Understanding How Software Developers Secure User Interfaces in Rapid Release Environments

Commonwealth Cyber Initiative (CCI) Workforce & Industry Engagement Program

Chris Brown (PI)
Assistant Professor
Department of Computer Science
Virginia Tech
dcbrown@vt.edu

Total Amount Requested: $10,000

1 Introduction

Graphic User Interface (GUI) testing is crucial for verifying visual elements of software applications and ensuring that user interfaces function as intended. For instance, GUI functions have been shown to affect the quality of entire systems and impact user experiences [3]. Further, many security vulnerabilities can be exploited through user interface components–such as cross site scripting, access management issues, and information leakage. To combat this, prior work has explored using GUI testing tools—such as Selenium [13]—to create tests to detect and prevent vulnerabilities in web applications [8, 9].

To meet the growing demands for software, rapid release processes are essential in modern software development to deploy software to users quickly. For example, continuous integration and continuous deployment (CI/CD) provides a pipeline of steps for developers to stage code changes, build projects, test software, and deploy to users more frequently and reliably [14]. Automation is effective for many types of testing (*i.e.,* unit and integration tests), however automating GUI testing is more challenging due to the complexity of user interfaces [10]. Thus, novel solutions for securing GUIs in rapid release projects are essential as web-based attacks become more prevalent and sophisticated.

2 Research Plan

The goal of the proposed work is to understand current practices and challenges for securing user interfaces in modern software. In particular, we will explore the following research question: **How do software developers secure user interfaces in rapid release environments?** To answer this question, we will conduct a series of research activities to investigate GUI testing for security in CI/CD projects and the challenges therein.

1. Literature Review. Our first step is to conduct a literature review to gain insight into prior work and inform our research methods. The literature review will identify techniques and tools for securing GUIs and challenges with adopting GUI testing in rapid release (*i.e.,* CI/CD) projects. We will systematically analyze existing literature and categorize identified techniques and challenges to use in the subsequent research activity.

2. Focus Group. We will conduct a focus group to gain insight from developers on techniques and challenges in securing GUIs in rapid release projects. We will recruit industry practitioners with expertise in CI/CD to participate, leveraging our workforce development component (see Section 3). The focus group will consist of: 1) a presentation of our preliminary findings and the practices and challenges identified through the literature review to provide context; 2) a semi-structured group interview for subjects to reflect on the presented content, describe their own experiences, and brainstorm ideas for technical (*i.e.,* tools) and non-technical (*i.e.,* guidelines) solutions to enhance user interface security; 3) an exit survey for participants to provide feedback and demographic information.

3. Data Analysis. We will receive IRB approval before starting this work. Pending IRB approval and participants' consent, the focus group will be recorded and transcribed by the research team. In the event the session cannot be recorded, the moderator will take extensive field notes for analysis [11]. We will use thematic analysis to analyze participant comments and derive themes related to GUI security testing practices and challenges [4].

Preliminary Results. We analyzed GitHub projects to study how developers use Selenium in CI/CD configuration files for open source projects across three popular platforms: GitHub Actions [7], Travis CI [2], and Jenkins [1].[1] We found Selenium significantly slows down build times and increases developer effort (*i.e.*, more commits and pull request activity), in addition to inconsistent usage across projects. Our current work extends this by distributing an online survey to discover the usage and challenges developers face integrating popular GUI testing frameworks in open source CI/CD projects.

3 Workforce Development

The research activities will be completed by two graduate students (one PhD, one MS) at Virginia Tech (GRAs). To support their workforce development, the GRAs will attend DevOpsDays [5]—an international conference series for developers focused on topics related to software development, IT operations and infrastructure, and their intersections. CI/CD is a critical DevOps practice, essential for validating software quality before deployment to a production environment [12]. For this project, the GRAs will attend DevOpsDays Baltimore [6], a regional conference in Baltimore, MD. This event was selected based on its proximity to Southwest Virginia and occurrence during the project period.

DevOpsDays Baltimore will provide several workforce development opportunities. First, the GRAs can network with industry professionals and companies from the Baltimore, Washington D.C., and Northern Virginia region. In addition, the GRAs will be able to attend talks from DevOps experts to "gain insights relevant to modern DevOps challenges and solutions" [6]. Finally, DevOpsDays Baltimore features a unique *Open Spaces* component, where any attendee can propose topics for discussion in small breakout groups. We will leverage this for our focus group (see Section 2). The PI and GRAs will organize an open space to gain insights from DevOps experts on challenges and solutions for securing user interfaces in rapid release processes. This will also allow us to disseminate research findings to industry practitioners—contributing to the broader impacts of this work.

4 Conclusion

Rapid release processes, such as CI/CD and DevOps, are increasingly adopted by development teams to streamline the deployment of software to users. However, these processes lack support for GUI testing–in particular automated tests to secure user interfaces. The proposed work aims to advance the state of the art in cybersecurity by engaging with practitioners to understand if and how developers secure user interfaces in CI/CD projects and motivate novel solutions to detect and prevent GUI-based security vulnerabilities. Funding from the CCI Workforce & Industry Engagement Program will provide support for graduate student researchers to complete the proposed work and advance their training and workforce development—allowing them to connect with industry experts, present research findings, and gain insights from DevOps practitioners at DevOpsDays Baltimore. This project is relevant to CCI goals and will contribute to innovative cybersecurity research and security-related workforce development in Virginia.

[1] Work in preparation at the time of proposal.

IDENTIFYING INFORMATION:

NAME: Brown, Chris

ORCID iD: https://orcid.org/0000-0002-6036-4733

POSITION TITLE: Assistant Professor

PRIMARY ORGANIZATION AND LOCATION: Virginia Tech, Blacksburg, Virginia, United States

Professional Preparation:

ORGANIZATION AND LOCATION	DEGREE (if applicable)	RECEIPT DATE	FIELD OF STUDY
North Carolina State University, Raleigh, North Carolina, United States	PHD	04/2021	Computer Science
North Carolina State University, Raleigh, North Carolina, United States	MS	05/2017	Computer Science
Duke University, Durham, North Carolina, United States	BS	09/2013	Computer Science

Appointments and Positions

2021 - present	Assistant Professor, Virginia Tech, College of Engineering, Blacksburg, Virginia, United States
2020 - 2020	Instructor of Record, North Carolina State University, College of Engineering, Raleigh, North Carolina, United States
2017 - 2017	Quality Engineering Intern, Red Hat, Raleigh, North Carolina, United States
2017 - 2017	Quality Engineering Intern, Red Hat, Raleigh, NC, US
2016 - 2021	Graduate Research Assistant, North Carolina State University, College of Engineering, Raleigh, North Carolina, United States
2016 - 2016	Software Quality Engineer Intern, Blackbaud, Charleston, South Carolina, United States
2015 - 2016	Graduate Teaching Assistant, North Carolina State University, College of Engineering, Raleigh, North Carolina, United States
2013 - 2015	Python Developer, Bank of America, Charlotte, North Carolina, United States

Products

Products Most Closely Related to the Proposed Project

1. Franke Lucas, Liang Huayu, Brantly Aaron, Davis James C, Brown Chris. A First Look at the General Data Protection Regulation (GDPR) in Open-Source Software. 2024.
2. Brown C, Parnin C. Understanding the impact of GitHub suggested changes on recommendations between developers. Proceedings of the 28th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering. ESEC/FSE '20: 28th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering; 08 1 20; Virtual Event USA. New York, NY, USA: ACM; c2020. Available from: https://dl.acm.org/doi/10.1145/3368089.3409722 DOI: 10.1145/3368089.3409722

3. Khalid S, Brown C. Software Engineering Approaches Adopted By Blockchain Developers. 2023 Tenth International Conference on Software Defined Systems (SDS). 2023 Tenth International Conference on Software Defined Systems (SDS); ; San Antonio, TX, USA. IEEE; c2023. Available from: https://ieeexplore.ieee.org/document/10329007/ DOI: 10.1109/SDS59856.2023.10329007
4. Brown C, Parnin C. Nudging Students Toward Better Software Engineering Behaviors. 2021 IEEE/ACM Third International Workshop on Bots in Software Engineering (BotSE). 2021 IEEE/ACM Third International Workshop on Bots in Software Engineering (BotSE); ; Madrid, Spain. IEEE; c2021. Available from: https://ieeexplore.ieee.org/document/9474399/ DOI: 10.1109/BotSE52550.2021.00010
5. Brown C, Parnin C. Comparing Different Developer Behavior Recommendation Styles. Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. ICSE '20: 42nd International Conference on Software Engineering; 27 0 20; Seoul Republic of Korea. New York, NY, USA: ACM; c2020. Available from: https://dl.acm.org/doi/10.1145/3387940.3391481 DOI: 10.1145/3387940.3391481

Other Significant Products, Whether or Not Related to the Proposed Project

1. Haroon Sabaat, Brown Chris, Gulzar Muhammad Ali. DeSQL: Interactive Debugging of SQL in Data-Intensive Scalable Computing. Foundations of Software Engineering; 2024; New York, NY, USA: Association for Computing Machinery; c2024.
2. Behroozi Mahnaz, Parnin Chris, Brown Chris. Asynchronous technical interviews: Reducing the effect of supervised think-aloud on communication ability. Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering; 2022; ACM; c2022.
3. Minkyuk Ko, Dibyendu Brinto Bose, Hemayet Ahmed Chowdhury, Mohammed Seyam, Chris Brown. Exploring the Barriers and Factors that Influence Debugger Usage for Students. Visual Languages and Human Centric Computing; 2023; c2023.
4. Palvannan N, Brown C. Suggestion Bot: Analyzing the Impact of Automated Suggested Changes on Code Reviews. 2023 IEEE/ACM 5th International Workshop on Bots in Software Engineering (BotSE). 2023 IEEE/ACM 5th International Workshop on Bots in Software Engineering (BotSE); ; Melbourne, Australia. IEEE; c2023. Available from: https://ieeexplore.ieee.org/document/10190399/ DOI: 10.1109/BotSE59190.2023.00015
5. Anjum Haque M, Ahmad W, Lourentzou I, Brown C. FixEval: Execution-based Evaluation of Program Fixes for Programming Problems. 2023 IEEE/ACM International Workshop on Automated Program Repair (APR). 2023 IEEE/ACM International Workshop on Automated Program Repair (APR); ; Melbourne, Australia. IEEE; c2023. Available from: https://ieeexplore.ieee.org/document/10189234/ DOI: 10.1109/APR59189.2023.00009

Synergistic Activities

1. Program committee member and reviewer for software engineering and HCI-related academic workshops and conferences, such as Computer-Supported and Cooperative Work (CSCW) 2024.
2. Reviewer for software engineering-related academic journals, such as the IEEE Software Special Issue on Developing your Software Engineering Career.

3. As an invited participant to the NII Shonan Meeting on Software Developer Diversity and Inclusion (SDDI), I collaborated with other researchers to discuss and develop plans to conduct cutting edge diversity and inclusion research and broaden the participation of underrepresented groups in software engineering.
4. As an invited speaker for the It Will Never Work in Theory session at the Strange Loop 2022, I presented my research on making effective recommendations for development tools to an audience of software practitioners at the industry-focused conference.
5. As a faculty mentor for Virginia Tech Multicultural Academic Opportunities Program (MAOP) Summer Research Internship for Summer 2023, I advised three undergraduate students from minority backgrounds for a 10-week program to gain research experience conducting innovative and impactful computing research.

Certification:

When the individual signs the certification on behalf of themselves, they are certifying that the information is current, accurate, and complete. This includes, but is not limited to, information related to domestic and foreign appointments and positions. Misrepresentations and/or omissions may be subject to prosecution and liability pursuant to, but not limited to, 18 U.S.C. §§ 287, 1001, 1031 and 31 U.S.C. §§ 3729-3733 and 3802.

Certified by Brown, Chris in SciENcv on 2024-03-05 14:01:02

CURRENT AND PENDING (OTHER) SUPPORT INFORMATION

Provide the following information for the Senior/key personnel and other significant contributors.
Follow this format for each person.

*NAME: Brown, Chris

*POSITION TITLE: Assistant Professor

*ORGANIZATION AND LOCATION: Virginia Tech, Blacksburg, Virginia, United States

Projects/Proposals

***Project/Proposal Title:** CCI: Understanding the Impact of Data Privacy Regulations on Software and Its Stakeholders

***Status of Support:** current

Proposal/Award Number:

***Source of Support:** Commonwealth Cyber Initiative

***Primary Place of Performance:** Virginia Tech

***Project/Proposal Support Start Date: (MM/YYYY):** 12/2022

***Project/Proposal Support End Date: (MM/YYYY):** 08/2024

***Total Award Amount:** $60,000

*** Person Months (Calendar/Academic/Summer) per budget period Committed to the Project:**

Year	Person Months
2023	1

***Overall Objectives:** Understand the impact of data privacy regulations on software code, developers, and users.

***Statement of Potential Overlap:** N/A

***Project/Proposal Title:** BPC-DP: Understanding Challenges and Exploring Inclusive Recruitment Practices for Women Candidates in Technical Interviews

***Status of Support:** pending

Proposal/Award Number:

***Source of Support:** NSF

***Primary Place of Performance:** Virginia Tech

***Project/Proposal Support Start Date: (MM/YYYY):** 12/2024

***Project/Proposal Support End Date: (MM/YYYY):** 11/2026

***Total Award Amount:** $300,000

*** Person Months (Calendar/Academic/Summer) per budget period Committed to the Project:**

Year	Person Months
2025	0.3
2026	0.3

***Overall Objectives:** Our goal is to broaden the participation of women in the tech industry by understanding and addressing challenges women job seekers face in technical interview settings.

***Statement of Potential Overlap:** This is the submitted proposal.

***Project/Proposal Title:** CCI: Understanding How Software Developers Secure User Interfaces in Rapid Release Environments (This Proposal)

***Status of Support:** pending

Proposal/Award Number:

***Source of Support:** Commonwealth Cyber Initiative

***Primary Place of Performance:** Virginia Tech

***Project/Proposal Support Start Date: (MM/YYYY):** 05/2024

***Project/Proposal Support End Date: (MM/YYYY):** 08/2024

***Total Award Amount:** $10,000

*** Person Months (Calendar/Academic/Summer) per budget period Committed to the Project:**

Year	Person Months
2024	0.5

***Overall Objectives:** Understand the current practices and challenges with securing user interfaces in rapid release software development environments.

***Statement of Potential Overlap:** N/A

***Project/Proposal Title:** CCI: Understanding User and Developer Perceptions of Dark Patterns in Software

***Status of Support:** pending

Proposal/Award Number:

***Source of Support:** Commonwealth Cyber Initiative

***Primary Place of Performance:** Virginia Tech

***Project/Proposal Support Start Date: (MM/YYYY):** 05/2024

***Project/Proposal Support End Date: (MM/YYYY):** 12/2024

***Total Award Amount:** $49,703

*** Person Months (Calendar/Academic/Summer) per budget period Committed to the Project:**

Year	Person Months
2024	1

***Overall Objectives:** Understand user and software developer perceptions of dark patterns in software designs.

***Statement of Potential Overlap:** N/A

***Project/Proposal Title:** Collaborative Research: EDU: Understanding Barriers in Technical Interview Settings and Training for Neurodiverse Candidates Joining the Tech Workforce

***Status of Support:** pending

Proposal/Award Number:

***Source of Support:** NSF

***Primary Place of Performance:** Virginia Tech

***Project/Proposal Support Start Date: (MM/YYYY):** 05/2024

***Project/Proposal Support End Date: (MM/YYYY):** 04/2027

***Total Award Amount:** $824,007

*** Person Months (Calendar/Academic/Summer) per budget period Committed to the Project:**

Year	Person Months
2024	1
2025	1
2026	1

***Overall Objectives:** We seek to understand barriers in technical interview settings and preparation techniques impeding neurodivergent candidates and engage with stakeholders to investigate awareness and mitigation techniques for these challenges.

***Statement of Potential Overlap:** This proposal also studies technical interviews for a different target group with a distinct approach. This proposal aims to take an asset-based approach to support neurodiverse job seekers in their preparation efforts for existing interview practices, whereas the submitted proposal focuses on women job seekers and aims to change current technical interview practices to make them more inclusive and promote gender fairness.

Certification:

When the individual signs the certification on behalf of themselves, they are certifying that the information is current, accurate, and complete. This includes, but is not limited to, information related to current, pending, and other support (both foreign and domestic) as defined in 42 U.S.C. §§ 6605. Misrepresentations and/or omissions may be subject to prosecution and liability pursuant to, but not limited to, 18 U.S.C. §§ 287, 1001, 1031 and 31 U.S.C. §§ 3729- 3733 and 3802.

Certified by Brown, Chris in SciENcv on 2024-03-05 12:12:58

References

[1] Jenkins. https://www.jenkins.io/.

[2] Travis CI. https://www.travis-ci.com/.

[3] I. Banerjee, B. Nguyen, V. Garousi, and A. Memon. Graphical user interface (gui) testing: Systematic mapping and repository. *Information and Software Technology*, 55(10):1679–1694, 2013.

[4] V. Clarke and V. Braun. Thematic analysis. *The journal of positive psychology*, 12(3):297–298, 2017.

[5] DevOpsDays. About devopsdays. https://devopsdays.org/about.

[6] DevOpsDays. Devopsdays baltimore. https://devopsdays.org/events/2024-baltimore/.

[7] GitHub. Automate your workflow from idea to production, 2022. https://github.com/features/actions.

[8] V. Kongsli. Towards agile security in web applications. In *Companion to the 21st ACM SIGPLAN symposium on Object-oriented programming systems, languages, and applications*, pages 805–808, 2006.

[9] V. Kongsli. Security testing with selenium. In *Companion to the 22nd ACM SIGPLAN conference on Object-oriented programming systems and applications companion*, pages 862–863, 2007.

[10] M. Nass, E. Alégroth, and R. Feldt. Why many challenges with gui test automation (will) remain. *Information and Software Technology*, 138:106625, 2021.

[11] J. Phillippi and J. Lauderdale. A guide to field notes for qualitative research: Context and conversation. *Qualitative Health Research*, 28(3):381–388, 2018. PMID: 29298584.

[12] Red Hat. Understanding devops. *Red Hat Blog*, 2022. https://www.redhat.com/en/topics/devops?cicd=32h281b.

[13] Selenium. https://www.selenium.dev/.

[14] M. Shahin, M. Ali Babar, and L. Zhu. Continuous integration, delivery and deployment: A systematic review on approaches, tools, challenges and practices. *IEEE Access*, 5:3909–3943, 2017.