大学共同利用機関法人 情報・システム研究機構
国立情報学研究所
National Institute of Informatics

トップエスイー ソフトウェア開発実践演習

セキュアプログラミング実践

NECソリューションイノベータ株式会社 小松佑樹
株式会社エヌ・ティ・ティ・データ 武田晃
キヤノン株式会社 堤忠臣
株式会社NTTデータ・アイ 新田海馬

開発における問題点

- セキュアプログラミング（脆弱性を作り込まない設計・実装）は，つながるサービスには必須になっている
- 設計・コードレビュー，静的解析，脆弱性診断等，基本的なセキュアプログラミングによって開発したソフトウェアにおいても脆弱性はなくならない．想定外のデータ入力による不正動作

手法・ツールの適用による解決

【ファジング】
予測できない入力データを与えて，バグや脆弱性を検出する手法（ブラックボックス，グレーボックス，ホワイトボックス）
【静的解析】
ソフトウェアを実際に動作させることなく解析する手法

取り組み内容

調査 → 適用 → 解析 → 整理

既知の脆弱性調査	手法・ツールを脆弱性に適用	手法・ツールの特徴，検出した脆弱性の解析	社内展開の課題を把握

既知の脆弱性調査

- Lighttpd のサービス拒否の脆弱性(CVE-2012-5533)
- Apache HTTP Serverのパストラバーサルの脆弱性（CVE-2021-41773）
- Apache HTTP Serverのサービス拒否の脆弱性(CVE-2021-41524)

手法・ツールを脆弱性のあるソフトウェアに適用

【ブラックボックス】
- booFuzz
- GitLab Protocol Fuzzer CE
- OWASP ZAP
- Wfuzz
- API Fuzzer

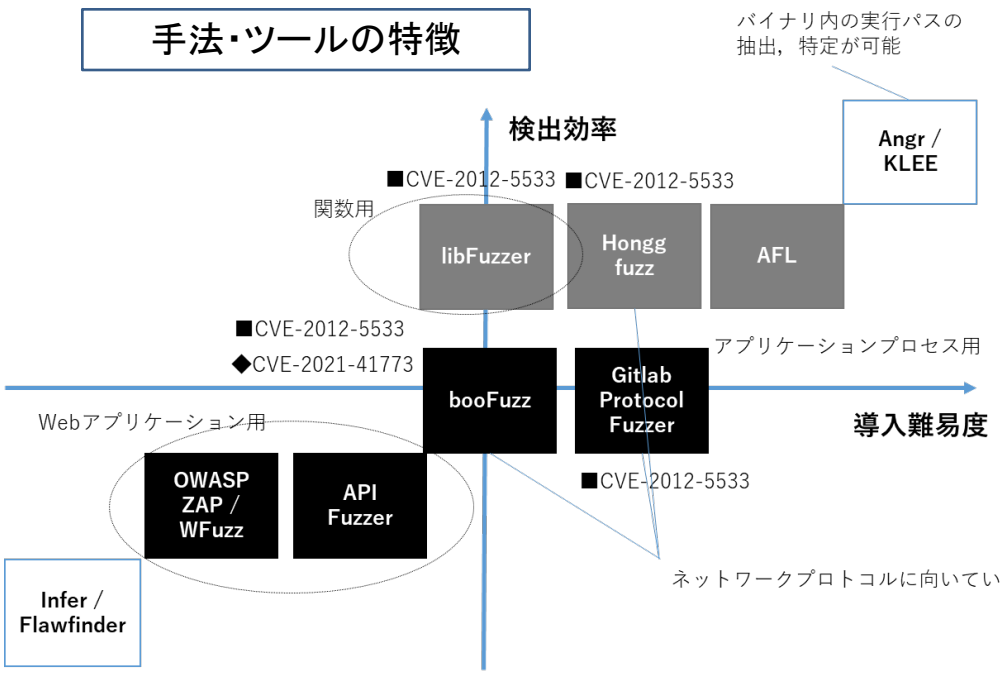
【グレーボックス】
- AFL
- LibFuzzer
- HonggFuzz

【ホワイトボックス】
- Angr
- KLEE

【静的解析】
- Infer
- Flawfinder

適用 → Apache HTTP Server, lighttpd

手法・ツールの特徴



■CVE-2012-5533
→ Connectionヘッダに不正な文字列「, , 」を含む場合に不正動作する

社内展開の例

組織	開発部門		評価部門
工程	実装	テスト	テスト
手法	静的解析	グレーボックス	ブラックボックス
		ホワイトボックス	

今後の展望

- ホワイトボックスファジングのより簡便な利用方法の模索
- 各種ファジングについて導入するための指南書の作成
- 検出できなかった脆弱性の原因について，ツールの性能なのか環境の問題なのかの切り分けが必要