SECURITY ASSESSMENT REPORT

Scan Overview

Target	dbu.edu.et
Scan Type	QUICK
Scan Date	2025-10-06T10:12:07.251417
Status	completed
Vulnerabilities Found	8

Vulnerability Summary

Severity Level	Count	Percentage
Critical	0	0.0%
High	4	50.0%
Medium	4	50.0%
Low	0	0.0%
TOTAL	8	100%

Detailed Findings

Finding #1: Open SSH Service - HIGH

Description:	Port 22/tcp is open running ssh
Port/Service:	22/ssh
CVE:	
Evidence:	22/tcp open ssh
Solution:	Use SSH key authentication and disable root login

Finding #2: SSH Service Exposed - HIGH

Description:	SSH service is accessible from network
Port/Service:	22/ssh
CVE:	Not specified
Evidence:	SSH running on port 22
Solution:	Restrict SSH access to trusted IPs and use key authentication

Finding #3: Open DOMAIN Service - HIGH

Description:	Port 53/tcp is open running domain
Port/Service:	53/domain
CVE:	
Evidence:	53/tcp open domain
Solution:	Secure DNS server configuration

Finding #4: Open HTTP Service - MEDIUM

Description:	Port 80/tcp is open running http
Port/Service:	80/http
CVE:	
Evidence:	80/tcp open http
Solution:	Ensure web server is properly secured

Finding #5: HTTP Service (Unencrypted) - MEDIUM

Description:	Web service running without encryption
Port/Service:	80/http
CVE:	Not specified
Evidence:	HTTP on port 80 - no encryption
Solution:	Use HTTPS with TLS encryption

Finding #6: Open HTTPS Service - HIGH

Description:	Port 443/tcp is open running https
Port/Service:	443/https
CVE:	
Evidence:	443/tcp open https
Solution:	Use HTTPS with proper TLS configuration

Finding #7: Open HTTP-PROXY Service - MEDIUM

Description:	Port 8080/tcp is open running http-proxy
Port/Service:	8080/http-proxy
CVE:	
Evidence:	8080/tcp open http-proxy
Solution:	Review if this service needs to be publicly accessible

Finding #8: Open HTTPS-ALT Service - MEDIUM

Description:	Port 8443/tcp is open running https-alt
Port/Service:	8443/https-alt
CVE:	
Evidence:	8443/tcp open https-alt
Solution:	Review if this service needs to be publicly accessible

Security Recommendations

• Regularly update and patch all identified services
• Implement proper network segmentation
• Use firewall rules to restrict unnecessary port access
• Enable security headers for web applications
• Conduct regular security assessments
• Implement monitoring and alerting for critical services

Report generated on 2025-10-06 10:13:29 by Security Scanner