■ MCP Security Scan Report

Security Assessment for http://localhost:3000

Target Server:	http://localhost:3000
Server Name:	Test Server
Port:	3000
Protocol:	HTTP
Scan Date:	2025-10-15 22:51:41

Executive Summary

This report presents the findings from a comprehensive security assessment of the MCP server at **http://localhost:3000**. The scan identified **7 security issues** that require attention.

Overall Risk Score: 33/100

Severity	Count	Risk
Critical	2	■ Immediate Action Required
High	2	■ Important
Medium	1	■ Should Address
Low	1	■ Minor
Info	1	■ Informational

Detailed Findings

1. Missing Authentication

ID:	MCP-AUTH-001
Severity:	CRITICAL
Category:	Authentication
CVSS Score:	9.8/10.0
CWE:	CWE-306

Description:
The MCP server at http://localhost:3000 does not require authentication. Any client can connect and access all available tools and resources.

Evidence:
• Server URL: http://localhost:3000
• Successfully connected without credentials
• Available tools: 3
• Available resources: 1

Remediation:
Implement authentication mechanism such as:
- API keys
- OAuth 2.0
- Mutual TLS (mTLS)
- JWT tokens

2. Dangerous Tools Exposed Without Authorization

ID:	MCP-AUTHZ-001
Severity:	CRITICAL
Category:	Authorization
CVSS Score:	9.1/10.0
CWE:	CWE-285

Description:
The MCP server exposes 2 potentially dangerous tools without proper authorization controls. Combined with missing authentication, these tools can be abused for system compromise.

Evidence:
• Dangerous tools found: read_file, execute_command
• Total tools exposed: 3
• Authentication required: False

Remediation:
Implement proper authorization:
- Role-based access control (RBAC)
- Principle of least privilege
- Input validation for all tools
- Audit logging for tool usage

3. Unencrypted Connection

ID:	MCP-CRYPTO-001
Severity:	HIGH
Category:	Encryption
CVSS Score:	7.5/10.0
CWE:	CWE-319

Description:
The MCP server at http://localhost:3000 does not use TLS/SSL encryption. All communication is transmitted in plaintext, allowing attackers to intercept sensitive data including credentials and API responses.

Evidence:
• Server URL: http://localhost:3000
• Protocol: HTTP (unencrypted)
• Traffic can be intercepted

Remediation:
Enable TLS/SSL encryption:
- Use HTTPS instead of HTTP
- Install valid SSL certificate
- Configure TLS 1.2 or higher
- Disable weak cipher suites

4. Command Execution Tools Exposed

ID:	MCP-INJ-004
Severity:	HIGH
Category:	Injection
CVSS Score:	8.1/10.0
CWE:	CWE-78

Description:
The MCP server at http://localhost:3000 exposes command execution tools (execute_command). These are high-risk tools that could allow command injection if not properly secured.

Evidence:
• Command execution tools: execute_command
• High-risk functionality exposed
• Potential for system compromise

Remediation:
Secure command execution tools:
- Implement strict input validation
- Use allowlists for permitted commands
- Never execute shell commands with user input
- Consider removing or restricting these tools
- Require authentication and authorization
- Log all command execution attempts

5. File Access Tools With Potential Path Traversal Risk

ID:	MCP-INJ-006
Severity:	MEDIUM
Category:	Injection
CWE:	CWE-22

Description:
The MCP server at http://localhost:3000 exposes file access tools (read_file) that may be vulnerable to path traversal if input validation is insufficient.

Evidence:
• File access tools: read_file
• Potential path traversal risk
• Input validation status unknown

Remediation:
Secure file access tools:
- Implement strict path validation
- Use allowlists for permitted directories
- Canonicalize paths before access
- Never trust user-supplied file paths
- Restrict file system access scope

6. Default Port Configuration

ID:	MCP-CONFIG-001
Severity:	LOW
Category:	Configuration

Description:
The MCP server is running on a default port (3000). This makes it easier for attackers to discover and target the server.

Evidence:
• Current port: 3000
• Default port detected

Remediation:
Change to a non-standard port:
- Use a random high port (>10000)
- Update firewall rules accordingly
- Document the port change

7. Version Information Disclosure

ID: MCP-INFO-001

Severity: INFO

Category: Information Disclosure

Description:
The server discloses its version (1.0.0), which can help attackers identify known vulnerabilities in that specific version.

Evidence:
• Disclosed version: 1.0.0

Remediation:
Minimize information disclosure:
- Remove or obfuscate version headers
- Use generic error messages
- Keep software updated regardless

Disclaimer:
This report is provided for informational purposes only. The findings represent potential security issues identified through automated scanning. Manual verification and testing are recommended before taking remediation actions.

Report Generated by: MCP Security Scanner v0.1.0
Generated: 2025-10-15 22:51:41

For more information, visit: https://github.com/Latteflo/mpc-security-scanner