BBC BANK UGANDA LIMITED

Information Security and Auditing (BUC3126) Capstone

VAPT REPORT TEMPLATE

Replace the italic prompts with your own work

1. Executive Summary

[One paragraph: what was tested, when, the overall security posture of the DMZ server, and the number of findings by severity. State the single most serious risk in plain language for management.]

Severity	Number of findings
Critical	[ ]
High	[ ]
Medium	[ ]
Low	[ ]
Total	[ ]

2. Scope and Authorisation

[State the authorised target, the isolated lab setup, the testing window, and reference the signed Authorisation to Test. Repeat the framing that this is a representative DMZ server, not the core banking application.]

3. Methodology and Tools

[Name the methodology (NIST SP 800-115 / PTES) and list the tools used in each phase: Nmap, OpenVAS or Nessus, Nikto, Metasploit, Hydra. State versions.]

4. Discovery Results

[Summarise the Nmap output: open ports, services and versions. Reference the full nmap file in your appendix.]

Port	Service	Version	Note
21/tcp	FTP	[ ]	[ ]
22/tcp	SSH	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]

5. Vulnerability Findings

[Complete one row per finding. Rank by CVSS. At least eight findings; mark those you confirmed by exploitation.]

ID	Vulnerability	Affected service	CVE	CVSS v3.1	Severity
V-01	[e.g. vsftpd 2.3.4 backdoor]	FTP (21)	CVE-2011-2523	10.0	Critical
V-02	[ ]	[ ]	[ ]	[ ]	[ ]
V-03	[ ]	[ ]	[ ]	[ ]	[ ]

6. Exploitation Evidence

[For each confirmed finding: describe the steps, paste the key command and result, and insert a timestamped screenshot. Show what was accessed.]

7. Business Impact for BBC Bank

[Translate the technical findings into risk to the bank: customer data confidentiality, integrity of transactions, availability, and regulatory exposure under the BoU Cyber and Technology Risk Management Guidelines, 2024 and the Data Protection and Privacy Act, 2019.]

8. Recommendations

[For each finding or theme: a specific, prioritised remediation with an owner and timeline. Group quick wins separately from strategic actions such as a patch management programme and threat-led penetration testing.]

Finding ID	Recommendation	Owner	Priority	Target date
V-01	[ ]	[ ]	[ ]	[ ]

9. Appendices

[Attach: full Nmap outputs, scanner report, Nikto output, exploitation screenshots, and the signed Authorisation to Test.]