

Improving Vulnerability Inspection Efficiency Using Active Learning

Zhe Yu, Christopher Theisen, Laurie Williams, *Fellow, IEEE*, and Tim Menzies, *Senior Member, IEEE*

Abstract—Society needs more secure software. But the subject matter experts in software security are in short supply. Hence, development teams are motivated to make the most of their limited time. The goal of this paper is to improve software vulnerability inspection efficiency via an active learning based inspection support tool HARMLESS. HARMLESS incrementally updates its vulnerability prediction model (VPM) based on latest human inspection results and then applies the model to prioritize human inspection efforts to source code files that are more likely to contain vulnerabilities. HARMLESS is designed to have three advantages over conventional software vulnerability prediction methods. Firstly, by integrating human and vulnerability prediction model in an active learning environment, HARMLESS keeps refining its VPM and can find vulnerabilities with reduced human inspection effort before a software's first release. Secondly, by estimating the total number of vulnerabilities in a software project, HARMLESS guides human to stop the inspection at a target recall (percentage of vulnerabilities found). Thirdly, HARMLESS applies redundant inspection (source code files inspected multiple times by different humans) on source code files that are more likely to contain missing vulnerabilities, so that vulnerabilities missed by human inspectors can be retrieved efficiently. We evaluate HARMLESS via a simulation with Mozilla Firefox vulnerability data. Our results demonstrate that (1) HARMLESS finds 60, 70, 80, 90, 95, 99% vulnerabilities by inspecting 6, 8, 10, 16, 20, 34% source code files, respectively. (2) During the simulation, when targeting at 90, 95, 99% recall, HARMLESS could stop early at 23, 30, 47% source code files inspected, respectively. (3) Even when human reviewers fail to identify half of the vulnerabilities (50% false negative rate), HARMLESS is able to cover 96% of the missing vulnerabilities by redundantly inspecting half of the classified files.

Index Terms—Active learning, security, vulnerabilities, prediction models, software engineering, error correction.

1 INTRODUCTION

Software security is a current and urgent issue. A recent report [1] from the US National Institute of Standards and Technology (NIST) warns that “current systems perform increasingly vital tasks and are widely known to possess *vulnerabilities*”. The vulnerabilities discussed in this paper are defined as follows:

- A mistake in software that can be directly used by a hacker to gain access to a system or network; or
- A mistake that lets attackers violate a security policy [2].

Government and scientific bodies stress the need for reducing software vulnerabilities. In a report to the White House Office of Science and Technology Policy, “Dramatically Reducing Software Vulnerabilities” [1], NIST encourages more research on approaches to reducing security vulnerabilities. The need to reduce vulnerabilities is also emphasized in the 2016 US Federal Cybersecurity Research and Development Strategic Plan [3].

To best protect a software from its vulnerabilities, it is vital to reveal and fix those vulnerabilities before that software is deployed. Code inspection is the key process for finding vulnerabilities before deployment. However, it requires software engineers to inspect large amount of code and such inspection is a lengthy and tedious process (e.g. check that no call to the “C” printf function can be supplied a format string that is mismatched to the type of the items being printed).

Resource limitations often preclude software engineers to inspect all source code files [4]. Making informed decisions on what source code files to inspect can improve a team’s ability to find and fix vulnerabilities. Vulnerability prediction models (VPMs) make such informed decisions by learning a supervised machine learning model from known vulnerabilities. The VPM is then applied to classify source code files as “vulnerable” or “non-vulnerable”. If software engineers only inspect the predicted “vulnerable” files, then human effort is reduced. That is, a good VPM finds *more* vulnerabilities by inspecting *less* code.

Although the state of the art VPMs have shown promising results on finding vulnerabilities with reduced human inspection effort [5], [6], [7], [8], [9], these approaches have limitations:

- Existing VPMs cannot work before a software’s first release when no labeled training data is available (cross project vulnerability prediction has been shown to perform worse than within project vulnerability prediction [10]).
- Existing VPMs do not allow users to choose what level of recall (percentage of vulnerabilities found) to reach, moreover, when software engineers finish inspecting the selected source code files, they do not know how many more vulnerabilities are buried in the rest “non-vulnerable” files.
- Human may inspect a file but fail to find vulnerabilities [11]. Redundant inspection (where files are inspected by many humans) is needed to cover such errors. Current VPM research does not discuss how to design cost-effective redundant inspections.

Our work addresses these problems using a novel active learning tool called HARMLESS. Using HARMLESS, engineers inspect some source code files while HARMLESS trains/updates a VPM based on the inspection results. Then HARMLESS applies the VPM to suggest which files should be inspected next. Through

• Z. Yu, L. Williams, and T. Menzies are with the Department of Computer Science, North Carolina State University, Raleigh, USA.
E-mail: {zyu9, lawilli3}@gmail.com, timm@ieee.org.

• C. Theisen is with Microsoft Research, Seattle, USA.
E-mail: theisen.cr@gmail.com

iterating this process, HARMLESS guides the human inspection efforts towards source code files that are more likely to contain vulnerabilities.

The key idea behind HARMLESS is active learning—a machine learning algorithm can train faster (i.e. using less data) if it is allowed to choose the data from which it learns [12]. The experience in other domains is that such *active learners* can significantly reduce the amount of effort required to achieve high recall [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24]. To understand active learning, consider the decision plane between the vulnerable and non-vulnerable source code files of Figure 1. Suppose we want to find more vulnerable files and we had access to the Figure 1 model. One tactic for quickly finding those vulnerable files would be to inspect unclassified files that fall into the red region of this figure, as far as possible from the green ones (this tactic is called *certainty sampling*). Another tactic would be to verify the position of the boundary; i.e. inspect unclassified files that are closest to the boundary (this tactic is called *uncertainty sampling*). HARMLESS initially uses uncertainty sampling to fast build a reliable model, then switches to certainty sampling to greedily find vulnerable files. This strategy significantly reduces the effort required to find some desired level of high recall of software vulnerabilities.

To test the effectiveness of HARMLESS, we simulate code inspections on C and C++ files from Mozilla Firefox project. The authors tagged the known vulnerabilities of the Mozilla Firefox project from existing bug reports up to November 21st, 2017. Among the 28,750 unique source code files, 271 files contain vulnerabilities. These known vulnerabilities from bug reports are treated as ground truth. During our simulation, when a human is asked to inspect a source code file and tell whether it has vulnerabilities or not, the ground truth is applied instead of a real code inspection. This enables our experiments to be repeated multiple times with different algorithm setups and provides reproducibility of this paper. For full details on that data, see §4.

Using this data, we explore four research questions:

RQ1: How much human inspection effort can be saved by applying HARMLESS to find a certain percentage of vulnerabilities? Simulated on the Mozilla Firefox data without prior known vulnerabilities as training data, we show that 60, 70, 80, 90, 95, 99% of the known vulnerabilities can be found by inspecting around 6, 8, 10, 16, 20, 34% of the source code files, respectively. This result assumes humans are infallible; i.e. they make no mistakes in their inspections (see RQ3,RQ4 for what happens when humans become fallible).

RQ2: When can we stop inspecting the code with a confidence that a predetermined percentage of vulnerabilities have been found?

We show that the total number of vulnerabilities in a project can be accurately estimated by HARMLESS during the process, thus providing information to stop the inspection when a predetermined percentage of vulnerabilities has been reached based upon the security risk of the product.

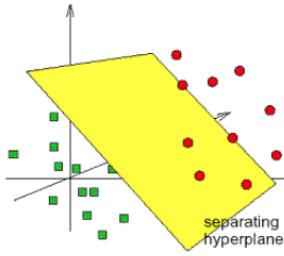


Fig. 1: Separating vulnerable (red) from non-vulnerable (green) files.

RQ3: How do human errors affect HARMLESS’s performance? Hatton [11] reports that when thoroughly inspecting codes for defects, human can miss 47% of the defects (47% false negative rate and 0% false positive rate). By adding in 10 to 50% false negative rate in human oracles randomly, we simulate the influence of growing human errors on HARMLESS’s performance. Such errors drastically and negatively impact our predictions— a result that motivates the next research question.

RQ4: Can HARMLESS correct human errors effectively?

As seen in §5.4, HARMLESS outperforms state of the art error correction mechanisms by redundantly inspecting only 50% of the classified files but covering 96% of the missing vulnerabilities.

1.1 Novel Contributions of this Paper

In summary, the contributions of this paper are:

- 1) HARMLESS, a novel and effective active learning strategy for finding vulnerabilities with reduced human inspection effort.
- 2) A demonstration that HARMLESS can find most vulnerabilities with a small portion of the codebase being inspected, before a software’s first release.
- 3) A comparison of using four types of features in HARMLESS—software metrics; text mining features; crash features; and hybrid features combining crash features and text mining features in active learning-based vulnerability predictions.
- 4) An estimator that can be applied along with the execution of HARMLESS to estimate the remaining number of vulnerabilities in the system. This estimator can be used to provide guidance to stop the security review at a desired percentage of vulnerabilities found.
- 5) An error correction mechanism that detects vulnerabilities that humans missed without imposing excessive extra human inspection effort.

1.2 Structure of this Paper

The rest of this paper is structured as follows. Some background and related work are discussed in §2. §3 describes our methodology. This is followed by the details on how to simulate the HARMLESS inspection process on Mozilla Firefox vulnerability dataset in §4. §5 describes our experiment designs while §6 answers the research questions with the experiment results. Threats to validity are analyzed in §7 while conclusion and future work are provided in §8.

2 BACKGROUND AND RELATED WORK

2.1 Vulnerability Prediction

Previous work in vulnerability prediction has focused on statistical classifiers on source code artifacts, such as binaries, files, and functions. These approaches classify code artifacts as either vulnerable or not vulnerable, and use an oracle of historical vulnerabilities tied to these code artifacts to determine the accuracy of the classifiers in practice. Some of the vulnerability datasets include the following: the Windows operating system [7], [8], the Mozilla Firefox web browser [25], [9], and the RedHat Enterprise Linux Kernel [25].

Zimmermann *et al.* [7] reported a median recall of 20% when using all available source code metrics they collected to build a Random Forest [26] classifier. Shin *et al.* [27], [25], [6] focused on churn and complexity with a different set of software metrics and achieved a higher recall of 83%.

Scandariato *et al.* [5] applied text mining to predict security vulnerabilities. Their hypothesis was that specific tokens found in source code files may indicate whether this file is more prone to vulnerabilities; for example, the presence of “`nullptr`” might mean a specific source code file is more prone to vulnerabilities resulting from null references. In their case studies [5], a static code analysis tool was used to label code components as “vulnerable” or not. Such static code analysis tools have a notoriously large false positive rate and may incorrectly decide that many code components are “vulnerable”.

Walden *et al.* [10] compared software metric-based approaches for vulnerability prediction to text mining approaches and found that text mining performed better in terms of precision and recall than software metric approaches. Later in §5, we show the same result with HARMLESS. They also reported that cross-project prediction performances were generally poor—49%, 36% of the source code files need to be reviewed for finding 66%, 70% of the vulnerabilities, respectively. These results suggest that training data from the same project are required for these VPMs. As a result, it is not recommended to apply VPMs before a software’s first release since no training data from the same project is available.

Theisen *et al.* [28], [8], [29] investigated using crash features extracted from crash dump stack traces, which are collected after the software’s first release, to approximate the attack surface and predict which part of the software are more prone to be vulnerable. They found that crash history is a strong indicator of vulnerabilities—48.4% of the “crashed” binaries in Windows contain 94.6% of known vulnerabilities [8], and 15.8% of the “crashed” source code files in Mozilla Firefox contain 73.6% of known vulnerabilities [29]. The advantage of this approach is that it is unsupervised—does not require the labeling of training data. However, one major drawback of Theisen *et al.* approach is that higher recall cannot be achieved since no information is provided in those source code files without crash history.

We note that HARMLESS is not another VPM trying to replace the above ones, rather, HARMLESS is a code inspection framework which incorporates the state of the art VPMs in an active learning framework to provide advantages discussed in §1. As a result, in our case studies in §4 and §5, all these types of the above mentioned features (text mining features, software metrics, crash features) are extracted and compared in the active learning framework of HARMLESS.

2.2 Total Recall

The *total recall problem* aims to optimize the cost for achieving very high recall—as close as practicable to 100%—with a human assessor in the loop [30]. The total recall problem has been extensively explored in many domains, including electronic discovery and evidence-based medicine.

In electronic discovery, attorneys are hired to review massive amount of documents looking for relevant ones for a certain legal case and provide those as evidences. Cormack and Grossman [17] proposed continuous active learning to save attorneys’ effort from reviewing non-relevant documents, which further can save a large amount of the cost of legal cases. Cormack and Grossman [13], [14], [15], [16], [17], [18] designed and applied continues active learning to retrieve relevant documents to a legal case while minimizing the cost for attorneys reading the documents.

In evidence-based medicine, researchers screen titles and abstracts to determine whether one paper should be included in a

certain systematic review. Wallace et al. [19] designed patient active learning to help researchers prioritize their effort on papers to be included. With patient active learning, half of the screening effort can be saved while still including most relevant papers [19].

Previously [24], the authors combined the techniques from Cormack and Wallace’s work and created an active learning tool called FASTREAD to identify relevant papers for software engineering literature reviews while minimizing the number of candidate literature being reviewed by humans. It incrementally learns what papers are more likely to be “relevant” based on previous decisions from humans and then guides the humans to read those papers next. Furthermore, SEMI, an estimator for the total number of relevant papers and DISAGREE, a technique to efficiently correct human classification errors were developed for FASTREAD to better support humans retrieving relevant research papers [31].

The core problem of vulnerability prediction is how to find most vulnerabilities with least code inspected. This problem can also be generalized as the total recall problem. Therefore the authors conjecture that active learning can also be the key to better solve the vulnerability prediction problem. As a result, Techniques from existing total recall solutions [24], [31], [17], [19], [32] are applied and adapted to HARMLESS for vulnerability inspection as described later in §3.1.

3 HARMLESS

This section provides details on how HARMLESS supports manual code inspection. Similar as the total recall solutions in §2.2, HARMLESS incrementally updates its vulnerability prediction model (VPM) based on latest human inspection results and then applies the model to prioritize human inspection efforts to source code files that are more likely to contain vulnerabilities. Inside this human-VPM inspection loop, HARMLESS

- refines its model according to latest inspection results, which enables HARMLESS to work before a software’s first release (HARMLESS applies domain knowledge or random sampling to find the first “vulnerable” file before its training starts);
- estimates the number of remaining vulnerabilities during the process with a semi-supervised learning approach so that human inspectors could decide when the target recall has been reached and then stop the inspection;
- suggests redundant inspections on parts of the inspected files that (1) have only been inspected once, (2) were labeled as “non-vulnerable”, and (3) according to the latest VPM, has a high confidence of being “vulnerable”. In this way, HARMLESS corrects more human errors with less redundant inspection comparing to other state of the art error correction mechanisms.

The rest of this section introduces the specific techniques utilized by HARMLESS in §3.1 and presents HARMLESS framework in §3.2.

3.1 HARMLESS Operators

HARMLESS imports and adapts several operators which, in prior work on analogous problems (total recall), was seen to perform better than alternatives [24], [31]. This section offers an overview of the seven operators that are used in the HARMLESS which is presented in §2.2. The last two operators were created and used in prior work as discussed in §2.2.

Features are not restricted in HARMLESS. Any types of features extracted from the source code can be used to predict

for vulnerabilities in HARMLESS. That said, users could extract their own features, but here we present three example types of features which are popular in existing vulnerability researches.

- Software metrics: followed by the work of Shin *et al.* [25], SciTools' Understand¹ is used to measure the static features of software.
- Crash features: followed by the work of Theisen *et al.* [8], the crash features measure the number of time each source code file has crashed. Such information is extracted from the crash dump stack trace data.
- Text mining features: different from the work of Scandariato *et al.* [5], where labels (vulnerable or non-vulnerable) are required to select tokens, we apply the same text mining feature extraction as the total recall approaches [24], [31]. Specifically, we:
 - 1) Tokenized all source code files without stop/control words removal or stemming.
 - 2) Select a token dictionary with largest tf-idf score across all source code files. For term t in document d ,

$$Tfidf(t, d) = w_d^t \times (\log \frac{|D|}{\sum_{d \in D} sgn(w_d^t)} + 1)$$

where w_i^t is the term frequency of term t in document d . For term t ,

$$Tfidf(t) = \sum_{d \in D} Tfidf(t, d)$$

- 3) Built a term frequency matrix with N tokens selected—according to our prior work in FASTREAD [24], [31], we use $N = 4000$.
- 4) Normalized each row (feature vector for each file) with their L2-norm².

Support vector machines (SVMs) are a well-known and widely-used classification technique. The idea behind SVMs is to map input data to a high-dimension feature space and then construct a linear decision plane in that feature space [33]. Linear SVM [34] has been proved to be a useful model in SE text mining [35] and is applied in the state-of-the-art total recall methods [24], [32], [19], [17].

Aggressive undersampling is a data balancing technique first created by Wallace *et al.* [19]. During the training process, aggressive undersampling throws away majority (non-vulnerable) training examples closest to SVM decision plane until reaching the same number of minority (vulnerable) training examples.

Presumptive non-relevant examples is a technique created by Cormack and Grossman [16] to alleviate the sampling bias of non-relevant (non-vulnerable) training examples. Each time before training, *presumptive non-relevant examples* samples randomly from the unlabeled examples and presumes the sampled examples to be non-relevant (non-vulnerable) in training. The rationale behind this technique is that given the low prevalence of relevant (vulnerable) examples, it is likely that most of the presumed ones are non-relevant (non-vulnerable).

Query strategy is the key part of active learning. The two query strategies applied in this paper are: 1) **uncertainty sampling**, which picks the unlabeled examples that the active learner is most uncertain about (examples that are closest to the SVM decision hyperplane); and 2) **certainty sampling**, which picks the unlabeled examples that the active learner is most certain to be

vulnerable (examples on the vulnerable side of and are furthest to the SVM decision hyperplane). Different approaches endorse different query strategy, e.g. Wallace *et al.* [19] applies uncertainty sampling in their patient active learning. Cormack *et al.* [17], [32] use certainty sampling from beginning to the end. Followed by our previous design for literature review [31], HARMLESS applies uncertainty sampling in early stage and certainty sampling afterwards.

SEMI is a semi-supervised estimator we designed for reading research papers [31]. SEMI utilizes a recursive *TemporaryLabel* technique. Each time the SVM model is retrained, SEMI assigns temporary labels to unlabeled examples and builds a logistic regression model on the temporary labeled data. It then uses the obtained regression model to predict on the unlabeled data and updates the temporary labels. This process is iterated until convergence and the final temporary labels are used as an estimation of the total number of positive examples in the dataset.

DISAGREE is an error correction mechanism designed for correcting both false negatives and false positives [31]. Its core assumption is:

Human classification errors are more likely to be found where human and machine classifiers disagree most.

Since the error distribution of the code inspection process is different from that of selecting research papers, it cannot be directly applied to vulnerability prediction. As a result, we adopt the same assumption as **DISAGREE**, and designed **DISPUTE**, which focuses on correcting false negatives only.

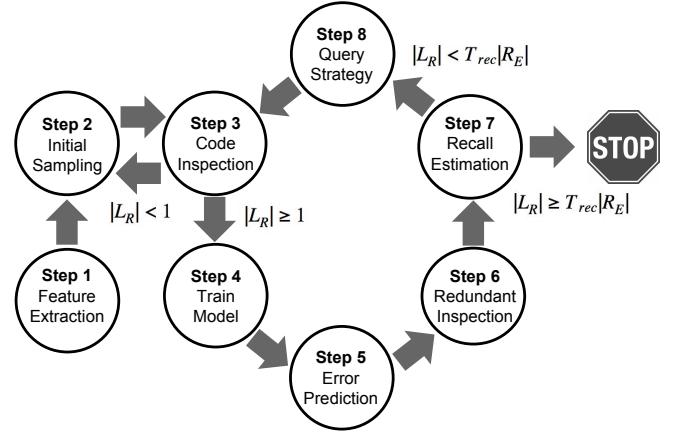


Fig. 2: Block Diagram of HARMLESS Framework

3.2 HARMLESS Framework

This section presents the HARMLESS framework in Figure 2, with the operators from §3.1 in bold.

Step 1 Feature Extraction: Given a set of source code files C , extract **features** from each source code file. Initialize the set of labeled files as $L \leftarrow \emptyset$ and the set of labeled target vulnerable files as $L_R \leftarrow \emptyset$.

Step 2 Initial Sampling: Sample without replacement N_1 unlabeled source code files from the codebase to generate a queue $Q \subset (C \setminus L)$ ³, (a) randomly, if not using crash

1. <http://www.scitools.com>

2. L2-norm for a vector x is $\sqrt{x^T x}$, where T denotes “transpose”

3. Let A and B be two sets. The set difference, denoted $A \setminus B$ consists of all elements of A except those which are also elements of B .

features; or (b) by descending order of the crash feature counts.

Step 3 Code Inspection: Each human is assigned one random source code file from the queue $x \in Q$; label it as “vulnerable” or “non-vulnerable” after performing the inspection. Add file x into the labeled set L ; if x is labeled “vulnerable” also add it into set L_R . The human is assigned another source code file until the queue is clear. Once the queue is cleared, proceed to **Step 4** to start training if at least one “vulnerable” file is found ($|L_R| \geq 1$), otherwise go back to **Step 2** to sample more.

Step 4 Train Model: Generate **presumptive non-relevant examples** to alleviate the sampling bias in “non-vulnerable” examples ($L \setminus L_R$). Apply **aggressive undersampling** to balance the training data. At last train a linear **support vector machine** (SVM) on the current labeled files L_R and L , using features extracted in **Step 1** to predict whether one file is vulnerable or not.

Step 5 Error Prediction (DISPUTE): Apply the SVM model trained in **Step 4** to predict on the source code files that have only been inspected once and are labeled as “non-vulnerable” ($L \setminus L_R$). Select N_2 files with highest prediction probability of being vulnerable and add the selected files into a queue for redundant inspections.

Step 6 Redundant Inspection: Each file in the queue from **Step 5** is assigned to different humans other than its original inspector for redundant inspection. Once the queue is cleared, proceed to **Step 7**.

Step 7 Recall Estimation: Estimate the total number of vulnerable files in the codebase $|R_E|$ with **SEMI** algorithm.

- **STOP** the inspection process and fix the vulnerabilities in L_R if $|L_R| \geq T_{rec}|R_E|$ (where T_{rec} represents the user target recall).
- Otherwise proceed to **Step 8**.

Step 8 Query Strategy: Apply the SVM model trained in **Step 4** to predict on unlabeled files ($C \setminus L$) and select top N files with vulnerability prediction probability closest to 0.5 (**uncertainty sampling**) if $|L_R| < N_3$ or 1.0 (**certainty sampling**) if $|L_R| \geq N_3$. Push the selected files into the queue Q , then go to **Step 3** for another round of inspection.

In the above, N_1, N_2, N_3 are engineering choices. N_1 is the batch size of the inspection process, larger batch size usually leads to fewer times of training but also worse overall performance. $N_2 = \alpha N_1$ where $\alpha \in [0, 1]$ reflects what percentage of the labeled files are redundantly inspected. Larger N_2 means more redundant inspection, which leads to more human false positives covered by also higher cost. N_3 is the threshold where the query strategy is switched from uncertainty sampling to certainty sampling. N_3 features the trade-off between faster building a better model and greedily applying the model to save inspection effort.

4 HARMLESS SIMULATION

While §3 shows how HARMLESS should be applied in practice, with humans inspecting codes, it is too expensive to experiment with humans to test different feature types and answer all the research questions. As a result, we show how HARMLESS is simulated on the Mozilla Firefox vulnerability dataset in this section.

4.1 Dataset

The Mozilla Firefox dataset focuses on C and C++ files in Mozilla Firefox. Metrics were collected for 28,750 unique source code files in the project, within which 271 vulnerabilities are manually labeled as the ground truth. These ground truth vulnerabilities are collected from Mozilla Foundation Security Advisories blog [36] and bug reports from Bugzilla⁴. The two raters individually classify each bug report into 21 types of vulnerabilities or “not a vulnerability”. After classifying each bug report, the raters then convene and resolve any differences that have occurred between the two. In the event that the two raters cannot come to a consensus, a third party arbitrator may be used to resolve the conflict.

Following the Common Weakness Enumeration (CWE) set of most commonly seen weaknesses in software⁵, the Mozilla Firefox dataset contains 14 different types of vulnerabilities and some files are associated with multiple types of vulnerabilities. To simulate security reviews targeting at specific types of vulnerabilities, we group the vulnerabilities into five categories to ensure that each category contains enough data (#Vulnerable Files) for a simulation, as shown in Table 1. In the following sections §5 and §6, we show results on simulations targeting each category of the vulnerability types. For example, when targeting at “Protection Mechanism Failure”, only the 119 files associated with this category are considered as vulnerable.

Here we briefly describe the three types of features extracted from the Mozilla Firefox vulnerability dataset and used in our simulations.

4.1.1 Software Metrics

SciTools’ Understand⁶ is used to measure the metrics from the Mozilla Firefox source code files. The list of the software metrics provided by the dataset is shown below:

- *CountClassBase* - The number of subclasses in the source code file.
- *CountClassCoupled* - The coupling of the classes in the source code file.
- *CountClassDerived* - The number of subclasses derived from classes originating in this source code file.
- *CountDeclInstanceVariablePrivate* - The number of private variables declared in this source code file.
- *CountDeclMethod* - The number of methods declared in this source code file.
- *CountInput* - The number of external calls made to this source code file.
- *CountOutput* - The number of external calls made from this source code file.
- *Cyclomatic* - The Cyclomatic Complexity of this source code file.
- *CountLine* - The number of lines of code (excluding comments and whitespace) in this source code file.
- *MaxInheritanceTree* - The size of the maximum leaf in the inheritance tree leading from this source code file.

Some metrics in Shin *et al.* [25] are not covered mainly due to the following reasons: (1) metrics that no public tool (to our knowledge) provides an equivalent to, e.g. incoming closure and outgoing closure; (2) metrics that do not apply to the Mozilla

4. <https://bugzilla.mozilla.org/>

5. <http://cwe.mitre.org/data/definitions/1003.html>

6. <http://www.scitools.com>

TABLE 1: Descriptive statistics for vulnerabilities types grouping

Vulnerability Type	#Vulnerable Files	Containing Types
Protection Mechanism Failure	119	protection mechanism failure.
Resource Management Errors	85	uncontrolled resource consumption, improper resource shutdown or release, resource management errors, use after free, resource leak.
Data Processing Errors	35	data processing errors.
Code Quality	29	code quality.
Other	32	race conditions, configuration, environment, traversal, link-following, other.
All	271	All 14 types of vulnerabilities.

Firefox project, e.g. organization intersection factor; (3) metrics that are identical to some already covered ones in Mozilla Firefox project, e.g. edit frequency.

4.1.2 Text Mining

As described in §3.1, text mining features are extracted by tokenizing the source code files, selecting top 4000 tokens based on tf-idf score, and then applying L2 normalization on files.

4.1.3 Crash Features

Crash dump stack trace data was collected from Mozilla Crash Reports⁷. We collected crashes from January 2017 to November 2017, with a total of 1,141,519 crashes collected. For each individual crash, the field marked “crashing thread” is observed and each file that appeared in the thread is added to the dataset. We also kept track of how many times a file was observed in different crashes since files crash more often have higher chance to contain vulnerabilities.

4.2 Simulation on Mozilla Firefox Dataset

Code inspection with HARMLESS, as described in §3.2, is simulated on the Mozilla Firefox dataset with the following settings:

Step 1 Feature Extraction: C is the set of all 28,750 source code files, R is the set of source code files containing the target type of vulnerabilities shown in Table 1, $L \leftarrow \emptyset$ is the set of labeled files, and $L_R \leftarrow \emptyset$ is the set of labeled target vulnerable files. Extract **features** from each source code file in C .

Step 2 Initial Sampling: The batch size is chosen as $N_1 = 100$. We use $N_1 = 100$ during our simulations for faster experiments. However it is suggested to use a smaller batch size, e.g. $N = 10$, in practice since the cost of training a model more often is usually much less than the cost of inspecting more code.

Step 3 Code Inspection: Rather than asking a human expert to inspect source code files, as specified in §3.2, the ground truth labels from Mozilla Firefox dataset are applied to simulate the inspection. Each vulnerable file $x \in Q \cap R$ has E_R chance of being wrongly labeled as “non-vulnerable” and $1 - E_R$ chance of being correctly labeled as “vulnerable”. Every non-vulnerable file $x \in Q \setminus R$ will be labeled as “non-vulnerable”. Here $E_R = 0, 10, 20, 30, 40, 50\%$ simulates the probability of a human expert missing the vulnerabilities (false negative rate).

Step 5 Error Prediction (DISPUTE): Half of the inspected files are selected for redundant inspection ($N_2 = 0.5N_1$) based on DISPUTE principle. We show later in §6 that by redundantly inspecting half of the labeled files, most (96%) of the human false negatives can be covered.

Step 8 Query Strategy: Uncertainty sampling if $|L_R| < N_3 = 10$ or certainty sampling when $|L_R| \geq N_3 = 10$.

7. <https://crash-stats.mozilla.com/home/product/Firefox>

5 EXPERIMENTS

This section describes experiments that assess HARMLESS’s performance. All the following experiments are simulated on the Mozilla Firefox case study, as described in §4 and are used to answer the research questions listed in §1.

5.1 Performance Metrics

Same as the task of total recall problems in §2.2, HARMLESS’s task is to optimize the inspection effort for achieving very high recall. Therefore HARMLESS focuses on recall rather than precision and its performance is evaluated by the cost for achieving certain recall.

$$\text{recall} = \frac{\# \text{ of vulnerable files found}}{\# \text{ of vulnerable files exist}} = \frac{|L_R|}{|R|}. \quad (1)$$

$$\text{cost} = \frac{\# \text{ of source code files reviewed}}{\# \text{ of source code files exist}} = \frac{|L|}{|C|}. \quad (2)$$

Where the numerator of cost in (2) counts the number of times the source code files being reviewed, i.e. it still increases when the same file is reviewed for a second time by a different reviewer. Using these two metrics, one treatment is considered better than another if it reaches the same target recall with lower cost.

Besides recall and cost, we use the Estimation vs Cost curve to assess the accuracy of SEMI for estimating the total number of vulnerable files in **Step 7**, here

$$\text{estimation} = \frac{\# \text{ of vulnerable files estimated}}{\# \text{ of vulnerable files exist}} = \frac{|R_E|}{|R|}. \quad (3)$$

The sooner this estimation converges to 1.0, the better the estimator is. As described in **Step 7**, the inspection process will stop when

$$|L_R| \geq T_{rec}|R_E|,$$

where T_{rec} represents the target recall. The closer the inspection stops to the target recall, the better the stopping rule.

5.2 Experiment for Vulnerability Inspection Efficiency

The first experiment focuses on **RQ1**. To test the vulnerability inspection efficiency, only the recall-cost curve is important, therefore, stopping rule and human errors are not considered, i.e. in §3.2, human error rate E_R in **Step 3** is set to be 0, **Step 5** and **Step 6** are disabled, and in **Step 7**, real recall is used for the stopping rule $|R_E| = |R|$. The following approaches with different feature types are compared in order to choose the best feature type for HARMLESS and to demonstrate the effectiveness of active learning in HARMLESS,

- **Metrics:** active learning approach, as described in **Step 4** and **Step 8**, trained on file level software metrics features (described in §4.1.1) which quantifies different types of software complexity and are collected from the source code.

- **Text:** active learning approach trained on file level text mining features (described in §4.1.2) which treats the source code as raw text and performs standard text mining feature extraction (term frequency with L2 normalization [24]) on it.
- **Crash:** no model is trained and source code files are selected in descending order of the number of times they crashed [28] (described in §4.1.3).
- **Hybrid:** combination of text mining features and crash features. This model is built by adding one column (number of times the source code file has crashed) to the term frequency matrix of the text mining features set before normalization. In **Step 2**, crash counts are applied as domain knowledge to first sample files which have crashed most frequently.
- **Random:** source code files are inspected in random order. This treatment serves as a baseline where code inspection is performed without any help from HARMLESS.

5.3 Experiment for Stopping Rule

The second experiment focuses on **RQ2**. Human errors are not considered in this experiment, therefore in §3.2, human error rate E_R in **Step 3** is set to be 0, and **Step 5** and **Step 6** are disabled. In **Step 8**, the SEMI estimator, described in §3.1, is applied to estimate the number of vulnerabilities when running HARMLESS with the best feature set picked from **RQ1**. The estimation from SEMI is then used as an indicator of whether the target recall has been reached and thus the review can be safely stopped. This experiment is designed to show how accurate the SEMI estimator can be and how close the review can stop at the target recall.

5.4 Experiment for Human Errors

The third experiment focuses on human errors: **RQ3** and **RQ4**. In this experiment, we adopt the human error model from Hatton [11]:

- False negative rate: each “vulnerable” file has up to 47% chance of being mislabeled as “non-vulnerable,” and every reviewer has the same false negative rate.
- No false positives: “non-vulnerable” files can never be mislabeled as “vulnerable” by a human reviewer.

In our simulations, with human errors introduced (false negative rate $E_R = 0, 10, 20, 30, 40, 50\%$), the following error correction mechanisms are compared:

- **None:** No error correction. This result is used to demonstrate how vulnerability prediction performance is affected by human errors.
- **Two-person** [11]: This is the standard error correction method applied in code inspection. For simplicity reason, we use Two-person as the abbreviation of two-person team in the rest of this paper. In **Step 3** of §3.2, if one file is labeled as “non-vulnerable” and has been reviewed by only one reviewer, it goes back into the queue (with its previous reviewer id) to wait for a different reviewer to recheck it.
- **Cormack’17** [13]: This is an advanced error correction method for citation screening. We reproduce half of Cormack’17 to correct false negatives only and incorporate it into the distributed framework: In **Step 8**, Cormack’17 utilizes a different stopping rule. This method detects the inflection point⁸ i of the current

⁸ The inflection point is the elbow of the recall curve, which features the longest distance to the straight line between the start point and end point of the recall curve [14].

recall curve, and compare the slopes before and after i . If $slope_{<i}/slope_{>i}$ is greater than a specific threshold $\rho = 6$, the review should be stopped. For details about this stopping rule, please refer to Cormack and Grossman [14]. After the stopping rule is satisfied in **Step 8**, send all files reviewed before the inflection point i and labeled as “non-vulnerable” to the queue. The security review and test stops after all the files in the queue have been reviewed by a different reviewer.

- **DISPUTE:** As described in §3.2, every iteration, $M = 0.5N$ of the labeled “non-vulnerable” files are selected based on how much the active learner disagrees with their current labels. It then pushes the selected files back into the queue and ask a different human expert for inspection. In simulations, this second inspection has the same false negative rate E_R .
- **DISPUTE(3):** Similar as DISPUTE but selected files are inspected by *two* humans (so “vulnerable” files are less likely to be missed again albeit doubling the redundant inspection cost).

6 RESULTS

In this section, we utilize the results from the designed experiments in §5 to answer our research questions.

RQ1: How much human inspection effort can be saved by applying HARMLESS to find a certain percentage of vulnerabilities? Table 2 shows the cost to reach different levels of recall. One method is considered better than another if it costs less to reach the same recall. Based on these results, we make the following observations:

- HARMLESS with active learning (Metrics, Text, Hybrid) is better than **Random**, indicating the effectiveness of the proposed active learning framework in HARMLESS.
- **Crash** performs well in early stages (when recall < 80%) but is unable to achieve certain target recall values (see the numerous “n/a” entries of Table 2). For vulnerabilities of type “Code Quality”, **Crash** performs better than any other approaches.
- Targeting at different types of vulnerabilities does not affect much of the performance of HARMLESS with active learning (Metrics, Text, Hybrid).

Therefore active learning based HARMLESS approach is recommended to reliably achieve high recall with low cost. Among the active learning based approaches:

- **Metrics** performs the worst—always cost more to reach same recall. Therefore we do not recommend using static software metrics as features to predict vulnerabilities in HARMLESS.
- When crash features are unavailable, e.g. before a software’s first release, **Text** performs the best.
- When crash features are available, **Hybrid** utilizes both **Text** and **Crash** and performs slightly better than **Text** in terms of median performances and greatly reduces the variance.

Summing up this work on **RQ1**, we say:

 **How much human inspection effort can be saved by applying HARMLESS to find a certain percentage of vulnerabilities?**

Before a software’s first release and targeting at any type of vulnerabilities, HARMLESS with text mining features is able to find 60, 70, 80, 90, 95, 99% of the target vulnerabilities by inspecting only 6, 8, 10, 16, 20, 34% of the source code files, respectively. If available, crash features can further boost the inspection efficiency when applied to guide the inspection order in the early stage.

	Vulnerability Type	Target recall							
		60	70	80	85	90	95	99	100
Metrics	Protection Mechanism Failure	50 (7)	56 (6)	60 (8)	63 (8)	67 (8)	79 (7)	94 (3)	99 (2)
	Resource Management Errors	49 (25)	57 (15)	63 (13)	67 (12)	71 (10)	75 (9)	99 (0)	99 (0)
	Data Processing Errors	35 (4)	41 (8)	45 (9)	61 (23)	70 (24)	78 (9)	82 (5)	82 (5)
	Code Quality	38 (6)	42 (20)	61 (19)	61 (18)	64 (12)	66 (9)	72 (3)	72 (3)
	Other	38(19)	45(17)	58(7)	60(6)	64(8)	70(10)	92(12)	92(12)
	All	49 (17)	53 (7)	60 (4)	63 (4)	66 (3)	72 (3)	94 (6)	99 (0)
	Median	42(18)	50(17)	59(12)	62(10)	67(8)	74(10)	91(15)	94(19)
Text	Protection Mechanism Failure	6 (1)	9 (2)	12 (1)	16 (1)	20 (3)	28 (3)	37 (9)	43 (7)
	Resource Management Errors	6 (1)	8 (2)	9 (1)	9 (2)	11 (3)	13 (2)	33 (4)	33 (4)
	Data Processing Errors	12 (4)	13 (2)	14 (4)	15 (4)	16 (4)	20 (4)	42 (15)	42 (15)
	Code Quality	4 (4)	5 (4)	8 (3)	10 (4)	19 (5)	21 (5)	30 (7)	30 (7)
	Other	5(3)	6(4)	11(5)	12(5)	14(4)	18(3)	33(2)	83(2)
	All	5 (0)	7 (0)	9 (1)	12 (1)	14 (1)	20 (2)	34 (2)	85 (0)
	Median	6(2)	8(3)	10(4)	13(4)	16(5)	20(7)	34(7)	43(49)
Crash	Protection Mechanism Failure	5 (0)	8 (0)	13 (0)	n/a	n/a	n/a	n/a	n/a
	Resource Management Errors	4 (0)	5 (0)	8 (0)	10 (0)	11 (0)	n/a	n/a	n/a
	Data Processing Errors	8 (0)	11 (0)	n/a	n/a	n/a	n/a	n/a	n/a
	Code Quality	1 (0)	2 (0)	4 (0)	4 (0)	10 (0)	11 (0)	12 (0)	12 (0)
	Other	6(0)	9(0)	12(0)	n/a	n/a	n/a	n/a	n/a
	All	5 (0)	8 (0)	11 (0)	14 (0)	n/a	n/a	n/a	n/a
	Median	5(1)	8(3)	11(4)	n/a	n/a	n/a	n/a	n/a
Hybrid	Protection Mechanism Failure	7 (0)	9 (0)	12 (0)	14 (0)	16 (1)	21 (3)	58 (1)	59 (1)
	Resource Management Errors	5 (0)	7 (0)	8 (0)	9 (0)	11 (0)	13 (2)	39 (0)	39 (0)
	Data Processing Errors	7 (0)	10 (0)	15 (0)	15 (0)	16 (0)	29 (2)	37 (3)	37 (3)
	Code Quality	3 (1)	4 (1)	4 (2)	5 (1)	10 (0)	12 (0)	16 (1)	16 (1)
	Other	4(0)	9(0)	11(0)	12(0)	14(0)	14(0)	37(9)	61(14)
	All	6 (0)	8 (0)	10 (0)	11 (0)	14 (0)	18 (2)	36 (0)	59 (0)
	Median	6(2)	8(1)	10(4)	12(5)	14(4)	17(7)	37(5)	41(22)
Random	Protection Mechanism Failure	59 (7)	70 (4)	80 (4)	85 (3)	90 (2)	95 (2)	98 (1)	99 (0)
	Resource Management Errors	59 (4)	69 (5)	77 (5)	84 (4)	88 (3)	94 (2)	99 (1)	99 (1)
	Data Processing Errors	57 (12)	70 (11)	78 (10)	84 (9)	86 (10)	94 (5)	97 (3)	97 (3)
	Code Quality	58 (8)	70 (10)	77 (11)	82 (8)	90 (9)	94 (6)	98 (2)	98 (2)
	Other	59(5)	67(5)	78(6)	83(5)	88(6)	93(5)	97(2)	97(2)
	All	59 (3)	69 (3)	79 (3)	84 (2)	89 (2)	94 (1)	98 (0)	99 (0)
	Median	59(6)	69(6)	79(5)	83(5)	89(4)	94(3)	98(1)	98(2)

TABLE 2: Cost (i.e. percent code reviewed) required to reach different levels of recall. Medians and IQRs (75th-25th percentile) are shown for 30 repeated simulations (IQR results are shown in brackets). **Crash** has many empty cells since it provides no information on vulnerabilities located in the files that have never crashed. In this table, *lower* median values are *better* so all the **Random** results are worse than anything else (as might be expected). Of the remaining results, **Text** and **Hybrid** perform better than **Metrics**. Important note: this table does not consider how to stop at the target recall, it only shows the cost when first reaching that recall. For experiments relating to stopping rules, see Table 3.

RQ2: When can we stop inspecting the code with a confidence that a predetermined percentage of vulnerabilities have been found? To answer this research question, we first show the accuracy of the estimation by presenting the Estimation vs Cost curve in Figure 3. In these plots, estimations, calculated as Equation (3), are considered accurate and useful if they converges to estimation=1.0 (denoted as the “true” line) early (when cost is small). According to Figure 3, the estimations from SEMI using either **Hybrid** or **Text** converges to 1.0 early on every target vulnerability types. Usually the estimation error become $\leq 5\%$ after cost ≥ 0.3 .

Then the results of using such estimation as stopping rule are shown in Table 3. That table’s numbers are generated as follows:

- For every N_1 files inspected by human, update the SVM model.
- Apply SEMI to estimate current recall $|R_E|$;
- Stop the security review and report the cost and actual recall if current estimated recall is greater than the target recall ($|L_R| \geq T_{rec} |R_E|$), otherwise, select next N_1 files for review.

In Table 2, percentage numbers show median results seen from 30 repeated simulations (and the values in brackets show the 75th-25th percentile range). From that figure we say:

- In most cases, the SEMI estimator slightly over-estimates

	Vulnerability Type	target recall					
		90	95	99	Recall	Cost	Recall
Text	Protection Mechanism Failure	87 (2)	18 (2)	91 (2)	22 (3)	98 (3)	33 (5)
	Resource Management Errors	96 (0)	19 (2)	98 (1)	26 (3)	100 (0)	46 (3)
	Data Processing Errors	96 (2)	36 (5)	100 (3)	46 (5)	100 (0)	56 (6)
	Code Quality	96 (3)	30 (7)	100 (0)	42 (6)	100 (0)	54 (7)
	Other	97(0)	25(6)	97(0)	32(6)	97(0)	50(5)
	All	90 (2)	15 (2)	95 (1)	21 (1)	99 (0)	43 (0)
	Median	96(6)	23(12)	97(4)	30(17)	99(2)	47(10)
Hybrid	Protection Mechanism Failure	84 (19)	14 (7)	94 (2)	20 (6)	98 (1)	44 (12)
	Resource Management Errors	93 (1)	12 (0)	98 (1)	17 (1)	100 (0)	48 (0)
	Data Processing Errors	96 (3)	31 (3)	100 (0)	45 (2)	100 (0)	58 (2)
	Code Quality	100 (0)	27 (0)	100 (0)	38 (0)	100 (0)	58 (1)
	Other	95(0)	20(0)	95(0)	28(1)	97(0)	52(3)
	All	67 (2)	8 (0)	70 (2)	8 (0)	99 (0)	46 (0)
	Median	93(11)	20(14)	96(5)	27(21)	100(1)	50(10)

TABLE 3: Using the SEMI estimator to stop at target recall, actual achieved recalls and cost. As in Table 2, numbers in brackets denote IQR values (75th-25th percentile ranges) and the other numbers are median values across 30 repeated simulations.

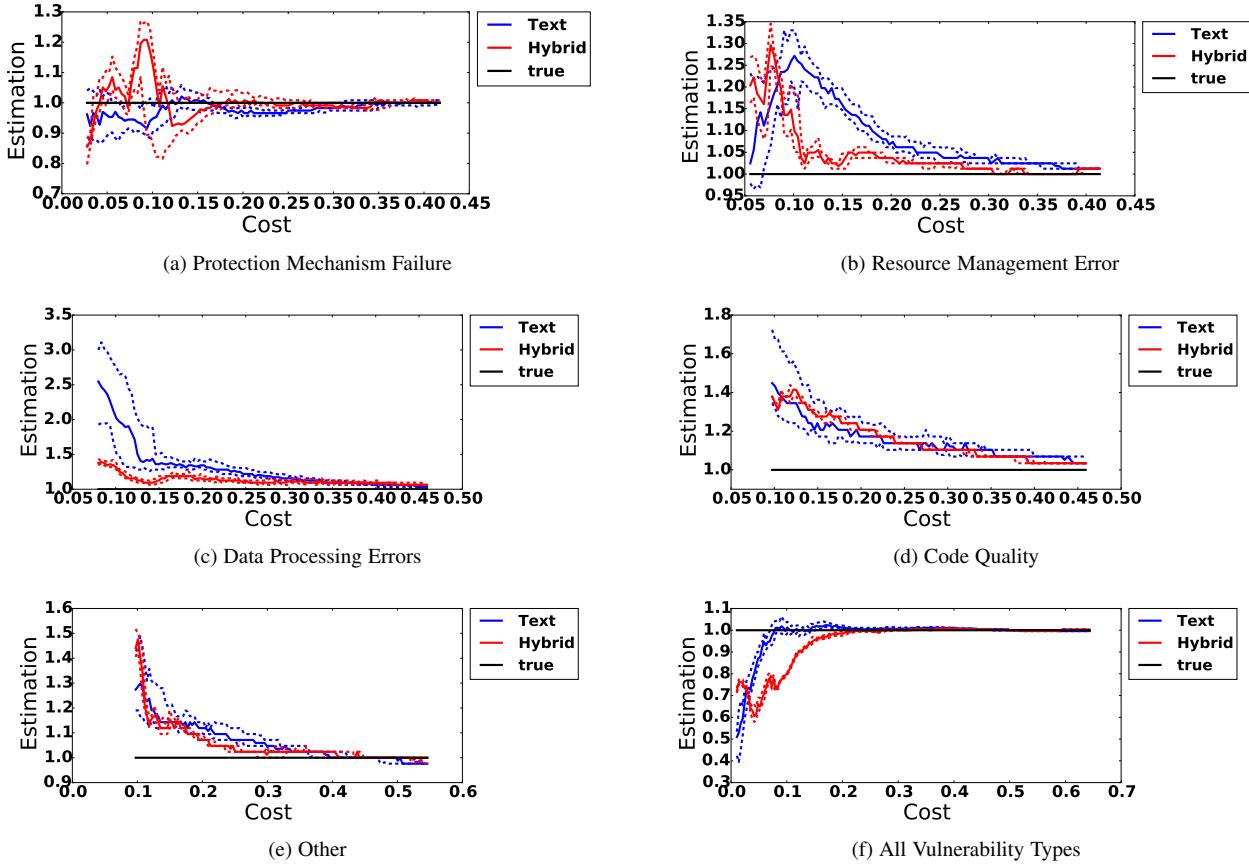


Fig. 3: Estimation vs Cost curves. Estimations (calculated as per Equation (3)) are considered accurate and useful if they converges to estimation=1.0 early (when cost is small). **Solid lines** represent the median estimations from 30 simulations while **dashed lines** show the 75th to 25th percentile range. In this figure, estimation=1.0 is denoted as the “true” line. When estimation converges to this line, it means that the estimated number of vulnerabilities equals to the true number. Also, when cost reaches 1.0, all source code files have been reviewed. For example, the estimation from **Text** and **Hybrid** on the entire project converges to 1.0 when cost is about 0.25, thus providing accurate estimation on whether the target recall has reached for cost ≥ 0.25 .

- $(|R_E| > |R|)$ to ensure the target recall is reached.
- The higher the target recall, the better the stopping rule works. This is because the estimation becomes more and more accurate when cost increases.
 - The stopping rule works better with **Text**, where the inspection usually stops with less than 6% error from target recall.
 - When using the stopping rule with **Hybrid**, it over-estimates ($|R_E| > |R|$) too much on “Code Quality” and under-estimates ($|R_E| < |R|$) on “All”. Overall, when using SEMI as a stopping rule, **Text** is better.

When can we stop inspecting the code with a confidence that a predetermined percentage of vulnerabilities have been found?

Through accurately estimating the number of vulnerabilities, we can stop the inspection process close to the target recall, especially when using **Text** and target recall is high (95% or 99%).

RQ3: How do human errors affect HARMLESS’s performance? In order to show how human error affect the performance, we take the results from HARMLESS with **Text**, target recall = 95% (Table 3) as baseline result and test the same algorithm with

human error rate increasing from 0% to 50%. Column None in Table 4 show the relative performance against the baseline result if no error correction is applied. As we can see, with 50% human error rate, the final recall becomes half of that of baseline recall.

How do human errors affect HARMLESS’s performance?

Human errors during the inspection process can adversely effect the performance of HARMLESS. Our simulation shows that without error correction, human agents with 50% recall result in a deterioration of recall from 96% to 48%.

Such large deterioration in recall motivates the next research question.

RQ4: Can HARMLESS correct human errors effectively? Table 4 compares DISPUTE and DISPUTE(3), the error correction methods from HARMLESS, against two state of the art error correction methods, Two-person and Cormack’17. One method is considered better than another if it achieves higher recall with lower cost. From this Table 4 we observe:

- Looking at the last line of the table, we see that all error correction methods achieve much higher recall than **None** (i.e. no error

TABLE 4: Experimental Results with Human Errors

Error Rate E_R	Vulnerability Type	Relative Recall = Observed Recall / Baseline Recall (from Table 3)					Relative Cost = Observed Cost / Baseline Cost (from Table 3)				
		None	Two-person	Cormack'17	DISPUTE	DISPUTE(3)	None	Two-person	Cormack'17	DISPUTE	DISPUTE(3)
0%	Protection Mechanism Failure	100 (1)	100 (1)	91 (8)	98 (2)	98 (2)	100 (11)	200 (22)	60 (22)	128 (27)	171 (36)
	Resource Management Errors	100 (0)	100 (0)	96 (0)	100 (0)	100 (0)	100 (5)	200 (10)	56 (13)	149 (7)	198 (9)
	Data Processing Errors	100 (0)	100 (0)	96 (0)	100 (0)	100 (0)	99 (12)	199 (24)	69 (21)	137 (13)	181 (17)
	Code Quality	100 (0)	100 (0)	89 (6)	100 (0)	100 (0)	100 (6)	200 (12)	43 (13)	145 (8)	192 (12)
	Other	100(0)	100(0)	78(17)	100(0)	100(0)	100(10)	200(20)	43(34)	144(11)	190(10)
	All	100 (0)	100 (0)	95 (0)	100 (0)	100 (0)	100 (0)	200 (0)	47 (6)	150 (1)	201 (2)
	Median	100(0)	100(0)	95(7)	100(0)	100(0)	100(6)	200(13)	52(22)	146(13)	192(19)
10%	Protection Mechanism Failure	90 (3)	99 (1)	87 (12)	96 (2)	97 (2)	97 (8)	199 (26)	58 (31)	116 (14)	148 (35)
	Resource Management Errors	91 (4)	98 (1)	95 (1)	99 (1)	99 (1)	102 (11)	199 (15)	57 (16)	147 (14)	197 (19)
	Data Processing Errors	90 (3)	100 (3)	90 (14)	98 (3)	100 (2)	105 (11)	201 (24)	61 (30)	140 (15)	180 (28)
	Code Quality	91 (6)	98 (3)	86 (5)	100 (2)	100 (0)	101 (8)	200 (17)	46 (28)	151 (10)	195 (7)
	Other	92(4)	100(0)	92(12)	100(1)	100(0)	101(8)	200(16)	59(44)	145(10)	191(8)
	All	90 (2)	99 (0)	92 (1)	98 (0)	100 (0)	99 (1)	200 (2)	49 (4)	149 (2)	200 (1)
	Median	90(4)	99(2)	91(9)	98(2)	100(1)	100(9)	200(15)	54(23)	146(14)	193(21)
20%	Protection Mechanism Failure	80 (1)	95 (2)	82 (9)	96 (4)	97 (3)	103 (11)	196 (26)	63 (26)	130 (23)	155 (37)
	Resource Management Errors	79 (2)	96 (2)	91 (5)	95 (2)	97 (2)	105 (11)	204 (22)	60 (4)	147 (15)	196 (19)
	Data Processing Errors	78 (9)	93 (5)	87 (28)	93 (3)	98 (3)	102 (9)	204 (28)	64 (38)	140 (15)	180 (20)
	Code Quality	86 (12)	96 (3)	79 (17)	96 (6)	98 (3)	105 (5)	210 (19)	39 (15)	154 (17)	197 (5)
	Other	82(7)	97(4)	86(20)	96(6)	100(0)	98(11)	202(26)	49(41)	147(14)	191(13)
	All	79 (2)	96 (1)	87 (2)	95 (1)	99 (0)	97 (2)	199 (3)	49 (7)	148 (4)	200 (3)
	Median	80(6)	96(3)	86(11)	95(3)	98(3)	101(11)	201(22)	52(28)	145(15)	194(19)
30%	Protection Mechanism Failure	68 (2)	91 (4)	65 (17)	88 (3)	93 (3)	101 (4)	201 (26)	40 (43)	116 (18)	160 (38)
	Resource Management Errors	74 (8)	90 (4)	84 (5)	91 (5)	96 (2)	104 (9)	199 (14)	69 (20)	147 (14)	209 (22)
	Data Processing Errors	75 (6)	90 (11)	84 (7)	90 (3)	95 (6)	105 (9)	204 (21)	59 (21)	148 (12)	179 (22)
	Code Quality	72 (3)	93 (6)	82 (8)	86 (6)	96 (2)	108 (5)	206 (11)	43 (43)	168 (13)	210 (19)
	Other	70(4)	87(4)	81(14)	90(6)	97(2)	105(8)	197(26)	45(52)	152(16)	190(12)
	All	70 (5)	91 (0)	82 (4)	90 (1)	97 (1)	96 (6)	197 (7)	47 (8)	142 (4)	196 (7)
	Median	70(7)	91(5)	82(10)	90(4)	96(3)	103(11)	200(18)	52(40)	148(17)	192(21)
40%	Protection Mechanism Failure	55 (11)	84 (3)	67 (10)	81 (4)	89 (5)	101 (13)	205 (35)	62 (50)	149 (19)	170 (57)
	Resource Management Errors	61 (7)	82 (2)	77 (7)	82 (4)	91 (3)	107 (11)	213 (15)	58 (14)	154 (38)	202 (13)
	Data Processing Errors	65 (0)	84 (6)	68 (9)	82 (8)	90 (4)	105 (5)	214 (12)	63 (29)	147 (19)	199 (13)
	Code Quality	75 (3)	86 (6)	72 (6)	82 (6)	86 (6)	108 (6)	209 (17)	45 (32)	162 (16)	208 (17)
	Other	60(10)	85(4)	73(12)	82(8)	90(1)	107(12)	202(24)	44(29)	152(19)	197(13)
	All	59 (1)	82 (1)	72 (3)	83 (2)	93 (2)	89 (3)	191 (5)	56 (13)	145 (16)	198 (8)
	Median	61(9)	83(4)	71(9)	82(5)	90(4)	105(11)	204(25)	57(24)	151(21)	199(16)
50%	Protection Mechanism Failure	51 (5)	76 (3)	59 (18)	70 (4)	81 (5)	112 (14)	203 (27)	58 (43)	146 (41)	184 (11)
	Resource Management Errors	50 (5)	73 (8)	68 (8)	72 (6)	86 (2)	112 (13)	216 (19)	81 (15)	154 (20)	205 (29)
	Data Processing Errors	48 (5)	73 (8)	31 (34)	81 (9)	89 (6)	107 (8)	217 (23)	36 (30)	148 (7)	200 (11)
	Code Quality	51 (3)	81 (9)	62 (15)	75 (5)	87 (8)	110 (7)	219 (14)	61 (27)	166 (12)	215 (12)
	Other	49 (2)	74 (12)	65 (17)	71 (8)	85 (7)	108 (9)	207 (21)	34 (68)	162 (11)	202 (16)
	All	50 (1)	74 (4)	68 (3)	74 (1)	85 (3)	96 (4)	193 (19)	66 (9)	136 (17)	186 (18)
	Median	50 (4)	75 (7)	65 (20)	74 (7)	86 (6)	110 (11)	206 (25)	64 (45)	154 (21)	197 (23)

This table shows the experimental results when human error rate E_R increases from 0% to 50%. Baseline recall and cost come from Table 3, Row Text, Column 95. All the numbers are percentages and in the format of median(IQR) from 30 repeated simulations. Each row presents performances on one group of target vulnerability types in the Mozilla Firefox dataset as described in Table 1. The “Median” row summarizes the median performance across all groups. The “None” columns show the performance of HARMLESS without any error correction method while other columns each documents the performance with a different error correction method. One method is considered better than another if it has higher relative recall and lower relative cost.

- correction). That is, error correction is strongly recommended when human inspectors are fallible.
- **Cormack'17** costs least among all the error correction methods, but also achieves lower recall. Given recall as highest priority, **Cormack'17** is not recommended.
- **DISPUTE** is better than Two-person; i.e. achieves similar recalls at less cost. For example, when $E_R = 50\%$, DISPUTE reaches $0.74 \times 0.96 = 71\%$ recall with $1.51 \times 0.26 = 39\%$ cost while Two-person reaches $0.75 \times 0.96 = 72\%$ recall with $2.06 \times 0.26 = 54\%$ cost.
- **DISPUTE(3)** is also better than Two-person; i.e. achieves higher recall with similar cost (achieves $0.86 \times 0.96 = 83\%$ recall with $1.96 \times 0.26 = 51\%$ cost when $E_R = 50\%$).
- Compared to **DISPUTE**, **DISPUTE(3)** costs more but also corrects more errors. Therefore one can always increase the number of humans rechecking the files selected by **DISPUTE**

to reach higher recall with higher cost.

- The coverage of false negatives by **DISPUTE** can be calculated as $\frac{\text{Relative Recall} - (1-E_R)}{(1-E_R)E_R} = \frac{0.74-0.5}{0.25} = 96\%$ when $E_R = 50\%$. Similarly, the coverage of false negatives by **DISPUTE(3)** can be calculated as $\frac{\text{Relative Recall} - (1-E_R)}{(1-E_R^2)E_R} = \frac{0.86-0.5}{0.375} = 96\%$ when $E_R = 50\%$. Therefore the core hypothesis of **DISPUTE** is valid: most human errors (96%) are in the files selected by **DISPUTE** (50% of the labeled files).

Can HARMLESS correct human errors effectively?

Yes. HARMLESS corrects more human errors with less redundant inspection when compared to other state of the art error correction methods. It redundantly inspects only 50% of the labeled files but covers 96% of the missing vulnerabilities.

7 THREATS TO VALIDITY

There are several validity threats [37] to the design of this study. Any conclusions made from this work must be considered with the following issues in mind:

Conclusion validity focuses on the significance of the treatment. To enhance conclusion validity, we ran each simulation 30 times with different random seeds.

Internal validity focuses on how sure we can be that the treatment caused the outcome. To enhance internal validity, we heavily constrained our experiments to the same dataset, with the same settings, except for the treatments to be compared.

Construct validity focuses on the relation between the theory behind the experiment and the observation. This applies to our analysis of which feature set provides best performance. When we conclude that software metrics performs worst and contributes little to the vulnerability prediction, other reasons such as the choice of classifier (different classifiers might work best with different feature sets) might be the real cause of the observation.

External validity concerns how well the conclusion can be applied outside. All the conclusions in this study are drawn from the experiments running on the Mozilla Firefox vulnerability dataset. When applied to other case studies, the following concerns might arise: 1) crash dump stack trace data may not be available; 2) the same settings that works on Mozilla Firefox dataset might not provide the best performance on other dataset. One possible solution to this problem can be hyperparameter tuning which adapts the parameter settings to the target dataset.

8 CONCLUSION AND FUTURE WORK

Reducing software security vulnerabilities is a crucial task of software development. However inspecting codes is a tedious and time consuming task. Software engineers can better find vulnerabilities with less effort if they are directed to the codes that are more likely to contain vulnerabilities. To this purpose, we propose HARMLESS, an active learning based vulnerability prediction framework. HARMLESS builds a support vector machine from the source code files reviewed to date; then suggests what other source code files might have vulnerabilities and need to be reviewed first. HARMLESS focuses on (1) saving cost when reaching different levels of recall, (2) providing a practical way to stop at the target recall, and (3) correcting human errors efficiently.

HARMLESS was tested on a Mozilla Firefox dataset using a simulation methodology. Given actual vulnerabilities found during actual inspections, we run multiple what-if simulations where we run over that data using a variety of code inspection policies. The goal of these inspections is to determine what might have happened in these policies were used prior to code being deployed.

What we found was that using text mining features alone, HARMLESS can efficiently reduce the cost to reach high recall for finding vulnerabilities before deployment; and if runtime data is available (e.g. the crash features used above), then that can boost vulnerability prediction in early stages. We also showed that the total number of vulnerabilities in one software project can be accurately estimated during the active learning process, thus providing a reliable stopping rule for the approach. Based on our results, HARMLESS can save 70, 69, 53% of the cost (comparing to reviewing and testing source code files in a random order) when applying the SEMI estimator to stop at 90, 95, 99% recall, respectively. Note that these results indicate that HARMLESS can result in, by practitioner choice, a recall value close to 100% given

TABLE 5: Comparison to the state-of-the-art frameworks

	HARMLESS	Supervised Learning	Crash Features
Can reach any target recall	✓	✓	
Guide on how to reach target recall	✓		
Works without crash features	✓		✓
Can start without labeled data	✓		
Utilize continuous human feedback	✓		
Correct human errors efficiently	✓		

trade-offs in recall and cost. Practitioners can have confidence that, if they so choose and have the resources to spare, the security review and test would identify 99% of the vulnerabilities without inspecting most of the source code.

Table 5 compares the advantages of HARMLESS with other approaches to vulnerability prediction, i.e. supervised learning [25], [7] and crash features [28], [8], [29]. We assert that HARMLESS does best due to its capability to make full use of continuous human feedback.

Therefore we recommend to

- Use the HARMLESS active learning approach to find software vulnerabilities with reduced human effort.
- Use the SEMI estimator to decide whether the target recall has been reached (thus whether to stop the review).
- Use the DISPUTE error correction method fix human errors without imposing too much extra cost.
- Use the DISPUTE(3) error correction method if human tends to make too many mistakes.

Considering the limitations and validity threats of this current work, our future works include:

- 1) The community requires more dataset like the Mozilla Firefox vulnerability dataset we described in this paper. Active learning tools like HARMLESS could be useful for reducing the cost of collecting such data.
- 2) This work applies some best practice settings (featurization, classifier, active learning, etc.) from other domains, this does not necessarily be the best practice for proactive vulnerability prediction. Further testing of other settings might provide improved results on this specific domain.
- 3) Further studies on how to tune parameters for a specific software project might improve the performance of HARMLESS.
- 4) As shown in §5.4, different level of human error rate E_R requires different error correction methods, e.g. if $E_R = 0$, using DISPUTE will cost 46% more than not using any error correction; and at high error rate $E_R = 50\%$, DISPUTE(3) is more desired than DISPUTE. Therefore how to accurately estimate the human error rate and adjust the error correction method correspondingly becomes an important future work.

We hope that this work will lay down a foundation and motivate further research on active learning-based vulnerability prediction.

ACKNOWLEDGEMENTS

This research was partially funded by a National Science Foundation Grant #1506586. The authors would like to thank the Mozilla Firefox team for making crash and defect data available to the public, which makes this research possible.

REFERENCES

- [1] P. E. Black, L. Badger, B. Guttman, and E. Fong, "Nistir 8151: Dramatically reducing software vulnerabilities," 2016.
- [2] N. Lewis, "Common vulnerabilities and exposures (cve)," 2016.
- [3] L. J. Trautman, "Cybersecurity: What about us policy?" 2015.
- [4] S. A. Slaughter, D. E. Harter, and M. S. Krishnan, "Evaluating the cost of software quality," *Communications of the ACM*, vol. 41, no. 8, pp. 67–73, 1998.
- [5] R. Scandariato, J. Walden, A. Hovsepyan, and W. Joosen, "Predicting vulnerable software components via text mining," *IEEE Transactions on Software Engineering*, vol. 40, no. 10, pp. 993–1006, 2014.
- [6] Y. Shin and L. Williams, "Can traditional fault prediction models be used for vulnerability prediction?" *Empirical Software Engineering*, vol. 18, no. 1, pp. 25–59, 2013.
- [7] T. Zimmermann, N. Nagappan, and L. Williams, "Searching for a needle in a haystack: Predicting security vulnerabilities for windows vista," in *Software Testing, Verification and Validation (ICST), 2010 Third International Conference on*. IEEE, 2010, pp. 421–428.
- [8] C. Theisen, K. Herzig, P. Morrison, B. Murphy, and L. Williams, "Approximating attack surfaces with stack traces," *IEEE/ACM 37th IEEE International Conference on Software Engineering*, pp. 199–208, 2015.
- [9] C. Theisen, T. Zhu, K. Oliver, and L. Williams, "Teaching secure software development through an online course," in *Secure Software Engineering in DevOps and Agile Development, International Workshop on*. ESORICS, 2017.
- [10] J. Walden, J. Stuckman, and R. Scandariato, "Predicting vulnerable components: Software metrics vs text mining," in *Software Reliability Engineering (ISSRE), 2014 IEEE 25th International Symposium on*. IEEE, 2014, pp. 23–33.
- [11] L. Hatton, "Testing the value of checklists in code inspections," *IEEE software*, vol. 25, no. 4, 2008.
- [12] B. Settles, "Active learning," *Synthesis Lectures on Artificial Intelligence and Machine Learning*, vol. 6, no. 1, pp. 1–114, 2012.
- [13] G. V. Cormack and M. R. Grossman, "Navigating imprecision in relevance assessments on the road to total recall: Roger and me," in *The International ACM SIGIR Conference*, 2017, pp. 5–14.
- [14] ——, "Engineering quality and reliability in technology-assisted review," pp. 75–84, 2016.
- [15] ——, "Scalability of continuous active learning for reliable high-recall text classification," in *Proceedings of the 25th ACM International Conference on Information and Knowledge Management*. ACM, 2016, pp. 1039–1048.
- [16] ——, "Autonomy and reliability of continuous active learning for technology-assisted review," *arXiv preprint arXiv:1504.06868*, 2015.
- [17] ——, "Evaluation of machine-learning protocols for technology-assisted review in electronic discovery," in *Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval*. ACM, 2014, pp. 153–162.
- [18] M. R. Grossman and G. V. Cormack, "The grossman-cormack glossary of technology-assisted review with foreword by john m. facciola, u.s. magistrate judge," *Federal Courts Law Review*, vol. 7, no. 1, pp. 1–34, 2013.
- [19] B. C. Wallace, T. A. Trikalinos, J. Lau, C. Brodley, and C. H. Schmid, "Semi-automated screening of biomedical citations for systematic reviews," *BMC bioinformatics*, vol. 11, no. 1, p. 1, 2010.
- [20] B. C. Wallace, K. Small, C. E. Brodley, and T. A. Trikalinos, "Active learning for biomedical citation screening," in *Proceedings of the 16th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2010, pp. 173–182.
- [21] ——, "Who should label what? instance allocation in multiple expert active learning." in *SDM*. SIAM, 2011, pp. 176–187.
- [22] B. C. Wallace and I. J. Dahabreh, "Class probability estimates are unreliable for imbalanced data (and how to fix them)," in *Data Mining (ICDM), 2012 IEEE 12th International Conference on*. IEEE, 2012, pp. 695–704.
- [23] B. C. Wallace, I. J. Dahabreh, K. H. Moran, C. E. Brodley, and T. A. Trikalinos, "Active literature discovery for scoping evidence reviews: How many needles are there," in *KDD workshop on data mining for healthcare (KDD-DMH)*, 2013.
- [24] Z. Yu, N. A. Kraft, and T. Menzies, "Finding better active learners for faster literature reviews," *Empirical Software Engineering*, Mar 2018. [Online]. Available: <https://doi.org/10.1007/s10664-017-9587-0>
- [25] Y. Shin, A. Meneely, L. Williams, and J. A. Osborne, "Evaluating complexity, code churn, and developer activity metrics as indicators of software vulnerabilities," *IEEE Transactions on Software Engineering*, vol. 37, no. 6, pp. 772–787, 2011.
- [26] L. Breiman, "Random forests," *Machine learning*, vol. 45, no. 1, pp. 5–32, 2001.
- [27] Y. Shin and L. Williams, "Is complexity really the enemy of software security?" in *Proceedings of the 4th ACM workshop on Quality of protection*. ACM, 2008, pp. 47–50.
- [28] C. Theisen, R. Krishna, and L. Williams, "Strengthening the evidence that attack surfaces can be approximated with stack traces," in *North Carolina State University Department of Computer Science TR2015-10, submitted to International Conference on Software Testing, Verification, and Validation (ICST) 2016*, 2015.
- [29] C. Theisen, K. Herzig, B. Murphy, and L. Williams, "Risk-based attack surface approximation: how much data is enough?" in *Software Engineering: Software Engineering in Practice Track (ICSE-SEIP), 2017 IEEE 39th International Conference on*. IEEE, 2017, pp. 273–282.
- [30] M. R. Grossman, G. V. Cormack, and A. Roegiest, "Trec 2016 total recall track overview," in *TREC*, 2016.
- [31] Z. Yu and T. Menzies, "Fast2: Better automated support for finding relevant se research papers," *CoRR*, vol. abs/1705.05420, 2017. [Online]. Available: <http://arxiv.org/abs/1705.05420>
- [32] M. Miwa, J. Thomas, A. O'Mara-Eves, and S. Ananiadou, "Reducing systematic review workload through certainty-based screening," *Journal of biomedical informatics*, vol. 51, pp. 242–253, 2014.
- [33] C. Cortes and V. Vapnik, "Support-vector networks," *Machine learning*, vol. 20, no. 3, pp. 273–297, 1995.
- [34] T. Joachims, "Training linear svms in linear time," in *Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*. ACM, 2006, pp. 217–226.
- [35] R. Krishna, Z. Yu, A. Agrawal, M. Dominguez, and D. Wolf, "The bigse project: lessons learned from validating industrial text mining," in *Proceedings of the 2nd International Workshop on BIG Data Software Engineering*. ACM, 2016, pp. 65–71.
- [36] (2017) Mozilla foundation security advisories. [Online]. Available: <https://www.mozilla.org/en-US/security/advisories/>
- [37] R. Feldt and A. Magazinius, "Validity threats in empirical software engineering research-an initial survey." in *SEKE*, 2010, pp. 374–379.

Zhe Yu is a forth year Ph.D. student in computer Science at North Carolina State University. He received his masters degree in Shanghai Jiao Tong University, China. His primary interest lies in the collaboration of human and machine learning algorithms that leads to better performance and higher efficiency. <http://azhe825.github.io/>



Christopher Theisen is with Microsoft Research. He received his Ph.D. in Computer Science from North Carolina State University. His research is focused in software security and software engineering, specifically developing attack surface metrics. <http://theisencr.github.io/>



Laurie Williams received her Ph.D. in Computer Science from the University of Utah. Her research focuses on software security; agile software development practices and processes, particularly continuous deployment; and software reliability, software testing and analysis. Prof. Williams has more than 230 refereed publications. <https://collaboration.csc.ncsu.edu/laurie/>



Tim Menzies is a Professor in CS at NcState His research interests include software engineering (SE), data mining, artificial intelligence, and search-based SE, open access science. <http://menzies.us>

