
# Daksh SCRA – Source Code Analysis Report

Dec 20, 2024

# Scan Summary

This section provides a summary of the selected inputs and essential metrics collected during the scanning process. It offers an overview of the key information, allowing users to grasp the important aspects of the scan at a glance. For more detailed information about the identified areas of interest, please refer to the respective sections.

```
[+] Inputs Selected:
    [-] Target Directory: sample/sample_programs/vulnerable_js_app/
    [-] Rule Selected: javascript
    [-] Total Rules Loaded: 43
        [-] Platform Specific Rules: javascript[19]
        [-] Common Rules: 24
    [-] File Types Selected: javascript
[+] Detection Summary:
    [-] Total Project Files Identified: 935
    [-] Total Files Identified (Based on Selected Rule): 493
    [-] Total Files Scanned (Based on Selected Rule): 493
    [-] File Extensions Identified (Based on Selected Rule):
        javascript: [.js, .ts]
    [-] Code Files - Areas-of-Interests (Rules Matched): 20
    [-] File Paths - Areas-of-Interests (Rules Matched): 5

[+] Scanning Timeline:
    [-] Scan start time: 2024-12-20 12:11:41
    [-] Scan end time: 2024-12-20 12:11:50
    [-] Scan completed in: 00Hr:00Min:09s:291ms
```

# Security - Areas of Interest

This section lists the key areas within the source code that need to be examined for identifying potential security weaknesses.

The code reviewer should carefully examine the identified areas and review any reported code snippets and file paths to validate the presence of any potential vulnerabilities. The validation process should involve a thorough analysis of the code and its associated components to determine the extent of the potential security risk. Any issues identified during the validation process should be documented.

## JAVASCRIPT FINDINGS

### ID: JAVASCRIPT-1 : Untrusted Data in InnerHTML

**Rule Description** : Detects potential security risks when assigning untrusted data to the innerHTML property.

**Issue Description** : This rule matches instances where potentially untrusted data is assigned to the innerHTML property. Assigning untrusted data directly to innerHTML can lead to cross-site scripting (XSS) vulnerabilities if proper input validation and output encoding are not performed.

**Developer Note** : Developers should avoid assigning untrusted data directly to the innerHTML property. They should implement proper input validation and output encoding techniques when updating the content of elements via innerHTML to prevent XSS vulnerabilities.

**Reviewer Note** : Reviewers should verify if potentially untrusted data is assigned to the innerHTML property. They should assess if the code implements proper input validation and output encoding techniques to prevent XSS vulnerabilities when updating element content.

---

- Source File : vulnerable_js_app/node_modules/object-inspect/test/browser/dom.js

```
1 [9]     d.innerHTML = '<b>wooo</b><i>iiiii</i>';
```

- Source File : vulnerable_js_app/node_modules/object-inspect/example/inspect.js

```
1 [8] d.innerHTML = '<b>wooo</b><i>iiiii</i>';
```

### ID: JAVASCRIPT-2 : Untrusted Data in 'document.write'

**Rule Description** : Detects potential DOM-based cross-site scripting (XSS) vulnerabilities.

**Issue Description** : This rule matches instances where the `document.write()` function or the assignment of potentially untrusted values to the `innerHTML` property is performed. These actions can introduce DOM-based cross-site scripting vulnerabilities if proper input validation and output encoding are not applied.

**Developer Note** : Developers should avoid using `document.write()` and should implement appropriate input validation and output encoding techniques when assigning values to the `innerHTML` property. They should ensure that user-supplied data is properly sanitized and encoded to prevent XSS attacks.

**Reviewer Note** : Reviewers should verify if the code uses `document.write()` or assigns potentially untrusted values to the `innerHTML` property. They should assess if proper input validation and output encoding techniques are implemented to prevent DOM-based cross-site scripting vulnerabilities.

---

- Source File : vulnerable_js_app/node_modules/object-inspect/test/browser/dom.js

```
1 [9]     d.innerHTML = '<b>wooo</b><i>iiiii</i>';
```

- Source File : vulnerable_js_app/node_modules/object-inspect/example/inspect.js

```
1 [8] d.innerHTML = '<b>wooo</b><i>iiiii</i>';
```

### ID: JAVASCRIPT-3 : Insecure Method Call: eval|setTimeout|setInterval

**Rule Description** : Detects the usage of the `eval`, `setTimeout`, and `setInterval` functions.

**Issue Description** : This rule matches instances where the `eval`, `setTimeout`, or `setInterval` functions are used. These functions can introduce security vulnerabilities if not used carefully, as they can execute arbitrary code and lead to code injection or unintended consequences.

**Developer Note** : Developers should avoid using the `eval`, `setTimeout`, and `setInterval` functions whenever possible. If their usage is necessary, developers should carefully validate and sanitize any input used within these functions to prevent code injection vulnerabilities.

**Reviewer Note** : Reviewers should verify whether the code uses the `eval`, `setTimeout`, or `setInterval` functions. They should assess if the usage is justified and if proper input validation and sanitization techniques are implemented to prevent code injection vulnerabilities.

---

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/multipartUploads.spec.js

```
[466]          setTimeout(() => {
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/uploadtimer.js

```
[20]     this.timer = setTimeout(() => {
```

- Source File : vulnerable_js_app/node_modules/busboy/test/test-types-multipart-stream-pause.js

```
[85]   setTimeout(() => {
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/rule.js

```
[184]       setTimeout(function () {
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/file_task.js

```
[76]     setTimeout(() => {
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/concurrent.jake.js

```
[6]       setTimeout(() => {
[16]       setTimeout(() => {
[26]       setTimeout(() => {
[36]       setTimeout(() => {
[46]       setTimeout(() => {
[56]       setTimeout(() => {
[65]       setTimeout(() => {
[73]       setTimeout(() => {
[81]       setTimeout(() => {
[89]       setTimeout(() => {
[97]       setTimeout(() => {
[105]       setTimeout(() => {
```

- Source File : vulnerable_js_app/node_modules/jake/lib/api.js

```
[49]       setTimeout(complete, 1000);
```

- Source File : vulnerable_js_app/node_modules/jake/lib/publish_task.js

```
[235]            setTimeout(function () {
```

- Source File : vulnerable_js_app/node_modules/jake/lib/task/task.js

```
[301]            setTimeout(this.run.bind(this), POLLING_INTERVAL);
[380]        setTimeout(() => {
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/index.js

```
[269]          setTimeout(function () { _run.call(self); }, 0);
```

- Source File : vulnerable_js_app/node_modules/ejs/ejs.js

```
[1556]         return setTimeout(fun, 0);
[1561]         return setTimeout(fun, 0);
```

- Source File : vulnerable_js_app/node_modules/async/log.js

```
[31]  *     setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/series.js

```
[57]  *         setTimeout(function() {
[63]  *         setTimeout(function() {
[76]  *         setTimeout(function() {
[82]  *         setTimeout(function() {
[95]  *         setTimeout(function() {
[100]  *         setTimeout(function() {
[114]  *         setTimeout(function() {
[120]  *         setTimeout(function() {
[137]  *                 setTimeout(function() {
[143]  *                 setTimeout(function() {
[162]  *                 setTimeout(function() {
[168]  *                 setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/compose.js

```
[36]  *     setTimeout(function () {
[42]  *     setTimeout(function () {
```

- Source File : vulnerable_js_app/node_modules/async/reflectAll.js

```
[31]  *         setTimeout(function() {
[40]  *         setTimeout(function() {
[58]  *         setTimeout(function() {
[66]  *         setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/race.js

```
[42]  *         setTimeout(function() {
[47]  *         setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/timeout.js

```
[85]         timer = setTimeout(timeoutCallback, milliseconds);
```

- Source File : vulnerable_js_app/node_modules/async/retry.js

```
[135]                 setTimeout(retryAttempt, options.intervalFunc(attempt - 1));
```

- Source File : vulnerable_js_app/node_modules/async/nextTick.js

```
[12]  * available, otherwise `setTimeout(callback, 0)`, which means other higher
```

- Source File : vulnerable_js_app/node_modules/async/setImmediate.js

```
[16]  * available, otherwise `setTimeout(callback, 0)`, which means other higher
```

- Source File : vulnerable_js_app/node_modules/async/during.js

```
[46]  *         setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/dir.js

```
[33]  *     setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/whilst.js

```
[46]  *         setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/parallel.js

```
[58]  *         setTimeout(function() {
[63]  *         setTimeout(function() {
[76]  *         setTimeout(function() {
[81]  *         setTimeout(function() {
```

```
[93]  *         setTimeout(function() {
[98]  *         setTimeout(function() {
[113]  *         setTimeout(function() {
[118]  *         setTimeout(function() {
[134]  *                 setTimeout(function() {
[139]  *                 setTimeout(function() {
[158]  *                 setTimeout(function() {
[163]  *                 setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/dist/async.js

```
[70]         setTimeout(fn, 0);
[2051]      *     setTimeout(function () {
[2057]      *     setTimeout(function () {
[2500]      *     setTimeout(function() {
[3345]      *     setTimeout(function() {
[3631]      * available, otherwise `setTimeout(callback, 0)`, which means other higher
[3725]      *         setTimeout(function() {
[3730]      *         setTimeout(function() {
[3743]      *         setTimeout(function() {
[3748]      *         setTimeout(function() {
[3760]      *         setTimeout(function() {
[3765]      *         setTimeout(function() {
[3780]      *         setTimeout(function() {
[3785]      *         setTimeout(function() {
[3801]      *                 setTimeout(function() {
[3806]      *                 setTimeout(function() {
[3825]      *                 setTimeout(function() {
[3830]      *                 setTimeout(function() {
[4223]      *         setTimeout(function() {
[4228]      *         setTimeout(function() {
[4355]      *         setTimeout(function() {
[4364]      *         setTimeout(function() {
[4382]      *         setTimeout(function() {
[4390]      *         setTimeout(function() {
[4663]                  setTimeout(retryAttempt, options.intervalFunc(attempt - 1));
[4784]      *         setTimeout(function() {
[4790]      *         setTimeout(function() {
[4803]      *         setTimeout(function() {
[4809]      *         setTimeout(function() {
[4822]      *         setTimeout(function() {
[4827]      *         setTimeout(function() {
[4841]      *         setTimeout(function() {
[4847]      *         setTimeout(function() {
[4864]      *                 setTimeout(function() {
[4870]      *                 setTimeout(function() {
[4889]      *                 setTimeout(function() {
[4895]      *                 setTimeout(function() {
[5305]            timer = setTimeout(timeoutCallback, milliseconds);
[5648]      *         setTimeout(function() {
```

- Source File : vulnerable_js_app/node_modules/async/internal/setImmediate.js

```
[15]     setTimeout(fn, 0);
```

## ID: JAVASCRIPT-4 : Weak Random Number Generation

**Rule Description** : Detects the usage of weak random number generation.

**Issue Description** : This rule matches instances where weak random number generation functions, such as `Math.random()` or `crypto.getRandomValues()`, are used. Weak random number generation can lead to predictable values, compromising the security of cryptographic operations or session tokens.

**Developer Note** : Developers should use strong and cryptographically secure random number generation functions, such as `crypto.getRandomValues()`, for any security-critical operations. They should avoid using `Math.random()` for generating random values that require high entropy.

**Reviewer Note** : Reviewers should verify if weak random number generation functions, such as `Math.random()`, are used. They should assess if the code relies on secure random number generation functions for cryptographic operations or generating unpredictable values.

---

- Source File : vulnerable_js_app/node_modules/brace-expansion/index.js

```
[6] var escSlash = '\0SLASH'+Math.random()+'\0';
[7] var escOpen = '\0OPEN'+Math.random()+'\0';
[8] var escClose = '\0CLOSE'+Math.random()+'\0';
[9] var escComma = '\0COMMA'+Math.random()+'\0';
[10] var escPeriod = '\0PERIOD'+Math.random()+'\0';
```

- Source File : vulnerable_js_app/node_modules/safer-buffer/tests.js

```
[277]       var length = Math.round(Math.random() * 1e5)
[292]     var length = Math.round(Math.random() * 2e6)
[313]       var length = Math.round(Math.random() * 2e6)
[337]     var length = Math.round(Math.random() * 2e6)
[338]     var fill = Math.round(Math.random() * 255)
[355]     var length = Math.round(Math.random() * 2e6)
[356]     var fill = Math.round(Math.random() * 255)
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/brace-expansion/index.js

```
[5] var escSlash = '\0SLASH'+Math.random()+'\0';
[6] var escOpen = '\0OPEN'+Math.random()+'\0';
[7] var escClose = '\0CLOSE'+Math.random()+'\0';
[8] var escComma = '\0COMMA'+Math.random()+'\0';
[9] var escPeriod = '\0PERIOD'+Math.random()+'\0';
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/index.js

```
[151]         uuid[i] = chars[0 | Math.random()*radix];
[165]           r = 0 | Math.random()*16;
```

## ID: JAVASCRIPT-5 : Weak Mitigation: Using disable|bypass|ignore|suppress|unsafe

---

**Rule Description** : Detects weak or inadequate security mitigations.

**Issue Description** : This rule matches instances where weak or inadequate security mitigations (such as disable, bypass, ignore, suppress, or unsafe) are used. Weak mitigations can lead to security vulnerabilities or provide a false sense of security, leaving the application exposed to attacks.

**Developer Note** : Developers should avoid using weak or inadequate security mitigations as they can create vulnerabilities in the application. They should implement strong and effective security measures that follow established best practices and standards.

**Reviewer Note** : Reviewers should identify weak or inadequate security mitigations in the code and recommend implementing stronger security measures. They should assess if the application applies appropriate security controls and avoids relying on weak mitigations that may be easily bypassed by attackers.

---

- Source File : vulnerable_js_app/node_modules/send/index.js

```
[119]     : 'ignore'
[121]   if (this._dotfiles !== 'ignore' && this._dotfiles !== 'allow' && this._dotfiles !==
'deny') {
[122]     throw new TypeError('dotfiles option must be "allow", "deny", or "ignore"')
[128]     deprecate('hidden: use dotfiles: \'' + (this._hidden ? 'allow' : 'ignore') + '\'
instead')
[176]  * Enable or disable etag generation.
[190]  * Enable or disable "hidden" (dot) files.
[206]  * value to disable index support.
[566]         ? (this._hidden ? 'allow' : 'ignore')
[577]       case 'ignore':
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/get.js

```
[8]        // eslint-disable-next-line no-extra-parens, no-proto
[16] // eslint-disable-next-line no-extra-parens
[27]                        // eslint-disable-next-line eqeqeq
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/set.js

```
[10]        obj.__proto__ = null; // eslint-disable-line no-proto
[19] // eslint-disable-next-line no-extra-parens
[24] // eslint-disable-next-line no-extra-parens
[28]                if (object == null) { // eslint-disable-line eqeqeq
[31]                // eslint-disable-next-line no-proto, no-param-reassign, no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/test/get.js

```
[9]                throw 'should never happen; this is just for type narrowing'; // eslint-
disable-line no-throw-literal
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/test/set.js

```
[9]                throw 'should never happen; this is just for type narrowing'; // eslint-
disable-line no-throw-literal
[41]                        function () { ({}).__proto__ = null; }, // eslint-disable-line no-
proto
```

- Source File : vulnerable_js_app/node_modules/side-channel-list/index.js

```
[14] // eslint-disable-next-line consistent-return
[20]        // eslint-disable-next-line eqeqeq
[25]                                // eslint-disable-next-line no-extra-parens
[27]                                list.next = curr; // eslint-disable-line no-param-reassign
[49]                objects.next = /** @type {import('./list.d.ts').ListNode<typeof value, typeof
key>} */ ({ // eslint-disable-line no-param-reassign, no-extra-parens
[64] // eslint-disable-next-line consistent-return
[107]                        // eslint-disable-next-line no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/get-intrinsic/index.js

```
[23] // eslint-disable-next-line consistent-return
[39]                        // eslint-disable-next-line no-unused-expressions, no-caller, no-
restricted-properties
[90]        '%eval%': eval, // eslint-disable-line no-eval
[149]                null.error; // eslint-disable-line no-unused-expressions
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/server.js

```
[33]     console.error(err); // eslint-disable-line
[67]         console.log('ERR', err); // eslint-disable-line
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/options.spec.js

```
[170]     it('Will ignore any decimal amount when evaluating for extension length.',
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/index.js

```
[7] const busboy = require('busboy'); // eslint-disable-line no-unused-vars
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/example/server.js

```
[24]   console.log('req.files >>>', req.files); // eslint-disable-line
[40]   console.log('Express server listening on port ', PORT); // eslint-disable-line
```

- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/test/index.js

```
[24]                // eslint-disable-next-line no-invalid-this
```

- Source File : vulnerable_js_app/node_modules/content-disposition/index.js

```
[30] var ENCODE_URL_ATTR_CHAR_REGEXP = /[\x00-\x20"'()*,/:;<=>?@[\\\]{}\x7f]/g // eslint-disable-
line no-control-regex
[55] var QESC_REGEXP = /\\([\u0000-\u007f])/g // eslint-disable-line no-control-regex
```

```
2
3 [89] var PARAM_REGEXP = /;[ x09 x20]*([!#$%&'*+.0-9A-Z^_`a-z|~-]+)[\x09\x20]*=[\x09\x20]*("(?:
  [\x20!\x23-\x5b\x5d-\x7e\x80-\xff]|\\[\x20-\x7e])*"|[!#$%&'*+.0-9A-Z^_`a-z|~-]+)[\x09\x20]*/g //
  eslint-disable-line no-control-regex
4 [131] var DISPOSITION_TYPE_REGEXP = /^([!#$%&'*+.0-9A-Z^_`a-z|~-]+)[\x09\x20]*(?:$|;)/ // eslint-
  disable-line no-control-regex
```

- Source File : vulnerable_js_app/node_modules/express/lib/application.js

```
1 [481] app.disable = function disable(setting) {
2 [646]   /* istanbul ignore next */
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
1 [1171]         /* istanbul ignore next: unreachable default */
```

- Source File : vulnerable_js_app/node_modules/fresh/index.js

```
1 [97]   // istanbul ignore next: guard against date.js Date.parse patching
```

- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxSafeInteger.js

```
1 [4] // eslint-disable-next-line no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxValue.js

```
1 [4] // eslint-disable-next-line no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/side-channel-map/index.js

```
1 [46]               get: function (key) { // eslint-disable-line consistent-return
```

- Source File : vulnerable_js_app/node_modules/safer-buffer/dangerous.js

```
1 [1] /* eslint-disable node/no-deprecated-api */
2 [27] // Copy those missing unsafe methods, if they are present
```

- Source File : vulnerable_js_app/node_modules/safer-buffer/tests.js

```
1 [1] /* eslint-disable node/no-deprecated-api */
```

- Source File : vulnerable_js_app/node_modules/safer-buffer/safer.js

```
1 [1] /* eslint-disable node/no-deprecated-api */
```

- Source File : vulnerable_js_app/node_modules/busboy/test/common.js

```
1 [86]   // eslint-disable-next-line no-unused-expressions
```

- Source File : vulnerable_js_app/node_modules/busboy/lib/utils.js

```
1 [569] /* eslint-disable no-multi-spaces */
```

- Source File : vulnerable_js_app/node_modules/busboy/lib/types/urlencoded.js

```
1 [329] /* eslint-disable no-multi-spaces */
```

- Source File : vulnerable_js_app/node_modules/safe-buffer/index.js

```
1 [2] /* eslint-disable node/no-deprecated-api */
```

- Source File : vulnerable_js_app/node_modules/filelist/index.js

```
1 [217] // Default file-patterns we want to ignore
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/minimatch.js

```
1 [279]       /* istanbul ignore if */
2 [353]         /* istanbul ignore if */
3 [398]     } else /* istanbul ignore else */ if (pi === pl) {
4 [407]     /* istanbul ignore next */
```

```
[488]         /* istanbul ignore next - completely not allowed, even escaped. */
[502]         /* istanbul ignore next */
[704]         /* istanbul ignore else - should already be done */
[802]     } catch (er) /* istanbul ignore next - should be impossible */ {
[879]     } catch (ex) /* istanbul ignore next - should be impossible */ {
```

- Source File : vulnerable_js_app/node_modules/qs/test/parse.js

```
[960]     t.test('should ignore an utf8 sentinel with an unknown value', function (st) {
```

- Source File : vulnerable_js_app/node_modules/qs/test/stringify.js

```
[854]     t.test('can disable uri encoding', function (st) {
```

- Source File : vulnerable_js_app/node_modules/qs/test/utils.js

```
[48]             observed[0] = observed[0]; // eslint-disable-line no-self-assign
```

- Source File : vulnerable_js_app/node_modules/qs/lib/parse.js

```
[259]         // eslint-disable-next-line no-implicit-coercion, no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/call-bound/index.js

```
[12]        // eslint-disable-next-line no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/content-type/index.js

```
[23] var PARAM_REGEXP = /; *([!#$%&'*+.^_`|~0-9A-Za-z-]+) *= *("(?:[\u000b\u0020\u0021\u0023-
\u005b\u005d-\u007e\u0080-\u00ff]|\\[\u000b\u0020-\u00ff])*"|[!#$%&'*+.^_`|~0-9A-Za-z-]+) */g //
eslint-disable-line no-control-regex
[24] var TEXT_REGEXP = /^[\u000b\u0020-\u007e\u0080-\u00ff]+$/ // eslint-disable-line no-control-
regex
[33] var QESC_REGEXP = /\\([\u000b\u0020-\u00ff])/g // eslint-disable-line no-control-regex
```

- Source File : vulnerable_js_app/node_modules/has-symbols/shams.js

```
[28]        for (var _ in obj) { return false; } // eslint-disable-line no-restricted-syntax, no-
unreachable-loop
[39]                // eslint-disable-next-line no-extra-parens
```

- Source File : vulnerable_js_app/node_modules/has-symbols/test/tests.js

```
[4] // eslint-disable-next-line consistent-return
[45]        // eslint-disable-next-line no-restricted-syntax, no-unused-vars
```

- Source File : vulnerable_js_app/node_modules/has-symbols/test/shams/get-own-property-symbols.js

```
[18]        /* eslint-disable global-require */
```

- Source File : vulnerable_js_app/node_modules/has-symbols/test/shams/core-js.js

```
[18]        /* eslint-disable global-require */
```

- Source File : vulnerable_js_app/node_modules/cookie/index.js

```
[72]  * cause the user agent to ignore the attribute.)
```

- Source File : vulnerable_js_app/node_modules/minimatch/minimatch.js

```
[363]       /* istanbul ignore next */
[649]   } catch (er) /* istanbul ignore next - should be impossible */ {
[707]   } catch (ex) /* istanbul ignore next - should be impossible */ {
[808]     /* istanbul ignore if */
[882]       /* istanbul ignore if */
[927]   } else /* istanbul ignore else */ if (pi === pl) {
[936]   /* istanbul ignore next */
```

- Source File : vulnerable_js_app/node_modules/function-bind/test/index.js

```
[1] // jscs:disable requireUseStrict
```

- Source File : vulnerable_js_app/node_modules/finalhandler/index.js

```
[30] /* istanbul ignore next */
[91]     // ignore 404 on in-flight response
```

- Source File : vulnerable_js_app/node_modules/object-inspect/index.js

```
[39]     [].__proto__ === Array.prototype // eslint-disable-line no-proto
[41]             return O.__proto__; // eslint-disable-line no-proto
[442]     // eslint-disable-next-line no-control-regex
[521]     for (var key in obj) { // eslint-disable-line no-restricted-syntax
[522]         if (!has(obj, key)) { continue; } // eslint-disable-line no-restricted-syntax, no-continue
[523]         if (isArr && String(Number(key)) === key && key < obj.length) { continue; } // eslint-disable-line no-restricted-syntax, no-continue
[526]             continue; // eslint-disable-line no-restricted-syntax, no-continue
```

- Source File : vulnerable_js_app/node_modules/object-inspect/test/fn.js

```
[57]     var anon = function () {}; // eslint-disable-line func-style
[66]     var anon2 = function () {}; // eslint-disable-line func-style
```

- Source File : vulnerable_js_app/node_modules/object-inspect/test/has.js

```
[9]     var arr = [1, , 3]; // eslint-disable-line no-sparse-arrays
```

- Source File : vulnerable_js_app/node_modules/object-inspect/test/bigint.js

```
[27]         /* eslint-disable no-new-func */
```

- Source File : vulnerable_js_app/node_modules/debug/karma.conf.js

```
[44]     // enable / disable colors in the output (reporters and logs)
[53]     // enable / disable watching file and executing tests whenever any file changes
```

- Source File : vulnerable_js_app/node_modules/debug/src/debug.js

```
[11] exports.disable = disable;
[148]     if (!split[i]) continue; // ignore empty strings
[164] function disable() {
```

- Source File : vulnerable_js_app/node_modules/debug/src/browser.js

```
[36]  * TODO: add a `localStorage` variable to explicitly enable/disable colors
```

- Source File : vulnerable_js_app/node_modules/chalk/source/index.js

```
[33]                // eslint-disable-next-line no-constructor-return
[146]                 // eslint-disable-next-line no-implicit-coercion
[224] const chalk = Chalk(); // eslint-disable-line new-cap
[226] chalk.stderr = Chalk({level: stderrColor ? stderrColor.level : 0}); // eslint-disable-line new-cap
```

- Source File : vulnerable_js_app/node_modules/chalk/source/templates.js

```
[104]       // eslint-disable-next-line max-params
```

- Source File : vulnerable_js_app/node_modules/destroy/index.js

```
[28]  * Destroy the given stream, and optionally suppress any future `error` events.
[31]  * @param {boolean} suppress
[35] function destroy (stream, suppress) {
[44]   if (isEventEmitter(stream) && suppress) {
[111]     // istanbul ignore if: node.js 0.8
[130]       // istanbul ignore next
[194] // istanbul ignore next: node.js 0.8
```

- Source File : vulnerable_js_app/node_modules/color-convert/conversions.js

```
[2] /* eslint-disable no-mixed-operators */
[381]        /* eslint-disable max-statements-per-line,no-multi-spaces */
[720]        /* eslint-disable max-statements-per-line */
```

- Source File : vulnerable_js_app/node_modules/on-finished/index.js

```
[31] /* istanbul ignore next */
[128]     // istanbul ignore next: node.js 0.8 patch
[187] // istanbul ignore next: node.js 0.8 patch
```

- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/json.js

```
[40] var FIRST_CHAR_REGEXP = /^[ x20 x09\x0a\x0d]*([^\x20\x09 x0a\x0d])/ // eslint-disable-line
no-control-regex
[169]     JSON.parse(partial); /* istanbul ignore next */ throw new SyntaxError('strict
violation')
```

- Source File : vulnerable_js_app/node_modules/jake/test/unit/parseargs.js

```
[62]   test('long preemptive opt and val with equal-sign, ignore further opts', function () {
[68]   test('long preemptive opt and val without equal-sign, ignore further opts', function () {
[74]   test('long preemptive opt and no val, ignore further opts', function () {
[85]   test('preemptive opt with no val, should be true and ignore further opts', function () {
```

- Source File : vulnerable_js_app/node_modules/ejs/ejs.js

```
[229]     // istanbul ignore if: should not happen at all
[475]         // items that are unsafe to be passed along with data, like `root`
[677]       // istanbul ignore else
[717]       } catch (e) {/* ignore */}
[949] /* istanbul ignore if */
[997]   // istanbul ignore if
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/ejs.js

```
[228]     // istanbul ignore if: should not happen at all
[474]         // items that are unsafe to be passed along with data, like `root`
[676]       // istanbul ignore else
[716]       } catch (e) {/* ignore */}
[948] /* istanbul ignore if */
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/utils.js

```
[42]   // istanbul ignore if
```

- Source File : vulnerable_js_app/node_modules/async/nextTick.js

```
[40] var _defer; /* istanbul ignore file */
```

- Source File : vulnerable_js_app/node_modules/async/dist/async.js

```
[63]     /* istanbul ignore file */
[2465]             /* istanbul ignore else */
[2467]                 /* istanbul ignore else */
[2469]                     /* istanbul ignore else */
[2473]                 } else if (console[name]) { /* istanbul ignore else */
[3626]     /* istanbul ignore file */
```

- Source File : vulnerable_js_app/node_modules/async/internal/consoleFunc.js

```
[16]         /* istanbul ignore else */
[18]             /* istanbul ignore else */
[20]                 /* istanbul ignore else */
[25]                 /* istanbul ignore else */
```

- Source File : vulnerable_js_app/node_modules/async/internal/setImmediate.js

```
[8] /* istanbul ignore file */
```

- Source File : vulnerable_js_app/node_modules/depd/index.js

```
[300]   // ignore useless type name
[424]   // eslint-disable-next-line no-new-func
```

- Source File : vulnerable_js_app/node_modules/inherits/inherits.js

```
[3]   /* istanbul ignore next */
[7]   /* istanbul ignore next */
```

- Source File : vulnerable_js_app/node_modules/side-channel-weakmap/index.js

```
[75]                                    // eslint-disable-next-line no-extra-parens
```

## ID: JAVASCRIPT-6 : Deprecated SQL Functions

**Rule Description** : Detects usage of deprecated or insecure SQL functions and dynamic SQL queries that may lead to security vulnerabilities in JavaScript applications.

**Issue Description** : If this rule matches, it indicates the usage of potentially insecure SQL functions or libraries that may be vulnerable to SQL injection or other security issues if used without proper configurations or parameterization.

**Developer Note** : Developers should avoid using deprecated SQL functions or dynamic query building, and instead use secure alternatives like prepared statements or parameterized queries available in Node.js libraries (`mysql`, `pg`, Sequelize).

**Reviewer Note** : Reviewers should check for deprecated SQL functions or dynamic SQL building with user input, ensuring secure alternatives are implemented and that input validation and query parameterization practices are followed in JavaScript applications.

---

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/index.js

```
[3] // Update this array if you add/rename/remove files in this directory.
```

- Source File : vulnerable_js_app/node_modules/escape-html/index.js

```
[28]  * @param  {string} string The string to escape for inserting into HTML
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/utilities.spec.js

```
[482]     const validInsertions = [
[490]     const invalidInsertions = [
[498]     validInsertions.forEach((insertion) => {
[499]       it(`Key ${insertion.key} should be valid for ${JSON.stringify(insertion.base)}`, ()
=> {
[500]         assert.equal(isSafeFromPollution(insertion.base, insertion.key), true);
[504]     invalidInsertions.forEach((insertion) => {
[505]       it(`Key ${insertion.key} should not be valid for ${JSON.stringify(insertion.base)}`,
() => {
[506]         assert.equal(isSafeFromPollution(insertion.base, insertion.key), false);
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/tempFileHandler.js

```
[39]       hash.update(data);
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/utilities.js

```
[98]  * Determines whether a key insertion into an object could result in a prototype pollution
[99]  * @param {Object} base - The object whose insertion we are checking
[100]  * @param {string} key - The key that will be inserted
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/memHandler.js

```
[26]       hash.update(data);
```

- Source File : vulnerable_js_app/node_modules/express/lib/application.js

```
[131]       throw new Error('\'app.router\' is deprecated!\nPlease see the 3.x to 4.x migration guide for details on how to update your app.');
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[827]       deprecate('res.clearCookie: Passing "options.maxAge" is deprecated. In v5.0.0 of Express, this option will be ignored, as res.clearCookie will automatically set cookies to expire immediately. Please update your code to omit this option.');
[830]       deprecate('res.clearCookie: Passing "options.expires" is deprecated. In v5.0.0 of Express, this option will be ignored, as res.clearCookie will automatically set cookies to expire immediately. Please update your code to omit this option.');
```

- Source File : vulnerable_js_app/node_modules/express/lib/request.js

```
[87]  * To do: update docs.
```

- Source File : vulnerable_js_app/node_modules/express/lib/router/index.js

```
[402]     // store updated value
```

- Source File : vulnerable_js_app/node_modules/filelist/index.js

```
[75]        // Update value of object to the one from otherObj
```

- Source File : vulnerable_js_app/node_modules/etag/index.js

```
[48]     .update(entity, 'utf8')
```

- Source File : vulnerable_js_app/node_modules/debug/src/browser.js

```
[95]   // figure out the correct index to insert the CSS into
```

- Source File : vulnerable_js_app/node_modules/cookie-signature/index.js

```
[21]     .update(val)
[50]   return crypto.createHash('sha1').update(str).digest('hex');
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakefile.js

```
[239]     fs.writeFileSync('foo/prereq.txt', 'UPDATED');
```

- Source File : vulnerable_js_app/node_modules/jake/lib/rule.js

```
[150]       // Insert the file task into Jake
```

- Source File : vulnerable_js_app/node_modules/jake/lib/publish_task.js

```
[127]       task('updateVersionFiles', function () {
[142]         // Update package.json or other files with the new version-info
[150]         // for this task can use it (e.g., to update other files before pushing
[155]       task('pushVersion', ['ensureClean', 'updateVersionFiles'], function () {
```

- Source File : vulnerable_js_app/node_modules/jake/lib/jake.js

```
[211]         // Task already exists and no action, just update prereqs, and return it.
```

- Source File : vulnerable_js_app/node_modules/jake/lib/task/directory_task.js

```
[22]       this.updateModTime();
```

- Source File : vulnerable_js_app/node_modules/jake/lib/task/file_task.js

```
[37]       this.updateModTime();
[63]         this.updateModTime();
[77]       // If any prereqs are newer, need to run the action to update
[106]   updateModTime() {
[113]       this.updateModTime();
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/file.js

```
[94]         // Otherwise, only update the mode if preserverMode is true.
```

- Source File : vulnerable_js_app/node_modules/async/applyEach.js

```
[42]  * const appliedFn = async.applyEach([enableSearch, updateSchema], 'bucket')
[46]  *     // results[1] is the results for `updateSchema`
[52]  *     async (bucket) => async.applyEach([enableSearch, updateSchema], bucket)(),
```

- Source File : vulnerable_js_app/node_modules/async/dist/async.js

```
[779]     * const appliedFn = async.applyEach([enableSearch, updateSchema], 'bucket')
[783]     *     // results[1] is the results for `updateSchema`
[789]     *     async (bucket) => async.applyEach([enableSearch, updateSchema], bucket)(),
[1393]        insertAfter(node, newNode) {
[1402]        insertBefore(node, newNode) {
[1412]            if (this.head) this.insertBefore(this.head, node);
[1417]            if (this.tail) this.insertAfter(this.tail, node);
[1501]        function _insert(data, insertAtFront, rejectOnError, callback) {
[1522]            if (insertAtFront) {
[1619]                    return data.map(datum => _insert(datum, false, false, callback))
[1621]                return _insert(data, false, false, callback);
[1626]                    return data.map(datum => _insert(datum, false, true, callback))
[1628]                return _insert(data, false, true, callback);
[1637]                    return data.map(datum => _insert(datum, true, false, callback))
[1639]                return _insert(data, true, false, callback);
[1644]                    return data.map(datum => _insert(datum, true, true, callback))
[1646]                return _insert(data, true, true, callback);
```

- Source File : vulnerable_js_app/node_modules/async/internal/DoublyLinkedList.js

```
[30]    insertAfter(node, newNode) {
[38]    insertBefore(node, newNode) {
[47]        if (this.head) this.insertBefore(this.head, node);else setInitial(this, node);
[51]        if (this.tail) this.insertAfter(this.tail, node);else setInitial(this, node);
```

- Source File : vulnerable_js_app/node_modules/async/internal/queue.js

```
[67]     function _insert(data, insertAtFront, rejectOnError, callback) {
[84]         if (insertAtFront) {
[180]                return data.map(datum => _insert(datum, false, false, callback));
[182]            return _insert(data, false, false, callback);
[187]                return data.map(datum => _insert(datum, false, true, callback));
[189]            return _insert(data, false, true, callback);
[198]                return data.map(datum => _insert(datum, true, false, callback));
[200]            return _insert(data, true, false, callback);
[205]                return data.map(datum => _insert(datum, true, true, callback));
[207]            return _insert(data, true, true, callback);
```

## ID: JAVASCRIPT-7 : Deprecated JS Function: escape|unescape|eval

**Rule Description** : Detects usage of deprecated JavaScript functions.

**Issue Description** : This rule matches instances where deprecated JavaScript functions (such as escape, unescape, or eval) are used. Deprecated functions may have security vulnerabilities or compatibility issues and should be replaced with modern, safer alternatives.

**Developer Note** : Developers should avoid using deprecated JavaScript functions as they may introduce security vulnerabilities. They should update their code to use modern alternatives and follow best practices to ensure the security and compatibility of their applications.

**Reviewer Note** : Reviewers should check for the usage of deprecated JavaScript functions and recommend replacing them with safer alternatives. They should assess if the codebase follows best practices and avoids deprecated functions that may pose security risks.

---

- Source File : vulnerable_js_app/node_modules/send/index.js

```
[20] var escapeHtml = require('escape-html')
```

- Source File : vulnerable_js_app/node_modules/send/node_modules/encodeurl/index.js

```
[18]  * and including invalid escape sequences.
```

- Source File : vulnerable_js_app/node_modules/brace-expansion/index.js

```
[74]   // this module is to match Bash's rules, we escape a leading {}
```

- Source File : vulnerable_js_app/node_modules/encodeurl/index.js

```
[18]  * and including invalid escape sequences.
```

- Source File : vulnerable_js_app/node_modules/serve-static/index.js

```
[17] var escapeHtml = require('escape-html')
```

- Source File : vulnerable_js_app/node_modules/get-intrinsic/index.js

```
[8] var $EvalError = require('es-errors/eval');
[90]        '%eval%': eval, // eslint-disable-line no-eval
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-data.js

```
[30]     //  * ISO2022-JP: Stateful encoding, with escape sequences to switch between ASCII,
```

- Source File : vulnerable_js_app/node_modules/escape-html/index.js

```
[2]  * escape-html
[28]  * @param  {string} string The string to escape for inserting into HTML
[41]   var escape;
[49]         escape = '&quot;';
[52]         escape = '&amp;';
[55]         escape = '&#39;';
[58]         escape = '&lt;';
[61]         escape = '&gt;';
[72]     html += escape;
```

- Source File : vulnerable_js_app/node_modules/content-disposition/index.js

```
[33]  * RegExp to match percent encoding escape.
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[20] var escapeHtml = require('escape-html');
[268]   var escape = app.get('json escape')
[271]   var body = stringify(val, replacer, spaces, escape)
[311]   var escape = app.get('json escape')
[314]   var body = stringify(val, replacer, spaces, escape)
[1145]  * ability to escape characters that can trigger HTML sniffing.
[1150]  * @param {boolean} escape
[1155] function stringify (value, replacer, spaces, escape) {
[1162]   if (escape && typeof json === 'string') {
```

- Source File : vulnerable_js_app/node_modules/es-errors/eval.js

```
[3] /** @type {import('./eval')} */
```

- Source File : vulnerable_js_app/node_modules/filelist/index.js

```
[36]     @param {String} string The string of chars to escape
[245]   // Switched to false after lazy-eval of files
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/brace-expansion/index.js

```
[73]   // this module is to match Bash's rules, we escape a leading {}
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/minimatch.js

```
[30] // don't need to escape / when using new RegExp()
[682]       // split where the last [ was, and escape it
[695]     // and escape any | chars that were passed through as-is for the regexp.
[696]     // Go through and escape them, taking care not to double-escape any
[706]           // the | isn't already escaped, so escape it.
[710]         // need to escape all those slashes *again*, without escaping the
[790]     // unescape anything in it, though, so that it'll be
```

- Source File : vulnerable_js_app/node_modules/qs/lib/utils.js

```
[114]         // unescape never throws, no try...catch needed:
[115]         return strWithoutPlus.replace(/%[0-9a-f]{2}/gi, unescape);
[144]         return escape(string).replace(/%u[0-9a-f]{4}/gi, function ($0) {
```

- Source File : vulnerable_js_app/node_modules/minimatch/minimatch.js

```
[21] // don't need to escape / when using new RegExp()
[532]     // split where the last [ was, and escape it
[545]   // and escape any | chars that were passed through as-is for the regexp.
[546]   // Go through and escape them, taking care not to double-escape any
[554]         // the | isn't already escaped, so escape it.
[558]       // need to escape all those slashes *again*, without escaping the
[640]   // unescape anything in it, though, so that it'll be
```

- Source File : vulnerable_js_app/node_modules/finalhandler/index.js

```
[16] var escapeHtml = require('escape-html')
```

- Source File : vulnerable_js_app/node_modules/debug/src/node.js

```
[103]  * Adds ANSI color escape codes if enabled.
```

- Source File : vulnerable_js_app/node_modules/chalk/source/templates.js

```
[20] function unescape(c) {
[45]                         results.push(matches[2].replace(ESCAPE_REGEX, (m, escape, character)
=> escape ? unescape(escape) : character));
[107]                         chunk.push(unescape(escapeCharacter));
```

- Source File : vulnerable_js_app/node_modules/jake/lib/jake.js

```
[284]           // modTime will be eval'd correctly
```

- Source File : vulnerable_js_app/node_modules/ejs/ejs.js

```
[520]   options.escapeFunction = opts.escape || opts.escapeFunction || utils.escapeXML;
[553]   EVAL: 'eval',
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/ejs.js

```
[519]   options.escapeFunction = opts.escape || opts.escapeFunction || utils.escapeXML;
[552]   EVAL: 'eval',
```

## ID: JAVASCRIPT-8 : Insecure Direct Object References (IDOR)

**Rule Description** : Detects potential Insecure Direct Object References (IDOR).

**Issue Description** : This rule matches potential Insecure Direct Object References (IDOR) vulnerabilities in the code. IDOR occurs when user-supplied input is used directly to access internal resources or sensitive objects without proper authorization or validation. Attackers can manipulate the input to access unauthorized resources, view sensitive data, or perform actions they are not allowed to.

**Developer Note** : Developers should implement proper authorization and access control mechanisms to prevent IDOR vulnerabilities. User input used to access resources should be validated, sanitized, and authorized based on the user's privileges. Additionally, developers should use indirect references or randomized identifiers to obfuscate direct object references.

**Reviewer Note** : Reviewers should verify whether the code implements proper authorization and access control mechanisms to prevent IDOR vulnerabilities. They should check if user input used to access resources is properly validated, sanitized, and authorized. Reviewers should assess the effectiveness of the implemented measures in mitigating IDOR risks.

---

- Source File : vulnerable_js_app/app.js

```
[18]   const message = req.query.message || 'Welcome to the Vulnerable Node App!';
[24]   const command = req.body.command;
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/server.js

```
[103]       if (!req.body[fields[i]] || !req.body[fields[i]].trim()) {
[110]     fields.forEach((field) => { fileData[field] = req.body[field]; });
[212]       if (!req.body[fields[i]] || !req.body[fields[i]].trim()) {
[218]       firstName: req.body.firstName,
[219]       lastName: req.body.lastName,
[220]       email: req.body.email
[229]     if (!req.body.name || !req.body.name.trim()) {
[233]     if (!req.body.hobbies || !req.body.hobbies.length == 2) {
[238]       name: req.body.name,
[239]       hobbies: req.body.hobbies
[248]     if (!req.body.name || !req.body.name.trim()) {
[252]     if (!req.body['hobbies[0]'] || !req.body['hobbies[0]'].trim()) {
[256]     if (!req.body['hobbies[1]'] || !req.body['hobbies[1]'].trim()) {
[261]       name: req.body.name,
[262]       'hobbies[0]': req.body['hobbies[0]'],
[263]       'hobbies[1]': req.body['hobbies[1]']
[272]     if (!req.body.testField) {
[276]     if (!Array.isArray(req.body.testField)) {
[280]     res.json(req.body.testField);
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/utilities.js

```
[113]  * Builds request fields (using to build req.body and req.files)
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/processMultipart.js

```
[55]     req.body = Object.create(null);
[58]   busboy.on('field', (field, val) => req.body = buildFields(req.body, field, val));
[167]      req.body = processNested(req.body);
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[315]   var callback = this.req.query[app.get('jsonp callback name')];
[404]  *       var uid = req.params.uid
[405]  *         , file = req.params.file;
[486]  *       var uid = req.params.uid
[487]  *         , file = req.params.file;
```

- Source File : vulnerable_js_app/node_modules/express/lib/request.js

```
[243]   deprecate('req.param(' + args + '): Use req.params, req.body, or req.query instead');
```

- Source File : vulnerable_js_app/node_modules/express/lib/router/index.js

```
[274]     req.params = self.mergeParams
[371]     paramVal = req.params[name];
[383]       req.params[name] = paramCalled.value;
[403]     paramCalled.value = req.params[key.name];
```

- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/json.js

```
[108]     req.body = req.body || {}
```

- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/urlencoded.js

```
[89]     req.body = req.body || {}
```

- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/text.js

```
[64]     req.body = req.body || {}
```

- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/raw.js

```
[62]     req.body = req.body || {}
```

## ID: JAVASCRIPT-9 : Prototype Pollution

**Rule Description** : Detects potential prototype pollution vulnerabilities.

**Issue Description** : This rule matches instances where the `__proto__` property or assignment to properties of `Object.prototype` (excluding `hasOwnProperty`) is performed. These actions can lead to prototype pollution vulnerabilities, allowing attackers to modify the behavior of objects and potentially compromise the application's security.

**Developer Note** : Developers should avoid using or modifying the `__proto__` property directly, and they should exercise caution when extending or modifying properties of `Object.prototype`. They should use safer alternatives, such as `Object.create()` or creating new objects with specific prototypes.

**Reviewer Note** : Reviewers should verify if the code directly uses or modifies the `__proto__` property or assigns values to properties of `Object.prototype` (excluding `hasOwnProperty`). They should assess if proper precautions are taken to prevent prototype pollution vulnerabilities.

---

- Source File : vulnerable_js_app/node_modules/dunder-proto/get.js

```
[9]        hasProtoAccessor = /** @type {{ __proto__?: typeof Array.prototype }} */ ([]).__proto__ === Array.prototype;
[17] var desc = !!hasProtoAccessor && gOPD && gOPD(Object.prototype, /** @type {keyof typeof Object.prototype} */ ('__proto__'));
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/set.js

```
[7] /** @type {{ __proto__?: object | null }} */
[10]        obj.__proto__ = null; // eslint-disable-line no-proto
[20] var desc = gOPD && gOPD(Object.prototype, /** @type {keyof typeof Object.prototype} */ ('__proto__'));
[27]                // this is node v0.10 or older, which doesn't have Object.setPrototypeOf and has undeniable __proto__
[29]                            throw new $TypeError('set Object.prototype.__proto__ called on null or undefined');
[32]                /** @type {{ __proto__?: object | null }} */ (object).__proto__ = proto;
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/test/get.js

```
[31]        t.notOk('__proto__' in Object.prototype, 'no __proto__ in Object.prototype');
```

- Source File : vulnerable_js_app/node_modules/dunder-proto/test/set.js

```
[38]        if ('__proto__' in Object.prototype) {
[41]                            function () { ({}).__proto__ = null; }, // eslint-disable-line no-proto
[43]                            'throws when setting Object.prototype.__proto__'
[46]                t.notOk('__proto__' in Object.prototype, 'no __proto__ in Object.prototype');
```

- Source File : vulnerable_js_app/node_modules/get-intrinsic/index.js

```
[68]        __proto__: null,
[183]        __proto__: null,
```

- Source File : vulnerable_js_app/node_modules/setprototypeof/index.js

```
[3] module.exports = Object.setPrototypeOf || ({ __proto__: [] } instanceof Array ? setProtoOf : mixinProperties)
[6]   obj.__proto__ = proto
```

- Source File : vulnerable_js_app/node_modules/setprototypeof/test/index.js

```
[15]     } else if ({ __proto__: [] } instanceof Array) {
[16]       assert.strictEqual(obj.__proto__, proto)
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/utilities.spec.js

```
[449]       { name: '__proto__', data: {} },
[485]       { base: { __proto__: { a: 1 } }, key: 'a' },
[487]       { base: { __proto__: [1] }, key: 0 }
[491]       { base: {}, key: '__proto__' },
[493]       { base: [1], key: '__proto__' },
[495]       { base: { __proto__: [1] }, key: 'length' }
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/processNested.spec.js

```
[50]     const pollutionOb1 = JSON.parse(`{"__proto__.POLLUTED1": "FOOBAR"}`);
```

- Source File : vulnerable_js_app/node_modules/filelist/index.js

```
[68]       if (key === '__proto__' || key === 'constructor') {
```

- Source File : vulnerable_js_app/node_modules/qs/dist/qs.js

```
[70] "use strict";var test={__proto__:null,foo:{}},$Object=Object;module.exports=function
hasProto(){return{__proto__:test}.foo===test.foo&&!(test instanceof $Object)};
```

- Source File : vulnerable_js_app/node_modules/qs/test/parse.js

```
[806]             { __proto__: null, a: { __proto__: null, b: 'c', toString: true } },
[814]         var payload =
'categories[__proto__]=login&categories[__proto__]&categories[length]=42';
[832]                 __proto__: null,
[834]                     __proto__: null,
[841]         var query =
qs.parse('categories[__proto__]=cats&categories[__proto__]=dogs&categories[some][json]=toInject',
{ allowPrototypes: true });
[849]             qs.parse('foo[__proto__][hidden]=value&foo[bar]=stuffs', { allowPrototypes:
true }),
[859]             qs.parse('foo[__proto__][hidden]=value&foo[bar]=stuffs', { allowPrototypes:
true, plainObjects: true }),
[861]                 __proto__: null,
[863]                     __proto__: null,
```

- Source File : vulnerable_js_app/node_modules/qs/lib/parse.js

```
[56]     var obj = { __proto__: null };
[149]             } else if (decodedRoot !== '__proto__') {
```

- Source File : vulnerable_js_app/node_modules/object-inspect/index.js

```
[39]     [].__proto__ === Array.prototype // eslint-disable-line no-proto
[41]             return O.__proto__; // eslint-disable-line no-proto
[73]     __proto__: null,
[78]     __proto__: null,
```

- Source File : vulnerable_js_app/node_modules/object-inspect/test/toStringTag.js

```
[17]     t.test('null objects', { skip: 'toString' in { __proto__: null } }, function (st) {
[20]         var dict = { __proto__: null, a: 1 };
```

- Source File : vulnerable_js_app/node_modules/ejs/ejs.js

```
[1095]       if (p === '__proto__' || p === 'constructor') {
[1126]         if (p === '__proto__' || p === 'constructor') {
[1185]   if (!({__proto__: null} instanceof Object)) {
[1187]       return {__proto__: null};
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/utils.js

```
[140]       if (p === '__proto__' || p === 'constructor') {
```

```
[171]         if (p === '__proto__' || p === 'constructor') {
[230]   if (!({__proto__: null} instanceof Object)) {
[232]       return {__proto__: null};
```

- Source File : vulnerable_js_app/node_modules/async/dist/async.js

```
[307]             if (key === '__proto__') {
```

- Source File : vulnerable_js_app/node_modules/async/internal/iterator.js

```
[42]         if (key === '__proto__') {
```

### ID: JAVASCRIPT-10 : Missing Cookie Security Flags

**Rule Description** : Detects the absence of important security flags in a cookie, such as 'httpOnly', 'secure', 'SameSite', and 'Domain' attributes.

**Issue Description** : If this rule matches, it indicates that one or more security flags are missing in a cookie. The absence of these flags can lead to security vulnerabilities, including cross-site scripting (XSS) attacks and information leakage.

**Developer Note** : Developers should ensure that cookies containing sensitive information have the necessary security flags set. This includes enabling the 'httpOnly' attribute, setting the 'secure' attribute for secure connections, and specifying appropriate values for the 'SameSite' and 'Domain' attributes. These measures help protect against various security risks, such as XSS attacks and cookie tampering.

**Reviewer Note** : Reviewers should verify whether the code correctly applies the necessary security flags to cookies. They should check for the presence of 'httpOnly', 'secure', 'SameSite', and 'Domain' attributes and confirm that they are set appropriately. Reviewers should assess the impact of missing security flags on the overall security posture of the application and provide recommendations for remediation.

---

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[850]  *    res.cookie('rememberme', '1', { expires: new Date(Date.now() + 900000), httpOnly:
true });
[853]  *    res.cookie('rememberme', '1', { maxAge: 900000, httpOnly: true })
```

- Source File : vulnerable_js_app/node_modules/express/lib/request.js

```
[335] defineGetter(req, 'secure', function secure(){
```

- Source File : vulnerable_js_app/node_modules/cookie/index.js

```
[174]  * serialize('foo', 'bar', { httpOnly: true })
[175]  *   => "foo=bar; httpOnly"
[219]     str += '; Domain=' + opt.domain;
[240]   if (opt.httpOnly) {
[277]         str += '; SameSite=Strict';
[280]         str += '; SameSite=Lax';
[283]         str += '; SameSite=Strict';
[286]         str += '; SameSite=None';
```

## COMMON FINDINGS

### ID: COMMON-1 : Authentication Modules

**Rule Description** : Detects common terms used in authentication functionalities, such as 'Login', 'authenticate', 'OAuth', and 'JWT', when used in likely function names or module references.

**Issue Description** : This rule matches on common function or module names associated with authentication. If not properly secured, these modules may expose vulnerabilities in user authentication, allowing unauthorized access.

**Developer Note** : Ensure authentication processes use secure configurations, apply best practices, and avoid using weak or generic names that could be predictable.

**Reviewer Note** : Verify that authentication mechanisms are implemented securely, with protections like parameterized inputs, encryption, and secure session management.

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[907]  *    res.location('../login');
[941]  *    res.redirect('../login'); // /blog/post/1 -> /blog/login
```

- Source File : vulnerable_js_app/node_modules/qs/test/parse.js

```
[814]         var payload =
'categories[__proto__]=login&categories[__proto__]&categories[length]=42';
```

## ID: COMMON-2 : File Upload Functionality

**Rule Description** : Detects likely implementations of file upload functionality by matching common terms associated with file upload services or modules.

**Issue Description** : If this rule matches, it indicates potential file upload functionality, which, if improperly secured, could allow unauthorized or malicious file uploads. This can lead to risks such as arbitrary code execution or data leakage.

**Developer Note** : Ensure file upload functionality is implemented securely with validation of file types, size limits, and access controls. Use established libraries or frameworks with built-in security features for file uploads to minimize risks.

**Reviewer Note** : Verify that secure file upload practices are followed, including file type validation, size restrictions, and appropriate access controls to prevent unauthorized file uploads.

- Source File : vulnerable_js_app/app.js

```
[3] const fileUpload = require('express-fileupload');
[13] app.use(fileUpload());
[34] // Insecure File Upload
[48]     res.send('File uploaded!');
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/multipartUploads.spec.js

```
[49] describe('multipartUploads: Test Single File Upload', function() {
[106] describe('multipartUploads: Test Single File Upload w/ .mv()', function() {
[134] describe('multipartUploads: Test Single File Upload w/ useTempFiles option.', function() {
[191] describe('multipartUploads: Single File Upload w/ useTempFiles & empty tempFileDir.',
function() {
[210] describe('multipartUploads: Test Single File Upload w/ .mv() Promise', function() {
[267] describe('multipartUploads: Test Single File Upload w/ .mv() Promise & useTempFiles',
function() {
[324] describe('multipartUploads: Test Multi-File Upload', function() {
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/server.js

```
[49] const setup = (fileUploadOptions) => {
[51]   const expressFileupload = require('../lib/index');
[55]   app.use(expressFileupload(fileUploadOptions || {}));
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/fileLimitUploads.spec.js

```
[10] describe('fileLimitUloads: Test Single File Upload With File Size Limit', function() {
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/tempFile.spec.js

```
[11] describe('tempFile: Test fileupload w/ useTempFiles.', function() {
[18]    * @param {object} options The expressFileUpload options.
[23]   function executeFileUploadTestWalk(
[61]       const fileUploadOptions = {
[68]       executeFileUploadTestWalk(
[69]         fileUploadOptions,
[76]       const fileUploadOptions = {
[82]       executeFileUploadTestWalk(
[83]         fileUploadOptions,
[93]         const fileUploadOptions = {
[100]         executeFileUploadTestWalk(
```

```
12 [101]           fileUploadOptions,
13 [111]         const fileUploadOptions = {
14 [118]         executeFileUploadTestWalk(
15 [119]           fileUploadOptions,
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/options.spec.js

```
1  [9] describe('options: File Upload Options Tests', function() {
2  [17]    * @param {object} options The expressFileUpload options.
3  [22]   function executeFileUploadTestWalk(options,
4  [44]         const fileUploadOptions = {safeFileNames: false};
5  [48]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
6  [53]         const fileUploadOptions = null;
7  [57]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
8  [62]         const fileUploadOptions = {safeFileNames: true};
9  [66]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
10 [71]         const fileUploadOptions = {safeFileNames: /[$#]/g};
11 [75]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
12 [82]         const fileUploadOptions = {safeFileNames: true, preserveExtension: false};
13 [86]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
14 [91]         const fileUploadOptions = {safeFileNames: true};
15 [95]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
16 [100]         const fileUploadOptions = {safeFileNames: true, preserveExtension: true};
17 [104]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
18 [109]         const fileUploadOptions = {safeFileNames: true, preserveExtension: true};
19 [113]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
20 [118]         const fileUploadOptions = {safeFileNames: true, preserveExtension: 7};
21 [122]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
22 [127]         const fileUploadOptions = {safeFileNames: true, preserveExtension: 2};
23 [131]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
24 [136]         const fileUploadOptions = {safeFileNames: true, preserveExtension: -5};
25 [140]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
26 [145]         const fileUploadOptions = {safeFileNames: true, preserveExtension: 0};
27 [149]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
28 [154]         const fileUploadOptions = {safeFileNames: true, preserveExtension: '3'};
29 [158]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
30 [163]         const fileUploadOptions = {safeFileNames: true, preserveExtension: 'not-a-#-but-
   truthy'};
31 [167]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
32 [172]         const fileUploadOptions = {safeFileNames: true, preserveExtension: 4.98};
33 [176]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
34 [181]         const fileUploadOptions = {safeFileNames: true, preserveExtension: true};
35 [185]         executeFileUploadTestWalk(fileUploadOptions, actualFileName, expectedFileName,
   done);
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/index.js

```
1 [28]  * Expose the file upload middleware
2 [30]  * @returns {Function} - express-fileupload middleware.
3 [36]       debugLog(uploadOptions, 'Request is not eligible for file upload!');
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/utilities.js

```
1 [143]  * @param {Object} fileUploadOptions
2 [147] const checkAndMakeDir = (fileUploadOptions, filePath) => {
```

```
3 [149]   if (!fileUploadOptions) return false;
4 [150]   if (!fileUploadOptions.createParentPath) return false;
5 [253]   // See Issue https://github.com/richardgirges/express-fileupload/issues/342.
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/processMultipart.js

```
1 [21]  * @param  {Object}   options expressFileupload and Busboy options
2 [92]       // https://github.com/richardgirges/express-fileupload/issues/259.
3 [120]       // Debug logging for file upload ending.
4 [124]       // See https://github.com/richardgirges/express-fileupload/issues/191
5 [158]     // Debug logging for a new file upload.
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/isEligibleRequest.js

```
1 [23]  * Ensures that only multipart requests are processed by express-fileupload
2 [36]  * Ensures that the request in question is eligible for file uploads
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/fileFactory.js

```
1  [17]  * @param {Object} fileUploadOptions - middleware options.
2  [20] const moveFromTemp = (filePath, options, fileUploadOptions) => (resolve, reject) => {
3  [21]   debugLog(fileUploadOptions, `Moving temporary file ${options.tempFilePath} to ${filePath}
   `);
4  [30]  * @param {Object} fileUploadOptions - middleware options.
5  [33] const moveFromBuffer = (filePath, options, fileUploadOptions) => (resolve, reject) => {
6  [34]   debugLog(fileUploadOptions, `Moving uploaded buffer to ${filePath}`);
7  [38] module.exports = (options, fileUploadOptions = {}) => {
8  [39]   // see: https://github.com/richardgirges/express-fileupload/issues/14
9  [42]   // if (!fileUploadOptions.useTempFiles && !options.buffer.length) return;
10 [56]       const moveFunc = fileUploadOptions.useTempFiles
11 [57]         ? moveFromTemp(filePath, options, fileUploadOptions)
12 [58]         : moveFromBuffer(filePath, options, fileUploadOptions);
13 [60]       checkAndMakeDir(fileUploadOptions, filePath);
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/example/server.js

```
1 [2] const fileUpload = require('../lib/index');
2 [9] app.use(fileUpload());
3 [35]     res.send('File uploaded to ' + uploadPath);
```

## ID: COMMON-3 : Password

**Rule Description** : Detects potential password-related strings in the code.

**Issue Description** : If this rule matches, it indicates the potential presence of password-related strings in the code, which can lead to security risks if not handled properly.

**Developer Note** : Developers should follow best practices for password handling, including strong encryption, salted hashing, and enforcing secure password policies.

**Reviewer Note** : Reviewers should assess the password handling mechanisms and verify if proper security measures are in place.

---

- Source File : vulnerable_js_app/node_modules/debug/src/node.js

```
1 [203]       // Test: ./node test/fixtures/echo.js < /etc/passwd
```

## ID: COMMON-4 : Server-side Secrets Handling

**Rule Description** : Detects potential server-side secrets handling vulnerabilities in the code.

**Issue Description** : If this rule matches, it indicates the potential presence of server-side secrets (e.g., hardcoded secrets, assignments) in the code, which can lead to security risks if not handled properly.

**Developer Note** : Developers should avoid storing secrets directly in the code and instead use secure methods such as environment variables or key management systems.

**Reviewer Note** : Reviewers should assess the handling of server-side secrets and verify if proper security measures are in place.

---

- Source File : vulnerable_js_app/node_modules/content-disposition/index.js

```
[68]  * token          = 1*<any CHAR except CTLs or separators>
[127]  * ext-token        = <the characters in token, followed by "*">
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[864]   var secret = this.req.secret;
```

- Source File : vulnerable_js_app/node_modules/vary/index.js

```
[20]  * token          = 1*tchar
```

- Source File : vulnerable_js_app/node_modules/content-type/index.js

```
[13]  * token          = 1*tchar
```

- Source File : vulnerable_js_app/node_modules/cookie/index.js

```
[31]  * token            = 1*tchar
```

- Source File : vulnerable_js_app/node_modules/media-typer/index.js

```
[11]  * token          = 1*<any CHAR except CTLs or separators>
```

## ID: COMMON-5 : Insecure HTTP Communication

---

**Rule Description** : Detects the use of insecure HTTP communication.

**Issue Description** : Using HTTP exposes the application to man-in-the-middle attacks, allowing attackers to intercept or manipulate traffic.

**Developer Note** : Use HTTPS for all network communication to ensure secure data transmission. Avoid using HTTP unless explicitly required and justified by the use case.

**Reviewer Note** : Review all URLs or network requests across source code, configuration files, and external API references to ensure HTTPS is used instead of HTTP.

---

- Source File : vulnerable_js_app/app.js

```
[53]   console.log('App running on http://localhost:3000');
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/utf7.js

```
[5] // See also below a UTF-7-IMAP codec, according to http://tools.ietf.org/html/rfc3501#section-5.1.3
[121] // RFC3501 Sec. 5.1.3 Modified UTF-7 (http://tools.ietf.org/html/rfc3501#section-5.1.3)
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/utf16.js

```
[70] // http://en.wikipedia.org/wiki/UTF-16 and http://encoding.spec.whatwg.org/#utf-16le
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-data.js

```
[39]     // Overall, it seems that it's a mess :( http://www8.plala.or.jp/tkubota1/unicode-symbols-map2.html
[70]     // http://en.wikipedia.org/wiki/GBK
[100]     // http://icu-project.org/docs/papers/gb18030.html
[101]     // http://source.icu-project.org/repos/icu/data/trunk/charset/data/xml/gb-18030-2000.xml
[102]     // http://www.khngai.com/chinese/charmap/tblgbk.php?page=0
[136]     // http://moztw.org/docs/big5/  http://www.haible.de/bruno/charsets/conversion-tables/Big5.html
[138]     //  * Windows CP 950: Microsoft variant of Big5. Canonical: http://www.unicode.org/Public/MAPPINGS/VENDORS/MICSFT/WINDOWS/CP950.TXT
[139]     //  * Windows CP 951: Microsoft variant of Big5-HKSCS-2001. Seems to be never public. http://me.abelcheung.org/articles/research/what-is-cp951/
[151]     //    Official spec: http://www.ogcio.gov.hk/en/business/tech_promotion/ccli/terms/doc/2003cmp_2008.txt
[152]     //                   http://www.ogcio.gov.hk/tc/business/tech_promotion/ccli/terms/doc/hkscs-2008-big5-
```

```
11 [154]     // Current understanding of how to deal with Big5(-HKSCS) is in the Encoding Standard, http://
   encoding.spec.whatwg.org/#big5-encoder
12 [155]     // Unicode mapping (http://www.unicode.org/Public/MAPPINGS/OBSOLETE/EASTASIA/OTHER/BIG5.TXT) is said to
   wrong.
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
1 [81]  *      next: 'http://api.example.com/users?page=2',
2 [82]  *      last: 'http://api.example.com/users?page=5'
3 [734]  *    res.append('Link', ['<http://localhost/>', '<http://localhost:3000/>']);
4 [906]  *    res.location('http://example.com');
5 [939]  *    res.redirect('http://example.com');
6 [940]  *    res.redirect(301, 'http://example.com');
```

- Source File : vulnerable_js_app/node_modules/type-is/index.js

```
1 [85]  * http://www.w3.org/Protocols/rfc2616/rfc2616-sec4.html#sec4.3
```

- Source File : vulnerable_js_app/node_modules/filelist/index.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/debug/src/browser.js

```
1 [47]   // is webkit? http://stackoverflow.com/a/16459606/376773
2 [50]     // is firebug? http://stackoverflow.com/a/398120/376773
```

- Source File : vulnerable_js_app/node_modules/color-convert/conversions.js

```
1 [354] // http://dev.w3.org/csswg/css-color/#hwb-to-rgb
```

- Source File : vulnerable_js_app/node_modules/color-convert/route.js

```
1 [21]                      // http://jsperf.com/1-vs-infinity
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/rule.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/file_task.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/file.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/publish.jake.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/rule.jake.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/unit/parseargs.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/unit/namespace.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/bin/cli.js

```
1 [10]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/parseargs.js

```
1 [9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/test_task.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/program.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/api.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/publish_task.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/package_task.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/jake.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/loader.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/index.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/file.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/ejs/ejs.js

```
[10]  *         http://www.apache.org/licenses/LICENSE-2.0
[23]  * @file Embedded JavaScript templating engine. {@link http://ejs.co}
[27]  * @license {@link http://www.apache.org/licenses/LICENSE-2.0 Apache License, Version 2.0}
[964]  *         http://www.apache.org/licenses/LICENSE-2.0
[1711]   "author": "Matthew Eernisse <mde@fleegix.org> (http://fleegix.org)",
```

- Source File : vulnerable_js_app/node_modules/ejs/bin/cli.js

```
[10]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/ejs.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
[22]  * @file Embedded JavaScript templating engine. {@link http://ejs.co}
[26]  * @license {@link http://www.apache.org/licenses/LICENSE-2.0 Apache License, Version 2.0}
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/utils.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/async/index.js

```
[357]  * use with [Node.js](http://nodejs.org) and installable via
```

- Source File : vulnerable_js_app/node_modules/async/series.js

```
[31]  * properties, the [ECMAScript Language Specification](http://www.ecma-international.org/
ecma-262/5.1/#sec-8.6)
```

- Source File : vulnerable_js_app/node_modules/async/ensureAsync.js

```
[21]  * [Zalgo](http://blog.izs.me/post/59142742143/designing-apis-for-asynchrony)
```

- Source File : vulnerable_js_app/node_modules/async/auto.js

```
[302]         // http://connalle.blogspot.com/2013/10/topological-sortingkahn-algorithm.html
```

- Source File : vulnerable_js_app/node_modules/async/dist/async.js

```
[1163]             // http://connalle.blogspot.com/2013/10/topological-sortingkahn-algorithm.html
[2756]      * [Zalgo](http://blog.izs.me/post/59142742143/designing-apis-for-asynchrony)
[4758]      * properties, the [ECMAScript Language Specification](http://www.ecma-international.org/ecma-262/5.1/#sec-8.6)
```

## ID: COMMON-6 : IPv4 / IPv6 Address

**Rule Description** : Detects potential IPv4 or IPv6 addresses in the code.

**Issue Description** : If this rule matches, it indicates the potential presence of IP addresses in the code, which can lead to security risks if not handled properly.

**Developer Note** : Developers should carefully validate and sanitize input related to IP addresses to prevent security vulnerabilities such as IP spoofing or injection attacks.

**Reviewer Note** : Reviewers should check for appropriate input handling and assess the implementation of input validation and sanitization techniques for IP addresses.

---

- Source File : vulnerable_js_app/node_modules/proxy-addr/index.js

```
[41]   linklocal: ['169.254.0.0/16', 'fe80::/10'],
[42]   loopback: ['127.0.0.1/8', '::1/128'],
[43]   uniquelocal: ['10.0.0.0/8', '172.16.0.0/12', '192.168.0.0/16', 'fc00::/7']
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/minimatch.js

```
[638]          //  first in the list.  -- POSIX.2 2.8.3.2
```

- Source File : vulnerable_js_app/node_modules/content-type/index.js

```
[10]  * RegExp to match *( ";" parameter ) in RFC 7231 sec 3.1.1.1
[41]  * RegExp to match type in RFC 7231 sec 3.1.1.1
```

- Source File : vulnerable_js_app/node_modules/minimatch/minimatch.js

```
[478]        //  first in the list.  -- POSIX.2 2.8.3.2
```

## ID: COMMON-7 : Trusted Or Untrusted URLs

**Rule Description** : Detects the presence of URLs in the application that may pose security risks or indicate potential trust issues with third-party URLs.

**Issue Description** : If this rule matches, it indicates the presence of URLs starting with http:// or https://, which could potentially pose security risks if not properly handled or validated. These URLs might involve data exfiltration or raise concerns about trusting third-party resources without thorough validation. Developers and reviewers should investigate these URLs to ensure their purpose, legitimacy, and adherence to security practices.

**Developer Note** : Developers should list and carefully review all URLs used in the application. They should implement proper URL validation and sanitization techniques to ensure the security and integrity of the application when dealing with user-provided or third-party URLs. It is important to prevent any unintentional exposure of sensitive information and perform thorough taint validation on third-party URLs to mitigate trust-related security risks.

**Reviewer Note** : Reviewers should verify the implementation of secure URL handling practices and assess if additional security measures are necessary. They should thoroughly investigate the presence of these URLs, determine their purpose, and ensure they undergo appropriate taint validation. Reviewers should pay special attention to URLs associated with data exfiltration concerns and assess the trustworthiness of third-party URLs to mitigate potential security risks.

---

- Source File : vulnerable_js_app/app.js

```
[53]   console.log('App running on http://localhost:3000');
```

- Source File : vulnerable_js_app/node_modules/streamsearch/lib/sbmh.js

```
1 [4]   by Hongli Lai at: https://github.com/FooBarWidget/boyer-moore-horspool
```

- Source File : vulnerable_js_app/node_modules/get-intrinsic/index.js

```
1 [151]               // https://github.com/tc39/proposal-shadowrealm/pull/
  384#issuecomment-1364264229
2 [245] /* adapted from https://github.com/lodash/lodash/blob/4.17.15/dist/lodash.js#L6735-L6744 */
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/utf7.js

```
1 [4] // UTF-7 codec, according to https://tools.ietf.org/html/rfc2152
2 [5] // See also below a UTF-7-IMAP codec, according to http://tools.ietf.org/html/
  rfc3501#section-5.1.3
3 [121] // RFC3501 Sec. 5.1.3 Modified UTF-7 (http://tools.ietf.org/html/rfc3501#section-5.1.3)
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/utf16.js

```
1 [70] // http://en.wikipedia.org/wiki/UTF-16 and http://encoding.spec.whatwg.org/#utf-16le
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-data.js

```
1  [39]     // Overall, it seems that it's a mess :( http://www8.plala.or.jp/tkubota1/unicode-symbols-map2.html
2  [70]     // http://en.wikipedia.org/wiki/GBK
3  [71]     // We mostly implement W3C recommendation: https://www.w3.org/TR/encoding/#gbk-encoder
4  [99]     // Main source: https://www.w3.org/TR/encoding/#gbk-encoder
5  [100]     // http://icu-project.org/docs/papers/gb18030.html
6  [101]     // http://source.icu-project.org/repos/icu/data/trunk/charset/data/xml/gb-18030-2000.xml
7  [102]     // http://www.khngai.com/chinese/charmap/tblgbk.php?page=0
8  [136]     // http://moztw.org/docs/big5/  http://www.haible.de/bruno/charsets/conversion-tables/Big5.html
9  [138]     //  * Windows CP 950: Microsoft variant of Big5. Canonical: http://www.unicode.org/Public/MAPPINGS/VENDORS/
   MICSFT/WINDOWS/CP950.TXT
10 [139]     //  * Windows CP 951: Microsoft variant of Big5-HKSCS-2001. Seems to be never public. http://
   me.abelcheung.org/articles/research/what-is-cp951/
11 [145]     //    Seems that Mozilla refused to support it for 10 yrs. https://bugzilla.mozilla.org/show_bug.cgi?id=
   https://bugzilla.mozilla.org/show_bug.cgi?id=310299
12 [149]     //    Great discussion & recap of what's going on https://bugzilla.mozilla.org/show_bug.cgi?id=912470#c
13 [151]     //    Official spec: http://www.ogcio.gov.hk/en/business/tech_promotion/ccli/terms/doc/2003cmp_2008.txt
14 [152]     //                   http://www.ogcio.gov.hk/tc/business/tech_promotion/ccli/terms/doc/hkscs-2008-big5-
15 [154]     // Current understanding of how to deal with Big5(-HKSCS) is in the Encoding Standard, http://
   encoding.spec.whatwg.org/#big5-encoder
16 [155]     // Unicode mapping (http://www.unicode.org/Public/MAPPINGS/OBSOLETE/EASTASIA/OTHER/BIG5.TXT) is said to be
   wrong.
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/index.js

```
1 [33]            console.error('Iconv-lite warning: decode()-ing strings is deprecated. Refer to
  https://github.com/ashtuchkin/iconv-lite/wiki/Use-Buffers-when-decoding');
2 [152]     console.error("iconv-lite warning: javascript files use encoding different from utf-8.
  See https://github.com/ashtuchkin/iconv-lite/wiki/Javascript-source-file-encodings for more
  info.");
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/extend-node.js

```
1 [21]            console.error("See more info at https://github.com/ashtuchkin/iconv-lite/wiki/
  Node-v4-compatibility");
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/utilities.js

```
1 [253]   // See Issue https://github.com/richardgirges/express-fileupload/issues/342.
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/processMultipart.js

```
1 [92]       // https://github.com/richardgirges/express-fileupload/issues/259.
2 [124]       // See https://github.com/richardgirges/express-fileupload/issues/191
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/fileFactory.js

```
1 [39]   // see: https://github.com/richardgirges/express-fileupload/issues/14
```

- Source File : vulnerable_js_app/node_modules/express/lib/application.js

```
[289]  * [Consolidate.js](https://github.com/tj/consolidate.js)
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[81]  *      next: 'http://api.example.com/users?page=2',
[82]  *      last: 'http://api.example.com/users?page=5'
[734]  *    res.append('Link', ['<http://localhost/>', '<http://localhost:3000/>']);
[906]  *    res.location('http://example.com');
[919]     deprecate('res.location("back"): use res.location(req.get("Referrer") || "/") and refer
to https://dub.sh/security-redirect for best practices');
[939]  *    res.redirect('http://example.com');
[940]  *    res.redirect(301, 'http://example.com');
[1157]   // https://bugs.chromium.org/p/v8/issues/detail?id=4730
```

- Source File : vulnerable_js_app/node_modules/express/lib/express.js

```
[112]       throw new Error('Most middleware (like ' + name + ') is no longer bundled with
Express and must be installed separately. Please see https://github.com/senchalabs/
connect#middleware.');
```

- Source File : vulnerable_js_app/node_modules/fresh/index.js

```
[45]   // https://tools.ietf.org/html/rfc2616#section-14.9.4
```

- Source File : vulnerable_js_app/node_modules/has-flag/index.d.ts

```
[2] Check if [`argv`](https://nodejs.org/docs/latest/api/
process.html#process_process_argv) has a specific flag.
```

- Source File : vulnerable_js_app/node_modules/type-is/index.js

```
[85]  * http://www.w3.org/Protocols/rfc2616/rfc2616-sec4.html#sec4.3
```

- Source File : vulnerable_js_app/node_modules/busboy/lib/index.js

```
[40] // See: https://github.com/mscdex/busboy/issues/121
```

- Source File : vulnerable_js_app/node_modules/safe-buffer/index.js

```
[1] /*! safe-buffer. MIT License. Feross Aboukhadijeh <https://feross.org/opensource> */
```

- Source File : vulnerable_js_app/node_modules/filelist/index.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/filelist/index.d.ts

```
[1] // IncludeOptions definitions copied from minimatch (https://github.com/DefinitelyTyped/
DefinitelyTyped/blob/master/types/minimatch/index.d.ts)
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/minimatch.js

```
[112]   // Thanks to Yeting Li <https://github.com/yetingli> for
```

- Source File : vulnerable_js_app/node_modules/has-symbols/shams.js

```
[18]        // temp disabled per https://github.com/ljharb/object.assign/issues/17
[20]        // temp disabled per https://github.com/WebReflection/get-own-property-symbols/
issues/4
```

- Source File : vulnerable_js_app/node_modules/cookie/index.js

```
[68]  * Keep support for leading dot: https://github.com/jshttp/cookie/issues/173
```

- Source File : vulnerable_js_app/node_modules/minimatch/minimatch.js

```
[262]   // Thanks to Yeting Li <https://github.com/yetingli> for
```

- Source File : vulnerable_js_app/node_modules/parseurl/index.js

```
[104]   // This takes the regexp from https://github.com/joyent/node/pull/7878
```

- Source File : vulnerable_js_app/node_modules/object-inspect/test/inspect.js

```
[134]         inspect(new URL('https://nodejs.org')),
```

- Source File : vulnerable_js_app/node_modules/debug/karma.conf.js

```
[12]     // available frameworks: https://npmjs.org/browse/keyword/karma-adapter
[30]     // available preprocessors: https://npmjs.org/browse/keyword/karma-preprocessor
[36]     // available reporters: https://npmjs.org/browse/keyword/karma-reporter
[58]     // available browser launchers: https://npmjs.org/browse/keyword/karma-launcher
```

- Source File : vulnerable_js_app/node_modules/debug/src/browser.js

```
[47]   // is webkit? http://stackoverflow.com/a/16459606/376773
[48]   // document is undefined in react-native: https://github.com/facebook/react-native/pull/1632
[50]     // is firebug? http://stackoverflow.com/a/398120/376773
[53]     // https://developer.mozilla.org/en-US/docs/Tools/Web_Console#Styling_messages
```

- Source File : vulnerable_js_app/node_modules/debug/src/node.js

```
[64]   util.deprecate(function(){}, 'except for stderr(2) and stdout(1), any other usage of DEBUG_FD is deprecated. Override debug.log if you want to use a different log function (https://git.io/debug_fd)')()
[179]       // See https://github.com/joyent/node/issues/1726
[209]       // See https://github.com/joyent/node/issues/1726
```

- Source File : vulnerable_js_app/node_modules/chalk/index.d.ts

```
[4] [More colors here.](https://github.com/chalk/chalk/blob/master/readme.md#256-and-truecolor-color-support)
[29] [More colors here.](https://github.com/chalk/chalk/blob/master/readme.md#256-and-truecolor-color-support)
[54] [More colors here.](https://github.com/chalk/chalk/blob/master/readme.md#256-and-truecolor-color-support)
[128]               @remarks Template literals are unsupported for nested calls (see [issue #341](https://github.com/chalk/chalk/issues/341))
[221]               Use a [Select/Set Graphic Rendition](https://en.wikipedia.org/wiki/ANSI_escape_code#SGR_parameters) (SGR) [color code number](https://en.wikipedia.org/wiki/ANSI_escape_code#3/4_bit) to set text color.
[229]               Use a [8-bit unsigned number](https://en.wikipedia.org/wiki/ANSI_escape_code#8-bit) to set text color.
[282]               Use a [Select/Set Graphic Rendition](https://en.wikipedia.org/wiki/ANSI_escape_code#SGR_parameters) (SGR) [color code number](https://en.wikipedia.org/wiki/ANSI_escape_code#3/4_bit) to set background color.
[291]               Use a [8-bit unsigned number](https://en.wikipedia.org/wiki/ANSI_escape_code#8-bit) to set background color.
```

- Source File : vulnerable_js_app/node_modules/chalk/source/index.js

```
[186]       // after next line to fix a bleed issue on macOS: https://github.com/chalk/chalk/pull/92
```

- Source File : vulnerable_js_app/node_modules/destroy/index.js

```
[99]  * PR to fix memory leak: https://github.com/nodejs/node/pull/23734
```

- Source File : vulnerable_js_app/node_modules/ansi-styles/index.d.ts

```
[202]               Use a [4-bit unsigned number](https://en.wikipedia.org/wiki/ANSI_escape_code#3/4-bit) to set text color.
[207]               Use an [8-bit unsigned number](https://en.wikipedia.org/wiki/ANSI_escape_code#8-bit) to set text color.
```

- Source File : vulnerable_js_app/node_modules/mime/src/build.js

```
[45] // https://tools.ietf.org/html/rfc6838#section-3.1
```

- Source File : vulnerable_js_app/node_modules/color-convert/conversions.js

```
[168]               See https://en.m.wikipedia.org/wiki/
Euclidean_distance#Squared_Euclidean_distance
[354] // http://dev.w3.org/csswg/css-color/#hwb-to-rgb
```

- Source File : vulnerable_js_app/node_modules/color-convert/route.js

```
[16]       // https://jsperf.com/object-keys-vs-for-in-with-closure/3
[21]                       // http://jsperf.com/1-vs-infinity
[31] // https://en.wikipedia.org/wiki/Breadth-first_search
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/rule.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/file_task.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/file.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/publish.jake.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/rule.jake.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/unit/parseargs.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/test/unit/namespace.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/bin/cli.js

```
[10]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/parseargs.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/test_task.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/program.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/api.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/publish_task.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/package_task.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/jake.js

```
[9]  *        http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/loader.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/index.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
[137]   // From Math.uuid.js, https://github.com/broofa/node-uuid
```

- Source File : vulnerable_js_app/node_modules/jake/lib/utils/file.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/ejs/ejs.js

```
[10]  *         http://www.apache.org/licenses/LICENSE-2.0
[23]  * @file Embedded JavaScript templating engine. {@link http://ejs.co}
[27]  * @license {@link http://www.apache.org/licenses/LICENSE-2.0 Apache License, Version 2.0}
[684]         e.message += 'https://github.com/RyanZim/EJS-Lint';
[964]  *         http://www.apache.org/licenses/LICENSE-2.0
[1711]   "author": "Matthew Eernisse <mde@fleegix.org> (http://fleegix.org)",
[1723]   "bugs": "https://github.com/mde/ejs/issues",
[1724]   "homepage": "https://github.com/mde/ejs",
```

- Source File : vulnerable_js_app/node_modules/ejs/bin/cli.js

```
[10]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/ejs.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
[22]  * @file Embedded JavaScript templating engine. {@link http://ejs.co}
[26]  * @license {@link http://www.apache.org/licenses/LICENSE-2.0 Apache License, Version 2.0}
[683]         e.message += 'https://github.com/RyanZim/EJS-Lint';
```

- Source File : vulnerable_js_app/node_modules/ejs/lib/utils.js

```
[9]  *         http://www.apache.org/licenses/LICENSE-2.0
```

- Source File : vulnerable_js_app/node_modules/async/index.js

```
[334]  * [ES2017 `async` function]{@link https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Statements/async_function}.
[357]  * use with [Node.js](http://nodejs.org) and installable via
```

- Source File : vulnerable_js_app/node_modules/async/series.js

```
[31]  * properties, the [ECMAScript Language Specification](http://www.ecma-international.org/ecma-262/5.1/#sec-8.6)
```

- Source File : vulnerable_js_app/node_modules/async/ensureAsync.js

```
[21]  * [Zalgo](http://blog.izs.me/post/59142742143/designing-apis-for-asynchrony)
```

- Source File : vulnerable_js_app/node_modules/async/auto.js

```
[301]         // https://en.wikipedia.org/wiki/Topological_sorting#Kahn.27s_algorithm
[302]         // http://connalle.blogspot.com/2013/10/topological-sortingkahn-algorithm.html
```

- Source File : vulnerable_js_app/node_modules/async/dist/async.js

```
[1162]             // https://en.wikipedia.org/wiki/Topological_sorting#Kahn.27s_algorithm
[1163]             // http://connalle.blogspot.com/2013/10/topological-sortingkahn-algorithm.html
[1367]     // Simple doubly linked list (https://en.wikipedia.org/wiki/Doubly_linked_list) implementation
[2294]      *     hostname: async.constant("https://server.net/"),
[2756]      * [Zalgo](http://blog.izs.me/post/59142742143/designing-apis-for-asynchrony)
[4758]      * properties, the [ECMAScript Language Specification](http://www.ecma-international.org/ecma-262/5.1/#sec-8.6)
```

```
[5825]      * [ES2017 `async` function]{@link https://developer.mozilla.org/en-US/docs/Web/
JavaScript/Reference/Statements/async_function}.
```

- Source File : vulnerable_js_app/node_modules/async/internal/DoublyLinkedList.js

```
[6] // Simple doubly linked list (https://en.wikipedia.org/wiki/Doubly_linked_list)
implementation
```

## ID: COMMON-8 : Unvalidated Redirects and Forwards

**Rule Description** : Detects potential unvalidated redirect and forward vulnerabilities.

**Issue Description** : If this rule matches, it indicates the presence of code patterns that may indicate vulnerabilities in unvalidated redirects and forwards, which can be exploited by attackers to redirect users to malicious websites or perform phishing attacks.

**Developer Note** : Developers should validate and sanitize all user-supplied input used in redirect and forward operations. They should also ensure that redirects and forwards are performed only to trusted and authorized destinations.

**Reviewer Note** : Reviewers should review the code for potential unvalidated redirect and forward vulnerabilities and verify if proper input validation and destination checks are implemented.

- Source File : vulnerable_js_app/node_modules/send/index.js

```
[471] SendStream.prototype.redirect = function redirect (path) {
[487]   // redirect
[722]     if (stat.isDirectory()) return self.redirect(path)
```

- Source File : vulnerable_js_app/node_modules/serve-static/index.js

```
[53]   // default redirect
[54]   var redirect = opts.redirect !== false
[68]   var onDirectory = redirect
[90]     // make sure redirect occurs at mount
[109]         // once file is determined, always forward error
[114]     // forward errors
[178]  * Create a directory listener that performs a redirect.
[183]   return function redirect (res) {
[200]     // send redirect response
```

- Source File : vulnerable_js_app/node_modules/statuses/index.js

```
[34] status.redirect = {
```

- Source File : vulnerable_js_app/node_modules/express/lib/response.js

```
[919]     deprecate('res.location("back"): use res.location(req.get("Referrer") || "/") and refer
to https://dub.sh/security-redirect for best practices');
[938]  *    res.redirect('/foo/bar');
[939]  *    res.redirect('http://example.com');
[940]  *    res.redirect(301, 'http://example.com');
[941]  *    res.redirect('../login'); // /blog/post/1 -> /blog/login
[946] res.redirect = function redirect(url) {
[957]       deprecate('res.redirect(url, status): Use res.redirect(status, url) instead');
```

- Source File : vulnerable_js_app/node_modules/async/index.js

```
[355]  * Async is a utility module which provides straight-forward, powerful functions
```

## ID: COMMON-9 : TODO Comments

**Rule Description** : Detects TODO comments in the code.

**Issue Description** : If this rule matches, it indicates the presence of TODO comments, which might indicate unfinished or pending tasks that could lead to security vulnerabilities or incomplete code functionality.

**Developer Note** : Developers should regularly review and address TODO comments to ensure the completion of tasks, proper code functionality, and security of the application.

**Reviewer Note** : Reviewers should check for the presence of TODO comments and verify if they have been properly addressed during code reviews and inspections.

---

- Source File : vulnerable_js_app/node_modules/side-channel-list/index.js

```
1 [111]       // @ts-expect-error TODO: figure out why this is erroring
```

- Source File : vulnerable_js_app/node_modules/mime-types/index.js

```
1 [54]   // TODO: use media-typer
2 [78]   // TODO: should this even be in this module?
3 [91]   // TODO: use content-type or other module
4 [112]   // TODO: use media-typer
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-codec.js

```
1 [348]                    // TODO: What if we have no default? (resCode == undefined)
2 [420]              // See todo above.
3 [472]              // TODO: Callback with seq.
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-data.js

```
1 [64]     // TODO: KDDI extension to Shift_JIS
2 [65]     // TODO: IBM CCSID 942 = CP932, but F0-F9 custom chars and other char changes.
3 [66]     // TODO: IBM CCSID 943 = Shift_JIS = CP932 with original Shift_JIS lower 128 chars.
```

- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/extend-node.js

```
1 [169]              // TODO: Set _charsWritten.
```

- Source File : vulnerable_js_app/node_modules/express/lib/request.js

```
1 [452] // TODO: change req.host to return host in next major
```

- Source File : vulnerable_js_app/node_modules/side-channel-map/index.js

```
1 [66]       // @ts-expect-error TODO: figure out why TS is erroring here
```

- Source File : vulnerable_js_app/node_modules/busboy/test/common.js

```
1 [73]   // TODO: remove origFn?
```

- Source File : vulnerable_js_app/node_modules/busboy/lib/utils.js

```
1 [392]       case 'ascii': // TODO: Make these a separate, strict decoder?
```

- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/minimatch.js

```
1 [648]           // TODO: It would probably be faster to determine this
```

- Source File : vulnerable_js_app/node_modules/qs/test/stringify.js

```
1 [516]             { skip: 'TODO: figure out what this should do' }
2 [1216]             { skip: 'TODO: figure out what this should do' }
```

- Source File : vulnerable_js_app/node_modules/side-channel/index.js

```
1 [41]       // @ts-expect-error TODO: figure out why this is erroring
```

- Source File : vulnerable_js_app/node_modules/minimatch/minimatch.js

```
1 [491]        // TODO: It would probably be faster to determine this
```

- Source File : vulnerable_js_app/node_modules/debug/src/browser.js

```
1 [36]  * TODO: add a `localStorage` variable to explicitly enable/disable colors
```

- Source File : vulnerable_js_app/node_modules/mime/src/test.js

```
[46] // TODO: Uncomment once #157 is resolved
```

- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/json.js

```
[77]       // TODO: maybe make this configurable or part of "strict" option
```

- Source File : vulnerable_js_app/node_modules/jake/lib/rule.js

```
[107]     // TODO: Write a utility function that appends a
```

- Source File : vulnerable_js_app/node_modules/side-channel-weakmap/index.js

```
[81]               // @ts-expect-error TODO: figure out why this is erroring
```

## ID: COMMON-10 : Insecure Cryptographic Algorithm

**Rule Description** : Detects the usage of insecure cryptographic algorithms in Java code.

**Issue Description** : If this rule matches, it indicates the potential vulnerability of using insecure cryptographic algorithms. Insecure algorithms such as MD5, SHA-1, or weak encryption algorithms can be exploited by attackers to bypass security measures or recover sensitive information.

**Developer Note** : Developers should use secure cryptographic algorithms, such as SHA-256 or SHA-3 for hashing and AES for encryption. They should avoid using deprecated or weak algorithms that have known vulnerabilities.

**Reviewer Note** : Reviewers should verify that secure cryptographic algorithms are used to mitigate the risk of cryptographic vulnerabilities. They should assess if deprecated or weak algorithms are used and recommend replacing them with stronger alternatives.

---

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/multipartUploads.spec.js

```
[4] const md5 = require('md5');
[34]     md5: md5(fileBuffer),
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/server.js

```
[42]   md5: file.md5,
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/tempFile.spec.js

```
[2] const md5 = require('md5');
[32]     let fileHash = md5(fileBuffer);
[47]         md5: fileHash,
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/fileFactory.spec.js

```
[4] const md5 = require('md5');
[14] const mockMd5 = md5(mockBuffer);
[41]     it('contains the md5 property', () => assert.equal(fileFactory(mockFileOpts).md5,
mockMd5));
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/test/utilities.spec.js

```
[6] const md5 = require('md5');
[29] const mockHash = md5(mockBuffer);
[33] const mockHashMove = md5(mockBufferMove);
[201]     const source = { option1: '1', option2: '2', hashAlgorithm: 'md5' };
[203]     const expected = { option1: '1', option2: '2', hashAlgorithm: 'md5' };
[287]           const fileHash = md5(fileBuffer);
[393]           let fileHash = md5(fileBuffer);
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/index.js

```
[24]   hashAlgorithm: 'md5'
```

- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/fileFactory.js

```
1 [53]     md5: options.hash,
```

- Source File : vulnerable_js_app/node_modules/etag/index.js

```
1 [47]     .createHash('sha1')
```

# Parsed Paths – Areas of Interest

This section contains a list of file paths that have been identified by matching them with a predefined set of keywords. These files are typically of interest to a code reviewer, and should be examined for possible security vulnerabilities or insecure implementations.

## 1. Rule Title: Session Management

- Source File: vulnerable_js_app/node_modules/cookie/index.js
- Source File: vulnerable_js_app/node_modules/cookie-signature/index.js

## 2. Rule Title: API

- Source File: vulnerable_js_app/node_modules/jake/lib/api.js

## 3. Rule Title: File Upload

- Source File: vulnerable_js_app/node_modules/express-fileupload/test/multipartUploads.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/server.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/uploadtimer.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/fileLimitUploads.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/tempFile.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/fileFactory.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/utilities.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/multipartFields.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/pretests.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/posttests.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/processNested.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/options.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/test/isEligibleRequest.spec.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/index.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/processNested.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/tempFileHandler.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/utilities.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/memHandler.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/processMultipart.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/uploadtimer.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/isEligibleRequest.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/lib/fileFactory.js
- Source File: vulnerable_js_app/node_modules/express-fileupload/example/server.js

## 4. Rule Title: Logging

- Source File: vulnerable_js_app/node_modules/debug/src/inspector-log.js
- Source File: vulnerable_js_app/node_modules/jake/lib/utils/logger.js
- Source File: vulnerable_js_app/node_modules/async/log.js

## 5. Rule Title: Database Interaction

- Source File: vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-codec.js
- Source File: vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-data.js
- Source File: vulnerable_js_app/node_modules/mime-db/index.js

# Identified Files Path

In this section, you'll find a comprehensive list of project file paths that were parsed during the analysis. This list was generated based on the selected file types during the scanning process and was used to identify the areas of interest listed in the previous sections. It's important to note that this list includes all the files, making it a superset of the list provided in the "Parsed Paths - Areas of Interest" section.

It is still recommended for code reviewers to review this list for any potentially interesting files that may have been overlooked in the "Parsed Paths - Areas of Interest" section.

- Source File : vulnerable_js_app/app.js
- Source File : vulnerable_js_app/node_modules/send/index.js
- Source File : vulnerable_js_app/node_modules/send/node_modules/ms/index.js
- Source File : vulnerable_js_app/node_modules/send/node_modules/encodeurl/index.js
- Source File : vulnerable_js_app/node_modules/dunder-proto/get.js
- Source File : vulnerable_js_app/node_modules/dunder-proto/set.js
- Source File : vulnerable_js_app/node_modules/dunder-proto/get.d.ts
- Source File : vulnerable_js_app/node_modules/dunder-proto/set.d.ts
- Source File : vulnerable_js_app/node_modules/dunder-proto/test/index.js
- Source File : vulnerable_js_app/node_modules/dunder-proto/test/get.js
- Source File : vulnerable_js_app/node_modules/dunder-proto/test/set.js
- Source File : vulnerable_js_app/node_modules/side-channel-list/index.js
- Source File : vulnerable_js_app/node_modules/side-channel-list/index.d.ts
- Source File : vulnerable_js_app/node_modules/side-channel-list/list.d.ts
- Source File : vulnerable_js_app/node_modules/side-channel-list/test/index.js
- Source File : vulnerable_js_app/node_modules/proxy-addr/index.js
- Source File : vulnerable_js_app/node_modules/array-flatten/array-flatten.js
- Source File : vulnerable_js_app/node_modules/supports-color/index.js
- Source File : vulnerable_js_app/node_modules/supports-color/browser.js
- Source File : vulnerable_js_app/node_modules/unpipe/index.js
- Source File : vulnerable_js_app/node_modules/forwarded/index.js
- Source File : vulnerable_js_app/node_modules/balanced-match/index.js
- Source File : vulnerable_js_app/node_modules/ms/index.js
- Source File : vulnerable_js_app/node_modules/http-errors/index.js
- Source File : vulnerable_js_app/node_modules/path-to-regexp/index.js
- Source File : vulnerable_js_app/node_modules/brace-expansion/index.js
- Source File : vulnerable_js_app/node_modules/encodeurl/index.js
- Source File : vulnerable_js_app/node_modules/serve-static/index.js
- Source File : vulnerable_js_app/node_modules/mime-types/index.js
- Source File : vulnerable_js_app/node_modules/streamsearch/.eslintrc.js
- Source File : vulnerable_js_app/node_modules/streamsearch/test/test.js
- Source File : vulnerable_js_app/node_modules/streamsearch/lib/sbmh.js
- Source File : vulnerable_js_app/node_modules/get-intrinsic/index.js
- Source File : vulnerable_js_app/node_modules/get-intrinsic/test/GetIntrinsic.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/index.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-codec.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/internal.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/sbcs-data-generated.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/sbcs-codec.js

- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/utf7.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/utf16.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/dbcs-data.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/encodings/sbcs-data.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/streams.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/index.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/extend-node.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/bom-handling.js
- Source File : vulnerable_js_app/node_modules/iconv-lite/lib/index.d.ts
- Source File : vulnerable_js_app/node_modules/escape-html/index.js
- Source File : vulnerable_js_app/node_modules/mime-db/index.js
- Source File : vulnerable_js_app/node_modules/setprototypeof/index.js
- Source File : vulnerable_js_app/node_modules/setprototypeof/index.d.ts
- Source File : vulnerable_js_app/node_modules/setprototypeof/test/index.js
- Source File : vulnerable_js_app/node_modules/negotiator/index.js
- Source File : vulnerable_js_app/node_modules/negotiator/lib/encoding.js
- Source File : vulnerable_js_app/node_modules/negotiator/lib/charset.js
- Source File : vulnerable_js_app/node_modules/negotiator/lib/mediaType.js
- Source File : vulnerable_js_app/node_modules/negotiator/lib/language.js
- Source File : vulnerable_js_app/node_modules/ee-first/index.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/multipartUploads.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/server.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/uploadtimer.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/fileLimitUploads.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/tempFile.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/fileFactory.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/utilities.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/multipartFields.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/pretests.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/posttests.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/processNested.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/options.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/test/isEligibleRequest.spec.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/index.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/processNested.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/tempFileHandler.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/utilities.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/memHandler.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/processMultipart.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/uploadtimer.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/isEligibleRequest.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/lib/fileFactory.js
- Source File : vulnerable_js_app/node_modules/express-fileupload/example/server.js
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/index.js
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/applyBind.js
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/reflectApply.js
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/actualApply.js

- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/functionApply.js
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/functionCall.js
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/reflectApply.d.ts
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/index.d.ts
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/functionCall.d.ts
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/actualApply.d.ts
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/applyBind.d.ts
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/functionApply.d.ts
- Source File : vulnerable_js_app/node_modules/call-bind-apply-helpers/test/index.js
- Source File : vulnerable_js_app/node_modules/statuses/index.js
- Source File : vulnerable_js_app/node_modules/content-disposition/index.js
- Source File : vulnerable_js_app/node_modules/express/index.js
- Source File : vulnerable_js_app/node_modules/express/lib/view.js
- Source File : vulnerable_js_app/node_modules/express/lib/application.js
- Source File : vulnerable_js_app/node_modules/express/lib/response.js
- Source File : vulnerable_js_app/node_modules/express/lib/request.js
- Source File : vulnerable_js_app/node_modules/express/lib/utils.js
- Source File : vulnerable_js_app/node_modules/express/lib/express.js
- Source File : vulnerable_js_app/node_modules/express/lib/router/index.js
- Source File : vulnerable_js_app/node_modules/express/lib/router/layer.js
- Source File : vulnerable_js_app/node_modules/express/lib/router/route.js
- Source File : vulnerable_js_app/node_modules/express/lib/middleware/query.js
- Source File : vulnerable_js_app/node_modules/express/lib/middleware/init.js
- Source File : vulnerable_js_app/node_modules/es-object-atoms/index.js
- Source File : vulnerable_js_app/node_modules/es-object-atoms/RequireObjectCoercible.js
- Source File : vulnerable_js_app/node_modules/es-object-atoms/ToObject.js
- Source File : vulnerable_js_app/node_modules/es-object-atoms/index.d.ts
- Source File : vulnerable_js_app/node_modules/es-object-atoms/ToObject.d.ts
- Source File : vulnerable_js_app/node_modules/es-object-atoms/RequireObjectCoercible.d.ts
- Source File : vulnerable_js_app/node_modules/es-object-atoms/test/index.js
- Source File : vulnerable_js_app/node_modules/methods/index.js
- Source File : vulnerable_js_app/node_modules/fresh/index.js
- Source File : vulnerable_js_app/node_modules/has-flag/index.js
- Source File : vulnerable_js_app/node_modules/has-flag/index.d.ts
- Source File : vulnerable_js_app/node_modules/color-name/index.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isInteger.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/floor.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/abs.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/mod.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/round.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/sign.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/max.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isNaN.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isNegativeZero.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/pow.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/min.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isFinite.js

- Source File : vulnerable_js_app/node_modules/math-intrinsics/pow.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isNegativeZero.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isFinite.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/abs.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isNaN.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/max.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/sign.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/isInteger.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/mod.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/floor.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/min.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/round.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/test/index.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxArrayLength.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxSafeInteger.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxValue.js
- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxSafeInteger.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxValue.d.ts
- Source File : vulnerable_js_app/node_modules/math-intrinsics/constants/maxArrayLength.d.ts
- Source File : vulnerable_js_app/node_modules/side-channel-map/index.js
- Source File : vulnerable_js_app/node_modules/side-channel-map/index.d.ts
- Source File : vulnerable_js_app/node_modules/side-channel-map/test/index.js
- Source File : vulnerable_js_app/node_modules/ipaddr.js/ipaddr.min.js
- Source File : vulnerable_js_app/node_modules/ipaddr.js/lib/ipaddr.js
- Source File : vulnerable_js_app/node_modules/ipaddr.js/lib/ipaddr.js.d.ts
- Source File : vulnerable_js_app/node_modules/safer-buffer/dangerous.js
- Source File : vulnerable_js_app/node_modules/safer-buffer/tests.js
- Source File : vulnerable_js_app/node_modules/safer-buffer/safer.js
- Source File : vulnerable_js_app/node_modules/type-is/index.js
- Source File : vulnerable_js_app/node_modules/es-errors/range.js
- Source File : vulnerable_js_app/node_modules/es-errors/uri.js
- Source File : vulnerable_js_app/node_modules/es-errors/index.js
- Source File : vulnerable_js_app/node_modules/es-errors/ref.js
- Source File : vulnerable_js_app/node_modules/es-errors/syntax.js
- Source File : vulnerable_js_app/node_modules/es-errors/eval.js
- Source File : vulnerable_js_app/node_modules/es-errors/type.js
- Source File : vulnerable_js_app/node_modules/es-errors/type.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/index.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/syntax.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/uri.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/ref.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/range.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/eval.d.ts
- Source File : vulnerable_js_app/node_modules/es-errors/test/index.js
- Source File : vulnerable_js_app/node_modules/raw-body/index.js
- Source File : vulnerable_js_app/node_modules/raw-body/index.d.ts
- Source File : vulnerable_js_app/node_modules/busboy/.eslintrc.js

- Source File : vulnerable_js_app/node_modules/busboy/test/test-types-multipart.js
- Source File : vulnerable_js_app/node_modules/busboy/test/test.js
- Source File : vulnerable_js_app/node_modules/busboy/test/test-types-multipart-charsets.js
- Source File : vulnerable_js_app/node_modules/busboy/test/test-types-multipart-stream-pause.js
- Source File : vulnerable_js_app/node_modules/busboy/test/test-types-urlencoded.js
- Source File : vulnerable_js_app/node_modules/busboy/test/common.js
- Source File : vulnerable_js_app/node_modules/busboy/bench/bench-multipart-files-100mb-big.js
- Source File : vulnerable_js_app/node_modules/busboy/bench/bench-multipart-fields-100mb-small.js
- Source File : vulnerable_js_app/node_modules/busboy/bench/bench-multipart-fields-100mb-big.js
- Source File : vulnerable_js_app/node_modules/busboy/bench/bench-urlencoded-fields-100pairs-small.js
- Source File : vulnerable_js_app/node_modules/busboy/bench/bench-multipart-files-100mb-small.js
- Source File : vulnerable_js_app/node_modules/busboy/bench/bench-urlencoded-fields-900pairs-small-alt.js
- Source File : vulnerable_js_app/node_modules/busboy/lib/index.js
- Source File : vulnerable_js_app/node_modules/busboy/lib/utils.js
- Source File : vulnerable_js_app/node_modules/busboy/lib/types/urlencoded.js
- Source File : vulnerable_js_app/node_modules/busboy/lib/types/multipart.js
- Source File : vulnerable_js_app/node_modules/safe-buffer/index.js
- Source File : vulnerable_js_app/node_modules/safe-buffer/index.d.ts
- Source File : vulnerable_js_app/node_modules/filelist/index.js
- Source File : vulnerable_js_app/node_modules/filelist/jakefile.js
- Source File : vulnerable_js_app/node_modules/filelist/index.d.ts
- Source File : vulnerable_js_app/node_modules/filelist/node_modules/brace-expansion/index.js
- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/minimatch.js
- Source File : vulnerable_js_app/node_modules/filelist/node_modules/minimatch/lib/path.js
- Source File : vulnerable_js_app/node_modules/vary/index.js
- Source File : vulnerable_js_app/node_modules/qs/dist/qs.js
- Source File : vulnerable_js_app/node_modules/qs/test/parse.js
- Source File : vulnerable_js_app/node_modules/qs/test/stringify.js
- Source File : vulnerable_js_app/node_modules/qs/test/utils.js
- Source File : vulnerable_js_app/node_modules/qs/test/empty-keys-cases.js
- Source File : vulnerable_js_app/node_modules/qs/lib/index.js
- Source File : vulnerable_js_app/node_modules/qs/lib/formats.js
- Source File : vulnerable_js_app/node_modules/qs/lib/parse.js
- Source File : vulnerable_js_app/node_modules/qs/lib/stringify.js
- Source File : vulnerable_js_app/node_modules/qs/lib/utils.js
- Source File : vulnerable_js_app/node_modules/call-bound/index.js
- Source File : vulnerable_js_app/node_modules/call-bound/index.d.ts
- Source File : vulnerable_js_app/node_modules/call-bound/test/index.js
- Source File : vulnerable_js_app/node_modules/content-type/index.js
- Source File : vulnerable_js_app/node_modules/has-symbols/index.js
- Source File : vulnerable_js_app/node_modules/has-symbols/shams.js
- Source File : vulnerable_js_app/node_modules/has-symbols/index.d.ts
- Source File : vulnerable_js_app/node_modules/has-symbols/shams.d.ts
- Source File : vulnerable_js_app/node_modules/has-symbols/test/index.js
- Source File : vulnerable_js_app/node_modules/has-symbols/test/tests.js
- Source File : vulnerable_js_app/node_modules/has-symbols/test/shams/get-own-property-symbols.js

- Source File : vulnerable_js_app/node_modules/has-symbols/test/shams/core-js.js
- Source File : vulnerable_js_app/node_modules/cookie/index.js
- Source File : vulnerable_js_app/node_modules/side-channel/index.js
- Source File : vulnerable_js_app/node_modules/side-channel/index.d.ts
- Source File : vulnerable_js_app/node_modules/side-channel/test/index.js
- Source File : vulnerable_js_app/node_modules/minimatch/minimatch.js
- Source File : vulnerable_js_app/node_modules/function-bind/index.js
- Source File : vulnerable_js_app/node_modules/function-bind/implementation.js
- Source File : vulnerable_js_app/node_modules/function-bind/test/index.js
- Source File : vulnerable_js_app/node_modules/hasown/index.js
- Source File : vulnerable_js_app/node_modules/hasown/index.d.ts
- Source File : vulnerable_js_app/node_modules/etag/index.js
- Source File : vulnerable_js_app/node_modules/finalhandler/index.js
- Source File : vulnerable_js_app/node_modules/parseurl/index.js
- Source File : vulnerable_js_app/node_modules/toidentifier/index.js
- Source File : vulnerable_js_app/node_modules/object-inspect/index.js
- Source File : vulnerable_js_app/node_modules/object-inspect/util.inspect.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test-core-js.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/err.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/toStringTag.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/fn.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/undef.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/has.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/bigint.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/element.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/indent-option.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/fakes.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/inspect.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/lowbyte.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/number.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/values.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/global.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/circular.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/holes.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/deep.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/quoteStyle.js
- Source File : vulnerable_js_app/node_modules/object-inspect/test/browser/dom.js
- Source File : vulnerable_js_app/node_modules/object-inspect/example/fn.js
- Source File : vulnerable_js_app/node_modules/object-inspect/example/inspect.js
- Source File : vulnerable_js_app/node_modules/object-inspect/example/circular.js
- Source File : vulnerable_js_app/node_modules/object-inspect/example/all.js
- Source File : vulnerable_js_app/node_modules/debug/karma.conf.js
- Source File : vulnerable_js_app/node_modules/debug/node.js
- Source File : vulnerable_js_app/node_modules/debug/src/index.js
- Source File : vulnerable_js_app/node_modules/debug/src/debug.js
- Source File : vulnerable_js_app/node_modules/debug/src/inspector-log.js
- Source File : vulnerable_js_app/node_modules/debug/src/browser.js

- Source File : vulnerable_js_app/node_modules/debug/src/node.js
- Source File : vulnerable_js_app/node_modules/merge-descriptors/index.js
- Source File : vulnerable_js_app/node_modules/accepts/index.js
- Source File : vulnerable_js_app/node_modules/chalk/index.d.ts
- Source File : vulnerable_js_app/node_modules/chalk/source/index.js
- Source File : vulnerable_js_app/node_modules/chalk/source/templates.js
- Source File : vulnerable_js_app/node_modules/chalk/source/util.js
- Source File : vulnerable_js_app/node_modules/destroy/index.js
- Source File : vulnerable_js_app/node_modules/ansi-styles/index.js
- Source File : vulnerable_js_app/node_modules/ansi-styles/index.d.ts
- Source File : vulnerable_js_app/node_modules/mime/mime.js
- Source File : vulnerable_js_app/node_modules/mime/cli.js
- Source File : vulnerable_js_app/node_modules/mime/src/test.js
- Source File : vulnerable_js_app/node_modules/mime/src/build.js
- Source File : vulnerable_js_app/node_modules/color-convert/index.js
- Source File : vulnerable_js_app/node_modules/color-convert/conversions.js
- Source File : vulnerable_js_app/node_modules/color-convert/route.js
- Source File : vulnerable_js_app/node_modules/on-finished/index.js
- Source File : vulnerable_js_app/node_modules/body-parser/index.js
- Source File : vulnerable_js_app/node_modules/body-parser/lib/read.js
- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/json.js
- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/urlencoded.js
- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/text.js
- Source File : vulnerable_js_app/node_modules/body-parser/lib/types/raw.js
- Source File : vulnerable_js_app/node_modules/range-parser/index.js
- Source File : vulnerable_js_app/node_modules/gopd/index.js
- Source File : vulnerable_js_app/node_modules/gopd/gOPD.js
- Source File : vulnerable_js_app/node_modules/gopd/index.d.ts
- Source File : vulnerable_js_app/node_modules/gopd/gOPD.d.ts
- Source File : vulnerable_js_app/node_modules/gopd/test/index.js
- Source File : vulnerable_js_app/node_modules/media-typer/index.js
- Source File : vulnerable_js_app/node_modules/cookie-signature/index.js
- Source File : vulnerable_js_app/node_modules/jake/jakefile.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/rule.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/publish_task.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/helpers.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/selfdep.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/task_base.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/concurrent.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/list_tasks.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakefile.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/file_task.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/file.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/concurrent.jake.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/publish.jake.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/rule.jake.js
- Source File : vulnerable_js_app/node_modules/jake/test/integration/jakelib/required_module.jake.js

- Source File : vulnerable_js_app/node_modules/jake/test/unit/parseargs.js
- Source File : vulnerable_js_app/node_modules/jake/test/unit/namespace.js
- Source File : vulnerable_js_app/node_modules/jake/test/unit/jakefile.js
- Source File : vulnerable_js_app/node_modules/jake/bin/cli.js
- Source File : vulnerable_js_app/node_modules/jake/lib/parseargs.js
- Source File : vulnerable_js_app/node_modules/jake/lib/test_task.js
- Source File : vulnerable_js_app/node_modules/jake/lib/rule.js
- Source File : vulnerable_js_app/node_modules/jake/lib/program.js
- Source File : vulnerable_js_app/node_modules/jake/lib/namespace.js
- Source File : vulnerable_js_app/node_modules/jake/lib/api.js
- Source File : vulnerable_js_app/node_modules/jake/lib/publish_task.js
- Source File : vulnerable_js_app/node_modules/jake/lib/package_task.js
- Source File : vulnerable_js_app/node_modules/jake/lib/jake.js
- Source File : vulnerable_js_app/node_modules/jake/lib/loader.js
- Source File : vulnerable_js_app/node_modules/jake/lib/task/task.js
- Source File : vulnerable_js_app/node_modules/jake/lib/task/index.js
- Source File : vulnerable_js_app/node_modules/jake/lib/task/directory_task.js
- Source File : vulnerable_js_app/node_modules/jake/lib/task/file_task.js
- Source File : vulnerable_js_app/node_modules/jake/lib/utils/index.js
- Source File : vulnerable_js_app/node_modules/jake/lib/utils/file.js
- Source File : vulnerable_js_app/node_modules/jake/lib/utils/logger.js
- Source File : vulnerable_js_app/node_modules/ejs/ejs.min.js
- Source File : vulnerable_js_app/node_modules/ejs/jakefile.js
- Source File : vulnerable_js_app/node_modules/ejs/ejs.js
- Source File : vulnerable_js_app/node_modules/ejs/bin/cli.js
- Source File : vulnerable_js_app/node_modules/ejs/lib/ejs.js
- Source File : vulnerable_js_app/node_modules/ejs/lib/utils.js
- Source File : vulnerable_js_app/node_modules/async/reject.js
- Source File : vulnerable_js_app/node_modules/async/log.js
- Source File : vulnerable_js_app/node_modules/async/parallelLimit.js
- Source File : vulnerable_js_app/node_modules/async/selectLimit.js
- Source File : vulnerable_js_app/node_modules/async/index.js
- Source File : vulnerable_js_app/node_modules/async/timesSeries.js
- Source File : vulnerable_js_app/node_modules/async/everySeries.js
- Source File : vulnerable_js_app/node_modules/async/series.js
- Source File : vulnerable_js_app/node_modules/async/compose.js
- Source File : vulnerable_js_app/node_modules/async/each.js
- Source File : vulnerable_js_app/node_modules/async/detectSeries.js
- Source File : vulnerable_js_app/node_modules/async/concat.js
- Source File : vulnerable_js_app/node_modules/async/retryable.js
- Source File : vulnerable_js_app/node_modules/async/filter.js
- Source File : vulnerable_js_app/node_modules/async/select.js
- Source File : vulnerable_js_app/node_modules/async/rejectLimit.js
- Source File : vulnerable_js_app/node_modules/async/findLimit.js
- Source File : vulnerable_js_app/node_modules/async/filterLimit.js
- Source File : vulnerable_js_app/node_modules/async/foldr.js
- Source File : vulnerable_js_app/node_modules/async/eachSeries.js

- Source File : vulnerable_js_app/node_modules/async/reflectAll.js
- Source File : vulnerable_js_app/node_modules/async/sortBy.js
- Source File : vulnerable_js_app/node_modules/async/flatMapSeries.js
- Source File : vulnerable_js_app/node_modules/async/groupBySeries.js
- Source File : vulnerable_js_app/node_modules/async/forEachSeries.js
- Source File : vulnerable_js_app/node_modules/async/flatMap.js
- Source File : vulnerable_js_app/node_modules/async/race.js
- Source File : vulnerable_js_app/node_modules/async/eachOfSeries.js
- Source File : vulnerable_js_app/node_modules/async/timeout.js
- Source File : vulnerable_js_app/node_modules/async/retry.js
- Source File : vulnerable_js_app/node_modules/async/findSeries.js
- Source File : vulnerable_js_app/node_modules/async/mapLimit.js
- Source File : vulnerable_js_app/node_modules/async/mapValuesSeries.js
- Source File : vulnerable_js_app/node_modules/async/allSeries.js
- Source File : vulnerable_js_app/node_modules/async/ensureAsync.js
- Source File : vulnerable_js_app/node_modules/async/some.js
- Source File : vulnerable_js_app/node_modules/async/foldl.js
- Source File : vulnerable_js_app/node_modules/async/timesLimit.js
- Source File : vulnerable_js_app/node_modules/async/cargoQueue.js
- Source File : vulnerable_js_app/node_modules/async/concatLimit.js
- Source File : vulnerable_js_app/node_modules/async/forEachOfLimit.js
- Source File : vulnerable_js_app/node_modules/async/tryEach.js
- Source File : vulnerable_js_app/node_modules/async/anyLimit.js
- Source File : vulnerable_js_app/node_modules/async/forever.js
- Source File : vulnerable_js_app/node_modules/async/inject.js
- Source File : vulnerable_js_app/node_modules/async/rejectSeries.js
- Source File : vulnerable_js_app/node_modules/async/nextTick.js
- Source File : vulnerable_js_app/node_modules/async/constant.js
- Source File : vulnerable_js_app/node_modules/async/setImmediate.js
- Source File : vulnerable_js_app/node_modules/async/someLimit.js
- Source File : vulnerable_js_app/node_modules/async/eachLimit.js
- Source File : vulnerable_js_app/node_modules/async/during.js
- Source File : vulnerable_js_app/node_modules/async/dir.js
- Source File : vulnerable_js_app/node_modules/async/asyncify.js
- Source File : vulnerable_js_app/node_modules/async/mapValues.js
- Source File : vulnerable_js_app/node_modules/async/mapValuesLimit.js
- Source File : vulnerable_js_app/node_modules/async/apply.js
- Source File : vulnerable_js_app/node_modules/async/priorityQueue.js
- Source File : vulnerable_js_app/node_modules/async/detect.js
- Source File : vulnerable_js_app/node_modules/async/seq.js
- Source File : vulnerable_js_app/node_modules/async/someSeries.js
- Source File : vulnerable_js_app/node_modules/async/reflect.js
- Source File : vulnerable_js_app/node_modules/async/doUntil.js
- Source File : vulnerable_js_app/node_modules/async/reduce.js
- Source File : vulnerable_js_app/node_modules/async/queue.js
- Source File : vulnerable_js_app/node_modules/async/transform.js
- Source File : vulnerable_js_app/node_modules/async/find.js

- Source File : vulnerable_js_app/node_modules/async/wrapSync.js
- Source File : vulnerable_js_app/node_modules/async/until.js
- Source File : vulnerable_js_app/node_modules/async/eachOf.js
- Source File : vulnerable_js_app/node_modules/async/whilst.js
- Source File : vulnerable_js_app/node_modules/async/applyEachSeries.js
- Source File : vulnerable_js_app/node_modules/async/map.js
- Source File : vulnerable_js_app/node_modules/async/doDuring.js
- Source File : vulnerable_js_app/node_modules/async/mapSeries.js
- Source File : vulnerable_js_app/node_modules/async/reduceRight.js
- Source File : vulnerable_js_app/node_modules/async/auto.js
- Source File : vulnerable_js_app/node_modules/async/forEachOf.js
- Source File : vulnerable_js_app/node_modules/async/any.js
- Source File : vulnerable_js_app/node_modules/async/all.js
- Source File : vulnerable_js_app/node_modules/async/eachOfLimit.js
- Source File : vulnerable_js_app/node_modules/async/allLimit.js
- Source File : vulnerable_js_app/node_modules/async/forEach.js
- Source File : vulnerable_js_app/node_modules/async/filterSeries.js
- Source File : vulnerable_js_app/node_modules/async/doWhilst.js
- Source File : vulnerable_js_app/node_modules/async/flatMapLimit.js
- Source File : vulnerable_js_app/node_modules/async/selectSeries.js
- Source File : vulnerable_js_app/node_modules/async/forEachOfSeries.js
- Source File : vulnerable_js_app/node_modules/async/forEachLimit.js
- Source File : vulnerable_js_app/node_modules/async/applyEach.js
- Source File : vulnerable_js_app/node_modules/async/everyLimit.js
- Source File : vulnerable_js_app/node_modules/async/cargo.js
- Source File : vulnerable_js_app/node_modules/async/groupByLimit.js
- Source File : vulnerable_js_app/node_modules/async/times.js
- Source File : vulnerable_js_app/node_modules/async/anySeries.js
- Source File : vulnerable_js_app/node_modules/async/detectLimit.js
- Source File : vulnerable_js_app/node_modules/async/memoize.js
- Source File : vulnerable_js_app/node_modules/async/unmemoize.js
- Source File : vulnerable_js_app/node_modules/async/parallel.js
- Source File : vulnerable_js_app/node_modules/async/waterfall.js
- Source File : vulnerable_js_app/node_modules/async/autoInject.js
- Source File : vulnerable_js_app/node_modules/async/every.js
- Source File : vulnerable_js_app/node_modules/async/groupBy.js
- Source File : vulnerable_js_app/node_modules/async/concatSeries.js
- Source File : vulnerable_js_app/node_modules/async/dist/async.js
- Source File : vulnerable_js_app/node_modules/async/dist/async.min.js
- Source File : vulnerable_js_app/node_modules/async/internal/reject.js
- Source File : vulnerable_js_app/node_modules/async/internal/range.js
- Source File : vulnerable_js_app/node_modules/async/internal/once.js
- Source File : vulnerable_js_app/node_modules/async/internal/filter.js
- Source File : vulnerable_js_app/node_modules/async/internal/awaitify.js
- Source File : vulnerable_js_app/node_modules/async/internal/consoleFunc.js
- Source File : vulnerable_js_app/node_modules/async/internal/Heap.js
- Source File : vulnerable_js_app/node_modules/async/internal/DoublyLinkedList.js

- Source File : vulnerable_js_app/node_modules/async/internal/withoutIndex.js
- Source File : vulnerable_js_app/node_modules/async/internal/promiseCallback.js
- Source File : vulnerable_js_app/node_modules/async/internal/wrapAsync.js
- Source File : vulnerable_js_app/node_modules/async/internal/setImmediate.js
- Source File : vulnerable_js_app/node_modules/async/internal/iterator.js
- Source File : vulnerable_js_app/node_modules/async/internal/onlyOnce.js
- Source File : vulnerable_js_app/node_modules/async/internal/createTester.js
- Source File : vulnerable_js_app/node_modules/async/internal/breakLoop.js
- Source File : vulnerable_js_app/node_modules/async/internal/queue.js
- Source File : vulnerable_js_app/node_modules/async/internal/asyncEachOfLimit.js
- Source File : vulnerable_js_app/node_modules/async/internal/map.js
- Source File : vulnerable_js_app/node_modules/async/internal/isArrayLike.js
- Source File : vulnerable_js_app/node_modules/async/internal/getIterator.js
- Source File : vulnerable_js_app/node_modules/async/internal/eachOfLimit.js
- Source File : vulnerable_js_app/node_modules/async/internal/initialParams.js
- Source File : vulnerable_js_app/node_modules/async/internal/applyEach.js
- Source File : vulnerable_js_app/node_modules/async/internal/parallel.js
- Source File : vulnerable_js_app/node_modules/es-define-property/index.js
- Source File : vulnerable_js_app/node_modules/es-define-property/index.d.ts
- Source File : vulnerable_js_app/node_modules/es-define-property/test/index.js
- Source File : vulnerable_js_app/node_modules/depd/index.js
- Source File : vulnerable_js_app/node_modules/depd/lib/browser/index.js
- Source File : vulnerable_js_app/node_modules/inherits/inherits.js
- Source File : vulnerable_js_app/node_modules/inherits/inherits_browser.js
- Source File : vulnerable_js_app/node_modules/concat-map/index.js
- Source File : vulnerable_js_app/node_modules/concat-map/test/map.js
- Source File : vulnerable_js_app/node_modules/concat-map/example/map.js
- Source File : vulnerable_js_app/node_modules/side-channel-weakmap/index.js
- Source File : vulnerable_js_app/node_modules/side-channel-weakmap/index.d.ts
- Source File : vulnerable_js_app/node_modules/side-channel-weakmap/test/index.js
- Source File : vulnerable_js_app/node_modules/bytes/index.js
- Source File : vulnerable_js_app/node_modules/utils-merge/index.js