# Scan Report

Generated on 2024-06-24 13:46:42

## Target Information

Target IP: 192.168.0.119

## Nmap Scan Results

Nmap scan report for 192.168.0.119

| Port | Service |
| --- | --- |
| 80/tcp | http nginx |
| 111/tcp | rpcbind 2-4 (RPC #100000) |
| 139/tcp | netbios-ssn Samba smbd 4.6.2 |
| 443/tcp | ssl/http nginx |
| 445/tcp | netbios-ssn Samba smbd 4.6.2 |
| 1080/tcp | http OpenResty web app server |
| 1081/tcp | http OpenResty web app server |
| 1443/tcp | ssl/ies-lm? |
| 2049/tcp | nfs 3-4 (RPC #100003) |
| 3000/tcp | ppp? |
| 3702/tcp | tcpwrapped |
| 5055/tcp | http Node.js Express framework |
| 5355/tcp | tcpwrapped |
| 6556/tcp | check_mk check_mk extension for Nagios 2.2.0p27 |
| 6767/tcp | bmc-perf-agent? |
| 7878/tcp | owms? |
| 8081/tcp | http nginx 1.18.0 |
| 8096/tcp | unknown |
| 8112/tcp | rtsp |
| 8191/tcp | http Pylons Waitress WSGI server |
| 9696/tcp | unknown |
| 33939/tcp | mountd 1-3 (RPC #100005) |
| 37227/tcp | mountd 1-3 (RPC #100005) |
| 44841/tcp | nlockmgr 1-4 (RPC #100021) |

| 46833/tcp | mountd 1-3 (RPC #100005) |
| 49949/tcp | status 1 (RPC #100024) |

# Nuclei Scan Results
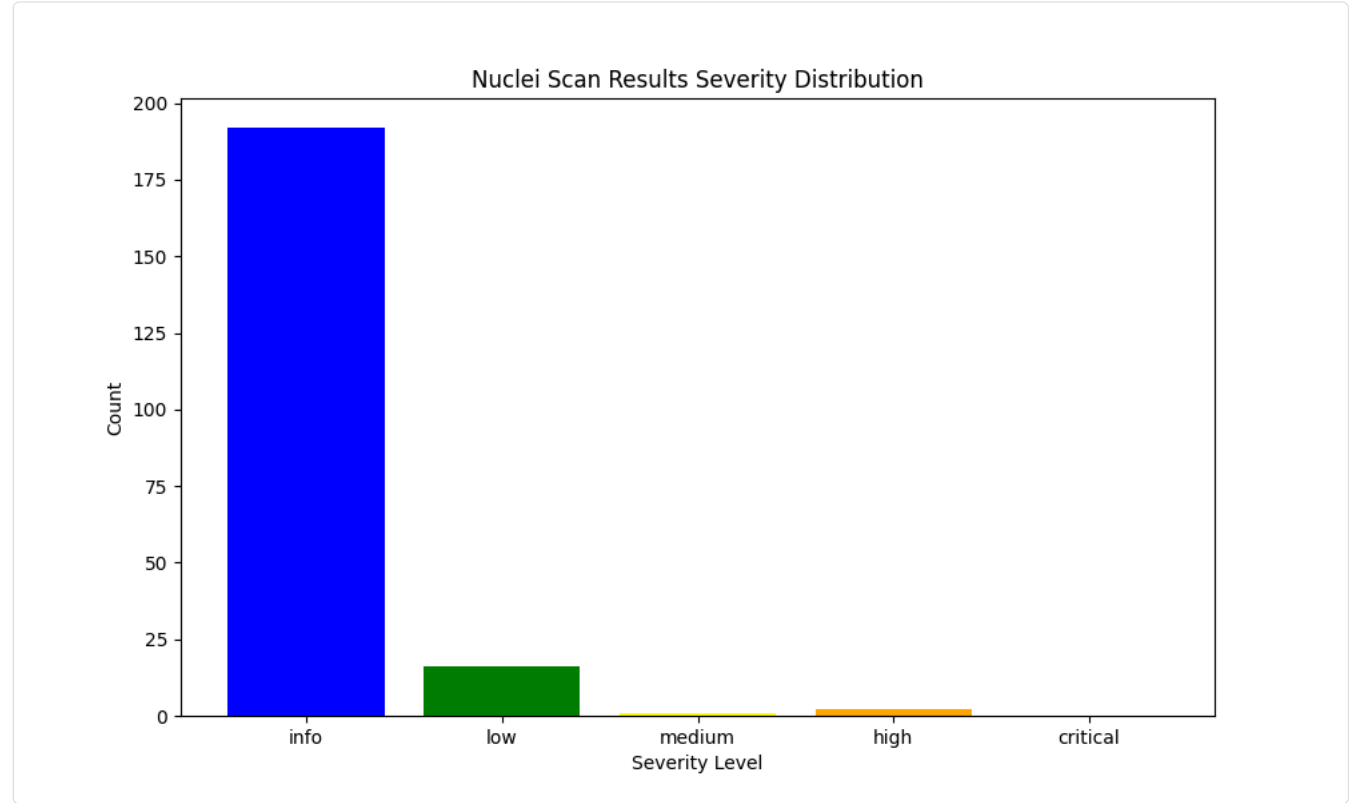


[external-service-interaction] [http] [info] https://cpskvoegdfnc4jlkh7vgge94zgama4o8a.oast.me:443/

[external-service-interaction] [http] [info] https://cpskvoegdfnc4jlkh7vgge94zgama4o8a.oast.me:443/

[external-service-interaction] [http] [info] http://192.168.0.119:80

[waf-detect:nginxgeneric] [http] [info] http://192.168.0.119:80

[smb2-capabilities] [javascript] [info] 192.168.0.119:445 ["["LargeMTU","Leasing"]"]

[smb2-server-time] [javascript] [info] 192.168.0.119:445 ["SystemTime: 2024-06-24T10:59:50.000Z ServerStartTime: 2009-04-22T19:24:48.000Z"]

[smb-anonymous-access] [javascript] [high] 192.168.0.119:445

[rpcbind-portmapper-detect] [tcp] [info] 192.168.0.119:111

[erlang-daemon] [tcp] [low] 192.168.0.119:111

[smb2-server-time] [javascript] [info] 192.168.0.119:139 ["SystemTime: 2024-06-24T11:05:10.000Z ServerStartTime: 2009-04-22T19:24:48.000Z"]

[erlang-daemon] [tcp] [low] 192.168.0.119:139

[tls-version] [ssl] [info] 192.168.0.119:443 ["tls12"]

[tls-version] [ssl] [info] 192.168.0.119:443 ["tls13"]

[smb2-server-time] [javascript] [info] 192.168.0.119:445 ["SystemTime: 2024-06-24T11:13:32.000Z ServerStartTime: 2009-04-22T19:24:48.000Z"]

[erlang-daemon] [tcp] [low] 192.168.0.119:445

[openresty-detect] [http] [info] http://192.168.0.119:1080

[tech-detect:bootstrap] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:1080

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:1080
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:1080
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:1080
[minecraft-enum] [javascript] [info] 192.168.0.119:1080 ["Version: Request\r\nServ Description:er: openresty\r\nDate: Mon, 24 Jun 2024 11:23:35 GMT\r\nContent-Type: text/html\r\nContent-Length: 154\r\nConnection: close\r\n\r\n\r\n\r\n\r\n\r\n

# 400 Bad Request

\r\n

---

openresty

\r\n \r\n"]
[redis-require-auth] [javascript] [info] 192.168.0.119:1080
[openresty-detect] [http] [info] http://192.168.0.119:1081
[nginx-proxy-manager] [http] [info] http://192.168.0.119:1081/login ["2.11.2"]
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:1081
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:1081
[minecraft-enum] [javascript] [info] 192.168.0.119:1081 ["Version: Request\r\nServ Description:er: openresty\r\nDate: Mon, 24 Jun 2024 11:31:16 GMT\r\nContent-Type: text/html\r\nContent-Length: 154\r\nConnection: close\r\n\r\n\r\n\r\n\r\n\r\n

# 400 Bad Request

\r\n

---

openresty

\r\n \r\n"]
[redis-require-auth] [javascript] [info] 192.168.0.119:1081
[openresty-detect] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:1443
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:1443
[redis-require-auth] [javascript] [info] 192.168.0.119:1443
[erlang-daemon] [tcp] [low] 192.168.0.119:2049
[xss-deprecated-header] [http] [info] http://192.168.0.119:3000 ["1; mode=block"]
[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:3000
[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:3000
[cors-misconfig:arbitrary-origin] [http] [info] http://192.168.0.119:3000 [cors_origin="https://uttd5.com"]

[minecraft-enum] [javascript] [info] 192.168.0.119:3000 ["Version: Request\r\nConn Description:ection: close Online Players:\n Maximum Players:"]

[redis-require-auth] [javascript] [info] 192.168.0.119:3000

[erlang-daemon] [tcp] [low] 192.168.0.119:3702

[options-method] [http] [info] http://192.168.0.119:5055 ["GET,HEAD"]

[credentials-disclosure] [http] [unknown] http://192.168.0.119:5055/login
["apikey":"API","ApiKey":"API","ApiKey":"You","accessToken":"Access","accessToken":"Application","AccessToken":"Access","AccessToken":"You"

[tech-detect:next.js] [http] [info] http://192.168.0.119:5055/login

[tech-detect:express] [http] [info] http://192.168.0.119:5055

[jellyseerr-login-panel] [http] [info] http://192.168.0.119:5055/login

[form-detection] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:5055/login

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:5055

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:5055

[swagger-api] [http] [info] http://192.168.0.119:5055/api-docs/swagger.json [paths="/api-docs/swagger.json"]

[erlang-daemon] [tcp] [low] 192.168.0.119:5355

[pop3-capabilities-enum] [javascript] [info] 192.168.0.119:6556 ["<<>> Version: 2.2.0p27 AgentOS: linux Hostname: Titan AgentDirectory: /etc/check_mk DataDirectory: /var/lib/check_mk_agent SpoolDirectory: /var/lib/check_mk_agent/spool PluginsDirectory: /usr/lib/check_mk_agent/plugins LocalDirectory: /usr/lib/check_mk_agent/local"]

[erlang-daemon] [tcp] [low] 192.168.0.119:6556

[options-method] [http] [info] http://192.168.0.119:6767 ["GET, HEAD, OPTIONS"]

[credentials-disclosure] [http] [unknown] http://192.168.0.119:6767 [""apiKey": "789bb7b4a5313c08812fe05fad2a4bcb""]

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:6767

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:6767

[swagger-api] [http] [info] http://192.168.0.119:6767/api/swagger.json [paths="/api/swagger.json"]

[redis-require-auth] [javascript] [info] 192.168.0.119:6767

[erlang-daemon] [tcp] [low] 192.168.0.119:6767

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:7878

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:7878

[robots-txt-endpoint] [http] [info] http://192.168.0.119:7878/robots.txt

[redis-require-auth] [javascript] [info] 192.168.0.119:7878

[erlang-daemon] [tcp] [low] 192.168.0.119:7878

[nginx-version] [http] [info] http://192.168.0.119:8081 ["nginx/1.18.0"]

[php-detect] [http] [info] http://192.168.0.119:8081 ["7.4.15"]

[cookies-without-httponly] [http] [info] http://192.168.0.119:8081

[cookies-without-secure] [http] [info] http://192.168.0.119:8081

[fingerprinthub-web-fingerprints:laravel] [http] [info] http://192.168.0.119:8081

[fingerprinthub-web-fingerprints:laravel-framework] [http] [info] http://192.168.0.119:8081

[tech-detect:laravel] [http] [info] http://192.168.0.119:8081

[tech-detect:nginx] [http] [info] http://192.168.0.119:8081

[tech-detect:php] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:8081

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:8081

[robots-txt-endpoint] [http] [info] http://192.168.0.119:8081/robots.txt

[htaccess-config] [http] [info] http://192.168.0.119:8081/.htaccess

[laravel-debug-enabled] [http] [medium] http://192.168.0.119:8081/_ignition/health-check

[waf-detect:nginxgeneric] [http] [info] http://192.168.0.119:8081

[smb2-capabilities] [javascript] [info] 192.168.0.119:445 ["["LargeMTU","Leasing"]"]

[smb2-server-time] [javascript] [info] 192.168.0.119:445 ["SystemTime: 2024-06-24T12:29:53.000Z ServerStartTime: 2009-04-22T19:24:48.000Z"]

[smb-anonymous-access] [javascript] [high] 192.168.0.119:445

[fingerprinthub-web-fingerprints:jellyfin] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:8096/web/

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:8096/web/

[jellyfin-detect] [http] [info] http://192.168.0.119:8096/web/index.html

[redis-require-auth] [javascript] [info] 192.168.0.119:8096

[erlang-daemon] [tcp] [low] 192.168.0.119:8096

[deluge-webui-panel] [http] [info] http://192.168.0.119:8112

[tech-detect:twistedweb] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:8112

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:8112

[redis-require-auth] [javascript] [info] 192.168.0.119:8112

[erlang-daemon] [tcp] [low] 192.168.0.119:8112

[options-method] [http] [info] http://192.168.0.119:8191 ["GET"]

[http-missing-security-headers:referrer-policy] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:content-security-policy] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:x-frame-options] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:x-content-type-options] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:clear-site-data] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:strict-transport-security] [http] [info] http://192.168.0.119:8191

[http-missing-security-headers:permissions-policy] [http] [info] http://192.168.0.119:8191

[redis-require-auth] [javascript] [info] 192.168.0.119:8191

[erlang-daemon] [tcp] [low] 192.168.0.119:8191

[external-service-interaction] [http] [info] http://cpsmttugdfncspiuquq0hpypmbj5g8cin.oast.me/login?returnUrl=%2F

[external-service-interaction] [http] [info] http://cpsmttugdfncspiuquq0hpypmbj5g8cin.oast.me/login?returnUrl=%2F

[external-service-interaction] [http] [info] http://192.168.0.119:9696

[erlang-daemon] [tcp] [low] 192.168.0.119:33939

[erlang-daemon] [tcp] [low] 192.168.0.119:44841

[erlang-daemon] [tcp] [low] 192.168.0.119:46833

[erlang-daemon] [tcp] [low] 192.168.0.119:49949

# Wapiti Scan Results

## Wapiti Scan Report

```
********************************************************************************
                Wapiti 3.0.4 — wapiti.sourceforge.io
                Report for http://192.168.0.119:80/
            Date of the scan : Fri, 21 Jun 2024 23:26:00 +0000
                    Scope of the scan : folder
********************************************************************************


Summary of vulnerabilities :
---------------------------

                                            Backup file :   0
                                    Blind SQL Injection :   0
                                      Weak credentials :   0
                                        CRLF Injection :   0
                Content Security Policy Configuration :   4
                              Cross Site Request Forgery :   0
                              Potentially dangerous file :   0
                                      Command execution :   0
                                        Path Traversal :   0
                                      Htaccess Bypass :   0
                                    HTTP Secure Headers :   3
                                    HttpOnly Flag cookie :   0
                                        Open Redirect :   0
                                      Secure Flag cookie :   0
                                          SQL Injection :   0
                              Server Side Request Forgery :   0
                                    Cross Site Scripting :   0
                                    XML External Entity :   0
********************************************************************************


Content Security Policy Configuration
------------------------------------
CSP attribute "default-src" is missing
```

```
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


CSP attribute "script-src" is missing
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


CSP attribute "object-src" is missing
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


CSP attribute "base-uri" is missing
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


********************************************************************************

HTTP Secure Headers
-------------------
X-Frame-Options is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


X-XSS-Protection is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


Strict-Transport-Security is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:80
cURL command PoC : "curl "http://192.168.0.119:80/""


                            *   *   *


********************************************************************************


Summary of anomalies :
---------------------
                                        Internal Server Error :   0
                                        Resource consumption :    0
********************************************************************************
Summary of additionals :
-----------------------
                                        Fingerprint web technology :   0
********************************************************************************


********************************************************************************
                    Wapiti 3.0.4 - wapiti.sourceforge.io
                    Report for http://192.168.0.119:111/
                Date of the scan : Fri, 21 Jun 2024 23:26:04 +0000
```

```
                         Scope of the scan : folder
    ***************************************************************************

    Summary of vulnerabilities :
    ---------------------------
                                               Backup file :   0
                                        Blind SQL Injection :   0
                                           Weak credentials :   0
                                              CRLF Injection :   0
                     Content Security Policy Configuration :   0
                                  Cross Site Request Forgery :   0
                                  Potentially dangerous file :   0
                                          Command execution :   0
                                              Path Traversal :   0
                                            Htaccess Bypass :   0
                                        HTTP Secure Headers :   0
                                        HttpOnly Flag cookie :   0
                                               Open Redirect :   0
                                          Secure Flag cookie :   0
                                               SQL Injection :   0
                                Server Side Request Forgery :   0
                                         Cross Site Scripting :   0
                                          XML External Entity :   0
    ***************************************************************************

    Summary of anomalies :
    ---------------------
                                        Internal Server Error :   0
                                        Resource consumption :   0
    ***************************************************************************
    Summary of additionals :
    ----------------------
                                    Fingerprint web technology :   0
    ***************************************************************************


    ***************************************************************************
                    Wapiti 3.0.4 - wapiti.sourceforge.io
                    Report for http://192.168.0.119:139/
            Date of the scan : Fri, 21 Jun 2024 23:26:48 +0000
                         Scope of the scan : folder
    ***************************************************************************

    Summary of vulnerabilities :
    ---------------------------
                                               Backup file :   0
                                        Blind SQL Injection :   0
                                           Weak credentials :   0
                                              CRLF Injection :   0
                     Content Security Policy Configuration :   0
                                  Cross Site Request Forgery :   0
                                  Potentially dangerous file :   0
                                          Command execution :   0
                                              Path Traversal :   0
                                            Htaccess Bypass :   0
                                        HTTP Secure Headers :   0
                                        HttpOnly Flag cookie :   0
                                               Open Redirect :   0
                                          Secure Flag cookie :   0
                                               SQL Injection :   0
                                Server Side Request Forgery :   0
                                         Cross Site Scripting :   0
                                          XML External Entity :   0
    ***************************************************************************

    Summary of anomalies :
    ---------------------
                                        Internal Server Error :   0
                                        Resource consumption :   0
    ***************************************************************************
    Summary of additionals :
    ----------------------
                                    Fingerprint web technology :   0
    ***************************************************************************


    ***************************************************************************
```

```
                        Wapiti 3.0.4 — wapiti.sourceforge.io
                        Report for http://192.168.0.119:443/
                    Date of the scan : Fri, 21 Jun 2024 23:27:33 +0000
                            Scope of the scan : folder
********************************************************************************

Summary of vulnerabilities :
---------------------------
                                                        Backup file :   0
                                                Blind SQL Injection :   0
                                                  Weak credentials :   0
                                                     CRLF Injection :   0
                            Content Security Policy Configuration :   1
                                        Cross Site Request Forgery :   0
                                        Potentially dangerous file :   0
                                                  Command execution :   0
                                                     Path Traversal :   0
                                                   Htaccess Bypass :   0
                                                HTTP Secure Headers :   4
                                              HttpOnly Flag cookie :   0
                                                      Open Redirect :   0
                                                Secure Flag cookie :   0
                                                      SQL Injection :   0
                                      Server Side Request Forgery :   0
                                              Cross Site Scripting :   0
                                                XML External Entity :   0
********************************************************************************

Content Security Policy Configuration
-------------------------------------
CSP is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:443
cURL command PoC : "curl "http://192.168.0.119:443/""


                              *   *   *


********************************************************************************

HTTP Secure Headers
-------------------
X-Frame-Options is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:443
cURL command PoC : "curl "http://192.168.0.119:443/""


                              *   *   *

X-XSS-Protection is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:443
cURL command PoC : "curl "http://192.168.0.119:443/""


                              *   *   *

X-Content-Type-Options is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:443
cURL command PoC : "curl "http://192.168.0.119:443/""


                              *   *   *

Strict-Transport-Security is not set
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.119:443
cURL command PoC : "curl "http://192.168.0.119:443/""


                              *   *   *


********************************************************************************
```

```
Summary of anomalies :
----------------------
                                          Internal Server Error :    0
                                          Resource consumption :     0
****************************************************************************
Summary of additionals :
-----------------------
                                          Fingerprint web technology :   0
****************************************************************************


****************************************************************************
                    Wapiti 3.0.4 – wapiti.sourceforge.io
                    Report for http://192.168.0.119:445/
              Date of the scan : Fri, 21 Jun 2024 23:28:17 +0000
                        Scope of the scan : folder
****************************************************************************

Summary of vulnerabilities :
---------------------------
                                                    Backup file :    0
                                            Blind SQL Injection :    0
                                               Weak credentials :    0
                                                  CRLF Injection :    0
                        Content Security Policy Configuration :    0
                                    Cross Site Request Forgery :    0
                                    Potentially dangerous file :    0
                                              Command execution :    0
                                                 Path Traversal :    0
                                                Htaccess Bypass :    0
                                            HTTP Secure Headers :    0
                                            HttpOnly Flag cookie :    0
                                                  Open Redirect :    0
                                              Secure Flag cookie :    0
                                                  SQL Injection :    0
                                    Server Side Request Forgery :    0
                                            Cross Site Scripting :    0
                                              XML External Entity :    0
****************************************************************************

Summary of anomalies :
----------------------
                                          Internal Server Error :    0
                                          Resource consumption :     0
****************************************************************************
Summary of additionals :
-----------------------
                                          Fingerprint web technology :   0
****************************************************************************

File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:1080_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:1081_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:1443_wapiti.txt for Wapiti on port None
****************************************************************************
                    Wapiti 3.0.4 – wapiti.sourceforge.io
                    Report for http://192.168.0.119:2049/
              Date of the scan : Fri, 21 Jun 2024 23:29:02 +0000
                        Scope of the scan : folder
****************************************************************************

Summary of vulnerabilities :
---------------------------
                                                    Backup file :    0
                                            Blind SQL Injection :    0
                                               Weak credentials :    0
                                                  CRLF Injection :    0
                        Content Security Policy Configuration :    0
                                    Cross Site Request Forgery :    0
                                    Potentially dangerous file :    0
                                              Command execution :    0
                                                 Path Traversal :    0
                                                Htaccess Bypass :    0
                                            HTTP Secure Headers :    0
                                            HttpOnly Flag cookie :    0
                                                  Open Redirect :    0
```

```
                                              Secure Flag cookie :   0
                                                 SQL Injection :   0
                                  Server Side Request Forgery :   0
                                          Cross Site Scripting :   0
                                           XML External Entity :   0
********************************************************************************
```

Summary of anomalies :
----------------------
```
                                           Internal Server Error :   0
                                           Resource consumption :   0
********************************************************************************
```
Summary of additionals :
------------------------
```
                                           Fingerprint web technology :   0
********************************************************************************
```

File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:3000_wapiti.txt for Wapiti on port None
```
********************************************************************************
                      Wapiti 3.0.4 - wapiti.sourceforge.io
                      Report for http://192.168.0.119:3702/
                 Date of the scan : Fri, 21 Jun 2024 23:29:07 +0000
                         Scope of the scan : folder
********************************************************************************
```

Summary of vulnerabilities :
---------------------------
```
                                                        Backup file :   0
                                                Blind SQL Injection :   0
                                                   Weak credentials :   0
                                                      CRLF Injection :   0
                                Content Security Policy Configuration :   0
                                          Cross Site Request Forgery :   0
                                          Potentially dangerous file :   0
                                                  Command execution :   0
                                                      Path Traversal :   0
                                                    Htaccess Bypass :   0
                                                HTTP Secure Headers :   0
                                                HttpOnly Flag cookie :   0
                                                       Open Redirect :   0
                                                  Secure Flag cookie :   0
                                                       SQL Injection :   0
                                          Server Side Request Forgery :   0
                                                Cross Site Scripting :   0
                                                 XML External Entity :   0
********************************************************************************
```

Summary of anomalies :
----------------------
```
                                           Internal Server Error :   0
                                           Resource consumption :   0
********************************************************************************
```
Summary of additionals :
------------------------
```
                                           Fingerprint web technology :   0
********************************************************************************
```

File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:5055_wapiti.txt for Wapiti on port None
```
********************************************************************************
                      Wapiti 3.0.4 - wapiti.sourceforge.io
                      Report for http://192.168.0.119:5355/
                 Date of the scan : Fri, 21 Jun 2024 23:29:12 +0000
                         Scope of the scan : folder
********************************************************************************
```

Summary of vulnerabilities :
---------------------------
```
                                                        Backup file :   0
                                                Blind SQL Injection :   0
                                                   Weak credentials :   0
                                                      CRLF Injection :   0
                                Content Security Policy Configuration :   0
                                          Cross Site Request Forgery :   0
                                          Potentially dangerous file :   0
                                                  Command execution :   0
```

```
                                    Path Traversal :    0
                                   Htaccess Bypass :    0
                               HTTP Secure Headers :    0
                               HttpOnly Flag cookie :   0
                                     Open Redirect :    0
                               Secure Flag cookie :    0
                                     SQL Injection :    0
                         Server Side Request Forgery :  0
                               Cross Site Scripting :    0
                                XML External Entity :    0
***********************************************************************
```

Summary of anomalies :
----------------------

```
                               Internal Server Error :   0
                               Resource consumption :    0
***********************************************************************
```

Summary of additionals :
-----------------------

```
                             Fingerprint web technology :   0
***********************************************************************


***********************************************************************
                   Wapiti 3.0.4 – wapiti.sourceforge.io
                   Report for http://192.168.0.119:6556/
              Date of the scan : Fri, 21 Jun 2024 23:29:16 +0000
                        Scope of the scan : folder
***********************************************************************
```

Summary of vulnerabilities :
---------------------------

```
                                        Backup file :    0
                                 Blind SQL Injection :    0
                                   Weak credentials :    0
                                      CRLF Injection :    0
                  Content Security Policy Configuration :   0
                          Cross Site Request Forgery :    0
                          Potentially dangerous file :    0
                                 Command execution :    0
                                    Path Traversal :    0
                                   Htaccess Bypass :    0
                               HTTP Secure Headers :    0
                               HttpOnly Flag cookie :    0
                                     Open Redirect :    0
                               Secure Flag cookie :    0
                                     SQL Injection :    0
                         Server Side Request Forgery :    0
                               Cross Site Scripting :    0
                                XML External Entity :    0
***********************************************************************
```

Summary of anomalies :
----------------------

```
                               Internal Server Error :   0
                               Resource consumption :    0
***********************************************************************
```

Summary of additionals :
-----------------------

```
                             Fingerprint web technology :   0
***********************************************************************
```

```
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:6767_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:7878_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:8081_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:8096_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:8112_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:8191_wapiti.txt for Wapiti on port None
File not found: results/192.168.0.119_24-06-2024/wapiti/192.168.0.119:9696_wapiti.txt for Wapiti on port None
***********************************************************************
                   Wapiti 3.0.4 – wapiti.sourceforge.io
                   Report for http://192.168.0.119:33939/
              Date of the scan : Fri, 21 Jun 2024 23:29:21 +0000
                        Scope of the scan : folder
***********************************************************************
```

```
Summary of vulnerabilities :
----------------------------
                                                   Backup file :   0
                                           Blind SQL Injection :   0
                                              Weak credentials :   0
                                                 CRLF Injection :   0
                         Content Security Policy Configuration :   0
                                    Cross Site Request Forgery :   0
                                    Potentially dangerous file :   0
                                             Command execution :   0
                                                Path Traversal :   0
                                               Htaccess Bypass :   0
                                           HTTP Secure Headers :   0
                                            HttpOnly Flag cookie :   0
                                                 Open Redirect :   0
                                             Secure Flag cookie :   0
                                                 SQL Injection :   0
                                    Server Side Request Forgery :   0
                                           Cross Site Scripting :   0
                                            XML External Entity :   0
*********************************************************************************

Summary of anomalies :
----------------------
                                            Internal Server Error :   0
                                             Resource consumption :   0
*********************************************************************************
Summary of additionals :
------------------------
                                          Fingerprint web technology :   0
*********************************************************************************


*********************************************************************************
                    Wapiti 3.0.4 – wapiti.sourceforge.io
                   Report for http://192.168.0.119:37227/
               Date of the scan : Fri, 21 Jun 2024 23:29:26 +0000
                         Scope of the scan : folder
*********************************************************************************

Summary of vulnerabilities :
----------------------------
                                                   Backup file :   0
                                           Blind SQL Injection :   0
                                              Weak credentials :   0
                                                 CRLF Injection :   0
                         Content Security Policy Configuration :   0
                                    Cross Site Request Forgery :   0
                                    Potentially dangerous file :   0
                                             Command execution :   0
                                                Path Traversal :   0
                                               Htaccess Bypass :   0
                                           HTTP Secure Headers :   0
                                            HttpOnly Flag cookie :   0
                                                 Open Redirect :   0
                                             Secure Flag cookie :   0
                                                 SQL Injection :   0
                                    Server Side Request Forgery :   0
                                           Cross Site Scripting :   0
                                            XML External Entity :   0
*********************************************************************************

Summary of anomalies :
----------------------
                                            Internal Server Error :   0
                                             Resource consumption :   0
*********************************************************************************
Summary of additionals :
------------------------
                                          Fingerprint web technology :   0
*********************************************************************************


*********************************************************************************
                    Wapiti 3.0.4 – wapiti.sourceforge.io
                   Report for http://192.168.0.119:44841/
               Date of the scan : Fri, 21 Jun 2024 23:29:31 +0000
```

```
                              Scope of the scan : folder
    **********************************************************************


Summary of vulnerabilities :
---------------------------
                                                          Backup file :   0
                                                  Blind SQL Injection :   0
                                                     Weak credentials :   0
                                                        CRLF Injection :   0
                          Content Security Policy Configuration :   0
                                        Cross Site Request Forgery :   0
                                        Potentially dangerous file :   0
                                                  Command execution :   0
                                                     Path Traversal :   0
                                                    Htaccess Bypass :   0
                                                HTTP Secure Headers :   0
                                                 HttpOnly Flag cookie :   0
                                                      Open Redirect :   0
                                                  Secure Flag cookie :   0
                                                       SQL Injection :   0
                                        Server Side Request Forgery :   0
                                                 Cross Site Scripting :   0
                                                 XML External Entity :   0
    **********************************************************************


Summary of anomalies :
---------------------
                                                  Internal Server Error :   0
                                                   Resource consumption :   0
    **********************************************************************
Summary of additionals :
-----------------------
                                                Fingerprint web technology :   0
    **********************************************************************


    **********************************************************************
                    Wapiti 3.0.4 – wapiti.sourceforge.io
                     Report for http://192.168.0.119:46833/
                Date of the scan : Fri, 21 Jun 2024 23:29:35 +0000
                              Scope of the scan : folder
    **********************************************************************


Summary of vulnerabilities :
---------------------------
                                                          Backup file :   0
                                                  Blind SQL Injection :   0
                                                     Weak credentials :   0
                                                        CRLF Injection :   0
                          Content Security Policy Configuration :   0
                                        Cross Site Request Forgery :   0
                                        Potentially dangerous file :   0
                                                  Command execution :   0
                                                     Path Traversal :   0
                                                    Htaccess Bypass :   0
                                                HTTP Secure Headers :   0
                                                 HttpOnly Flag cookie :   0
                                                      Open Redirect :   0
                                                  Secure Flag cookie :   0
                                                       SQL Injection :   0
                                        Server Side Request Forgery :   0
                                                 Cross Site Scripting :   0
                                                 XML External Entity :   0
    **********************************************************************


Summary of anomalies :
---------------------
                                                  Internal Server Error :   0
                                                   Resource consumption :   0
    **********************************************************************
Summary of additionals :
-----------------------
                                                Fingerprint web technology :   0
    **********************************************************************


    **********************************************************************
```

```
              Wapiti 3.0.4 - wapiti.sourceforge.io
              Report for http://192.168.0.119:49949/
            Date of the scan : Fri, 21 Jun 2024 23:29:40 +0000
                  Scope of the scan : folder
**********************************************************************

Summary of vulnerabilities :
---------------------------
                                          Backup file :   0
                                  Blind SQL Injection :   0
                                     Weak credentials :   0
                                        CRLF Injection :   0
                  Content Security Policy Configuration :   0
                              Cross Site Request Forgery :   0
                            Potentially dangerous file :   0
                                    Command execution :   0
                                      Path Traversal :   0
                                     Htaccess Bypass :   0
                                  HTTP Secure Headers :   0
                                  HttpOnly Flag cookie :   0
                                        Open Redirect :   0
                                    Secure Flag cookie :   0
                                        SQL Injection :   0
                            Server Side Request Forgery :   0
                                  Cross Site Scripting :   0
                                    XML External Entity :   0
**********************************************************************

Summary of anomalies :
---------------------
                                  Internal Server Error :   0
                                  Resource consumption :   0
**********************************************************************
Summary of additionals :
-----------------------
                                Fingerprint web technology :   0
**********************************************************************
```

# WhatWeb Scan Results

## WhatWeb Scan Report

```
WhatWeb report for http://192.168.0.119:80
Status    : 302 Found
Title     : 302 Found
IP        : 192.168.0.119
Country   : RESERVED, ZZ

Summary     : HTTPServer[nginx], nginx, RedirectLocation[https://192.168.0.119:443/], UncommonHeaders[x-content-type-
options,referrer-policy,content-security-policy]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String       : nginx (from server string)


[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String       : https://192.168.0.119:443/ (from location)


[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
```

```
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String      : x-content-type-options,referrer-policy,content-security-policy (from headers)


[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 302 Moved Temporarily
        Server: nginx
        Date: Fri, 21 Jun 2024 23:22:37 GMT
        Content-Type: text/html
        Content-Length: 138
        Connection: close
        Location: https://192.168.0.119:443/
        X-Content-Type-Options: nosniff
        Referrer-Policy: same-origin
        Content-Security-Policy: frame-ancestors 'self' https://connect.myunraid.net/

WhatWeb report for https://192.168.0.119/Dashboard
Status    : 302 Found
Title     : 302 Found
IP        : 192.168.0.119
Country   : RESERVED, ZZ

Summary    : HTTPServer[nginx], nginx, RedirectLocation[https://192.168.0.119/login], UncommonHeaders[x-content-type-
options,referrer-policy,content-security-policy]

Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String      : nginx (from server string)

[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String      : https://192.168.0.119/login (from location)

[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String      : x-content-type-options,referrer-policy,content-security-policy (from headers)

[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website     : http://nginx.net/

HTTP Headers:
        HTTP/1.1 302 Moved Temporarily
        Server: nginx
        Date: Fri, 21 Jun 2024 23:22:41 GMT
        Content-Type: text/html
        Content-Length: 138
        Connection: close
        Location: https://192.168.0.119/login
        X-Content-Type-Options: nosniff
        Referrer-Policy: same-origin
        Content-Security-Policy: frame-ancestors 'self' https://connect.myunraid.net/

WhatWeb report for https://192.168.0.119/
```

```
Status    : 302 Found
Title     : 302 Found
IP        : 192.168.0.119
Country   : RESERVED, ZZ


Summary   : HTTPServer[nginx], nginx, RedirectLocation[https://192.168.0.119/Dashboard], UncommonHeaders[x-content-type-
options,referrer-policy,content-security-policy]


Detected Plugins:
[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String        : nginx (from server string)


[ RedirectLocation ]
        HTTP Server string location. used with http-status 301 and
        302

        String        : https://192.168.0.119/Dashboard (from location)


[ UncommonHeaders ]
        Uncommon HTTP server headers. The blacklist includes all
        the standard headers and many non standard but common ones.
        Interesting but fairly common headers should have their own
        plugins, eg. x-powered-by, server and x-aspnet-version.
        Info about headers can be found at www.http-stats.com

        String        : x-content-type-options,referrer-policy,content-security-policy (from headers)


[ nginx ]
        Nginx (Engine-X) is a free, open-source, high-performance
        HTTP server and reverse proxy, as well as an IMAP/POP3
        proxy server.

        Website       : http://nginx.net/

HTTP Headers:
        HTTP/1.1 302 Moved Temporarily
        Server: nginx
        Date: Fri, 21 Jun 2024 23:22:40 GMT
        Content-Type: text/html
        Content-Length: 138
        Connection: close
        Location: https://192.168.0.119/Dashboard
        X-Content-Type-Options: nosniff
        Referrer-Policy: same-origin
        Content-Security-Policy: frame-ancestors 'self' https://connect.myunraid.net/

WhatWeb report for https://192.168.0.119/login
Status    : 200 OK
Title     : Titan/Login
IP        : 192.168.0.119
Country   : RESERVED, ZZ


Summary    : HTML5, HTTPServer[nginx], nginx, PasswordField[password], Script[text/javascript], UncommonHeaders[x-
content-type-options,referrer-policy,content-security-policy], X-UA-Compatible[IE=edge]


Detected Plugins:
[ HTML5 ]
        HTML version 5, detected by the doctype declaration


[ HTTPServer ]
        HTTP server header string. This plugin also attempts to
        identify the operating system from the server header.

        String        : nginx (from server string)

[ PasswordField ]
        find password fields

        String        : password (from field name)

[ Script ]
```

```
            This plugin detects instances of script HTML elements and
            returns the script language/type.

            String       : text/javascript

[ UncommonHeaders ]
            Uncommon HTTP server headers. The blacklist includes all
            the standard headers and many non standard but common ones.
            Interesting but fairly common headers should have their own
            plugins, eg. x-powered-by, server and x-aspnet-version.
            Info about headers can be found at www.http-stats.com

            String       : x-content-type-options,referrer-policy,content-security-policy (from headers)

[ X-UA-Compatible ]
            This plugin retrieves the X-UA-Compatible value from the
            HTTP header and meta http-equiv tag. - More Info:
            http://msdn.microsoft.com/en-us/library/cc817574.aspx

            String       : IE=edge

[ nginx ]
            Nginx (Engine-X) is a free, open-source, high-performance
            HTTP server and reverse proxy, as well as an IMAP/POP3
            proxy server.

            Website      : http://nginx.net/

HTTP Headers:
            HTTP/1.1 200 OK
            Server: nginx
            Date: Fri, 21 Jun 2024 23:22:42 GMT
            Content-Type: text/html; charset=UTF-8
            Transfer-Encoding: chunked
            Connection: close
            X-Content-Type-Options: nosniff
            Referrer-Policy: same-origin
            Content-Security-Policy: frame-ancestors 'self' https://connect.myunraid.net/


WhatWeb report for http://192.168.0.119:443
Status    : 400 Bad Request
Title     : 400 The plain HTTP request was sent to HTTPS port
IP        : 192.168.0.119
Country   : RESERVED, ZZ

Summary   : HTTPServer[nginx], nginx

Detected Plugins:
[ HTTPServer ]
            HTTP server header string. This plugin also attempts to
            identify the operating system from the server header.

            String       : nginx (from server string)

[ nginx ]
            Nginx (Engine-X) is a free, open-source, high-performance
            HTTP server and reverse proxy, as well as an IMAP/POP3
            proxy server.

            Website      : http://nginx.net/

HTTP Headers:
            HTTP/1.1 400 Bad Request
            Server: nginx
            Date: Fri, 21 Jun 2024 23:24:32 GMT
            Content-Type: text/html
            Content-Length: 248
            Connection: close


File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:1080_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:1081_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:1443_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:3000_whatweb.txt for WhatWeb on port None
```

```
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:5055_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:6767_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:7878_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:8081_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:8096_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:8112_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:8191_whatweb.txt for WhatWeb on port None
File not found: results/192.168.0.119_24-06-2024/whatweb/192.168.0.119:9696_whatweb.txt for WhatWeb on port None
```

# Nikto Scan Results

### Nikto Scan Report

```
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:80_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:111_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:139_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:443_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:445_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:1080_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:1081_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:1443_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:2049_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:3000_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:3702_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:5055_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:5355_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:6556_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:6767_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:7878_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:8081_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:8096_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:8112_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:8191_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:9696_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:33939_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:37227_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:44841_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:46833_nikto.txt for Nikto on port None
File not found: results/192.168.0.119_24-06-2024/nikto/192.168.0.119:49949_nikto.txt for Nikto on port None
```

# Dirb Scan Results

### Dirb Scan Report

# XSS Scan Results

### XSS Scan Report

```
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:80_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:111_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:139_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:443_xss.txt for XSS on port None
```

```
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:445_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:1080_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:1081_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:1443_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:2049_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:3000_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:3702_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:5055_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:5355_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:6556_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:6767_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:7878_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:8081_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:8096_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:8112_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:8191_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:9696_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:33939_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:37227_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:44841_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:46833_xss.txt for XSS on port None
File not found: results/192.168.0.119_24-06-2024/xss/192.168.0.119:49949_xss.txt for XSS on port None
```

## SQLi Scan Results

### SQLi Scan Report

```
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:80_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:111_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:139_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:443_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:445_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:1080_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:1081_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:1443_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:2049_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:3000_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:3702_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.168.0.119:5055_sqli.txt for SQLi on port None
File not found: results/192.168.0.119_24-06-2024/sqli/192.
```