header indicates that that a HTTP/1.1 compliant caching server is in use. |
| Instances | 17 |
| Solution | Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:<br><br>Cache-Control: no-cache, no-store, must-revalidate, private<br><br>Pragma: no-cache<br><br>Expires: 0<br><br>This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request. |
| | https://tools.ietf.org/html/rfc7234 |

| | |
|---|---|
| Reference | https://tools.ietf.org/html/rfc7231<br>http://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html (obsoleted by rfc7234) |
| CWE Id | |
| WASC Id | |
| Plugin Id | 10050 |

| **Informational** | **Session Management Response Identified** |
|---|---|
| Description | The given response has been identified as containing a session management token. The 'Other Management Method. If the request is in a context which has a Session Management Method s identified. |
| URL | https://bat.bing.com/action/0?ti=4065243&Ver=2&mid=df55305e-061b-407c-b6e5-d75b7aa93d39&sid=393ddff0fe7611eea398d53bdab27b47&vid=393ec230fe7611eea74ba7f4d4 US&sw=1753&sh=944&sc=24&nwd=1&tl=Instructor-Led%20Online%20Training%20with%2024 20online%20course,%20Android%20training,%20%20edureka,%20online%20course,big%20da 20Computing,%20development,%20online%20training,%20devops,%20tableau,%20python,%2 2F&r=&lt=14322&evt=pageLoad&sv=1&rn=980584 |
| Method | GET |
| Attack | |
| Evidence | 07F6CCED066C6CFC30E9D88B079E6DA8 |
| Other Info | cookie:MUID |
| URL | https://googleads.g.doubleclick.net/pagead/viewthroughconversion/965688462/?random=1713549421289&cv=11&fst=1713549421289&bg=ffffff&guid=ON&async=1&gtm=45be 3A%2F%2Fwww.edureka.co%2F&hn=www.googleadservices.com&frm=0&tiba=Instructor-Led% 20Edureka&npa=0&pscdl=noapi&auid=243454040.1713549409&fdr=QA&rfmt=3&fmt=4 |
| Method | GET |
| Attack | |
| Evidence | CheckForPermission |
| Other Info | cookie:test_cookie |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 |
| Method | GET |
| Attack | |
| Evidence | v=2&020bbfeb-ed57-40b3-8d04-5e1931b483bf |
| Other Info | cookie:bcookie cookie:lidc cookie:li_sugr |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true |
| Method | GET |
| Attack | |
| Evidence | AQJkiECfjw0LZgAAAY73gVRrtWbxiJn4ZdO418tU-w9QCjR7H9oCdfrGqk9ZgxaTspcCmmO1Kb |
| Other Info | cookie:AnalyticsSyncHistory cookie:bcookie cookie:li_sugr cookie:UserMatchHistory |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | v=2&020bbfeb-ed57-40b3-8d04-5e1931b483bf |
| Other | |

| | |
|---|---|
| Info | cookie:bcookie cookie:li_sugr |
| URL | https://www.clarity.ms/tag/bu6mlgzzxv |
| Method | GET |
| Attack | |
| Evidence | 0b523347acd3406ab0f6755478c0ed82.20240419.20250419 |
| Other Info | cookie:CLID |
| URL | https://www.edureka.co/ |
| Method | GET |
| Attack | |
| Evidence | %7B%22date%22%3A%222024-04-19+23%3A22%3A17%22%2C%22count%22%3A1%7D |
| Other Info | cookie:CakeCookie[Visited] cookie:CakeCookie[timezoneprefrence] cookie:f_l_i_s_p cookie:_ut |
| URL | https://www.linkedin.com/px/li_sync?redirect=https%3A%2F%2Fpx.ads.linkedin.com%2Fcollect 3Dc179cf8a-4c6d-4b63-bd84-34747184b4db%26url%3Dhttps%253A%252F%252Fwww.edurek |
| Method | GET |
| Attack | |
| Evidence | v=1&20240419175715a2da1ba6-444d-42a5-8ef7-d39b989e30a9AQHhWK6uYLI0NzwCEcR9-c |
| Other Info | cookie:bscookie |
| URL | https://px.ads.linkedin.com/collect?v=2&fmt=js&pid=180467&time=1713549421165&li_adsId=c1 2F&cookiesTest=true&liSync=true |
| Method | GET |
| Attack | |
| Evidence | https://www.edureka.co/ |
| Other Info | url:url |
| URL | https://px.ads.linkedin.com/wa |
| Method | GET |
| Attack | |
| Evidence | AQJkiECfjw0LZgAAAY73gVRrtWbxiJn4ZdO418tU-w9QCjR7H9oCdfrGqk9ZgxaTspcCmmO1Kb |
| Other Info | cookie:AnalyticsSyncHistory |
| URL | https://px.ads.linkedin.com/wa |
| Method | GET |
| Attack | |
| Evidence | "v=2&020bbfeb-ed57-40b3-8d04-5e1931b483bf" |
| Other Info | cookie:bcookie |
| URL | https://px.ads.linkedin.com/wa |
| Method | GET |
| Attack | |
| Evidence | e0475219-6a09-417f-b2b1-0bda3b23c2d8 |
| Other Info | cookie:li_sugr |

| | |
|---|---|
| URL | https://px.ads.linkedin.com/wa |
| Method | GET |
| Attack | |
| Evidence | "b=OGST05:s=O:r=O:a=O:p=O:g=3033:u=1:x=1:i=1713549427:t=1713635827:v=2:sig=AQGqC |
| Other Info | cookie:lidc |
| URL | https://px.ads.linkedin.com/wa |
| Method | GET |
| Attack | |
| Evidence | AQK5Fsihhbt7wQAAAY73gVRrn_h_d0ul4sFOBueXg2DlYYk0VXijJmGczF8b8572iijoYHBzIzcO |
| Other Info | cookie:UserMatchHistory |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | [[www.edureka.co/]](direct)&1713549413159.1713549413159.1 |
| Other Info | cookie:__reff |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | 1713549413159.1713549413159.1 |
| Other Info | cookie:__sreff |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | 10j29tq%7C2%7Cfl2%7C0%7C1570 |
| Other Info | cookie:_clck |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | GA1.2.1883432736.1713549408 |
| Other Info | cookie:_ga |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | GS1.1.1713549407.1.0.1713549407.60.0.0 |
| Other Info | cookie:_ga_6JVFN5CRMW |
| URL | https://www.edureka.co/lazyload |
| | |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | 1.1.243454040.1713549409 |
| Other Info | cookie:_gcl_au |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | GA1.2.1292194650.1713549421 |
| Other Info | cookie:_gid |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | eyJpZCI6IjgzMWQzNzE5LTU4YWMtNGU1OC1hMWRhLTIxNjhlNDZiZGVhZCIsImMiOjE3MTM |
| Other Info | cookie:_hjSession_1826269 |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | eyJpZCI6ImVjYzIzMjk4LTlhNTUtNTQ2Ni05NzIzLTdjN2JlZTIyMWFkOCIsImNyZWF0ZWQiOjE3 |
| Other Info | cookie:_hjSessionUser_1826269 |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | 393ddff0fe7611eea398d53bdab27b47 |
| Other Info | cookie:_uetsid |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | 393ec230fe7611eea74ba7f4d4a33498 |
| Other Info | cookie:_uetvid |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | http%3A%2F%2Fwww.edureka.co%2F |
| Other Info | cookie:_utm_wb_term |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |

| | |
|---|---|
| Evidence | jn3a9dbppo42kbj9d9grkgng14 |
| Other Info | cookie:brain4ce_n |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | getcoursedata |
| Other Info | cookie:CakeCookie[landingpage] |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | Asia%2FKolkata |
| Other Info | cookie:CakeCookie[timezoneprefrence] |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | %7B%22date%22%3A%222024-04-19+23%3A22%3A17%22%2C%22count%22%3A1%7D |
| Other Info | cookie:CakeCookie[Visited] |
| URL | https://www.edureka.co/lazyload |
| Method | GET |
| Attack | |
| Evidence | %7B%22p%22%3A1%7D |
| Other Info | cookie:WZRK_S_654-ZKZ-856Z |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | GA1.1.1883432736.1713549408 |
| Other Info | cookie:_ga |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | GS1.1.1713549407.1.0.1713549425.42.0.0 |
| Other Info | cookie:_ga_6JVFN5CRMW |
| URL | https://www.edureka.co/users/removeredirectreferrer |
| Method | GET |
| Attack | |
| Evidence | GS1.1.1713549424.1.0.1713549424.0.0.0 |
| | |

| | |
|---|---|
| Other Info | cookie:_ga_XWKD9DJ015 |
| URL | https://www.facebook.com/tr/?id=674497915940609&ev=PageView&dl=https%3A%2F%2Fwww&r=stable&ec=0&o=4126&fbp=fb.1.1713549423645.757158361&ler=empty&it=1713549420688 |
| Method | GET |
| Attack | |
| Evidence | fb.1.1713549423645.757158361 |
| Other Info | url:fbp |
| URL | https://www.google-analytics.com/collect?v=1&_v=j101&a=1815402468&t=event&_s=6&dl=http20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&sd=24-bit&sr=1753x944&vp=1280x702&je=0&ec=Inquiry_Funnel&ea=Drop_Us_Query_Prompt_Open2023%3A27%3A29%20GMT%2B0530%20(India%20Standard%20Time)%2C%20Country%3A20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&ev=0&_u=aDDAAEABAAAA1713549421&cd1=false&cd4=1883432736.1713549408&cd5=1932024.1883432736.17135494F10j29tq%2F9ti624&z=95299747 |
| Method | GET |
| Attack | |
| Evidence | https://www.edureka.co/ |
| Other Info | url:dl |
| URL | https://analytics.google.com/g/collect?v=2&tid=G-6JVFN5CRMW&gtm=45je44h0v893889588za1713549408&ul=en-us&sr=1753x944&ir=1&pscdl=noapi&_eu=EA&_s=3&sid=1713549407&sct20Training%20with%2024X7%20Lifetime%20Support%20%7C%20Edureka&en=initiate_gener20Course&ep.website_action=Drop_Us_Query_Prompt_Opened_Automatic&ep.timestamp=Fri |
| Method | POST |
| Attack | |
| Evidence | https://www.edureka.co/ |
| Other Info | url:dl |
| URL | https://b.clarity.ms/collect |
| Method | POST |
| Attack | |
| Evidence | 07F6CCED066C6CFC30E9D88B079E6DA8 |
| Other Info | cookie:MUID |
| Instances | 38 |
| 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 Controllable HTML Element Attribute (Potential XSS)** |
|---|---|
| Description | This check looks at user-supplied input in query string parameters and POST data to identify wh attribute values might be controlled. This provides hot-spot detection for XSS (cross-site scriptin further review by a security analyst to determine exploitability. |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om |

| | |
|---|---|
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Ldp5aooAAAAANIW2DevNVZr5QfSexqPIGx9StbG&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=invisible&cb=r2cwssyaj7om appears to include [html] tag [lang] attribute The user input found was: hl=en The user-controlled value was: en |
| URL | https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJ0aj&co=aHR0cHM6Ly93d3cuZWR1cmVrYS5jbzo0NDM.&hl=en&v=rz4DvU-cY2JYCwHSTck0_&size=compact&cb=v7l0sv7mkvwv |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.google.com/recaptcha/api2/anchor?ar=1&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj&co=aHR0cHM6Ly93d3cuZWR1c&hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&size=compact&cb=v7l0sv7mkvwv appears to include (n) [html] tag [lang] attribute The user input found was: hl=en The user-controlled value was: en |
| URL | https://www.google.com/recaptcha/api2/bframe?hl=en&v=rz4DvU-cY2JYCwHSTck0_qm-&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj |
| Method | GET |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.google.com/recaptcha/api2/bframe?hl=encY2JYCwHSTck0_qm-&k=6Lf4mSYUAAAAAEaBoohSdOcvtcUgJg3Dad0R-0aj appears to inclu(n) [html] tag [lang] attribute The user input found was: hl=en The user-controlled value was: en |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include utag [class] attribute The user input found was: requestedData[categories][0][icon_name]=icon-CThe user-controlled value was: icon-cloud_computing |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u[a] tag [href] attribute The user input found was: requestedData[categories][0][slug]=https://wwwcomputing-certification-courses The user-controlled value was: https://www.edureka.co/cloud-ccertification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS |

| | |
|---|---|
| Other Info | possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][10][icon_name]=icon- The user-controlled value was: icon-software_testing |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][10][slug]=https://ww /software-testing-certification-courses The user-controlled value was: https://www.edureka.co/s certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][11][icon_name]=icon- controlled value was: icon-frontend |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][11][slug]=https://ww /frontend-development-certification-courses The user-controlled value was: https://www.edureka development-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][12][icon_name]=icon- controlled value was: icon-database |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][12][slug]=https://ww /databases-certification-courses The user-controlled value was: https://www.edureka.co/databa courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| | |

| | |
|---|---|
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][13][icon_name]=icon- controlled value was: icon-robotics |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][13][slug]=https://ww /robotic-process-automation-certification-courses The user-controlled value was: https://www.ed process-automation-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][14][icon_name]=icon- n-ETL The user-controlled value was: icon-data-warehousing-n-etl |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][14][slug]=https://ww warehousing-and-etl-certification-courses The user-controlled value was: https://www.edureka.c warehousing-and-etl-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][15][icon_name]=icon- user-controlled value was: icon-mobile_appd |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][15][slug]=https://ww /mobile-development-certification-courses The user-controlled value was: https://www.edureka.c development-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |

| | |
|---|---|
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][16][icon_name]=icon- The user-controlled value was: icon-operating-system |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][16][slug]=https://ww /operating-systems-certification-courses The user-controlled value was: https://www.edureka.co systems-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][17][icon_name]=icon- Design-Patterns The user-controlled value was: icon-architecture-n-design-patterns |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][17][slug]=https://ww /architecture-and-design-patterns-certification-courses The user-controlled value was: https://ww /architecture-and-design-patterns-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][18][icon_name]=icon- user-controlled value was: icon-blockchain |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][18][slug]=https://ww /blockchain-certification-courses The user-controlled value was: https://www.edureka.co/blockch courses |
| URL | https://www.edureka.co/elements |

| | |
|---|---|
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][19][icon_name]=icon- The user-controlled value was: icon-digital-marketing |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][19][slug]=https://ww /digital-marketing-certification-courses The user-controlled value was: https://www.edureka.co/d certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][1][icon_name]=icon-D controlled value was: icon-devops |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][1][slug]=https://ww /devops-certification-courses The user-controlled value was: https://www.edureka.co/devops-ce |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][2][icon_name]=icon- Cyber_Security_Category The user-controlled value was: icon-cyber_security_category |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][2][slug]=https://ww security-certification-courses The user-controlled value was: https://www.edureka.co/cyber-secu courses |

| | |
|---|---|
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][3][icon_name]=icon-B The user-controlled value was: icon-bi-n-visualization |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][3][slug]=https://www visualization-certification-courses The user-controlled value was: https://www.edureka.co/bi-and certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][4][icon_name]=icon-Programming_WebD The user-controlled value was: icon-programming_webd |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][4][slug]=https://www /programming-and-frameworks-certification-courses The user-controlled value was: https://www /programming-and-frameworks-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][5][icon_name]=icon-D user-controlled value was: icon-data-science |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][5][slug]=https://www |

| | |
|---|---|
| Info | science-certification-courses The user-controlled value was: https://www.edureka.co/data-scien courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][6][icon_name]=icon-Project_Management The user-controlled value was: icon-project_management |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][6][slug]=https://www /project-management-and-methodologies-certification-courses The user-controlled value was: h edureka.co/project-management-and-methodologies-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][7][icon_name]=icon-pg user-controlled value was: icon-pgp-category |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][7][slug]=https://www /executive-programs The user-controlled value was: https://www.edureka.co/executive-program |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][8][icon_name]=icon-A controlled value was: icon-ai |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u |

| | |
|---|---|
| Other Info | [a] tag [href] attribute The user input found was: requestedData[categories][8][slug]=https://www /artificial-intelligence-certification-courses The user-controlled value was: https://www.edureka.c intelligence-certification-courses |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u tag [class] attribute The user input found was: requestedData[categories][9][icon_name]=icon-B The user-controlled value was: icon-bigdata_analytics |
| URL | https://www.edureka.co/elements |
| Method | POST |
| Attack | |
| Evidence | |
| Other Info | User-controlled HTML attribute values were found. Try injecting special characters to see if XSS possible. The page at the following URL: https://www.edureka.co/elements appears to include u [a] tag [href] attribute The user input found was: requestedData[categories][9][slug]=https://www data-and-analytics The user-controlled value was: https://www.edureka.co/big-data-and-analytic |
| Instances | 43 |
| Solution | Validate all input and sanitize output it before writing to any HTML attributes. |
| Reference | http://websecuritytool.codeplex.com/wikipage?title=Checks#user-controlled-html-attribute |
| CWE Id | 20 |
| WASC Id | 20 |
| Plugin Id | 10031 |