Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2025-07-30

Generated by Acunetix

Scan of 100.100.0.5:9443

Scan details

Scan information	
Start time	2025-07-29T17:00:57.262156+00:00
Start url	https://100.100.0.5:9443/
Host	100.100.0.5:9443
Scan time	734 minutes, 5 seconds
Profile	Full Scan
Server information	nginx/1.22.1
Responsive	True
Server OS	Unknown
Application build	25.1.250204093

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	24
Critical	0
High	0
Medium	9
Low	3
Informational	12

Affected items

Web Server	
Alert group	**DataTables Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	This affects the package datatables.net before 1.11.3. If an array is passed to the HTML escape entities function it would not have its contents escaped.
Recommendations	
Alert variants	
Details	datatables v1.10.22-1.10.22

Web Server	
Alert group	**HTTP Strict Transport Security (HSTS) Policy Not Enabled**
Severity	Medium
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.
Recommendations	It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information
Alert variants	
Details	URLs where HSTS is not enabled: • https://100.100.0.5:9443/index.cgi • https://100.100.0.5:9443/styles/default/plugins/datepicker/locales/bootstrap-datepicker.en.js • https://100.100.0.5:9443/registration.cgi • https://100.100.0.5:9443/admin/index.cgi • https://100.100.0.5:9443/ • https://100.100.0.5:9443/admin/

```
GET / HTTP/1.1
Host: 100.100.0.5:9443
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
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/131.0.0.0 Safari/537.36
```

/admin/index.cgi	
Alert group	**Host header attack**
Severity	Medium

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.
Recommendations	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.
Alert variants	
Details	Host header **evilhost42MIECYv.com** was reflected inside an **FORM** tag (**action** attribute).

```
GET /admin/index.cgi HTTP/1.1
Host: evilhost42MIECYv.com
X-Forwarded-Host: 100.100.0.5:9443
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/131.0.0.0 Safari/537.36
Connection: Keep-alive
```

/index.cgi	
Alert group	**Host header attack**
Severity	Medium
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.
Recommendations	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.
Alert variants	
Details	Host header **evilhostSBcUvVb1.com** was reflected inside an **FORM** tag (**action** attribute).

```
GET /index.cgi HTTP/1.1
Host: evilhostSBcUvVb1.com
X-Forwarded-Host: 100.100.0.5:9443
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/131.0.0.0 Safari/537.36
Connection: Keep-alive
```

/registration.cgi	
Alert group	**Host header attack**
Severity	Medium

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.
Recommendations	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.
Alert variants	
Details	Host header **evilhostmrNpSHpP.com** was reflected inside an **FORM** tag (**action** attribute).

```
GET /registration.cgi HTTP/1.1
Host: evilhostmrNpSHpP.com
X-Forwarded-Host: 100.100.0.5:9443
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/131.0.0.0 Safari/537.36
Connection: Keep-alive
```

Web Server	
Alert group	**Invalid SSL Certificate**
Severity	Medium
Description	One of the TLS/SSL certificates sent by your server has either expired or is not yet valid. Most web browsers will present end-users with a security warning, asking them to manually confirm the authenticity of your certificate chain. Software or automated systems may silently refuse to connect to the server. This alert is not necessarily caused by the server (leaf) certificate, but may have been triggered by an intermediate certificate. Please refer to the certificate serial number in the alert details to identify the affected certificate.
Recommendations	Verify Start Date and/or End Dates of your SSL Certificate.
Alert variants	
Details	The TLS/SSL certificate (serial: 00cdae2408c6868a80) has expired.. The certificate validity period is between **Sun Mar 10 2019 07:35:43 GMT+0000 (UTC)** and **Tue Mar 09 2021 07:35:43 GMT+0000 (UTC)**

Web Server	
Alert group	**SSL Certificate Name Hostname Mismatch**
Severity	Medium
Description	Acunetix detected a hostname mismatch in the SSL certificate. This happens when the common name to which an SSL Certificate is issued (e.g., www.example.com) doesn't exactly match the name displayed in the URL bar.
Recommendations	The process of fixing name-hostname mismatch issues varies depending on the host or the certificate authority used. Please refer to the corresponding documentation.

Alert variants	
Details	**Subject:** C=AU,ST=Some-State,O=Internet Widgits Pty Ltd **Issuer:** C=AU,ST=Some-State,O=Internet Widgits Pty Ltd **Public Key Algorithm:** rsaEncryption **Hash Algorithm:** sha256 **Certificate:** -----BEGIN CERTIFICATE----- MIIDBjCCAe4CCQDNriQIxoaKgDANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJB VTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0 cyBQdHkgTHRkMB4XDTE5MDMxMDA3MzU0M1oXDTIxMDMwOTA3MzU0M1owRTELMAkG A1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoMGEludGVybmV0 IFdpZGdpdHMgUHR5IEx0ZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB AMB7YoTgRYhwezGo5qOq9EMrf84iX5013C+ScOjZBx580LBMpl+caiDZc2569hfn b2qWnHZLF+6cqBUV9KmA0qlsMzeevMLoTuo2T26m1/xIvyECUGsJoBF2+CTleRav XOju6xOwxErBrZGUODfOuHfPy/a9GQYDDmNy0CHVA5QFacSuWsFxyvHIayPrCBIe CiwArlPQqWrqs3cQjKWTBPMrcJiHEX4cD7uVuo6ckawI3+uVN5uPUZg6JaoWm9ki zVvSKHfaB3bIYqcwVhbiLBhkEEg7RwRxRNuPH5WrrlghsdyW1bjfJ0WL5l/nEEf+ 6UyTl9tIakovvD1Z373Eb30CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAG3wqZeb9 21gRaePVeQ1boVUdLEdbV3coorO/hy0IriVbW6HRi4Ph8nAeL8VGYsvqCR0usoqp vNikMld/YnVL1PdE4P9z2yzy7SjtBrX4otzV5rAE3ZyQpUM+cKoY4PBqBj/dmH/C HVP80YaPDIYVNvh9PPWD5VntTTbGqbr0UktoTl5QrJwUIdrZl+YObdeS1LAUGXvd fO2Zs1IqbBEUEfuZb95+DospMOcOuesfqG44raKasxjXncDDtms4JF8p1rwJ3MOA OfCoVE9sZxnnRisJCjmQzGmUJaNOW0qOMYY5uhZLfyzRaIiN2285R8NLA/KonvEU BTO+ahJT7BW/yg== -----END CERTIFICATE-----

Web Server	
Alert group	**SSL Untrusted Root Certificate**
Severity	Medium
Description	Acunetix detected that the SSL Certificate is not signed by the trusted root.
Recommendations	The process of fixing untrusted root certificate issues varies depending on the host or the certificate authority used. Please refer to the corresponding documentation.
Alert variants	

Details	**Subject:** C=AU,ST=Some-State,O=Internet Widgits Pty Ltd **Issuer:** C=AU,ST=Some-State,O=Internet Widgits Pty Ltd **Public Key Algorithm:** rsaEncryption **Hash Algorithm:** sha256 **Certificate:** -----BEGIN CERTIFICATE----- MIIDBjCCAe4CCQDNriQIxoaKgDANBgkqhkiG9w0BAQsFADBFMQswCQYDVQQGEwJB VTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UECgwYSW50ZXJuZXQgV2lkZ2l0 cyBQdHkgTHRkMB4XDTE5MDMxMDA3MzU0M1oXDTIxMDMwOTA3MzU0M1owRTELMAkG A1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUxITAfBgNVBAoMGEludGVybmV0 IFdpZGdpdHMgUHR5IEx0ZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB AMB7YoTgRYhwezGo5qOq9EMrf84iX5013C+ScOjZBx580LBMpl+caiDZc2569hfn b2qWnHZLF+6cqBUV9KmA0qlsMzeevMLoTuo2T26m1/xIvyECUGsJoBF2+CTleRav XOju6xOwxErBrZGUODfOuHfPy/a9GQYDDmNy0CHVA5QFacSuWsFxyvHIayPrCBIe CiwArlPQqWrqs3cQjKWTBPMrcJiHEX4cD7uVuo6ckawI3+uVN5uPUZg6JaoWm9ki zVvSKHfaB3bIYqcwVhbiLBhkEEg7RwRxRNuPH5WrrlghsdyW1bjfJ0WL5l/nEEf+ 6UyTl9tIakovvD1Z373Eb30CAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAG3wqZeb9 21gRaePVeQ1boVUdLEdbV3coorO/hy0IriVbW6HRi4Ph8nAeL8VGYsvqCR0usoqp vNikMld/YnVL1PdE4P9z2yzy7SjtBrX4otzV5rAE3ZyQpUM+cKoY4PBqBj/dmH/C HVP80YaPDIYVNvh9PPWD5VntTTbGqbr0UktoTl5QrJwUIdrZl+YObdeS1LAUGXvd fO2Zs1IqbBEUEfuZb95+DospMOcOuesfqG44raKasxjXncDDtms4JF8p1rwJ3MOA OfCoVE9sZxnnRisJCjmQzGmUJaNOW0qOMYY5uhZLfyzRaIiN2285R8NLA/KonvEU BTO+ahJT7BW/yg== -----END CERTIFICATE-----

Web Server	
Alert group	**TLS/SSL Weak Cipher Suites**
Severity	Medium
Description	The remote host supports TLS/SSL cipher suites with weak or insecure properties.
Recommendations	Reconfigure the affected application to avoid use of weak cipher suites.
Alert variants	

Details	Weak TLS/SSL Cipher Suites: (offered via TLS1.2 on port 9443): • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CCM_8 • TLS_RSA_WITH_AES_256_CCM • TLS_RSA_WITH_ARIA_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CCM_8 • TLS_RSA_WITH_AES_128_CCM • TLS_RSA_WITH_ARIA_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_CAMELLIA_256_CBC_SHA • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_CAMELLIA_128_CBC_SHA

Web Server	
Alert group	**Clickjacking: CSP frame-ancestors missing**
Severity	Low
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.
Recommendations	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.
Alert variants	
Details	Paths without CSP frame-ancestors: • https://100.100.0.5:9443/registration.cgi • https://100.100.0.5:9443/admin/index.cgi • https://100.100.0.5:9443/index.cgi • https://100.100.0.5:9443/ • https://100.100.0.5:9443/admin/

```
GET / HTTP/1.1
Host: 100.100.0.5:9443
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
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/131.0.0.0 Safari/537.36
```

Web Server	
Alert group	**Cookies with missing, inconsistent or contradictory properties (verified)**
Severity	Low
Description	At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.
Recommendations	Ensure that the cookies configuration complies with the applicable standards.
Alert variants	

Details	List of cookies with missing, inconsistent or contradictory properties:
	• https://100.100.0.5:9443/index.cgi
	Cookie was set with:
	`Set-Cookie: language=english; expires="Fri, 1-Jan-2038 00:00:01"`
	This cookie has the following issues:
	`- SameSite attribute with invalid value.`
	`As the SameSite attribute has evolved over time, values other th`
	• https://100.100.0.5:9443/admin/index.cgi
	Cookie was set with:
	`Set-Cookie: language=english; expires="Fri, 1-Jan-2038 00:00:01"`
	This cookie has the following issues:
	`- SameSite attribute with invalid value.`
	`As the SameSite attribute has evolved over time, values other th`
	• https://100.100.0.5:9443/admin/index.cgi
	Cookie was set with:
	`Set-Cookie: language=russian; expires="Fri, 1-Jan-2038 00:00:01"`
	This cookie has the following issues:
	`- SameSite attribute with invalid value.`
	`As the SameSite attribute has evolved over time, values other th`
	• https://100.100.0.5:9443/index.cgi
	Cookie was set with:
	`Set-Cookie: language=russian; expires="Fri, 1-Jan-2038 00:00:01"`
	This cookie has the following issues:
	`- SameSite attribute with invalid value.`
	`As the SameSite attribute has evolved over time, values other th`
	• https://100.100.0.5:9443/registration.cgi
	Cookie was set with:
	`Set-Cookie: language=english; expires="Fri, 1-Jan-2038 00:00:01"`
	This cookie has the following issues:
	`- SameSite attribute with invalid value.`
	`As the SameSite attribute has evolved over time, values other th`

- https://100.100.0.5:9443/registration.cgi

  Cookie was set with:

  ```
  Set-Cookie: language=russian; expires="Fri, 1-Jan-2038 00:00:01"
  ```

  This cookie has the following issues:

  ```
   - SameSite attribute with invalid value.
  As the SameSite attribute has evolved over time, values other th
  ```

```
GET /index.cgi?&language=russian&login_page=1 HTTP/1.1
Referer: https://100.100.0.5:9443/
Cookie: language=english
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Possible sensitive directories**
Severity	Low
Description	One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.
Recommendations	Restrict access to these directories or remove them from the website.
Alert variants	
Details	Possible sensitive directories: • https://100.100.0.5:9443/**admin**

```
GET /admin/ HTTP/1.1
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Access-Control-Allow-Origin header with wildcard (*) value**
Severity	Informational

Description	Cross-origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g. fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on the value of the Origin request header, "*", or "null" in the response. If a website responds with Access-Control-Allow-Origin: * the requested resource allows sharing with every origin. Therefore, any website can make XHR (XMLHTTPRequest) requests to the site and access the responses.
Recommendations	Check whether Access-Control-Allow-Origin: * is appropriate for the resource/response.
Alert variants	
Details	Affected paths (max. 25): • /index.cgi • /registration.cgi • /api.cgi/builds • /admin/index.cgi • /api.cgi/ • /api.cgi/streets • / • /admin/

```
GET / HTTP/1.1
Origin: https://100.100.0.5
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**An Unsafe Content Security Policy (CSP) Directive in Use (verified)**
Severity	Informational
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.
Recommendations	See alert details for available remediation advice.
Alert variants	

Details	• **An Unsafe Content Security Policy (CSP) Directive in Use** ◦ **First observed on:** https://100.100.0.5:9443/ ◦ **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' https:; style-src 'self' 'unsafe-inline'; img-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

```
GET / HTTP/1.1
Host: 100.100.0.5:9443
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
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/131.0.0.0 Safari/537.36
```

Web Server	
Alert group	**Content Security Policy (CSP) Not Implemented**
Severity	Informational

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.

Recommendations	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.
Alert variants	
Details	Paths without CSP header: • https://100.100.0.5:9443/styles/default/plugins/datepicker/locales/bootstrap-datepicker.en.js

```
GET /styles/default/plugins/datepicker/locales/bootstrap-datepicker.en.js HTTP/1.1
Referer: https://100.100.0.5:9443/admin/index.cgi
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Generic Email Address Disclosure**
Severity	Informational
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.
Recommendations	Check references for details on how to solve this problem.
Alert variants	
Details	Emails found: • https://100.100.0.5:9443/registration.cgi **account@mail.com**

```
GET /registration.cgi?module=Msgs HTTP/1.1
Referer: https://100.100.0.5:9443/registration.cgi
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries (verified)**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.

Alert variants	
Details	• **jQuery 3.5.1** ◦ URL: https://100.100.0.5:9443/styles/default/js/jquery.min.js ◦ Detection method: The library's name and version were determined based on the file's syntax fingerprint, and contents. Acunetix verified the library version with the file's unique syntax fingerprint, which matched the syntax fingerprint expected by Acunetix. ◦ References: ▪ https://code.jquery.com/

```
GET /styles/default/js/jquery.min.js HTTP/1.1
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	• **JavaScript Cookie 2.0.3** ◦ URL: https://100.100.0.5:9443/styles/default/js/js.cookies.js ◦ Detection method: The library's name and version were determined based on the file's contents. ◦ References: ▪ https://github.com/js-cookie/js-cookie/releases

```
GET /styles/default/js/js.cookies.js HTTP/1.1
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.
Alert variants	

Details	• **mustache.js 2.2.1** ◦ URL: https://100.100.0.5:9443/styles/default/js/mustache.min.js ◦ Detection method: The library's name and version were determined based on the file's contents. ◦ References: ▪ https://github.com/janl/mustache.js/releases

```
GET /styles/default/js/mustache.min.js HTTP/1.1
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Outdated JavaScript libraries**
Severity	Informational
Description	You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.
Recommendations	Upgrade to the latest version.
Alert variants	
Details	• **Select2 4.0.10** ◦ URL: https://100.100.0.5:9443/styles/default/js/select2.min.js ◦ Detection method: The library's name and version were determined based on the file's contents. ◦ References: ▪ https://github.com/select2/select2/tags

```
GET /styles/default/js/select2.min.js HTTP/1.1
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Permissions-Policy header not implemented**
Severity	Informational
Description	The Permissions-Policy header allows developers to selectively enable and disable use of various browser features and APIs.
Recommendations	
Alert variants	

Details	Locations without Permissions-Policy header: • https://100.100.0.5:9443/styles/default/plugins/datepicker/locales/bootstrap-datepicker.en.js • https://100.100.0.5:9443/img/logo/ • https://100.100.0.5:9443/captcha/ • https://100.100.0.5:9443/styles/default/img/social/ • https://100.100.0.5:9443/styles/default/img/admin/ • https://100.100.0.5:9443/styles/default/webfonts/ • https://100.100.0.5:9443/styles/default/css/skins/ • https://100.100.0.5:9443/styles/default/js/acp/ • https://100.100.0.5:9443/api/ • https://100.100.0.5:9443/error/ • https://100.100.0.5:9443/img/ • https://100.100.0.5:9443/styles/ • https://100.100.0.5:9443/styles/default/fonts/ • https://100.100.0.5:9443/styles/default/ • https://100.100.0.5:9443/styles/default/css/images/ • https://100.100.0.5:9443/styles/default/css/modules/ • https://100.100.0.5:9443/styles/default/plugins/datatables/images/ • https://100.100.0.5:9443/styles/default/js/chat/ • https://100.100.0.5:9443/styles/default/js/docs/ • https://100.100.0.5:9443/styles/default/js/info/ • https://100.100.0.5:9443/styles/default/js/old/

```
GET /styles/default/js/old/ HTTP/1.1
Referer: https://100.100.0.5:9443/styles/default/js/
Cookie: language=russian
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/131.0.0.0 Safari/537.36
Host: 100.100.0.5:9443
Connection: Keep-alive
```

Web Server	
Alert group	**Scheme URI Detected in Content Security Policy (CSP) Directive (verified)**
Severity	Informational
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.
Recommendations	See alert details for available remediation advice.
Alert variants	
Details	• **Scheme URI Detected in Content Security Policy (CSP) Directive** ◦ **First observed on:** https://100.100.0.5:9443/ ◦ **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' https:; style-src 'self' 'unsafe-inline'; img-src 'self' data:; ◦ **CSP Source:** header ◦ **Summary:** Acunetix detected that scheme URI was used in CSP directive. ◦ **Impact:** This means that scheme URI in script-src (http: or https:) allows the execution of unsafe scripts. ◦ **Remediation:** Replace the scheme URI with the domain that you trust. ◦ **References:** ▪ N/A

```
GET / HTTP/1.1
Host: 100.100.0.5:9443
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
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/131.0.0.0 Safari/537.36
```

Web Server	
Alert group	**data: Used in a Content Security Policy (CSP) Directive (verified)**
Severity	Informational
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.
Recommendations	See alert details for available remediation advice.
Alert variants	
Details	• **data: Used in a Content Security Policy (CSP) Directive** ◦ **First observed on:** https://100.100.0.5:9443/ ◦ **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' https:; style-src 'self' 'unsafe-inline'; img-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

```
GET / HTTP/1.1
Host: 100.100.0.5:9443
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
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/131.0.0.0 Safari/537.36
```

Web Server	
Alert group	**default-src Used in Content Security Policy (CSP) (verified)**
Severity	Informational

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.
Recommendations	See alert details for available remediation advice.
Alert variants	
Details	• **default-src Used in Content Security Policy (CSP)** ◦ **First observed on:** https://100.100.0.5:9443/ ◦ **CSP Value:** default-src 'self'; script-src 'self' 'unsafe-inline' https:; style-src 'self' 'unsafe-inline'; img-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

```
GET / HTTP/1.1
Host: 100.100.0.5:9443
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
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/131.0.0.0 Safari/537.36
```

Scanned items (coverage report)

https://100.100.0.5:9443/
https://100.100.0.5:9443/admin/
https://100.100.0.5:9443/admin/index.cgi
https://100.100.0.5:9443/api.cgi/
https://100.100.0.5:9443/api.cgi/builds
https://100.100.0.5:9443/api.cgi/streets
https://100.100.0.5:9443/api/
https://100.100.0.5:9443/captcha/
https://100.100.0.5:9443/error/
https://100.100.0.5:9443/img/
https://100.100.0.5:9443/img/logo/
https://100.100.0.5:9443/index.cgi
https://100.100.0.5:9443/registration.cgi
https://100.100.0.5:9443/robots.txt
https://100.100.0.5:9443/styles/
https://100.100.0.5:9443/styles/default/
https://100.100.0.5:9443/styles/default/css/
https://100.100.0.5:9443/styles/default/css/QBInfo.css
https://100.100.0.5:9443/styles/default/css/adminlte.min.css
https://100.100.0.5:9443/styles/default/css/bs-stepper.min.css
https://100.100.0.5:9443/styles/default/css/client.css
https://100.100.0.5:9443/styles/default/css/font-awesome.min.css
https://100.100.0.5:9443/styles/default/css/images/
https://100.100.0.5:9443/styles/default/css/modules/
https://100.100.0.5:9443/styles/default/css/select2.css
https://100.100.0.5:9443/styles/default/css/skins/
https://100.100.0.5:9443/styles/default/css/skins/_all-skins.css
https://100.100.0.5:9443/styles/default/css/social_button.css
https://100.100.0.5:9443/styles/default/css/style.css
https://100.100.0.5:9443/styles/default/fonts/
https://100.100.0.5:9443/styles/default/img/
https://100.100.0.5:9443/styles/default/img/admin/
https://100.100.0.5:9443/styles/default/img/social/
https://100.100.0.5:9443/styles/default/js/
https://100.100.0.5:9443/styles/default/js/QBinfo.js
https://100.100.0.5:9443/styles/default/js/acp/
https://100.100.0.5:9443/styles/default/js/acp/control-web-client.js
https://100.100.0.5:9443/styles/default/js/adminlte.min.js
https://100.100.0.5:9443/styles/default/js/autosize.min.js
https://100.100.0.5:9443/styles/default/js/bootstrap.bundle.min.js
https://100.100.0.5:9443/styles/default/js/bs-stepper.min.js
https://100.100.0.5:9443/styles/default/js/chat/
https://100.100.0.5:9443/styles/default/js/docs/
https://100.100.0.5:9443/styles/default/js/dynamicForms.js
https://100.100.0.5:9443/styles/default/js/events.js
https://100.100.0.5:9443/styles/default/js/functions-admin.js
https://100.100.0.5:9443/styles/default/js/functions-client.js
https://100.100.0.5:9443/styles/default/js/functions.js
https://100.100.0.5:9443/styles/default/js/info/
https://100.100.0.5:9443/styles/default/js/jquery-ui.min.js
https://100.100.0.5:9443/styles/default/js/jquery.min.js
https://100.100.0.5:9443/styles/default/js/js.cookies.js
https://100.100.0.5:9443/styles/default/js/keys.js
https://100.100.0.5:9443/styles/default/js/messageChecker.js
https://100.100.0.5:9443/styles/default/js/modals.js
https://100.100.0.5:9443/styles/default/js/modules/
https://100.100.0.5:9443/styles/default/js/mustache.min.js
https://100.100.0.5:9443/styles/default/js/navBarCollapse.js
https://100.100.0.5:9443/styles/default/js/old/
https://100.100.0.5:9443/styles/default/js/permanent_data.js
https://100.100.0.5:9443/styles/default/js/polyfill.js
https://100.100.0.5:9443/styles/default/js/search.js

https://100.100.0.5:9443/styles/default/js/select2.min.js
https://100.100.0.5:9443/styles/default/js/tinyco.min.js
https://100.100.0.5:9443/styles/default/js/websocket_client.js
https://100.100.0.5:9443/styles/default/plugins/
https://100.100.0.5:9443/styles/default/plugins/datatables/
https://100.100.0.5:9443/styles/default/plugins/datatables/dataTables.bootstrap.css
https://100.100.0.5:9443/styles/default/plugins/datatables/dataTables.bootstrap.min.js
https://100.100.0.5:9443/styles/default/plugins/datatables/images/
https://100.100.0.5:9443/styles/default/plugins/datatables/jquery.dataTables.min.js
https://100.100.0.5:9443/styles/default/plugins/datepicker/
https://100.100.0.5:9443/styles/default/plugins/datepicker/bootstrap-datepicker.js
https://100.100.0.5:9443/styles/default/plugins/datepicker/datepicker3.css
https://100.100.0.5:9443/styles/default/plugins/datepicker/locales/
https://100.100.0.5:9443/styles/default/plugins/datepicker/locales/bootstrap-datepicker.en.js
https://100.100.0.5:9443/styles/default/plugins/datepicker/locales/bootstrap-datepicker.ru.js
https://100.100.0.5:9443/styles/default/plugins/daterangepicker/
https://100.100.0.5:9443/styles/default/plugins/daterangepicker/daterangepicker.css
https://100.100.0.5:9443/styles/default/plugins/daterangepicker/daterangepicker.js
https://100.100.0.5:9443/styles/default/plugins/datetimepicker/
https://100.100.0.5:9443/styles/default/plugins/datetimepicker/datetimepicker.min.css
https://100.100.0.5:9443/styles/default/plugins/datetimepicker/datetimepicker.min.js
https://100.100.0.5:9443/styles/default/plugins/moment/
https://100.100.0.5:9443/styles/default/plugins/moment/moment.min.js
https://100.100.0.5:9443/styles/default/plugins/pace/
https://100.100.0.5:9443/styles/default/plugins/pace/pace.js
https://100.100.0.5:9443/styles/default/plugins/pace/pace.min.css
https://100.100.0.5:9443/styles/default/plugins/timepicker/
https://100.100.0.5:9443/styles/default/plugins/timepicker/bootstrap-timepicker.min.css
https://100.100.0.5:9443/styles/default/plugins/timepicker/bootstrap-timepicker.min.js
https://100.100.0.5:9443/styles/default/webfonts/