Security Report for 192.168.0.200

Report generated on: 2024-06-22 00:20:59

Nmap Scan Results

```
# Nmap 7.94SVN scan initiated Fri Jun
21 23:34:48 2024 as: nmap -sC -sV -p- --open -Pn
-o results/192.168.0.200_21-06-
2024/nmap/192.168.0.200_nmap.txt -T4
192.168.0.200
Nmap scan report for
192.168.0.200
Host is up (0.00059s
latency).
Not shown: 65524 closed tcp ports
(reset), 3 filtered tcp ports (no-
response)
Some closed ports may be reported as
filtered due to --defeat-rst-ratelimit
PORT
STATE SERVICE       VERSION
554/tcp   open
tcpwrapped
555/tcp   open  dsf?
556/tcp
open  remotefs?
557/tcp   open  http
lighttpd
|_http-title: SAMSUNG TECHWIN NVR Web
Viewer
558/tcp   open  rtsp
|_rtsp-methods:
ERROR: Script execution failed (use -d to
debug)
| fingerprint-strings:
|
FourOhFourRequest, GetRequest, HTTPOptions,
RTSPRequest:
|     RTSP/1.0 404 Not Found
|
CSeq: 0
|_    Date: Sat Jun 22 00:33:30 2024
GMT
4000/tcp  open  http
lighttpd
|_http-title: SAMSUNG TECHWIN NVR Web
Viewer
9192/tcp  open  unknown
25000/tcp
open  icl-twobase1?
```

1 service unrecognized
despite returning data. If you know the
service/version, please submit the following
fingerprint at https://nmap.org/cgi-
bin/submit.cgi?new-service :
SF-Port558-
TCP:V=7.94SVN%I=7%D=6/21%Time=66760E27%P=x86_64-
pc-linux-gnu%r(
SF:GetRequest,47,"RTSP/1\.0\x20
404\x20Not\x20Found\r\nCSeq:\x200\r\nDate:\
SF:
x20Sat\x20Jun\x2022\x2000:33:30\x202024\x20GMT\r\n
\r\n")%r(HTTPOptions,
SF:47,"RTSP/1\.0\x20404\x
20Not\x20Found\r\nCSeq:\x200\r\nDate:\x20Sat\x20J<
br>SF:un\x2022\x2000:33:30\x202024\x20GMT\r\n\r\n"
)%r(RTSPRequest,47,"RTSP/1\
SF:.0\x20404\x20Not
\x20Found\r\nCSeq:\x200\r\nDate:\x20Sat\x20Jun\x20
22\x2
SF:000:33:30\x202024\x20GMT\r\n\r\n")%r(F
ourOhFourRequest,47,"RTSP/1\.0\x2
SF:0404\x20No
t\x20Found\r\nCSeq:\x200\r\nDate:\x20Sat\x20Jun\x2
022\x2000:3
SF:3:30\x202024\x20GMT\r\n\r\n");**MAC Address: 00:16:6C:98:E9:AE (Samsung Electronics)**

Service detection performed.
Please report any incorrect results at
https://nmap.org/submit/ .
 # Nmap done at Fri
Jun 21 23:38:03 2024 -- 1 IP address (1 host up)
scanned in 195.17 seconds

Nuclei Scan Results

[erlang-daemon] [tcp] [low]
192.168.0.200:554
[redis-require-auth]
[javascript] [info] 192.168.0.200:555
[erlang-
daemon] [tcp] [low] 192.168.0.200:556
[cookies-
without-httponly] [http] [info]
http://192.168.0.200:557
[cookies-without-
secure] [http] [info]
http://192.168.0.200:557
[http-missing-
security-headers:strict-transport-security] [http]
[info] http://192.168.0.200:557
[http-missing-

security-headers:x-frame-options] [http] [info]
http://192.168.0.200:557
[http-missing-
security-headers:x-content-type-options] [http]
[info] http://192.168.0.200:557
[http-missing-
security-headers:x-permitted-cross-domain-
policies] [http] [info]
http://192.168.0.200:557
[http-missing-
security-headers:clear-site-data] [http] [info]
http://192.168.0.200:557
[http-missing-
security-headers:cross-origin-opener-policy]
[http] [info] http://192.168.0.200:557
[http-
missing-security-headers:content-security-policy]
[http] [info] http://192.168.0.200:557
[http-
missing-security-headers:permissions-policy]
[http] [info] http://192.168.0.200:557
[http-
missing-security-headers:referrer-policy] [http]
[info] http://192.168.0.200:557
[http-missing-
security-headers:cross-origin-embedder-policy]
[http] [info] http://192.168.0.200:557
[http-
missing-security-headers:cross-origin-resource-
policy] [http] [info]
http://192.168.0.200:557
[missing-sri] [http]
[info] http://192.168.0.200:557 ["http://192.168.0
.200:557/resource/js/common/jsbn.js","http://192.1
68.0.200:557/resource/js/common/jsbn2.js","http://
192.168.0.200:557/resource/js/common/prng4.js","ht
tp://192.168.0.200:557/resource/js/common/rng.js",
"http://192.168.0.200:557/resource/js/common/jquer
y-
1.7.2.min.js","http://192.168.0.200:557/resource/j
s/common/rsa.js","http://192.168.0.200:557/resourc
e/js/common/base64.js","http://192.168.0.200:557/r
esource/js/common/jquery.ui.dialog.js","http://192
.168.0.200:557/resource/js/common/jquery.input.js"
,"http://192.168.0.200:557/resource/js/login/login
.js","http://192.168.0.200:557/index.php/commonJS"
,"http://192.168.0.200:557/resource/js/common/jque
ry.ua.custom.js","http://192.168.0.200:557/resourc
e/js/common/util.js","http://192.168.0.200:557/res
ource/js/common/functionsfive.js","http://192.168.
0.200:557/index.php/commonJS/lang_js","http://192.
168.0.200:557/resource/js/common/jquery.sha256.js"
,"http://192.168.0.200:557/resource/js/common/rsa2
.js","http://192.168.0.200:557/resource/js/common/

jquery-ui-
1.8.18.custom.min.js","http://192.168.0.200:557/re
source/js/common/jQueryRotate.2.2.js"]
[cors-
misconfig:arbitrary-origin] [http] [info]
http://192.168.0.200:557 [cors_origin="https://192
.168.0.200.kswvj.com"]
[erlang-daemon] [tcp]
[low] 192.168.0.200:558
[cookies-without-
httponly] [http] [info]
http://192.168.0.200:4000
[cookies-without-
secure] [http] [info]
http://192.168.0.200:4000
[http-missing-
security-headers:referrer-policy] [http] [info]
http://192.168.0.200:4000
[http-missing-
security-headers:clear-site-data] [http] [info]
http://192.168.0.200:4000
[http-missing-
security-headers:cross-origin-opener-policy]
[http] [info] http://192.168.0.200:4000
[http-
missing-security-headers:content-security-policy]
[http] [info] http://192.168.0.200:4000
[http-
missing-security-headers:x-frame-options] [http]
[info] http://192.168.0.200:4000
[http-missing-
security-headers:x-content-type-options] [http]
[info] http://192.168.0.200:4000
[http-missing-
security-headers:x-permitted-cross-domain-
policies] [http] [info]
http://192.168.0.200:4000
[http-missing-
security-headers:cross-origin-embedder-policy]
[http] [info] http://192.168.0.200:4000
[http-
missing-security-headers:cross-origin-resource-
policy] [http] [info]
http://192.168.0.200:4000
[http-missing-
security-headers:strict-transport-security] [http]
[info] http://192.168.0.200:4000
[http-missing-
security-headers:permissions-policy] [http] [info]
http://192.168.0.200:4000
[missing-sri] [http]
[info] http://192.168.0.200:4000 ["http://192.168.
0.200:4000/resource/js/common/rsa2.js","http://192
.168.0.200:4000/resource/js/common/base64.js","htt

p://192.168.0.200:4000/resource/js/login/login.js"
,"http://192.168.0.200:4000/index.php/commonJS","h
ttp://192.168.0.200:4000/resource/js/common/jquery
.sha256.js","http://192.168.0.200:4000/resource/js
/common/rng.js","http://192.168.0.200:4000/resourc
e/js/common/jquery.input.js","http://192.168.0.200
:4000/resource/js/common/jquery-
1.7.2.min.js","http://192.168.0.200:4000/resource/
js/common/jsbn2.js","http://192.168.0.200:4000/res
ource/js/common/prng4.js","http://192.168.0.200:40
00/resource/js/common/jquery-ui-
1.8.18.custom.min.js","http://192.168.0.200:4000/r
esource/js/common/util.js","http://192.168.0.200:4
000/resource/js/common/jsbn.js","http://192.168.0.
200:4000/resource/js/common/rsa.js","http://192.16
8.0.200:4000/resource/js/common/jquery.ua.custom.j
s","http://192.168.0.200:4000/resource/js/common/f
unctionsfive.js","http://192.168.0.200:4000/index.
php/commonJS/lang_js","http://192.168.0.200:4000/r
esource/js/common/jquery.ui.dialog.js","http://192
.168.0.200:4000/resource/js/common/jQueryRotate.2.
2.js"]
[cors-misconfig:arbitrary-origin] [http]
[info] http://192.168.0.200:4000
[cors_origin="https://krakh0.200"]

Wapiti Scan Results

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

Wapiti 3.0.4 - wapiti.sourceforge.io

Report for http://192.168.0.200:554/

Date of the scan : Sat, 22 Jun 2024 00:08:11
+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://192.168.0.200:555/

Date of the scan : Sat, 22 Jun 2024 00:08:23 +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://192.168.0.200:556/

Date of the scan : Sat, 22 Jun 2024 00:08:28
+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://192.168.0.200:557/

Date of the scan : Sat, 22 Jun 2024 00:08:37
+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 :  16

Open Redirect :   0

Secure Flag cookie :  16

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: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*   *   *

****
****

HTTP Secure
Headers

X-Frame-Options
is not set
Evil request:
    GET /
HTTP/1.1
    Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*   *   *

X-XSS-Protection is not
set
Evil request:
    GET / HTTP/1.1

Host: 192.168.0.200:557
cURL command PoC :
"curl "http://192.168.0.200:557/""

*   *   *

X-Content-Type-Options is not
set
Evil request:
    GET / HTTP/1.1

Host: 192.168.0.200:557
cURL command PoC :
"curl "http://192.168.0.200:557/""

*   *   *

Strict-Transport-Security is not
set

```
Evil request:
    GET / HTTP/1.1

Host: 192.168.0.200:557
cURL command PoC :
"curl "http://192.168.0.200:557/""


*   *   *

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

HttpOnly Flag
cookie
--------------------
HttpOnly flag is
not set in the cookie : POE_SWITCH_STATUS
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""


*   *   *

HttpOnly flag is not set in the
cookie : POWEROFF_ALARMOUT_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""


*   *   *

HttpOnly flag is not set in the
cookie : NUM_ALARM_IN
Evil request:
    GET
/ HTTP/1.1
    Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""


*   *   *
```

HttpOnly flag is not set in the cookie : NUM_ALARM_OUT
Evil request:
GET / HTTP/1.1
Host: 192.168.0.200:557
cURL command PoC : "curl "http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the cookie : CAMERA_DEFAULT_PW_SUPPORT
Evil request:
GET / HTTP/1.1
Host: 192.168.0.200:557
cURL command PoC : "curl "http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the cookie : KEEP_ASPECT_RATIO_SUPPORT
Evil request:
GET / HTTP/1.1
Host: 192.168.0.200:557
cURL command PoC : "curl "http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the cookie : TOE_SUPPORT
Evil request:
GET / HTTP/1.1
Host: 192.168.0.200:557
cURL command PoC : "curl "http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the

cookie : MAX_SEARCH_USER_NUMBER
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : VPM_KINDERGARTEN_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : nvr_lang
Evil request:
GET /
HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : NVR_MODEL_CODE
Evil request:

GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : NVR_MODEL_NAME
Evil request:

GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : EPOS_SUPPORT
Evil request:
GET
/ HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : VIDEO_SUMMARY_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : CHANNEL_COUNT
Evil request:
GET
/ HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

HttpOnly flag is not set in the
cookie : LANGUAGE_SUPPORT
Evil request:

GET / HTTP/1.1

```
    Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""


*   *   *

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

Secure Flag
cookie
-----------------
Secure flag is not
set in the cookie : POE_SWITCH_STATUS
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""


*   *   *

Secure flag is not set in the
cookie : POWEROFF_ALARMOUT_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""


*   *   *

Secure flag is not set in the
cookie : NUM_ALARM_IN
Evil request:
    GET
/ HTTP/1.1
    Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""


*   *   *

Secure flag is not set in the
```

cookie : NUM_ALARM_OUT
Evil request:
GET
/ HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : CAMERA_DEFAULT_PW_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : KEEP_ASPECT_RATIO_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : TOE_SUPPORT
Evil request:
GET /
HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : MAX_SEARCH_USER_NUMBER
Evil

request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : VPM_KINDERGARTEN_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : nvr_lang
Evil request:
GET /
HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : NVR_MODEL_CODE
Evil request:

GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""

*** * ***

Secure flag is not set in the
cookie : NVR_MODEL_NAME
Evil request:

GET / HTTP/1.1

**Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""**

*** * ***

**Secure flag is not set in the
cookie : EPOS_SUPPORT
Evil request:
GET
/ HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""**

*** * ***

**Secure flag is not set in the
cookie : VIDEO_SUMMARY_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:557
cURL command PoC : "curl
"http://192.168.0.200:557/""**

*** * ***

**Secure flag is not set in the
cookie : CHANNEL_COUNT
Evil request:
GET
/ HTTP/1.1
Host: 192.168.0.200:557
cURL
command PoC : "curl
"http://192.168.0.200:557/""**

*** * ***

**Secure flag is not set in the
cookie : LANGUAGE_SUPPORT
Evil request:**

**GET / HTTP/1.1
Host:
192.168.0.200:557**

cURL command PoC : "curl
"http://192.168.0.200:557/""

* * *

****
****

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://192.168.0.200:558/

Date of the scan : Sat, 22 Jun 2024 00:10:39
+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://192.168.0.200:4000/

Date of the scan : Sat, 22 Jun 2024 00:10:52 +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 : 16

Open Redirect : 0

Secure Flag cookie : 16

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: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

* * *

****
****

HTTP Secure
Headers

X-Frame-Options
is not set
Evil request:
GET /
HTTP/1.1
Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

* * *

X-XSS-Protection is not
set
Evil request:
GET / HTTP/1.1

Host: 192.168.0.200:4000
cURL command PoC :
"curl "http://192.168.0.200:4000/""

* * *

X-Content-Type-Options is not
set
Evil request:
GET / HTTP/1.1

Host: 192.168.0.200:4000

cURL command PoC :
"curl "http://192.168.0.200:4000/""

*   *   *

Strict-Transport-Security is not
set
Evil request:
    GET / HTTP/1.1

Host: 192.168.0.200:4000
cURL command PoC :
"curl "http://192.168.0.200:4000/""

*   *   *

****
****

HttpOnly Flag
cookie

HttpOnly flag is
not set in the cookie : POE_SWITCH_STATUS
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : POWEROFF_ALARMOUT_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : NUM_ALARM_IN
Evil request:
    GET

/ HTTP/1.1
    Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : NUM_ALARM_OUT
Evil request:
    GET
/ HTTP/1.1
    Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : CAMERA_DEFAULT_PW_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : KEEP_ASPECT_RATIO_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : TOE_SUPPORT
Evil request:
    GET /
HTTP/1.1
    Host: 192.168.0.200:4000

cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

HttpOnly flag is not set in the
cookie : MAX_SEARCH_USER_NUMBER
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

HttpOnly flag is not set in the
cookie : VPM_KINDERGARTEN_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

HttpOnly flag is not set in the
cookie : nvr_lang
Evil request:
GET /
HTTP/1.1
Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

HttpOnly flag is not set in the
cookie : NVR_MODEL_CODE
Evil request:

GET / HTTP/1.1
Host:
192.168.0.200:4000
cURL command PoC : "curl

"http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the cookie : NVR_MODEL_NAME
Evil request:

GET / HTTP/1.1
    Host: 192.168.0.200:4000
cURL command PoC : "curl "http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the cookie : EPOS_SUPPORT
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.200:4000
cURL command PoC : "curl "http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the cookie : VIDEO_SUMMARY_SUPPORT
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.200:4000
cURL command PoC : "curl "http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the cookie : CHANNEL_COUNT
Evil request:
    GET / HTTP/1.1
    Host: 192.168.0.200:4000
cURL command PoC : "curl "http://192.168.0.200:4000/""

*   *   *

HttpOnly flag is not set in the
cookie : LANGUAGE_SUPPORT
Evil request:

GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

****
****

Secure Flag
cookie

Secure flag is not
set in the cookie : POE_SWITCH_STATUS
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : POWEROFF_ALARMOUT_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : NUM_ALARM_IN
Evil request:
    GET
/ HTTP/1.1
    Host: 192.168.0.200:4000

cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

Secure flag is not set in the
cookie : NUM_ALARM_OUT
Evil request:
GET
/ HTTP/1.1
Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

Secure flag is not set in the
cookie : CAMERA_DEFAULT_PW_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

Secure flag is not set in the
cookie : KEEP_ASPECT_RATIO_SUPPORT
Evil
request:
GET / HTTP/1.1
Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*** * ***

Secure flag is not set in the
cookie : TOE_SUPPORT
Evil request:
GET /
HTTP/1.1
Host: 192.168.0.200:4000
cURL
command PoC : "curl

"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : MAX_SEARCH_USER_NUMBER
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : VPM_KINDERGARTEN_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : nvr_lang
Evil request:
    GET /
HTTP/1.1
    Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : NVR_MODEL_CODE
Evil request:

GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : NVR_MODEL_NAME
Evil request:

GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : EPOS_SUPPORT
Evil request:
    GET
/ HTTP/1.1
    Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : VIDEO_SUMMARY_SUPPORT
Evil
request:
    GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

Secure flag is not set in the
cookie : CHANNEL_COUNT
Evil request:
    GET
/ HTTP/1.1
    Host: 192.168.0.200:4000
cURL
command PoC : "curl
"http://192.168.0.200:4000/""

*   *   *

```
Secure flag is not set in the
cookie : LANGUAGE_SUPPORT
Evil request:

GET / HTTP/1.1
    Host:
192.168.0.200:4000
cURL command PoC : "curl
"http://192.168.0.200:4000/""


*   *   *

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

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://192.168.0.200:9192/

Date of the scan : Sat, 22 Jun 2024 00:13:36
+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://192.168.0.200:25000/

Date of the scan : Sat, 22 Jun 2024 00:15:01
+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://192.168.0.200:557
Status    : 200
OK
Title     : SAMSUNG TECHWIN NVR Web
Viewer
IP        : 192.168.0.200
Country   :
RESERVED, ZZ

Summary   : Cookies[CAMERA_DEF
AULT_PW_SUPPORT,CHANNEL_COUNT,DATA2,EPOS_SUPPORT,K
EEP_ASPECT_RATIO_SUPPORT,LANGUAGE_SUPPORT,MAX_SEAR
CH_USER_NUMBER,NUM_ALARM_IN,NUM_ALARM_OUT,NVR_MODE
L_CODE,NVR_MODEL_NAME,POE_SWITCH_STATUS,POWEROFF_A
LARMOUT_SUPPORT,TOE_SUPPORT,VIDEO_SUMMARY_SUPPORT,
VPM_KINDERGARTEN_SUPPORT,cs_id,is_login_ok,nvr_lan
g,setup1,ss_id], Frame, JQuery[1.7.2], PasswordFie
ld[chn_user_new_confirm_pwd,chn_user_new_pwd,chn_u
ser_pwd], Script[javascript,text/javascript],
X-UA-Compatible[IE=edge,requiresActiveX=true]
<
br>Detected Plugins:
```

[Cookies]

Display the names of cookies in the HTTP headers.
The
      values are not returned to save on
space.

      String   :
NVR_MODEL_CODE
       String   :
POE_SWITCH_STATUS
    String   :
NVR_MODEL_NAME
       String   :
EPOS_SUPPORT
 String   :
VIDEO_SUMMARY_SUPPORT
        String   :
CHANNEL_COUNT
        String   :
LANGUAGE_SUPPORT
     String   :
POWEROFF_ALARMOUT_SUPPORT
    String   :
NUM_ALARM_IN
 String   : NUM_ALARM_OUT

String   : CAMERA_DEFAULT_PW_SUPPORT

String   : KEEP_ASPECT_RATIO_SUPPORT

String   : TOE_SUPPORT
  String   :
MAX_SEARCH_USER_NUMBER
       String   :
VPM_KINDERGARTEN_SUPPORT
     String   :
NVR_MODEL_CODE
       String   :
NVR_MODEL_NAME
       String   :
EPOS_SUPPORT
 String   :
VIDEO_SUMMARY_SUPPORT
        String   :
CHANNEL_COUNT
        String   :
LANGUAGE_SUPPORT
     String   :
POWEROFF_ALARMOUT_SUPPORT
    String   :
NUM_ALARM_IN
 String   : NUM_ALARM_OUT

String : CAMERA_DEFAULT_PW_SUPPORT

String : KEEP_ASPECT_RATIO_SUPPORT

String : TOE_SUPPORT
String :
MAX_SEARCH_USER_NUMBER
String :
VPM_KINDERGARTEN_SUPPORT
String :
POE_SWITCH_STATUS
String : DATA2

String : cs_id
String :
ss_id
String : is_login_ok

String : NVR_MODEL_CODE
String
: NVR_MODEL_NAME
String :
EPOS_SUPPORT
String :
VIDEO_SUMMARY_SUPPORT
String :
LANGUAGE_SUPPORT
String :
CHANNEL_COUNT
String :
nvr_lang
String : setup1

[
Frame]
This plugin detects instances of
frame and iframe HTML
elements.

[JQuery]
A fast, concise,
JavaScript that simplifies how to traverse

HTML documents, handle events, perform animations,
and add
AJAX.

Version :
1.7.2
Website :
http://jquery.com/

[PasswordField]

find password fields

String : chn_user_pwd (from field name)
String : chn_user_new_pwd (from field name)
String : chn_user_new_confirm_pwd (from field name)

[Script]
This plugin detects instances of script HTML elements and

returns the script language/type.

String : javascript,text/javascript

[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
String : requiresActiveX=true

HTTP Headers:

HTTP/1.1 200 OK
X-UA-Compatible: requiresActiveX=true
Set-Cookie: NVR_MODEL_CODE=301; path=/
Set-Cookie: POE_SWITCH_STATUS=1; path=/
Set-Cookie: NVR_MODEL_NAME=SRN-873S; path=/
Set-Cookie: EPOS_SUPPORT=1; path=/
Set-Cookie: VIDEO_SUMMARY_SUPPORT=0; path=/
Set-Cookie: CHANNEL_COUNT=8; path=/
Set-Cookie:

```
LANGUAGE_SUPPORT=16777215; path=/
       Set-
Cookie: POWEROFF_ALARMOUT_SUPPORT=1; path=/

Set-Cookie: NUM_ALARM_IN=4; path=/
  Set-
Cookie: NUM_ALARM_OUT=3; path=/
 Set-Cookie:
CAMERA_DEFAULT_PW_SUPPORT=0; path=/
     Set-
Cookie: KEEP_ASPECT_RATIO_SUPPORT=1; path=/

Set-Cookie: TOE_SUPPORT=1; path=/
   Set-
Cookie: MAX_SEARCH_USER_NUMBER=3; path=/

Set-Cookie: VPM_KINDERGARTEN_SUPPORT=0; path=/

Set-Cookie: NVR_MODEL_CODE=301; path=/

Set-Cookie: NVR_MODEL_NAME=SRN-873S; path=/

Set-Cookie: EPOS_SUPPORT=1; path=/
  Set-
Cookie: VIDEO_SUMMARY_SUPPORT=0; path=/
 Set-
Cookie: CHANNEL_COUNT=8; path=/
 Set-Cookie:
LANGUAGE_SUPPORT=16777215; path=/
       Set-
Cookie: POWEROFF_ALARMOUT_SUPPORT=1; path=/

Set-Cookie: NUM_ALARM_IN=4; path=/
  Set-
Cookie: NUM_ALARM_OUT=3; path=/
 Set-Cookie:
CAMERA_DEFAULT_PW_SUPPORT=0; path=/
     Set-
Cookie: KEEP_ASPECT_RATIO_SUPPORT=1; path=/

Set-Cookie: TOE_SUPPORT=1; path=/
   Set-
Cookie: MAX_SEARCH_USER_NUMBER=3; path=/

Set-Cookie: VPM_KINDERGARTEN_SUPPORT=0; path=/

Set-Cookie: POE_SWITCH_STATUS=1; path=/

Set-Cookie: DATA2=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: cs_id=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
```

```
Set-Cookie: ss_id=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: is_login_ok=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: NVR_MODEL_CODE=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: NVR_MODEL_NAME=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: EPOS_SUPPORT=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: VIDEO_SUMMARY_SUPPORT=deleted;
expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
 Set-Cookie: LANGUAGE_SUPPORT=deleted;
expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
      Set-Cookie: CHANNEL_COUNT=deleted;
expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
 Set-Cookie: nvr_lang=1; path=/

Set-Cookie: setup1=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Last-Modified: Sat, 22 Jun 2024 01:02:45 GMT

Cache-Control: no-store, no-cache, must-
revalidate, max-age=0
       Cache-Control:
post-check=0, pre-check=0
    Pragma: no-
cache
    Content-type: text/html;
charset=UTF-8
      Connection: close

Transfer-Encoding: chunked
  Date: Sat, 22 Jun
2024 01:02:44 GMT


WhatWeb report for
http://192.168.0.200:4000
Status    : 200
OK
Title     : SAMSUNG TECHWIN NVR Web
Viewer
```

```
IP        : 192.168.0.200
Country   :
RESERVED, ZZ

Summary   : Cookies[CAMERA_DEF
AULT_PW_SUPPORT,CHANNEL_COUNT,DATA2,EPOS_SUPPORT,K
EEP_ASPECT_RATIO_SUPPORT,LANGUAGE_SUPPORT,MAX_SEAR
CH_USER_NUMBER,NUM_ALARM_IN,NUM_ALARM_OUT,NVR_MODE
L_CODE,NVR_MODEL_NAME,POE_SWITCH_STATUS,POWEROFF_A
LARMOUT_SUPPORT,TOE_SUPPORT,VIDEO_SUMMARY_SUPPORT,
VPM_KINDERGARTEN_SUPPORT,cs_id,is_login_ok,nvr_lan
g,setup1,ss_id], Frame, JQuery[1.7.2], PasswordFie
ld[chn_user_new_confirm_pwd,chn_user_new_pwd,chn_u
ser_pwd], Script[javascript,text/javascript],
X-UA-Compatible[IE=edge,requiresActiveX=true]
<
br>Detected Plugins:
[ Cookies ]
  Display
the names of cookies in the HTTP headers. The

values are not returned to save on space.


String       : NVR_MODEL_CODE
       String
: POE_SWITCH_STATUS
    String       :
NVR_MODEL_NAME
       String       :
EPOS_SUPPORT
 String       :
VIDEO_SUMMARY_SUPPORT
        String       :
CHANNEL_COUNT
        String       :
LANGUAGE_SUPPORT
     String       :
POWEROFF_ALARMOUT_SUPPORT
    String       :
NUM_ALARM_IN
 String       : NUM_ALARM_OUT

String       : CAMERA_DEFAULT_PW_SUPPORT

String       : KEEP_ASPECT_RATIO_SUPPORT

String       : TOE_SUPPORT
  String       :
MAX_SEARCH_USER_NUMBER
       String       :
VPM_KINDERGARTEN_SUPPORT
     String       :
NVR_MODEL_CODE
```

```
       String       :
NVR_MODEL_NAME
       String       :
EPOS_SUPPORT
 String       :
VIDEO_SUMMARY_SUPPORT
        String       :
CHANNEL_COUNT
        String       :
LANGUAGE_SUPPORT
     String       :
POWEROFF_ALARMOUT_SUPPORT
    String       :
NUM_ALARM_IN
 String       : NUM_ALARM_OUT

String       : CAMERA_DEFAULT_PW_SUPPORT

String       : KEEP_ASPECT_RATIO_SUPPORT

String       : TOE_SUPPORT
  String       :
MAX_SEARCH_USER_NUMBER
       String       :
VPM_KINDERGARTEN_SUPPORT
     String       :
POE_SWITCH_STATUS
    String       : DATA2

String       : cs_id
        String       :
ss_id
        String       : is_login_ok

String       : NVR_MODEL_CODE
       String
: NVR_MODEL_NAME
       String       :
EPOS_SUPPORT
 String       :
VIDEO_SUMMARY_SUPPORT
        String       :
LANGUAGE_SUPPORT
     String       :
CHANNEL_COUNT
        String       :
nvr_lang
     String       : setup1

[
Frame ]
      This plugin detects instances of
frame and iframe HTML
     elements.
```

[JQuery]
    A fast, concise,
JavaScript that simplifies how to traverse

HTML documents, handle events, perform animations,
and add
 AJAX.

  Version   :
1.7.2
        Website   :
http://jquery.com/

[PasswordField]

find password fields

   String   :
chn_user_pwd (from field name)
       String
: chn_user_new_pwd (from field name)
   String
: chn_user_new_confirm_pwd (from field
name)

[Script]
 This plugin detects
instances of script HTML elements and

returns the script language/type.

String   : javascript,text/javascript

[
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
      String   :
requiresActiveX=true

HTTP Headers:

```
HTTP/1.1 200 OK
     X-UA-Compatible:
requiresActiveX=true
       Set-Cookie:
NVR_MODEL_CODE=301; path=/
      Set-Cookie:
POE_SWITCH_STATUS=1; path=/
     Set-Cookie:
NVR_MODEL_NAME=SRN-873S; path=/
 Set-Cookie:
EPOS_SUPPORT=1; path=/
  Set-Cookie:
VIDEO_SUMMARY_SUPPORT=0; path=/
 Set-Cookie:
CHANNEL_COUNT=8; path=/
 Set-Cookie:
LANGUAGE_SUPPORT=16777215; path=/
       Set-
Cookie: POWEROFF_ALARMOUT_SUPPORT=1; path=/

Set-Cookie: NUM_ALARM_IN=4; path=/
  Set-
Cookie: NUM_ALARM_OUT=3; path=/
 Set-Cookie:
CAMERA_DEFAULT_PW_SUPPORT=0; path=/
     Set-
Cookie: KEEP_ASPECT_RATIO_SUPPORT=1; path=/

Set-Cookie: TOE_SUPPORT=1; path=/
   Set-
Cookie: MAX_SEARCH_USER_NUMBER=3; path=/

Set-Cookie: VPM_KINDERGARTEN_SUPPORT=0; path=/

Set-Cookie: NVR_MODEL_CODE=301; path=/

Set-Cookie: NVR_MODEL_NAME=SRN-873S; path=/

Set-Cookie: EPOS_SUPPORT=1; path=/
  Set-
Cookie: VIDEO_SUMMARY_SUPPORT=0; path=/
 Set-
Cookie: CHANNEL_COUNT=8; path=/
 Set-Cookie:
LANGUAGE_SUPPORT=16777215; path=/
       Set-
Cookie: POWEROFF_ALARMOUT_SUPPORT=1; path=/

Set-Cookie: NUM_ALARM_IN=4; path=/
  Set-
Cookie: NUM_ALARM_OUT=3; path=/
 Set-Cookie:
CAMERA_DEFAULT_PW_SUPPORT=0; path=/
     Set-
```

```
Cookie: KEEP_ASPECT_RATIO_SUPPORT=1; path=/

Set-Cookie: TOE_SUPPORT=1; path=/
   Set-
Cookie: MAX_SEARCH_USER_NUMBER=3; path=/

Set-Cookie: VPM_KINDERGARTEN_SUPPORT=0; path=/

Set-Cookie: POE_SWITCH_STATUS=1; path=/

Set-Cookie: DATA2=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: cs_id=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: ss_id=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: is_login_ok=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: NVR_MODEL_CODE=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: NVR_MODEL_NAME=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: EPOS_SUPPORT=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Set-Cookie: VIDEO_SUMMARY_SUPPORT=deleted;
expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
 Set-Cookie: LANGUAGE_SUPPORT=deleted;
expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
      Set-Cookie: CHANNEL_COUNT=deleted;
expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0;
path=/
 Set-Cookie: nvr_lang=1; path=/

Set-Cookie: setup1=deleted; expires=Thu,
01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/

Expires: Mon, 26 Jul 1997 05:00:00 GMT

Last-Modified: Sat, 22 Jun 2024 01:03:39 GMT

Cache-Control: no-store, no-cache, must-
revalidate, max-age=0
       Cache-Control:
post-check=0, pre-check=0
    Pragma: no-
```

```
cache
    Content-type: text/html;
charset=UTF-8
      Connection: close

Transfer-Encoding: chunked
  Date: Sat, 22 Jun
2024 01:03:38 GMT
```

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
```

Dirb Scan Results

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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:554_dirb.txt
START_TIME
: Sat Jun 22 00:15:45 2024
URL_BASE:
http://192.168.0.200:554/
WORDLIST_FILES: wordl
ists/big.txt

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

```
GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:554/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: EMPTY REPLY FROM
SERVER)

-----------------
END_TIME: Sat
Jun 22 00:15:57 2024
DOWNLOADED: 0 - FOUND:
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:555_dirb.txt
START_TIME
: Sat Jun 22 00:15:57 2024
URL_BASE:
http://192.168.0.200:555/
WORDLIST_FILES: wordl
ists/big.txt

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


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:555/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: EMPTY REPLY FROM
SERVER)

-----------------
END_TIME: Sat
Jun 22 00:15:57 2024
DOWNLOADED: 0 - FOUND:
```

```
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:556_dirb.txt
START_TIME
: Sat Jun 22 00:15:57 2024
URL_BASE:
http://192.168.0.200:556/
WORDLIST_FILES: wordl
ists/big.txt

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


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:556/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: EMPTY REPLY FROM
SERVER)

-----------------
END_TIME: Sat
Jun 22 00:15:57 2024
DOWNLOADED: 0 - FOUND:
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:557_dirb.txt
START_TIME
: Sat Jun 22 00:15:57 2024
URL_BASE:
```

```
http://192.168.0.200:557/
WORDLIST_FILES: wordl
ists/big.txt

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


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:557/ ----
==>
DIRECTORY: http://192.168.0.200:557/cgi-
bin/
==> DIRECTORY:
http://192.168.0.200:557/image/

----
Entering directory: http://192.168.0.200:557/cgi-
bin/ ----

---- Entering directory:
http://192.168.0.200:557/image/
----

-----------------
END_TIME: Sat Jun
22 00:15:58 2024
DOWNLOADED: 1665 - FOUND:
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:558_dirb.txt
START_TIME
: Sat Jun 22 00:15:58 2024
URL_BASE:
http://192.168.0.200:558/
WORDLIST_FILES: wordl
ists/big.txt

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


GENERATED WORDS: 555
```

```
---- Scanning
URL: http://192.168.0.200:558/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: UNSUPPORTED
PROTOCOL)

-----------------
END_TIME:
Sat Jun 22 00:15:58 2024
DOWNLOADED: 0 - FOUND:
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:4000_dirb.txt
START_TIM
E: Sat Jun 22 00:15:58 2024
URL_BASE:
http://192.168.0.200:4000/
WORDLIST_FILES: word
lists/big.txt

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


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:4000/ ----
==>
DIRECTORY: http://192.168.0.200:4000/cgi-
bin/
==> DIRECTORY:
http://192.168.0.200:4000/image/

----
Entering directory: http://192.168.0.200:4000/cgi-
bin/ ----

---- Entering directory:
http://192.168.0.200:4000/image/
----
```

```
-----------------
END_TIME: Sat Jun
22 00:15:58 2024
DOWNLOADED: 1665 - FOUND:
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
2024/dirb/192.168.0.200:9192_dirb.txt
START_TIM
E: Sat Jun 22 00:15:58 2024
URL_BASE:
http://192.168.0.200:9192/
WORDLIST_FILES: word
lists/big.txt

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


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:9192/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: OPERATION
TIMEOUT)

-----------------
END_TIME: Sat
Jun 22 00:18:28 2024
DOWNLOADED: 0 - FOUND:
0


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

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

OUTPUT_FILE: res
ults/192.168.0.200_21-06-
```

```
2024/dirb/192.168.0.200:25000_dirb.txt
START_TI
ME: Sat Jun 22 00:18:28 2024
URL_BASE:
http://192.168.0.200:25000/
WORDLIST_FILES: wor
dlists/big.txt

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


GENERATED WORDS: 555

---- Scanning
URL: http://192.168.0.200:25000/ ----

(!)
FATAL: Too many errors connecting to host

(Possible cause: OPERATION
TIMEOUT)

-----------------
END_TIME: Sat
Jun 22 00:20:58 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
```

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