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

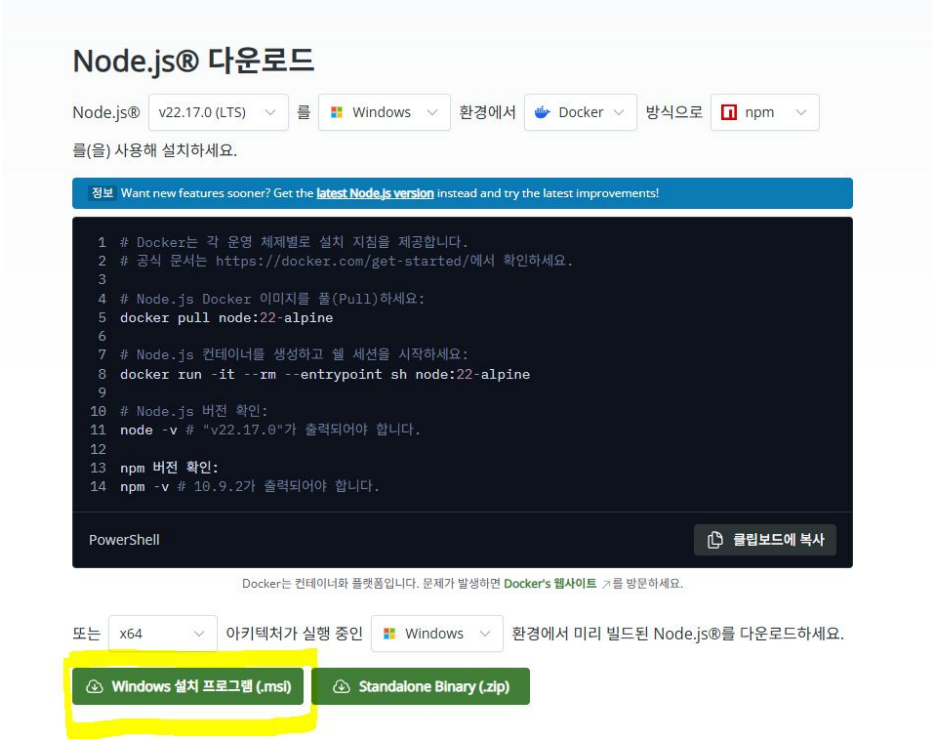
- 취약점 목록

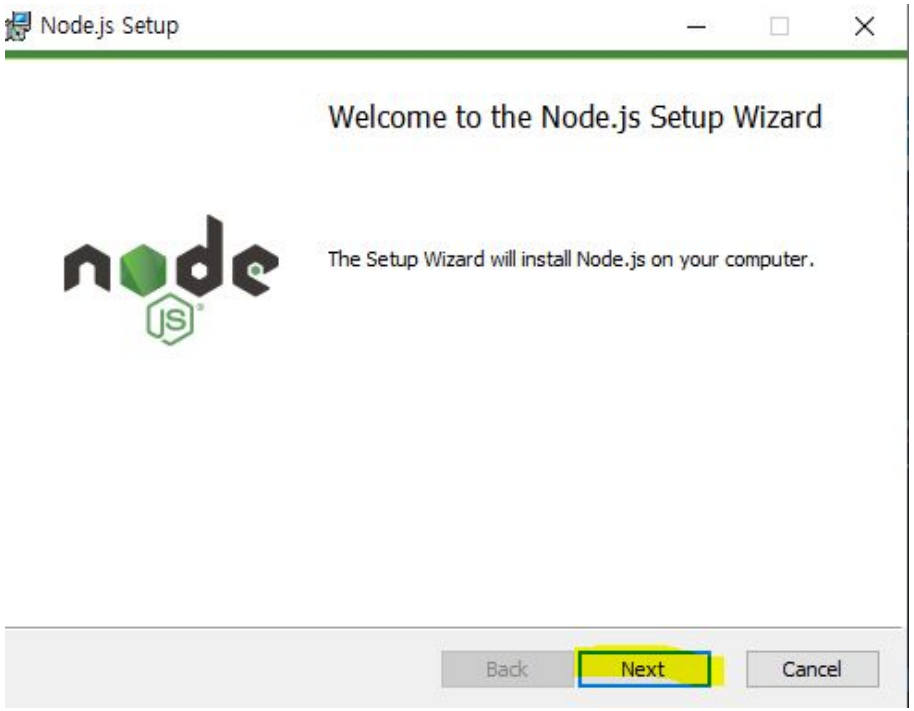
- 명령어 실행 취약점
- 파일 시스템 접근 취약점
- 입력 검증 부족
- 권한 및 인증 부족
- 정보 노출
- 리소스 고갈 공격

MCP 툴 설치하기 (Windows 기준)

- Node js 설치

- https://nodejs.org/ko/download
- Msi 파일 다운받고 계속 Next 누르기





MCP 툴 설치하기

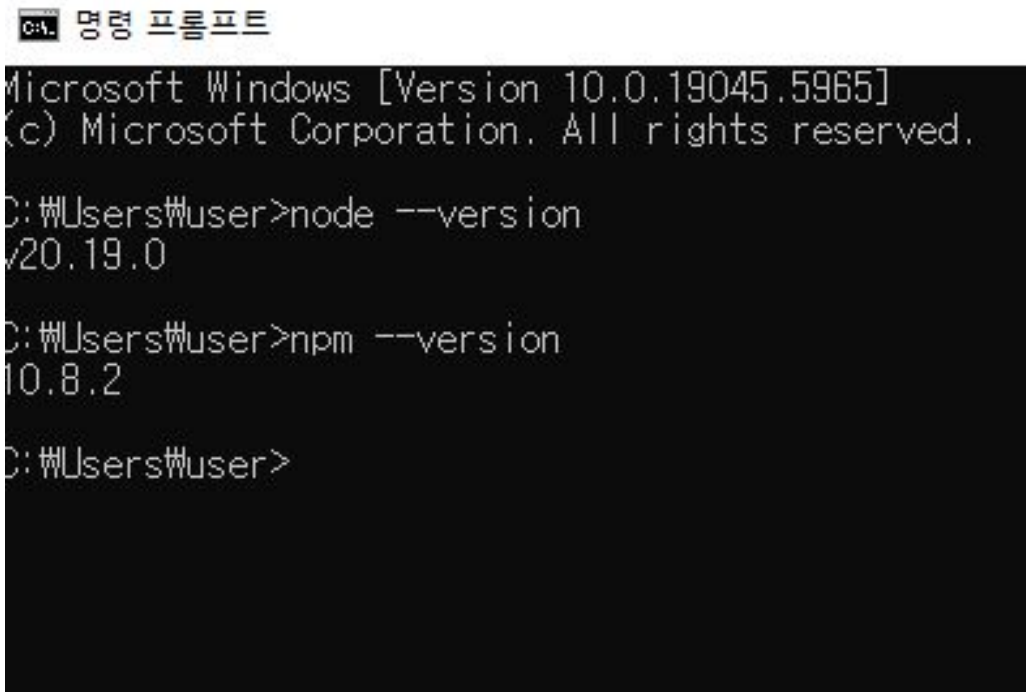
- Node.js 설치 확인

❒ CMD에서 다음 명령어 입력:

node --version (버전 달라도 상관없어요)

npm –version

❒ 숫자가 뜨면 Node.js 설치완료



MCP 툴 설치하기

- MCP Inspector 설치

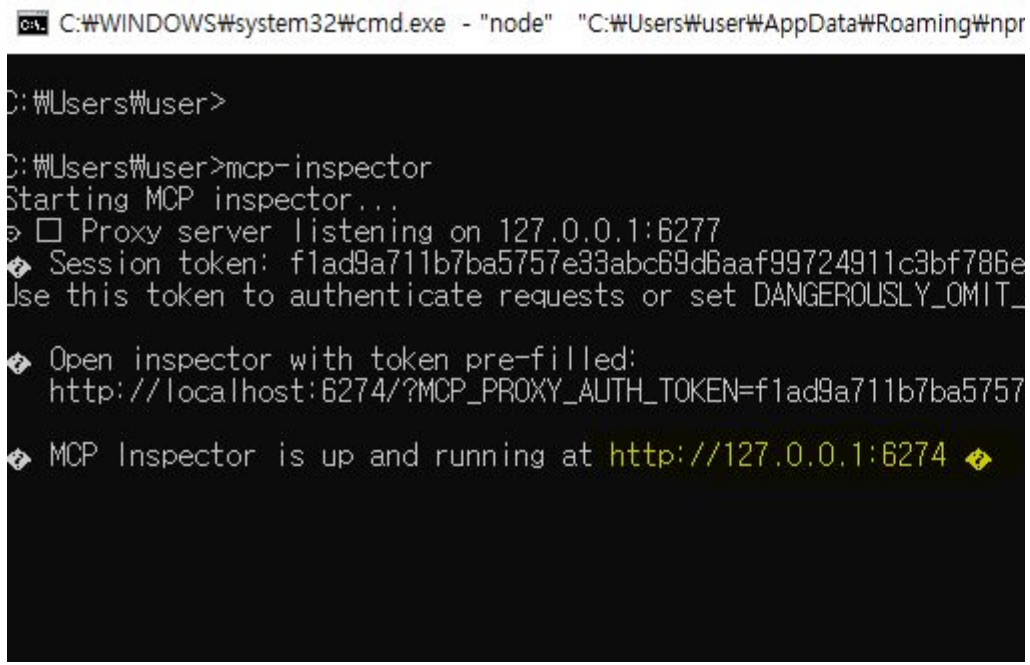
MCP Inspector는 MCP 서버를 테스트하고 디버깅할 수 있는 개발자 도구입니다.

❒ 글로벌 설치 (권장)

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

❒ MCP Inspector 실행

```
mcp-inspector
```



MCP 툴 설치하기

- MCP Inspector 실행

❒ 실행하기

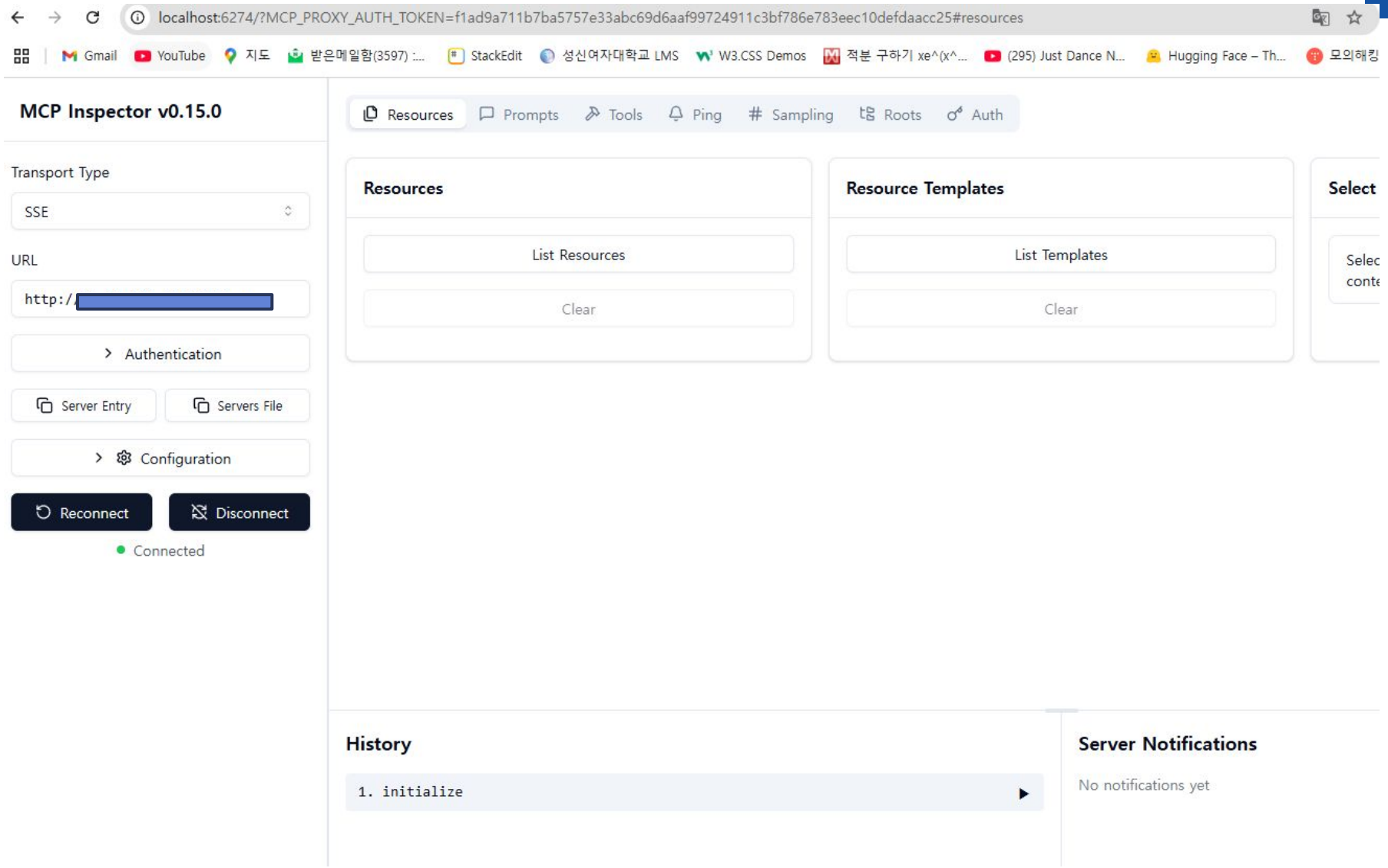
웹 브라우저에

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

복사 붙여넣기

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
History
1. initialize
Server Notifications
No notifications yet

MCP 툴 설명

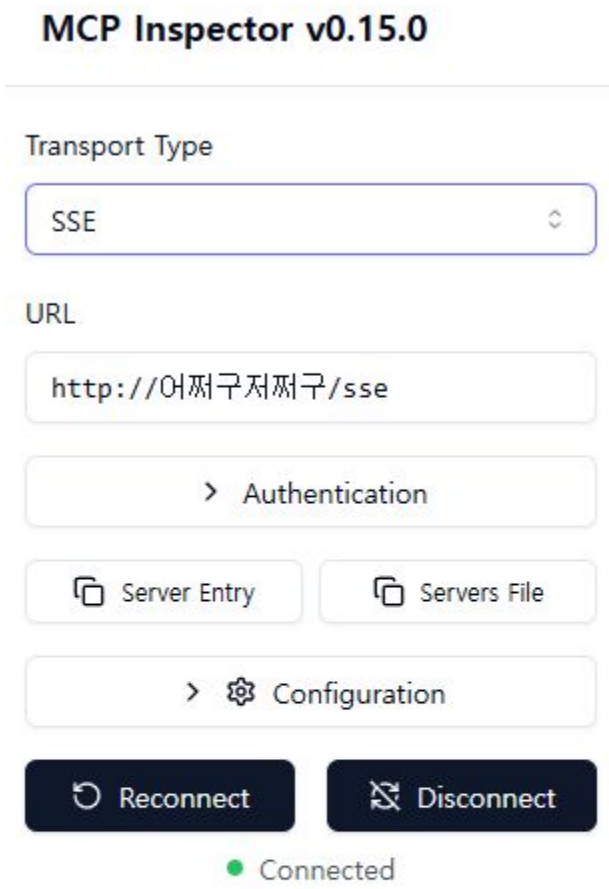
- 첫 화면

- Transport Type: SSE
- URL:

  http://ip:port/sse

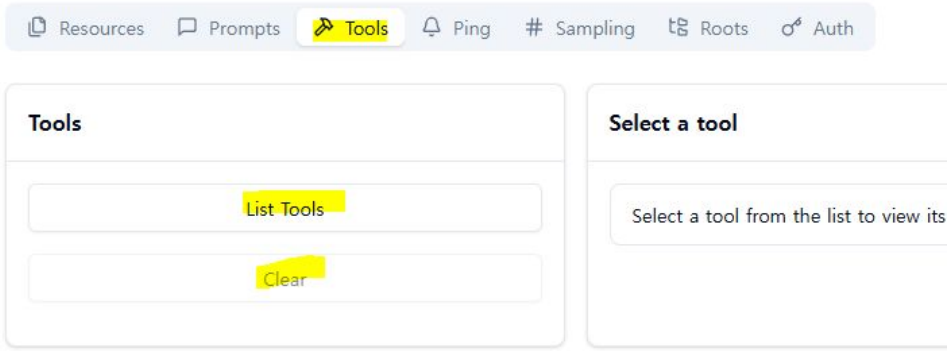
  (CTFD 플랫폼 내의 주소를 붙여넣어 주세요.)

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



MCP란?

- 툴 활용법



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

새 URL을 연결하셨거나, 상태가 변경되었을 때에는 꼭 Clear을 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"
      ]
    },
```

Thank you