RESUNGA MULTIPLE CAMPUS

Independent Security Audit Proposal
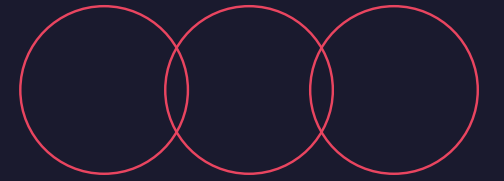
Presented by Anuj Panthi
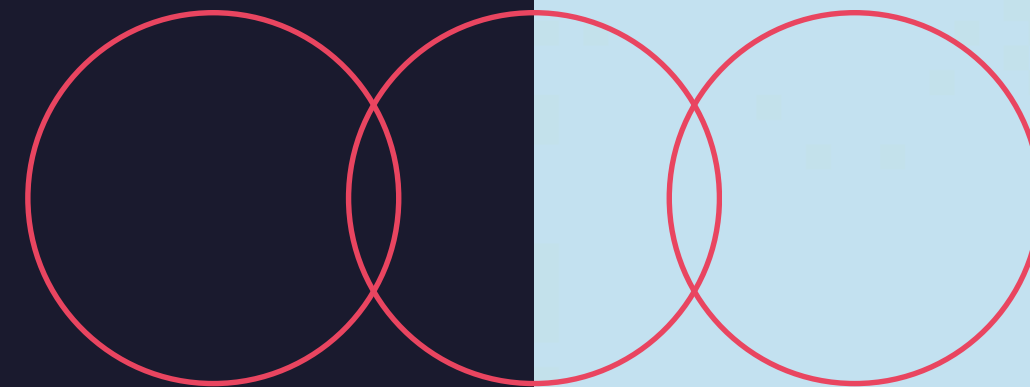
Purpose and Scope

Audit Objectives Defined

Identifying Weaknesses

The audit will focus on **detecting vulnerabilities** in internet-facing systems that could potentially be exploited, ensuring the security of the campus's publicly accessible services.

Strengthening Posture

By assessing the current security measures, the audit aims to **enhance resilience** against external threats, thereby improving the overall security posture of the Resunga Multiple Campus.

OSINT Techniques

Utilizing Open Source Intelligence (OSINT) allows for thorough data gathering, providing insights into potential weaknesses that may not be immediately visible through traditional security measures.

Methodology Overview

Reconnaissance
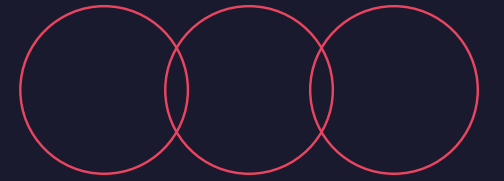
Scanning

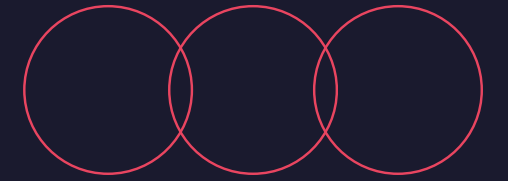## Vulnerability Detection

Gathering intelligence through OSINT, DNS queries, and subdomain discovery.

Identifying open ports, services, and technology stacks for assessment.

Conducting non-destructive tests to find injection flaws and misconfigurations.

Deliverables and Outcomes

Tangible benefits for campus

Executive Summary

A concise **overview of findings** will be provided, highlighting critical vulnerabilities and risks identified during the audit, enabling stakeholders to understand the current security posture quickly.

Vulnerability Report

A detailed report will include **CVSS risk classifications** for each vulnerability, allowing the client to prioritize remediation efforts based on the severity and potential impact of identified issues.

Attack Surface Map

A visual representation of the **external attack surface** will be delivered, outlining the components exposed to potential threats, which assists in comprehensively understanding security weaknesses and prioritizing mitigation strategies.

Legal and Ethical Compliance
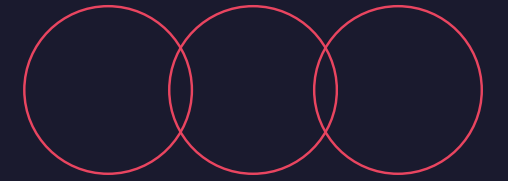
Ensuring integrity throughout audit

Authorized Testing

All audit activities are conducted **only with explicit authorization** from Resunga Multiple Campus, ensuring compliance with legal and ethical standards while protecting stakeholder interests during the assessment process.

Non-Intrusive Methods

The audit employs **external, non-destructive testing** techniques, focusing on publicly accessible systems to identify vulnerabilities without compromising system integrity or disrupting normal operations of the campus environment.

Confidentiality Assurance

Data collected during the audit will be handled with strict confidentiality in accordance with best practices, safeguarding sensitive information and aligning with established standards such as OWASP and NIST. Upon completion, a refined and non-sensitive version of the audit—containing only publicly permissible insights—may be published in the author's professional portfolio, with full credit attributed to Anuj Panthi.