



# All Components tested

Sites: <http://localhost:3000> <http://localhost:8000>

Generated on Thu, 19 Dec 2024 05:50:09

ZAP Version: 2.15.0

ZAP by [Checkmarx](#)

## Summary of Alerts

Risk Level	Number of Alerts
High	1
Medium	4
Low	4
Informational	5

## Alerts

Name	Risk Level	Number of Instances
<a href="#">Cloud Metadata Potentially Exposed</a>	High	1
<a href="#">CSP: Wildcard Directive</a>	Medium	13
<a href="#">Content Security Policy (CSP) Header Not Set</a>	Medium	9
<a href="#">Directory Browsing</a>	Medium	2
<a href="#">Missing Anti-clickjacking Header</a>	Medium	8
<a href="#">Cookie without SameSite Attribute</a>	Low	19
<a href="#">Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)</a>	Low	46
<a href="#">Timestamp Disclosure - Unix</a>	Low	1
<a href="#">X-Content-Type-Options Header Missing</a>	Low	73
<a href="#">Information Disclosure - Suspicious Comments</a>	Informational	83
<a href="#">Loosely Scoped Cookie</a>	Informational	122
<a href="#">Modern Web Application</a>	Informational	8
<a href="#">Session Management Response Identified</a>	Informational	102
<a href="#">User Agent Fuzzer</a>	Informational	160

## Alert Detail

High	Cloud Metadata Potentially Exposed
Description	The Cloud Metadata Attack attempts to abuse a misconfigured NGINX server in order to access the instance metadata maintained by cloud service providers such as AWS, GCP and Azure.

	All of these providers provide metadata via an internal unroutable IP address '169.254.169.254' - this can be exposed by incorrectly configured NGINX servers and accessed by using this IP address in the Host header field.
URL	<a href="http://localhost:3000/latest/meta-data/">http://localhost:3000/latest/meta-data/</a>
Method	GET
Attack	169.254.169.254
Evidence	
Other Info	Based on the successful response status code cloud metadata may have been returned in the response. Check the response data to see if any cloud metadata has been returned. The meta data returned can include information that would allow an attacker to completely compromise the system.
Instances	1
Solution	Do not trust any user data in NGINX configs. In this case it is probably the use of the \$host variable which is set from the 'Host' header and can be controlled by an attacker.
Reference	<a href="https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/">https://www.nginx.com/blog/trust-no-one-perils-of-trusting-user-input/</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">90034</a>

<b>Medium</b>	<b>CSP: Wildcard Directive</b>
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	<a href="http://localhost:8000/accountant/payments/3/adjust">http://localhost:8000/accountant/payments/3/adjust</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/accountant/payments/5/adjust">http://localhost:8000/accountant/payments/5/adjust</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/accountant/payments/adjustments">http://localhost:8000/accountant/payments/adjustments</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL	<a href="http://localhost:8000/auth/login">http://localhost:8000/auth/login</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/auth/register">http://localhost:8000/auth/register</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/auth/staff/login">http://localhost:8000/auth/staff/login</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/books">http://localhost:8000/books</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/favicon.ico">http://localhost:8000/favicon.ico</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/purchaseMan/createMedia">http://localhost:8000/purchaseMan/createMedia</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.

URL	<a href="http://localhost:8000/purchaseMan/purchaseOrder">http://localhost:8000/purchaseMan/purchaseOrder</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/purchaseMan/updateOrderStatus">http://localhost:8000/purchaseMan/updateOrderStatus</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	default-src 'none'
Other Info	The following directives either allow wildcard sources (or ancestors), are not defined, or are overly broadly defined: frame-ancestors, form-action The directive(s): frame-ancestors, form-action are among the directives that do not fallback to default-src, missing/excluding them is the same as allowing anything.
Instances	13
Solution	Ensure that your web server, application server, load balancer, etc. is properly configured to set the Content-Security-Policy header.
Reference	<a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://caniuse.com/#search=content+security+policy">https://caniuse.com/#search=content+security+policy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a> <a href="https://github.com/HtmlUnit/htmlunit-csp">https://github.com/HtmlUnit/htmlunit-csp</a> <a href="https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources">https://developers.google.com/web/fundamentals/security/csp#policy_applies_to_a_wide_variety_of_resources</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10055</a>

Medium	Content Security Policy (CSP) Header Not Set
Description	Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page

	— covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.
URL	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	
Evidence	
Other Info	

URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:8000/wishlist/getWishlist">http://localhost:8000/wishlist/getWishlist</a>
Method	GET
Attack	
Evidence	
Other Info	
Instances	9
Solution	Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy">https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy</a> <a href="https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html</a> <a href="https://www.w3.org/TR/CSP/">https://www.w3.org/TR/CSP/</a> <a href="https://w3c.github.io/webappsec-csp/">https://w3c.github.io/webappsec-csp/</a> <a href="https://web.dev/articles/csp">https://web.dev/articles/csp</a> <a href="https://caniuse.com/#feat=contentsecuritypolicy">https://caniuse.com/#feat=contentsecuritypolicy</a> <a href="https://content-security-policy.com/">https://content-security-policy.com/</a>
CWE Id	<a href="#">693</a>
WASC Id	15
Plugin Id	<a href="#">10038</a>

<b>Medium</b>	<b>Directory Browsing</b>
Description	It is possible to view the directory listing. Directory listing may reveal hidden scripts, include files, backup source files, etc. which can be accessed to read sensitive information.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js/">http://localhost:3000/_next/static/chunks/pages/catalog.js/</a>
Method	GET
Attack	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js/">http://localhost:3000/_next/static/chunks/pages/catalog.js/</a>
Evidence	directory
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js/">http://localhost:3000/_next/static/chunks/pages/index.js/</a>
Method	GET
Attack	<a href="http://localhost:3000/_next/static/chunks/pages/index.js/">http://localhost:3000/_next/static/chunks/pages/index.js/</a>
Evidence	directory
Other Info	
Instances	2
Solution	Disable directory browsing. If this is required, make sure the listed files does not induce risks.
Reference	<a href="https://httpd.apache.org/docs/mod/core.html#options">https://httpd.apache.org/docs/mod/core.html#options</a>
CWE Id	<a href="#">548</a>

WASC Id	48
Plugin Id	<a href="#">0</a>

Medium	Missing Anti-clickjacking Header
Description	The response does not protect against 'ClickJacking' attacks. It should include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options.
URL	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET

Attack	
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	
Evidence	
Other Info	
Instances	8
Solution	<p>Modern Web browsers support the Content-Security-Policy and X-Frame-Options HTTP headers. Ensure one of them is set on all web pages returned by your site/app.</p> <p>If you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. Alternatively consider implementing Content Security Policy's "frame-ancestors" directive.</p>
Reference	<a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options</a>
CWE Id	<a href="#">1021</a>
WASC Id	15
Plugin Id	<a href="#">10020</a>

<b>Low</b>	<b>Cookie without SameSite Attribute</b>
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	<a href="http://localhost:8000">http://localhost:8000</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/accountant/members">http://localhost:8000/accountant/members</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/3/adjust">http://localhost:8000/accountant/payments/3/adjust</a>
Method	GET



Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books">http://localhost:8000/books</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/29">http://localhost:8000/books/29</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid

Other Info	
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/branches">http://localhost:8000/purchaseMan/branches</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/vendors">http://localhost:8000/purchaseMan/vendors</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	

URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	Set-Cookie: connect.sid
Other Info	
Instances	19
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	<a href="https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site">https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site</a>
CWE Id	<a href="#">1275</a>
WASC Id	13
Plugin Id	<a href="#">10054</a>

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	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	

Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	
Evidence	X-Powered-By: Next.js
Other Info	
URL	<a href="http://localhost:8000">http://localhost:8000</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/members">http://localhost:8000/accountant/members</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/3/adjust">http://localhost:8000/accountant/payments/3/adjust</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other	

Info	
URL	<a href="http://localhost:8000/accountant/payments/5/adjust">http://localhost:8000/accountant/payments/5/adjust</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/adjustments">http://localhost:8000/accountant/payments/adjustments</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/analytics">http://localhost:8000/accountant/payments/analytics</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/extendedAnalytics?timeFrame=today">http://localhost:8000/accountant/payments/extendedAnalytics?timeFrame=today</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/history">http://localhost:8000/accountant/payments/history</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/history/20">http://localhost:8000/accountant/payments/history/20</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/methods">http://localhost:8000/accountant/payments/methods</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/payments/outstanding">http://localhost:8000/accountant/payments/outstanding</a>

Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/accountant/reports/export?type=revenue&amp;timeFrame=month">http://localhost:8000/accountant/reports/export?type=revenue&amp;timeFrame=month</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/auth/login">http://localhost:8000/auth/login</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/auth/register">http://localhost:8000/auth/register</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/auth/staff/login">http://localhost:8000/auth/staff/login</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books">http://localhost:8000/books</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/29">http://localhost:8000/books/29</a>
Method	GET

Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express

Other Info	
URL	<a href="http://localhost:8000/books/search?query=j">http://localhost:8000/books/search?query=j</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/favicon.ico">http://localhost:8000/favicon.ico</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/branches">http://localhost:8000/purchaseMan/branches</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/createMedia">http://localhost:8000/purchaseMan/createMedia</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/orderDetails/3">http://localhost:8000/purchaseMan/orderDetails/3</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/purchaseOrder">http://localhost:8000/purchaseMan/purchaseOrder</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	



URL	<a href="http://localhost:8000/purchaseMan/updateOrderStatus">http://localhost:8000/purchaseMan/updateOrderStatus</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/purchaseMan/vendors">http://localhost:8000/purchaseMan/vendors</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
URL	<a href="http://localhost:8000/wishlist/getWishlist">http://localhost:8000/wishlist/getWishlist</a>
Method	GET
Attack	
Evidence	X-Powered-By: Express
Other Info	
Instances	46
Solution	Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.
Reference	<a href="https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework">https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/08-Fingerprint_Web_Application_Framework</a> <a href="https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html">https://www.troyhunt.com/2012/02/shhh-dont-let-your-response-headers.html</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10037</a>

<b>Low</b>	<b>Timestamp Disclosure - Unix</b>
Description	A timestamp was disclosed by the application/web server. - Unix
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET

Attack	
Evidence	1719601643
Other Info	1719601643, which evaluates to: 2024-06-28 20:07:23.
Instances	1
Solution	Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.
Reference	<a href="https://cwe.mitre.org/data/definitions/200.html">https://cwe.mitre.org/data/definitions/200.html</a>
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10096</a>

<b>Low</b>	<b>X-Content-Type-Options Header Missing</b>
Description	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.
URL	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their declared content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their declared content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitHookEffectListMount&amp;arguments=&amp;lineNumber=10732&amp;column=29">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitHookEffectListMount&amp;arguments=&amp;lineNumber=10732&amp;column=29</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their declared content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitHookPassiveMountEffects&amp;arguments=&amp;lineNumber=10852&amp;column=29">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitHookPassiveMountEffects&amp;arguments=&amp;lineNumber=10852&amp;column=29</a>
Method	GET
Attack	
Evidence	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitPassiveMountOnFiber&amp;arguments=&amp;lineNumber=12620&amp;column=11">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitPassiveMountOnFiber&amp;arguments=&amp;lineNumber=12620&amp;column=11</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitPassiveMountOnFiber&amp;arguments=&amp;lineNumber=12627&amp;column=13">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitPassiveMountOnFiber&amp;arguments=&amp;lineNumber=12627&amp;column=13</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitPassiveMountOnFiber&amp;arguments=&amp;lineNumber=12729&amp;column=11">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=commitPassiveMountOnFiber&amp;arguments=&amp;lineNumber=12729&amp;column=11</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=recursivelyTraversePassiveMountEffects&amp;arguments=&amp;lineNumber=12601&amp;column=11">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=recursivelyTraversePassiveMountEffects&amp;arguments=&amp;lineNumber=12601&amp;column=11</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=runWithFiberInDEV&amp;arguments=&amp;lineNumber=544&amp;column=16">http://localhost:3000/_nextjs_original-stack-frame?isServer=false&amp;isEdgeServer=false&amp;isAppDirectory=false&amp;errorMessage=TypeError%3A+Failed+to+fetch&amp;file=webpack-internal%3A%2F%2F%2F.%2Fnode_modules%2Freact-dom%2Freact-dom-client.development.js&amp;methodName=runWithFiberInDEV&amp;arguments=&amp;lineNumber=544&amp;column=16</a>
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F0083%2F9780008380809.jpg&amp;w=384&amp;q=75">http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F0083%2F9780008380809.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F0919%2F9780091956141.jpg&amp;w=384&amp;q=75">http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F0919%2F9780091956141.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F1411%2F9780141182636.jpg&amp;w=384&amp;q=75">http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F1411%2F9780141182636.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F3409%2F9780340960196.jpg&amp;w=384&amp;q=75">http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F3409%2F9780340960196.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F7123%2F9780712355568.jpg&amp;w=384&amp;q=75">http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9780%2F7123%2F9780712355568.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9781%2F5291%2F9781529157468.jpg&amp;w=384&amp;q=75">http://localhost:3000/next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9781%2F5291%2F9781529157468.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	

Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9781%2F8049%2F9781804990926.jpg&amp;w=384&amp;q=75">http://localhost:3000/_next/image?url=https%3A%2F%2Fcdn.waterstones.com%2Fbookjackets%2Flarge%2F9781%2F8049%2F9781804990926.jpg&amp;w=384&amp;q=75</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book/%5BbookId%5D.js">http://localhost:3000/_next/static/chunks/pages/book/%5BbookId%5D.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js">http://localhost:3000/_next/static/chunks/pages/catalog.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js">http://localhost:3000/_next/static/chunks/pages/index.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/login.js">http://localhost:3000/_next/static/chunks/pages/staff/login.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/react-refresh.js">http://localhost:3000/_next/static/chunks/react-refresh.js</a>
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/development/_buildManifest.js">http://localhost:3000/_next/static/development/_buildManifest.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/development/_devMiddlewareManifest.json">http://localhost:3000/_next/static/development/_devMiddlewareManifest.json</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/development/_devPagesManifest.json">http://localhost:3000/_next/static/development/_devPagesManifest.json</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/development/_ssgManifest.js">http://localhost:3000/_next/static/development/_ssgManifest.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/0d5870edbbaf5874.webpack.hot-update.json">http://localhost:3000/_next/static/webpack/0d5870edbbaf5874.webpack.hot-update.json</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/0ea99626dcc6cae0.webpack.hot-update.json">http://localhost:3000/_next/static/webpack/0ea99626dcc6cae0.webpack.hot-update.json</a>
Method	GET



Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/653202093d51266b.webpack.hot-update.json">http://localhost:3000/_next/static/webpack/653202093d51266b.webpack.hot-update.json</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/f3029ff52cb4ba1d.webpack.hot-update.json">http://localhost:3000/_next/static/webpack/f3029ff52cb4ba1d.webpack.hot-update.json</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.0d5870edbbaf5874.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.0d5870edbbaf5874.hot-update.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.0ea99626dcc6cae0.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.0ea99626dcc6cae0.hot-update.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.653202093d51266b.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.653202093d51266b.hot-update.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.f3029ff52cb4ba1d.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.f3029ff52cb4ba1d.hot-update.js</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.



URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/favicon.ico">http://localhost:3000/favicon.ico</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000">http://localhost:8000</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/members">http://localhost:8000/accountant/members</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments/analytics">http://localhost:8000/accountant/payments/analytics</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments/extendedAnalytics?timeFrame=today">http://localhost:8000/accountant/payments/extendedAnalytics?timeFrame=today</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments/history">http://localhost:8000/accountant/payments/history</a>
Method	GET

Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments/history/20">http://localhost:8000/accountant/payments/history/20</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments/methods">http://localhost:8000/accountant/payments/methods</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/payments/outstanding">http://localhost:8000/accountant/payments/outstanding</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/accountant/reports/export?type=revenue&amp;timeFrame=month">http://localhost:8000/accountant/reports/export?type=revenue&amp;timeFrame=month</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/29">http://localhost:8000/books/29</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.

URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	

Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by browser sniffing injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/books/search?query=j">http://localhost:8000/books/search?query=j</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by browser sniffing injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/purchaseMan/branches">http://localhost:8000/purchaseMan/branches</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by browser sniffing injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/purchaseMan/orderDetails/3">http://localhost:8000/purchaseMan/orderDetails/3</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by browser sniffing injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by browser sniffing injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
URL	<a href="http://localhost:8000/purchaseMan/vendors">http://localhost:8000/purchaseMan/vendors</a>
Method	GET
Attack	
Evidence	
Other Info	This issue still applies to error type pages (401, 403, 500, etc.) as those pages are often still affected by browser sniffing injection issues, in which case there is still concern for browsers sniffing pages away from their intended content type. At "High" threshold this scan rule will not alert on client or server error responses.
Instances	73
Solution	<p>Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the Content-Type-Options header to 'nosniff' for all web pages.</p> <p>If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.</p>
Reference	<a href="https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)">https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)</a> <a href="https://owasp.org/www-community/Security_Headers">https://owasp.org/www-community/Security_Headers</a>
CWE Id	<a href="#">693</a>

WASC Id	15
Plugin Id	<a href="#">10021</a>

Informational	Information Disclosure - Suspicious Comments
Description	The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.
URL	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{},"page":"/","query":{},"buildId":"development","next", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{},"page":"/","query":{},"buildId":"development","next", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	Bug
Other Info	The following pattern was used: \bBUG\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("/ * eslint-disable * / // @ts-nocheck\n// Copied from https://github.com/medialize/ally.js\n// Licens", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 23 times, the first in the element starting with: "eval(__webpack_require__.ts("\trimStart\in String.prototype )(String.prototype.trimStart=String.prototype.trimLeft),\trimEnd\", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 106 times, the first in the element starting with: "eval(__webpack_require__.ts("\nObject.defineProperty(exports, \n__esModule\", {\n value: true\n});\nObject.defineProperty(e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET

Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected 12 times, the first in the element starting with: "eval(__webpack_require__.ts("\nObject.defineProperty(exports, \"__esModule\", ({\n value: true\n}));\n0 && (0);\nfunction _ex", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 3 times, the first in the element starting with: " * If you are trying to read the output file, select a different devtool ( <a href="https://webpack.js.org/configuration/devtool/">https://webpack.js.org/configuration/devtool/</a> )", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 19 times, the first in the element starting with: "eval(__webpack_require__.ts("\nvar _s = \$RefreshSig\$();\n\"use strict\";\nObject.defineProperty(exports, \"__esModule\", ({\n ", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("\nvar _s = \$RefreshSig\$();\n\"use strict\";\nObject.defineProperty(exports, \"__esModule\", ({\n ", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "eval(__webpack_require__.ts("\nObject.defineProperty(exports, \"__esModule\", ({\n value: true\n}));\n0 && (0);\nfunction _ex", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/main.js">http://localhost:3000/_next/static/chunks/main.js</a>
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("\nObject.defineProperty(exports, \"__esModule\", ({\n value: true\n}));\n0 && (0);\nfunction _ex", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	

Evidence	admin
Other Info	The following pattern was used: \bADMIN\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("/**\n * The functions provided by this module are used to communicate certain properties\n * about ", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	bugs
Other Info	The following pattern was used: \bBUGS\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("\n\nvar _interopRequireDefault = __webpack_require__(/?! @babel/runtime/helpers/interopRequireDefau", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 17 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 77 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	



Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 5 times, the first in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("/*\n MIT License http://www.opensource.org/licenses/mit-license.php\n Author Tobias Koppers @sokr", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 10 times, the first in the element starting with: "/* */ ./node_modules/lucide-react/dist/esm/icons/user.js":", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("\nvar _s = \$RefreshSig\$();\n\n"use strict";\nObject.defineProperty(exports, \"__esModule\", {\n \" , see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book/%5BbookId%5D.js">http://localhost:3000/_next/static/chunks/pages/book/%5BbookId%5D.js</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book/%5BbookId%5D.js">http://localhost:3000/_next/static/chunks/pages/book/%5BbookId%5D.js</a>
Method	GET
Attack	
Evidence	select

Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js">http://localhost:3000/_next/static/chunks/pages/catalog.js</a>
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("/ * __next_internal_client_entry_do_not_use__ cjs */\nObject.defineProperty(exports, \"__esModule\", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js">http://localhost:3000/_next/static/chunks/pages/catalog.js</a>
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval(__webpack_require__.ts("var __dirname = \"^\";\n/* provided dependency */ var process = __webpack_require__(/*! process */ ", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js">http://localhost:3000/_next/static/chunks/pages/catalog.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("/ **\n * A shared function, used on both client and server, to generate a SVG blur placeholder.\n */", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js">http://localhost:3000/_next/static/chunks/pages/catalog.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/catalog.js">http://localhost:3000/_next/static/chunks/pages/catalog.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("\nObject.defineProperty(exports, \"__esModule\", ({\n value: true\n}));\n0 && (0);\nfunction _ex", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js">http://localhost:3000/_next/static/chunks/pages/index.js</a>
Method	GET
Attack	
Evidence	bug
Other Info	The following pattern was used: \bBUG\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("/ * __next_internal_client_entry_do_not_use__ cjs */\nObject.defineProperty(exports, \"__esModule\", see evidence field for the suspicious comment/snippet.

	comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js">http://localhost:3000/_next/static/chunks/pages/index.js</a>
Method	GET
Attack	
Evidence	debug
Other Info	The following pattern was used: \bDEBUG\b and was detected in the element starting with: "eval(__webpack_require__.ts("var __dirname = \"^\";\n/* provided dependency */ var process = __webpack_require__(/*! process */ ", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js">http://localhost:3000/_next/static/chunks/pages/index.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("/*\n * A shared function, used on both client and server, to generate a SVG blur placeholder.\n */", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js">http://localhost:3000/_next/static/chunks/pages/index.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/index.js">http://localhost:3000/_next/static/chunks/pages/index.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("\nObject.defineProperty(exports, \"__esModule\", {\n value: true\n});\n0 && (0);\nfunction _ex", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 12 times, the first in the element starting with: "eval(__webpack_require__.ts("var __dirname = \"^\";\n(function(){var e={675:function(e,r){\"use strict\";r.byteLength=byteLength", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 8 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.

URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 66 times, the first in the element starting with: " * If you are trying to read the output file, select a different devtool ( <a href="https://webpack.js.org/configuration/devtool/">https://webpack.js.org/configuration/devtool/</a> )", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js">http://localhost:3000/_next/static/chunks/pages/staff/CreateOrder.js</a>
Method	GET
Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/login.js">http://localhost:3000/_next/static/chunks/pages/staff/login.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/login.js">http://localhost:3000/_next/static/chunks/pages/staff/login.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/login.js">http://localhost:3000/_next/static/chunks/pages/staff/login.js</a>

Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool ( <a href="https://webpack.js.org/configuration/devtool/">https://webpack.js.org/configuration/devtool/</a> )", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 12 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 67 times, the first in the element starting with: " * If you are trying to read the output file, select a different devtool ( <a href="https://webpack.js.org/configuration/devtool/">https://webpack.js.org/configuration/devtool/</a> )", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js">http://localhost:3000/_next/static/chunks/pages/staff/ManageMemberships.js</a>
Method	GET

Attack	
Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 12 times, the first in the element starting with: "eval(__webpack_require__.ts("var __dirname = \"^\";\n(function(){var e={675:function(e,r){\"use strict\";r.byteLength=byteLength", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 5 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	
Evidence	User
Other Info	The following pattern was used: \bUSER\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js">http://localhost:3000/_next/static/chunks/pages/staff/Payment-reconciliation.js</a>
Method	GET
Attack	

Evidence	where
Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 12 times, the first in the element starting with: "eval(__webpack_require__.ts("var __dirname = \"\";\n(function(){var e={675:function(e,r){\"use strict\";r.byteLength=byteLength", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 6 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 67 times, the first in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 3 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Reports.js">http://localhost:3000/_next/static/chunks/pages/staff/Reports.js</a>
Method	GET
Attack	
Evidence	where

Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 12 times, the first in the element starting with: "eval(__webpack_require__.ts("var __dirname = \"^\";\n(function(){var e={675:function(e,r){\"use strict\";r.byteLength=byteLength", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 5 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected 66 times, the first in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	user
Other Info	The following pattern was used: \bUSER\b and was detected 4 times, the first in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	username
Other Info	The following pattern was used: \bUSERNAME\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js">http://localhost:3000/_next/static/chunks/pages/staff/Tracking.js</a>
Method	GET
Attack	
Evidence	where



Other Info	The following pattern was used: \bWHERE\b and was detected in the element starting with: "eval(__webpack_require__.ts("__webpack_require__.r(__webpack_exports__);\n/* harmony export */ __webpack_require__.d(__webpack_e", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/react-refresh.js">http://localhost:3000/_next/static/chunks/react-refresh.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/react-refresh.js">http://localhost:3000/_next/static/chunks/react-refresh.js</a>
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected 2 times, the first in the element starting with: "eval(__webpack_require__.ts("\n/**\n * MIT License\n *\n * Copyright (c) Facebook, Inc. and its affiliates.\n *\n * Permission i", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	
Evidence	from
Other Info	The following pattern was used: \bFROM\b and was detected 6 times, the first in the element starting with: "/*****/ " ) from disposed module " +", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	
Evidence	later
Other Info	The following pattern was used: \bLATER\b and was detected 3 times, the first in the element starting with: "/*****/ // create error before stack unwound to get useful stacktrace later", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	
Evidence	TODO
Other Info	The following pattern was used: \bTODO\b and was detected in the element starting with: "/*****/ /** @type {TODO} */", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.0d5870edbbaf5874.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.0d5870edbbaf5874.hot-update.js</a>

Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.0ea99626dcc6cae0.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.0ea99626dcc6cae0.hot-update.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.653202093d51266b.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.653202093d51266b.hot-update.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/_next/static/webpack/webpack.f3029ff52cb4ba1d.hot-update.js">http://localhost:3000/_next/static/webpack/webpack.f3029ff52cb4ba1d.hot-update.js</a>
Method	GET
Attack	
Evidence	select
Other Info	The following pattern was used: \bSELECT\b and was detected in the element starting with: " * If you are trying to read the output file, select a different devtool (https://webpack.js.org/configuration/devtool/)", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{},"page":"/staff/CreateOrder","query":{},"buildId":"d", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{},"page":"/staff/login","query":{},"buildId":"develop", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	
Evidence	query

Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{}}, "page":"/staff/ManageMemberships", "query":{},"build", see evidence field for the suspicious comment/snippet.
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{}}, "page":"/staff/Payment-reconciliation", "query":{},"", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{}}, "page":"/staff/Reports", "query":{},"buildId":"devel", see evidence field for the suspicious comment /snippet.
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	
Evidence	query
Other Info	The following pattern was used: \bQUERY\b and was detected in the element starting with: "<script id="__NEXT_DATA__" type="application/json">{"props":{"pageProps":{}}, "page":"/staff/Tracking", "query":{},"buildId":"deve", see evidence field for the suspicious comment /snippet.
Instances	83
Solution	Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.
Reference	
CWE Id	<a href="#">200</a>
WASC Id	13
Plugin Id	<a href="#">10027</a>

Informational	Loosely Scoped Cookie
Description	Cookies can be scoped by domain or path. This check is only concerned with domain scope. The domain scope applied to a cookie determines which domains can access it. For example, a cookie can be scoped strictly to a subdomain e.g. www.nottrusted.com, or loosely scoped to a parent domain e.g. nottrusted.com. In the latter case, any subdomain of nottrusted.com can access the cookie. Loosely scoped cookies are common in mega-applications like google.com and live.com. Cookies set from a subdomain like app.foo.bar are transmitted only to that domain by the browser. However, cookies scoped to a parent-level domain may be transmitted to the parent, or any subdomain of the parent.
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other	The origin domain used for comparison was: localhost next-auth.csrf-token=07775c4aa2c147c44bfc048a3919ad5d024e60ab46a5696757cc27698c68eb13%

Info	7C9954470390691f1e4cf1ec8d3e73af33edf42a405a9d7c19919fc05aa1efb839 next-auth. callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf- token=1f3c8419cd86a12ae140b76c25060c450fcb8ac14ec7f0dcf72fbefa996a04% 7Cfe591d3cefab1cd3c01693cda993564ab2786ef407810c223757238ddeb9ddc next-auth. callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf- token=276ac804dc1db56b90638c137abb65c051bcb48b5094c99efcb3f2e490838a3e% 7C494f53a391a8547403db9a8914fd91c8e206cf676c699a06e776487e151993bb next-auth. callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf- token=278d9660a55f6787b3c01dc9e275846d6b58f0a5ae632256759058b3bc4ea194% 7C6b75e2bffb75c17e582ead64a510d607b4856176d29f3ec1ddbb684a5e23ac3f next-auth. callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf- token=2a4f691ce40a3254ad896ee2d2d93cf284aee201af941e9870111a80905745ea% 7C0013e640ee45e10128d257f866055fb38b9a63856bce3cf79433b07ed0f76791 next-auth. callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf- token=2d752bb69754f2437129e3b00a600654adef57bc07cf8f7ce71bccf9ccfd01e1% 7C9d0caaa82d52fedde24934ea7d73d5926967d81463c98a4a3cf7863809baae86 next-auth. callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf- token=51b4217aec9be0ea4753a242cbe7eb8269d10e06091067617297d02578e2cfd1% 7Cba219249bbcaec6480c230cb3bb38a2f1a690062bd36863e166c59682480713 next-

	auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=6b65140fb7cf6c6bd0db80033dd79b4e72158c1bbf0079a06b3cec368d2beff1%7C085936a9f3b883d37d43ba55df472309eb424606f63693ae32be5938995f9f4e next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=7aa71aa411b9128a7b752f3b01b84a13dbc46addd6ee33e24b78651848ba86b2%7C3a72b3848d910559beb5699e7eed612c7549b587dee0cee2614742745cb1e6b2 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=81124b39d221c312f75994181e511f6b142b31457faa8eeb5cd4ef38f2a44484%7C064c0efb6f2c3349ae8c5e3f48231f33bc475a58a201ee589d0874d2c6513a2f next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=8328848b6ea1138b010f15f766fd6ec7650ee2e5fb3d10f2e38c655b691c4f76%7C61a8794cb5b36b789c8a468a447d12f8430449697a8dd2b18164455422005c63 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=90dd230200372bf8adb213b651be522899704321e8f0bd930cab715627934495%7C88d9568a81881389c5bec1b3ab73b8da8f38f39aa87b1e1aaaf1e172e43f27ac next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=929659e1de81f8e15fc8bd9cdc406842298a52034a5a14136cb9bd4f0bf97e9b%7C6e8c0d22338351e8afa1e8914bc12722d29a149534686f039fd216f75f2d374d next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000

URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=aece030e061ee6a8a8d4c3193f34bd60e3553d8931eba349814f32119d138aa4%7C7e8ff52749c0cd2b5b56c077dc3bce27fae89dc2081b2b03e677c3dbeabaf989 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=b8094dea3f95cee24b78203980681e01deac3a3d3516b2d38b5ebc736b2fecad%7C7f9cabf59f8f5d501ee55ad91163b87a86ce73c4f8a3228a1e0e8f430d8a157d next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=ba874504d43361f25e5b7032d39bb384416318b5f90bb0ecff8b4c052f261b32%7C18ab4ba5aeb91b145cb2583f3c94895926ac9e6b622a4c097bae64df1c9816cb next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=c449d832191d3722e8a64b0304902229dac417f2faab911032c9ffaf30e316ee%7Ce6fa0a52bf4bd36ece63f9f4788895f70594ca382cc4a5d0780b5ecf40604c0e next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=cc31518e86ab7b24e39b94ff618b81d3057e9c093b3a0843dc5e3b823ea52d05%7C8ae572cff40cc33e8f68604df137bc11b042fad8d5c071f46c9cb4157a296d01 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=d4f2c35e5bb3fcc18d58c9081cc3d020c53c4b21dc57e7406ed42dfd624f7825%7Ca68391bcd0a58a5553d2f1e57b15d023710c30c5f150f31e1921363d6573e09f next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000

URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=e2c013b6a2fdc09ee23f66385f64ab714d55a1a41a02f25b5d465634b54ab493%7C96e58c055f83a2d526950c5eb7ae7d5f46b3e3b1a405cc4ddb93129f70d5cfb2 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=f366dec59e7d19aca23d19f0d5cad359d030de149101c4864a109e96cd77ff4c%7C1e67390658b1e8fac9e2247abfc62fb2ab6beff79e2451a9b04734de0caffaff next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost next-auth.csrf-token=f5154491e2a9c4cb27d4746c498be2955ba8d42120364606c989da4779caa4cd%7C52da2aaa2c609c97ccecea2a76038f3e6cba174a8df71649e11db3cff8f33af9 next-auth.callback-url=http%3A%2F%2Flocalhost%3A3000
URL	<a href="http://localhost:8000">http://localhost:8000</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AtNnLak15q_UUn1wr9Y81O2eY7r_dBXdl.M5VkrjWNDdkm86Xc%2FITKuccwaLDjIXZdNrxiqsk1r%2B0
URL	<a href="http://localhost:8000/accountant/members">http://localhost:8000/accountant/members</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Amhd49wDyDyr7bL8W0_GUY2B6sPSNT6R_.yiEfe%2B5yAlm1DHN25uulBJYhuwTxg4xOQtAUCUFZU0c
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A8pB553Df7_ea5ypbq4Q6YFKAGgNzd4Ls.XQmdJimLLTnhw3vbF4k2PBz3YO8bDMkuUvfl06%2FOWTc
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET

Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AqkrV2z5TH9x_qvAv_SnpWxjJAn5mHA-a.hICRngpPOlOn4jYkx9hCgStovPsACYA5EDjiTDkv96o
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ATCtgF5fzeIYmXnC5m4Z1Qjig7UEy7W8V.3p1vPCq9U9symAnJfun20x%2FeFAqrPI25ryTRA3UMtO4
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Ay5QNa9-g9LCHtUTZgbCDUjRFXc3P-ESk.kWsz08EhLeqCHMotumkT5oPj4lOEknMMjbG%2Bi0q7Xto
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AZHmvo4IGWMfWHL_tvI2sySdZQ-ni37l.JSD8inPYe%2BTZhxxPuN4Til6749%2F4%2BiXIRmThEnQuHsQ
URL	<a href="http://localhost:8000/accountant/payments/3/adjust">http://localhost:8000/accountant/payments/3/adjust</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AyX7nCaHfdQLdZGHsG40oTgK94RAvud9f.4ltixKSpjPp5%2FE2QGd%2BfST495j606BcQ%2Fb4JWfI0Deo
URL	<a href="http://localhost:8000/books">http://localhost:8000/books</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AI2cVuxOkqy_mjZCSxAJH8Ab6XmMo3-fB.hJ6ginKhiXDD4rhbex3kQTmE7xZnn7J9I6quE%2B7%2BLwM
URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AGfxlan5LgkqknnpkQ-Q13_XBkpZb8XY2.gmLigaZ0DJCzV%2BwiCU4of3YfpvZkr2L4JKjcJnqQJnU



URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AmxQkmfq2V-eDcMzpGi7ZWtSrQltqms67.bw2HQ9HYDf1X1BtIP%2Bxi1IX62S4CrUseEle5MK%2BMyVE
URL	<a href="http://localhost:8000/books/29">http://localhost:8000/books/29</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Aa6P9iOD3Y9sojqezgeLgL5qAbFIM44rm.7rIQTzfdF3j08zlGesH5%2BiriAx%2BLGhzDtdblq76WHlg
URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AjHiKBG7tr_IZOspbVx31-vJWZZSt7TQC.e2yC%2Fa5on1DGkgo%2B%2BCA7usGpJ59eeUsq3xjMOW37L4A
URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ASNmWK7wPq66hszodJlhh_YH4gm3vxtHM.wj%2FSo%2FI8tA8RtR.JLB4DoJeg%2BpBvK%2FMTPaTz8sU%2FtE0k
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A44wDup-P9tRnE36N1_Zvuko68xPNWxQ8.Le%2FfwZqEBtQoAb47IKpn7vd7mqS0%2FYLSGyyCJn%2BM1oE
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AKZy_ZFH08_Lr2V5kKadNflrOUV3GJ8hX.a4SiECjrdTdsVymZiHHI4nbOE0jUpmJJX8%2F7GOQ2laE
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	
Other	The origin domain used for comparison was: localhost connect.sid=s%3Ajd7pHq2op9hU-

Info	tCILWlaUKk7mCACWfl.0xB0Cxxo7cDzZVSSjvJ4jKAHGjvQZ%2BZdcYYA8J%2FMNAA
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AtkIM3ZVavGgKvcWf-GyohYKRzQ5fdRfC.YRgrkV09IWc07XNgxZXmRWBPtrwNe8R%2F9PH7plbldg4
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A2bAHBWc-FFjhrFiH9kEda6sxrUirf5xP.IIHGx9C4C0b3DeLuY%2Fdw3WJ1qs8hbszk6%2F75M9pcjtg
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AC2gXFLSVIbkxS_h3AmcuzboKQhSuDSXK.vERTsA1q%2BVYEIBaWbW0caXIK5b5CLvO0z%2BzysE3Z0j0
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ADaHKzCEJd6Kbj2owgYQ_UbkOzwKBfk6.%2BS6CVr6A%2F2PI9c1s1CDVZeMGzQrZeWTWqxd%2BcJVYbs
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ASv8B1FcdNLZng_SuL-QONazgLbg5HUbW.W9mOj0J9PqC14d12doZdMvniVg1cQX8jynt80y2uzrU
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A6P1z95z7i1B-IRe8qUmprQmdqNDdbHG.qgfkOsyhxtab2mkhOWuDrfzUyqvX%2FIXId5kYdbofADE
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	

Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AvcZ-g3zzSdj0izil9rDcdmqxsyibEqQ-.hg080jjXJltKtUCdq88mzvo%2BYiRztE1X5Q0QvUPBwaU
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A18pPPIyszXMG0GojEHOeiWx1QGkRPfli.6xt16vOaHQxhR6CeAOLLy4bbf6mspl2qmSg3%2FGynl%2BM
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A1qHZLc48vyoDA-xl7Y3FGn1wmx2cUVIm.loRPhO0dsc91%2FDj5Bg4XF7gxNaVJBZocwBn3jn6%2FGa8
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AbG_NMpEwbdYbmgHGY1C_TN0KICvOAZNh.blz3Gjh49loWy6q1Z8q5ewrhqPLq2Wh8k2NpcTDiFGE
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Ac56TEQG5aw1CpJE581OCAQs9KSP3MMJy.2VNaOhor6omxEI%2BqYxSlmKmnY5uw9xrbS4AhhHbZpY
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Ad4GJdITQOJ95MRR3hJ049U2V1NMGJRFC.gG%2BzYmVn%2F1cZFMi9LtnpjpjGNy5UudV4itdjePoe21A
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AdIB9Cetf-rnejnA1dVbxngBqNV9Jf2gh.y0mYxlwUqsO%2F7%2F2ook2NNu98RhqEplql%2BPqWiwafrJI
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	

Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AFn6PJj4Xh9Kk2LHa4VFlinHV4XfllFuM.CgegYLDIOelcaMVQHEg6b7PkADNnq6G%2FMEnll1QNbF4
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AgXm0R1BsJ4k5IUMj6KD4k1H_EEjxgPzb.eYZIebgKAgAAD9YRpvNENYx08IH5Mml3qvmAqiG3%2ByA
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AHTeTYViSljWJwKDUfsK7Bm5KFi25aKtk.Dpr6551%2BFLczMITI%2B8tDcmHzg8%2BafsjiFJdDKEfUY80
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AIAxzkc9ypVnroxViSn3f5mFSZnojRhMr.qt63orJxpK9ZGqEOsQxSeza%2BnCNmlyHxwewrG5l4urU
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AiDnK16TBWFjzFx-XjQnHZiek-xJQ4e20.bDkJUMNOD7gsZ7N3faM%2F8iHrcixofUPf4ZR3PJl%2BaCA
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AjToDLxX_MAAhW3jrSrAfuyecfIFSQdNX.rgz6%2B%2BD7zjCL8rUql3qjJD8gFmFYnB3kXimHQvzZ1XM
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Ak7sLGyJSfbDy9-WVJVdHO5fnmCKLJPwg.x5HNLpTamqkVV5Ud%2BkfwjL1I5uMv2pZ9DIWwpvl9Eb0
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET

Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AK_WYSjsw1f7mKW6dLVkDcai5BiH54w36.SUngKp8Iz%2FzesCh1DcX6f0ZpHuTeE9T1xBDhIPo1QJw
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AkEIWfGP0VBYgnllhI0r6E9Fr1t_LnyLc.n9yiNgCj8tzFzzZ1ApD9WB8w6VKVMFo%2B59F4TlubMTY
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Akh1PIARUn0oNsctJWAKAvhQxgPxTWK7D.7qfmSKd%2FKV7357BihGF3fdK5JDleEoWdg9vg33LxEJc
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AKuYZj38IzvE37bPLiU3Ws1BMILj8c7ZR.mQlyr3omp3ovzGWabxURx0GTFUZKJ6htp3i1EGPZ3gA
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AM0RuW_it3V56JlZ-cvEbl_qtdmEFM0WI.O9iT1ALWSobu%2B5%2FwYJM%2FcC0Fo%2BPcsu2KZlcLlkFv%2FIQ
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AmMkMF04oNkTFoPTwBprkd8zUwOEPBjPu.1CyKGfvUuTlixBJmlihayhVD7t8fZTKQa7GX%2F08E2Bk
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AnhCOI6KtDyJ9IFxzZl29ZLomSjdtw2P.bbYGQkukYchI3bJUqNutWCy2%2BazzwmOSEMdAP5vhLYU

URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ApWXmXD0OmFMI7qpdA8SglQoP6nU7VS_O.OPLMZb5Ch7nZ6sqRKXq5%2Bqmthag5Nsoj7wsU2D4TQwNg
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AqmUPUcA33Tj8IIQVKdVXwHJ5cJyYb29.7DVv27WHqH5M0Ws1YI9ftCGcTqKUKZvNYY3FxxE8YbQ
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ARAk5uYWOVFonPovNRAXa2_rDHvoy6FeW.x9RmsI%2B2gEISvHEw0LWPKldv0iHB%2B3Tv6PjaV2CD0Wk
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ARUImhCBv6ONXRp_zpNG0svneJYZItF_r.WRVPP3HgGFbx470CB%2FkOg5athuKG6P6xdYDr8DX5Mws
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AsMEDWexChMh41MN32F0IOu2wFt82_7TB.MfI%2ByTERZb6Q2Qw1PwalgozC0MmEOS0IRWUU%2FvhZKNk
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ATb7MhQvKTtFjUAAV-s4ACefw_O5zADkq.qy7QNqSu00LSQgble5C0K8l6r1W8AmFqr7sbKhROKs0
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	

Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Au2jBewLrFQ6rl4Bm2JZa3qe3qOHe68Fl.L%2BJyNReSV0WwT2V8HeEvcyqOcadCPi2pgnSce%2BkpXZs
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AuGsXFIMfGRCEk1-LpyLTHBAhAancM7dP.ivV4e9cGDrDXMo3lOabEECsBd%2B1l6crfWisPfc%2B0XS4
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AUw2S-IgQRATlix7BeuWwO7Sw5iAJPeEF.wE1qDB8xyW9pvlj1Ylk%2FFR9QsMEICJwfHZWREjAK%2Fo4
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AVQTzZ3sdbO_IsNj2V1VDPvEqFEjT4wqn.bOccK3qeF%2B1Hnez8BrsrQGPriZYApip4q2XSg2wxyOg
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AwGo3Kbhbc6GxmdIDrzT4M0UYPCJ-SwHi.hZ7sTI5X5JdZn5w%2FZK%2BnCHAEKaORC8wlo1aaJlaiHRg
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AX2Bu7CvDk2hY7m7UNLPuodvWK9doUgAP.bRKQmGb7FNYHfrFWQgzSPXMVcj%2FmlsrMSZZNhF5tMG0
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AzhzTcFluhj2GavCRqVzYGHhN4yUgPYqM.0sEhHB5OPok7puR80t%2B%2F%2B8W%2FWX2Xr6thPI%2Fu%2Fk%2FZ%2Fjw
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET

Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AzLxNJHpqmf7HZfr62J62s010RD-bdnEB.DYeeICRpmQFf2AlnvjRbhBt3CHDRd2BgR%2BxsaHTPbOA
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A-C-slrgh2uxP6Q_ITGFG3c0g1dkY7L59.%2Fd%2FnGJ9PmgZUeLW2gdtuE951MBb4%2BWEkXaiJsHs0JyU
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A2Ftj7KY9f-zusulfORYqlxcAs1LNwWuN.jb6bTTHTrjG1exVx1lb8%2BYq9d13h5MOVRfJ8tx%2BvrBw
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A2G-XKroELiPGhMXqArbspyN7Ky5Trx5l.ZV1qSdZH2DUCdeIRXCb8OKJ4eTwlQDa5%2BJzThdTmMjo
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A2R55JK3we_aVpuKiF-hsrMRKJju-F1U.FVr0ule5lObyMcs8Uih6R6s3EqXs3rMmESFWF7g0mCs
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A3e8EFiUDOJAmSLyoXCG0kFuLErmPe_xz.NMT5vzs%2By0H6oz0DuSAG3fkJsdSsJMB7LkLiY4h%2FUs
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A8C2IFmjk98NBHESbRmArFZKRzAGhmPwf.wi286KlZi%2B5jaVRasuAKZoi95%2BgVdG5HBSvJ5a0%2FTw
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>



Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A9pqGhdLOj48EvH-W6vU1jQb4hJGjIMTv.%2FtEMxCZLRjNuhVpqqcKE9v45SrX1D753sJtCqB8NbY
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A9ZWE4YBasswOOrHoUB3x_8wMj50zUJo2.FZSKOYelvfnqXEM%2F7oq0Yo4udlgLYyv%2BP6SsuVx38yk
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AAyH_QAxTu9Rf4ixwtO8W20PO3BoXNEyu.Yh8IT%2F44aCu0h6oPdVP6XyJgBw5dsP4imdecJWY1uCs
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ABAXduFt9bSp3DLyFbx9Fi6PYKZgWcrEl.j8446lby1rwlmlL1IHOJtgovepxF%2BU6hP93cy0rJT1s
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ACbhCvWyVQurXgDFH2eJ-NIpfZtNG5i_c.1buJL8%2BSzc8keRu9okZWYmQUmbJvptmoDBuUfvQkkCo
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AdW_1us31P0wruluj0xXWOT_hw1XDNa33.4keQo3A%2FuyllzjJtCw%2Bchs8GtG37IDY%2F7Ua50qpHEWQ
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other	The origin domain used for comparison was: localhost connect.sid=s%3AFEAQ5u7mVTsVZtB0SuGgVt7E4FnH_z_a.xk080oC1egzjgepp%2BILJutBxK%2FC%

Info	2Fd7hyoGrzaPwBRjM
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AFUJPPhX_tOSbIT5s9UmAm4glbihaPZiL.39G7%2BZ4ETa1rUMH0hxJxUM9eH1AcFAjPK25f0NB0aQ
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AI8TPH22k7trDPx_mr4Cqu805su2uC3RM.5d3VdhDTFoK6vKQaIxuKmHMkm7d4oa8o8HrkjBvHhR4
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Akgpkjedvr1Dsm7NWr7CZM9vbdK0ywkJe.hV4g%2FvN2luZP%2FRhD5jUmWv9o9pFZF75QG3U4svQyBS4
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AMFrDA9MjResRIMevkdEWWDLZjsAxSlm.CdLNAEVfDqZD2W5QxonA3nT%2F96noK1OxRIGH9ikp2jk
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AnXosvAZn3E6yNluQrrXEkhYAhNqZfv_.zyPp%2FTdo1Qw8iT9KNcA2hhwF7YSANBX7UxUJ8n7xaTY
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Aouhyk9KczEAqWNLbGrWdfjH_fBAhaY_e.sMAJBEf7Yyrbu0JVdMpinK%2BiIPv66jrorzIFvDT3kEA
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	

Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ApstqAyCMiaOeHwqqRhjN8NiHWCPcqZn1.ADv9v6CgRU1ILbzWBn%2FJOAhD7UY2%2BTZvcgRJIB%2BcuQ
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AQRuZUhhcxkyrqfTUgi7gSYyBE-HyeZzQ.ro3pSIPExqhdKaDsQ67HpK0zhcMVHK7HvjnRt4RGfKY
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3ARufEjU-wqeY04H30aEaqDEvWlo4Udpop.zvU2FKyt1waFuM5znHZI7Bf9LI8p1mWdt3mvD%2BZhUIw
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AT66nTA2s1JCSGI391Xy-iXZh__HDPFvB.TSqIXaR%2BIbvoTdS6pPi8UBeYSbKxuY94gZS4eroJ0Uk
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Au7_laFoCsF0IFh2I7eydWYYC0ja2-FIQ.6liBuHxXDb6eMLYL8VNzS4KS8p%2Bp7U1t0WTGt8W8QVI
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AuHrh5J-qLF1cl955yKPrYLFaHupc2MUR.esyf2IHeVDzawCoSkIfRQT%2BMmfTOdNBfJscB7oRIImU
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AukBt_joyX3bodOchAKInCbK6rO5moRYBK.sboly08X7IXpwc1Q7w2hKkoIFCCS50hzFrQW09zkWqE
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET

Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AumrQdg1norOQAeve7jfpQXn4vie3syVf.xY3NW5LauBexRfaizWPAFM8v5G3Jaj20zMIQotFf0cc
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AUn_xz5UEYKKyczmyfkBjYWePtUNoyY8A.rRyE4wDzc6bFJHot4lbKDepUXa3LAp3dG4OT%2BLAxNoU
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AVhceq__CblObBpJgh7PAoRQY-QbKdyNe.iJacwglNiD0hc1882VXEB2zzFlxBhjuT%2F6FvpGdsktg
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AvkkVcyu8RkJ8as9FiMkh33fvzMIgoRnD.sCMhxj7OugCMIInH8xom%2F1em%2FKsCzwxRqiXAellXgRXI
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Ax_Adul-RS6QcZb-awVgrwu8JsmF4IAy4.%2BPCej1ch7swBWAhhtvj4F3Z52VW%2FGK9Gy4eqky%2FCQiE
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AxATmvshYZ6nHjZp7S9zY6jimx5Z2LfoJ.8HqkM0RIuukWmCbbSndi5a3tqSlct%2BMcBx4tgrb0gBc
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AyO_nrV-izPltTCXRA8cAFb_dJHmKrC8p.LRLGpaUZ%2FtvgUIjbq3JDkKwy1CJ6kg4DKJoyZ9%2Fmln8

URL	<a href="http://localhost:8000/purchaseMan/branches">http://localhost:8000/purchaseMan/branches</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Aets20BivNJnlx0fNKzGn9jQ_MsKOlt_R.w4AOwshWaNc046Gmw1rQ95ObNQRUufeAZh18o94uO8Q
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AJ2ynHnoGDI-NlfjKFwQfMp4t_XjfKfSv.V6cHhLN9slDWnu6DM0LOJNFYcKRsrqbUB%2ByN46A%2BGcM
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3Am1zrS79aCTwMd-KQkPLnecnd1-LZp9Kz.qTTQs%2FZiKZskLzrbi%2BcMTSNnwhyIqID8GU0Nu68p44
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AmnS07_DhFDt-qYV-rrn4ivSQzyxj2A2c.OxvP1QLOVzEHYGuOHtBUw%2FIUI8kW0ToCOwmc80N6Yic
URL	<a href="http://localhost:8000/purchaseMan/vendors">http://localhost:8000/purchaseMan/vendors</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AG-WIL3JM-RLu_YseVW6S12bZtwjyBf4N.QFLgl1RuNdtjYOsQzF3Y5GqvyIQKjWmCN3t%2BPc6Hpb4
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AcPUqwwlOmLPujxA4j_Lgf-4lozHrmOBC.6AR1KdT6Rr9xhZY4ihrWc2d8m3djdq%2B9WqTFMhilo7M
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AMwe489DI7dZJ89tHGIVC237dtt8_cWBw.ACKrnLVkL94JpOPszCOiippwUHK%2FX5Y5dS1AgNAY6C0

URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3A8ju52AFL3fvpUWlfTniEWrmOcRsinUm4.ozwsQoGKDhw4epxgb2Hw3qqb5BOeXfPhhsWEGIEZKh8
URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	
Other Info	The origin domain used for comparison was: localhost connect.sid=s%3AnZeU3y7KYUOTlhZi2sl7HXfmXkDiV_xE.41iJZcYaf35k8sJl1yTNfmFS3aoF51Mq87QJLAbpEcM
Instances	122
Solution	Always scope cookies to a FQDN (Fully Qualified Domain Name).
Reference	<a href="https://tools.ietf.org/html/rfc6265#section-4.1">https://tools.ietf.org/html/rfc6265#section-4.1</a> <a href="https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html">https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/06-Session_Management_Testing/02-Testing_for_Cookies_Attributes.html</a> <a href="https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies">https://code.google.com/p/browsersec/wiki/Part2#Same-origin_policy_for_cookies</a>
CWE Id	<a href="#">565</a>
WASC Id	15
Plugin Id	<a href="#">90033</a>

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	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	
Evidence	<noscript data-next-hide-fouc="true"><style>body{display:block}</style></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	
Evidence	<noscript data-next-hide-fouc="true"><style>body{display:block}</style></noscript>
Other Info	A noScript tag has been found, which is an indication that the application works differently with JavaScript enabled compared to when it is not.
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	
Evidence	<script defer="" noModule="" src="/_next/static/chunks/polyfills.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>

Method	GET
Attack	
Evidence	<a href="#" class="text-sm text-blue-600 hover:underline">Forgot password?</a>
Other Info	Links have been found that do not have traditional href attributes, which is an indication that this is a modern web application.
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	
Evidence	<script defer="" noModule="" src="/_next/static/chunks/polyfills.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	
Evidence	<script defer="" noModule="" src="/_next/static/chunks/polyfills.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	
Evidence	<script defer="" noModule="" src="/_next/static/chunks/polyfills.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	
Evidence	<script defer="" noModule="" src="/_next/static/chunks/polyfills.js"></script>
Other Info	No links have been found while there are scripts, which is an indication that this is a modern web application.
Instances	8
Solution	This is an informational alert and so no changes are required.
Reference	
CWE Id	
WASC Id	
Plugin Id	<a href="#">10109</a>

Informational	Session Management Response Identified
Description	The given response has been identified as containing a session management token. The 'Other Info' field contains a set of header tokens that can be used in the Header Based Session Management Method. If the request is in a context which has a Session Management Method set to "Auto-Detect" then this rule will change the session management to use the tokens identified.
URL	<a href="http://localhost:3000/api/auth/session">http://localhost:3000/api/auth/session</a>
Method	GET
Attack	
Evidence	http%3A%2F%2Flocalhost%3A3000

Other Info	cookie:next-auth.callback-url cookie:next-auth.csrf-token
URL	<a href="http://localhost:8000">http://localhost:8000</a>
Method	GET
Attack	
Evidence	s%3AtNnLAK15q_UUn1wr9Y81O2eY7r_dBXdl.M5VkrjWNDdkm86Xc%2FITKuccwaLDjlXZdNrxiqsk1r%2B0
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/members">http://localhost:8000/accountant/members</a>
Method	GET
Attack	
Evidence	s%3Amhd49wDyDyr7bL8W0_GUY2B6sPSNT6R_.yiEfe%2B5yAlm1DHN25uulBJYhuwTxg4xOQtAUCUFZU0c
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	s%3A8pB553Df7_ea5ypbq4Q6YFKAGgNzd4Ls.XQmdJimLLTnhw3vbF4k2PBz3YO8bDMkuUvfl06%2FOwTc
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	s%3ATCtgF5fzeIYmXnC5m4Z1Qjig7UEy7W8V.3p1vPCq9U9symAnJfun20x%2FeFAqrPI25ryTRA3UMtO4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	s%3AZHmvo4IGWMfWHL_tvI2syeSdZQ-ni37l.JSD8inPYe%2BTZhxxPuN4Til6749%2F4%2BiXIRmThEnQuHsQ
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	s%3AqkrV2z5TH9x_qvAv_SnpWxjJAn5mHA-a.hICRngpPOlOn4jYkx9hCgStovPsACYA5EDjiTDkv96o
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET



Attack	
Evidence	s%3Ay5QNa9-g9LCHtUTZgbCDUjRFXc3P-ESk. kWszo8EhLeqcHMotumkT5oPj4IOEknMMjbG%2Bi0q7Xto
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments/3/adjust">http://localhost:8000/accountant/payments/3/adjust</a>
Method	GET
Attack	
Evidence	s%3AyX7nCaHfdQLdZGHsG40oTgK94RAvud9f.4ltixKSpjPp5%2FE2QGd% 2BfST495j606BcQ%2Fb4JWfl0Deo
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books">http://localhost:8000/books</a>
Method	GET
Attack	
Evidence	s%3Al2cVuxOkqy_mjZCSxAJH8Ab6XmMo3-fB. hJ6ginKhiXDD4rhbex3kQTmE7xZnn7J9I6quE%2B7%2BLwM
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	s%3AGfxlan5LgkqknnpkQ-Q13_XBkpZb8XY2.gmLigaZ0DJCzV% 2BwiCU4of3YfpvZkr2L4JKjcJnqOJnU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/28">http://localhost:8000/books/28</a>
Method	GET
Attack	
Evidence	s%3AmxQkmfq2V-eDcMzpGi7ZWtSrQltqms67.bw2HQ9HYDf1X1BtIP% 2Bxi1IX62S4CrUseEle5MK%2BMyVE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/29">http://localhost:8000/books/29</a>
Method	GET
Attack	
Evidence	s%3Aa6P9iOD3Y9sojqezgeLgL5qAbFIM44rm.7rIQTzfdF3j08zlGesH5%2BiriAx% 2BLGhzDtdblq76WHlg
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	s%3ASNmWK7wPq66hszodJlhh_YH4gm3vxtHM.wj%2FSo%2FI8tA8RtRJLB4DoJeg% 2BpBvK%2FMTPaTz8sU%2FtE0k
Other Info	cookie:connect.sid

URL	<a href="http://localhost:8000/books/30">http://localhost:8000/books/30</a>
Method	GET
Attack	
Evidence	s%3AjHiKBG7tr_IZOspbVx31-vJWZZSt7TQC.e2yC%2Fa5on1DGkgo%2B%2BCA7usGpJ59eeUsq3xjMOW37L4A
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	s%3A44wDup-P9tRnE36N1_Zvuko68xPNWxQ8.Le%2FfwZqEBtQoAb47IKpn7vd7mqS0%2FYLSGyyCJn%2BM1oE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/42">http://localhost:8000/books/42</a>
Method	GET
Attack	
Evidence	s%3AKZy_ZFHo8_Lr2V5kKadNflrOUV3GJ8hX.a4SiECjrdTdSVyMZiHHI4nbOE0jUpmJJX8%2F7GOQ2laE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	s%3AjdV7pHq2op9hU-tCILWlaUKk7mCACWfl.0xB0Cxxo7cDzZVSSjvJ4jKAHGjvQZ%2BZdcYYA8J%2FMNAA
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/50">http://localhost:8000/books/50</a>
Method	GET
Attack	
Evidence	s%3AtkIM3ZVavGgKvcWf-GyohYKRzQ5fdRfC.YRgrkV09IWc07XNgxZXmRWBPTrwNe8R%2F9PH7plbldg4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	s%3A2bAHBWc-FFjhrFiH9kEda6sxrUirl5xP.IIHGx9C4C0b3DeLuY%2FdW3WJ1qs8hbszk6%2F75M9pcjtg
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	s%3AC2gXFLSVlbkxS_h3AmcuzboKQhSuDSXK.vERTsA1q%2BVYEIBaWbW0caXIK5b5CLvO0z%2BzysE3Z0j0

Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	s%3ADaHKzCEJd6Kbj2owgYQ_UbkOzwKBflk6.%2BS6CVr6A%2F2PI9c1s1CDVZeMGzQrZeWTWqxdu%2BcJVYbs
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/52">http://localhost:8000/books/52</a>
Method	GET
Attack	
Evidence	s%3ASv8B1FcdNLZng_SuL-QONazgLbg5HUbW.W9mOj0J9PqC14d12doZdMvniVg1cQX8jynt80y2uzrU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	s%3A6P1z95z7i1IB-IRe8qUmprQmdqNDdbHG.qgfkOsyhxtab2mkhOWuDrfzUyqvX%2FIXId5kYdbofADE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/59">http://localhost:8000/books/59</a>
Method	GET
Attack	
Evidence	s%3AvcZ-g3zzSdj0izil9rDcdmqxyibEqQ-.hg080jjXJltKtUCdq88mzvo%2BYiRztE1X5Q0QvUPBwaU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3A18pPPIyszXMG0GojEHOeiWx1QGkRPfli.6xt16vOaHQxhR6CeAOLLy4bbf6mspl2qmSg3%2FGynl%2BM
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3A1qHZLc48vyoDA-xl7Y3FGn1wmx2cUVIm.loRPnO0dsc91%2FDj5Bg4XF7gxNaVJBZocwBn3jn6%2FGa8
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET

Attack	
Evidence	s%3AFn6PJj4Xh9Kk2LHa4VFlinHV4XfIfuM.CgegYLDIOelcaMVQHEg6b7PkADNnq6G%2FMEnlI1QNbF4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AHTeTYViSljWJwKDUfsK7Bm5KFi25aKTK.Dpr6551%2BFLczMITI%2B8tDcmHzg8%2BafsjiFJdDKEfUY80
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AIAxzkc9ypVnroxViSn3f5mFSZnojRhMr.qt63orJxpK9ZGqEOsQxSeza%2BnCNmlyHxwewrG5l4urU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AK_WYSjsw1f7mKW6dLVkDcai5BiH54w36.SUngKp8Iz%2FzesCh1DcX6f0ZpHuTeE9T1xBDhIPo1QJw
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AKuYZj38IzvE37bPLiU3Ws1BMILj8c7ZR.mQlyr3omp3ovzGWabxURx0GTFUZKJ6htp3i1EGPZ3gA
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AM0RuW_it3V56Jlz-cvEbl_qtdmEFM0WI.O9iT1ALWSobu%2B5%2FwYJM%2FcC0Fo%2BPcsu2KZlcLkFv%2FIQ
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3ARAK5uYWOVFonPovNRAXa2_rDHvoy6FeW.x9RmsI%2B2gEISvHEw0LWPKldv0iHB%2B3Tv6PjaV2CD0Wk
Other Info	cookie:connect.sid

URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3ARUImhCBv6ONXRp_zpNG0svneJYZltF_r.WRVPP3HgGFbx470CB%2FkOg5athuKG6P6xdYDr8DX5Mws
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3ATb7MhQvKTtFjUAAV-s4ACefw_O5zADkq.qy7QNqSu00LSQgble5C0K8l6r1W8AmFqr7sbKhROKs0
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AUw2S-IgQRATlix7BeuWwO7Sw5iAJPeEF.wE1qDB8xyW9pvIj1Ylk%2FFR9QsMEICJwfHZWREjAK%2Fo4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AVQTzZ3sdbO_IsNj2V1VDPvEqFEjT4wqn.bOccK3qeF%2B1Hnez8BrsrQGPriZYApip4q2XSg2wxyOg
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AX2Bu7CvDk2hY7m7UNLPuodvWK9doUgAP.bRKQmGb7FNYHfrFWQgzSPXMVcj%2FmlsrMSZZNhF5tMG0
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AbG_NMpEwbdYbmgHGY1C_TN0KICvOAZNh.blz3Gjh49loWy6q1Z8q5ewrhqPLq2Wh8k2NpcTDiFGE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3Ac56TEQG5aw1CpJE581OCAQs9KSP3MMJy.2VNaOhor6omxEI%2BqYxSlmKmny5uw9xrbS4AhhHbZpY

Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3Ad4GJdITQOJ95MRR3hJ049U2V1NMGJRFC.gG%2BzYmVn%2F1cZFMi9LtnpjpjGNy5UudV4itdjePoe21A
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AdlB9Cetf-rnejnA1dVbxngBqNV9Jf2gh.y0mYxIwUqsO%2F7%2F2ook2NNu98RhqEplql%2BPqWiwafrJl
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AgXm0R1BsJ4k5IUMj6KD4k1H_EEjxgPzb.eYZIebgKAgAAD9YRpvNENYx08IH5MmI3qvmAqiG3%2ByA
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AiDnK16TBWFjzFx-XjQnHZiek-xJQ4e20.bDkJUMNOD7gsZ7N3faM%2F8iHrcixofUPf4ZR3PJl%2BaCA
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AjToDLxX_MAAhW3jrSrAfuyecfIFSQdNX.rgz6%2B%2BD7zjCL8rUql3qjJD8gFmFYnB3kXimHQvzZ1XM
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3Ak7sLGyJSfbDy9-WVJVdHO5fnmCKLJPwg.x5HNLpTamqkVV5Ud%2BkfwjL1I5uMv2pZ9DIWwpvl9Eb0
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET

Attack	
Evidence	s%3AkEIWfGP0VBYgnllhI0r6E9Fr1t_LnyLc.n9yiNgCj8tzFzzZ1ApD9WB8w6VKVMFo%2B59F4TlubMTY
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3Akh1PIARUn0oNsctJWAKAvhQxgPxTWK7D.7qfmSKd%2FKV7357BihGF3fdK5JDleEoWdg9vg33LxEJc
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AmMkMF04oNkTFoPTwBprkd8zUwOEPBjPu.1CyKGfvUuTlixBJmlihayhVD7t8fZTKQa7GX%2F08E2Bk
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AnhCOI6KtTDyJ9IFxzZI29ZLomSjdtw2P.bbYGQkukYchI3bJUqNutWCy2%2BazzwmOSEMdAP5vhLYU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3ApWXmXD0OmfmI7qpdA8SglQoP6nU7VS_O.OPLMZb5Ch7nZ6sqRKXq5%2Bqmhag5Nsoj7wsU2D4TQwNg
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AqmUPUcA33Tj8lIQVKdVXwHJ5cJyYb29.7DVv27WHqH5M0Ws1YI9ftCGcTqKUKZvNYY3FxxE8YbQ
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AsMEDWexChMh41MN32F0IOu2wFt82_7TB.Mfl%2ByTERZb6Q2Qw1PwalgozC0MmEOS0IRWUU%2FvhZKNk
Other Info	cookie:connect.sid

URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3Au2jBewLrFQ6rl4Bm2JZa3qe3qOHe68FI.L% 2BJyNReSV0WwT2V8HeEvcygOcadCPi2pgnSce%2BkpXZs
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AuGsXFIMfGRCEk1-LpyLTHBAhAancM7dP.ivV4e9cGDrDXMo3IOabEECsBd% 2B1I6crfWisPfc%2B0XS4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AwGo3Kbhbc6GxmdIDrzT4M0UYPCj-SwHi.hZ7sTI5X5JdZn5w%2FZK% 2BnCHAEKaORC8wlo1aaJlaiHRg
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AzLxNJHpmf7HZfr62J62s010RD-bdnEB.DYeeICRpmQFf2AInvjRbhBt3CHDRd2BgR% 2BxsaHTPbOA
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/newBooks?limit=10">http://localhost:8000/books/newBooks?limit=10</a>
Method	GET
Attack	
Evidence	s%3AzhzTcFluhj2GavCRqVzYGHhN4yUgPYqM.0sEhHB5OPok7puR80t%2B%2F% 2B8W%2FWX2Xr6thPI%2Fu%2Fk%2FZ%2Fjw
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A-C-slrgh2uxP6Q_ITGFG3c0g1dkY7L59.%2Fd% 2FnGJ9PmgZUeLW2gdtuE951MBb4%2BWEkXaiJsHs0JyU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A2Ftj7KY9f-zusulfORYqlxcAs1LNwWuN.jb6bTTHTrjG1exVx1lb8% 2BYq9d13h5MOVrfJ8tx%2BvrBw



Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A2G-XXkroELiPGhMXqArbspyN7Ky5Trx5l. ZV1qSdZH2DUCdeIRXcb8OKJ4eTwlQDa5%2BjzThdTmMjo
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A2R55IJK3we_aVpuKiF-hsrMRKJju-F1U. FVr0ule5IObymCs8Uih6R6s3EqXs3rMmESFWF7g0mCs
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A3e8EFiUDOJAmSLyoXCG0kFuLErmPe_xz.NMT5vzs% 2By0H6oz0DuSAG3fkJsdSsJMB7LkLliY4h%2FUs
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A8C2IFmjk98NBHESbRmArFZKRzAGhmPwf.wi286KlZi%2B5jaVRasuAKZoi95% 2BgVdG5HBSvJ5a0%2FTw
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A9ZWE4YBasswOOrHoUB3x_8wMj50zUJo2.FZSKOYelvnqXEM% 2F7oq0Yo4udlgLYyv%2BP6SsuVx38yk
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3A9pqGhdLOj48EvH-W6vU1jQb4hJGjIMTv.% 2FtEMxCZLRjNuhVpqgcKE9vf45SrX1D753sJtCqB8NbY
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET

Attack	
Evidence	s%3AAyH_QAxTu9Rf4ixwtO8W20PO3BoXNEyu.Yh8IT%2F44aCu0h6oPdVP6XyJgBw5dsP4imdecJWY1uCs
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3ABAXduFt9bSp3DLyFbx9Fi6PYKZgWcrEI.j8446lby1rwlmlL1IHOJtgovepxF%2BU6hP93cy0rJT1s
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3ACbhCvWyVQurXgDFH2eJ-NlpfZtNG5i_c.1buJL8%2BSzc8keRu9okZWYmQUmbJvptmoDBuUfvQkkCo
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AFEAQ5t5u7mVTsVZtB0SuGgVt7E4FnhZ_a.xk080oC1egzjgepp%2BILJutBxK%2FC%2Fd7hyoGrzaPwBRjM
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AFUJPPhX_tOSbIT5s9UmAm4glbihaPZiL.39G7%2BZ4ETa1rUMH0hxJxUM9eH1AcFAjPK25f0NB0aQ
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AI8TPH22k7trDPx_mr4Cqu805su2uC3RM.5d3VdhDTFoK6vKQalxuKmHMkm7d4oa8o8HrkjBvHhR4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AMFrDA9MjResRIMevkdEWWDLZjzsAxSlm.CdLNAEVfDqZD2W5QxonA3nT%2F96noK1OxRIGH9ikp2jk
Other Info	cookie:connect.sid

URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AQRuZUhhcxkyrqfTUgi7gSYyBE-HyeZzQ. ro3pSIPExqhdKaDsQ67HpK0zhcMVHK7HvjnRt4RGfKY
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3ARufEjU-wqeY04H30aEaqDEvWlo4Udpop. zvU2FKyt1waFuM5znHZI7Bf9LI8p1mWdt3mvD%2BZhUIw
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AT66nTA2s1JCSGI391Xy-iXZh__HDPFvB.TSqIXaR% 2BIbvoTdS6pPi8UBeYSbKxuY94gZS4eroJ0Uk
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AUh_xz5UEYKKyczmyfkBjYWePtUNoyY8A. rRyE4wDzc6bFJHot4IbKDepUXa3LAp3dG4OT%2BLAxNoU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AVhceq__CbIObBpJgh7PAoRQY-QbKdyNe.iJacwglNiD0hc1882VXEB2zzFlxBhjuT% 2F6FvpGdsktg
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AdW_1us31P0wruluj0xXWOT_hw1XDNa33.4keQo3A%2FuyllzjJtCw% 2Bchs8GtG37IDY%2F7Ua50qpHEWQ
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3Akpgkjedvr1Dsm7NWr7CZM9vbdK0ywkJe.hV4g%2FvN2luZP% 2FRhD5jUmWv9o9pFZF75QG3U4svQyBS4

Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AnXosvAZn3E6yNluQrrXEkhYAhNqZfv_.zyPp%2FTdo1Qw8iT9KNcA2hhwF7YSANBX7UxUJ8n7xaTY
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3Aouhyk9KczEAqWNLbGrWDfjH_fBAhaY_e.sMAJBEf7Yyrbu0JVdMpinK%2BilPv66jrorzIFvDT3kEA
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3ApstqAyCMiaOeHwqqRhjN8NiHWCPcqZn1.ADv9v6CgRU1ILbzWBn%2FJOFAhD7UY2%2BTZvcgRJIB%2BcuQ
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3Au7_laFoCsF0IFh2I7eydWYYC0ja2-FIQ.6liBuHxXDb6eMLYL8VNzS4KS8p%2Bp7U1t0WTGt8W8QVI
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AuHrh5J-qLF1cl955yKPrYLFAHupc2MUR.esyf2lHeVDzawCoSkIfRQT%2BMmfTOdNBfJscB7oRIImU
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AukBt_joX3bodOchAKInCbK6rO5moRYBK.sboly08X7IXpwc1Q7w2hKkoIFCCS50hzFrQW09zkWqE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET

Attack	
Evidence	s%3AumrQdg1norOQAeve7jfpQXn4vie3syVf. xY3NW5LauBexRfaizWPAFM8v5G3Jaj20zMIQotFf0cc
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AvkkVcyu8RkJ8as9FiMkh33fvzMlgoRnD.sCMhxj7OugCMIhH8xom%2F1em% 2FKsCzwxRqiXAellXgRXI
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AxAATmvshYZ6nHjZp7S9zY6jimx5Z2LfOJ.8HqkM0RIuukWmCbbSndi5a3tqSlct% 2BMcBx4tgrb0gBc
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AxA_Adul-RS6QcZb-awVgrwu8JsmF4IAy4.%2BPcEj1ch7swBWAhhtvj4F3Z52VW% 2FGK9Gy4eqky%2FCQiE
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/books/random">http://localhost:8000/books/random</a>
Method	GET
Attack	
Evidence	s%3AyO_nrV-izPltTCXRA8cAFb_dJHmKrC8p.LRLGpaUZ% 2FtvgUljbq3JDkKwy1CJ6kg4DKJoyZ9%2Fmln8
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/purchaseMan/branches">http://localhost:8000/purchaseMan/branches</a>
Method	GET
Attack	
Evidence	s%3Aets20BivNJnlx0fNKzGn9jQ_MsKOlt_R. w4AOwshWaNc046Gmw1rQ95ObNQRUufeAZh18o94uO8Q
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	s%3AJ2ynHnoGDI-NIfjKFwQfMp4t_XjfKfSv.V6cHhLN9sIDWnu6DM0LOJNFYcKRsrqbUB% 2ByN46A%2BGcM
Other Info	cookie:connect.sid

URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	s%3Am1zrS79aCTwMd-KQkPLnecnd1-LZp9Kz.qTTQs%2FZiKZskLzxrbi%2BcMTSNnwhyIqID8GU0Nu68p44
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/purchaseMan/trackingOrders">http://localhost:8000/purchaseMan/trackingOrders</a>
Method	GET
Attack	
Evidence	s%3AmnS07_DhFDt-qYV-rrn4ivSQzyxj2A2c.OxvP1QLOVzEHYGUOHtBUw%2FIUI8kW0ToCOwmc80N6Yic
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/purchaseMan/vendors">http://localhost:8000/purchaseMan/vendors</a>
Method	GET
Attack	
Evidence	s%3AG-WIL3JM-RLu_YseVW6S12bZtwjyBf4N.QFLgl1RuNdtjYOsQzF3Y5GqvyIQKjWmCN3t%2BPc6Hpb4
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	s%3AMwe489DI7dZJ89tHGIVC237dt8_cWBw.ACKrnLVkL94JpOPszCOiippwUHK%2FX5Y5dS1AgNAY6C0
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/robots.txt">http://localhost:8000/robots.txt</a>
Method	GET
Attack	
Evidence	s%3AcPUqwwlOmLPujxA4j_Lgf-4lozHrmOBC.6AR1KdT6Rr9xhZY4ihrWc2d8m3djdq%2B9WqTFMhlo7M
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	s%3A8ju52AFL3fvpUWlftNiEWrmOcRsinUm4.ozwsQoGKDhw4epxgb2Hw3qqb5BOeXfPhhsWEGIEZKh8
Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/sitemap.xml">http://localhost:8000/sitemap.xml</a>
Method	GET
Attack	
Evidence	s%3AnZeU3y7KYUOTlhZi2sl7HXfmXkDiV_xE.41iJZcYaf35k8sJl1yTNfmFSaoF51Mq87QJLAbpEcM

Other Info	cookie:connect.sid
URL	<a href="http://localhost:8000/accountant/payments">http://localhost:8000/accountant/payments</a>
Method	GET
Attack	
Evidence	s%3Ay5QNa9-g9LCHtUTZgbCDUjRFXc3P-ESk. kWszo8EhLeqCHMotumkT5oPj4IOEknMMjbG%2Bi0q7Xto
Other Info	cookie:connect.sid
Instances	102
Solution	This is an informational alert rather than a vulnerability and so there is nothing to fix.
Reference	<a href="https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id">https://www.zaproxy.org/docs/desktop/addons/authentication-helper/session-mgmt-id</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10112</a>

Informational	User Agent Fuzzer
Description	Check for differences in response based on fuzzed User Agent (eg. mobile sites, access as a Search Engine Crawler). Compares the response statuscode and the hashcode of the response body with the original response.
URL	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000">http://localhost:3000</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/">http://localhost:3000/</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other	

Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	



URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next">http://localhost:3000/_next</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>

Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static">http://localhost:3000/_next/static</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks">http://localhost:3000/_next/static/chunks</a>

Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>

Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages">http://localhost:3000/_next/static/chunks/pages</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET

Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET

Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/_app.js">http://localhost:3000/_next/static/chunks/pages/_app.js</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko



Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18

Attack	(KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/pages/book">http://localhost:3000/_next/static/chunks/pages/book</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36

Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/chunks/webpack.js">http://localhost:3000/_next/static/chunks/webpack.js</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	

Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	

Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/development">http://localhost:3000/_next/static/development</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	

Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	

Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/_next/static/webpack">http://localhost:3000/_next/static/webpack</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other	

Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api">http://localhost:3000/api</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other	



Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	

URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/api/auth">http://localhost:3000/api/auth</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)
Evidence	
Other Info	

URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Trident/7.0; rv:11.0) like Gecko
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3739.0 Safari/537.36 Edg/75.0.109.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.124 Safari/537.36
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:93.0) Gecko/20100101 Firefox/91.0
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>

Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff">http://localhost:3000/staff</a>
Method	GET
Attack	msnbot/1.1 (+http://search.msn.com/msnbot.htm)
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/CreateOrder">http://localhost:3000/staff/CreateOrder</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/login">http://localhost:3000/staff/login</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other	

Info	
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/ManageMemberships">http://localhost:3000/staff/ManageMemberships</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Payment-reconciliation">http://localhost:3000/staff/Payment-reconciliation</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Reports">http://localhost:3000/staff/Reports</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; CPU iPhone OS 8_0_2 like Mac OS X) AppleWebKit/600.1.4 (KHTML, like Gecko) Version/8.0 Mobile/12A366 Safari/600.1.4

Evidence	
Other Info	
URL	<a href="http://localhost:3000/staff/Tracking">http://localhost:3000/staff/Tracking</a>
Method	GET
Attack	Mozilla/5.0 (iPhone; U; CPU iPhone OS 3_0 like Mac OS X; en-us) AppleWebKit/528.18 (KHTML, like Gecko) Version/4.0 Mobile/7A341 Safari/528.16
Evidence	
Other Info	
Instances	160
Solution	
Reference	<a href="https://owasp.org/wstg">https://owasp.org/wstg</a>
CWE Id	
WASC Id	
Plugin Id	<a href="#">10104</a>