SECURITY ASSESSMENT REPORT

Scan Overview

Target	dbu.edu.et
Scan Type	VULNERABILITY
Scan Date	2025-10-01T12:24:17.907643
Status	completed
Vulnerabilities Found	47

Vulnerability Summary

Severity Level	Count	Percentage
Critical	0	0.0%
High	4	8.5%
Medium	43	91.5%
Low	0	0.0%
TOTAL	47	100%

Detailed Findings

Finding #1: Open SSH Service - HIGH

Description:	Port 22/tcp is open running ssh OpenSSH 8.0 (protocol 2.0)
Port/Service:	22/ssh
CVE:	
Evidence:	22/tcp open ssh OpenSSH 8.0 (protocol 2.0)
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: Security Finding - MEDIUM

Description:	| vulners:
Port/Service:	N/A/N/A
CVE:	
Evidence:	| vulners:
Solution:	Investigate this security finding

Finding #4: Security Finding - MEDIUM

Description:	| ■PACKETSTORM:173661■9.8■https://vulners.com/packetstorm/PACKETSTORM:173661
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■PACKETSTORM:173661■9.8■https://vulners.com/packetstorm/PACKETSTORM:173661
Solution:	Investigate this security finding

Finding #5: Security Finding - MEDIUM

Description:	| ■F0979183-AE88-53B4-86CF-3AF0523F3807■9.8■https://vulners.com/githubexploit/F097
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■F0979183-AE88-53B4-86CF-3AF0523F3807■9.8■https://vulners.com/githubexploit/F097
Solution:	Investigate this security finding

Finding #6: Security Finding - MEDIUM

Description:	| ■CVE-2023-38408■9.8■https://vulners.com/cve/CVE-2023-38408
Port/Service:	N/A/N/A
CVE:	CVE-2023-38408
Evidence:	| ■CVE-2023-38408■9.8■https://vulners.com/cve/CVE-2023-38408
Solution:	Investigate this security finding

Finding #7: Security Finding - MEDIUM

Description:	| ■B8190CDB-3EB9-5631-9828-8064A1575B23■9.8■https://vulners.com/githubexploit/B81
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■B8190CDB-3EB9-5631-9828-8064A1575B23■9.8■https://vulners.com/githubexploit/B81
Solution:	Investigate this security finding

Finding #8: Security Finding - MEDIUM

Description:	| ■8FC9C5AB-3968-5F3C-825E-E8DB5379A623■9.8■https://vulners.com/githubexploit/8F(
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■8FC9C5AB-3968-5F3C-825E-E8DB5379A623■9.8■https://vulners.com/githubexploit/8F(
Solution:	Investigate this security finding

Finding #9: Security Finding - MEDIUM

Description:	| ■8AD01159-548E-546E-AA87-2DE89F3927EC■9.8■https://vulners.com/githubexploit/8AI
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■8AD01159-548E-546E-AA87-2DE89F3927EC■9.8■https://vulners.com/githubexploit/8AI
Solution:	Investigate this security finding

Finding #10: Security Finding - MEDIUM

Description:	| ■2227729D-6700-5C8F-8930-1EEAFD4B9FF0■9.8■https://vulners.com/githubexploit/222
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■2227729D-6700-5C8F-8930-1EEAFD4B9FF0■9.8■https://vulners.com/githubexploit/222
Solution:	Investigate this security finding

Finding #11: Security Finding - MEDIUM

Description:	| ■0221525F-07F5-5790-912D-F4B9E2D1B587■9.8■https://vulners.com/githubexploit/0221
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■0221525F-07F5-5790-912D-F4B9E2D1B587■9.8■https://vulners.com/githubexploit/0221
Solution:	Investigate this security finding

Finding #12: Security Finding - MEDIUM

Description:	| ■BA3887BD-F579-53B1-A4A4-FF49E953E1C0■8.1■https://vulners.com/githubexploit/BA
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■BA3887BD-F579-53B1-A4A4-FF49E953E1C0■8.1■https://vulners.com/githubexploit/BA
Solution:	Investigate this security finding

Finding #13: Security Finding - MEDIUM

Description:	| ■4FB01B00-F993-5CAF-BD57-D7E290D10C1F■8.1■https://vulners.com/githubexploit/4F
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■4FB01B00-F993-5CAF-BD57-D7E290D10C1F■8.1■https://vulners.com/githubexploit/4F
Solution:	Investigate this security finding

Finding #14: Security Finding - MEDIUM

Description:	| ■CVE-2020-15778■7.8■https://vulners.com/cve/CVE-2020-15778
Port/Service:	N/A/N/A
CVE:	CVE-2020-15778
Evidence:	| ■CVE-2020-15778■7.8■https://vulners.com/cve/CVE-2020-15778
Solution:	Investigate this security finding

Finding #15: Security Finding - MEDIUM

Description:	| ■CVE-2019-16905■7.8■https://vulners.com/cve/CVE-2019-16905
Port/Service:	N/A/N/A
CVE:	CVE-2019-16905
Evidence:	| ■CVE-2019-16905■7.8■https://vulners.com/cve/CVE-2019-16905
Solution:	Investigate this security finding

Finding #16: Security Finding - MEDIUM

Description:	| ■C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3■7.8■https://vulners.com/githubexploit/C9
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■C94132FD-1FA5-5342-B6EE-0DAF45EEFFE3■7.8■https://vulners.com/githubexploit/C9
Solution:	Investigate this security finding

Finding #17: Security Finding - MEDIUM

Description:	| ■2E719186-2FED-58A8-A150-762EFBAAA523■7.8■https://vulners.com/gitee/2E719186-
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■2E719186-2FED-58A8-A150-762EFBAAA523■7.8■https://vulners.com/gitee/2E719186-
Solution:	Investigate this security finding

Finding #18: Security Finding - MEDIUM

Description:	| ■23CC97BE-7C95-513B-9E73-298C48D74432■7.8■https://vulners.com/githubexploit/23C
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■23CC97BE-7C95-513B-9E73-298C48D74432■7.8■https://vulners.com/githubexploit/23C
Solution:	Investigate this security finding

Finding #19: Security Finding - MEDIUM

Description:	| ■10213DBE-F683-58BB-B6D3-353173626207■7.8■https://vulners.com/githubexploit/1021
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■10213DBE-F683-58BB-B6D3-353173626207■7.8■https://vulners.com/githubexploit/1021
Solution:	Investigate this security finding

Finding #20: Security Finding - MEDIUM

Description:	| ■SSV:92579■7.5■https://vulners.com/seebug/SSV:92579■*EXPLOIT*
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■SSV:92579■7.5■https://vulners.com/seebug/SSV:92579■*EXPLOIT*
Solution:	Investigate this security finding

Finding #21: Security Finding - MEDIUM

Description:	| ■1337DAY-ID-26576■7.5■https://vulners.com/zdt/1337DAY-ID-26576■*EXPLOIT*
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■1337DAY-ID-26576■7.5■https://vulners.com/zdt/1337DAY-ID-26576■*EXPLOIT*
Solution:	Investigate this security finding

Finding #22: Security Finding - MEDIUM

Description:	| ■CVE-2021-41617■7.0■https://vulners.com/cve/CVE-2021-41617
Port/Service:	N/A/N/A
CVE:	CVE-2021-41617
Evidence:	| ■CVE-2021-41617■7.0■https://vulners.com/cve/CVE-2021-41617
Solution:	Investigate this security finding

Finding #23: Security Finding - MEDIUM

Description:	| ■284B94FC-FD5D-5C47-90EA-47900DAD1D1E■7.0■https://vulners.com/githubexploit/28
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■284B94FC-FD5D-5C47-90EA-47900DAD1D1E■7.0■https://vulners.com/githubexploit/28
Solution:	Investigate this security finding

Finding #24: Security Finding - MEDIUM

Description:	| ■PACKETSTORM:189283■6.8■https://vulners.com/packetstorm/PACKETSTORM:189283
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■PACKETSTORM:189283■6.8■https://vulners.com/packetstorm/PACKETSTORM:189283
Solution:	Investigate this security finding

Finding #25: Security Finding - MEDIUM

Description:	| ■CVE-2025-26465■6.8■https://vulners.com/cve/CVE-2025-26465
Port/Service:	N/A/N/A
CVE:	CVE-2025-26465
Evidence:	| ■CVE-2025-26465■6.8■https://vulners.com/cve/CVE-2025-26465
Solution:	Investigate this security finding

Finding #26: Security Finding - MEDIUM

Description:	| ■9D8432B9-49EC-5F45-BB96-329B1F2B2254■6.8■https://vulners.com/githubexploit/9D8
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■9D8432B9-49EC-5F45-BB96-329B1F2B2254■6.8■https://vulners.com/githubexploit/9D8
Solution:	Investigate this security finding

Finding #27: Security Finding - MEDIUM

Description:	| ■85FCDCC6-9A03-597E-AB4F-FA4DAC04F8D0■6.8■https://vulners.com/githubexploit/85
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■85FCDCC6-9A03-597E-AB4F-FA4DAC04F8D0■6.8■https://vulners.com/githubexploit/85
Solution:	Investigate this security finding

Finding #28: Security Finding - MEDIUM

Description:	| ■1337DAY-ID-39918■6.8■https://vulners.com/zdt/1337DAY-ID-39918■*EXPLOIT*
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■1337DAY-ID-39918■6.8■https://vulners.com/zdt/1337DAY-ID-39918■*EXPLOIT*
Solution:	Investigate this security finding

Finding #29: Security Finding - MEDIUM

Description:	| ■D104D2BF-ED22-588B-A9B2-3CCC562FE8C0■6.5■https://vulners.com/githubexploit/D
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■D104D2BF-ED22-588B-A9B2-3CCC562FE8C0■6.5■https://vulners.com/githubexploit/D
Solution:	Investigate this security finding

Finding #30: Security Finding - MEDIUM

Description:	| ■CVE-2023-51385■6.5■https://vulners.com/cve/CVE-2023-51385
Port/Service:	N/A/N/A
CVE:	CVE-2023-51385
Evidence:	| ■CVE-2023-51385■6.5■https://vulners.com/cve/CVE-2023-51385
Solution:	Investigate this security finding

Finding #31: Security Finding - MEDIUM

Description:	| ■C07ADB46-24B8-57B7-B375-9C761F4750A2■6.5■https://vulners.com/githubexploit/C07
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■C07ADB46-24B8-57B7-B375-9C761F4750A2■6.5■https://vulners.com/githubexploit/C07
Solution:	Investigate this security finding

Finding #32: Security Finding - MEDIUM

Description:	| ■A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C■6.5■https://vulners.com/githubexploit/A
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■A88CDD3E-67CC-51CC-97FB-AB0CACB6B08C■6.5■https://vulners.com/githubexploit/A
Solution:	Investigate this security finding

Finding #33: Security Finding - MEDIUM

Description:	| ■65B15AA1-2A8D-53C1-9499-69EBA3619F1C■6.5■https://vulners.com/githubexploit/65B
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■65B15AA1-2A8D-53C1-9499-69EBA3619F1C■6.5■https://vulners.com/githubexploit/65B
Solution:	Investigate this security finding

Finding #34: Security Finding - MEDIUM

Description:	| ■5325A9D6-132B-590C-BDEF-0CB105252732■6.5■https://vulners.com/gitee/5325A9D6-
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■5325A9D6-132B-590C-BDEF-0CB105252732■6.5■https://vulners.com/gitee/5325A9D6-
Solution:	Investigate this security finding

Finding #35: Security Finding - MEDIUM

Description:	| ■530326CF-6AB3-5643-AA16-73DC8CB44742■6.5■https://vulners.com/githubexploit/530
Port/Service:	N/A/N/A
CVE:	
Evidence:	| ■530326CF-6AB3-5643-AA16-73DC8CB44742■6.5■https://vulners.com/githubexploit/530
Solution:	Investigate this security finding

Finding #36: Security Finding - MEDIUM

Description:	| ■CVE-2023-48795■5.9■https://vulners.com/cve/CVE-2023-48795
Port/Service:	N/A/N/A
CVE:	CVE-2023-48795
Evidence:	| ■CVE-2023-48795■5.9■https://vulners.com/cve/CVE-2023-48795
Solution:	Investigate this security finding

Finding #37: Security Finding - MEDIUM

Description:	| ■CVE-2020-14145■5.9■https://vulners.com/cve/CVE-2020-14145
Port/Service:	N/A/N/A
CVE:	CVE-2020-14145
Evidence:	| ■CVE-2020-14145■5.9■https://vulners.com/cve/CVE-2020-14145
Solution:	Investigate this security finding

Finding #38: Security Finding - MEDIUM

Description:	| ■CVE-2016-20012■5.3■https://vulners.com/cve/CVE-2016-20012
Port/Service:	N/A/N/A
CVE:	CVE-2016-20012
Evidence:	| ■CVE-2016-20012■5.3■https://vulners.com/cve/CVE-2016-20012
Solution:	Investigate this security finding

Finding #39: Security Finding - MEDIUM

Description:	| ■CVE-2025-32728■4.3■https://vulners.com/cve/CVE-2025-32728
Port/Service:	N/A/N/A
CVE:	CVE-2025-32728
Evidence:	| ■CVE-2025-32728■4.3■https://vulners.com/cve/CVE-2025-32728
Solution:	Investigate this security finding

Finding #40: Security Finding - MEDIUM

Description:	| ■CVE-2021-36368■3.7■https://vulners.com/cve/CVE-2021-36368
Port/Service:	N/A/N/A
CVE:	CVE-2021-36368
Evidence:	| ■CVE-2021-36368■3.7■https://vulners.com/cve/CVE-2021-36368
Solution:	Investigate this security finding

Finding #41: Security Finding - MEDIUM

Description:	|_ ■PACKETSTORM:140261■0.0■https://vulners.com/packetstorm/PACKETSTORM:14026
Port/Service:	N/A/N/A
CVE:	
Evidence:	|_ ■PACKETSTORM:140261■0.0■https://vulners.com/packetstorm/PACKETSTORM:14026
Solution:	Investigate this security finding

Finding #42: Open DOMAIN Service - HIGH

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

Finding #43: Open HTTP Service - MEDIUM

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

Finding #44: 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 #45: Open SSL/HTTP Service - HIGH

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

Finding #46: Open TCPWRAPPED Service - MEDIUM

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

Finding #47: Open SSL/HTTPS-ALT Service - MEDIUM

Description:	Port 8443/tcp is open running ssl/https-alt sw-cp-server
Port/Service:	8443/ssl/https-alt
CVE:	
Evidence:	8443/tcp open ssl/https-alt sw-cp-server
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 2025-10-01 12:26:02 by Security Scanner