Injectable Exploits

Kevin Johnson – kevin@inguardians.com

Justin Searle – justin@inguardians.com

Frank DiMaggio – 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

' or 42=42 --

It’s not the Answer

' or 42=42 --

It’s the question!

Injection Flaws

- Injection flaws == the attacker is able to inject content into the application

- We love applications that trust users

- Categories include
  - SQL injection
  - XSS
  - CSRF
  - Command Injection
  - etc...

Injectable Exploits

- Injectable exploits == FUN!
- Many different things can happen
- SQL injection is one of the most popular
- Many different attacks
  - Retrieving records
  - Changing transaction
  - Execute Commands
  - Write files!

Laudanum

http://laudanum.inguardians.com

Laudanum

- Laudanum: also known as opium tincture or tincture of opium, is an alcoholic herbal preparation of opium. It is made by combining ethanol with opium latex or powder. Laudanum contains almost all of the opium alkaloids, including morphine and codeine. A highly potent narcotic by virtue of its morphine content. –wikipedia
- An awesome open source project that makes exploitation easier.

Pieces of Laudanum

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

Examples of Included Functions

- –DNS Query
- –Active Directory Query
- –Nmap Scans
- –LDAP Retrieval
- –Shell (Yeah!)

SQL Injection to Write Files

- Use the INTO directive

```
SELECT * FROM table INTO dumpfile '/
  result';
```

- Can write anywhere MySQL has permissions
  - Got root?

Shells

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

Utilities

- Many scripts that are useful during pen-tests
  - DNS Retrieval
  - Active Directory Querying
  - Port Scanners
  - Vuln Scanners

Proxying

- Scripts to proxy web requests
- Allows us to browse the internal sites
- Potentially bypassing IP restrictions
  - Browse admin pages

Scope Limitations

- Features within the scripts
- Allows us to control who can access
  - IP restrictions
  - Authentication
- Limits who can be attacked by the features

Yokoso!

http://yokoso.inguardians.com/

Yokoso!

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.

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

Yokoso!

- "So what can you do with XSS?" - we hope that Yokoso! answers that question.
- JavaScript and Flash objects that are able to be delivered via XSS attacks.
- Payloads will contain the fingerprinting information used to map out a network and the devices and software it contains.

Pieces of Yokoso!

- Yokoso! contains various pieces
- Main feature is the fingerprints
  - All of the other features use these
- Infrastructure discovery finds the hosts
- History browsing for users visiting the fingerprinted URLs
- Modules for popular Frameworks

Fingerprints Wanted!

- Yokoso! project is collecting fingerprints of devices and software
- Collect fingerprints using interception proxies like Burp or WebScarab
- Save those logs
- Remove all unrelated requests and responses
- PURGE private data from remaining data
- Send us the what's left

Infrastructure Discovery

- JavaScript leverages the included fingerprints to look for “interesting” devices
  - Server Remote Management
    - HP ILO (Insight Lights Out)
    - Dell RAC (Remote Access Card)
  - IP-based KVMs (Avocent, HP, IBM, etc...)
  - Web-based Admin Interfaces
    - Network Devices (Routers, Switches, & Firewalls)
    - Security Devices (IDS/IPS, AntiVirus, DLP, Proxies)
    - Information Storehouses (Help Desk, SharePoint, Email)
    - Virtualization Host Servers (VMware, Citrix)

History Browsing

- Allows us to determine if someone has been to the page
  - Identifies Administrators
  - Widens the attack surface
  - Give us more to do with XSS
- Further aids in determining the existing infrastructure

Framework Modules

- Yokoso! Includes modules to integrate into popular frameworks
  - BeEF
  - BrowserRider
  - Others...

Scope Limitations

- The project focus is on penetration testing
- Include various methods to limit attack scope
- Prevents us from accidently pwning out-of-scope parties! ;-)

SamuraiWTF

(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:
  - w3af
  - BeEF
  - Burp Suite
  - Grendel-Scan
  - Dirbuster
  - Maltego CE
  - Nikto
  - WebScarab
  - Rat Proxy
  - Zenmap

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