Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2024-02-15

Generated by Acunetix

Scan of inventory-stg.nexdecade.com

Scan details

Scan information	
Start time	2024-02-15T15:02:14.929971+00:00
Start url	https://inventory-stg.nexdecade.com/
Host	inventory-stg.nexdecade.com
Scan time	43 minutes, 45 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	1
Informational	3

Alerts summary

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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-16

Affected items	Variation
Web Server	1

Cookies Not Marked as HttpOnly

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:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: Required Scope: Unchanged 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-1004

Affected items	Variation
Web Server	1

Content Security Policy (CSP) 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

Generic Email Address Disclosure

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/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: None 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:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N Base Score: 0.0 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged 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-200

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

HTTP Strict Transport Security (HSTS) Policy Not Enabled

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

Description

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org (https://hstspreload.org/)
Strict-Transport-Security (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security)

Affected items

Web Server
Details
URLs where HSTS is not enabled: • https://inventory-stg.nexdecade.com/index.php/assets/js/login.js • https://inventory-stg.nexdecade.com/index.php/assets/css/style.css • https://inventory-stg.nexdecade.com/index.php/assets/js/tailwind.js • https://inventory-stg.nexdecade.com/index.php/assets/css/login.css • https://inventory-stg.nexdecade.com/index.php/assets/css/tailwind.min.css • https://inventory-stg.nexdecade.com/index.php/assets/img/ • https://inventory-stg.nexdecade.com/index.php/assets/favicon/ • 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/js/login.js HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IjVqcjc1QktvaG5obnJGcnd3ejRYMXc9PSIsInZhbHVlIjoib29tWXFYbTh3RHBCVFlBaXYvUH
QyS1Q1OU1VcHMzTWZaWEdJY3pHUXRsbExtWkJZSUtuQnE4N0xYTlkrKzNXZ1ZpRkNidGYzcEVxV2o2azQ0VXRzYk
hEM3lqOTE3eVkyMzN6U1gvRE05M0ZvUDVwUUNLWmhrUGlJRTNmeVNXcFoiLCJtYWMiOiI3YjZjYjI2MjI4YWRjNz
FlYWI1NjliZmFmNzg0NDhjYTBlOGFjOGVlOGU0ZDY1MGM4YjVhYmIwMDJhOTI1YWNhIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6InlXTnJubWRYTE5ZVFFEU0V5RDZWUmc9PSIsInZhbHVlIjoiTEIz
L3dKSE9tMTl3MXVkL2FOT3Ixb0E3NVJndXgyOEFCdDhrdkpOZWV4Uk5iVWlpTnVHNkVHb2kwemk2UTk4dGh3UTNR
bDVZV3lQRUM4N1lFYkcxVG9tcUlJQTN1ai9DN3l1QnIxY2ZNTUEzLzRhcERWVGU1SkpXU3IrNXNzdFIiLCJtYWMi
OiJkOGE3ZTRiZDcyZGEzMGVlODFhNzNkYTYwOGQ0Y2I3NDM3ZTM0YmJmNmQ0OTc1ZTkwY2Q5NjY3Yjg2YmFlMmZi
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
```

Cookies Not Marked as HttpOnly

Severity	**Low**
Reported by module	/RPA/Cookie_Without_HttpOnly.js

Description

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Affected items

Web Server
Verified vulnerability
Details

Cookies without HttpOnly flag set:

- https://inventory-stg.nexdecade.com/index.php/login

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6InBlaVdpRnhtUzk5U3RlK1JTc1NoU0E9PSIsInZhbHVlIjoiSSttQi`

- https://inventory-stg.nexdecade.com/

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IlpyQWxsYVJGT3JZNFE4bWJXZC9nUGc9PSIsInZhbHVlIjoidm9MaF`

- https://inventory-stg.nexdecade.com/login

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IjVqcjc1QktvaG5obnJGcnd3ejRYMXc9PSIsInZhbHVlIjoib29tWX`

- https://inventory-stg.nexdecade.com/index.php/login

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IjQ5alFUUlhjUTNsRnM5VG93WENhcHc9PSIsInZhbHVlIjoiSjNUOT`

- https://inventory-stg.nexdecade.com/login

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IkVud2J5eGdTay85MzFxL1RKQlpyRkE9PSIsInZhbHVlIjoiYk9iaF`

- https://inventory-stg.nexdecade.com/index.php

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IjJHTjliNGY5SjhIRWJtNytmb1RMekE9PSIsInZhbHVlIjoiWVA3bE`

- https://inventory-stg.nexdecade.com/index.php/

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6InFYSEFiZzdQWkdJQ29LODQ3OE9CNVE9PSIsInZhbHVlIjoiZ1JPbn`

- https://inventory-stg.nexdecade.com/

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6InQvRFJNeFBjbmVIRWlNRW5sNlJtY0E9PSIsInZhbHVlIjoidXk1eX`

- https://inventory-stg.nexdecade.com/index.php

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IjdPdWtBSGZLcHhxeStRNjhZYlA1bUE9PSIsInZhbHVlIjoiaUl1UU`

- https://inventory-stg.nexdecade.com/login

  `Set-Cookie: XSRF-TOKEN=eyJpdiI6IjhiKzJJdEJxdXM4OEhIcWJZcE1admc9PSIsInZhbHVlIjoib2Fad3`

- https://inventory-stg.nexdecade.com/index.php/

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6ImF4b3dIc2o2RDYxak9JWmp6b2R5VEE9PSIsInZhbHVlIjoiMGtvQ2
```

- https://inventory-stg.nexdecade.com/index.php/login

```
Set-Cookie: XSRF-TOKEN=eyJpdiI6IlFOWnJjbHR1ajZGQ3RYMzU0ZEMxWGc9PSIsInZhbHVlIjoiRVQyVH
```

Request headers

```
POST /index.php/login HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IjVqcjc1QktvaG5obnJGcnd3ejRYMXc9PSIsInZhbHVlIjoib29tWXFYbTh3RHBCVFlBaXYvUH
QyS1Q1OU1VcHMzTWZaWEdJY3pHUXRsbExtWkJZSUtuQnE4N0xYTlkrKzNXZ1ZpRkNidGYzcEVxV2o2azQ0VXRzYk
hEM3lqOTE3eVkyMzN6U1gvRE05M0ZvUDVwUUNLWmhrUGlJRTNmeVNXcFoiLCJtYWMiOiI3YjZjYjI2MjI4YWRjNz
FlYWI1NjliZmFmNzg0NDhjYTBlOGFjOGVlOGU0ZDY1MGM4YjVhYmIwMDJhOTI1YWNhIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6InlXTnJubWRYTE5ZVFFEU0V5RDZWUmc9PSIsInZhbHVlIjoiTEIz
L3dKSE9tMTl3MXVkL2FOT3Ixb0E3NVJndXgyOEFCdDhrdkpOZWV4Uk5iVWlpTnVHNkVHb2kwemk2UTk4dGh3UTNR
bDVZV3lQRUM4N1lFYkcxVG9tcUlJQTN1ai9DN3l1QnIxY2ZNTUEzLzRhcERWVGU1SkpXU3IrNXNzdFIiLCJtYWMi
OiJkOGE3ZTRiZDcyZGEzMGVlODFhNzNkYTYwOGQ0Y2I3NDM3ZTM0YmJmNmQ0OTc1ZTkwY2Q5NjY3Yjg2YmFlMmZi
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=D0iqDGQO95JJzI25QOdJLjWcitGq65PZVyhuKGOn&email=testing%40example.com&password=u]H
[ww6KrA9F.x-F&remember=on
```

Content Security Policy (CSP) Not Implemented

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

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.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
    default-src 'self';
    script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP

header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP) (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP)
Implementing Content Security Policy (https://hacks.mozilla.org/2016/02/implementing-content-security-policy/)

Affected items

Web Server
Details
Paths without CSP header: • https://inventory-stg.nexdecade.com/index.php/assets/js/login.js • https://inventory-stg.nexdecade.com/index.php/assets/css/style.css • https://inventory-stg.nexdecade.com/index.php/assets/js/tailwind.js • https://inventory-stg.nexdecade.com/index.php/assets/css/login.css • https://inventory-stg.nexdecade.com/index.php/assets/css/tailwind.min.css • https://inventory-stg.nexdecade.com/index.php/assets/img/ • https://inventory-stg.nexdecade.com/index.php/assets/favicon/ • https://inventory-stg.nexdecade.com/login • https://inventory-stg.nexdecade.com/index.php/login • 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/js/login.js HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IjVqcjc1QktvaG5obnJGcnd3ejRYMXc9PSIsInZhbHVlIjoib29tWXFYbTh3RHBCVFlBaXYvUH
QyS1Q1OU1VcHMzTWZaWEdJY3pHUXRsbExtWkJZSUtuQnE4N0xYTlkrKzNXZ1ZpRkNidGYzcEVxV2o2azQ0VXRzYk
hEM3lqOTE3eVkyMzN6U1gvRE05M0ZvUDVwUUNLWmhrUGlJRTNmeVNXcFoiLCJtYWMiOiI3YjZjYjI2MjI4YWRjNz
FlYWI1NjliZmFmNzg0NDhjYTBlOGFjOGVlOGU0ZDY1MGM4YjVhYmIwMDJhOTI1YWNhIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6InlXTnJubWRYTE5ZVFFEU0V5RDZWUmc9PSIsInZhbHVlIjoiTEIz
L3dKSE9tMTl3MXVkL2FOT3Ixb0E3NVJndXgyOEFCdDhrdkpOZWV4Uk5iVWlpTnVHNkVHb2kwemk2UTk4dGh3UTNR
bDVZV3lQRUM4N1lFYkcxVG9tcUlJQTN1ai9DN3l1QnIxY2ZNTUEzLzRhcERWVGU1SkpXU3IrNXNzdFIiLCJtYWMi
OiJkOGE3ZTRiZDcyZGEzMGVlODFhNzNkYTYwOGQ0Y2I3NDM3ZTM0YmJmNmQ0OTc1ZTkwY2Q5NjY3Yjg2YmFlMmZi
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
```

Generic Email Address Disclosure

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

Description

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques (https://en.wikipedia.org/wiki/Anti-spam_techniques)

Affected items

Web Server
Details
Emails found: • https://inventory-stg.nexdecade.com/login **nexdecade@gmail.com** • https://inventory-stg.nexdecade.com/index.php/login **nexdecade@gmail.com**
Request headers

```
GET /login HTTP/1.1
Host: inventory-stg.nexdecade.com
Pragma: no-cache
Cache-Control: no-cache
accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*
/*;q=0.8,application/signed-exchange;v=b3;q=0.7
accept-language: en-US
upgrade-insecure-requests: 1
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
cookie: XSRF-
TOKEN=eyJpdiI6IlpyQWxsYVJGT3JZNFE4bWJXZC9nUGc9PSIsInZhbHVlIjoidm9MaFF1TWlCOTdKSUFkaHdzMk
NkeFFpTmp3TWE3TGxKa2lnbFBlZkFIZkhkd0pqVTVDUC9NRGxJTXdjNnNXVTRBdWYrYkFoOEZzZzFZeUhpZnVWcT
FKS2Y4dzREc1I2dzZkaDE1RjlaT01aVGtheEFYencxWVJadmZkZnBGYVgiLCJtYWMiOiI0MzI3ZGQ1ZDIyZDFkMj
YyYzBlODBkNzQzMWYyNGM0ODI5MjRiZWJjMDRlYzY1NTM2MjA0M2NjOGM4MzQzY2Q3IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IjlDVENGWkpUQjU3MXdTdlJuTHg0QUE9PSIsInZhbHVlIjoiU3lO
T3RWa3hoMkllaWhpMndFZVpQOWV2d01hN1pQNVhmazJ0R3hPMnB0bWlNZ0YxNmpmMjFRVk5oMWdjOVJuLzEycS9Y
VTNGRVFrRXJ3UitVUVpLYkdZYVA3YUw0MW1sL0djcG1GQmovNTdsYWZmR3NyL05PbUZjMWFOUU9rOTAiLCJtYWMi
OiJhODA0MmVlZTc2MDllZTllMDZkMWZhMTY0NmRiMTQxZjJkNTY4YmY4ZTY0YTQwM2M3NzcxYzNjNTA0N2U1YzFi
IiwidGFnIjoiIn0%3D
Accept-Encoding: gzip,deflate,br
Connection: keep-alive
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
```

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)
Permissions Policy (W3C) (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/js/login.js
- https://inventory-stg.nexdecade.com/index.php/assets/css/style.css
- https://inventory-stg.nexdecade.com/index.php/assets/js/tailwind.js
- https://inventory-stg.nexdecade.com/index.php/assets/css/login.css
- https://inventory-stg.nexdecade.com/index.php/assets/css/tailwind.min.css
- https://inventory-stg.nexdecade.com/index.php/assets/img/
- https://inventory-stg.nexdecade.com/index.php/assets/favicon/
- https://inventory-stg.nexdecade.com/login
- https://inventory-stg.nexdecade.com/index.php/login
- https://inventory-stg.nexdecade.com/uploads/
- 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/
- https://inventory-stg.nexdecade.com/uploads/users/

Request headers

```
GET /index.php/assets/js/login.js HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6IjVqcjc1QktvaG5obnJGcnd3ejRYMXc9PSIsInZhbHVlIjoib29tWXFYbTh3RHBCVFlBaXYvUH
QyS1Q1OU1VcHMzTWZaWEdJY3pHUXRsbExtWkJZSUtuQnE4N0xYTlkrKzNXZ1ZpRkNidGYzcEVxV2o2azQ0VXRzYk
hEM3lqOTE3eVkyMzN6U1gvRE05M0ZvUDVwUUNLWmhrUGlJRTNmeVNXcFoiLCJtYWMiOiI3YjZjYjI2MjI4YWRjNz
FlYWI1NjliZmFmNzg0NDhjYTBlOGFjOGVlOGU0ZDY1MGM4YjVhYmIwMDJhOTI1YWNhIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6InlXTnJubWRYTE5ZVFFEU0V5RDZWUmc9PSIsInZhbHVlIjoiTEIz
L3dKSE9tMTl3MXVkL2FOT3Ixb0E3NVJndXgyOEFCdDhrdkpOZWV4Uk5iVWlpTnVHNkVHb2kwemk2UTk4dGh3UTNR
bDVZV3lQRUM4N1lFYkcxVG9tcUlJQTN1ai9DN3l1QnIxY2ZNTUEzLzRhcERWVGU1SkpXU3IrNXNzdFIiLCJtYWMi
OiJkOGE3ZTRiZDcyZGEzMGVlODFhNzNkYTYwOGQ0Y2I3NDM3ZTM0YmJmNmQ0OTc1ZTkwY2Q5NjY3Yjg2YmFlMmZi
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/login.css
https://inventory-stg.nexdecade.com/assets/css/style.css
https://inventory-stg.nexdecade.com/assets/css/tailwind.min.css
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/login.js
https://inventory-stg.nexdecade.com/assets/js/tailwind.js
https://inventory-stg.nexdecade.com/assets/scripts/
https://inventory-stg.nexdecade.com/images/
https://inventory-stg.nexdecade.com/index.php
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/login.css
https://inventory-stg.nexdecade.com/index.php/assets/css/style.css
https://inventory-stg.nexdecade.com/index.php/assets/css/tailwind.min.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/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/
https://inventory-stg.nexdecade.com/uploads/users/