Vulnerability Assessment Report

PDF Test

Vulnerability Assessment Report

PDF Test

Report Date: 2025-10-07

Project Version: 1.0.0

Assessment Type: Comprehensive Security Analysis

Methodology: Static Code Analysis + Manual Validation

Executive Summary

This report presents the findings of a comprehensive security assessment of **PDF Test**. The assessment identified **89 validated vulnerabilities** requiring immediate attention.

Risk Overview

Severity	Count	Risk Weight
■ Critical	59	590
■ High	30	150
■ Medium	0	0
■ Low	0	0
Total	**89**	**740/890**

Overall Risk Score: 83.1/100

■■ **CRITICAL**: 59 critical vulnerability(ies) require **immediate** remediation. These vulnerabilities pose severe security risks and should be addressed within 24-48 hours.

Table of Contents

1. [Executive Summary](#executive-summary)

2. [Vulnerability Findings](#vulnerability-findings)

- [1. Cross-Site Scripting in train_multitask_vulnhunter.py](#finding-1-cross-site-scripting-in-train_multitask_vulnhunter.py)

- [2. Command Injection in train_multitask_vulnhunter.py](#finding-2-command-injection-in-train_multitask_vulnhunter.py)

- [3. SQL Injection in vulnerability_predictor.py](#finding-3-sql-injection-in-vulnerability_predictor.py)

- [4. Command Injection in vulnerability_predictor.py](#finding-4-command-injection-in-vulnerability_predictor.py)

- [5. Command Injection in vulnerability_predictor.py](#finding-5-command-injection-in-vulnerability_predictor.py)

- [6. Cross-Site Scripting in demo_hackerone_fp_system.py](#finding-6-cross-site-scripting-in-demo_hackerone_fp_system.py)

- [7. Cross-Site Scripting in train_hackerone_fp_model.py](#finding-7-cross-site-scripting-in-train_hackerone_fp_model.py)

- [8. Cross-Site Scripting in train_hackerone_fp_model.py](#finding-8-cross-site-scripting-in-train_hackerone_fp_model.py)

- [9. Command Injection in train_hackerone_fp_model.py](#finding-9-command-injection-in-train_hackerone_fp_model.py)

- [10. Command Injection in train_hackerone_fp_model.py](#finding-10-command-injection-in-train_hackerone_fp_model.py)

- [11. Cross-Site Scripting in gpu_optimization_utils.py](#finding-11-cross-site-scripting-in-gpu_optimization_utils.py)

- [12. Command Injection in gpu_optimization_utils.py](#finding-12-command-injection-in-gpu_optimization_utils.py)

- [13. SQL Injection in false_positive_reduction.py](#finding-13-sql-injection-in-false_positive_reduction.py)

- [14. SQL Injection in zero_false_positive_engine.py](#finding-14-sql-injection-in-zero_false_positive_engine.py)

- [15. Command Injection in zero_false_positive_engine.py](#finding-15-command-injection-in-zero_false_positive_engine.py)

- [16. Cross-Site Scripting in enhanced_beast_http_analyzer.py](#finding-16-cross-site-scripting-in-enhanced_beast_http_analyzer.py)

- [17. Command Injection in enhanced_beast_http_analyzer.py](#finding-17-command-injection-in-enhanced_beast_http_analyzer.py)

- [18. Command Injection in enhanced_beast_http_analyzer.py](#finding-18-command-injection-in-enhanced_beast_http_analyzer.py)

- [19. Command Injection in enhanced_beast_http_analyzer.py](#finding-19-command-injection-in-enhanced_beast_http_analyzer.py)

- [20. Command Injection in professional_bounty_reporter.py](#finding-20-command-injection-in-professional_bounty_reporter.py)

- [21. Command Injection in professional_bounty_reporter.py](#finding-21-command-injection-in-professional_bounty_reporter.py)

- [22. Cross-Site Scripting in vulnerability_validator.py](#finding-22-cross-site-scripting-in-vulnerability_validator.py)

- [23. SQL Injection in ast_feature_extractor.py](#finding-23-sql-injection-in-ast_feature_extractor.py)

- [24. SQL Injection in z3_verification_module.py](#finding-24-sql-injection-in-z3_verification_module.py)

- [25. Cross-Site Scripting in z3_verification_module.py](#finding-25-cross-site-scripting-in-z3_verification_module.py)

- [26. Command Injection in z3_verification_module.py](#finding-26-command-injection-in-z3_verification_module.py)

- [27. Command Injection in z3_verification_module.py](#finding-27-command-injection-in-z3_verification_module.py)

- [28. Command Injection in z3_verification_module.py](#finding-28-command-injection-in-z3_verification_module.py)

- [29. Command Injection in z3_verification_module.py](#finding-29-command-injection-in-z3_verification_module.py)

- [30. Command Injection in z3_verification_module.py](#finding-30-command-injection-in-z3_verification_module.py)

- [31. Command Injection in z3_verification_module.py](#finding-31-command-injection-in-z3_verification_module.py)

- [32. Command Injection in z3_verification_module.py](#finding-32-command-injection-in-z3_verification_module.py)

- [33. Command Injection in z3_verification_module.py](#finding-33-command-injection-in-z3_verification_module.py)

- [34. Command Injection in z3_verification_module.py](#finding-34-command-injection-in-z3_verification_module.py)

- [35. Command Injection in z3_verification_module.py](#finding-35-command-injection-in-z3_verification_module.py)

- [36. Command Injection in huntr_pattern_extractor.py](#finding-36-command-injection-in-huntr_pattern_extractor.py)

- [37. Cross-Site Scripting in http_security_dataset_builder.py](#finding-37-cross-site-scripting-in-http_security_dataset_builder.py)

- [38. Cross-Site Scripting in http_security_dataset_builder.py](#finding-38-cross-site-scripting-in-http_security_dataset_builder.py)

- [39. Command Injection in http_security_dataset_builder.py](#finding-39-command-injection-in-http_security_dataset_builder.py)

- [40. Command Injection in http_security_dataset_builder.py](#finding-40-command-injection-in-http_security_dataset_builder.py)

- [41. Command Injection in http_security_dataset_builder.py](#finding-41-command-injection-in-http_security_dataset_builder.py)

- [42. Command Injection in http_security_dataset_builder.py](#finding-42-command-injection-in-http_security_dataset_builder.py)

- [43. Command Injection in http_security_dataset_builder.py](#finding-43-command-injection-in-http_security_dataset_builder.py)

- [44. Command Injection in http_security_dataset_builder.py](#finding-44-command-injection-in-http_security_dataset_builder.py)

- [45. Cross-Site Scripting in enhanced_gnn_trainer.py](#finding-45-cross-site-scripting-in-enhanced_gnn_trainer.py)

- [46. Command Injection in enhanced_gnn_trainer.py](#finding-46-command-injection-in-enhanced_gnn_trainer.py)

- [47. SQL Injection in hackerone_dataset_builder.py](#finding-47-sql-injection-in-hackerone_dataset_builder.py)

- [48. SQL Injection in hackerone_dataset_builder.py](#finding-48-sql-injection-in-hackerone_dataset_builder.py)

- [49. SQL Injection in hackerone_dataset_builder.py](#finding-49-sql-injection-in-hackerone_dataset_builder.py)

- [50. Cross-Site Scripting in hackerone_dataset_builder.py](#finding-50-cross-site-scripting-in-hackerone_dataset_builder.py)

- [51. Cross-Site Scripting in hackerone_dataset_builder.py](#finding-51-cross-site-scripting-in-hackerone_dataset_builder.py)

- [52. Cross-Site Scripting in hackerone_dataset_builder.py](#finding-52-cross-site-scripting-in-hackerone_dataset_builder.py)

- [53. Cross-Site Scripting in hackerone_dataset_builder.py](#finding-53-cross-site-scripting-in-hackerone_dataset_builder.py)

- [54. Cross-Site Scripting in hackerone_dataset_builder.py](#finding-54-cross-site-scripting-in-hackerone_dataset_builder.py)

- [55. Command Injection in hackerone_dataset_builder.py](#finding-55-command-injection-in-hackerone_dataset_builder.py)

- [56. Command Injection in hackerone_dataset_builder.py](#finding-56-command-injection-in-hackerone_dataset_builder.py)

- [57. Command Injection in hackerone_dataset_builder.py](#finding-57-command-injection-in-hackerone_dataset_builder.py)

- [58. Command Injection in hackerone_dataset_builder.py](#finding-58-command-injection-in-hackerone_dataset_builder.py)

- [59. Command Injection in hackerone_dataset_builder.py](#finding-59-command-injection-in-hackerone_dataset_builder.py)

- [60. Command Injection in hackerone_dataset_builder.py](#finding-60-command-injection-in-hackerone_dataset_builder.py)

- [61. Path Traversal in hackerone_dataset_builder.py](#finding-61-path-traversal-in-hackerone_dataset_builder.py)

- [62. Path Traversal in hackerone_dataset_builder.py](#finding-62-path-traversal-in-hackerone_dataset_builder.py)

- [63. Cross-Site Scripting in sota_baselines.py](#finding-63-cross-site-scripting-in-sota_baselines.py)

- [64. Cross-Site Scripting in sota_baselines.py](#finding-64-cross-site-scripting-in-sota_baselines.py)

- [65. Cross-Site Scripting in sota_baselines.py](#finding-65-cross-site-scripting-in-sota_baselines.py)