بررسی MCP با مثالهایی از امنیت سایبری

Onhexgroup.ir

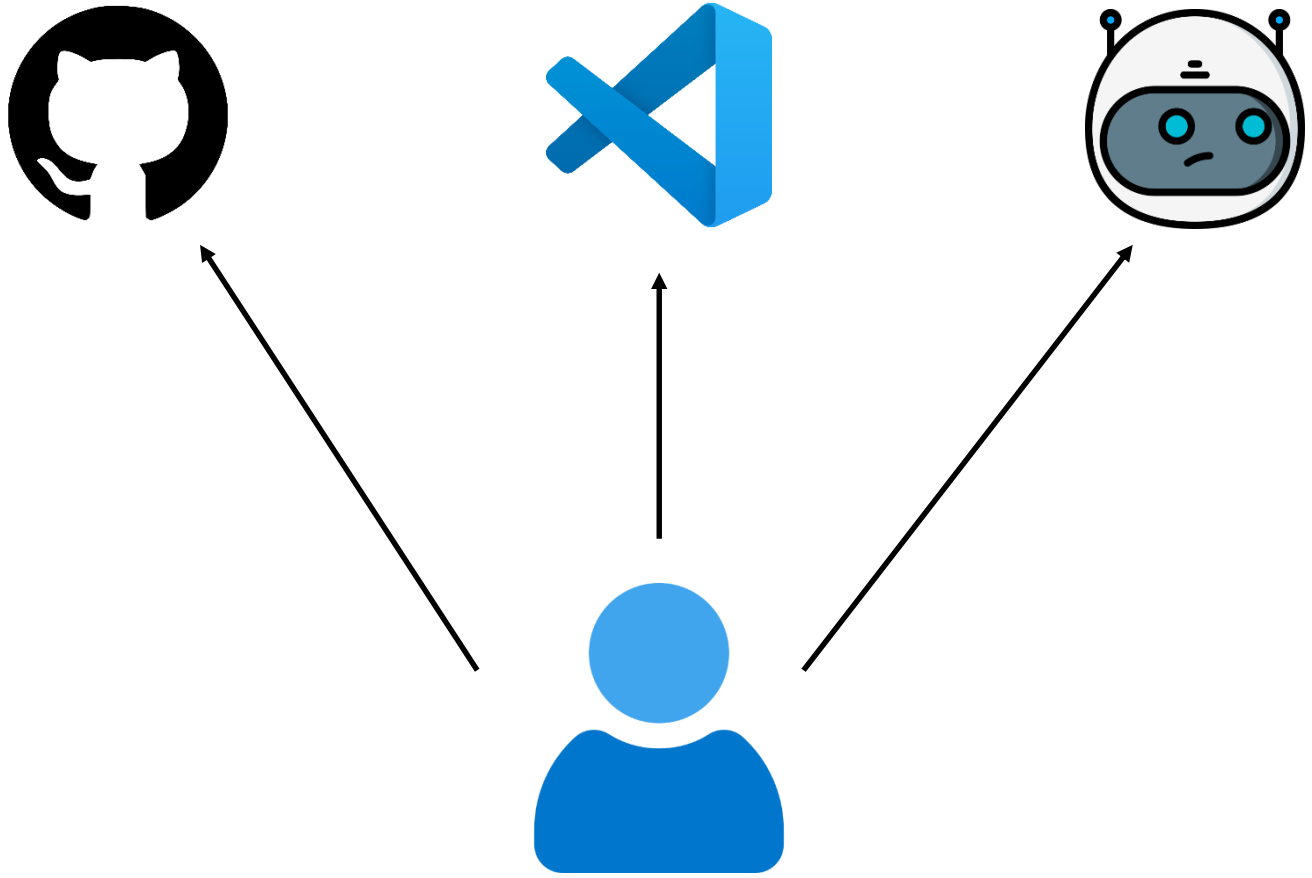
Github: onhexgroup

Telegram: onhex_ir

Youtube: onhexgroup

Youtube: onhexgroup

مدلهای زبانی بزرگ (LLM)

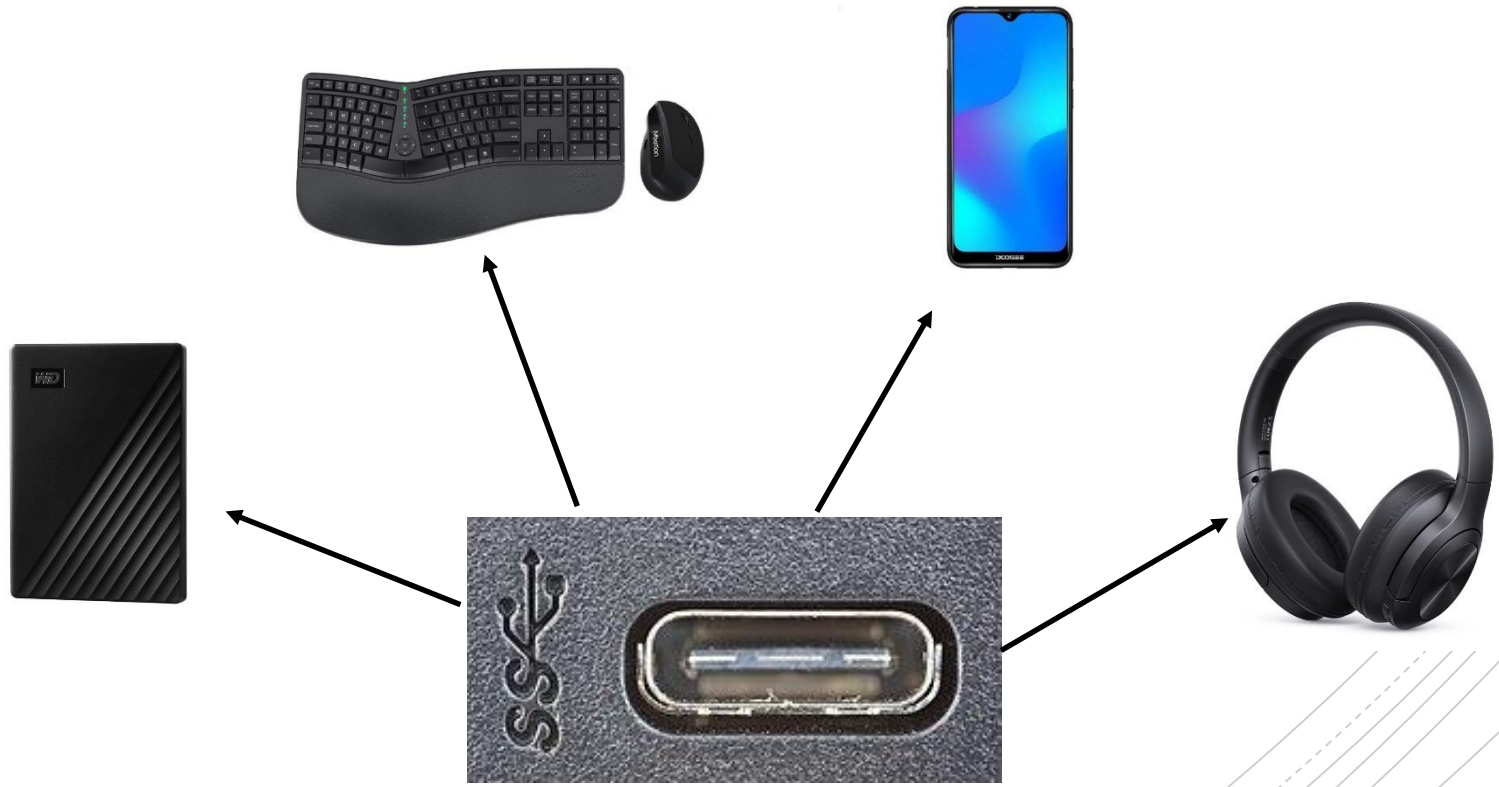


Github: onhexgroup

Model Context Protocol (MCP)

MCP یک پروتکل بازه که بستر ارتباط بین برنامه ها و مدلهای زبانی بزرگ رو استاندارد میکنه.

MCP مانند **USB-C** برای **LLM**هاست.



Aparat: onhexgroup

Model Context Protocol (MCP)

- مزایای MCP:
  - **انعطاف‌پذیری**: میتونیم سرورهای مختلف برای کارهای مختلف داشته باشیم (یکی برای فایلها، یکی برای اینترنت).
  - **نظم**: هر بخش کار خودش رو می‌کنه
  - **امنیت**: سرورها فقط به منابعی دسترسی دارن که اجازه‌ش رو دادیم.

Site: onhexgroup.ir

معماری کلی MCP

MCP از یک معماری کلاینت-سروری استفاده میکنه.

مولفه های تشکیل دهنده ی **MCP** موارد زیر هستن:

- **میزبان:** ابزارهایی که امکان چت با **LLM** رو فراهم میکنن. مانند **IDE**ها، **Claude Desktop** و ... .
- **کلاینت**: ارتباط بین میزبان و سرور رو فراهم میکنن.
- **سرور**: برنامه هایی خاصی که هر کدوم قابلیت های خاصی رو ارائه میدن.
- **منابع داده ای محلی**: داده های روی سیستم
- **سرویس راه دور**: سرویس های خارجی که از طریق اینترنت در دسترس هستن

Youtube: onhexgroup

معماری کلی MCP

ShadowMap

Remote Services

Server

Client

Local Data Sources

Server

Client

عکس ساعت ۱۲ ظهر گرفته شده

HOST

ارگ علیشاه تبریز ...

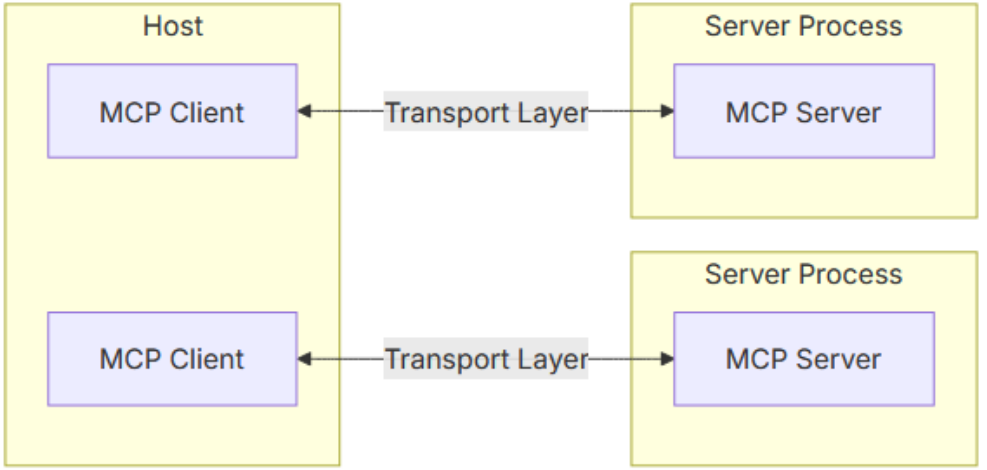
عکس رو بخون و بگو داخلش چیه و چه ساعتی گرفته شده؟

- **Transport** روش ارتباط بین پیامهای کلاینت و سرور رو مشخص میکنه.
- انواع پیام: درخواست (**request**) ، جواب (**response**) ، اعلان (**notification**) و خطا (**Errors**)
- همه ی پیامها باید در فرمت **JSON-RPC 2.0** باشن.

Transports

```
{
  "jsonrpc": "2.0",
  "method": "add",
  "params": [5, 3],
  "id": 1
}
```

```
{
  "jsonrpc": "2.0",
  "result": 8,
  "id": 1
}
```



Youtube: onhexgroup

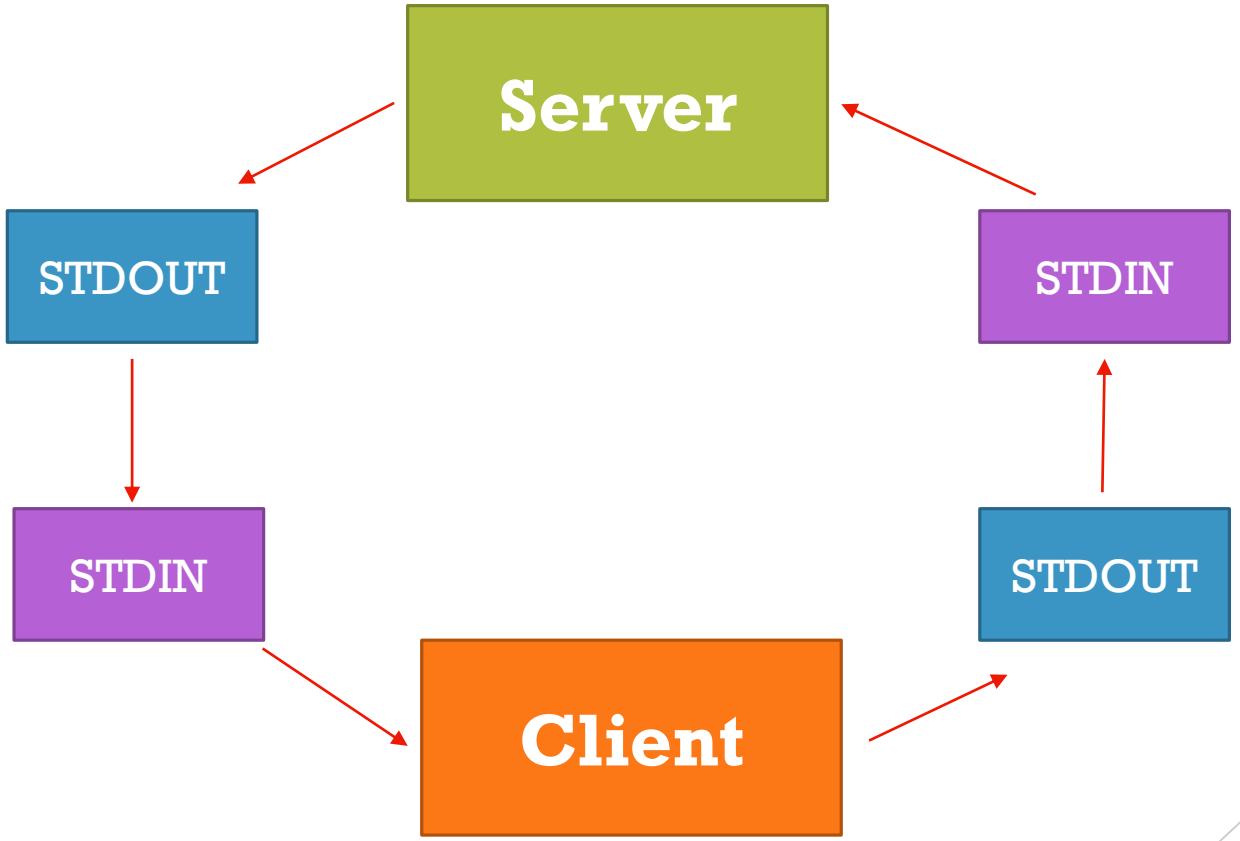
انواع Transport

- انواع Transport:
  - STDIO
  - SSE (Server-Sent Events)
  - روش اختصاصی

Site: onhexgroup.ir

Transport: STDIO

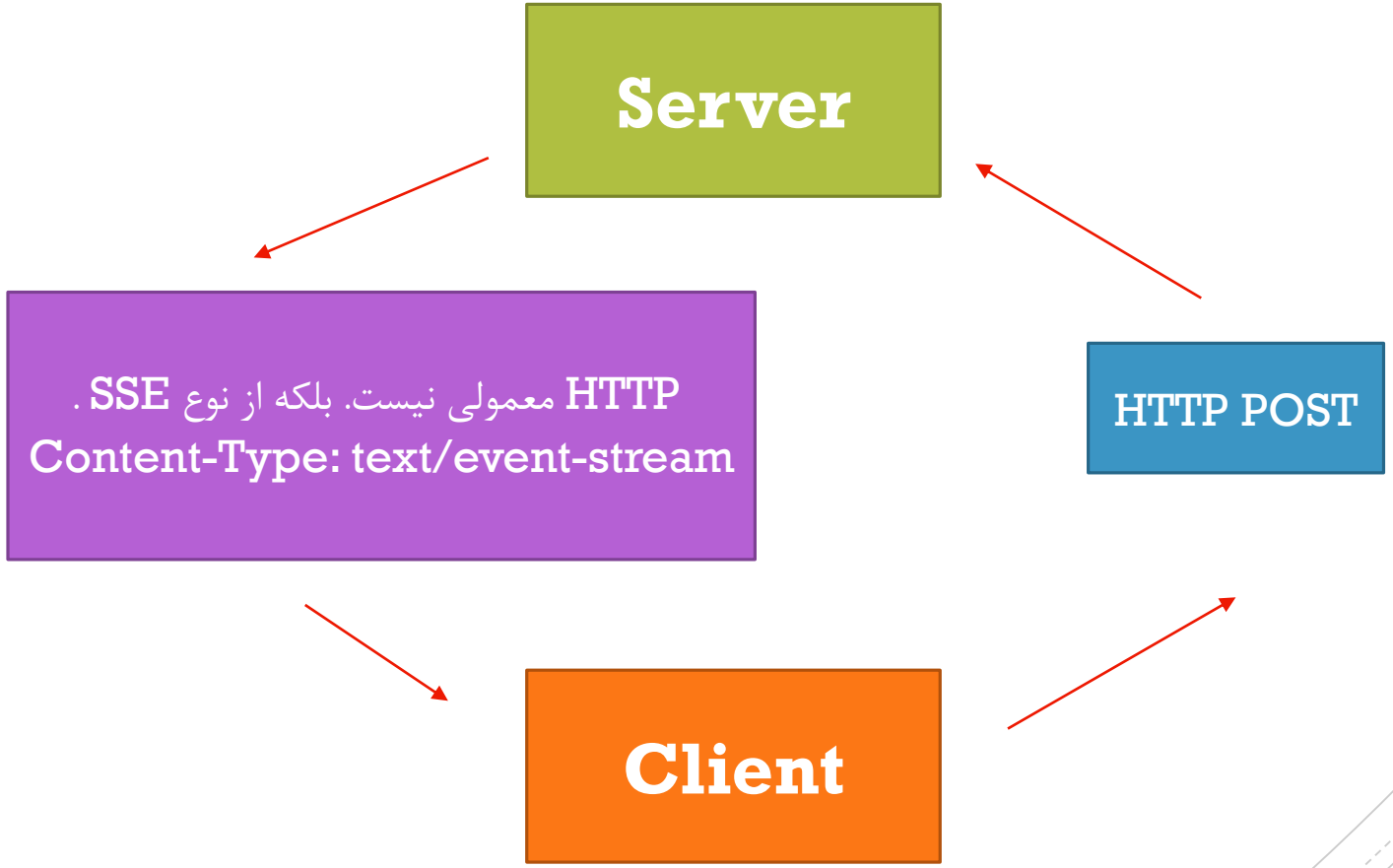
- **STDIO** از روش استاندارد **IO** استفاده میکنه.
- کاربردش بصورت محلی. کامند لاین و اسکریپت و ... .
- مثال: هوش مصنوعی میخواد به فایلهای روی سیستم دسترسی داشته باشه.



Github: onhexgroup

Transport: SSE

- **SSE** از پروتکل **HTTP** استفاده میکنه.
- کاربردش بصورت ریموت. سرویس های آنلاین و ... .
- مثال: هوش مصنوعی میخواد به قیمت لحظه ای دلار دسترسی پیدا کنه.



Twitter: onhexgroup

Transport: اختصاصی

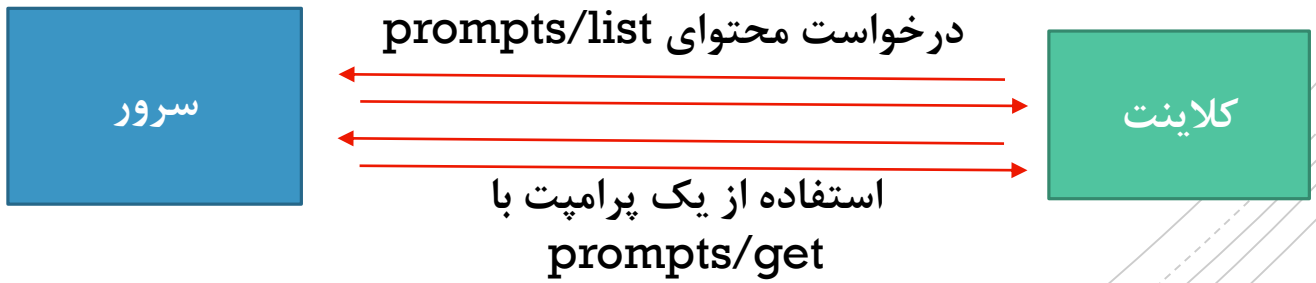
- **Transport** اختصاصی زمانی کاربرد داره که دو روش قبلی قابل استفاده نباشه.
- برای روش اختصاصی باید یسری قوانین رو رعایت کنیم:
  - فرمت پیامها روی **JSON-RPC 2.0** باشه.
  - خطاها مدیریت بشن
- مثال: بلوتوث

Youtube: onhexgroup

Prompts

- در دنیای هوش مصنوعی، معمولا به سوالات از مدل میگن، اما در **MCP** منظور یک درخواست آمده و قابل استفاده مجدد هستش.
- کلاینت با **prompts/list**، لیست پرامپتهارو میگیره و با **prompts/get** یک درخواست میگیره.

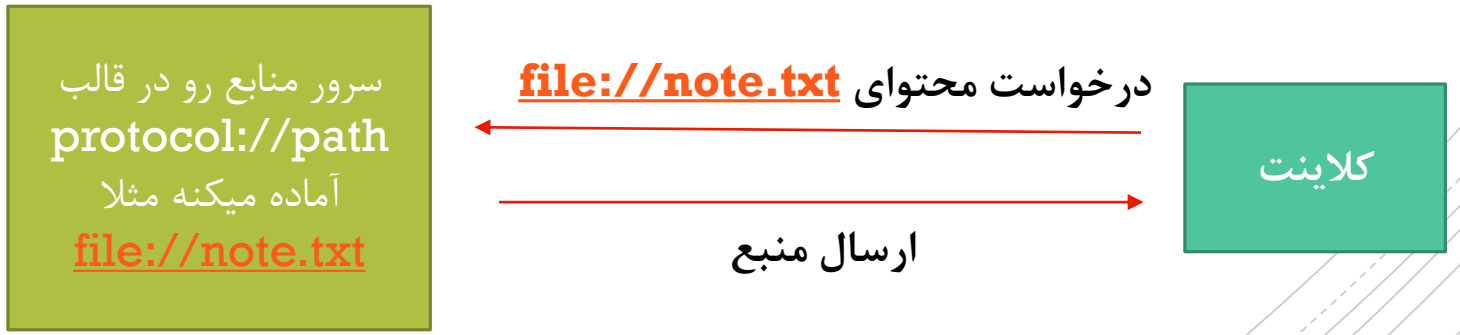
```
{
    name: "translate-text",
   description?:"translate txt from EN",
    arguments": {
                        "text": "Hello world",
                        "to_language": "fa"  }
}
```



Youtube: onhexgroup

منابع

- اطلاعاتی که سرورها آماده میکنن، تا کلاینتها (در نهایت **LLM**)، برای بهتر جواب دادن به سوالات ما ازش استفاده کنن. مانند عکس، سند، کد و ...
- انواع منبع:
  - متنی (کد، سند، یادداشت و ...)
  - باینری (عکس، ویدیو و ... | کد شده با **Base64**)



twitter: onhexgroup

ابزار

- توابع یا دستوراتی که سرورها آماده میکنن، تا کلاینتها (در نهایت **LLM**)، برای بهتر جواب دادن به سوالات ما ازش استفاده کنن. مانند گرفتن اطلاعات، محاسبه ی چیزی و ...
- کلاینت از طریق **tools/list** ، لیست ابزارهارو بدست بیاره.
- کلاینت از طریق **tools/call**، ابزارهارو فراخوانی میکنه.
- منابع معمولا بدون تغییر هستن اما ابزارها حالت داینامیک دارن.
- هر ابزار یک اسم، توضیحات (اختیاری) و یک **inputSchema** داره که میگه چه اطلاعاتی نیاز داره.

```
{
  name: string;          // Unique identifier for the tool
  description?: string;  // Human-readable description
  inputSchema: {         // JSON Schema for the tool's parameters
    type: "object",
    properties: { ... }  // Tool-specific parameters
  }
}
```

یک MCP Server برای خوندن RSS FEEDها

Github: onhexgroup

مثال

TOOLS: FeedReader

Server

1- a....
2- b....
3- c....

Client

HOST

3 تا از آخرین پستهای سایت NY رو لیست کن.

Youtube: onhexgroup

IDA pro MCP SERVER

تابع **Main** رو پیدا کن.

HOST

Client

Server

Site: onhexgroup.ir

Burp Suite MCP SERVER

سایت **openai.com** رو اسکن کن

HOST

Client

Server

Github: onhexgroup

Shodan MCP SERVER

اهدافی برای آسیب پذیری
CVE-2025-2945
میخواستم

HOST

Client

Server

SHODAN

Github: onhexgroup

منابع

- https://github.com/mrexodia/ida-pro-mcp
- https://git-scm.com/downloads/win
- https://github.com/mrexodia/mcp-reversing-dataset
- https://jro.sg/ida-mcp-exec.html
- https://github.com/PortSwigger/mcp-server?tab=readme-ov-file#manual-installations
- https://github.com/BurtTheCoder/mcp-shodan
- https://nodejs.org/en
- https://modelcontextprotocol.io/introduction
- https://mcpmarket.com/categories/security-testing
- https://github.com/apappascs/mcp-servers-hub