IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

安全なウェブアプリケーション構築のための開発環境

～Webアプリ開発基礎体力の向上について～

IPAセキュリティセンター研究員
園田道夫

開発力とは

- プログラミングスキルのこと？
- スキルがそもそも無いときは？（初心者問題）
- スキルを発揮する時間・予算が無いときは？
- スキルを習得する時間・予算が無いときは？

開発環境整備で補えること

- ノウハウのポインタだけでも重要
  - 具体性？
- ノウハウがライブラリ化してるともっと使える
- フレームワーク化してるとさらに使える？
- チェッカー？

マイクロソフト社のこころみ

- **開発者向けセキュリティポータル**
  http://www.microsoft.com/japan/msdn/security/
- **Web Service Security（英文）**
  http://msdn.microsoft.com/practices/default.aspx?pull=/library/en-us/dnpag2/html/wssp.asp
- **Web アプリケーション セキュリティ強化: 脅威とその対策**
  http://www.microsoft.com/japan/msdn/security/guidance/secmod71.mspx

マイクロソフト社のこころみ･続

- **開発者向け セキュリティ オンライン セミナー**
  http://www.microsoft.com/japan/msdn/security/seminars/
- **Microsoft Anti-Cross Site Scripting Library V1.0**
  http://www.microsoft.com/downloads/details.aspx?FamilyID=9A2B9C92-7AD9-496C-9A89-AF08DE2E5982&displaylang=en
- **関連情報＝**
  - http://japan.zdnet.com/news/devsys/story/0,2000052522,20092501,00.htm

オープンソース関連では？

- **フレームワーク、ライブラリ、ドキュメントもあまり無いらしい･･･**
- **マンチェスター大学のこころみ**
  http://www.sve.man.ac.uk/Research/AtoZ/ILCT (SOAP**ベース**)
- **藤原さん@**WASF**のフレームワーク**Falcon**くらい？** (JAVA**ベース**)

開発方法論その他

- **PQL(Program Query Language)**
  http://suif.stanford.edu/papers/oopsla05pql.pdf
- **Securing Web Application Code by Static Analysis and Runtime Protection**
  http://www2004.org/proceedings/docs/1p40.pdf
- **Verifying Web Applications Using Bounded Model Checking**
  http://www.uweb.ucsb.edu/~yuf/paper/DSN04.pdf

商用などでは

- **SecureBlocker(R)**
  http://www.nttdata.co.jp/services/s090295.html
  - SecureBlocker**は入力パラメータを検査し、(可能なものは)自動的に無害化してくれる**Java**クラスライブラリです。 (説明文より)**
- **その他いくつかあるようですが、**.NET**ベースとかが多いようです**

参考：ソースコードチェッカー

- **Pixy (the open source prototype implementation of our concepts, is targeted at detecting cross-site scripting vulnerabilities in PHP scripts.)**
  http://www.seclab.tuwien.ac.at/papers/pixy.pdf
- **Source Code Analysis Tools**
  https://buildsecurityin.us-cert.gov/portal/article/tools/code_analysis/overview.xml
  - **参考**：https://buildsecurityin.us-cert.gov/portal/article/bestpractices/code_analysis/overview.xml

Webアプリソースのチェッカー？

- **入出力時のデータ要件の定義とトレース→コンパイラか？**
- **セッション管理の妥当性チェックはツール化困難？**
- **外部仕様によるツールチェックの限界**

ライブラリ化による機能強化？

- **入出力の直接攻撃の回避は可能**
- **セッション管理は難しいか？**

スキャナ

- AppScan (**テクマトリックス**)
- ScanDO (**ディアイティ**)
- WebInspect (**住商情報システム**)
- AppDetective (LAC、ID**ネットワーク**)
- SQL GUARD (AIR)
- Web Vulnerability Scanner
  http://www.acunetix.com/websitesecurity/web-site-security.htm
- nikto
  http://www.cirt.net/code/nikto.shtml
- wikto
  http://www.sensepost.com/research/wikto/

周辺ツール

- Watchfire Powertools
  http://www.watchfire.com/securityzone/product/powertools.aspx
  - HTTP Proxy、Connection Test、HTTP Request Editor、Expression Test、Encode/Decode
  - .NET Framework
- WebProbe (**高木さん謹製**)
  http://www.softek.co.jp/Sec/WebProbe/

修正予算調達のために

- **セキュア要求仕様ガイドライン「Webシステムセキュリティ要求仕様」**
  http://www.jnsa.org/active/houkoku/web_system.pdf

対策用参考文献

- http://www.webappsec.org/whitepapers.shtml**経由、Stopping Automated Attack Tools**
  http://www.ngssoftware.com/papers/StoppingAutomatedAttackTools.pdf
- **Automatically Hardening Web Applications Using Precise Tainting**
  http://www.cs.virginia.edu/~an7s/publications/sec2005.pdf

まとめ

- **普通にセキュリティに関心がない環境でも使える、目に触れるものが少なすぎるのでは？**
- **普通のプログラマにとって、安全なセッション管理は難しすぎるのでは？**
  - **動作系、実行系だけに頼っていていいのか？**