



확실히하고 오래 성하는 지키는 장인들
融保工

MCP 툴 사용법

-융보공 CTF-



MCP (Model Context Protocol)

소개

- MCP란?
- ❑ Model Context Protocol (MCP)는 Anthropic에서 개발한 개방형 프로토콜로, AI 어시스턴트가 외부 도구와 데이터 소스에 안전하게 연결할 수 있도록 해주는 표준화된 통신 규약입니다.
- ❑ MCP의 핵심 구성 요소
 - ❑ **Tools**: AI가 실행할 수 있는 함수들 (파일 읽기, API 호출 등)
 - ❑ **Resources**: AI가 접근할 수 있는 데이터 소스 (파일, 데이터베이스 등)
 - ❑ **Prompts**: 미리 정의된 프롬프트 템플릿
 - ❑ **Sampling**: AI 모델에서 텍스트 생성 요청





MCP (Model Context Protocol)

소개

- MCP 서버-클라이언트 구조
- ❑ MCP 서버: 도구와 리소스를 제공하는 프로그램
- ❑ MCP 클라이언트: AI 어시스턴트 (Claude Desktop 등)
- ❑ 통신: JSON-RPC 2.0 프로토콜 사용





MCP 보안 취약점 및 주의사항

- 취약점 목록

- ❑ 명령어 실행 취약점
- ❑ 파일 시스템 접근 취약점
- ❑ 입력 검증 부족
- ❑ 권한 및 인증 부족
- ❑ 정보 노출
- ❑ 리소스 고갈 공격





MCP 툴 설치하기 (Windows 기준)

- Node js 설치

☐ <https://nodejs.org/ko/download>

☐ Msi 파일 다운받고 계속 Next 누르기

Node.js® 다운로드

Node.js® v22.17.0 (LTS) 를 Windows 환경에서 Docker 방식으로 npm 를(을) 사용해 설치하세요.

정보 Want new features sooner? Get the latest Node.js version instead and try the latest improvements!

```
1 # Docker는 각 운영 체제별로 설치 지침을 제공합니다.
2 # 공식 문서는 https://docker.com/get-started/에서 확인하세요.
3
4 # Node.js Docker 이미지를 풀(Pull)하세요:
5 docker pull node:22-alpine
6
7 # Node.js 컨테이너를 생성하고 쉘 세션을 시작하세요:
8 docker run -it --rm --entrypoint sh node:22-alpine
9
10 # Node.js 버전 확인:
11 node -v # "v22.17.0"가 출력되어야 합니다.
12
13 npm 버전 확인:
14 npm -v # 10.9.2가 출력되어야 합니다.
```

PowerShell [클립보드에 복사](#)

Docker는 컨테이너와 플랫폼입니다. 문제가 발생하면 [Docker's 웹사이트](#)를 방문하세요.

또는 x64 아키텍처가 실행 중인 Windows 환경에서 미리 빌드된 Node.js®를 다운로드하세요.

[Windows 설치 프로그램 \(.msi\)](#) [Standalone Binary \(.zip\)](#)

Node.js Setup

Welcome to the Node.js Setup Wizard

The Setup Wizard will install Node.js on your computer.

[Back](#) [Next](#) [Cancel](#)





MCP 툴 설치하기

- Node.js 설치 확인

❑ CMD에서 다음 명령어 입력:

`node --version` (버전 달라도 상관없어요)

`npm --version`

❑ 숫자가 뜨면 Node.js 설치완료

C:\> 명령 프롬프트

```
Microsoft Windows [Version 10.0.19045.5965]
(c) Microsoft Corporation. All rights reserved.

C:\Users\User>node --version
v20.19.0

C:\Users\User>npm --version
10.8.2

C:\Users\User>
```





MCP 툴 설치하기

- MCP Inspector 설치

□ 글로벌 설치 (권장)

MCP Inspector는 MCP 서버를 테스트하고 디버깅할 수 있는 개발자 도구입니다.

```
npm install -g @modelcontextprotocol/inspector
```

```
C:\Users\User>npm install -g @modelcontextprotocol/inspector  
/
```

□ MCP Inspector 실행

```
mcp-inspector
```

C:\WINDOWS\system32\cmd.exe - "node" "C:\Users\User\AppData\Roaming\npm"

```
C:\Users\User>  
C:\Users\User>mcp-inspector  
Starting MCP inspector...  
  □ Proxy server listening on 127.0.0.1:6277  
  ⓘ Session token: f1ad9a711b7ba5757e33abc69d6aaf99724911c3bf786e  
  ⓘ Use this token to authenticate requests or set DANGEROUSLY_OMIT_TOKEN  
  
  ⓘ Open inspector with token pre-filled:  
    http://localhost:6274/?MCP_PROXY_AUTH_TOKEN=f1ad9a711b7ba5757  
  
  ⓘ MCP Inspector is up and running at http://127.0.0.1:6274 ⓘ
```





MCP 툴 설치하기

- MCP Inspector 실행

□ 실행하기

웹 브라우저에

http://localhost:6274/?MCP_PROXY_AUTH_TOKEN...

복사 붙여넣기

```
C:\Users\User>mcp-inspector
Starting MCP inspector...
  □ Proxy server listening on 127.0.0.1:6277
  ♦ Session token: f1ad9a711b7ba5757e33abc69d6aaf99724911c3bf786e783eec10defdaacc25
  Use this token to authenticate requests or set DANGEROUSLY_OMIT_AUTH=true to disable

  ♦ Open inspector with token pre-filled:
    http://localhost:6274/?MCP_PROXY_AUTH_TOKEN=f1ad9a711b7ba5757e33abc69d6aaf99724911

  ♦ MCP Inspector is up and running at http://127.0.0.1:6274
```





MCP 툴 설명

■ 첫 화면

localhost:6274/?MCP_PROXY_AUTH_TOKEN=f1ad9a711b7ba5757e33abc69d6aaf99724911c3bf786e783eec10defdaacc25#resources

Gmail YouTube 지도 받은메일함(3597) StackEdit 성신여자대학교 LMS W3.CSS Demos 적분 구하기 xe^(x^... (295) Just Dance N... Hugging Face - Th... 모의해킹

MCP Inspector v0.15.0

Transport Type
SSE

URL
http://

> Authentication

Server Entry Servers File

> Configuration

Reconnect Disconnect

Connected

Resources Prompts Tools Ping Sampling Roots Auth

Resources

List Resources

Clear

Resource Templates

List Templates

Clear

Select

Select content

History

1. initialize

Server Notifications

No notifications yet





MCP 툴 설명

- 첫 화면

☐ Transport Type: SSE

☐ URL:

http://ip:port/sse

(CTFD 플랫폼 내의 주소를
붙여넣어 주세요.)

Connect 혹은 Reconnect 버튼으로
연결한 후, 하단에 Connected의
초록불이 들어오면 성공

MCP Inspector v0.15.0

Transport Type

SSE

URL

http://어쩌구저쩌구/sse

> Authentication

Server Entry

Servers File

> Configuration

Reconnect

Disconnect

Connected

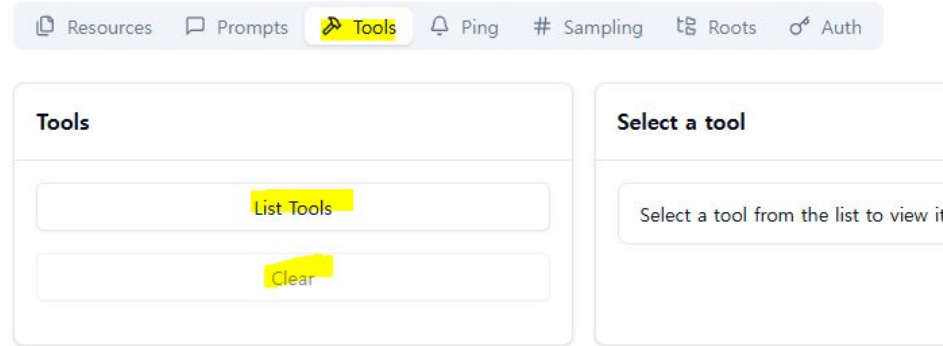




MCP란?

■ 툴 활용법

- ☐ Resources
 - ☐ List Resources / Clear
- ☐ Tools
 - ☐ List Tools / Clear



새 URL을 연결하셨거나, 상태가 변경되었을 때에는 꼭 **Clear**를 누른 후에 버튼을 눌러 주세요! **Clear** 누른 후 다시 **List** 해서 불러와주세요.

오류가 생길 경우 오픈채팅방에 스크린샷과 함께 문의주세요.
해당 툴은 AI를 사용하지 않습니다! AI를 활용하는 문제는 출제되지 않았으니,
툴의 기능을 사용하여 취약점을 찾아주세요.

<https://open.kakao.com/o/sC8BDREh>





다른 툴을 사용하고 싶은 경우

- Cursor / Claude Desktop

□ Config.json 파일에 다음과 같이 주소만 바꾸어 설정해주시면 됩니다.

```
"mcpServers": {  
  "Challenge 1": {  
    "command": "npx",  
    "args": [  
      "mcp-remote",  
      "http://127.0.0.1:9001/sse"  
    ]  
  },  
}
```

```
{  
  "mcpServers": {  
    "Challenge 1": {  
      "command": "npx",  
      "args": [  
        "mcp-remote",  
        "http://127.0.0.1:9001/sse"  
      ]  
    },  
    "Challenge 2": {  
      "command": "npx",  
      "args": [  
        "mcp-remote",  
        "http://127.0.0.1:9002/sse"  
      ]  
    },  
    [...]  
    "Challenge 9": {  
      "command": "npx",  
      "args": [  
        "mcp-remote",  
        "http://127.0.0.1:9010/sse"  
      ]  
    }  
  }  
}
```



Thank you

