ratproxyで
Webアプリケーションの
安全確認

2009/4/11
FM-Tokyoライトニングトーク発表資料

松尾 篤（株式会社エミック）

株式会社エミック

Webアプリケーション開発者にとって
セキュリティ対策は必須課題

「安全なウェブサイトの作りかた」

を読んだ上で開発しているときに発生するひとつの疑問

疑問

- Webアプリケーションの安全性をチェックできる手段はないのか？

例えばどのようなもの

- Webブラウザーからのリクエストと Webアプリケーションからのレスポンスの内容を確認してくれるもの
- 手元（クライアント側）で確認できるもの
- 導入コストを抑えられるもの

ratproxy

- Webアプリケーション脆弱性検知ツール
- Proxyサーバーとして動作
- Googleがオープンソースとして公開
- Apache License 2.0

ratproxy

- XSSやXSRF、文字コードに関する問題などを検出可能
- レポートを出力して結果を確認できる
- Mac OS X、Windows（Cygwin）、Linux、FreeBSDで動作

効果的に使うには

- ratproxyは手軽なチェックに使えるが万能ではない
- Selenium IDEなどのツールを併用することでより効果的なチェックが可能
- 適切にチェックできるテストケースも考える必要がある

参考

- http://code.google.com/p/ratproxy/
- http://journal.mycom.co.jp/articles/2008/07/17/ratproxy/