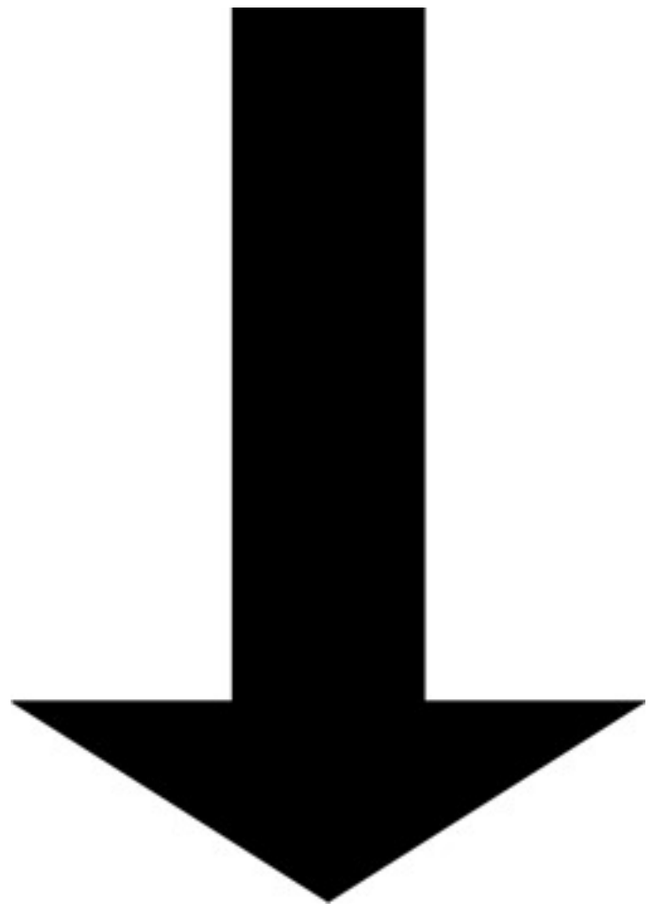
PRELIMINARY SLIDES



THIS WAY


CRAWLING, SLIMY THINGS
ATTACK OF THE 50 FT. WOMAN
CARL LAEMMLE presents
The OLD DARK
J.B. PRIESTLY
OFF
OUGLAS
STUART
AUGHTON
BOND
WHALE
TURE
STRIKES!
H THE SEA
MONSTER FROM THE OCEAN FLOOR
MGM PRESENTS
FORBIDDEN PLANET
AMAZING!
WALTER PIDGEON · ANNE FRANCIS · LESLIE NIELSEN
WARREN STEVENS
ROBBY THE ROBOT
CINEMASCOPE COLOR
1972: DRACULA COLPISCE ANCORA!
CHRISTOPHER LEE · PETER CUSHING
ALLISON HAYES

NO, it is not about horror stories concerning JavaScript

WE ALL LOVE FEAR-MONGERING.

starting with the credits...

A Short History

of the javascript security arsenal

Cast

cfcd208495d565ef66e7dff9f98764da
c4ca4238a0b923820dcc509a6f75849b
c81e728d9d4c2f636f067f89cc14862c
eccbc87e4b5ce2fe28308fd9f2a7baf3
a87ff679a2f3e71d9181a67b7542122c
e4da3b7fbbce2345d7772b0674a318d5
1679091c5a880faf6fb5e6087eb1b2dc
8f14e45fceea167a5a36dedd4bea2543
c9f0f895fb98ab9159f51fd0297e236d
45c48cce2e2d7fbdea1afc51c7c6ad26
d3d9446802a44259755d38e6d163e820
6512bd43d9caa6e02c990b0a82652dca
c20ad4d76fe97759aa27a0c99bff6710
c51ce410c124a10e0db5e4b97fc2af39
aab3238922bcc25a6f606eb525ffdc56
9bf31c7ff062936a96d3c8bd1f8f2ff3
c74d97b01eae257e44aa9d5bade97baf
70efdf2ec9b086079795c442636b55fb

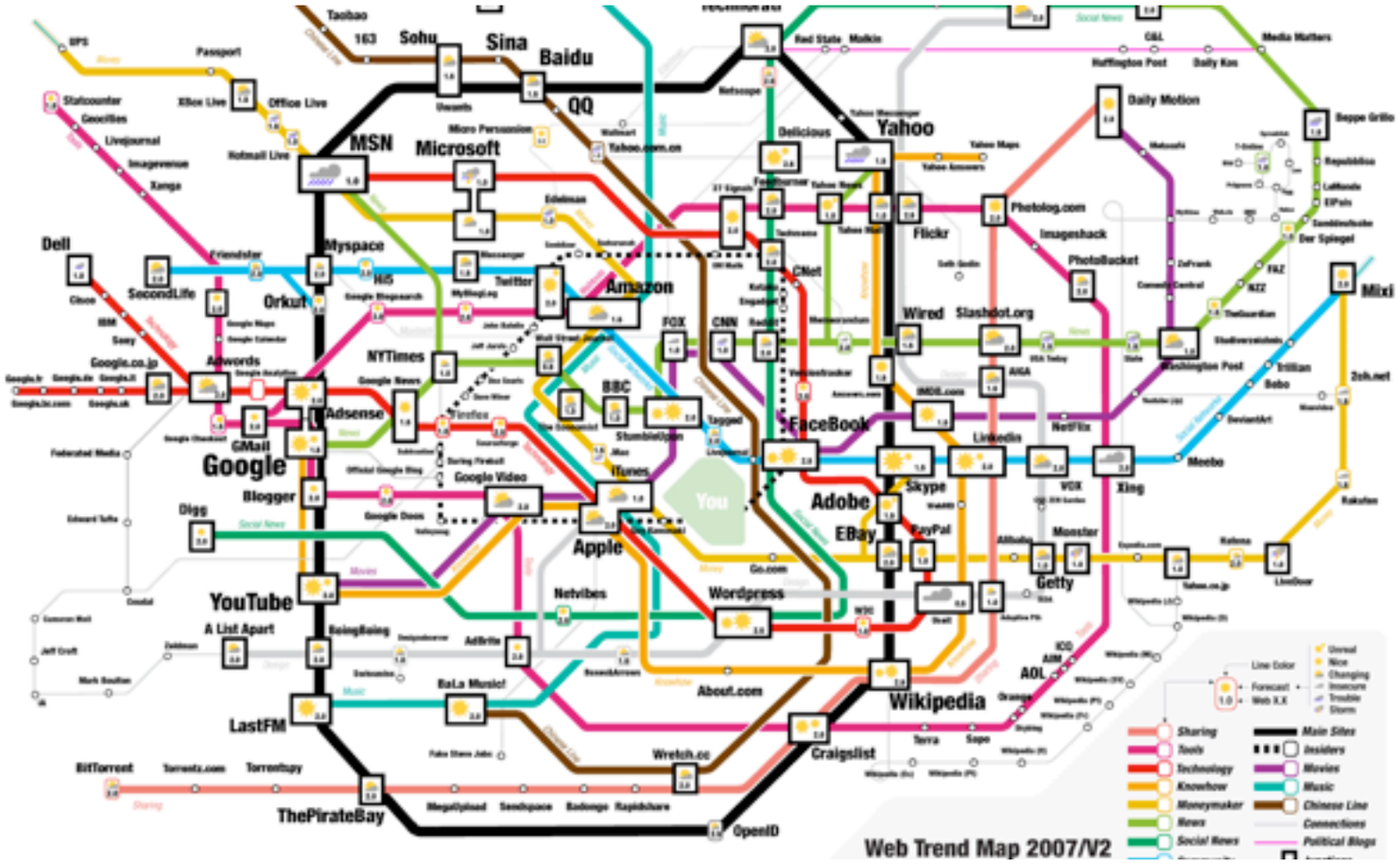
...

...

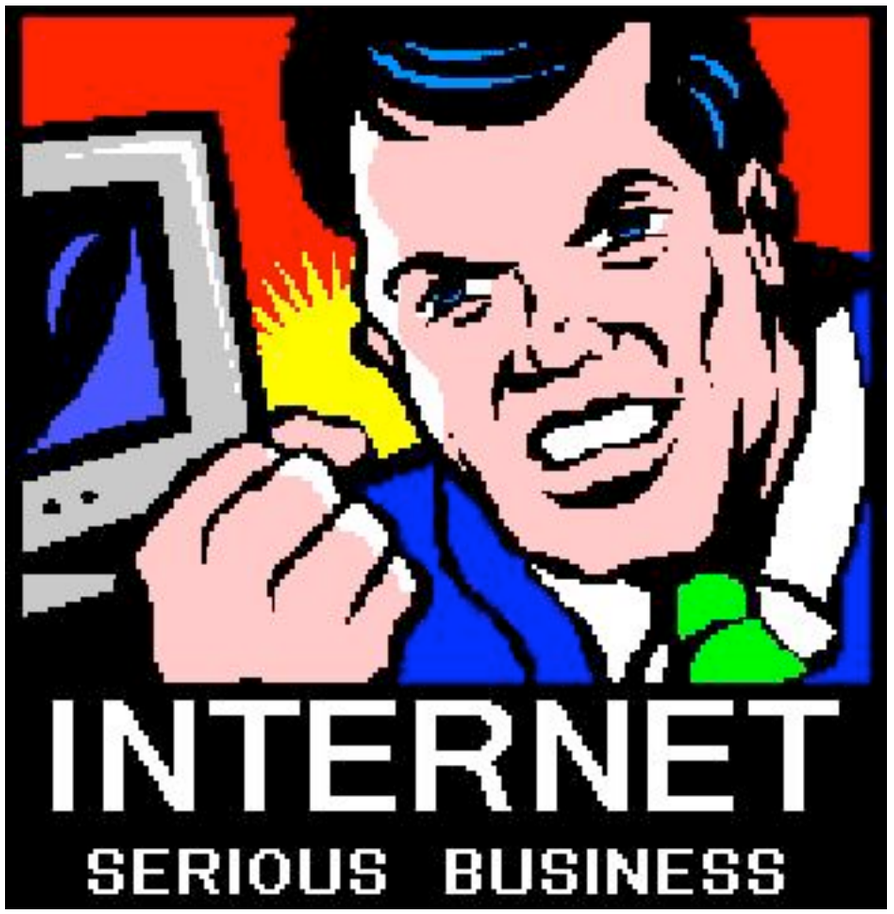
Web Technologies Of The 90s

Web Technologies As Of Today

NOISE


Taobao
163
Sohu
Sina
Baidu
QQ
MSN
Microsoft
Yahoo
Delicious
Flickr
Photolog.com
Daily Motion
Imageshack
PhotoBucket
Dell
Myspace
Friendster
SecondLife
Orkut
Amazon
CNet
Wired
Slashdot.org
Mixi
Google.co.jp
Adwords
Adsense
NYTimes
BBC
CNN
FOX
FaceBook
Google
GMail
Blogger
Digg
Google Video
iTunes
Apple
Adobe
EBay
PayPal
Skype
Linkedin
NetFlix
Xing
Meebo
Wordpress
Netvibes
YouTube
A List Apart
BoingBoing
AdBrite
LastFM
BaLa Music!
About.com
Wikipedia
Craigslist
AOL
ICQ
AIM
Getty
BitTorrent
Torrentz.com
Torrentspy
ThePirateBay
MegaUpload
Sendspace
Badongo
Rapidshare
Wretch.cc
OpenID
You
Web Trend Map 2007/V2
Sharing
Tools
Technology
Knowhow
Moneymaker
News
Social News
Main Sites
Insiders
Movies
Music
Chinese Line
Connections
Political Blogs

THE WWW MAP



SERIOUS BUSINESS

SECURITY IS FASHION

Top Web Hacking Techniques 2007

- XSS Vulnerabilities in Common Shockwave Flash Files
- Universal XSS in Adobe's Acrobat Reader Plugin
- Firefox's JAR: Protocol Issues
- Cross-site Printing (Printer Spamming)
- Hiding JS in Valid Images
- Firefoxurl URI Handler Flow
- Anti-DNS Pinning (DNS Rebinding)
- Google Gmail E-mail Hijack Techniques
- PDF XSS Can Compromise Your Machine
- Port Scan without JavaScript

Top Web Hacking Techniques 2008

- GIFAR
- Breaking Google Gears' Cross-Origin Communication Model
- Safari Carpet Bomb
- Clickjacking/Videojacking
- A Different Opera
- Abusing HTML 5 Structured Client-side Storage
- Cross-domain leaks of site logins via Authenticated CSS
- Tunneling TCP over HTTP over SQL Injection
- ActiveX Repurposing
- Flash Parameter Injection

Top Web Hacking Techniques 2009

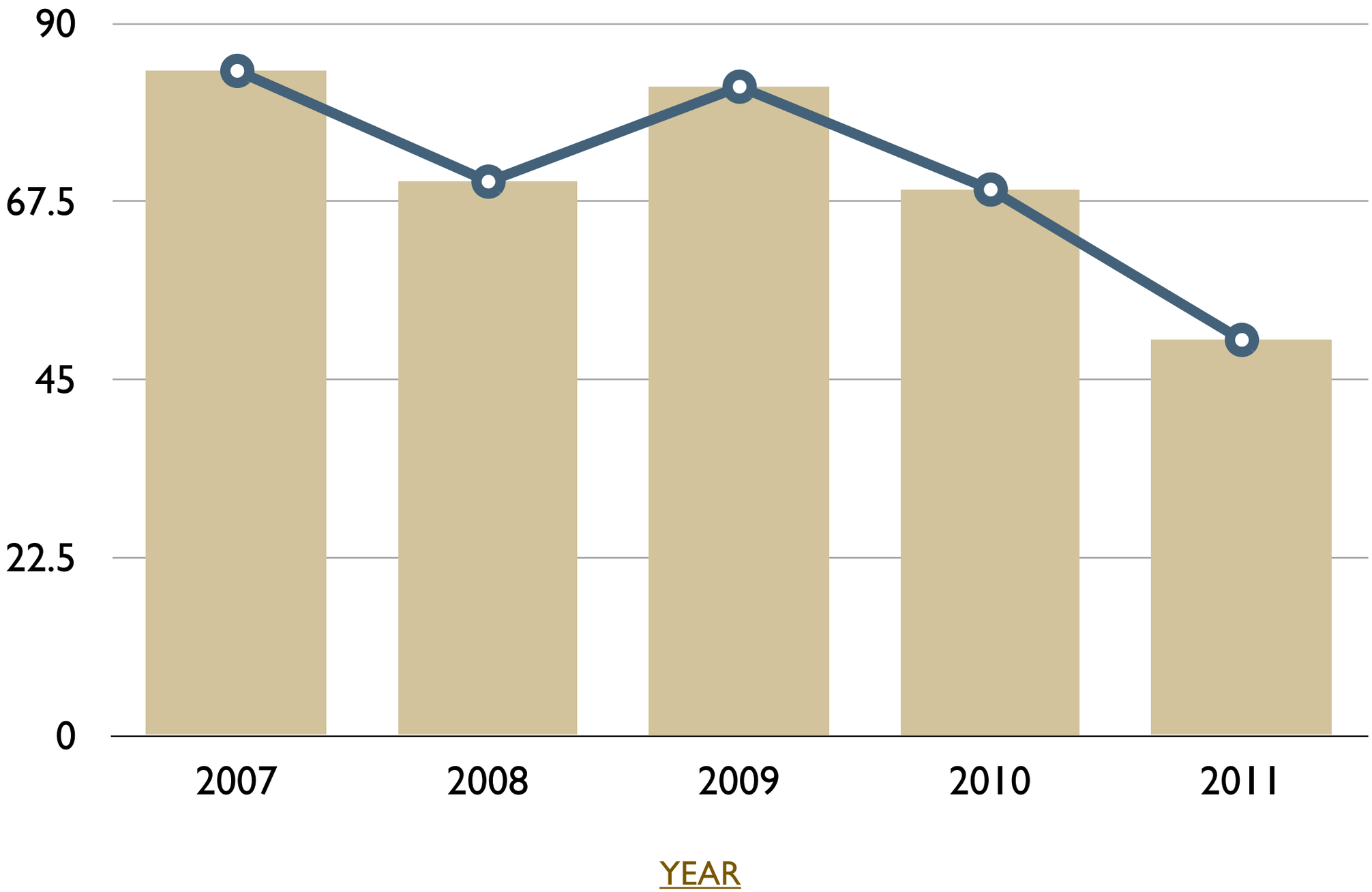
- Creating a rogue CA certificate
- HTTP Parameter Pollution (HPP)
- Flickr's API Signature Forgery Vulnerability (MD5 extension attack)
- Cross-domain search timing
- Slowloris HTTP DoS
- Microsoft IIS 0-Day Vulnerability Parsing Files (semi-colon bug)
- Exploiting exploitable XSS
- Our Favorite XSS Filters and how to Attack them
- RFC1918 Caching Security Issues
- DNS Rebinding – Persistent Cookies, Scarping & Spamming and Session Fixation

Top Web Hacking Techniques 2010

- Padding Oracle' Crypto Attack
- Evercookie
- Hacking Auto-Complete
- Attacking HTTPS with Cache Injection
- Bypassing CSRF protections with ClickJacking and HTTP Parameter Pollution
- Universal XSS in IE8
- HTTP POST DoS
- JavaSnoop
- CSS History Hack in Firefox Without JavaScript for Intranet Portscanning
- Java Applet DNS Rebinding

Top Web Hacking Techniques 2011

- Bypassing Flash's local-with-filesystem sandbox
- Abusing HTTP Status Codes to Expose Private Information
- SpyTunes: Find out what iTunes music someone else has
- CSRF: Flash + 307 redirect = Game Over
- Close encounter of the third kind (client-side JavaScript vulnerabilities)
- Tracking users that block cookies with a HTTP redirect
- The Failure of Noise-Based Non-Continuous Audio Captchas
- Kindle Touch (5.0) Jailbreak/Root and SSH
- NULLs in entities in Firefox
- Timing Attacks on CSS Shaders


90
67.5
45
22.5
0
COUNT
2007
2008
2009
2010
2011
YEAR

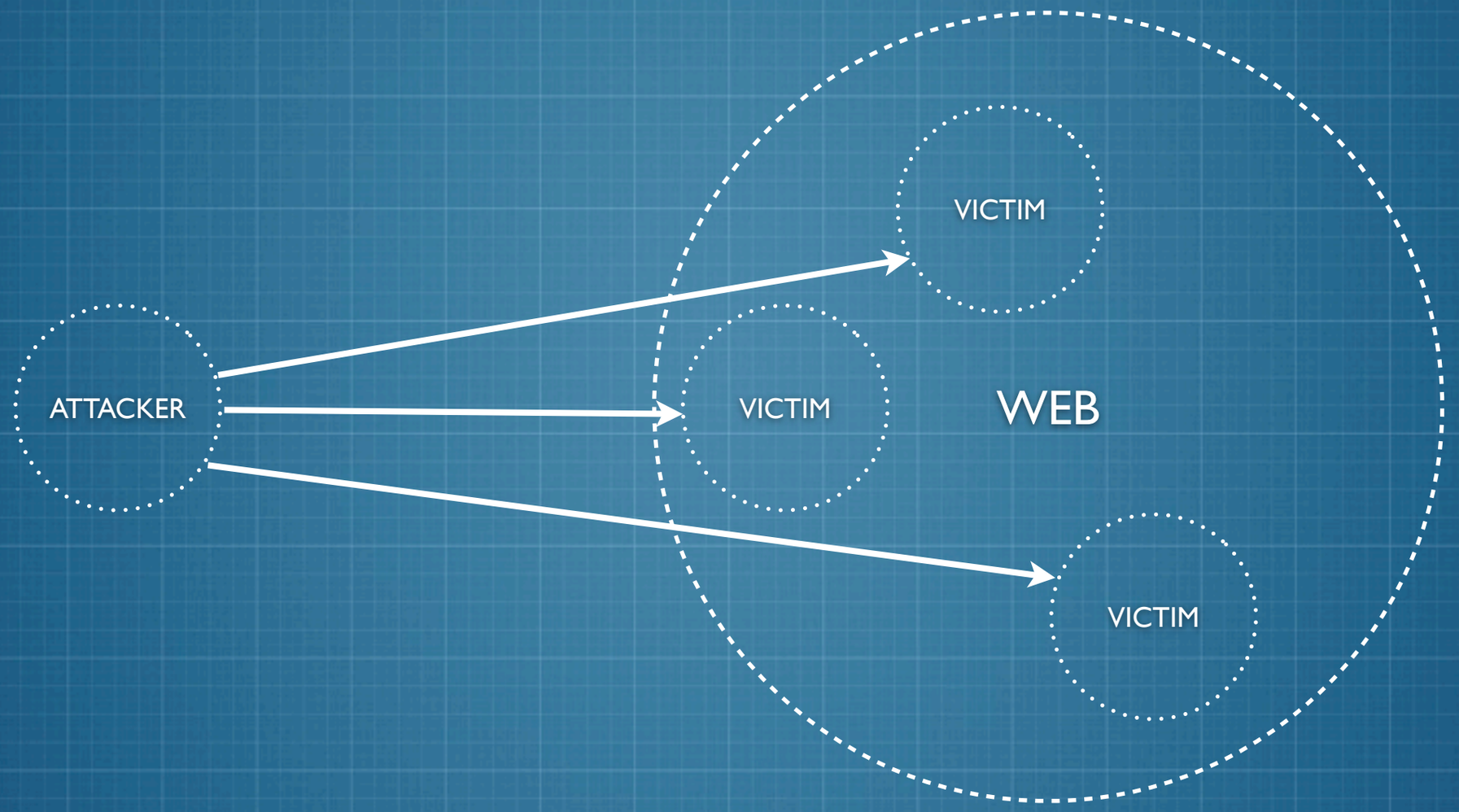
WARNING

JAVASCRIPT

NOT AJAX

JUST JAVASCRIPT

XSS



```
alert(1);
```

Some XSS Attacks

- 2005 - Myspace Worm, Facebook Worm
- 2006 - Yammaner Worm
- 2007 - Orkut Worm
- 2008 - Yahoo IM XSS
- 2009 - Twitter hit by multiple XSS variants, Memova XSS
- 2010 - Apache XSS Attack
- 2011 - Obama XSS, PWN2OWN via XSS, Skype XSS
- 2012 - Facebook Math.Random XSS, Gmail Stored XSS

...inspiration for this presentation...

JIKTO

ATTACKAPI

MYSPACEWORM

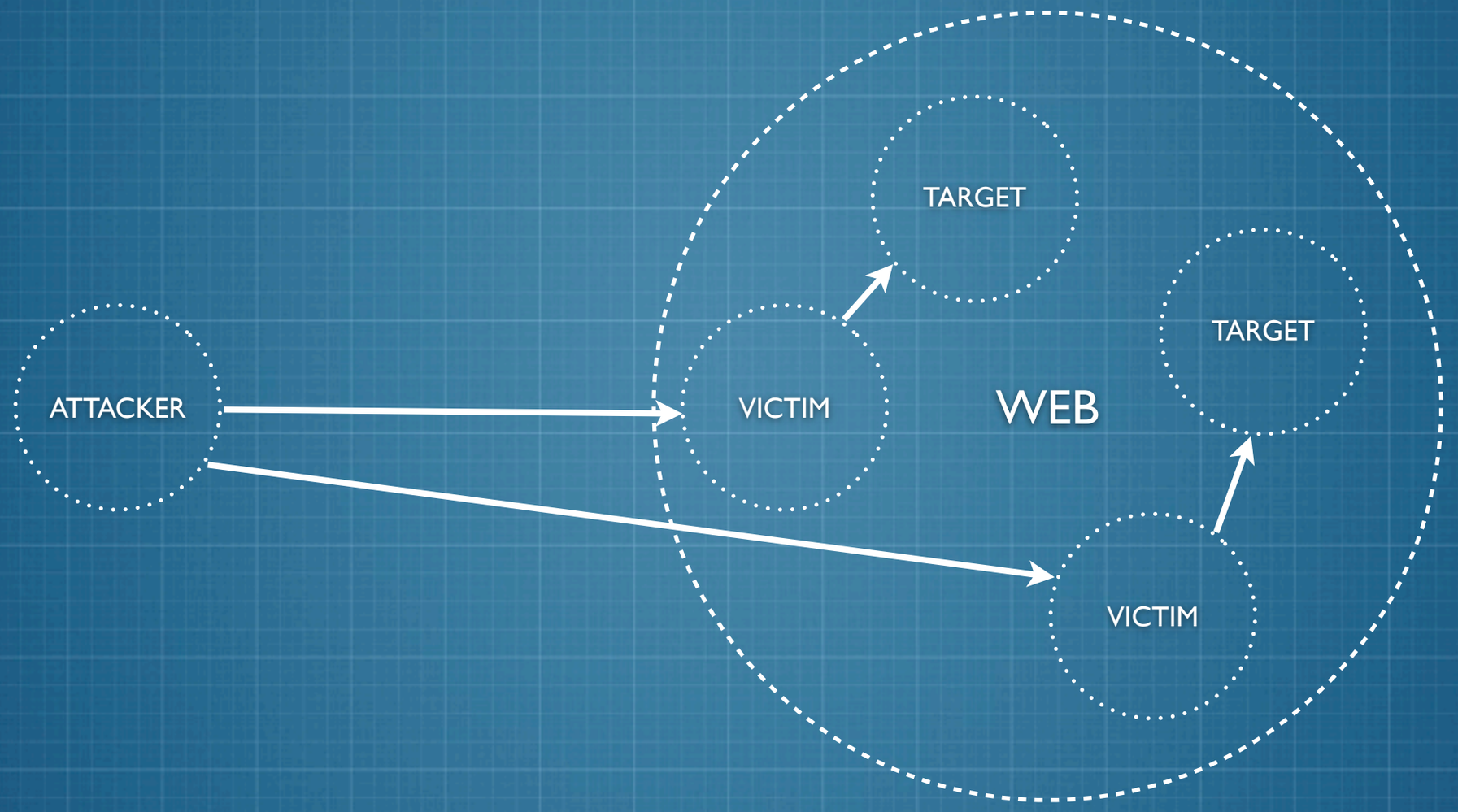
3 Evil Plans


EVIL PLAN 01
TARGET
TARGET
ATTACKER
VICTIM
WEB
VICTIM
User the victim's browser to
attack other web targets.


EVIL PLAN 02
RESOURCE
ATTACKER
VICTIM
NETWORK
RESOURCE
User the victim's browser to
compromise the local network.


EVIL PLAN 03
VICTIM
ATTACKER
VICTIM
SOCIAL
NETWORK
VICTIM
User the victim's browser to
attack other people's profiles.

EVIL PLAN 01

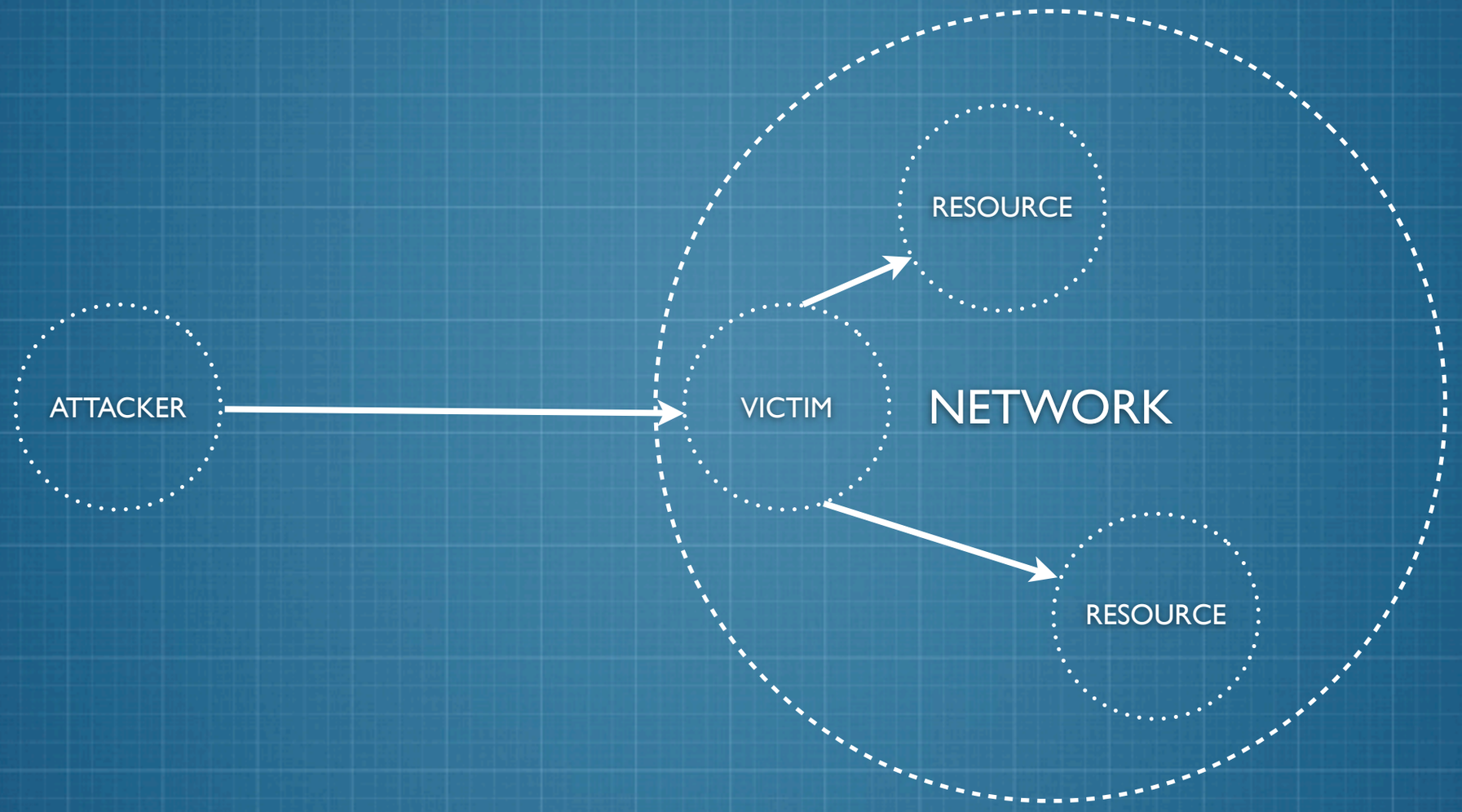


User the victim's browser to attack other web targets.

Evil Plan 01

JIKTO

EVIL PLAN 02

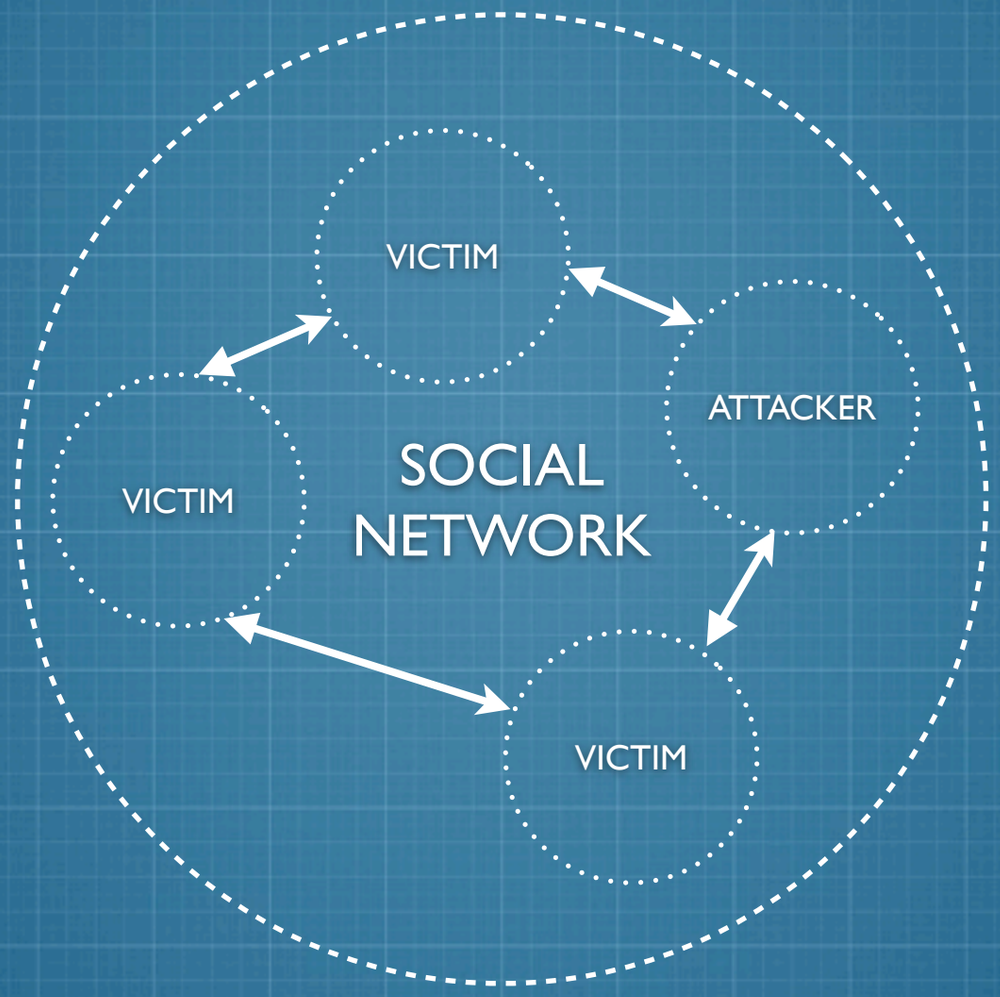


User the victim's browser to compromise the local network.

Evil Plan 02

- JavaScript Port Scanner
- JavaScript Authorisation Brutforcer
- Attacking UPnP
- CSRF and Authentication Bypass in home routers
- Attacking Linksys cameras
- Attacking other embedded network devices

EVIL PLAN 03



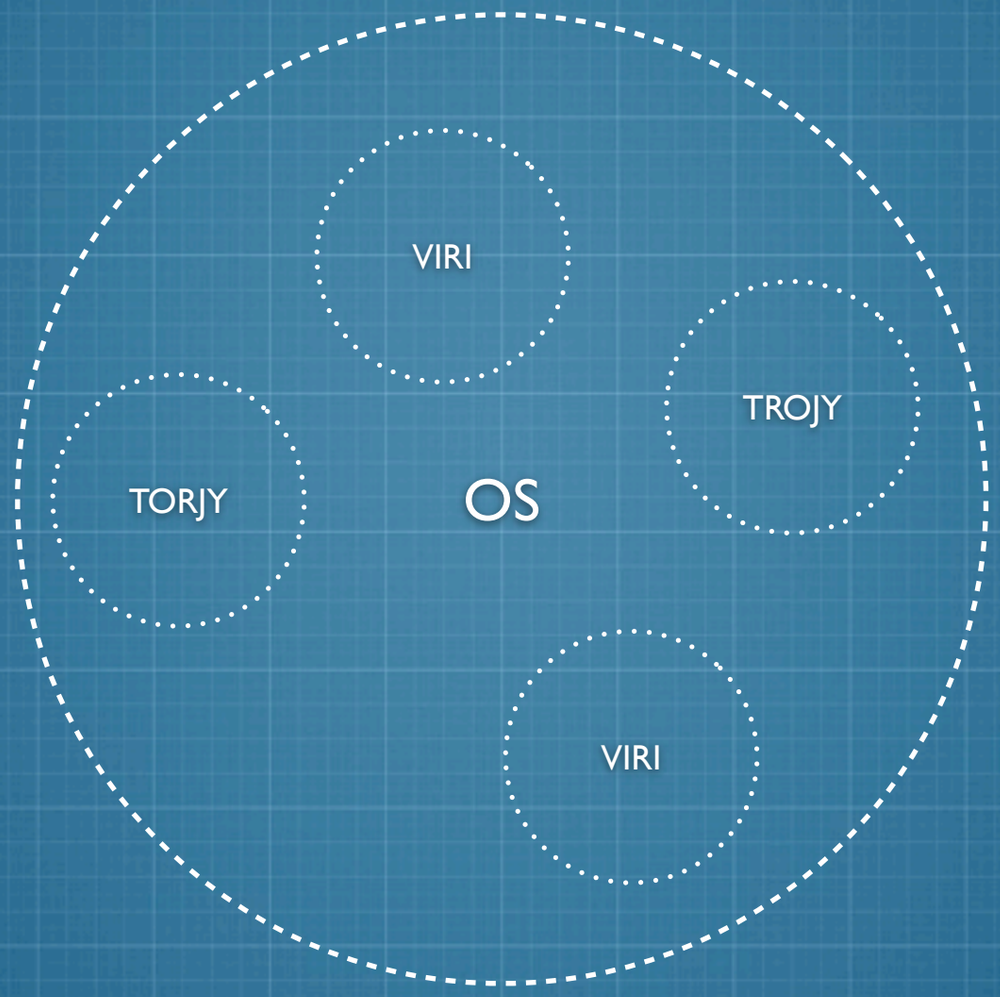
User the victim's browser to attack other people's profiles.

Evil Plan 03

ALL OF ‘EM

...but there is also this....

BONUS EVIL PLAN



User the victim's browser to compromise the system.

Bonus Evil Plan

- Attacking Browsers and Browser Chrome
- Abuse Browser Extension System
- Weaken Browser Security Controls
- Use other system tools like JScript, etc.

GNUCITIZEN

2005, 2006, 2007, 2008

TOOLS

Client-Side Exploitation

&& metasploit®

JUST

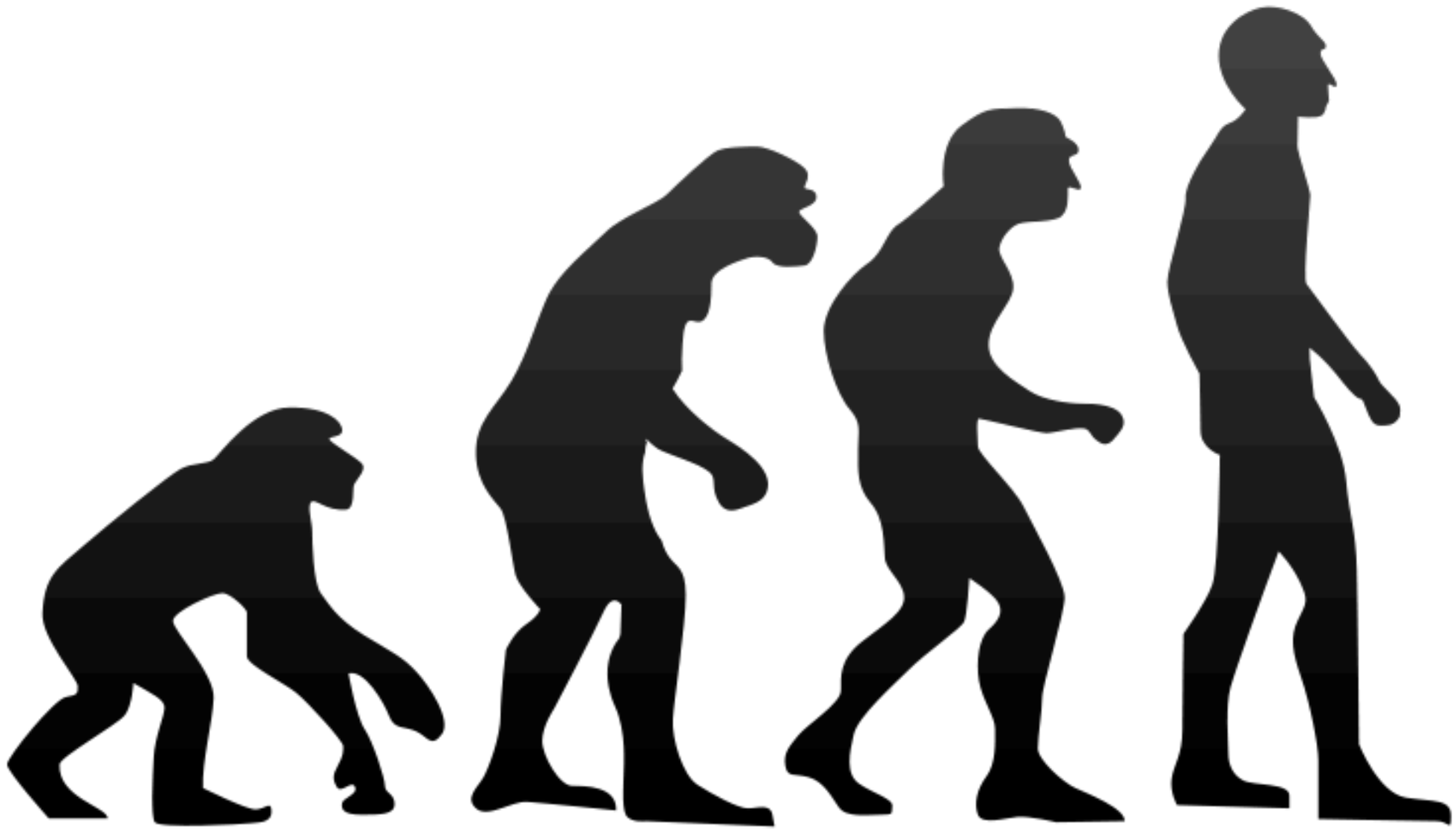
...but also...
SET, XSSF, XSSER, WebSploit

...it is about using the browser for security testing....

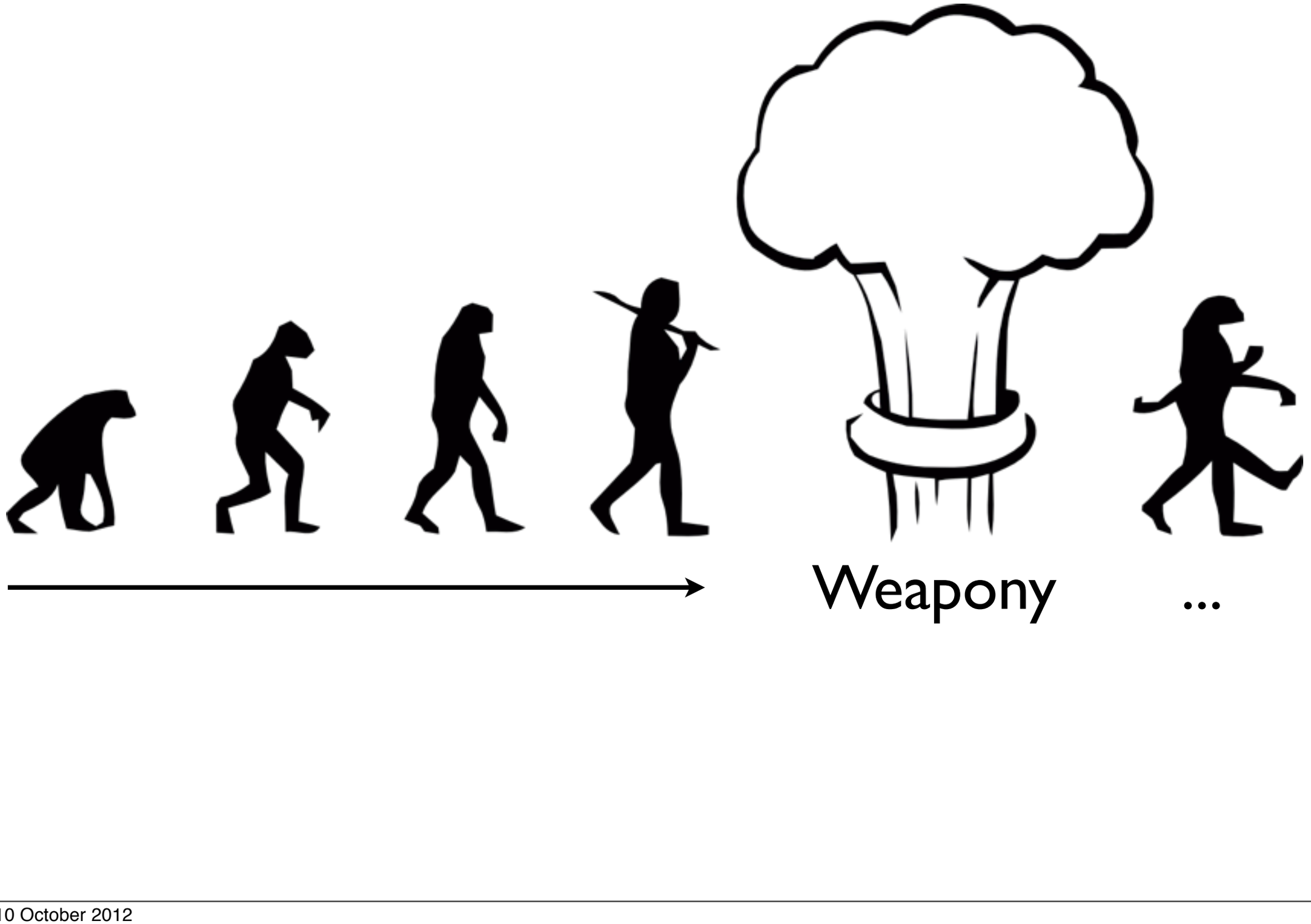
THE WEB IN A BOX

GNUCITIZEN

2009, 2010, 2011, 2012



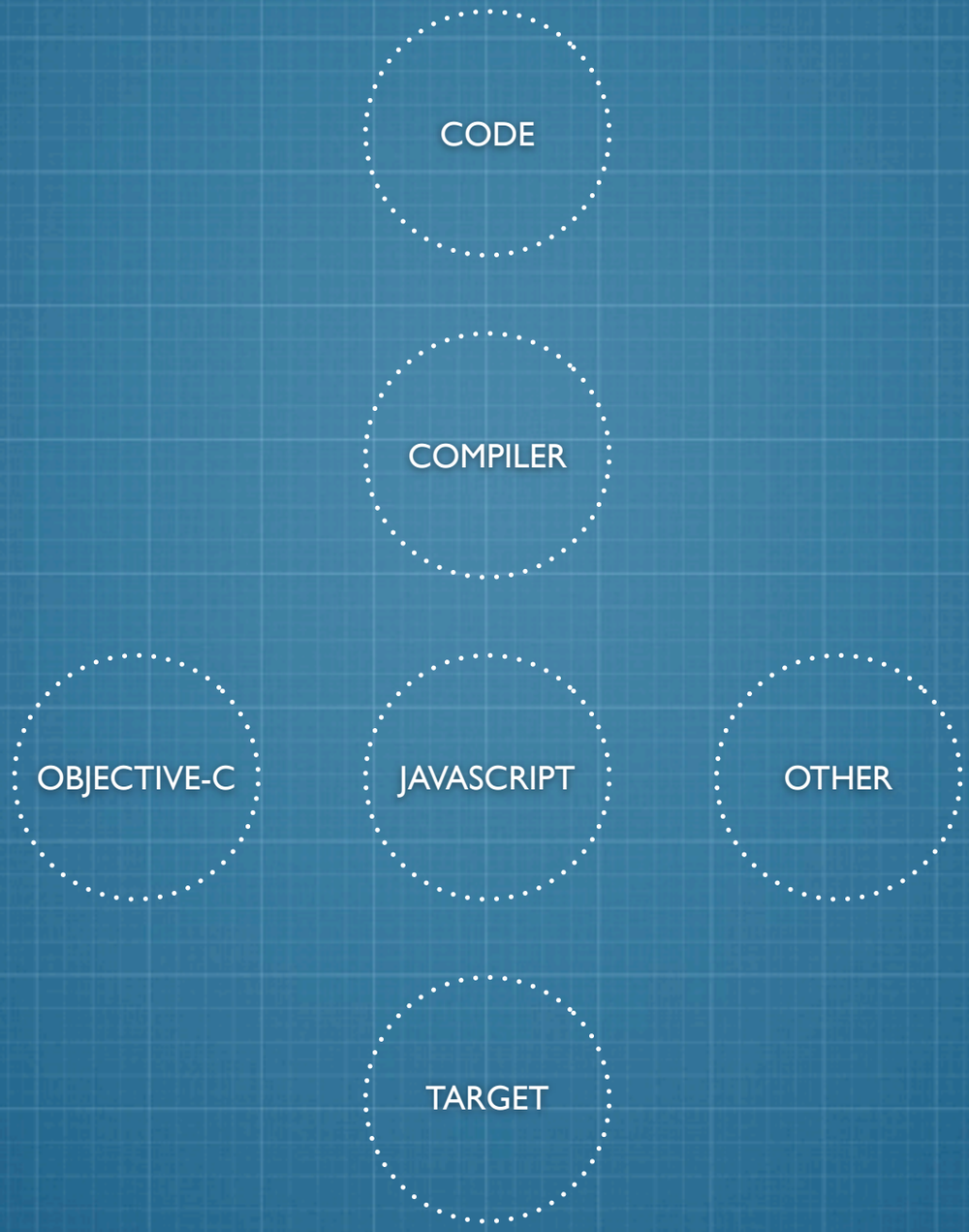
JS Port Scanner AttackAPI Websecurify Suite Weaponry


Weapony
...

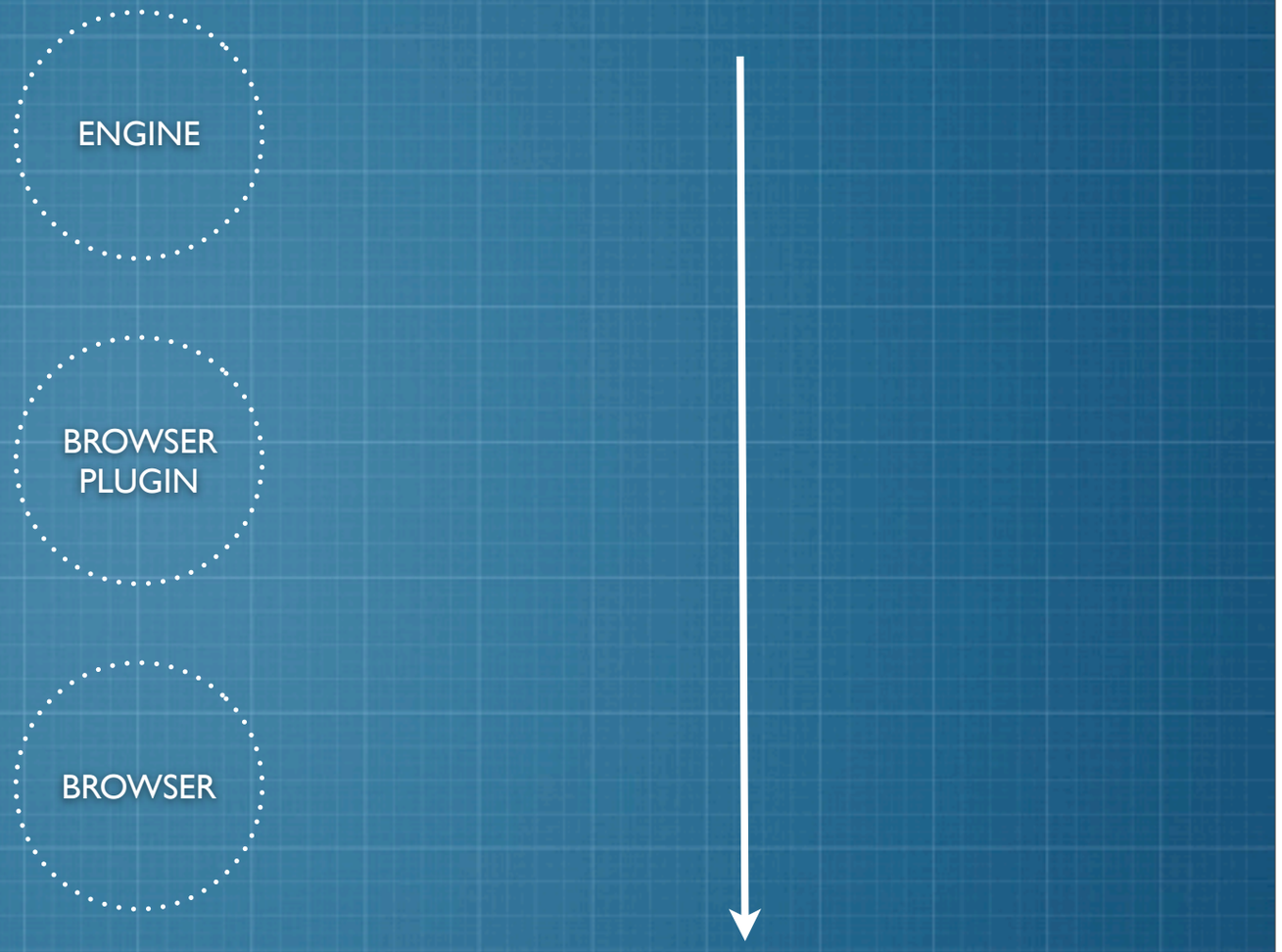
- Create a Client-side Security Scanner
- Create Client-side Security Tools

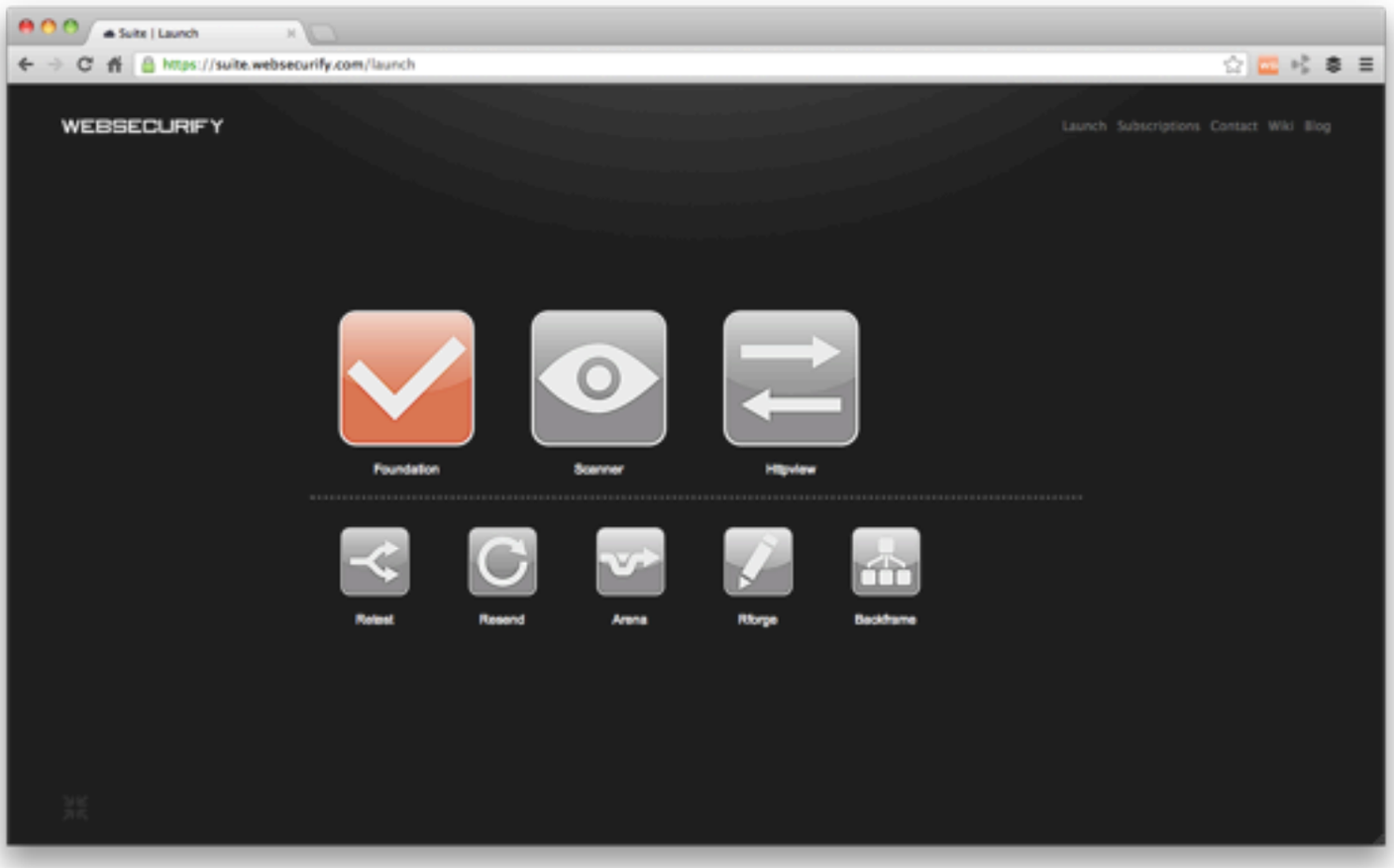
BUT JAVASCRIPT ****S

ARCHITECTURE



ARCHITECTURE





I BELIEVE IN THIS

So Long, and Thanks for All the Fish 

@ryancbarnett @securityshell @soaj1664ashar
@olemoudi @troyhunt @bdpuk @BGInfoSecKnight
@mcarli @Rob_OEM @antisnatchor @ethicalhack3r
@madpowah @marcwickenden

~LinsenSchuss
Tkgd2007
Anonymous Contributors

Universal Pictures, MGM, etc...

Pentesting In Action