



# Injectable Exploits

New Tools for Pwning Web Apps and Browsers

Kevin Johnson – [kevin@inguardians.com](mailto:kevin@inguardians.com)

Justin Searle – [justin@inguardians.com](mailto:justin@inguardians.com)

Frank DiMaggio – [frank@secureideas.net](mailto:frank@secureideas.net)



# Who are we?

---

- Kevin Johnson
  - BASE/SamuraiWTF/Laudanum/Yokoso! Project Lead
  - Penetration Tester
  - Author and instructor of SANS SEC542
- Justin Searle
  - SamuraiWTF/Yokoso!/Middler Project Lead
  - Penetration Tester
  - SmartGrid and Embedded Hardware Researcher
- Frank DiMaggio
  - Web App Security Researcher
  - Laudanum Project Lead
  - SamuraiWTF/Yokoso!/BASE Core Developer



# Laudanum

<http://laudanum.inguardians.com>



# Writing Files with SQL Injection

---

- Most RDBMS' can write to files
- For example MySQL has the INTO directive

```
SELECT * FROM table INTO outfile 'data.txt';
```

- Can write anywhere MySQL has permissions
- Got root?



# Controlling Output

---

- But we can control the output

```
SELECT "Injectable Files are Cool!"  
FROM table;
```

- It's not a search of the table
- Returns a record set that is just the string!



# Milk and Cookies

---

- By combining the previous two queries
- We can inject files of our choosing
- Written to where the RDBMS has permissions



---

# Laudanum

provides the payloads for this injection!



# Pieces of Laudanum

---

- Exploit scripts designed for injection
- Multiple functions
  - Written in popular web scripting languages
  - PHP, ASP, CFM, JSP





# Shells

---

- Shell access is a win!
- Scripts to provide shell access
  - Web based shell so no interactive commands
- Can use BASE64 encoding to bypass IDS and monitoring



# Utilities

---

- Many scripts that are useful during pen-tests are in development
  - DNS Retrieval
  - Active Directory Querying
  - Port Scanners
  - Vuln Scanners
  - Limited by our Imagination!



# Scope Limitations

---

- Important for Pen-Tests
- Built-in features in the scripts
- Allows us to control who can access
  - IP restrictions
  - Authentication
- Returns 404 Status Codes if you fail scope check



Yokoso!

<http://yokoso.inguardians.com/>

# Yokoso!



**Yokoso JAPAN**

*Yokoso means "Welcome."*

It's our way of inviting you to our home, our Japan. Discover the warmth and hospitality of a gentle, ancient culture. A place that can only be experienced up close and personal.

*Enter site*

- All foreign nationals landing in Japan are required to submit to fingerprinting and having their picture taken since November 2007.



# What is Yokoso!

---

- Yokoso is a collection of fingerprints
- These can be used in multiple ways
  - XSS
  - Mapping Function
  - Attack Scripts



# Fingerprints?

---

- More of our infrastructure is web-managed
- Fingerprints are the URLs of unique resources
  - Resources within the administration
  - Unique files that identify the system
    - index\_ie.htm
    - pb\_apache.gif



# Pre or Post Auth

---

- Some resources require authentication
- Yokoso! contains both pre and post authentication fingerprints
  - Pre auth fingerprints are used for infrastructure discovery
  - Post auth fingerprints are used for user mapping



# Usages for the Fingerprints

---



- These fingerprints can be used within XSS attacks
  - Infrastructure Discovery
    - Determining critical devices
    - Within the attacked browser's network
  - History Browsing
    - Where has this browser been
    - Are they interesting to us?

# Fingerprints Wanted!


---



- Collect fingerprints using interception proxies like Burp or WebScarab
- Save those logs
- Remove all unrelated requests and responses
- PURGE private data from remaining data
  - Put a placeholder in the place of the data
- Send us what's left
- Tell us what we are looking at!



# 侍 SAMURAI



WEB TESTING FRAMEWORK

<http://samurai.inguardians.com/>



# SamuraiWTF

---

- 2 Versions: Live CD and VMware Image
- Based on the latest version of Ubuntu
- A few of the tools included:
  - Laudanum
  - Yokoso!
  - w3af
  - BeEF
  - Burp Suite
  - Grendel-Scan
  - Dirbuster
  - WebScarab
  - ratproxy
  - nmap

# Future plans for SamuraiWTF

---



- Move to Kubuntu
- Move toward the Ubuntu build process
- Move all software and configurations to Debian packages
  - Software upgrades between official releases
  - Easier for users to customize the distro
  - Provides access to WTF tools in all Ubuntu installs
  - Facilitate collaboration within dev team



# How Can You Help?!

---

- Project Links
  - <http://laudanum.inguardians.com/>
  - <http://yokoso.inguardians.com/>
  - <http://samurai.inguardians.com/>
- Join one of the projects.
- If you like the tools (we think you will), pass the word.



# Thanks!

---

- Kevin Johnson
  - kevin@inguardians.com
  - Twitter @secureideas
- Justin Searle
  - justin@inguardians.com
  - Twitter @meeas
- Frank DiMaggio
  - frank@secureideas.net
  - Twitter @hanovrfst