

Department of Systemics

School Of Computer Science

UNIVERSITY OF PETROLEUM & ENERGY STUDIES,

DEHRADUN - 248007, Uttarakhand 

**MAJOR PROJECT**

**SYNOPSIS**

For

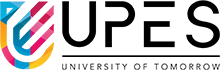
FlawFix: Identifying And Patching Security Flaws

Submitted By

| **Specialization** | **SAP ID** | **Name** |
| --- | --- | --- |
| CSF | 500096452 | Saurabh Kumar |
| CSF | 500098158 | Anmol Gulia |
| CSF | 500098081 | Vaibhav Patel |
| CSF | 500096628 | Aryaman Khare |

Dr. Akashdeep Bharadwaj Dr. Ajay Prasad

**Project Guide Cluster Head**



**School of Computer Science**

University of Petroleum & Energy Studies, Dehradun

**1. Project Title**

FlawFix: Identifying And Patching Security Flaws

**2. Abstract**

The increasing reliance on digital systems has led to a parallel rise in cyber threats, necessitating a proactive approach to identifying and mitigating security flaws. "FlawFix: Identifying and Patching Security Flaws" is a project aimed at creating a deliberately vulnerable operating system (OS) to simulate a variety of known security vulnerabilities. The project involves the development of this OS, the systematic exploitation of its vulnerabilities, and the implementation of effective remediation strategies. By addressing these flaws, the project seeks to enhance understanding of common security weaknesses and provide practical solutions to mitigate such risks in real-world systems.

**3. Introduction**

 Cybersecurity is a critical concern in today’s digital landscape, where the consequences of security breaches can be severe. Operating systems, being the backbone of digital infrastructure, are frequent targets for attackers seeking to exploit vulnerabilities. Understanding the nature of these vulnerabilities and how to effectively patch them is essential for building resilient systems. This project, "FlawFix: Identifying and Patching Security Flaws," aims to simulate real-world security challenges by creating a vulnerable OS, exploiting its weaknesses, and applying remediation techniques. The project will provide valuable insights into the lifecycle of security flaws—from identification to verification of remediations.

**4. Literature Review**

The exploration of security vulnerabilities and their mitigation is a well-documented area within cybersecurity research. [1] provides valuable insights into the dynamics of vulnerability management and highlights the critical role of systematic analysis in securing systems. [1] emphasizes the importance of timely detection and patching of vulnerabilities to minimize the window of opportunity for potential exploits. [2] provides the importance of awareness in mitigating cybersecurity attacks. [2] underscores the need for continuous monitoring and updating of systems to address emerging threats. Both studies collectively highlight the necessity of a thorough understanding of vulnerabilities and the implementation of timely remediation strategies, forming a strong foundation for the objectives of the "FlawFix" project.

**5. Problem Statement**

Operating systems are susceptible to a wide range of security vulnerabilities, many of which remain unpatched due to a lack of awareness or understanding. These vulnerabilities can be exploited by malicious actors, leading to significant damage and data loss. The problem lies in the difficulty of identifying these flaws and implementing effective remediation strategies before they can be exploited. This project addresses this issue by creating a vulnerable OS, deliberately exposing its weaknesses, and systematically applying patches to eliminate these flaws.

**6. Objectives**

* To develop an operating system with intentionally embedded security vulnerabilities.
* To exploit these vulnerabilities using various techniques to simulate potential real-world attacks.
* To analyze the exploited vulnerabilities to understand their impact on the system.
* To apply appropriate remediation strategies and document the process of patching the identified flaws.
* To evaluate the effectiveness of the patches in preventing future exploitation.

**7. Methodology**

1. **Development of Vulnerable OS:**

* Design and implement an operating system with a range of known security vulnerabilities, including but not limited to buffer overflows, SQL injections, and improper access controls.
* Use open-source tools and frameworks to embed these vulnerabilities in the OS.

1. **Vulnerability Exploitation:**

* Utilize penetration testing tools such as Metasploit, Nmap, and others to exploit the vulnerabilities.

1. **Vulnerability Analysis:**

* Analyze the impact & Identify the root cause of each vulnerability and categorize them based on their severity.

1. **Remediation and Patching:**

* Develop and implement patches to fix the identified vulnerabilities.
* Ensure that the patches address the root cause of each flaw and prevent further exploitation.

1. **Evaluation of Patches:**

* Re-test the system post-patching to ensure the effectiveness of the remediation.
* Assess the overall security of the system after the application of all patches.

**8.Pert Chart**

****

**9. References**

1. G. V. Marconato, V. Nicomette and M. Kaâniche, "Security-related vulnerability life cycle analysis," *2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS)*
2. Ö. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," *2017 International Conference on Cyberworlds (CW)*
3. National Vulnerability Database. <https://nvd.nist.gov/>
4. OWASP Top 10 Vulnerabilities <https://owasp.org/www-project-top-ten/>
5. Exploit DB <https://www.exploit-db.com/>