

開発者の行動を観察することで、彼らがSecurity Bug発見ツールにどのような情報を求めているかを分析.

Questions Developers Ask While Diagnosing Potential Security Vulnerabilities with Static Analysis

著者紹介

Justin Smith

Brittany Johnson

Emerson Murphy-Hill

Bill Chu

Heather Richter Lipford



背景

- ▷ FSB (Find Security Bug) の遍満
 - 現在50以上！
- ▷ 統計解析ソフトが開発者に浸透しない問題
 - 開発者の興味に一致していない
 - どのようなニーズに応えるかを示していない

FSBの例

```
34 private List<String> parseAndCache(String fileName)
35     throws FileNotFoundException, IOException {
36     List<String> queries = parseSQLFile(fileName);
37     cache.put(fileName, queries);
38     return queries;
39 }
40 private List<String> parseSQLFile(String filepath)
41     throws FileNotFoundException, IOException {
42     List<String> queries = new ArrayList<String>();
43     BufferedReader reader =
44         new BufferedReader(new FileReader(new File(filepath)));
```



 Bug Info 

SQLFileCache.java: 44

 Navigation

Bug: An instance of java.io.File is created to read a file.

A file is open to read its content. The path given is a **dynamic** parameter.



統計解析ソフトの浸透のため、
開発者が脆弱性について、
どのような情報を
欲しているかを調べる。

ケーススタディ

被験者にFSBを使った
グループワークをしてもらう



アンケート調査



結果の分析

被験者

Participant	Job Title	Vulnerability Familiarity	Experience Years
P1*	Student	●●●○○○	4.5
P2*	Test Engineer	●●●○○○	8
P3	Development Tester	●●○○○○	6
P4*	Software Developer	●●○○○○	6
P5*	Student	●●●●○○	10
P6	Student	●○○○○○	4
P7	Software Developer	●●●●○○	4.5
P8	Student	●●●○○○	7
P9	Software Consultant	●●●○○○	5
P10	Student	●●●○○○	8

質問の抽出

P: 18:11 So I want know where this is being used. Is it being passed to an SQL query or one of these kinds of things? Okay, so now it's creating a form that it's going to ... I forget what forms are used for... I'm clicking on this to select all the instances of form so I can figure out where down here it's being used. Now it's in addRecordsRelease, so I think that is going to become a database call at some point.

Comment [J1]: Where are these variables being used?

Comment [BJ2]: Where is this value/variable being used?

Comment [J3]: Is this variable being passed to a SQL query or anything else the bug warns me about?

Comment [BJ4]: What are forms used for?

Comment [J5]: Where is the form used later in this method?

Comment [BJ6]: Is it going to become a database call at some point?

先行研究の知見から、
被験者の発言を定量的に分析

1. 明白な回答
2. 段階的な回答
3. “I assume”や“I guess”というキーワード
4. 確信がない様子(Clearly)
5. 情報の不足を表現

結果

▷ Code and Application

- バグの位置の情報
「このコードはどこで使われてる？」
- 処理の流れと呼び出し
「どこでこのメソッドが呼ばれてる？」
- データの流れと蓄積
「この情報はどこに行く？」
- コードの背景と機能性
「このコードは何をしてる？」
- 文脈と文法
「この脆弱性の文脈は？」

結果

- ▷ Individuals
 - 開発計画と自省
「私は理解してる？」
 - 概念の理解
「この概念はなに？」

結果

- ▷ Problem Solving Support
 - 資源とドキュメント
「もっと情報をくれる？」
 - 脆弱性の酷さランキング
「この脆弱性はどれくらい深刻？」
 - 警告文
「この警告文は何を言ってるの？」

開発者が使いがちな 脆弱性に対する3つの戦略

1. メソッドチェーンからデータの流を追う
この脆弱性の元凶はどのメソッドにあるんだろう…
2. クラス名による推測
テスト用のメソッドで出た脆弱性はユーザーに直面していないだろう…
3. 対処は参加者の知識に依存してる
この辺りが怪しいな…

開発者が行う対処の3つの側面

1. 良い対処法をなおざりにした対処
ツールに有用な情報が出ているのに、とりあえずググる…
2. 対処法を実行するツールの不使用
選択した対処法を実行するツールがあるのに、それを使わない…
3. 進捗管理を自分でする
研究者は開発者の**記憶による曖昧な進捗管理**に警鈴を鳴らしている…

まとめ

- ▷ 開発者が脆弱性に対処するときの行動を明白にした
- ▷ 今後のFSB開発は本論の視点を活用して、開発者のニーズに合わせた開発が必要

所感

- ▷ FSBの利用者側にも問題がある
- ▷ ソフトウェア開発は本当にツールで管理できるのか疑問

Thanks!

Any questions?