Security Report for 192.168.0.119

Report generated on: 2024-06-21 23:34:45

Nmap Scan Results

```
# Nmap 7.94SVN scan initiated Fri Jun
21 23:01:22 2024 as: nmap -sC -sV -p- --open -Pn
-o results/192.168.0.119_21-06-
2024/nmap/192.168.0.119_nmap.txt -T4
192.168.0.119
Nmap scan report for
192.168.0.119
Host is up (0.0000050s
latency).
Not shown: 65505 closed tcp ports
(reset), 16 filtered tcp ports (no-
response)
Some closed ports may be reported as
filtered due to --defeat-rst-ratelimit
PORT
STATE SERVICE     VERSION
80/tcp    open  http
nginx
|_http-title: Did not follow redirect to
https://192.168.0.119:443/
111/tcp   open
rpcbind     2-4 (RPC #100000)
| rpcinfo:
|
program version    port/proto  service
|
100000  2,3,4        111/tcp   rpcbind
|
100000  2,3,4        111/udp   rpcbind
|
100000  3,4          111/tcp6  rpcbind
|
100000  3,4          111/udp6  rpcbind
|
100003  3           2049/udp   nfs
|   100003
3,4         2049/tcp   nfs
|   100005  1,2,3
46833/tcp   mountd
|   100005  1,2,3
50570/udp   mountd
|   100005  1,2,3
54741/tcp6  mountd
|   100005  1,2,3
58836/udp6  mountd
```

```
|   100021  1,3,4
39958/udp   nlockmgr
|   100021  1,3,4
44841/tcp   nlockmgr
|   100021  1,3,4
45995/tcp6  nlockmgr
|   100021  1,3,4
52741/udp6  nlockmgr
|   100024  1
49949/tcp   status
|   100024  1
54599/udp6  status
|   100024  1
55260/udp   status
|_  100024  1
58997/tcp6  status
139/tcp   open  netbios-ssn
Samba smbd 4.6.2
443/tcp   open  ssl/http
nginx
| tls-alpn:
|   h2
|
http/1.1
|   http/1.0
|_  http/0.9
|_ssl-
date: TLS randomness does not represent time
|
http-title: Titan/Login
|_Requested resource
was https://192.168.0.119/login
| ssl-cert:
Subject:
commonName=Titan.local/organizationName=Self-
signed
| Subject Alternative Name:
DNS:Titan.local
| Not valid before:
2023-02-24T19:19:12
|_Not valid after:
2033-02-21T19:19:12
|_http-trane-info: Problem
with XML parsing of /evox/about
| http-
robots.txt: 1 disallowed entry
|_/
445/tcp
open  netbios-ssn Samba smbd 4.6.2
2049/tcp
open  nfs         3-4 (RPC #100003)
3702/tcp
open  tcpwrapped
5355/tcp  open
```

```
tcpwrapped
6556/tcp  open  check_mk    check_mk
extension for Nagios 2.2.0p27
33939/tcp open
mountd      1-3 (RPC #100005)
37227/tcp open
mountd      1-3 (RPC #100005)
44841/tcp open
nlockmgr    1-4 (RPC #100021)
46833/tcp open
mountd      1-3 (RPC #100005)
49949/tcp open
status      1 (RPC #100024)

Host script
results:
| smb2-security-mode:
|   3:1:1:

|_    Message signing enabled but not
required
| smb2-time:
|   date:
2024-06-21T23:01:44
|_  start_date:
N/A

Service detection performed. Please
report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Fri
Jun 21 23:01:50 2024 -- 1 IP address (1 host up)
scanned in 27.38 seconds
```

Nuclei Scan Results

```
[tech-detect:nginx] [http] [info]
http://192.168.0.119:80
[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: 2024-06-21T23:03:24.000Z
ServerStartTime:
2009-04-22T19:24:48.000Z"]
[smb-anonymous-
access] [javascript] [high]
```

```
192.168.0.119:445
File not found for Nuclei on
port nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
File not found for Nuclei on port
nuclei
[smb2-server-time] [javascript] [info]
192.168.0.119:139 ["SystemTime:
2024-06-21T23:07:24.000Z 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:
2024-06-21T23:14:45.000Z ServerStartTime:
2009-04-22T19:24:48.000Z"]
[erlang-daemon]
[tcp] [low] 192.168.0.119:445
[erlang-daemon]
[tcp] [low] 192.168.0.119:2049
[erlang-daemon]
[tcp] [low] 192.168.0.119:44841
```

Wapiti Scan Results

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


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 Configura
tion
-------------------------------------

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

File not found for Wapiti
on port wapiti
File not found for Wapiti on
port wapiti
File not found for Wapiti on port
wapiti
File not found for Wapiti on port
wapiti
File not found for Wapiti on port
wapiti
File not found for Wapiti on port
wapiti
File not found for Wapiti on port
wapiti
File not found for Wapiti on port
wapiti
File not found for Wapiti on port wapiti

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

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 Configura
tion
-------------------------------------

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

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

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

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

**************************
**************************************************
****
                     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 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/



File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
File not found for WhatWeb on port
whatweb
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
```

Nikto Scan Results

```
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
```

```
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
File not found for Nikto on port
nikto
```

Dirb Scan Results

```

-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:80_dirb.txt
START_TIME:
Fri Jun 21 23:29:45 2024
URL_BASE:
http://192.168.0.119:80/
WORDLIST_FILES: wordli
sts/big.txt

-----------------
```

```
GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:80/ ----
(!) WARNING:
NOT_FOUND[] not stable, unable to determine
correct URLs {30X}.
    (Try using FineTunning:
'-f')

-----------------
END_TIME: Fri
Jun 21 23:29:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:111_dirb.txt
START_TIME
: Fri Jun 21 23:29:45 2024
URL_BASE:
http://192.168.0.119:111/
WORDLIST_FILES: wordl
ists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:111/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: RECV
ERROR)

-----------------
END_TIME: Fri
Jun 21 23:29:45 2024
DOWNLOADED: 0 - FOUND:
0
```

```
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb
File not found for Dirb on port
dirb

-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:139_dirb.txt
START_TIME
: Fri Jun 21 23:29:45 2024
URL_BASE:
http://192.168.0.119:139/
WORDLIST_FILES: wordl
ists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:139/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: OPERATION
TIMEOUT)

-----------------
END_TIME: Fri
Jun 21 23:32:15 2024
DOWNLOADED: 0 - FOUND:
```

```
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:443_dirb.txt
START_TIME
: Fri Jun 21 23:32:15 2024
URL_BASE:
http://192.168.0.119:443/
WORDLIST_FILES: wordl
ists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:443/
----

-----------------
END_TIME: Fri Jun
21 23:32:15 2024
DOWNLOADED: 555 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:445_dirb.txt
START_TIME
: Fri Jun 21 23:32:15 2024
URL_BASE:
http://192.168.0.119:445/
WORDLIST_FILES: wordl
ists/big.txt

-----------------
```

```
GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:445/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: OPERATION
TIMEOUT)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:2049_dirb.txt
START_TIM
E: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:2049/
WORDLIST_FILES: word
lists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:2049/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: EMPTY REPLY FROM
SERVER)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
```

```
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:3702_dirb.txt
START_TIM
E: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:3702/
WORDLIST_FILES: word
lists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:3702/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: EMPTY REPLY FROM
SERVER)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:5355_dirb.txt
START_TIM
E: Fri Jun 21 23:34:45 2024
```

```
URL_BASE:
http://192.168.0.119:5355/
WORDLIST_FILES: word
lists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:5355/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: COULDNT
CONNECT)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:6556_dirb.txt
START_TIM
E: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:6556/
WORDLIST_FILES: word
lists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:6556/ ----

(!)
FATAL: Too many errors connecting to host
```

```
(Possible cause: UNSUPPORTED
PROTOCOL)

-----------------
END_TIME:
Fri Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:33939_dirb.txt
START_TI
ME: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:33939/
WORDLIST_FILES: wor
dlists/big.txt

-----------------



GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:33939/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: RECV
ERROR)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------
```

```
OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:37227_dirb.txt
START_TI
ME: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:37227/
WORDLIST_FILES: wor
dlists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:37227/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: RECV
ERROR)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:44841_dirb.txt
START_TI
ME: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:44841/
WORDLIST_FILES: wor
dlists/big.txt

-----------------


GENERATED WORDS: 555
```

```
---- Scanning
URL: http://192.168.0.119:44841/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: EMPTY REPLY FROM
SERVER)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0


-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:46833_dirb.txt
START_TI
ME: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:46833/
WORDLIST_FILES: wor
dlists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:46833/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: RECV
ERROR)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0
```

```
-----------------
DIRB v2.22

By The Dark
Raver
-----------------

OUTPUT_FILE: res
ults/192.168.0.119_21-06-
2024/dirb/192.168.0.119:49949_dirb.txt
START_TI
ME: Fri Jun 21 23:34:45 2024
URL_BASE:
http://192.168.0.119:49949/
WORDLIST_FILES: wor
dlists/big.txt

-----------------


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.119:49949/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: RECV
ERROR)

-----------------
END_TIME: Fri
Jun 21 23:34:45 2024
DOWNLOADED: 0 - FOUND:
0
```

XSS Scan Results

```
File not found for XSS on port
xss
File not found for XSS on port xss
File
not found for XSS on port xss
File not found
for XSS on port xss
File not found for XSS on
port xss
File not found for XSS on port
xss
File not found for XSS on port xss
File
not found for XSS on port xss
File not found
```

```
for XSS on port xss
File not found for XSS on
port xss
File not found for XSS on port
xss
File not found for XSS on port xss
File
not found for XSS on port xss
File not found
for XSS on port xss
File not found for XSS on
port xss
File not found for XSS on port
xss
File not found for XSS on port xss
File
not found for XSS on port xss
File not found
for XSS on port xss
File not found for XSS on
port xss
File not found for XSS on port
xss
File not found for XSS on port xss
File
not found for XSS on port xss
```

SQLi Scan Results

```
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
```

```
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port
sqli
File not found for SQLi on port sqli
```