# Web Exploitation Framework "wXf"

Seth Law

Chris Gates

Ken Johnson

# Seth Law Bio

Seth Law is a Principal Consultant at FishNet Security, specializing in Application Security. He has specialized in information security since 2004 and enjoys researching complex vulnerabilities and exploits. He has worked previously as an unix administrator, coder, and security administrator. Seth is currently based in Salt Lake City where he lives for the winter snowboarding and summer climbing.

# Chris Gates Bio

- Blogger--
  >carnal0wnage.attackresearch.com
- Metasploit Project
- AttackResearch
- Security Twit → carnal0wnage

# Ken Johnson Bio

Blog: cktricky.blogspot.com

BtoD

Dirchex/Dirsnatch

NoVA Hacker

# Framework Overview

# Another framework?

- Prior experience with other web centric frameworks

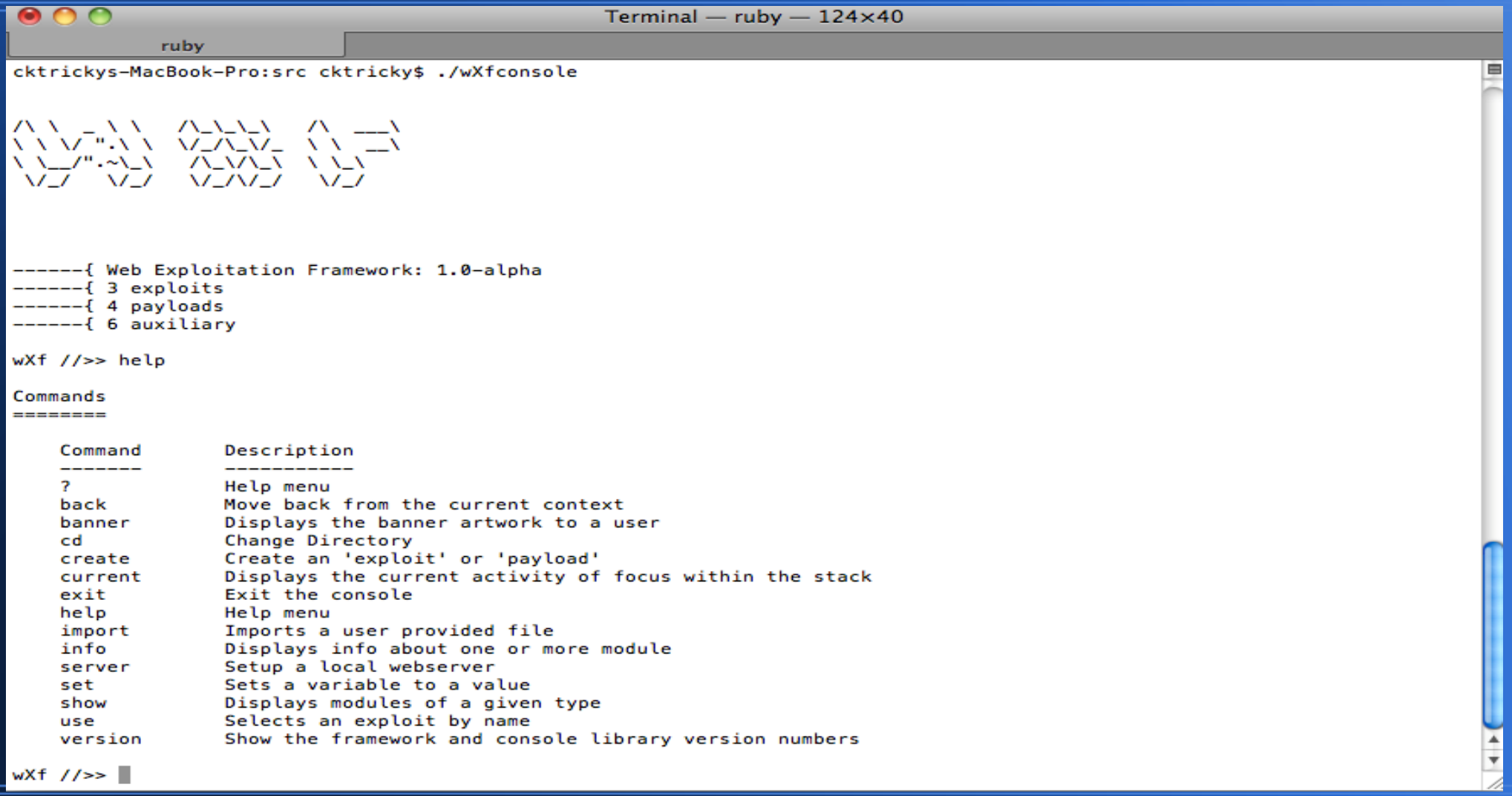
# What about Metasploit?

- Educational, fun, challenging
- Unrestricted core development
- Web 2.0
- AppSec community involvement
- We want more pwnage

# Interface Design

- ...Speaking of MetaSploit
- “Easy Way” = proprietary design
- “wXf Way” = Hard for us, easy for you

# Interface Design



# Framework Core

# Console

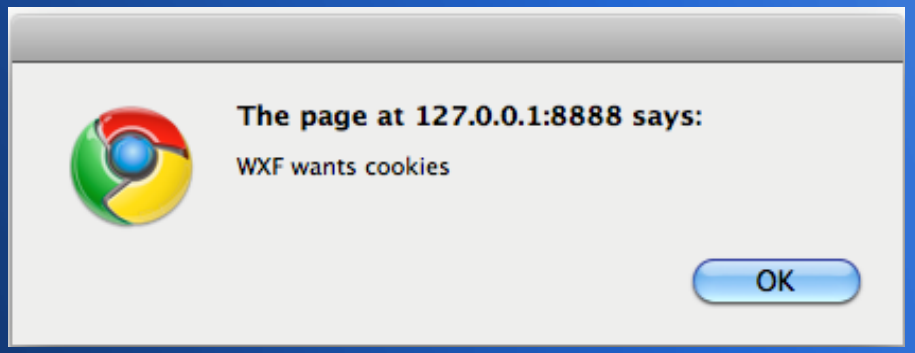
- Rb-readline, readline
- Commands – use, set, help, etc
- DB Interface provided thru console

# Storage

- DB Based Exploits and Payloads, SQLite3
- File based modules
- Deciding which storage to use...

# WebStack

- Hosts RFI Shell
- LFILE / LHTML
- Instances limited by port numbers
- Ability to manage
- Various uses for WebStack...



# WebStack

Potential uses for WebStack, conceptual

- Phish and report
- User-Agent detection, redirection (mobile pwnage)
- Java Version detection and subsequent processing
- Login form overlay, snatch credentials

# WebStack

Examples

- Respond to simple webdav requests
  - Java JNLP vuln via webdav
- Do “stuff” based on user agent received
- Serve up an empty applet to determine java version, then do “stuff”
- Phishing
- General ability to respond to requests...

# WebStack Demo

Video Demonstration

# wXf Application Extensions (wAx)

- Means of extending what wXf can do
- Contains web libraries, re-usable console libraries. Anything that can be re-used should be contained in wAx
- Gem inclusion, version control for wrappers

# Current Libraries

- Mechanize
- Nokogiri
- Savon
- Can be extended

# Planned/Future Libraries

- Requirements
  - Must be tested
  - License must allow for inclusion
  - Has to be stable
  - Must have a use case
- Examples
  - JSON
  - FLASH/AMF
  - DB Translation (candidate SEQUEL)

# Support Platform, Architecture

- *Nix
- Mac OSX
- Ruby 1.8.6, 1.8.7 and testing 1.9.1 (plan for 1.9)
- **HIGHLY** dependent on libxml2
- Requirement for mechanize/nokogiri anyway

# Modules, Exploits and Payloads

# Modules

- Auxiliary, currently, is the only file based module
- 'Assists', think 'mixins' – Wrappers
- Shims provide interoperability and flexible porting
- Allows you to do send_request_cgi, print_status
- Global and Local Options

# Exploits / Payloads

Video Demonstration(s)

# Exploits

- Current
  - RFI
  - XSS
- Future
  - Blind SQLi
  - Oracle
  - Directory Traversal
  - Command Injection
  - File Upload Exploitation

# Payloads (current)

- RFI
  - *PHP Shell
- XSS
  - *alert_from_file
  - *beef hook
  - *webserver stack files

# Auxiliary

Chris Gates - Aux Mods Demo

# Auxiliary

- user_agent_test
  - Port of Chris John Riley's user agent tester
- dir_trav_fuzz
  - Fuzz http services for directory traversals
- passive_enum
  - Gather info based on return server headers
  - Server version from headers
  - Web service toolkits id from cookies, x-powered-by, etc

# Auxiliary

Ken Johnson – Aux Mods Demo

# Future Framework uses

WAF Detection and Evasion

IDS Detection / Evasion

Scanner Modules, exploit tie-in

# Reporting

- Planned future reporting methods (out)
  - Dradis hook
  - XML Export
- Planned future reporting methods (in)
  - Burp Import
  - Nikto Import

# Summary

- AppSec community involvement pivotal in success
- Road-Map
- Release
- Beta Testers

# Contact Information

- Twitter
  - @wXframework
  - @sethlaw
  - @carnal0wnage
  - @cktricky
- Email – wXfdev@gmail.com

# Questions?

# Web Exploitation Framework

Thank you!!!