Example Questionnaire Response

Section 1

Your Institution: University of Georgia
Name of POC: Roberto Perdisci
Email of POC: poc@exampleinstitution.edu
Name of POC Presenting Research Foci of the Institution: Roberto Perdisci

Section 2: First Research Presentation

Name(s) of Faculty/Student Presenting Recently Accepted/Published Research Results: An Chen, Kyu Hyung Lee
Email of Presenter(s): presenter1@exampleinstitution.edu
Title of First Research Presentation: SYNTHDB: Synthesizing Database via Program Analysis for Security Testing of Web Applications
Authors of First Recently Accepted/Published Paper: An Chen, JiHo Lee, Basanta Chaulagain, Yonghwi Kwon, and Kyu Hyung Lee
Venue of First Recently Accepted/Published Paper: Network and Distributed System Security (NDSS) 2023
Abstract of First Recently Accepted/Published Paper: "Testing database-backed web applications is challenging because their behaviors (e.g., control flow) are highly dependent on data returned from SQL queries. Without a database containing sufficient and realistic data, it is challenging to reach potentially vulnerable code snippets, limiting various existing dynamic-based security testing approaches. However, obtaining such a database for testing is difficult in practice as it often contains sensitive information. Sharing it can lead to data leaks and privacy issues.

In this paper, we present SYNTHDB, a program analysis based database generation technique for database-backed PHP applications. SYNTHDB leverages a concolic execution engine to identify interactions between PHP codebase and the SQL queries. It then collects and solves various constraints to reconstruct a database that can enable exploring uncovered program paths without violating database integrity. Our evaluation results show that the database generated by SYNTHDB outperforms state-ofthe-arts database generation techniques in terms of code and query coverage in 17 real-world PHP applications. Specifically, SYNTHDB generated databases achieve 62.9% code and 77.1% query coverages, which are 14.0% and 24.2% more in code and query coverages than the state-of-the-art techniques. Furthermore, our security analysis results show that SYNTHDB effectively aids existing security testing tools: Burp Suite, Wfuzz, and webFuzz. Burp Suite aided by SYNTHDB detects 76.8% of vulnerabilities while other existing techniques cover 55.7% or fewer. Impressively, with SYNTHDB, Burp Suite discovers 33 previously unknown vulnerabilities from 5 real-world applications."

Link to Where First Recently Accepted/Published Paper Can be Downloaded:
https://kyuhlee.github.io/publications/ndss23-SynthDB.pdf

Section 3: Second Research Presentation[1]

Name(s) of Faculty/Student Presenting Recently Accepted/Published Research Results: Karthika Subramani
Email of Presenter(s): presenter2@exampleinstitution.edu
Title of Second Research Presentation: PhishInPatterns: Measuring Elicited User Interactions at Scale on Phishing Websites
Authors of Second Recently Accepted/Published Paper: Karthika Subramani, Oleksii Starov, William Melicher, Phani Vadrevu, and Roberto Perdisci
Venue of Second Recently Accepted/Published Paper: ACM Internet Measurement Conference 2022
Abstract of Second Recently Accepted/Published Paper: "Despite phishing attacks and detection systems being extensively studied, phishing is still on the rise and has recently reached an all-time high. Attacks are becoming increasingly sophisticated, leveraging new web design patterns to add perceived legitimacy and, at the same time, evade state-of-the-art detectors and web security crawlers.

In this paper, we study phishing attacks from a new angle, focusing on how modern phishing websites are designed. Specifically, we aim to better understand what type of user interactions are elicited by phishing websites and how their user experience (UX) and interface (UI) design patterns can help them accomplish two main goals: i) lend a sense of professionalism and legitimacy to the phishing website, and ii) contribute to evading phishing detectors and web security crawlers. To study phishing at scale, we built an intelligent crawler that combines browser automation with machine learning methods to simulate user interactions with phishing pages and explore their UX and UI characteristics. Using our novel methodology, we explore more than 50,000 phishing websites and make the following new observations: i) modern phishing sites often impersonate a brand (e.g., Microsoft Office), but surprisingly, without necessarily cloning or closely mimicking the design of the corresponding legitimate website; ii) they often elicit personal information using a multi-step (or multi-page) process, to mimic users' experience on legitimate sites; iii) they embed modern user verification systems (including CAPTCHAs); and ironically, iv) they sometimes conclude the phishing experience by reassuring the user that their private data was not stolen. We believe our findings can help the community gain a more in-depth understanding of how web-based phishing attacks work from a users' perspective and can be used to inform the development of more accurate and robust phishing detectors."
Link to Where Second Recently Accepted/Published Paper Can be Downloaded:
https://dl.acm.org/doi/abs/10.1145/3517745.3561467

[1] You may provide details for a second research presentation if applicable; otherwise, answer N/A for all questions.

Section 4: Closing

Any other comments?: Optional. Add comments here as appropriate and Bo Yuan and/or Roberto Perdisci will address them as necessary.