Black Hat 2008 Highlights

OWASP KC Meeting
Aug 21, 2008
Rohini Sulatycki

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License.
Contents

■ *DNS Flaw* – Dan Kaminsky

■ Xploiting Google Gadgets: Gmalware and Beyond - Robert Hansen and Tom Stracener

■ Get Rich or Die Trying “Making money on the Web, the black hat way“ - Jeremiah Grossman and Arian Evans

■ Bad Sushi: Beating Phishers at their Own Game- Nitesh Dhanjani & Billy Rios

■ *Spring framework vulnerability* – Ounce Labs
DNS Flaw - Dan Kaminsky
DNS Flaw - Dan Raminsky

- Distributed DNS
  - Map names to numbers
  - Delegation and name servers
    - Send message out
    - Receive replies back

- Bad guys vs Good guys (good name server)
  - Race between good guy and bad guy
    - Bad guy could guess TXID and reply first
    - Odds are with the good guy

- Bad guy
  - could start multiple races with good name server
    - 1.foo.com, 2.foo.com etc
  - When he gets one he could say:
    - Go ask www.foo.com and here’s it’s address and set TTL
DNS Flaw Contd..

- Transaction ID – “random” number between 0 and 65535. The real name server knows the number, because it was contained in the request. The bad guy doesn’t know – at best, he can guess

- TTL not a security feature
  - 1 day
  - 1 hour
  - ...

- Issues
  - Redirect to malicious sites
  - Intercept and corrupt email attachments
  - ...
DNS Patching
Xploiting Google Gadgets: Gmalware and Beyond
- Robert Hansen and Tom Stracener
Xploiting Google Gadgets: Gmalware and Beyond
- Robert Hansen and Tom Stracener

- Gadgets are web-based software components based on HTML, CSS, and JavaScript.
  

- Gadget server must be able to satisfy a Gadget Rendering Request and a JavaScript Request
  
  - Get XML
  - Parse XML
  - Identify Locale and fetch messages
  - ..
  - Output gadget content
- Gadgets are largely 3rd party code and potentially malicious
- Gadgets can be easily weaponized into attack tools or payloads
- Gadgets can attack other gadgets, the desktop, or web sites
- Gadgets can have (most of) the same vulnerabilities as web applications
Threat vectors

- Spyware
- Malware
- Worms
- Personal information theft

- Gmodules domain vulnerable to XSS
- Hosted code insecure
- Current architecture flawed
  - Security model opt-in
Get Rich or Die Trying “Making money on the Web, the black hat way” - Jeremiah Grossman and Arian Evans
CAPTCHA

- Solving Captcha’s for cash
  - CAPTCHA
    - Automated turing test to test for humans vs. bots

- Why?
  - Spammers would like to register for multiple email addresses
Solving Captcha’s for cash

- **CAPTCHA**
  - Automated turing test to test for humans vs. bots

Why?

- Spammers would like to register for multiple email addresses
How?

- Flawed implementation
  - Answer replay
- Low cost automated attack
- Mechanical turk
- Low cost
  - “300-500 CAPTCHAs per person per hour. The clients pay between $9-15 per 1000 CAPTCHAs solved”
Password Recovery

- China-based online “Password Recovery” services:
  - You pay them to hack into “your” account.
  - 300 Yuan ($43) to break an overseas mailbox password,
    with 85% probability of success.
  - 200 Yuan ($29) to break a domestic mailbox password,
    with 90% probability of success.
  - 1000 Yuan ($143) to break a company’s mailbox
    password (no success rate given).
OTHER

- Hire to Hack
- Monetize eCoupon
- Hacking banks
- Flawed return policies
- ...

...
Bad Sushi: Beating Phishers at their Own Game—Nitesh Dhanjani & Billy Rios
- Backtrack phishing e-mails to their malware and data repositories Monetize eCoupon
- Phishers use poor programming practices
  - Store credentials unprotected
  - Store CVV2
  - Sell credit cards and CVV2
    - 500 credit card numbers for $2500
- ATM Skimmers
  - Link to sites that sell physical skimming equipment
Spring Framework Vulnerability - Ounce Labs
Data Submission of non-editable fields

- Web MVC
- DataBinder will bind all parameters to a server side command object
- Hackers could use this to add parameters to submit data to non-editable fields
- Mitigation: Explicitly configure set of fields to bind by calling the setAllowedFields property of each dataBinder

ModelView Injection

- Client data is used as view name
- http://www.springsource.com/securityadvisory