DeVAIC Security Analysis Report

Files analyzed: 10

Total vulnerabilities: 143

Analysis duration: 0.50s

Vulnerabilities by Severity:

- CRITICAL: 44
- LOW: 23
- HIGH: 50
- MEDIUM: 26

Detected Vulnerabilities:

1. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_js_test.js:6

Description: Potential Cross-Site Scripting (XSS) vulnerability

2. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_js_test.js:7

Description: Potential Cross-Site Scripting (XSS) vulnerability

3. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_js_test.js:8

Description: Potential Cross-Site Scripting (XSS) vulnerability

4. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_js_test.js:9

Description: Potential Cross-Site Scripting (XSS) vulnerability

5. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_js_test.js:18

Description: Potential Cross-Site Scripting (XSS) vulnerability

6. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_js_test.js:19

Description: Potential Cross-Site Scripting (XSS) vulnerability

7. Prototype Pollution (HIGH)

File: test_files/vulnerable_js_test.js:23

Description: Potential prototype pollution vulnerability

8. Prototype Pollution (HIGH)

File: test_files/vulnerable_js_test.js:24

Description: Potential prototype pollution vulnerability

9. Prototype Pollution (HIGH)

File: test_files/vulnerable_js_test.js:25

Description: Potential prototype pollution vulnerability

10. Prototype Pollution (CRITICAL)

File: test_files/vulnerable_js_test.js:29

Description: Potential prototype pollution vulnerability

11. Code Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:34

Description: Code execution via eval() or dynamic code execution

12. Code Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:35

Description: Code execution via eval() or dynamic code execution

13. Code Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:36

Description: Code execution via eval() or dynamic code execution

14. Code Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:37

Description: Code execution via eval() or dynamic code execution

15. Code Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:40

Description: Code execution via eval() or dynamic code execution

16. Code Injection (HIGH)

File: test_files/vulnerable_js_test.js:43

Description: Code execution via eval() or dynamic code execution

17. Code Injection (HIGH)

File: test_files/vulnerable_js_test.js:48

Description: Code execution via eval() or dynamic code execution

18. Code Injection (HIGH)

File: test_files/vulnerable_js_test.js:51

Description: Code execution via eval() or dynamic code execution

19. Code Injection (HIGH)

File: test_files/vulnerable_js_test.js:58

Description: Code execution via eval() or dynamic code execution

20. Code Injection (HIGH)

File: test_files/vulnerable_js_test.js:84

Description: Code execution via eval() or dynamic code execution

21. Code Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:90

Description: Code execution via eval() or dynamic code execution

22. Cross-Site Scripting (XSS) (MEDIUM)

File: test_files/vulnerable_js_test.js:61

Description: Unsafe DOM manipulation with user input

23. Cross-Site Scripting (XSS) (MEDIUM)

File: test_files/vulnerable_js_test.js:62

Description: Unsafe DOM manipulation with user input

24. Cross-Site Scripting (XSS) (MEDIUM)

File: test_files/vulnerable_js_test.js:63

Description: Unsafe DOM manipulation with user input

25. Weak Cryptography (MEDIUM)

File: test_files/vulnerable_js_test.js:66

Description: Insecure random number generation

26. Weak Cryptography (HIGH)

File: test_files/vulnerable_js_test.js:67

Description: Weak hash algorithm

27. Weak Cryptography (HIGH)

File: test_files/vulnerable_js_test.js:68

Description: Weak encryption algorithm

28. Weak Cryptography (LOW)

File: test_files/vulnerable_js_test.js:69

Description: Base64 encoding/decoding is not encryption

29. Weak Cryptography (LOW)

File: test_files/vulnerable_js_test.js:90

Description: Base64 encoding/decoding is not encryption

30. Weak Cryptography (MEDIUM)

File: test_files/vulnerable_js_test.js:103

Description: Insecure random number generation

31. Weak Cryptography (MEDIUM)

File: test_files/vulnerable_js_test.js:104

Description: Weak cryptographic practice

32. Weak Cryptography (MEDIUM)

File: test_files/vulnerable_js_test.js:105

Description: Insecure random number generation

33. Hardcoded Credentials (HIGH)

File: test_files/vulnerable_js_test.js:72

Description: Hardcoded secrets or credentials detected

34. Hardcoded Credentials (HIGH)

File: test_files/vulnerable_js_test.js:73

Description: Hardcoded secrets or credentials detected

35. Hardcoded Credentials (CRITICAL)

File: test_files/vulnerable_js_test.js:74

Description: Hardcoded secrets or credentials detected

36. Hardcoded Credentials (CRITICAL)

File: test_files/vulnerable_js_test.js:74

Description: Hardcoded secrets or credentials detected

37. Hardcoded Credentials (CRITICAL)

File: test_files/vulnerable_js_test.js:75

Description: Hardcoded secrets or credentials detected

38. Hardcoded Credentials (CRITICAL)

File: test_files/vulnerable_js_test.js:75

Description: Hardcoded secrets or credentials detected

39. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:78

Description: Potentially vulnerable regular expression that could cause ReDoS

40. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:78

Description: Potentially vulnerable regular expression that could cause ReDoS

41. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:79

Description: Potentially vulnerable regular expression that could cause ReDoS

42. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:79

Description: Potentially vulnerable regular expression that could cause ReDoS

43. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:81

Description: Potentially vulnerable regular expression that could cause ReDoS

44. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:81

Description: Potentially vulnerable regular expression that could cause ReDoS

45. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_js_test.js:81

Description: Potentially vulnerable regular expression that could cause ReDoS

46. Path Traversal (HIGH)

File: test_files/vulnerable_js_test.js:94

Description: Potential path traversal vulnerability

47. Path Traversal (HIGH)

File: test_files/vulnerable_js_test.js:94

Description: Potential path traversal vulnerability

48. Path Traversal (HIGH)

File: test_files/vulnerable_js_test.js:94

Description: Potential path traversal vulnerability

49. Path Traversal (HIGH)

File: test_files/vulnerable_js_test.js:95

Description: Potential path traversal vulnerability

50. Template Injection (HIGH)

File: test_files/vulnerable_js_test.js:98

Description: Potential server-side template injection vulnerability

51. Template Injection (HIGH)

File: test_files/vulnerable_js_test.js:99

Description: Potential server-side template injection vulnerability

52. NoSQL Injection (HIGH)

File: test_files/vulnerable_js_test.js:108

Description: Potential NoSQL injection vulnerability

53. Unsafe Deserialization (HIGH)

File: test_files/vulnerable_js_test.js:29

Description: Unsafe deserialization of user input

54. Command Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:35

Description: Command injection vulnerability through user input

55. Command Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:37

Description: Command injection vulnerability through user input

56. Command Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:48

Description: Command injection vulnerability through user input

57. Command Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:51

Description: Command injection vulnerability through user input

58. Command Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:54

Description: Command injection vulnerability through user input

59. Command Injection (CRITICAL)

File: test_files/vulnerable_js_test.js:55

Description: Command injection vulnerability through user input

60. Hardcoded Credentials (CRITICAL)

File: test_files/test_owasp_llm.py:8

Description: Hardcoded secret or credential detected

61. Hardcoded Credentials (CRITICAL)

File: test_files/test_owasp_llm.py:9

Description: Hardcoded secret or credential detected

62. Hardcoded Credentials (CRITICAL)

File: test_files/test_owasp_llm.py:10

Description: Hardcoded secret or credential detected

63. Code Injection (CRITICAL)

File: test_files/test_owasp_llm.py:20

Description: Potential command injection vulnerability detected

64. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_ts_test.ts:12

Description: Potential Cross-Site Scripting (XSS) vulnerability

65. Cross-Site Scripting (XSS) (HIGH)

File: test_files/vulnerable_ts_test.ts:13

Description: Potential Cross-Site Scripting (XSS) vulnerability

66. Cross-Site Scripting (XSS) (CRITICAL)

File: test_files/vulnerable_ts_test.ts:18

Description: Potential Cross-Site Scripting (XSS) vulnerability

67. Prototype Pollution (HIGH)

File: test_files/vulnerable_ts_test.ts:83

Description: Potential prototype pollution vulnerability

68. Code Injection (CRITICAL)

File: test_files/vulnerable_ts_test.ts:32

Description: Code execution via eval() or dynamic code execution

69. Code Injection (CRITICAL)

File: test_files/vulnerable_ts_test.ts:59

Description: Code execution via eval() or dynamic code execution

70. Code Injection (CRITICAL)

File: test_files/vulnerable_ts_test.ts:89

Description: Code execution via eval() or dynamic code execution

71. Code Injection (CRITICAL)

File: test_files/vulnerable_ts_test.ts:90

Description: Code execution via eval() or dynamic code execution

72. Code Injection (CRITICAL)

File: test_files/vulnerable_ts_test.ts:91

Description: Code execution via eval() or dynamic code execution

73. Code Injection (CRITICAL)

File: test_files/vulnerable_ts_test.ts:92

Description: Code execution via eval() or dynamic code execution

74. Code Injection (HIGH)

File: test_files/vulnerable_ts_test.ts:97

Description: Code execution via eval() or dynamic code execution

75. Code Injection (HIGH)

File: test_files/vulnerable_ts_test.ts:100

Description: Code execution via eval() or dynamic code execution

76. Code Injection (HIGH)

File: test_files/vulnerable_ts_test.ts:177

Description: Code execution via eval() or dynamic code execution

77. Weak Cryptography (MEDIUM)

File: test_files/vulnerable_ts_test.ts:162

Description: Insecure random number generation

78. Weak Cryptography (MEDIUM)

File: test_files/vulnerable_ts_test.ts:166

Description: Weak cryptographic practice

79. Hardcoded Credentials (HIGH)

File: test_files/vulnerable_ts_test.ts:119

Description: Hardcoded secrets or credentials detected

80. Hardcoded Credentials (HIGH)

File: test_files/vulnerable_ts_test.ts:130

Description: Hardcoded secrets or credentials detected

81. Hardcoded Credentials (HIGH)

File: test_files/vulnerable_ts_test.ts:131

Description: Hardcoded secrets or credentials detected

82. Hardcoded Credentials (HIGH)

File: test_files/vulnerable_ts_test.ts:132

Description: Hardcoded secrets or credentials detected

83. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:24

Description: Non-null assertion operator may cause runtime errors

84. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:30

Description: Usage of 'any' type defeats TypeScript benefits

85. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:30

Description: Usage of 'any' type defeats TypeScript benefits

86. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:38

Description: Non-null assertion operator may cause runtime errors

87. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:49

Description: Non-null assertion operator may cause runtime errors

88. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:55

Description: Usage of 'any' type defeats TypeScript benefits

89. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:58

Description: Usage of 'any' type defeats TypeScript benefits

90. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:65

Description: Usage of 'any' type defeats TypeScript benefits

91. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:65

Description: Usage of 'any' type defeats TypeScript benefits

92. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:69

Description: Usage of 'any' type defeats TypeScript benefits

93. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:69

Description: Usage of 'any' type defeats TypeScript benefits

94. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:73

Description: Usage of 'any' type defeats TypeScript benefits

95. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:73

Description: Usage of 'any' type defeats TypeScript benefits

96. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:77

Description: Usage of 'any' type defeats TypeScript benefits

97. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:77

Description: Usage of 'any' type defeats TypeScript benefits

98. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:82

Description: Usage of 'any' type defeats TypeScript benefits

99. Unsafe Type Assertion (MEDIUM)

File: test_files/vulnerable_ts_test.ts:109

Description: Unsafe type assertion bypassing TypeScript type checking

100. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:109

Description: Non-null assertion operator may cause runtime errors

101. Unsafe Type Assertion (MEDIUM)

File: test_files/vulnerable_ts_test.ts:123

Description: Unsafe type assertion bypassing TypeScript type checking

102. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:123

Description: Usage of 'any' type defeats TypeScript benefits

103. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:123

Description: Usage of 'any' type defeats TypeScript benefits

104. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:123

Description: Usage of 'any' type defeats TypeScript benefits

105. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:125

Description: Non-null assertion operator may cause runtime errors

106. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:133

Description: Non-null assertion operator may cause runtime errors

107. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:141

Description: Non-null assertion operator may cause runtime errors

108. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:144

Description: Non-null assertion operator may cause runtime errors

109. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:145

Description: Non-null assertion operator may cause runtime errors

110. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:172

Description: Usage of 'any' type defeats TypeScript benefits

111. Unsafe Type Assertion (MEDIUM)

File: test_files/vulnerable_ts_test.ts:173

Description: Unsafe type assertion bypassing TypeScript type checking

112. Null Pointer Dereference Risk (MEDIUM)

File: test_files/vulnerable_ts_test.ts:173

Description: Non-null assertion operator may cause runtime errors

113. Unsafe Type Assertion (MEDIUM)

File: test_files/vulnerable_ts_test.ts:176

Description: Unsafe type assertion bypassing TypeScript type checking

114. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:176

Description: Usage of 'any' type defeats TypeScript benefits

115. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:176

Description: Usage of 'any' type defeats TypeScript benefits

116. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:176

Description: Usage of 'any' type defeats TypeScript benefits

117. Use of Any Type (LOW)

File: test_files/vulnerable_ts_test.ts:189

Description: Usage of 'any' type defeats TypeScript benefits

118. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_ts_test.ts:136

Description: Potentially vulnerable regular expression that could cause ReDoS

119. Regular Expression Denial of Service (ReDoS) (HIGH)

File: test_files/vulnerable_ts_test.ts:137

Description: Potentially vulnerable regular expression that could cause ReDoS

120. Path Traversal (HIGH)

File: test_files/vulnerable_ts_test.ts:91

Description: Potential path traversal vulnerability

121. Path Traversal (HIGH)

File: test_files/vulnerable_ts_test.ts:148

Description: Potential path traversal vulnerability

122. Path Traversal (HIGH)

File: test_files/vulnerable_ts_test.ts:148

Description: Potential path traversal vulnerability

123. Code Injection (CRITICAL)

File: test_files/test_eval.js:5

Description: Code execution via eval() or dynamic code execution

124. Code Injection (CRITICAL)

File: test_files/test_eval.js:8

Description: Code execution via eval() or dynamic code execution

125. Hardcoded Credentials (CRITICAL)

File: test_files/test_owasp_web.py:11

Description: Hardcoded secret or credential detected

126. Hardcoded Credentials (CRITICAL)

File: test_files/test_owasp_web.py:12

Description: Hardcoded secret or credential detected

127. Code Injection (CRITICAL)

File: test_files/test_owasp_web.py:15

Description: Potential command injection vulnerability detected

128. Code Injection (CRITICAL)

File: test_files/test_owasp_web.py:16

Description: Potential command injection vulnerability detected

129. Weak Cryptography (MEDIUM)

File: test_files/test_owasp_web.py:10

Description: Weak cryptographic algorithm detected

130. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:50

Description: Hardcoded secret or credential detected

131. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:50

Description: Hardcoded secret or credential detected

132. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:51

Description: Hardcoded secret or credential detected

133. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:52

Description: Hardcoded secret or credential detected

134. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:52

Description: Hardcoded secret or credential detected

135. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:53

Description: Hardcoded secret or credential detected

136. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:106

Description: Hardcoded secret or credential detected

137. Hardcoded Credentials (CRITICAL)

File: test_files/owasp_test.py:151

Description: Hardcoded secret or credential detected

138. SQL Injection (HIGH)

File: test_files/owasp_test.py:122

Description: Potential SQL injection vulnerability detected

139. Code Injection (CRITICAL)

File: test_files/owasp_test.py:67

Description: Potential command injection vulnerability detected

140. Code Injection (CRITICAL)

File: test_files/owasp_test.py:68

Description: Potential command injection vulnerability detected

141. Command Injection (HIGH)

File: test_files/owasp_test.py:126

Description: Potential command injection vulnerability detected

142. Weak Cryptography (MEDIUM)

File: test_files/owasp_test.py:109

Description: Weak cryptographic algorithm detected

143. Weak Cryptography (MEDIUM)

File: test_files/owasp_test.py:110

Description: Weak cryptographic algorithm detected