Don’t be a tool’s fool
About Me

• Dave van Stein
  • 40 years
  • Started testing in 2001
    – Functional Testing
    – Interface / Legacy Testing
    – Performance Testing
    – Web Application Security Testing

• ISTQB certified tester
• EC-Council C|EH
• SANS 542 / GIAC GWAPT

• Hobbies: World of Warcraft, Geocaching
• Not the goal:
  – Promote or push tool X
  – Put tool Y in a bad light

• But instead
  – Show easy to forget options
  – Show how to be creative
  – Discussion
• History

• Some tools with demos

• Security Testing
The old days

THE NEO PHYTE'S GUIDE TO HACKING

1993 Edition
Completed on 08/28/93
Modification 1.1 Done on 10/10/93
Modification 1.2 Done on 10/23/93

by

>>> Deicide <<<

The author of this file grants permission to reproduce and redistribute this file in any way the reader sees fit, including the inclusion of this file in newsletter, print, or other media, provided the file is kept whole and complete without any modifications, deletions, or omissions.

(c) 1993, Deicide
Nowadays
• Metasploit
  – Collection of exploits
  – Framework driven

• Pro
  – High quality, often updated
  – Fun to demo :)

• Con
  – Exploit based
Demo 1

OWASP
The Open Web Application Security Project

METASPLOITABLE

METASPLOIT FRAMEWORK

vs

(just for the fun of it)
• Know the limitations of your tool

• No result != no vulnerabilities

• Update tools often
• Nikto
  – Webserver configuration issues
  – Known and common locations, files, options, etc

• Pro
  – Finds a lot of easy to miss items

• Con
  – SSL sometimes gives out-of-memory
  – By default assumes / is root folder
  – Only shows positives
Toolchaining nikto with Burp
Things to remember

• Know the quirks of your tool

• Testing > hacking
  – Negatives are just as important

• Combine tools for additional information
• SQLmap
  – SQL injection scanner and exploiter (yeah, really)

• Pro
  – Huge amount of options
  – Contains lots of evasion filters

• Con
  – Huge amount of options
  – Default option are in ‘safe mode’
An interesting characteristic of ASP is the ability to add as many percentage signs as you want in between characters. For example, `AND 1=%0%0%0%0%0%0%0%0%1` is completely valid.
Things to remember

- Always review default options
- In white-box and grey-box scenarios identify relevant information
• Firefox add-ons
  – Additional functionality

• Pro
  – Flexible, many different add-ons
  – Great for ‘quick & dirty’ testing

• Con
  – Every add-on makes firefox slower
  – Cluttered interface
Multiple profiles in Firefox

"C:\Program Files\Mozilla Firefox\firefox.exe" -no-remote -profilemanager
Things to remember

- Be careful with add-ons
- Use profiles and templates where possible
• Don’t bet on a single tool

Source: The Web Application Hacker’s Handbook
Structured Security Testing

• Use a result collection tool

Gremwell Magictree (local)
  • Burp (as of Burp Suite version 1.3.07)
  • Nmap
  • Nikto
  • Nessus XML v.1
  • Nessus XML v.2
  • OpenVAS
  • Qualys
  • Imperva Scuba
  • w3af
  • Acunetix
  • Rapid 7 NeXpose
  • Arachni
  • OWASP Zed Attack Proxy
  • Metasploit
  • IBM Rational AppScan

Dradis Framework (web application)
  • Burp Scanner
  • Metasploit
  • Nessus
  • NeXpose
  • Nikto
  • Nmap
  • OpenVAS
  • OSVDB
  • Retina
  • SureCheck
  • VulnDB
  • w3af
  • wXf
  • Zed Attack Proxy
• Know the limitations of your tool
• Know the quirks of your tool
• Update tools often

• Always review default options
• In white-box and grey-box scenarios identify relevant information

• No result != no vulnerabilities
• Testing > hacking
  – Negatives are just as important
• Combine tools for additional information
• Use a result collection tool

• Be careful with add-ons
• Use profiles and templates where possible