EFFICACY OF LAYERED APPLICATION SECURITY THROUGH THE LENS OF HACKER

Gyan Prakash
Chief Security Architect
VISA Inc.

Bill Yue Chen
Chief Security Architect
VISA Inc.
Agenda

- Threat Model
- Observations
- Optimizing App Security Life-Cycle Controls
- Agility with Security
- What Pen Test Should Focus on
- Recommendations
"Know yourself, also know your rival."

-Sun Tzu, 545-470 B.C.
Threat Model Over The Kill Chain

1. Recon.
   - Scans, DNS, Asset discovery, Social Eng., etc.

2. Delivery
   - Malware, Open Source Poisoning, Faked Web, etc.

3. Exploit
   - Passive Traps & Proactive Attacks

4. Installation
   - Network, Infra, OWASP Vuln IAM Issues, etc.

5. Act. & Obj.
   - Camouflaged Actions, APT, Outbound control exploit

6. Weaponizing
   - Malware, Open Source Poisoning, Faked Web, etc.

7. Proactive Attacks
   - Network, Infra, OWASP Vuln IAM Issues, etc.

8. Outbound control exploit
   - Camouflaged Actions, APT, Outbound control exploit

- ML Assisted Social Engineering
- Advanced Spearphishing (e.g. SNAP_R)
- Automated CAPTCHA Reader
- Advanced PW Guessing (e.g. PassGAN)
Just Overview!

Web Vul.
Scanner
WAF
RASP
Binary Composition
Pen Test
SAST
IAST
DAST
IAST
App Vul.
Monitoring
Observations

Thousands

Hundreds

Thou
sand
s

Hun
dre
d
s
Observations: Application Vulnerabilities

- Flawed Authentication
- Security Misconfigurations
- Sensitive Data Exposure
- Insecure TLS/SSL usage
- Cross-Site scripting
- Injection
- Using vulnerable components
- Inappropriate error handling
- CSRF
Optimizing App Security Coverage

- **SAST**
  - More Than One Third
    - Injections
    - Sensitive Data Exposure
    - XML External Entities (XXE)
    - Cross-Site Scripting
    - Insecure Deserialization

- **IAST**
  - Around Two Third
    - Injections
    - Sensitive Data Exposure
    - XML External Entities (XXE)
    - Cross-Site Scripting
    - Insecure Deserialization
    - Security Misconfigurations
    - 3rd Party Vulnerable Lib

- **DAST**
  - Around One Third
    - Injections
    - Sensitive Data Exposure
    - XML External Entities (XXE)
    - Cross-Site Scripting
    - Security Misconfigurations
Security Embedded with Agile
Security Embedded with Agile

> 80 % with <<
What Pen Test should focus on?

- Authentication & Authorization
  - Authentication flow and design, Passwords, 2FA, Security questions, Access Control
- Session management
- Business Logic
- All possible bypassing issues
- Data flows that are not covered by scanners, such as email, SSH, SAML etc.
- Examine Attack surface
- Sampling test Injection, XSS, to validate SAST/IAST/DAST controls
- Last but not the least, Infrastructure
Completing the Puzzle
Recommendations

- **Shift Left** – Train and Empower Developers to Security Champions
- **Automation** - Empower engineers with SAST, IAST, OSS, and WVS
- **Pen test smartly** – Focus on the limitation area of tools
- **Implement multi-factor authentication**
- **Check password blacklist**
- **Phishing/social engineering awareness training**
Questions & Answers

Sprint Backlog Iteration Product Shipping

Developer
Workspace
Daily
Builds
SPRINT
1 - 3 weeks
SAST
IAST
DAST
SAST
IAST
SAST
Pen
Test
CI Automation
Web Vul. Scanner
Real time Analytics
PRODUCTION

WAF
Web Vul. Scanner
Scanner
Real time
Analytics
PRODUCTION

Web Vul.
Scanner
Real time
Analytics
PRODUCTION