Bug Bounty Recon Report on FUTA (futa.edu.ng)

1. Executive Summary

This report documents the bug bounty reconnaissance conducted on futa.edu.ng. Using MagicRecon, a comprehensive information-gathering tool, no significant vulnerabilities were identified during the recon phase. However, the collected data provides a foundational understanding of the target's online infrastructure.

---

2. Tools Used

- **MagicRecon**: MagicRecon is a tool used for automating reconnaissance in bug bounty hunting. It integrates various techniques and tools to collect useful information about a target, such as subdomains, technologies used, and DNS configurations.

---

3. Methodology

1. **Initial Setup**

   o   Target Domain: futa.edu.ng

   o   Tool: MagicRecon

2. **Subdomain Enumeration**

   o   MagicRecon was used to discover potential subdomains of futa.edu.ng.

3. **Service Detection**

   o   A port scan was performed to identify open services on the discovered subdomains.

4. **Technology Stack Identification**

   o   Technologies used by the website and its subdomains were enumerated to identify potential attack vectors.

5. **DNS Configuration & Whois Lookup**

   o   DNS and Whois lookups were conducted to gather information about the domain's registration and name server configurations.

---

4. Recon Results

- **Subdomains Identified**:

- - www.futa.edu.ng
- **Services Detected**:
- **Technologies Detected**:
- **DNS Findings**:

---

5. Conclusion

The reconnaissance phase on futa.edu.ng did not reveal any immediate security vulnerabilities. However, the information gathered lays the groundwork for further targeted vulnerability assessments. Continuous monitoring and deeper analysis are recommended to identify potential threats.

---

6. Recommendations

- Regularly monitor and patch the web server and application components.
- Conduct periodic vulnerability assessments to identify potential security gaps.
- Implement security headers (if missing) to mitigate common web attacks.
- Ensure all subdomains are regularly monitored for unauthorized access or exposure.