Acunetix
by Invicti

Developer Report

Acunetix Security Audit

2024-03-04

Generated by Acunetix

Scan of inventory-stg.nexdecade.com

Scan details

Scan information	
Start time	2024-03-04T12:28:10.630239+00:00
Start url	https://inventory-stg.nexdecade.com/
Host	inventory-stg.nexdecade.com
Scan time	32 minutes, 47 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	7
Critical	0
High	0
Medium	2
Low	1
Informational	4

Alerts summary

Host header attack

Classification	
CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/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: None Integrity Impact to the Vulnerable System: Low 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:L/A:N Base Score: 5.3 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Unchanged Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 2.6 Access Vector: Local_access Access Complexity: High Authentication: None Confidentiality Impact: Partial Integrity Impact: Partial Availability Impact: None Exploitability: Unproven Remediation Level: Workaround 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-20

Affected items	Variation
/index.php/login	1

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

Clickjacking: CSP frame-ancestors missing

Classification

CVSS4	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Base Score: 5.1 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: Low 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:N/I:L/A:N Base Score: 5.8 Attack Vector: Network Attack Complexity: Low Privileges Required: None User Interaction: None Scope: Changed Confidentiality Impact: None Integrity Impact: Low Availability Impact: None
CVSS2	Base Score: 4.3 Access Vector: Network_accessible Access Complexity: Medium Authentication: None Confidentiality Impact: None Integrity Impact: Partial 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

ⓘ 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

Host header attack

Severity	**Medium**
Reported by module	/Scripts/PostCrawl/Host_Header_Attack.script

Description

In many cases, developers are trusting the HTTP Host header value and using it to generate links, import scripts and even generate password resets links with its value. This is a very bad idea, because the HTTP Host header can be controlled by an attacker. This can be exploited using web-cache poisoning and by abusing alternative channels like password reset emails.

Impact

An attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways.

Recommendation

The web application should use the SERVER_NAME instead of the Host header. It should also create a dummy vhost that catches all requests with unrecognized Host headers. This can also be done under Nginx by specifying a non-wildcard SERVER_NAME, and under Apache by using a non-wildcard serverName and turning the UseCanonicalName directive on. Consult references for detailed information.

References

[Practical HTTP Host header attacks](https://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html) (https://www.skeletonscribe.net/2013/05/practical-http-host-header-attacks.html)
[Apache](http://httpd.apache.org/docs/trunk/vhosts/examples.html#defaultallports) (http://httpd.apache.org/docs/trunk/vhosts/examples.html#defaultallports)
[nginx](https://www.nginx.com/resources/wiki/start/topics/examples/server_blocks/) (https://www.nginx.com/resources/wiki/start/topics/examples/server_blocks/)
[Automated Detection of Host Header Attacks](https://www.acunetix.com/blog/articles/automated-detection-of-host-header-attacks/) (https://www.acunetix.com/blog/articles/automated-detection-of-host-header-attacks/)

Affected items

/index.php/login

Details

Host header **evilhostaf5e4x8m.com** was reflected inside an **LINK** tag (**href** attribute).

Request headers

```
GET https://inventory-stg.nexdecade.com/index.php/login HTTP/1.1
Host: evilhostaf5e4x8m.com
X-Forwarded-Host: evilhostaf5e4x8m.com
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
Connection: Keep-alive
```

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=eyJpdiI6IlBqVnc1bXFOVUlSL3Flc2ZMYkNMNGc9PSIsInZhbHVlIjoiN3RqZlN4UkFLZmVMZk1uS1V5NH
BqK0ZiWXNoWUU0d3ByMm9TeEF1NXIxR1oxMVNOWWFSUkFhSEFJTElvODNRYmRjVDN3OVlXVDVtU1VZK1pieXMxMF
JhTFBXWXJWWVUxaWZ0OEJEK01ISUNjUTFuVUFPZGptNisrUXRGaGVvbkYiLCJtYWMiOiI2NDdlZjdlYTczYjRiZj
BlYmQ1YTNhNjJhYzllM2E5M2U2MDA0ODBmN2ZjYmYwOTM3ZmMxYTg5MjBhOTQ3OGFlIiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IkdQcHZpRzhEVTIzQWRmSWVDMGtyb1E9PSIsInZhbHVlIjoibEg2
UG01Z2FUd0YzQWtib2I1RkNydDhSUldGM3plTVhrZmh4eGpmdnZncE9oZkE2aWpkUkw2eXlvVVNZaDAwTjdVZFRG
dHlwSGNsdHd3T2YzTldRdzZrcXFyYzBZMlRiOHpWdGFnUUpXcWl6akw4cHF3cy9BeDB1UTcza1prVHEiLCJtYWMi
OiJhYjQ3MWY0YjUwYzliNDAxYTczZDE0NzQxMDMyMGM3MzM0ZWM2MzQ5NmU1OGUyNzNiNmI1NzcyYTRjZjBjZGQy
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
```

Clickjacking: CSP frame-ancestors missing

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

Description

Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

The server didn't return a **frame-ancestors** directive in the Content-Security-Policy header which means that this website could be at risk of a clickjacking attack. The frame-ancestors directives can be used to indicate whether or not a browser should be allowed to render a page inside a frame. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.

Impact

The impact depends on the affected web application.

Recommendation

Configure your web server to include a CSP header with frame-ancestors directive and an X-Frame-Options header. Consult Web references for more information about the possible values for this header.

References

OWASP Clickjacking (https://cheatsheetseries.owasp.org/cheatsheets/Clickjacking_Defense_Cheat_Sheet.html)
CSP: frame-ancestors (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy/frame-ancestors)
The X-Frame-Options response header (https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options)

Affected items

Web Server
Details
Paths without CSP frame-ancestors: • https://inventory-stg.nexdecade.com/index.php/assets/css/tailwind.min.css • https://inventory-stg.nexdecade.com/index.php/assets/css/style.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/js/tailwind.js • https://inventory-stg.nexdecade.com/index.php/assets/css/login.css • https://inventory-stg.nexdecade.com/index.php/assets/js/login.js • https://inventory-stg.nexdecade.com/login • https://inventory-stg.nexdecade.com/index.php/login • https://inventory-stg.nexdecade.com/_ignition/ • 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/tailwind.min.css HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6ImZCZFczVHRnUER2NGJmbVg4SVhFdnc9PSIsInZhbHVlIjoiY1Nhcy9NeCswckhrUlBWU1V5SG
hqbkNQaCtFbGNMTnRxOG1NL2dyUzg5alc1Vm1pdkluQjVQd0F1Qko1RXZxOVEzcGF1VXRvWkVsRmoyL1lQNk5JUT
VZRnd3Ri9pdUhtc1IvYkN0V1BBOFRUdlRjOHhlMUhFTFpyWWd5dEt6eDMiLCJtYWMiOiI3NDdlOWFjZjViZDMxOT
ljZjBkNTZjOGE4ZGJmNzdmMTVmNmM4ZWUwM2Y0Y2Y0MmM5YWE2Y2Y5OGUxNGQ3NmI5IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IjcxczlSeExFVi9MVTVnS0x2YU9lTHc9PSIsInZhbHVlIjoiTDVl
WE9KTnBtQXRpNEVwZWtpWUlsWDk0eGtvVW9iVDZQYmdieUtDbDhnSUE3WmNwYVpUbWMxdTJqUk1seHVSLzFndFFG
ZjZNaDVNeEJBT0NKS3V5ZExaMXFGdHNDdzBRRUZ2UUVpaFhMMmgzRWJzbVI1ZVU1K25vL0F3eW83UHAiLCJtYWMi
OiI2ODdhOGZiYTA2ZGU4NjlmY2JkZWRkNTZmNDMzMDE1YmEyOWNmZTBiZTM3YmQ5MTBiYjk4NGMzZGI5YjU2MmZl
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/)
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

- **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'; img-src * data:; style-src 'self' https://cdnjs.cloudflare.com/ https://fonts.googleapis.com/ 'unsafe-inline'; base-uri 'self'; form-action 'self'; script-src 'self' https://cdnjs.cloudflare.com/ https://fonts.googleapis.com/ https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/ 'unsafe-inline' 'unsafe-eval'; font-src 'self' data: https://cdnjs.cloudflare.com/ajax/libs/ https://fonts.gstatic.com/s/;
    - **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=eyJpdiI6ImZCZFczVHRnUER2NGJmbVg4SVhFdnc9PSIsInZhbHVlIjoiY1Nhcy9NeCswckhrUlBWU1V5SG
hqbkNQaCtFbGNMTnRxOG1NL2dyUzg5alc1Vm1pdkluQjVQd0F1Qko1RXZxOVEzcGF1VXRvWkVsRmoyL1lQNk5JUT
VZRnd3Ri9pdUhtc1IvYkN0V1BBOFRUdlRjOHhlMUhFTFpyWWd5dEt6eDMiLCJtYWMiOiI3NDdlOWFjZjViZDMxOT
ljZjBkNTZjOGE4ZGJmNzdmMTVmNmM4ZWUwM2Y0Y2Y0MmM5YWE2Y2Y5OGUxNGQ3NmI5IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IjcxczlSeExFVi9MVTVnS0x2YU9lTHc9PSIsInZhbHVlIjoiTDVl
WE9KTnBtQXRpNEVwZWtpWUlsWDk0eGtvVW9iVDZQYmdieUtDbDhnSUE3WmNwYVpUbWMxdTJqUk1seHVSLzFndFFG
ZjZNaDVNeEJBT0NKS3V5ZExaMXFGdHNDdzBRRUZ2UUVpaFhMMmgzRWJzbVI1ZVU1K25vL0F3eW83UHAiLCJtYWMi
OiI2ODdhOGZiYTA2ZGU4NjlmY2JkZWRkNTZmNDMzMDE1YmEyOWNmZTBiZTM3YmQ5MTBiYjk4NGMzZGI5YjU2MmZl
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=dZBaZ0qQZi1uzkmKkp90OeFrGLhh8mKO9J5ohvmb&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/)](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

- **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'; img-src * data:; style-src 'self' https://cdnjs.cloudflare.com/ https://fonts.googleapis.com/ 'unsafe-inline'; base-uri 'self'; form-action 'self'; script-src 'self' https://cdnjs.cloudflare.com/ https://fonts.googleapis.com/ https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/ 'unsafe-inline' 'unsafe-eval'; font-src 'self' data: https://cdnjs.cloudflare.com/ajax/libs/ https://fonts.gstatic.com/s/;
  - **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=eyJpdiI6ImZCZFczVHRnUER2NGJmbVg4SVhFdnc9PSIsInZhbHVlIjoiY1Nhcy9NeCswckhrUlBWU1V5SG
hqbkNQaCtFbGNMTnRxOG1NL2dyUzg5alc1Vm1pdkluQjVQd0F1Qko1RXZxOVEzcGF1VXRvWkVsRmoyL1lQNk5JUT
VZRnd3Ri9pdUhtc1IvYkN0V1BBOFRUdlRjOHhlMUhFTFpyWWd5dEt6eDMiLCJtYWMiOiI3NDdlOWFjZjViZDMxOT
ljZjBkNTZjOGE4ZGJmNzdmMTVmNmM4ZWUwM2Y0Y2Y0MmM5YWE2Y2Y5OGUxNGQ3NmI5IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IjcxczlSeExFVi9MVTVnS0x2YU9lTHc9PSIsInZhbHVlIjoiTDVl
WE9KTnBtQXRpNEVwZWtpWUlsWDk0eGtvVW9iVDZQYmdieUtDbDhnSUE3WmNwYVpUbWMxdTJqUk1seHVSLzFndFFG
ZjZNaDVNeEJBT0NKS3V5ZExaMXFGdHNDdzBRRUZ2UUVpaFhMMmgzRWJzbVI1ZVU1K25vL0F3eW83UHAiLCJtYWMi
OiI2ODdhOGZiYTA2ZGU4NjlmY2JkZWRkNTZmNDMzMDE1YmEyOWNmZTBiZTM3YmQ5MTBiYjk4NGMzZGI5YjU2MmZl
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=dZBaZ0qQZi1uzkmKkp90OeFrGLhh8mKO9J5ohvmb&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/)
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
• **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'; img-src * data:; style-src 'self' https://cdnjs.cloudflare.com/ https://fonts.googleapis.com/ 'unsafe-inline'; base-uri 'self'; form-action 'self'; script-src 'self' https://cdnjs.cloudflare.com/ https://fonts.googleapis.com/ https://cdnjs.cloudflare.com/ajax/libs/font-awesome/6.5.1/webfonts/ 'unsafe-inline' 'unsafe-eval'; font-src 'self' data: https://cdnjs.cloudflare.com/ajax/libs/ https://fonts.gstatic.com/s/; ◦ **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=eyJpdiI6ImZCZFczVHRnUER2NGJmbVg4SVhFdnc9PSIsInZhbHVlIjoiY1Nhcy9NeCswckhrUlBWU1V5SG
hqbkNQaCtFbGNMTnRxOG1NL2dyUzg5alc1Vm1pdkluQjVQd0F1Qko1RXZxOVEzcGF1VXRvWkVsRmoyL1lQNk5JUT
VZRnd3Ri9pdUhtc1IvYkN0V1BBOFRUdlRjOHhlMUhFTFpyWWd5dEt6eDMiLCJtYWMiOiI3NDdlOWFjZjViZDMxOT
ljZjBkNTZjOGE4ZGJmNzdmMTVmNmM4ZWUwM2Y0Y2Y0MmM5YWE2Y2Y5OGUxNGQ3NmI5IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IjcxczlSeExFVi9MVTVnS0x2YU9lTHc9PSIsInZhbHVlIjoiTDVl
WE9KTnBtQXRpNEVwZWtpWUlsWDk0eGtvVW9iVDZQYmdieUtDbDhnSUE3WmNwYVpUbWMxdTJqUk1seHVSLzFndFFG
ZjZNaDVNeEJBT0NKS3V5ZExaMXFGdHNDdzBRRUZ2UUVpaFhMMmgzRWJzbVI1ZVU1K25vL0F3eW83UHAiLCJtYWMi
OiI2ODdhOGZiYTA2ZGU4NjlmY2JkZWRkNTZmNDMzMDE1YmEyOWNmZTBiZTM3YmQ5MTBiYjk4NGMzZGI5YjU2MmZl
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=dZBaZ0qQZi1uzkmKkp90OeFrGLhh8mKO9J5ohvmb&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)
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/css/tailwind.min.css
- https://inventory-stg.nexdecade.com/index.php/assets/css/style.css
- https://inventory-stg.nexdecade.com/index.php/assets/img/
- https://inventory-stg.nexdecade.com/index.php/assets/js/tailwind.js
- https://inventory-stg.nexdecade.com/index.php/assets/favicon/
- https://inventory-stg.nexdecade.com/index.php/assets/css/login.css
- https://inventory-stg.nexdecade.com/index.php/assets/js/login.js
- 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/_ignition/
- 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/tailwind.min.css HTTP/1.1
Referer: https://inventory-stg.nexdecade.com/
Cookie: XSRF-
TOKEN=eyJpdiI6ImZCZFczVHRnUER2NGJmbVg4SVhFdnc9PSIsInZhbHVlIjoiY1Nhcy9NeCswckhrUlBWU1V5SG
hqbkNQaCtFbGNMTnRxOG1NL2dyUzg5alc1Vm1pdkluQjVQd0F1Qko1RXZxOVEzcGF1VXRvWkVsRmoyL1lQNk5JUT
VZRnd3Ri9pdUhtc1IvYkN0V1BBOFRUdlRjOHhlMUhFTFpyWWd5dEt6eDMiLCJtYWMiOiI3NDdlOWFjZjViZDMxOT
ljZjBkNTZjOGE4ZGJmNzdmMTVmNmM4ZWUwM2Y0Y2Y0MmM5YWE2Y2Y5OGUxNGQ3NmI5IiwidGFnIjoiIn0%3D;
nexdecade_inventory_session=eyJpdiI6IjcxczlSeExFVi9MVTVnS0x2YU9lTHc9PSIsInZhbHVlIjoiTDVl
WE9KTnBtQXRpNEVwZWtpWUlsWDk0eGtvVW9iVDZQYmdieUtDbDhnSUE3WmNwYVpUbWMxdTJqUk1seHVSLzFndFFG
ZjZNaDVNeEJBT0NKS3V5ZExaMXFGdHNDdzBRRUZ2UUVpaFhMMmgzRWJzbVI1ZVU1K25vL0F3eW83UHAiLCJtYWMi
OiI2ODdhOGZiYTA2ZGU4NjlmY2JkZWRkNTZmNDMzMDE1YmEyOWNmZTBiZTM3YmQ5MTBiYjk4NGMzZGI5YjU2MmZl
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/_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/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/