Research Portfolio

Navid Fazle Rabbi
Security Researcher
Senior Offensive Security Engineer
bKash Ltd.

B. Sc. Engg. (EEE)
Islamic University of Technology (IUT)
Gazipur, Bangladesh

navidnaf.com | navidfazlerabbi@iut-dhaka.edu

"

Computer has always been my main interest. I was astonished by the dynamics it offered. Eventual knowledge gathering made me interested in **Cybersecurity**. Why? It's because you can deal with whatever you have related to computer and connected devices. So, as I got older, I realized the importance of Cybersecurity and its usage in every day of life.

After completing my bachelor's degree in **Electrical and Electronic Engineering** at **Islamic University of Technology (IUT)**, I knew that I wanted to specialize in cybersecurity. It wasn't until I discovered **Offensive Security Research** that I discovered my true passion in the field. I was attracted to the challenge of identifying flaws in complex web and mobile applications. The process of identifying and resolving these vulnerabilities requires a comprehensive understanding of how these applications work as well as a mix of technical expertise. I find it incredibly satisfying to be able to contribute to the security of these systems, which is like a fascinating puzzle that requires attention to detail.

As I learned more about offensive security research, I became interested in how **Automated** tools could help speed up the process of identifying and handling vulnerabilities. I started making my own tools and methods and sharing the security research community about them through my website and social media.

My passion for Offensive Security Research has played a key role in shaping my career. I am currently working as a **Senior Engineer in Offensive Security Research**, a position I was promoted to for my outstanding research excellence. In this position, I am in charge of research projects and work closely with other security experts to find and fix gaps in complex systems.

Over the years, I've had the chance to work on a wide range of projects, from making **Advanced Tools for Automated Vulnerability Identification and Management** to doing **Complex Penetration Testing** for **Enterprise-Level Applications**. My passion for **Offensive Security Research** has stayed the same through everything, and I am always looking for new challenges and chances to push the limits of what is possible in this field.

At the same time, I was getting better at **Secure Enterprise Architecture** by coming up with new **Methodologies** and Solutions to protect my organization's assets from cyber threats. I got several certifications, such as Certified Ethical Hacker, Certified in Cybersecurity, and Certified Payment Industry Security Implementor, to increase my knowledge and skills in the field.

Now that I have found something I am truly passionate about, cybersecurity, I want to further my education in the field. My ultimate career objective is to forge a successful career as a **Security Researcher** and make significant strides in the field of cybersecurity. I'm eager to continue learning from, collaborating with, and contributing to security research with top researchers and academics as I work on several ongoing projects, such as the creation of cutting-edge tools and techniques for automated vulnerability identification and management.

"

Table of Contents

Education

Islamic University of Technology (IUT)

Undergraduate | Bachelor of Science in Engineering (EEE)

Admission Rank 70 | Recipient of OIC Scholarship

Notable Course-works	• Communication Engineering • Microprocessor & Assembly Language • Wireless Communication • Micro-Controller Based System Design • Data Communication & Networking • Embedded Systems • Advanced Communication Techniques

In the year 2019, I graduated from the **Islamic University of Technology** with a **Bachelor of Science in Electrical and Electronic Engineering**. I was able to excel academically and gain experience in areas like determination, hard work, research methodology, and leadership through my participation in extracurricular activities.

Along with my academic success, I was able to hone my leadership and communication skills through my positions as **President** of **IUT Career & Business Society** and **Chair** of **IEEE IUT Student Branch**. The things I've learned have given me the confidence to go out and make a positive change in the world.

The electrical and electronic engineering skills I learned in university as well as through extracurriculars have been invaluable as I work toward a career in cybersecurity. As I continue my education in this field, I feel well-equipped thanks to my time at the Islamic University of Technology.

Work Experience

bKash Ltd.

bKash Ltd. is a leading provider of digital financial services in Bangladesh that has become an integral part of the daily lives of millions of people. Globally and locally, bKash has been recognized for its contributions to financial inclusion and social development since its founding in 2011. With its quick, simple, and secure digital transactions, bKash enables people to realize their dreams and advance the nation.

- **Senior Engineer, Offensive Security Research**

  May 2023 – Present

  Continuing as **Team Lead for Web Application, API, and Mobile Application Security Testing Team**, my new role incorporates the following:

  - ✓ Working with **ASMs** and **Red Team Operation Tools** to manage **attack surfaces** and **identify/resolve potential vulnerabilities**.
  - ✓ Conducting **Cloud Security Posture Management** to maintain a secure and compliant cloud infrastructure.
  - ✓ Performing **Cloud Penetration Testing** to identify and remediate vulnerabilities in cloud-based systems.
  - ✓ Implementing **ISO 27001:2022 security framework** to ensure compliance and improve information security.
  - ✓ Implementing **DevSecOps** to integrate CI/CD with **DASTs**, ensuring security throughout the software development lifecycle.
  - ✓ Implementing **IAST** for early detection and remediation of security vulnerabilities in the software development lifecycle, while continuously monitoring applications and providing guidance on best practices.

- **Engineer, Offensive Security & Compliance**

  April 2021 – April 2023

  As the **Team Lead for the Web Application, API, and Mobile Application Security Team**, my key responsibilities include:

  - ✓ Leading **Red Team Operations** to ensure the organization's **Cyber Resilience** against **APTs** using advanced offensive security tactics.

- ✓ Collaboration with **Vulnerability Management**, **Security Implementation**, and other security programs to exploit weaknesses and prioritize attack vectors in order to effectively identify the company's security defense deficiencies.
- ✓ **Developing and Implementing Exploits** for vulnerabilities in the bKash system and environment through **Penetration Testing** and **Offensive Security Techniques**.
- ✓ Conducting **Reverse Engineering** and **analyzing software and mobile applications** using information security best practices.
- ✓ **Programming and analyzing malware** for research and development purposes, with a focus on information security.
- ✓ Testing **cloud and scalable infrastructure** for vulnerabilities and implementing necessary **hardening measures** to ensure information security.
- ✓ **Analyzing and sanitizing source code** using information security guidelines.
- ✓ Performing **fraud analysis and detection** to protect against information security threats.
- ✓ Building **secured architecture to enhance cyber resilience**.
- ✓ Protecting against data loss through comprehensive information security measures.

Enterprise Tools Utilized

Burp Suite Professional (*Pentesting*), Postman (*Pentesting*), Genymotion (*Emulator*), Netsparker (*Web Application Vulnerability Scanner*), Tenable.io (*Cloud Vulnerability Management*), Tenable.sc (*Vulnerability Management*), SysDig (*Cloud Security Posture Management*), Mandiant Advanced (*Attack Surface Management*, *Cyber Threat Intelligence*), Randori (*Attack Surface Management*), MobSF (*Application Vulnerability Management*), Wireshark (*Packet Analyzer*), Core Impact (*Exploitation Framework*), Metasploit Pro (*Exploitation Framework*), etc.

Security & Governance Frameworks

OWASP Web Application Testing Guide, OWASP Mobile Application Testing Guide, NIST Cybersecurity Framework, ISO27001:2013, ISO27001:2022, COBIT2019

Research & Papers

Interest

The importance of strong cybersecurity cannot be overstated in our rapidly digitizing world where technology permeates every aspect of our lives. The importance of safeguarding our digital assets and privacy is becoming increasingly clear to me as I consider the consequences of a hyper-connected society. The urgency of bolstering cybersecurity measures is highlighted by the pervasiveness of cyber threats, which can range from sophisticated attacks on organizations to breaches of privacy on an individual level.

I see cybersecurity as a calling to protect the honesty of digital interactions and the privacy of personal information. The idea that we can create a world where ideas can thrive, businesses can prosper, and people can use technology without fear motivates me to devote so much time and energy to

My entire academic career has been fueled by my insatiable curiosity about the ever-evolving field of offensive security and how it interacts with cutting-edge tools. To further my goal of expanding the boundaries of cybersecurity, I have zeroed in on three key areas: Artificial Intelligence, Blockchain Technology, and the Web3. In this section.

Offensive Security

Because of the ever-changing nature of the threats and the pressing need for novel approaches to security, the field of offensive security holds my interest. The ability to get inside the heads of adversaries and proactively secure systems from threats fascinates me. As I learn more about offensive security, one of my goals is to improve my knowledge of vulnerability assessment, penetration testing, and threat intelligence in order to better protect businesses.

Cybersecurity & AI

Integrating AI into cybersecurity could completely change the game. Making smart systems that can spot anomalies and fix themselves thrills me. I'm excited to work on creating AI-powered solutions for robust digital ecosystems. My fascination with Cybersecurity & AI has grown as I learn more about the importance of protecting AI systems like ChatGPT and Bard. I will do what I can to ensure that our technological future is safe.

Blockchain Security

Despite the widespread disruption that blockchain technology has wrought, it also comes with its own set of security risks. Consensus algorithms, smart contract vulnerabilities, and decentralized governance are all areas of blockchain security that pique my interest. My research in this area is motivated by a desire to strengthen decentralized system underpinnings and promote trustless, secure communication.

Web3 and Decentralized Applications (DApps)

Web3 is the next generation of the internet; it is user-driven, collaborative, and decentralized. As I learn more about Web3 and DApps, I hope to aid in the creation of privacy-conscious, cross-platform apps that give users agency over their digital lives and reshape the way we interact online.

Skillset

High Level Programming Language	Python, JavaScript, PHP
Systems Programming Language	C
Scripting Language	Bash, cURL
Low Level Programming Language	Assembly Language
Web Development	HTML, CSS
Database Query Language	SQL
Relational Database	MySQL, SQLite3
NoSQL Database	MongoDB
In Memory Database	Redis
API Testing & Development	Postman, GraphQL
Penetration Testing & Security Tools	Burp Suite Professional, Burp Suite Enterprise, Acunetix, Netsparker, mitmproxy, OWASP Zap
Mobile Application Analysis	apktool, MobSF
Reverse Engineering	radare2, Ghidra, IDA Pro
Digital Forensics	Autopsy
Cloud Environments	AWS
Cloud & Vulnerability Management	Tenable.io, Tenable.sc, SysDig, AquaSec
Attack Surface Management & Cyber Threat Intelligence	Mandiant Advanced, Randori
Network & Packet Analysis	Wireshark
Exploitation Framework	Core Impact, Metasploit
Containerization & Orchestration	Docker, Kubernetes
Configuration Management	YAML

Productivity & Project Management	Microsoft Office Suite, Adobe Illustrator, Adobe Premiere Pro, Adobe After Effects, Adobe Photoshop, Trello, Jira, Confluence, Notion
Version Control & CI/CD	git, Jenkins
Monitoring & Analytics	Grafana

Undergraduate Thesis

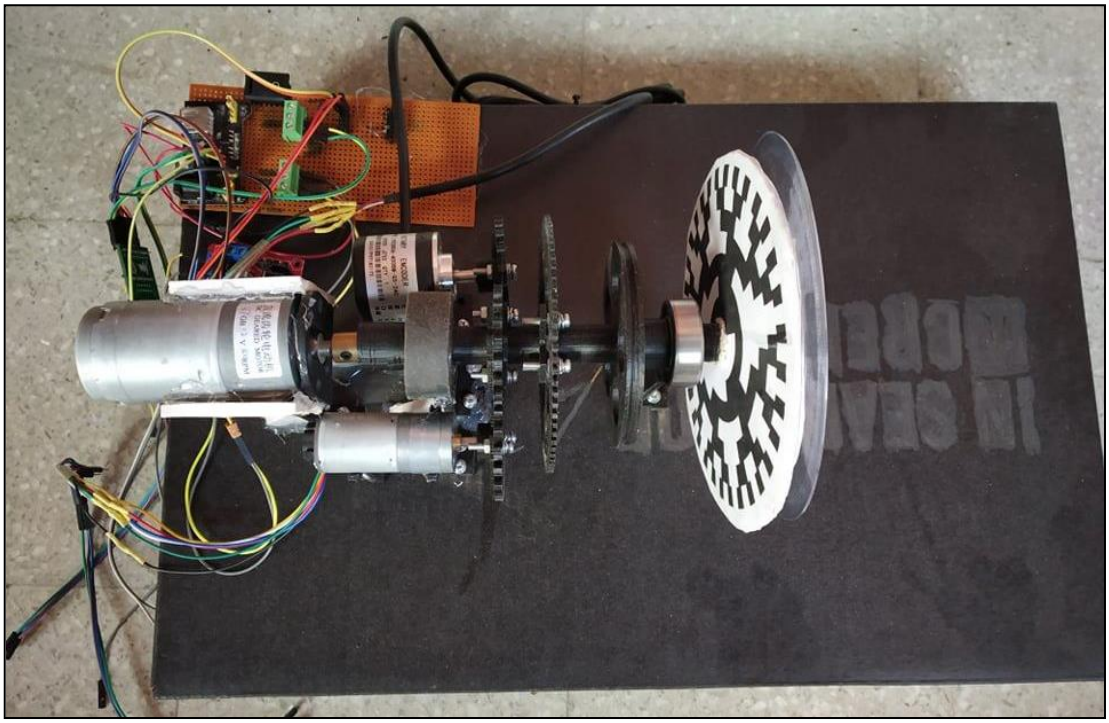
Design and Implementation of Server Based Position and Angle Measurement and Control of DC Motor

Institutional Repository

Supervisor:

Dr. Golam Sarowar
Professor, Electrical & Electronic Engineering (EEE)
Profile | Google Scholar

The undergraduate thesis project focuses on developing a server-based system to accurately measure and control the position and angle of a DC motor. The research involves **hardware schematic design**, **user interface development**, **JSON data parsing for calculations**, and **real-time communication between the server and the machine**.



How it Works

- ✓ **Hardware Schematic Design & Assemble**
  A Hardware design schematic was created. It was made by gathering and assembling the necessary hardware components. The incremental rotary encoders along with appropriate sensors were linked.

- ✓ **User Interface Development**
  To control the interaction between the Server and the Machine, a graphical interface was created that, enabled the machine to send requests to the server in JSON format, specifying the required measurements or control actions, and the sensor data.

- ✓ **Server Processing**
  After the server received the request, it processed the sensor data and made the results available for viewing. We would make adjustments to the information and retransmit it to the computer if necessary.

- ✓ **Real-Time Communication**
  The communication between the server and the machine was in real time. After receiving the response, the machine can immediately implement the changes to adjust the motor's behavior accordingly.

How it Helps

- ✓ Precise Position and Angle Measurement
- ✓ Real-Time Control
- ✓ User-Friendly Interface

Technologies Utilized

The thesis employs the following technologies:

- ✓ Hardware Components: Rotary incremental encoders and relevant sensors
- ✓ JSON Data Formatting
- ✓ Python (PyQT, Requests Module)
- ✓ Server Technologies: Python (Flask)

Preprint

Design, Implementation, Comparison, and Performance analysis between Analog Butterworth and Chebyshev-I Low Pass Filter Using Approximation, Python and Proteus

Access | Code Repository

The research paper focuses on the design, implementation, comparison, and performance analysis of Analog Butterworth and Chebyshev-I Low Pass Filters. These filters play a crucial role in signal processing and communication systems. The study involves manual calculations using approximations, verification with Python programming language, simulation in Proteus 8 Professional, and practical implementation in the Hardware Lab using necessary components.

How it Works

- ✓ **Design and Implementation of Filters**
  Both Butterworth and Chebyshev-I Low Pass Filter circuits are designed and implemented in the research. The design process includes determining the required filter specifications, such as cutoff frequency and order, based on the application's requirements.

- ✓ **Manual Calculations and Approximations**
  The research employs manual computations and approximations to derive the filter characteristics and transfer functions for both Butterworth and Chebyshev-I filters. These calculations serve as a reference for later comparisons and performance analysis.

- ✓ **Verification with Python**
  To ensure accuracy and correctness, the filters' theoretical calculations are verified using Python programming language. Python code is written to simulate the filter responses and observe their behavior under various input conditions.

- ✓ **Simulation in Proteus 8 Professional**
  The designed filters are further simulated in Proteus 8 Professional, a widely used simulation software for electronic circuits. This step helps validate the filters' performance and provides insights into their behavior in different scenarios.

- ✓ **Hardware Implementation**
  The next phase involves the practical implementation of Butterworth and Chebyshev-I filters in the Hardware Lab. Necessary electronic components are used to construct the analog filter circuits.

How it Helps

- ✓ **Design and Implementation of Analog Filters**
  The study provides a comprehensive understanding of the design and practical implementation of both Butterworth and Chebyshev-I Low Pass Filters.

- ✓ **Comparison of Theory and Simulation**
  By comparing the theoretical calculations, Python simulations, and Proteus simulations, the research highlights the consistency and accuracy of the filter designs.

- ✓ **Python Code for Filter Simulation**
  The Python code developed during the research allows researchers and engineers to simulate and analyze the filters easily.

Key Technical Takeaways

The primary objective of the research is to accurately develop, execute, compare, and assess Butterworth and Chebyshev-I filters. It explores the filters' performance in both hardware and software domains and their suitability for various applications in signal processing and communication systems.

Technologies Used

The research utilizes the following technologies:

- ✓ **Analog Circuit Design:** Techniques for designing Butterworth and Chebyshev-I Low Pass Filter circuits.
- ✓ **Python Programming Language:** Used for verification and simulation of the filters' behavior. NumPy, SciPy, Matplotlib.
- ✓ **Proteus 8 Professional:** Employed for circuit simulation and analysis.

Undergraduate Projects

- ### Design and Hardware Implementation of Calculator using Basic Logic Circuits

  2nd Semester Project

  The project focuses on the design and hardware implementation of a calculator using basic logic circuits. The objective is to create a functional calculator that can perform arithmetic operations using electronic components and logic circuits. The calculator will be capable of handling addition, subtraction, multiplication, and division operations.

  Technologies Used

  - ✓ **Basic Logic Circuit Design:** This involves designing the logic circuits for various arithmetic operations, including addition, subtraction, multiplication, and division, using logic gates and combinational circuits.
  - ✓ **PCB Design and Implementation:** After designing the logic circuits, a printed circuit board (PCB) is designed to integrate and interconnect all the electronic components efficiently.

- ### RaspberryPi Security Camera Network

  4th Semester Project | Project

  The project builds a Raspberry Pi-based security camera system that captures HD video when motion is detected. It offers live streaming on web browsers and mobile devices, records motion events as video files, and utilizes cloud storage for media. Users can access the camera feed remotely from any location, enhancing security and monitoring capabilities.

  Technologies Used

  - ✓ **Raspberry Pi:** The core component of the security camera system, responsible for capturing and processing video, as well as running the necessary software applications.
  - ✓ **HD Camera Module:** An HD camera module is used to capture high-quality video footage of the monitored area.
  - ✓ **Motion Detection Algorithms:** Software algorithms are employed to detect motion in the camera's field of view, triggering video recording when movement is detected.
  - ✓ **Web Streaming:** The system incorporates web streaming technology to enable users to access a live video feed from the camera using any web browser.
  - ✓ **Cloud Storage:** Cloud storage services are used to store captured photos and videos, providing a secure and accessible storage solution.

- **Energy Conversion: Python Implementation for – IV Curve Calculation, Maximum Power Point Tracking, Incremental Conductance**

  5th Semester Course-work | Code Repository | Project

  The project focuses on implementing various algorithms for solar photovoltaic (PV) modules using Python programming. The project covers concepts such as IV curve calculation, Maximum Power Point Tracking (MPPT), and Incremental Conductance in the context of solar PV technologies. The implementation involves modeling an electromechanical system and applying the principles of energy balance equations to simulate solar cell applications. This was my attempt to use Python programming to put together a few algorithms for solar PV modules. This wasn't required, but it was done because it was interesting.

  Technologies Used

  ✓ **Python Programming Language:** Python is the primary programming language used for implementing the algorithms related to IV curve calculation, MPPT, and Incremental Conductance for solar PV modules. Frameworks used: pvlib, pandas, matplotlib

- **Prospects of Energy Harvesting in Three Different Sectors (Cycling, Running, Sewing Machines) in Bangladesh**

  6th Semester Project

  Increasing the use of green energy will require a more strategic way to store the energy we use every day. This study looks at how bicycles, running, and hand sewing machines can be used to collect energy. Bicycles have been used as an example and the possibilities have been looked at. The initiative has led to a big increase in the amount of energy collected, giving people more options as they look for sustainable green energy.

- **Speech Recognition using MATLAB**

  7th Semester Project

  The project focuses on developing a voice recognition system using MATLAB. The objective is to create a recognizer capable of identifying individuals based on their speech patterns. The system takes voice inputs, evaluates the characteristics of the speech using Voice Features software, and displays the resulting data. It compares the extracted voice characteristics with the information stored in a database containing previously saved voice samples to determine the person's identity.

  Technologies Used

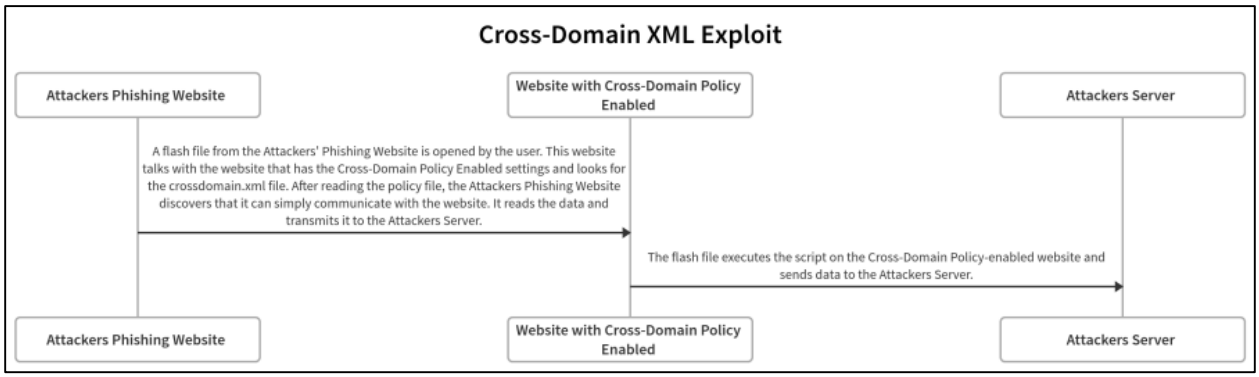
  ✓ **MATLAB:** MATLAB is the primary programming platform used to develop the speech recognition system. It provides tools and functionalities for signal processing, feature extraction, and data analysis.

Security Research & Developments

CrossDomain XML Exploit

Exploit	Action Script, Python	Exploit | Document | Blog

The Cross-Domain XML Exploit showcases how misconfigured crossdomain.xml files can be exploited to compromise sensitive data in Flash-like browsers. This attack takes advantage of the same-origin policy to gain unauthorized access to restricted resources. The research provides insights into the potential security risks posed by improperly configured cross-domain policies.



How it Works

- ✓ **Creating a Phishing Website**
  Attackers set up a phishing website containing a malicious Flash file. Unsuspecting victims access this website, unknowingly initiating the attack.

- ✓ **Identifying crossdomain.xml File**
  The malicious Flash file scans the victim's system for the presence of a crossdomain.xml file. This file governs cross-domain access policies for the targeted website.

- ✓ **Connecting with Targeted Website**
  Upon locating the crossdomain.xml file, the phishing website attempts to connect with the targeted website, utilizing the Cross-Domain Policy Activated settings.

- ✓ **Data Exfiltration**
  After reviewing the crossdomain.xml file, the attackers' phishing website gains access to restricted resources on the targeted website. It then reads sensitive data and transmits it to the attackers' server without the victim's knowledge or consent.

How it Helps

This research sheds light on the potential risks associated with misconfigured crossdomain.xml files. By demonstrating the exploitation of such misconfigurations, it underscores the importance of properly configuring cross-domain policies to safeguard sensitive data and prevent unauthorized access. The research serves as a cautionary demonstration of the consequences of misconfigured crossdomain.xml files, urging website administrators to implement secure cross-domain policies to protect their users' sensitive data.

Key Technical Takeaways

- ✓ **Understanding Cross-Domain Policy Vulnerabilities**
  The research highlights the risks posed by improperly configured crossdomain.xml files and the implications for data security.

- ✓ **Security Implications in Flash-like Browsers**
  The attack exploits the same-origin policy in Flash-like browsers, drawing attention to potential vulnerabilities in these environments.

- ✓ **Importance of Secure Cross-Domain Policies**
  Properly configuring cross-domain policies is crucial to prevent unauthorized access and data exfiltration.

Technologies Used

The Cross-Domain XML Exploit utilizes the following technologies:

- ✓ **Flash:** The malicious Flash file is the primary tool for initiating the attack and interacting with the targeted website.
- ✓ **Python:** A Python web server is used to host the phishing website and deliver the malicious content to victims.
- ✓ **ActionScript:** The "crossDomainExploit.as" file contains the ActionScript code used to render the SWF file and execute the attack.

Fraud Impersonation: Business Logic Flaw in bKash iOS Application

Fraud Reference: Scamming from a quiet village | Patronized by **bKash Offensive Security Research**

High Level Overview

The bKash Mobile App can only be used with the SIM card that was used to create the account, and cannot be used in any other device. However, unlike Android devices, iPhones do not have a SIM verification feature, so the application's attempts to deliver on the promise of its Business Logic fall flat. The vulnerability is being exploited in fraudulent activities.

Through the investigation, we were able to impersonate fraudsters and offer suggestions for how to stop it.

What has been described so far is a high-level synopsis of the problem and its resolution. The Confidentiality Agreement prohibits disclosing any specifics about the solution.

dl_bfb (Authentication Brute-Force)

Tool	Python	Tool

The dl_bfb tool is a powerful authentication brute-force attacker designed to perform brute-force attacks on servers with username and password-based authentication. Leveraging Python and various algorithms, the tool takes a CSV file containing usernames and passwords as inputs and systematically generates authentication attempts using JSON payloads. It targets application/JSON content type forms connected to a specified URL and is equipped with the DarkLord_BruteForceBomb dictionary for enhanced attack capabilities.

How it Works

- ✓ **Input Data**
  The tool takes a CSV file as input, containing a list of usernames and corresponding passwords for the brute-force attack.

- ✓ **Target Selection**
  The user specifies the target URL, which represents the server with the form to be attacked.

- ✓ **Brute-Force Attack**
  dl_bfb systematically generates combinations of username and password pairs from the provided CSV file. It then sends these combinations as JSON payloads to the specified URL for authentication attempts.

- ✓ **Content Type Restriction**
  The tool exclusively operates with the application/JSON content type, limiting its applicability to JSON-based applications.

How it Helps

- ✓ **Efficient Brute-Force Attacks**
  By leveraging Python's capabilities and efficient algorithms, dl_bfb facilitates swift and effective brute-force attacks on username and password-based authentication systems.

- ✓ **Vulnerability Identification**
  Through simulated attacks, the tool helps identify weaknesses in authentication mechanisms, enabling organizations to bolster security measures.

Key Technical Takeaways

- ✓ **Python for Web-Based Attacks**
  Understanding Python's suitability for web-based attack tools, showcasing its potential for handling HTTP requests and responses.

- ✓ **Brute-Force Algorithm Design**
  Learning about the algorithmic design that powers dl_bfb's systematic generation of username and password combinations.

- ✓ **JSON Payload Construction**
  Insight into the structure and content of JSON payloads used in the authentication attempts.

Technologies Used

The dl_bfb tool leverages the following technologies:

- ✓ **Python:** The primary programming language for building the tool's functionality and interacting with web servers. Requests Module.
- ✓ **Algorithms:** Various algorithms are employed to generate and handle the combinations of username and password pairs.
- ✓ **CSV File Handling:** The tool utilizes CSV file reading and parsing techniques to extract input data.
- ✓ **JSON:** JSON is used for constructing authentication payloads sent to the targeted server.

Knock! Knock! (Subdomain & Directory Enumerator)

Tool	Python	Tool | Blog

Knock! Knock! is a powerful enumeration tool specifically designed to fuzz and identify probable directories or subdomains on a target website. Written in Python, the tool employs a systematic method of enumeration to discover potential subdomains and directories, assisting security professionals in identifying potential attack vectors.

How it Works

- ✓ **Attacker Initiation**
  The security professional launches the tool as the attacker, providing the target domain as the input for enumeration.

- ✓ **Fuzzing List**
  The tool employs a pre-defined fuzzing list, containing a comprehensive set of common subdomains and directory names. These names are systematically appended to the target domain during the enumeration process.

- ✓ **Repeat Fuzzing**
  Knock! Knock! systematically fuzzes through the entire list of subdomains and directories, generating possible combinations for the target domain.

- ✓ **Probable Subdomains/Directories List**
  After repeated fuzzing attempts, the tool generates a list of potential subdomains and directories that are likely to exist on the target website.

How it Helps

- ✓ **Discovery of Hidden Attack Vectors**
  By systematically fuzzing for subdomains and directories, the tool helps security professionals discover potential hidden entry points for attackers.

- ✓ **Identification of Vulnerable Areas**
  The enumeration process assists in identifying vulnerable subdomains or directories that could lead to potential security risks.

- ✓ **Enhancing Security Posture**
  Knock! Knock! empowers organizations to enhance their security posture by proactively identifying and securing potential weak spots.

Key Technical Takeaways

- ✓ **Enumeration Methodology**
  Understanding the systematic approach to fuzzing for subdomains and directories.

- ✓ **Python Implementation**
  Insight into the usage of Python programming language for building the enumeration tool.

- ✓ **Fuzzing List**
  The significance of a comprehensive fuzzing list containing common subdomain and directory names.

Technologies Used

The Knock! Knock! enumeration tool leverages the following technologies:

- ✓ **Python:** The core functionality of the tool is implemented using Python programming language.
- ✓ **Fuzzing Techniques:** The tool employs fuzzing techniques to systematically generate subdomains and directories for the target domain.

Cookie Monster (Automated Cookie/Session Modifier)

Tool	Python	Tool | Blog

Cookie Monster is a powerful automated tool designed to test various cookie manipulation-based security flaws. It specifically targets HTTP cookies and session storage, aiming to assess the security of web applications against cookie poisoning attacks. Developed in Python using Selenium, the tool enables security professionals to identify and mitigate potential cookie-related vulnerabilities.

How it Works

The tool employs Selenium's web automation capabilities to manipulate cookies and session storage during security testing. The algorithmic process includes the following steps:

- ✓ **WebDriver Setup**
  The tool configures the web driver (in this case, Firefox) to automate the web browsing process and interact with the targeted web application.

- ✓ **Collecting Username & Password**
  The tool collects the username and password from a legitimate user during the login process. This allows for automated login sessions later.

- ✓ **Automating Login Session**
  Cookie Monster attempts to automate the login session using the provided legitimate user credentials. This step ensures the tool operates within the context of a real user.

- ✓ **Collecting Cookie/Session Storage**
  Upon successful login, the tool captures the generated cookie or session storage data associated with the user's session.

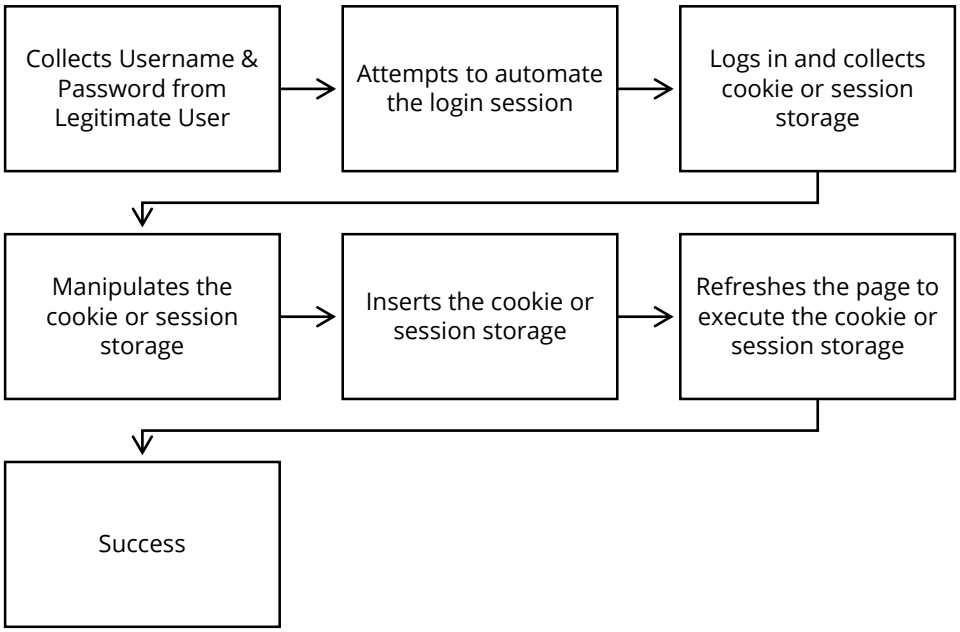
- ✓ **Cookie/Session Manipulation**
  Cookie Monster manipulates the collected cookie or session storage values, simulating different scenarios to test for potential security flaws.

- ✓ **Removing Existing Cookie/Storage**
  Cookie Monster removes the existing user-related cookie or local storage data using JavaScript. This step clears any previously set values.

- ✓ **Inserting Modified Cookie/Storage**
  The tool inserts the modified cookie or session storage values back into the web application.

- ✓ **Refresh and Execute**
  To execute the modified cookie or session storage, Cookie Monster refreshes the page. This allows the tool to observe how the web application behaves with the altered data.

- ✓ **Success Evaluation**
  Cookie Monster evaluates the web application's response to the manipulated cookie or session storage data to determine if potential security vulnerabilities are present.



How it Helps

- ✓ **Security Assessment**
  The tool automates the process of cookie and session manipulation, enabling security professionals to perform comprehensive security assessments. By testing various scenarios, the tool helps identify potential cookie-related vulnerabilities and session manipulation flaws.

- ✓ **Vulnerability Detection**
  Cookie Monster's automated approach aids in detecting cookie poisoning and session storage issues that could lead to unauthorized access or data exposure. By simulating attack scenarios, the tool assists in pinpointing security weaknesses in web applications.

- ✓ **Proactive Mitigation**
  Identifying and understanding potential cookie manipulation risks empowers organizations to take proactive measures in securing their web applications. By mitigating vulnerabilities, they can enhance the overall security posture and protect user data.

- ✓ **Real User Simulation**
  The tool's ability to collect and use legitimate user credentials ensures that the tests are performed in a realistic user context. This allows for accurate assessment of security controls and user interactions.

- ✓ **Efficiency and Accuracy**
  Cookie Monster's automation reduces the manual effort required for security testing, increasing efficiency and accuracy in identifying security flaws.

Key Technical Takeaways

- ✓ **Selenium Web Automation**
  Understanding how Selenium's capabilities are utilized to automate the login session and interact with the web application.

- ✓ **JavaScript Execution**
  Cookie Monster uses JavaScript to manipulate and insert modified cookie or session storage data.

- ✓ **Security Testing Focus**
  The tool is tailored to identify and test cookie poisoning and session manipulation vulnerabilities.

Technologies Used

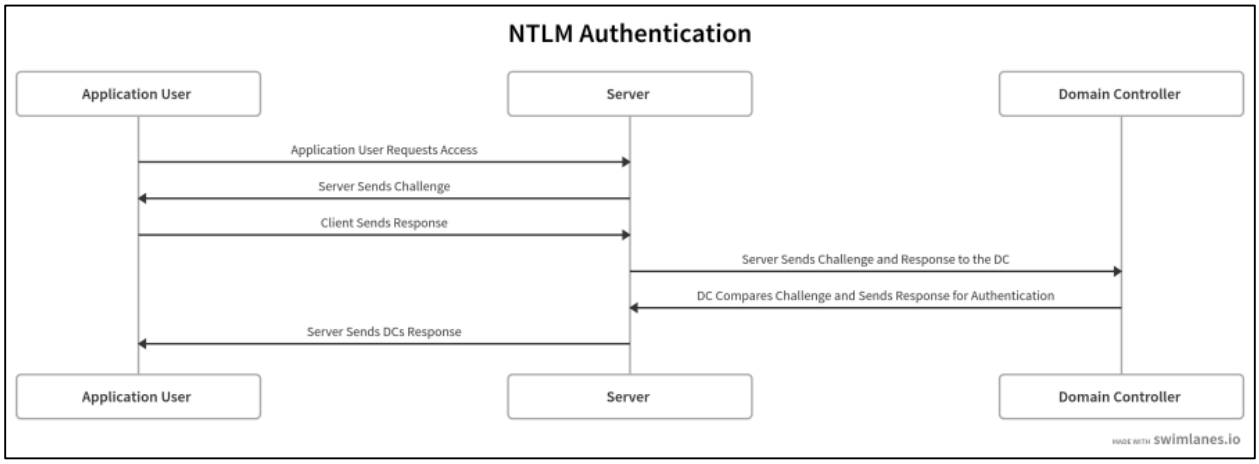
The Cookie Monster tool relies on the following technologies:

- ✓ **Python:** The tool is developed in Python to implement the automation and manipulation functionalities. Cookie Monster utilizes the following library dependencies: selenium, time, maskpass, and pyfiglet.
- ✓ **Selenium:** Selenium is used for web automation, allowing Cookie Monster to interact with the web application and execute JavaScript.

NTLM_Spray (Password Sprayer)

Tool	Python	Tool | Blog

NTLM_Spray is a specialized password spraying tool designed for enumerating usernames on Microsoft's Windows New Technology LAN Manager (NTLM) authentication system. NTLM is a security protocol that enables single sign-on (SSO) and verifies user identities without directly requesting passwords. To avoid triggering account lockouts in Active Directory (AD) environments, NTLM_Spray adopts a password spraying technique. Instead of attempting multiple passwords, the tool selects one password and tests it across a list of usernames to retrieve valid login credentials.



How it Works

✓ **Attacker Initiation**
The tool is operated by the attacker, who sets up and configures the NTLM_Spray parameters.

✓ **Spraying List**
NTLM_Spray requires a list of usernames to target during the password spraying attack. This list serves as the input for the tool's spraying process.

✓ **Repeat Spraying**
The tool systematically sprays the chosen password across the entire list of usernames. It applies the password in a controlled manner to avoid triggering account lockouts.

✓ **Success Evaluation**
NTLM_Spray monitors the responses from the NTLM authentication system. If the spraying attempt is successful, valid login credentials are retrieved, indicating a potential target username.

How it Helps

✓ **Password Enumeration**
By using password spraying, the tool efficiently enumerates valid usernames on NTLM-based systems without triggering account lockouts.

✓ **Account Discovery**
NTLM_Spray assists security professionals in discovering valid accounts, which is crucial for identifying potential security risks and unauthorized access.

✓ **Efficient Testing**
The tool employs a controlled approach to spraying passwords, reducing the risk of account lockouts and enabling efficient security testing.

Key Technical Takeaways

✓ **Password Spraying Technique**
Understanding the concept of password spraying, where one password is systematically tested across multiple usernames.

✓ **Account Lockout Avoidance**
The tool's controlled approach ensures that account lockouts are prevented, making it a safer alternative to brute-force attacks.

Technologies Used

NTLM_Spray is developed using the following technologies:

✓ **Python:** The tool is written in Python, which enables efficient and flexible scripting for password spraying.

Base64 Brute-Force

Tool	Python	Tool | Blog

The Base64 Brute-Force tool is designed to perform efficient brute-forcing on services that utilize Base64 encoding for username and password authentication. Some services employ Base64 encoding to filter and secure login credentials transmitted over the Authorization request headers. This tool reads usernames and passwords from a dictionary, encodes them in Base64, and then utilizes the encoded data in the Authorization header to perform successful brute-force attacks.

How it Works

- ✓ **Importing Username & Password List**
  The tool reads a list of usernames and passwords from a dictionary file in .txt format. This list serves as the input data for the brute-force attack.

- ✓ **Base64 Conversion**
  The tool takes each username and password pair from the dictionary and converts them to their respective Base64 encoded forms. This encoding ensures secure transmission over the Authorization request headers.

- ✓ **Authorization Header Usage**
  After Base64 encoding the username and password combinations, the tool uses the encoded data in the Authorization header of the HTTP GET request. This enables the tool to attempt brute-force attacks with the encoded credentials.

- ✓ **Performing Brute-force**
  The Base64 Brute-Force tool systematically iterates through the dictionary's username and password combinations. For each combination, it constructs the Authorization header with the corresponding Base64 encoded data and sends the GET request to the target service, attempting to log in.

Dependencies

The Base64 Brute-Force tool has the following dependencies:

- ✓ **Dictionary Files:** The dictionary files should be in .txt format, containing lists of usernames and passwords for the brute-force attack.
- ✓ **GET Request:** The tool currently supports only GET requests in this version.

How it Helps

- ✓ **Efficient Base64 Brute-Forcing**
  By employing Base64 encoding, the tool ensures secure transmission of login credentials and performs efficient brute-forcing on services with filtered usernames and passwords.

- ✓ **Enhanced Security Testing**
  The tool assists security professionals in identifying vulnerabilities and weaknesses in services that rely on Base64 encoded authentication.

- ✓ **Automated Approach**
  Base64 Brute-Force automates the process of testing numerous username and password combinations, saving time and effort during security assessments.

Key Technical Takeaways

- ✓ **Base64 Encoding**
  Understanding the significance of Base64 encoding for secure transmission of login credentials.

- ✓ **HTTP Authorization Header**
  Utilizing the Authorization header in HTTP GET requests to test brute-force attempts with Base64 encoded credentials.

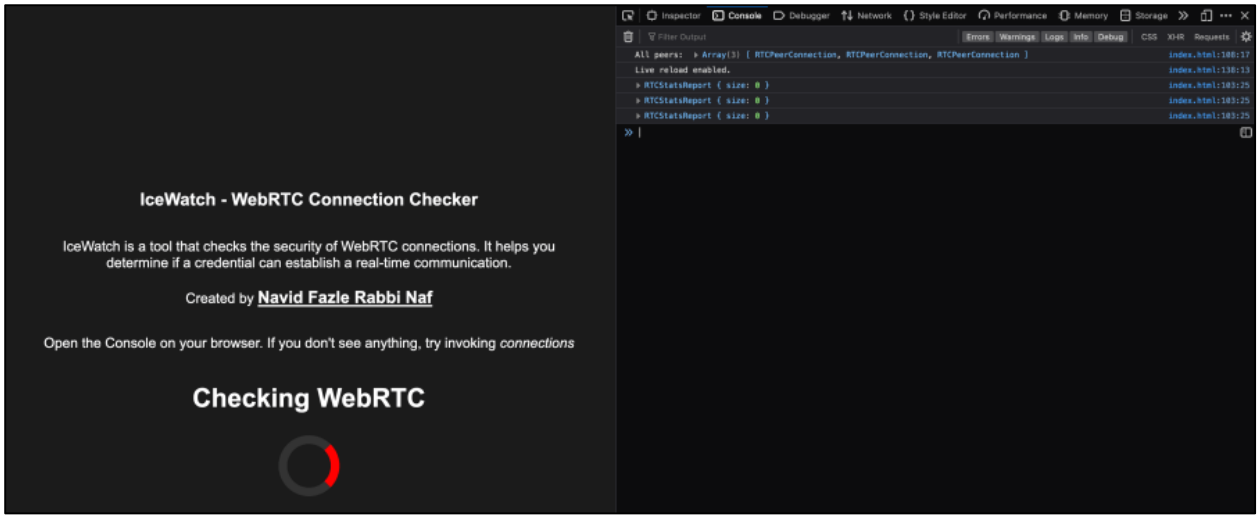
Technologies Used

The Base64 Brute-Force tool leverages the following technologies:

- ✓ **Python:** The tool is developed in Python, enabling efficient handling of dictionary files and Base64 encoding.

Ice Watch (WebRTC Connection Checker)

Tool	HTML, JavaScript	Tool | Blog



IceWatch is a vital tool designed to prevent potential credential leaks and ensure the security of WebRTC connections. Leveraging JavaScript and the RTCPeerConnection API, the tool examines WebRTC connection setups using provided credentials and logs the status of each connection. It plays a critical role in safeguarding communication links and preventing unauthorized access to sensitive information.

How it Works

✓ **WebRTC Connection Setup Check**
The tool examines the setup of WebRTC connections using the provided credentials. It thoroughly analyzes the configuration to detect any potential security flaws or unauthorized access.

✓ **Connection Logging**
IceWatch establishes multiple connections and meticulously logs the status of each connection. By recording all connected peers, it enables in-depth analysis of communication links for any signs of unauthorized access.

How it Helps

✓ **Credential Leak Prevention**
By utilizing JavaScript and RTCPeerConnection, IceWatch ensures the prevention of credential leaks, safeguarding sensitive credentials from exposure.

✓ **Proactive Security Measures**

With real-time connection checks, IceWatch enables the organization's Red team to proactively identify and address potential security concerns, strengthening the overall security posture.

✓ **Early Detection of Unauthorized Access**
Through detailed logging and analysis, IceWatch facilitates the early detection of unauthorized access attempts, empowering quick revocation of access and protection of sensitive data.

Key Technical Takeaways

✓ **WebRTC and RTCPeerConnection API**
Understanding the critical role of JavaScript and the RTCPeerConnection API in examining WebRTC connection setups.

✓ **Real-time Analysis**
The significance of real-time connection checks to identify and address security vulnerabilities promptly.

Technologies Used

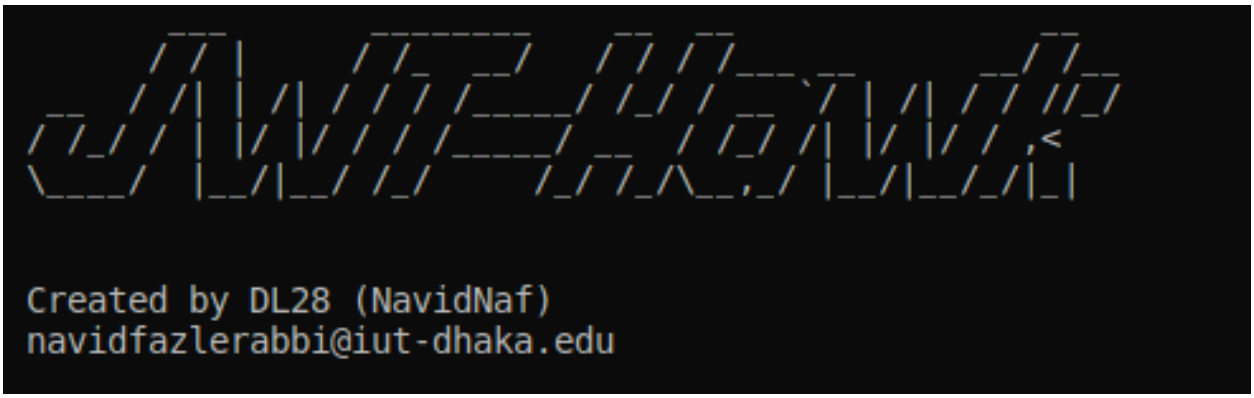
IceWatch leverages the following technologies:

✓ **JavaScript:** The core functionality of the tool is implemented using JavaScript, allowing for comprehensive analysis of WebRTC connections.

✓ **RTCPeerConnection API:** IceWatch utilizes the RTCPeerConnection API to interact with WebRTC connections, enabling thorough examination and logging.

JWT Hawk (JSON Web Token Decoder)

Tool	Python	Tool | Blog



JWT-Hawk is a powerful Python tool that assists in decoding JWT tokens by attempting multiple secrets from a provided list. It proves beneficial for individuals who need to decode JWT tokens but lack the secret information. The tool extracts and prints the header and payload values of a given JWT token, provided that the secret matches. To use JWT-Hawk, users can clone the repository, install the necessary dependencies, and create a file containing the secrets to be tried for decoding.

How it Works

- ✓ **Prepare Secrets File**
  Create a file containing a list of secrets that you want to try for decoding the JWT token.

- ✓ **Run the Script**
  Execute the JWT-Hawk script by running: python3 jwt_hawk.py <secrets_file> where <secrets_file> is the name of the file containing the secrets.

- ✓ **Provide JWT Token**
  Enter the JWT token when prompted by the tool.

- ✓ **Decoding Attempt**
  JWT-Hawk will proceed to decode the JWT token using each secret from the provided list. If a match is found, the tool will display the header and payload values, along with the decoded signature.

How it Helps

- ✓ **Enhanced Security Assessment**
  The tool aids security professionals in identifying potential vulnerabilities and weaknesses in JWT token security, empowering proactive measures to safeguard sensitive data.

✓ **Quick Detection of Unauthorized Access**
JWT-Hawk swiftly detects unauthorized access attempts by continuously trying different secrets, enabling prompt revocation of access and protection of sensitive information.

✓ **Real-World Application**
JWT-Hawk is valuable for red teams and security analysts engaged in ethical testing of systems and web applications, helping to ensure the integrity and confidentiality of JWT-based authentication.

Key Technical Takeaways

✓ **Efficient JWT Token Decoding**
The tool automates the process of decoding JWT tokens using a list of potential secrets, saving time and effort for users.

✓ **Secret Matching**
JWT-Hawk systematically tries each secret in the list, ensuring comprehensive decoding attempts for JWT tokens.

✓ **Streamlined Usage**
With clear instructions and a straightforward interface, users can easily utilize JWT-Hawk for their JWT token decoding needs.

Technologies Used

IceWatch leverages the following technologies:

✓ Python: JWT-Hawk is developed using Python, harnessing its capabilities for efficient token decoding and manipulation.
- **jwt Library:** The jwt library is a crucial dependency, enabling JWT token processing and validation.
- **termcolor Library:** This library enhances terminal text formatting, improving the readability of the tool's output.
- **pyfiglet Library:** JWT-Hawk utilizes pyfiglet to create stylish ASCII art banners for an appealing display.

Integration of Burp Suite Enterprise with CI/CD Pipeline & Code Sanitization

Type: **DevSecOps, Vulnerability Analysis** | Patronized by **bKash Offensive Security Research**

The project focuses on automating vulnerability assessments throughout the Development Lifecycle by integrating Burp Suite Enterprise with SonarQube. The objective is to establish a Secure Continuous Integration/Continuous Delivery (CI/CD) Pipeline, ensuring constant delivery and deployment while maintaining robust security practices.

How it Works

- ✓ **Automated Vulnerability Analysis**
  By incorporating Burp Suite Enterprise into the CI/CD Pipeline, the system automatically performs vulnerability assessments on code changes at the time of committing.

- ✓ **Code Sanitization**
  SonarQube & Snyk, integrated with the pipeline, ensures that code is analyzed and sanitized to identify and mitigate potential security flaws.

- ✓ **Continuous Delivery and Deployment**
  With automated vulnerability analysis and code sanitization, the pipeline supports continuous delivery and deployment while ensuring security best practices are followed.

How it Helps

- ✓ **Efficient Vulnerability Assessment**
  Automation streamlines the vulnerability assessment process, allowing security checks to be conducted in real-time during code commits.

- ✓ **Enhanced Security**
  By integrating vulnerability analysis and code sanitization into the CI/CD Pipeline, DevSecOps principles are effectively implemented, resulting in a more secure development environment.

- ✓ **Reduced Time-to-Market**
  Automated security assessments enable faster identification and resolution of vulnerabilities, leading to quicker release cycles and reduced time-to-market.

Key Technical Takeaways

- ✓ **Integration with Jenkins**
  The integration of Burp Suite Enterprise with Jenkins enables automated vulnerability analysis within the CI/CD Pipeline.

- ✓ **Code Analysis with SonarQube**
  SonarQube is utilized to perform code analysis and ensure code sanitization for improved security.

- ✓ **Dependency Scanning with Snyk**
  Snyk is employed to scan and identify vulnerabilities in project dependencies, enhancing the overall security of the application.

Technologies Used

The integration of the Secure CI/CD Pipeline involves the following technologies:

- ✓ **Burp Suite Enterprise:** Burp Suite Enterprise is employed to automate vulnerability assessments.
- ✓ **Jenkins:** Jenkins is utilized as the CI/CD automation server, incorporating Burp Suite Enterprise for security analysis.
- ✓ **SonarQube:** SonarQube plays a vital role in code analysis and sanitization, ensuring secure code practices.
- ✓ **Snyk:** Snyk is integrated to perform dependency scanning and identify vulnerabilities in project dependencies, bolstering the application's overall security.

Ongoing Research & Projects

Fraud Replication & Understanding Attack-Vector

Type: **API, Attack Surface** | Patronized by **bKash Offensive Security Research**

The project aims to address the persistent issue of fraud cases by implementing a Fraud Replication system. With the use of legacy cases, the project focuses on automating the process of impersonating Fraud Cases. By leveraging this system, it becomes possible to efficiently identify and scrutinize fraudulent or malicious transactions, thus enhancing fraud detection and prevention mechanisms.

High-Level Technical Methodology

- ✓ **Legacy Case Utilization**
  The project utilizes legacy cases, which serve as a reference dataset containing historical information about past fraud cases.

- ✓ **Automation of Impersonation**
  The system employs automation techniques to impersonate Fraud Cases based on the characteristics and patterns observed in the legacy cases.

- ✓ **Fraudulent Transaction Identification**
  Through the impersonation process, the system can effectively identify and flag suspicious transactions with potential fraudulent behavior.

- ✓ **Attack-Vector Understanding**
  By analyzing and replicating fraudulent scenarios, the project aims to gain a deeper understanding of the attack vectors used by malicious actors.

Intended Technologies to Use

- ✓ **API Integration:** The project may involve integrating with relevant APIs to access and process data, facilitating the replication of fraud cases.
- ✓ **Data Analysis Tools:** Utilizing data analysis tools, the system can identify patterns and trends in the legacy cases, which will guide the impersonation process.
- ✓ **Automation Frameworks:** Automation frameworks will be employed to streamline the impersonation of Fraud Cases, enhancing efficiency and accuracy.

Advance Malware Analysis & Antivirus Tool using Python

Type: **Security, Malware Analysis, Machine Learning**

The ongoing research and project aim to develop an advanced Malware Analysis and Antivirus Tool using Python. The primary objective is to create a powerful software solution capable of detecting and mitigating various forms of malware and ensuring robust cybersecurity.

High-Level Technical Methodology

- ✓ **Malicious Software Detection**
  The software subcomponent will undergo analysis, and if a match is found with known malware signatures or patterns, it will be labeled as malicious and subjected to appropriate actions.

- ✓ **Source Code Inspection**
  In cases where no immediate match is identified, the program will be further dissected by inspecting its source code. This step aims to deduce the program's purpose and ascertain whether it exhibits any malicious behavior.

- ✓ **Machine Learning Integration**
  The findings obtained from source code inspection will be incorporated into the program. The tool leverages machine learning techniques to enhance its capability to identify new and evolving malware threats. By continuously learning from new samples, the tool stays up-to-date with emerging threats.

Intended Technologies to Use

The following technologies are intended to be used in the research and project:

- ✓ **Python:** The primary programming language for developing the Malware Analysis and Antivirus Tool, known for its versatility and ease of implementation.
- ✓ **Machine Learning Libraries:** Python's machine learning libraries, such as scikit-learn, TensorFlow, or Keras, will be utilized to train and deploy machine learning models for malware detection.
- ✓ **Malware Databases:** External malware databases will be integrated to compare and identify known malware signatures during the detection process.
- ✓ **Source Code Analysis Tools:** Python-based tools or libraries for source code analysis will be incorporated to inspect the programs for potential malicious behavior.

Web Application Firewall Identification from Server Response using Python

Type: **Cybersecurity, Web Application Security, Network Security**

The project centers around developing a Python-based solution to identify Web Application Firewalls (WAFs) from server responses. By analyzing server responses, the project aims to determine the presence of WAFs, which play a critical role in securing web applications against various cyber threats.

High-Level Technical Methodology

- ✓ **Server Response Analysis**
  The project utilizes Python to analyze the server responses received during interactions with web applications.

- ✓ **WAF Detection Algorithms**
  Advanced algorithms are implemented to detect patterns, behaviors, or signatures characteristic of Web Application Firewalls.

- ✓ **Signature-Based Identification**
  The system employs signature-based techniques to match server response attributes with known WAF patterns.

- ✓ **Behavioral Analysis**
  In addition to signature-based detection, the project may employ behavioral analysis to identify WAF behavior during response handling.

Intended Technologies to Use

- ✓ **Python Requests Library:** Python's Requests library facilitates interactions with web applications, enabling the retrieval and analysis of server responses.
- ✓ **WAF Databases:** The project may utilize databases containing WAF signatures and behavior patterns for comparison and identification.
- ✓ **Machine Learning (*Optional*):** Machine learning models can be implemented to enhance the accuracy of WAF detection based on behavioral analysis.

Web Application Vulnerability Scanner

Type: **Web Application Vulnerability Scanner**

The project focuses on developing a comprehensive Web Application Vulnerability Scanner. The scanner aims to identify potential vulnerabilities and security weaknesses in web applications, enabling organizations to proactively address and mitigate security risks.

High-Level Technical Methodology

- ✓ **Automated Scanning**
  The project utilizes automation to systematically scan web applications for vulnerabilities, ensuring thorough coverage and efficiency.

- ✓ **Vulnerability Detection**
  The scanner employs advanced techniques to identify various types of vulnerabilities, such as SQL injection, cross-site scripting (XSS), and insecure configurations.

- ✓ **Reporting and Prioritization**
  Upon detecting vulnerabilities, the scanner generates detailed reports, highlighting the identified issues and prioritizing them based on their severity.

Intended Technologies to Use

- ✓ **Python:** Python will be used to build a Web Crawler. The tool will continuously generate requests and crawl to websites different pages/links to identify issues. The issues will be compared to a vulnerability database, that will map the vulnerability with different severity level and indices.
- ✓ **Vulnerability Databases:** The project may leverage databases containing known vulnerabilities to compare and identify potential security weaknesses.

Advanced Analysis of Codes, Attribution Analysis and Malicious Intent Identification

Type: **Security, Malware Analysis, Code Attribution**

The project focuses on advancing the analysis of codes to identify malicious intent in software components. It involves attribution analysis and code analysis techniques to deduce the intent behind certain codes and determine their authorship. The primary goal is to enhance cybersecurity measures by accurately detecting malicious code and attributing it to potential threat actors.

High-Level Technical Methodology

- ✓ **Code Analysis Techniques**
  The project employs advanced code analysis methodologies to delve into the structure, behavior, and patterns of software components.

- ✓ **Attribution Analysis**
  Attribution analysis techniques are applied to trace the origins of code, helping identify potential authors or threat actors involved.

- ✓ **Malicious Intent Identification**
  Through code analysis, the project aims to recognize and characterize malicious intent embedded within software components.

- ✓ **Behavior-Based Detection**
  The project may utilize behavior-based detection to identify suspicious or abnormal activities in codes.

Intended Technologies to Use

- ✓ **Static Code Analysis Tools:** Static code analysis tools are used to examine source code without executing it, providing insights into code vulnerabilities and potential malicious behavior.
- ✓ **Machine Learning for Attribution Analysis:** Machine learning models may be employed to attribute code to potential authors based on stylistic and behavioral patterns.
- ✓ **Behavior-Based Detection:** Behavior-based detection helps identify anomalous behavior in code, indicating possible malicious intent.

Face Detecting Surveillance System

Type: **Web Application, Deep Learning, Network**

The project aims to develop a Face Detecting Surveillance System as a web application. Leveraging Deep Learning and moder Web Frameworks, the system's primary objective is to recognize and identify faces it has encountered before and also from an existing database.

High-Level Technical Methodology

- ✓ **Face Recognition**
  The system will utilize advanced Deep Learning techniques for accurate face recognition based on the existing database of known faces.

- ✓ **Learning New Faces**
  Ongoing research is being conducted to enable the system to learn and understand new faces, expanding its adaptability and recognition capabilities.

Intended Technologies to Use

- ✓ **Deep Learning Frameworks:** Frameworks will be employed to train and fine-tune the face recognition model.
- ✓ **Web Application Development:** A Web Application will be developed as part of this solution, so that remote access is possible, to properly monitor the system.

Initiatives

Seminars

Starting a Career in Cyber Security, Enterprise Cybersecurity & Role of CTF

Read More

On March 15, 2023, I had the privilege of delivering a seminar at Islamic University of Technology (IUT) titled "Starting a Career in Cyber Security, Enterprise Cybersecurity & Role of CTF." In this captivating presentation, I delved into the critical importance of cybersecurity across multiple industries and shed light on the unique challenges faced by large organizations. I talked about how important it is for security teams to protect against cyber threats and how Capture the Flag (CTF) competitions help people improve their cybersecurity skills.

During the session, I gave helpful tips on how people can find the motivation and resources they need to improve their cybersecurity skills. I also took the audience on a fascinating journey through my own experiences and discoveries in the field of cybersecurity, which is always changing and growing.

The goal of the seminar was to get people interested in careers in cybersecurity by talking about how they could have a big impact on making sure digital systems are safe and making organizations more resistant to cyber threats. It was a great chance to share ideas, have in-depth conversations, and work together to make the digital world safer and more secure for everyone in the future.

Entrepreneurship

Entrepreneurship in the security field motivates me to devise novel solutions to problems that benefit the community and the world. As someone interested in cyber security, I want to make significant contributions to a rapidly changing field. I want to push boundaries and find creative answers to new security issues. With the goal of improving digital landscapes, I want to launch a company that provides cutting-edge solutions to assist businesses and individuals in dealing with ever-changing cyber threats. I'm determined to make a positive difference and contribute to making everyone's digital future safer and more secure through my businesses.

With this vision in mind, **RedHawks Cybersecurity** has emerged as a manifestation of my passion for fortifying digital landscapes. Because of its unwavering commitment to innovation and excellence, RedHawks Cybersecurity is a leading provider of offensive security solutions. Our team is committed to empowering organizations and individuals with offensive security services that identify and address vulnerabilities proactively. In addition, we place a significant emphasis on security awareness, providing comprehensive training and education programs to equip individuals with the knowledge and skills necessary to remain vigilant in the face of cyber threats. RedHawks Cybersecurity is driven by the desire to make the world a safer place through its pioneering contributions in the field of cybersecurity.

Official Website: https://red-hawks.com/

Official Facebook Page: https://www.facebook.com/redhawks.cyber

CTFs, Awards & Others

I find myself immersed in the thrilling world of cybersecurity as a dedicated participant in CTF events and various CTF Playgrounds. These exhilarating competitions have become my arena for honing my abilities, exploring new security concepts, and mastering the art of exploiting vulnerabilities. Platforms such as TryHackMe, HackTheBox, and picoCTF have become my virtual training grounds, where I continually push the boundaries of my knowledge and proficiency with essential cybersecurity tools.

I go by the handle DL28. (https://ctftime.org/user/126363) Being a member of the esteemed **IUT Genesis team**, the **official CTF First Team of Islamic University of Technology**, is a major highlight of my journey. Together, we have achieved an impressive **second place in the nation** and a commendable **206th place worldwide**. (https://ctftime.org/team/175924)

I mentor university students in the fields of Web Exploitation and Network, guiding them through their own thrilling cybersecurity adventures.

Leading the bKash CTF team was a rewarding experience, as we placed second in the 2021 Financial Institution Cyberdrill of Bangladesh and third in the 2022 competition. These achievements strengthen my resolve to continue pushing the limits of cybersecurity excellence.

In my quest to share my expertise with a wider audience, I am currently authoring a book on Basic CTF and NMAP, with the hope of unveiling it to the world in February 2024.

Through this endeavor, I aspire to empower aspiring cybersecurity enthusiasts to embark on their own CTF journeys, unraveling the mysteries of the digital realm, one challenge at a time. Embracing every opportunity to contribute to the cybersecurity community, I am determined to make a lasting impact on the world of cybersecurity, shaping a more secure and resilient digital future for all.

Socials

navidnaf.com | navidfazlerabbi@iut-dhaka.edu
LinkedIn | GitHub | CTFTime | TryHackMe | Researchgate | Google Scholar