It's All Fun In The Sun
Until Someone Gets Burned
About Me
Objectives

- Attack Life Cycle
- Demo – Compromise
- Incident Response
- Demo – Cleanup
- Questions
Attack Life Cycle

- Reconnaissance
- Scanning
- Exploitation
- Maintaining Access
Reconnaissance

- Vulnerability Databases
- Exploit Databases
- Search Engine Discovery
Scanning

• Spiders, Robots, and Crawlers
• Vulnerability Scanners
• Review Comments and Metadata
• Identify Entry Points
Exploitation

• Utilize Entry Points
• Authentication/Authorization
• Business Logic
• Data Validation
Maintaining Access

- Backdoors
- Adding Users
- Creating Valid Sessions
- Reading Config Files
Incident Response

- Preparation
- Detection and Analysis
- Containment/Eradication/Recovery
- Post Incident
Preparation

- What Resources Are Available
- What Is Logged / Where
- What Are Your Threats
- Backup Schedule
- Password Strength / Rotation
Detection and Analysis

- Know Your Content
- Has Your Site Changed
- Review Your Logs
- What Stands Out
Recovery

- Review Your Content
- Scan Your Local Systems
- Restore From Clean Backups
- Review Again
- Update Everything
Post Incident

- What Happened
- What Went Right
- What Went Wrong
- How Can This Be Prevented
Resources

• Data Validation - http://codex.wordpress.org/Data_Validation


• Exploit Database - http://www.exploit-db.com/

• Open Source Vulnerability Database - http://osvdb.org/search/search?search%5Bvuln_title%5D=wordpress

• OWASP - https://www.owasp.org