Developer Report

Acunetix Security Audit

2024-03-06

Generated by Acunetix

Scan of inventory-stg.nexdecade.com

Scan details

Scan information	
Start time	2024-03-06T07:45:57.748889+00:00
Start url	https://inventory-stg.nexdecade.com/
Host	inventory-stg.nexdecade.com
Scan time	35 minutes, 35 seconds
Profile	Full Scan
Server information	nginx
Responsive	True
Server OS	Unknown

Threat level

Acunetix Threat Level 2

One or more medium-severity type vulnerabilities have been discovered by the scanner. You should investigate each of these vulnerabilities to ensure they will not escalate to more severe problems.

Alerts distribution

Total alerts found	5
⚠ Critical	0
⌃⌃ High	0
⌃ Medium	1
⌄ Low	0
ⓘ Informational	4

Alerts summary

Laravel debug mode enabled

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 6.9 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Confidentiality Impact to the Vulnerable System: Low Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: Low Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 5.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: Partial Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-200

Affected items	Variation
Web Server	1

An Unsafe Content Security Policy (CSP) Directive in Use

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

data: Used in a Content Security Policy (CSP) Directive

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

ⓘ default-src Used in Content Security Policy (CSP)

Classification	
CWE	CWE-16

Affected items	Variation
Web Server	1

ⓘ Permissions-Policy header not implemented

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Active Confidentiality Impact to the Vulnerable System: None Integrity Impact to the Vulnerable System: None Availability Impact to the Vulnerable System: None Confidentiality Impact to the Subsequent System: None Integrity Impact to the Subsequent System: None Availability Impact to the Subsequent System: None
CVSS3	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Changed Confidentiality Impact: None Integrity Impact: None Availability Impact: None
CVSS2	Base Score: 0.0 Access Vector: Network_accessible Access Complexity: Low Authentication: None Confidentiality Impact: None Integrity Impact: None Availability Impact: None Exploitability: Not_defined Remediation Level: Not_defined Report Confidence: Not_defined Availability Requirement: Not_defined Collateral Damage Potential: Not_defined Confidentiality Requirement: Not_defined Integrity Requirement: Not_defined Target Distribution: Not_defined
CWE	CWE-1021

Affected items	Variation

Web Server	1

Alerts details

Laravel debug mode enabled

Severity	**Medium**
Reported by module	/httpdata/laravel_audit.js

Description

The web application uses Laravel framework. Laravel Debug mode is enabled. Debug mode should be turned off in production environment, as it leads to disclosure of sensitive information about the web application.

Impact

The web application in debug mode discloses sensitive information. This information can be used to launch further attacks.

Recommendation

Disable the debug mode by setting APP_DEBUG to false

References

[Error Handling (https://laravel.com/docs/7.x/errors#configuration)](https://laravel.com/docs/7.x/errors#configuration)

Affected items

Web Server

Details

Request headers

```
GET /_ignition/health-check HTTP/1.1
Cookie: XSRF-
TOKEN=eyJpdiI6InZrQ1VhL2xxNnRBNnB5c0VwYkhFcGc9PSIsInZhbHVlIjoiNlBBYjFjejQrVXo3WEdqZG9KN3
R6Zm5lU2pQM213eVlXM3diZW5wOXU3UGlvT1A5LzU2cXAycTZTOTBBSThQUlBnRWVodUxyd01pN2QwTllkWWIzWE
55THNRZ0hTVWpjalV1a3dYbGhlL1BhdnBNNVRObkxEdiszTm9PdWo4c2QiLCJtYWMiOiI2YzI4M2FiZmFhZmNlNW
I5N2NhN2Q0YmIxMWFiMmM1MjI2YWFmMGFlZDcwM2M5NDllMmIyYjAyMTc2OWRlOGE4IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IkgwMllUeFBPZS9aS1lCZldMZ05uQUE9PSIsInZhbHVlIjoiRzd5
WDdzOHVNMENNNkNmbUwxMDZGQjZjNVYxNS9iNFVkTTZOL0lEakR0cFViaUhOSVYxM2I2RTBtZFpzSVhyWFdma2FN
QTdBdDkwRDI4elVPL3lITUxyVmEwa2VXZUdkKzNqbFVDSEJ4ek9CVDJKYTArYzJOTVlxbFFOTmtPNUgiLCJtYWMi
OiJlYjhlYjM3YjIxODNiMGU1M2Q5YjU3ZmYzZTM4YzZmYjY3NjU0Y2YxM2NlOGIyOGViMDM4ZDNlMzg0MGFmY2Iy
IiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
Host: inventory-stg.nexdecade.com
Connection: Keep-alive
```

An Unsafe Content Security Policy (CSP) Directive in Use

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy (CSP) to Secure Web Applications](https://www.invicti.com/blog/web-security/content-security-policy/)(https://www.invicti.com/blog/web-security/content-security-policy/)
[The dangers of incorrect CSP implementations](https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)(https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
[Leverage Browser Security Features to Secure Your Website](https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)(https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server

Verified vulnerability

Details

- **An Unsafe Content Security Policy (CSP) Directive in Use**
  - **First observed on:** https://inventory-stg.nexdecade.com/index.php/login
  - **CSP Value:** default-src 'self'; connect-src 'self'; frame-ancestors 'self'; img-src * data: blob:; style-src 'self' 'unsafe-inline'; base-uri 'self'; form-action 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; font-src 'self' data:;
  - **CSP Source:** header
  - **Summary:** Acunetix detected that one of following CSP directives is used: unsafe-eval, unsafe-inline. By using unsafe-eval, you allow the use of string evaluation functions like eval. By using unsafe-inline, you allow the execution of inline scripts, which almost defeats the purpose of CSP. When this is allowed, it's very easy to successfully exploit a Cross-site Scripting vulnerability on your website.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully.
  - **Remediation:** If possible remove unsafe-eval and unsafe-inline from your CSP directives.
  - **References:**
    - N/A

Request headers

```
POST /index.php/login HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IlNRUitRWjN6dXBkNzdsc1JoVC9kMkE9PSIsInZhbHVlIjoiRFJFN3FyNUM2Mi9HMkdtbmVWNm
J3MTczb3BJbHJSaG9DSXdXT0pEUEdKYjlqbDM0cDdtalNOS09PeE1BQVNjeFBHMUVnL2NpM1NLZjZXVDhqR25IST
AwVWtsQ0tMTG5yWmx1d1I0OVdhaG13eGRNeFQzbEUrUzg1aFpWQTBNUGYiLCJtYWMiOiJkZjlhMjFjYWFlNmY0Yz
YxMDk4NjY5ZjA5MjZhYTM4YzNhZmMyNzk2NmY3ZTJkMGI5MWZmYTM5NTVlYWU4MTMzIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6Ik9hVUdEK2dISk1IMUxSNi9LSEt0ZXc9PSIsInZhbHVlIjoiNHF2
V1QvVW40Q3IzaTliNktNckFHQW1kYkhxUkVaUnpFbnlQMGNXM3Vzcm5CZVd0QytLaEpVRGd6UWIzaE1YZWlmbW1B
VnJyZDN6a1ErMk1ndkUzU1dNUDRDeTlFaEZSdm9UakwwM1JHa3FXaHVDN1ByejE2ME51Zk1BNGpNZlIiLCJtYWMi
OiJjYTFhOWM5Zjg5ZDliYzkxZGRjMGE5NzI0ODgzZTcxODZiZTJiMmZhZDRiMjA2ODdjMGNiNTQwNTU4ZWVhMmRi
IiwidGFnIjoiIn0%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
Host: inventory-stg.nexdecade.com
Connection: Keep-alive

_token=QMqn3FfD7Vt6qsEGL6SokjOjmc1wWiaCvQVxDnV2&email=testing%40example.com&password=u]H
[ww6KrA9F.x-F&remember=on
```

ⓘ data: Used in a Content Security Policy (CSP) Directive

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

Using Content Security Policy (CSP) to Secure Web Applications (https://www.invicti.com/blog/web-security/content-security-policy/)
The dangers of incorrect CSP implementations (https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
Leverage Browser Security Features to Secure Your Website (https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server
Verified vulnerability
Details

- **data: Used in a Content Security Policy (CSP) Directive**
  - **First observed on:** https://inventory-stg.nexdecade.com/index.php/login
  - **CSP Value:** default-src 'self'; connect-src 'self'; frame-ancestors 'self'; img-src * data: blob:; style-src 'self' 'unsafe-inline'; base-uri 'self'; form-action 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; font-src 'self' data:;
  - **CSP Source:** header
  - **Summary:** Acunetix detected data: use in a CSP directive.
  - **Impact:** An attacker can bypass CSP and exploit a Cross-site Scripting vulnerability successfully by using data: protocol.
  - **Remediation:** Remove data: sources from your CSP directives.
  - **References:**
    - N/A

Request headers

```
POST /index.php/login HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IlNRUitRWjN6dXBkNzdsc1JoVC9kMkE9PSIsInZhbHVlIjoiRFJFN3FyNUM2Mi9HMkdtbmVWNm
J3MTczb3BJbHJSaG9DSXdXT0pEUEdKYjlqbDM0cDdtalNOS09PeE1BQVNjeFBHMUVnL2NpM1NLZjZXVDhqR25IST
AwVWtsQ0tMTG5yWmx1d1I0OVdhaG13eGRNeFQzbEUrUzg1aFpWQTBNUGYiLCJtYWMiOiJkZjlhMjFjYWFlNmY0Yz
YxMDk4NjY5ZjA5MjZhYTM4YzNhZmMyNzk2NmY3ZTJkMGI5MWZmYTM5NTVlYWU4MTMzIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6Ik9hVUdEK2dISk1IMUxSNi9LSEt0ZXc9PSIsInZhbHVlIjoiNHF2
V1QvVW40Q3IzaTliNktNckFHQW1kYkhxUkVaUnpFbnlQMGNXM3Vzcm5CZVd0QytLaEpVRGd6UWIzaE1YZWlmbW1B
VnJyZDN6a1ErMk1ndkUzU1dNUDRDeTlFaEZSdm9UakwwM1JHa3FXaHVDN1ByejE2ME51Zk1BNGpNZlIiLCJtYWMi
OiJjYTFhOWM5Zjg5ZDliYzkxZGRjMGE5NzI0ODgzZTcxODZiZTJiMmZhZDRiMjA2ODdjMGNiNTQwNTU4ZWVhMmRi
IiwidGFnIjoiIn0%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
Host: inventory-stg.nexdecade.com
Connection: Keep-alive

_token=QMqn3FfD7Vt6qsEGL6SokjOjmc1wWiaCvQVxDnV2&email=testing%40example.com&password=u]H
[ww6KrA9F.x-F&remember=on
```

ⓘ default-src Used in Content Security Policy (CSP)

Severity	**Informational**
Reported by module	/httpdata/content_security_policy.js

Description

Acunetix evaluated the scan target's Content Security Policies, checked for misconfigurations and potentially unintended side-effects of otherwise valid configurations, and offers the following suggestions on how to change existing policies for improved security and maximum compatibility.

Impact

Consult References for more information.

Recommendation

See alert details for available remediation advice.

References

[Using Content Security Policy (CSP) to Secure Web Applications](https://www.invicti.com/blog/web-security/content-security-policy/)(https://www.invicti.com/blog/web-security/content-security-policy/)
[The dangers of incorrect CSP implementations](https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)(https://www.invicti.com/blog/web-security/negative-impact-incorrect-csp-implementations/)
[Leverage Browser Security Features to Secure Your Website](https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)(https://www.invicti.com/blog/web-security/leverage-browser-security-features-secure-website/)

Affected items

Web Server

Verified vulnerability

Details

- **default-src Used in Content Security Policy (CSP)**
    - **First observed on:** https://inventory-stg.nexdecade.com/index.php/login
    - **CSP Value:** default-src 'self'; connect-src 'self'; frame-ancestors 'self'; img-src * data: blob:; style-src 'self' 'unsafe-inline'; base-uri 'self'; form-action 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; font-src 'self' data:;
    - **CSP Source:** header
    - **Summary:** Acunetix detected that you used default-src in CSP directive. It is important to know that default-src cannot be used as a fallback for the functions below: base-uri, form-action, frame-ancestors, plugin-types, report-uri, sandbox
    - **Impact:** N/A
    - **Remediation:** N/A
    - **References:**
        - N/A

Request headers

```
POST /index.php/login HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IlNRUitRWjN6dXBkNzdsc1JoVC9kMkE9PSIsInZhbHVlIjoiRFJFN3FyNUM2Mi9HMkdtbmVWNm
J3MTczb3BJbHJSaG9DSXdXT0pEUEdKYjlqbDM0cDdtalNOS09PeE1BQVNjeFBHMUVnL2NpM1NLZjZXVDhqR25IST
AwVWtsQ0tMTG5yWmx1d1I0OVdhaG13eGRNeFQzbEUrUzg1aFpWQTBNUGYiLCJtYWMiOiJkZjlhMjFjYWFlNmY0Yz
YxMDk4NjY5ZjA5MjZhYTM4YzNhZmMyNzk2NmY3ZTJkMGI5MWZmYTM5NTVlYWU4MTMzIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6Ik9hVUdEK2dISk1IMUxSNi9LSEt0ZXc9PSIsInZhbHVlIjoiNHF2
V1QvVW40Q3IzaTliNktNckFHQW1kYkhxUkVaUnpFbnlQMGNXM3Vzcm5CZVd0QytLaEpVRGd6UWIzaE1YZWlmbW1B
VnJyZDN6a1ErMk1ndkUzU1dNUDRDeTlFaEZSdm9UakwwM1JHa3FXaHVDN1ByejE2ME51Zk1BNGpNZlIiLCJtYWMi
OiJjYTFhOWM5Zjg5ZDliYzkxZGRjMGE5NzI0ODgzZTcxODZiZTJiMmZhZDRiMjA2ODdjMGNiNTQwNTU4ZWVhMmRi
IiwidGFnIjoiIn0%3D
Content-Type: application/x-www-form-urlencoded
Content-Length: 113
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
Host: inventory-stg.nexdecade.com
Connection: Keep-alive

_token=QMqn3FfD7Vt6qsEGL6SokjOjmc1wWiaCvQVxDnV2&email=testing%40example.com&password=u]H
[ww6KrA9F.x-F&remember=on
```

ⓘ Permissions-Policy header not implemented

Severity	**Informational**
Reported by module	/httpdata/permissions_policy.js

Description

The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.

Impact

Recommendation

References

[Permissions-Policy / Feature-Policy (MDN)](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)(https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy)
[Permissions Policy (W3C)](https://www.w3.org/TR/permissions-policy-1/)(https://www.w3.org/TR/permissions-policy-1/)

Affected items

Web Server

Details

Locations without Permissions-Policy header:

- https://inventory-stg.nexdecade.com/index.php/assets/css/style.css
- https://inventory-stg.nexdecade.com/index.php/assets/css/login.css
- https://inventory-stg.nexdecade.com/index.php/assets/favicon/
- https://inventory-stg.nexdecade.com/index.php/assets/css/FontAwesome5.6.1.css
- https://inventory-stg.nexdecade.com/index.php/assets/js/tailwind.js
- https://inventory-stg.nexdecade.com/index.php/login
- https://inventory-stg.nexdecade.com/index.php/assets/img/
- https://inventory-stg.nexdecade.com/index.php/assets/css/DaisyUi.full.min.css
- https://inventory-stg.nexdecade.com/index.php/assets/css/RobotoFonts.css
- https://inventory-stg.nexdecade.com/index.php/assets/js/login.js
- https://inventory-stg.nexdecade.com/index.php/assets/js/jquery@3.7.1.min.js
- https://inventory-stg.nexdecade.com/login
- https://inventory-stg.nexdecade.com/uploads/
- https://inventory-stg.nexdecade.com/_ignition/
- https://inventory-stg.nexdecade.com/assets/css/Roboto/
- https://inventory-stg.nexdecade.com/assets/css/webfonts/
- https://inventory-stg.nexdecade.com/index.php/assets/
- https://inventory-stg.nexdecade.com/index.php/assets/js/
- https://inventory-stg.nexdecade.com/index.php/assets/css/

Request headers

```
GET /index.php/assets/css/style.css HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IlNRUitRWjN6dXBkNzdsc1JoVC9kMkE9PSIsInZhbHVlIjoiRFJFN3FyNUM2Mi9HMkdtbmVWNm
J3MTczb3BJbHJSaG9DSXdXT0pEUEdKYjlqbDM0cDdtalNOS09PeE1BQVNjeFBHMUVnL2NpM1NLZjZXVDhqR25IST
AwVWtsQ0tMTG5yWmx1d1I0OVdhaG13eGRNeFQzbEUrUzg1aFpWQTBNUGYiLCJtYWMiOiJkZjlhMjFjYWFlNmY0Yz
YxMDk4NjY5ZjA5MjZhYTM4YzNhZmMyNzk2NmY3ZTJkMGI5MWZmYTM5NTVlYWU4MTMzIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6Ik9hVUdEK2dISk1IMUxSNi9LSEt0ZXc9PSIsInZhbHVlIjoiNHF2
V1QvVW40Q3IzaTliNktNckFHQW1kYkhxUkVaUnpFbnlQMGNXM3Vzcm5CZVd0QytLaEpVRGd6UWIzaE1YZWlmbW1B
VnJyZDN6a1ErMk1ndkUzU1dNUDRDeTlFaEZSdm9UakwwM1JHa3FXaHVDN1ByejE2ME51Zk1BNGpNZlIiLCJtYWMi
OiJjYTFhOWM5Zjg5ZDliYzkxZGRjMGE5NzI0ODgzZTcxODZiZTJiMmZhZDRiMjA2ODdjMGNiNTQwNTU4ZWVhMmRi
IiwidGFnIjoiIn0%3D
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/119.0.0.0 Safari/537.36
Host: inventory-stg.nexdecade.com
Connection: Keep-alive
```

Scanned items (coverage report)

https://inventory-stg.nexdecade.com/
https://inventory-stg.nexdecade.com/assets/
https://inventory-stg.nexdecade.com/assets/css/
https://inventory-stg.nexdecade.com/assets/css/DaisyUi.full.min.css
https://inventory-stg.nexdecade.com/assets/css/FontAwesome5.6.1.css
https://inventory-stg.nexdecade.com/assets/css/login.css
https://inventory-stg.nexdecade.com/assets/css/Roboto/
https://inventory-stg.nexdecade.com/assets/css/RobotoFonts.css
https://inventory-stg.nexdecade.com/assets/css/style.css
https://inventory-stg.nexdecade.com/assets/css/webfonts/
https://inventory-stg.nexdecade.com/assets/favicon/
https://inventory-stg.nexdecade.com/assets/img/
https://inventory-stg.nexdecade.com/assets/js/
https://inventory-stg.nexdecade.com/assets/js/jquery@3.7.1.min.js
https://inventory-stg.nexdecade.com/assets/js/login.js
https://inventory-stg.nexdecade.com/assets/js/tailwind.js
https://inventory-stg.nexdecade.com/assets/scripts/
https://inventory-stg.nexdecade.com/_ignition/
https://inventory-stg.nexdecade.com/_ignition/health-check
https://inventory-stg.nexdecade.com/images/
https://inventory-stg.nexdecade.com/index.php/
https://inventory-stg.nexdecade.com/index.php/assets/
https://inventory-stg.nexdecade.com/index.php/assets/css/
https://inventory-stg.nexdecade.com/index.php/assets/css/DaisyUi.full.min.css
https://inventory-stg.nexdecade.com/index.php/assets/css/FontAwesome5.6.1.css
https://inventory-stg.nexdecade.com/index.php/assets/css/login.css
https://inventory-stg.nexdecade.com/index.php/assets/css/RobotoFonts.css
https://inventory-stg.nexdecade.com/index.php/assets/css/style.css
https://inventory-stg.nexdecade.com/index.php/assets/favicon/
https://inventory-stg.nexdecade.com/index.php/assets/img/
https://inventory-stg.nexdecade.com/index.php/assets/js/
https://inventory-stg.nexdecade.com/index.php/assets/js/jquery@3.7.1.min.js
https://inventory-stg.nexdecade.com/index.php/assets/js/login.js
https://inventory-stg.nexdecade.com/index.php/assets/js/tailwind.js
https://inventory-stg.nexdecade.com/index.php/login
https://inventory-stg.nexdecade.com/login
https://inventory-stg.nexdecade.com/robots.txt
https://inventory-stg.nexdecade.com/uploads/