Security Assessment Report

ESLint Security Issues: 24

ZAP Alerts: 10

OWASP ZAP Baseline Report

ZAP Scanning Report

Site: http://host.docker.internal:3000

Generated on Thu, 27 Nov 2025 10:54:31

ZAP Version: 2.16.1

ZAP by Checkmarx

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	1
Low	4
Informational	5
False Positives:	0

Summary of Sequences

For each step: result (Pass/Fail) - risk (of highest alert(s) for the step, if any).

Alerts

Name	Risk Level	Number of Instances
CSP: style-src unsafe-inline	Medium	3
Dangerous JS Functions	Low	1
Insufficient Site Isolation Against Spectre Vulnerability	Low	13
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	3
Timestamp Disclosure - Unix	Low	1
Information Disclosure - Suspicious Comments	Informational	10
Modern Web Application	Informational	2
Non-Storable Content	Informational	9
Storable and Cacheable Content	Informational	2
Storable but Non-Cacheable Content	Informational	1

Alert Detail

Medium	**CSP: style-src unsafe-inline**
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks. Including (but not limited to) Cross Site Scripting (XSS), and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	http://host.docker.internal:3000
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; font-src 'self' data:; script-src 'self'; connect-src 'self'; frame-ancestors 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; font-src 'self' data:; script-src 'self'; connect-src 'self'; frame-ancestors 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	Content-Security-Policy
Attack	
Evidence	default-src 'self'; img-src 'self' data: blob:; style-src 'self' 'unsafe-inline'; font-src 'self' data:; script-src 'self'; connect-src 'self'; frame-ancestors 'none'; base-uri 'self'; form-action 'self'
Other Info	style-src includes unsafe-inline.
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	https://www.w3.org/TR/CSP/ https://caniuse.com/#search=content+security+policy https://content-security-policy.com/ https://github.com/HtmlUnit/htmlunit-csp https://web.dev/articles/csp#resource-options
CWE Id	693
WASC Id	15
Plugin Id	10055

Low	**Dangerous JS Functions**
Description	A dangerous JS function seems to be in use that would leave the site vulnerable.
URL	http://host.docker.internal:3000/_next/static/chunks/turbopack-_cdba956c._.js
Method	GET
Parameter	
Attack	
Evidence	eval(
Other Info	

Instances	1
Solution	See the references for security advice on the use of these functions.
Reference	https://v17.angular.io/guide/security
CWE Id	749
WASC Id	
Plugin Id	10110

Low **Insufficient Site Isolation Against Spectre Vulnerability**

Description	Cross-Origin-Resource-Policy header is an opt-in header designed to counter side-channels attacks like Spectre. Resource should be specifically set as shareable amongst different origins.
URL	http://host.docker.internal:3000
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/%5Broot-of-the-server%5D__28bc9c2a._.css
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/%5Bturbopack%5D_browser_dev_hmr-client_hmr-client_ts_57d40746._.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/_a0ff3932._.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/app_favicon_ico_mjs_e98bdb63._.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/app_layout_tsx_0a548d63._.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	

Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/app_page_tsx_89f5f50e._.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_%40swc_helpers_cjs_b3dc30d6._.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_client_components_builtin_global-error_89f5f50e.js
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/media/797e433ab948586e-s.p.dbea232f.woff2
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000/_next/static/media/caa3a2e1cccd8315-s.p.853070df.woff2
Method	GET
Parameter	Cross-Origin-Resource-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000
Method	GET
Parameter	Cross-Origin-Embedder-Policy
Attack	
Evidence	
Other Info	
URL	http://host.docker.internal:3000
Method	GET
Parameter	Cross-Origin-Opener-Policy
Attack	
Evidence	
Other Info	
Instances	13

	Ensure that the application/web server sets the Cross-Origin-Resource-Policy header appropriately, and that it sets the Cross-Origin-Resource-Policy header to 'same-origin' for all web pages. 'same-site' is considered as less secured and should be avoided.
Solution	If resources must be shared, set the header to 'cross-origin'. If possible, ensure that the end user uses a standards-compliant and modern web browser that supports the Cross-Origin-Resource-Policy header (https://caniuse.com/mdn-http_headers_cross-origin-resource-policy).
Reference	https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cross-Origin-Embedder-Policy
CWE Id	693
WASC Id	14
Plugin Id	90004

Low	**Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**
Description	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
Instances	3
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework https://www.troyhunt.com/shhh-dont-let-your-response-headers/
CWE Id	497
WASC Id	13
Plugin Id	10037

Low	**Timestamp Disclosure - Unix**
Description	A timestamp was disclosed by the application/web server. - Unix
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_client_cf1d9188._.js

Method	GET
Parameter	
Attack	
Evidence	1451617521
Other Info	1451617521, which evaluates to: 2016-01-01 03:05:21.
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	https://cwe.mitre.org/data/definitions/200.html
CWE Id	497
WASC Id	13
Plugin Id	10096

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker.
URL	http://host.docker.internal:3000/_next/static/chunks/_c0136c24._.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "// Clear any previous error when user selects a valid image", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_ce688355._.js
Method	GET
Parameter	
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected in likely comment: "//# sourceMappingURL=user.js.map", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_8db7fb1f._.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in likely comment: "// TODO: Once we start tracking back/forward history at each route level,", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_b0daae9a._.js
Method	GET
Parameter	
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in likely comment: "// where rust does not have easy way to repreesnt js's 53-bit float number type for the matching", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_build_polyfills_polyfill-nomodule.js
Method	GET
Parameter	

Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//github.com/zloirock/core-js/blob/v3.38.1/LICENSE",source:"https://github.com/zloirock/core-js"})}),nt=function(t,e){return rt[", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_client_cf1d9188._.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//# sourceMappingURL=set-attributes-from-props.js.map", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_compiled_5150ccfd._.js
Method	GET
Parameter	
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in likely comment: "// TODO: rename these fields to something more meaningful.", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_compiled_next-devtools_index_a9cb0712.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "//getbootstrap.com/)\n * Copyright 2011-2019 The Bootstrap Authors\n * Copyright 2011-2019 Twitter, Inc.\n * Licensed under MIT ", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_compiled_react-dom_1e674e59._.js
Method	GET
Parameter	
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in likely comment: "//react.dev/link/invalid-hook-call for tips about how to debug and fix this problem.");", see evidence field for the suspicious comment/snippet.
URL	http://host.docker.internal:3000/_next/static/chunks/turbopack-_cdba956c._.js
Method	GET
Parameter	
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected in likely comment: "// We need to store this here instead of accessing it from the module object to:", see evidence field for the suspicious comment/snippet.
Instances	10
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	615

WASC Id	13
Plugin Id	10027

Informational **Modern Web Application**

Description	The application appears to be a modern web application. If you need to explore it automatically then the Ajax Spider may well be more effective than the standard one.
URL	http://host.docker.internal:3000/robots.txt
Method	GET
Parameter	
Attack	
Evidence	<script src="/_next/static/chunks/node_modules_next_dist_compiled_react-dom_1e674e59._.js" async=""></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	http://host.docker.internal:3000/sitemap.xml
Method	GET
Parameter	
Attack	
Evidence	<script src="/_next/static/chunks/node_modules_next_dist_compiled_react-dom_1e674e59._.js" async=""></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	2
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	10109

Informational **Non-Storable Content**

Description	The response contents are not storable by caching components such as proxy servers. If the response does not contain sensitive, personal or user-specific information, it may benefit from being stored and cached, to improve performance.
URL	http://host.docker.internal:3000
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/%5Broot-of-the-server%5D__28bc9c2a._.css
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/%5Bturbopack%5D_browser_dev_hmr-client_hmr-client_ts_57d40746._.js
Method	GET
Parameter	

Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/_a0ff3932._.js
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/app_favicon_ico_mjs_e98bdb63._.js
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/app_layout_tsx_0a548d63._.js
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/app_page_tsx_89f5f50e._.js
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_%40swc_helpers_cjs_b3dc30d6._.js
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
URL	http://host.docker.internal:3000/_next/static/chunks/node_modules_next_dist_client_components_builtin_global-error_89f5f50e.js
Method	GET
Parameter	
Attack	
Evidence	no-store
Other Info	
Instances	9
Solution	The content may be marked as storable by ensuring that the following conditions are satisfied: The request method must be understood by the cache and defined as being cacheable ("GET", "HEAD", and "POST" are currently defined as cacheable)

The response status code must be understood by the cache (one of the 1XX, 2XX, 3XX, 4XX, or 5XX response classes are generally understood)

The "no-store" cache directive must not appear in the request or response header fields

For caching by "shared" caches such as "proxy" caches, the "private" response directive must not appear in the response

For caching by "shared" caches such as "proxy" caches, the "Authorization" header field must not appear in the request, unless the response explicitly allows it (using one of the "must-revalidate", "public", or "s-maxage" Cache-Control response directives)

In addition to the conditions above, at least one of the following conditions must also be satisfied by the response:

It must contain an "Expires" header field

It must contain a "max-age" response directive

For "shared" caches such as "proxy" caches, it must contain a "s-maxage" response directive

It must contain a "Cache Control Extension" that allows it to be cached

It must have a status code that is defined as cacheable by default (200, 203, 204, 206, 300, 301, 404, 405, 410, 414, 501).

Reference
https://datatracker.ietf.org/doc/html/rfc7234
https://datatracker.ietf.org/doc/html/rfc7231
https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html

CWE Id 524

WASC Id 13

Plugin Id 10049

Informational **Storable and Cacheable Content**

Description

The response contents are storable by caching components such as proxy servers, and may be retrieved directly from the cache, rather than from the origin server by the caching servers, in response to similar requests from other users. If the response data is sensitive, personal or user-specific, this may result in sensitive information being leaked. In some cases, this may even result in a user gaining complete control of the session of another user, depending on the configuration of the caching components in use in their environment. This is primarily an issue where "shared" caching servers such as "proxy" caches are configured on the local network. This configuration is typically found in corporate or educational environments, for instance.

URL http://host.docker.internal:3000/_next/static/media/797e433ab948586e-s.p.dbea232f.woff2

Method GET

Parameter

Attack

Evidence max-age=31536000

Other Info

URL http://host.docker.internal:3000/_next/static/media/caa3a2e1cccd8315-s.p.853070df.woff2

Method GET

Parameter

Attack

Evidence max-age=31536000

Other Info

Instances 2

Solution

Validate that the response does not contain sensitive, personal or user-specific information. If it does, consider the use of the following HTTP response headers, to limit, or prevent the content being stored and retrieved from the cache by another user:

Cache-Control: no-cache, no-store, must-revalidate, private

Pragma: no-cache

	Expires: 0 This configuration directs both HTTP 1.0 and HTTP 1.1 compliant caching servers to not store the response, and to not retrieve the response (without validation) from the cache, in response to a similar request.
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049
Informational	Storable but Non-Cacheable Content
Description	The response contents are storable by caching components such as proxy servers, but will not be retrieved directly from the cache, without validating the request upstream, in response to similar requests from other users.
URL	http://host.docker.internal:3000/favicon.ico?favicon.0b3bf435.ico
Method	GET
Parameter	
Attack	
Evidence	max-age=0
Other Info	
Instances	1
Solution	
Reference	https://datatracker.ietf.org/doc/html/rfc7234 https://datatracker.ietf.org/doc/html/rfc7231 https://www.w3.org/Protocols/rfc2616/rfc2616-sec13.html
CWE Id	524
WASC Id	13
Plugin Id	10049

Sequence Details

With the associated active scan results.

ESLint Security Findings (JSON)


```
[
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\__tests__\\imageUpla
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\__tests__\\inputFiel
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
```

```
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\__tests__\\profileFo
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\__tests__\\profilePr
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\__tests__\\socialFie
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\__tests__\\textarea.
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\app\\layout.tsx",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\app\\page.tsx",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\ProfileF
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
```

```
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\ProfileP
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
      "warningCount": 0,
      "fixableErrorCount": 0,
      "fixableWarningCount": 0,
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\input-fi
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
      "warningCount": 0,
      "fixableErrorCount": 0,
      "fixableWarningCount": 0,
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\input-fi
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
      "warningCount": 0,
      "fixableErrorCount": 0,
      "fixableWarningCount": 0,
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\input-fi
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
      "warningCount": 0,
      "fixableErrorCount": 0,
      "fixableWarningCount": 0,
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\input-fi
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
      "warningCount": 0,
      "fixableErrorCount": 0,
      "fixableWarningCount": 0,
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\input-fi
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
      "warningCount": 0,
      "fixableErrorCount": 0,
      "fixableWarningCount": 0,
      "usedDeprecatedRules": []
    },
    {
      "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\components\\input-fi
      "messages": [],
      "suppressedMessages": [],
      "errorCount": 0,
      "fatalErrorCount": 0,
```

```
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\eslint.config.mjs",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\jest.config.ts",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\jest.setup.ts",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\next.config.ts",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\postcss.config.mjs",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\scripts\\security-re
    "messages": [
      {
        "ruleId": "@typescript-eslint/no-require-imports",
        "severity": 2,
        "message": "A `require()` style import is forbidden.",
        "line": 1,
        "column": 12,
        "nodeType": "CallExpression",
        "messageId": "noRequireImports",
        "endLine": 1,
        "endColumn": 25
      },
```

```
      {
        "ruleId": "@typescript-eslint/no-require-imports",
        "severity": 2,
        "message": "A `require()` style import is forbidden.",
        "line": 2,
        "column": 14,
        "nodeType": "CallExpression",
        "messageId": "noRequireImports",
        "endLine": 2,
        "endColumn": 29
      },
      {
        "ruleId": "@typescript-eslint/no-require-imports",
        "severity": 2,
        "message": "A `require()` style import is forbidden.",
        "line": 3,
        "column": 19,
        "nodeType": "CallExpression",
        "messageId": "noRequireImports",
        "endLine": 3,
        "endColumn": 39
      }
    ],
    "suppressedMessages": [],
    "errorCount": 3,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "source": "const fs = require('fs');\r\nconst path = require('path');\r\nconst puppeteer = require(

ZAP report not found. Run security:zap.

';\r\n  const zapJson = fs.existsSync(zapJsonPath)\r\n    ? JSON.parse(fs.readFileSync(zapJsonPath, 'ut
```


Security Assessment Report

\r\n
\r\n

ESLint Security Issues: ${summary.eslintIssues}

\r\n

ZAP Alerts: ${summary.zapAlerts}

\r\n
\r\n\r\n
\r\n

OWASP ZAP Baseline Report

\r\n ${zapHtml}\r\n
\r\n\r\n
\r\n

ESLint Security Findings (JSON)

\r\n


```
  ${eslintData ? JSON.stringify(eslintData, null, 2) : 'No eslint.json found'}
```


\r\n
\r\n   \r\n `;\r\n\r\n const outHtml = path.join(artifactsDir, 'security-report.html');\r\n fs.writ


```
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\security-tests\\unit
    "messages": [
      {
```

```
        "ruleId": "@typescript-eslint/ban-ts-comment",
        "severity": 2,
        "message": "Use \"@ts-expect-error\" instead of \"@ts-ignore\", as \"@ts-ignore\" will do nothi
        "line": 5,
        "column": 5,
        "nodeType": "Line",
        "messageId": "tsIgnoreInsteadOfExpectError",
        "endLine": 5,
        "endColumn": 48,
        "suggestions": [
          {
            "messageId": "replaceTsIgnoreWithTsExpectError",
            "fix": {
              "range": [
                161,
                204
              ],
              "text": "// @ts-expect-error headers exists per NextConfig"
            },
            "desc": "Replace \"@ts-ignore\" with \"@ts-expect-error\"."
          }
        ]
      }
    ],
    "suppressedMessages": [],
    "errorCount": 1,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "source": "import nextConfig from '../../next.config';\r\n\r\ndescribe('Security Headers', () => {\
    "usedDeprecatedRules": []
  },
  {
    "filePath": "C:\\Projects\\Nextjs\\TestDrivenDevelopment\\nextjs_unit_testing\\types\\global.ts",
    "messages": [],
    "suppressedMessages": [],
    "errorCount": 0,
    "fatalErrorCount": 0,
    "warningCount": 0,
    "fixableErrorCount": 0,
    "fixableWarningCount": 0,
    "usedDeprecatedRules": []
  }
]
```