

robots.txtとError handling

-
- The screenshot shows the Burp Suite Professional v2.3.20 interface. The 'Target' tab is selected, displaying a site map of the target application. The site map shows a root directory 'http://10.10.10.10:3000/#/' with several sub-directories and files listed, including 'api', 'assets', 'main.js', 'polyfills.js', 'rest', 'runtime.js', 'socket.io', 'styles.css', 'support', and 'vendor.js'. The 'Issues' tab is also visible, showing a list of issues. The 'Advisory' tab is also visible, showing a list of advisories.

-
- Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders
- Contents Issues
- | Host | Method | URL | Params | Status | Length |
|-------------|--------|---|--------|--------|--------|
| 10.10.10.10 | GET | /socket.io/?EIO=4&transport=websocket&sid=... | ✓ | 101 | 129 |
| 10.10.10.10 | GET | /api/Challenges/ | | 200 | 74061 |
| 10.10.10.10 | GET | /rest/products/search | | 200 | 13218 |
| 10.10.10.10 | GET | /robots.txt | | 200 | 355 |
| 10.10.10.10 | GET | /socket.io/?EIO=4&transport=websocket&sid=... | ✓ | 200 | 232 |
| 10.10.10.10 | POST | /socket.io/?EIO=4&transport=websocket&sid=... | ✓ | 200 | 121 |
| 10.10.10.10 | GET | /socket.io/?EIO=4&transport=websocket&sid=... | ✓ | 200 | 168 |
| 10.10.10.10 | GET | /socket.io/?EIO=4&transport=websocket&sid=... | ✓ | 200 | 136 |
| 10.10.10.10 | GET | /assets | | 301 | 544 |
| 10.10.10.10 | GET | / | | 304 | 340 |
| 10.10.10.10 | GET | /Materialicons-Regular... | | 304 | 341 |
- Request
- Raw Hex \n ☰
- ```

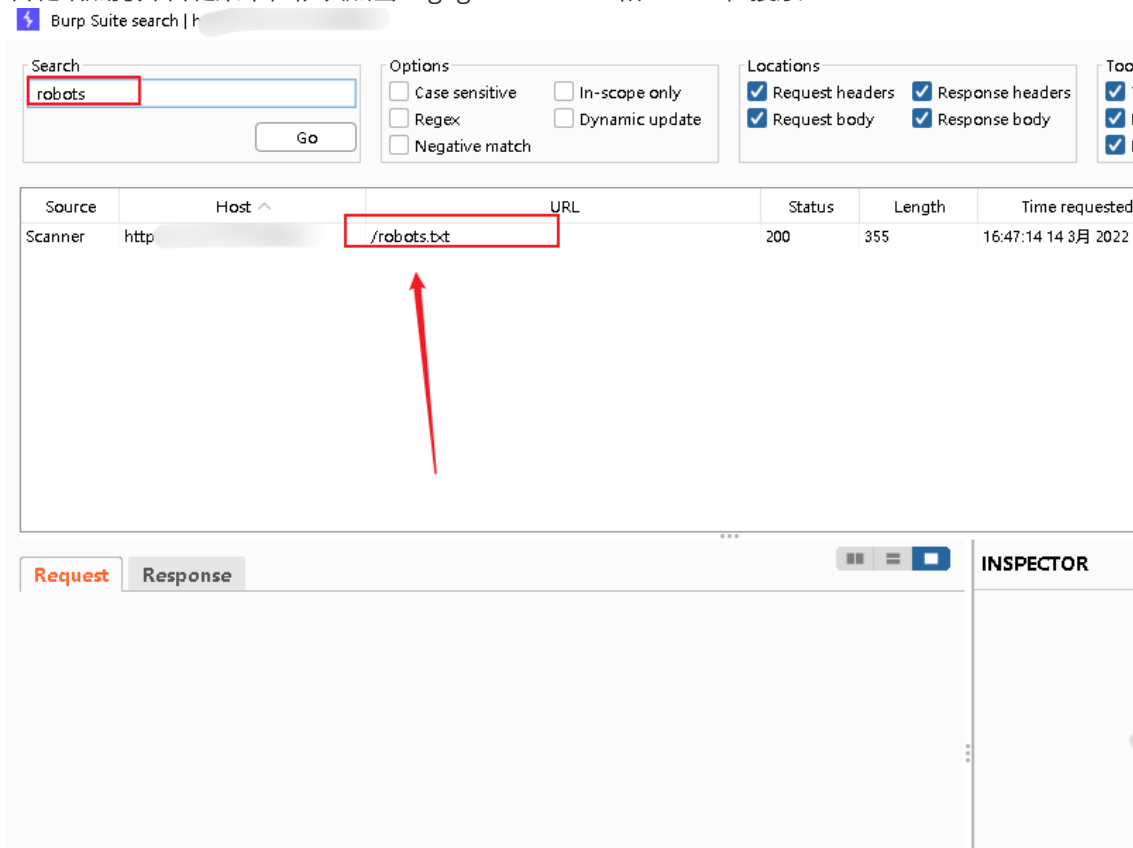
1 GET /socket.io/?EIO=4&transport=websocket&sid=
2 MCn-URRCcM9nkd0TAAId HTTP/1.1
3 Host: 10.10.10.10
4 Connection: Upgrade
5 pragma: no-cache
6 Cache-Control: no-cache
7 User-Agent: Mozilla/5.0 (Windows NT 10.0;
8 Win64; x64) AppleWebKit/537.36 (KHTML, like
9 Gecko) Chrome/95.0.4638.54 Safari/537.36
10 Upgrade: websocket
11 Origin: http://
12 Sec-WebSocket-Version: 13
13 Accept-Encoding: gzip, deflate
14 Accept-Language: zh-CN,zh;q=0.9
15 Cookie: language=en; welcomebanner_status=
16 dismiss; cookieconsent_status=dismiss; token=
17 eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0
18 dXMiOiJzdWN1ZXRzLCJlYiI6ZGF0YXN1ZSIsImVudCI6ImVzZ
19

```
- Response
- Pretty Raw Hex
- ```

1 HTTP/1.1 101 Sw
2 Upgrade: websock
3 Connection: Upgr
4 Sec-WebSocket-A
5 FxikXFtjntdVlw5
6

```

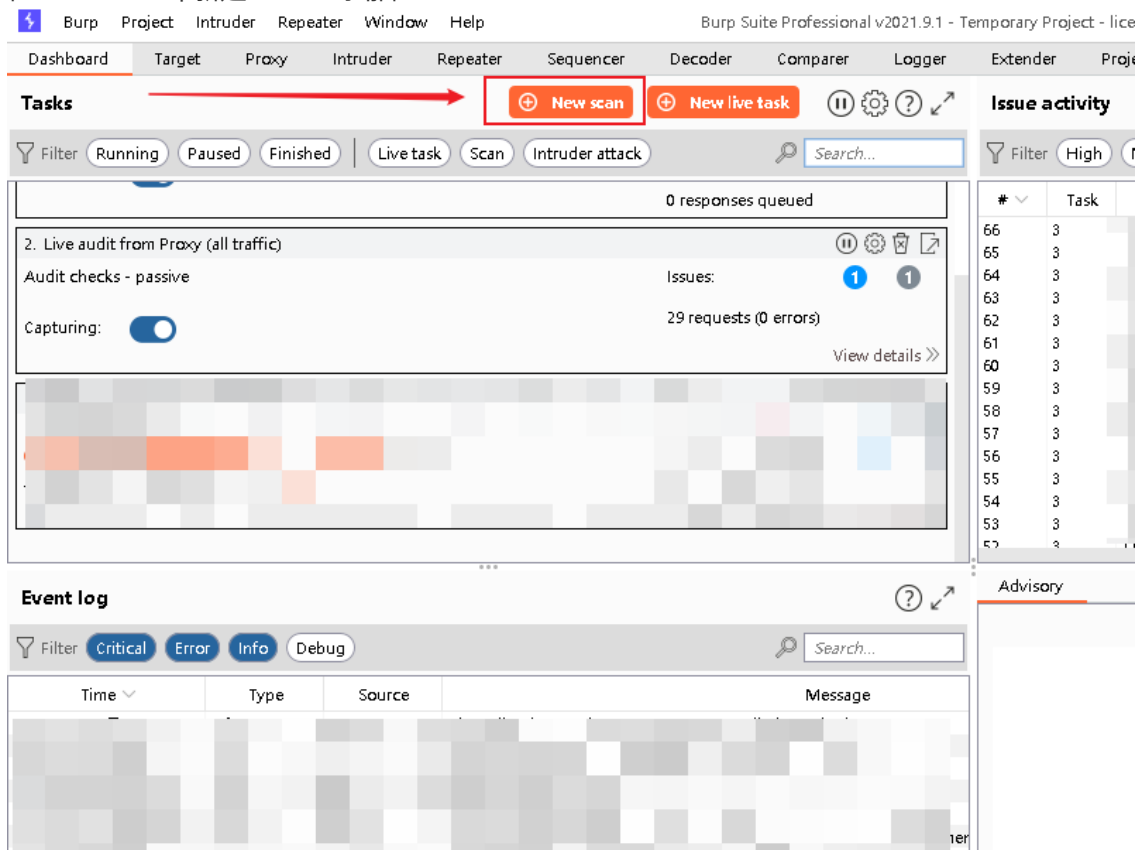
3. 右键站点打开右键菜单，依次点击Engagement tools和Search，搜索robots



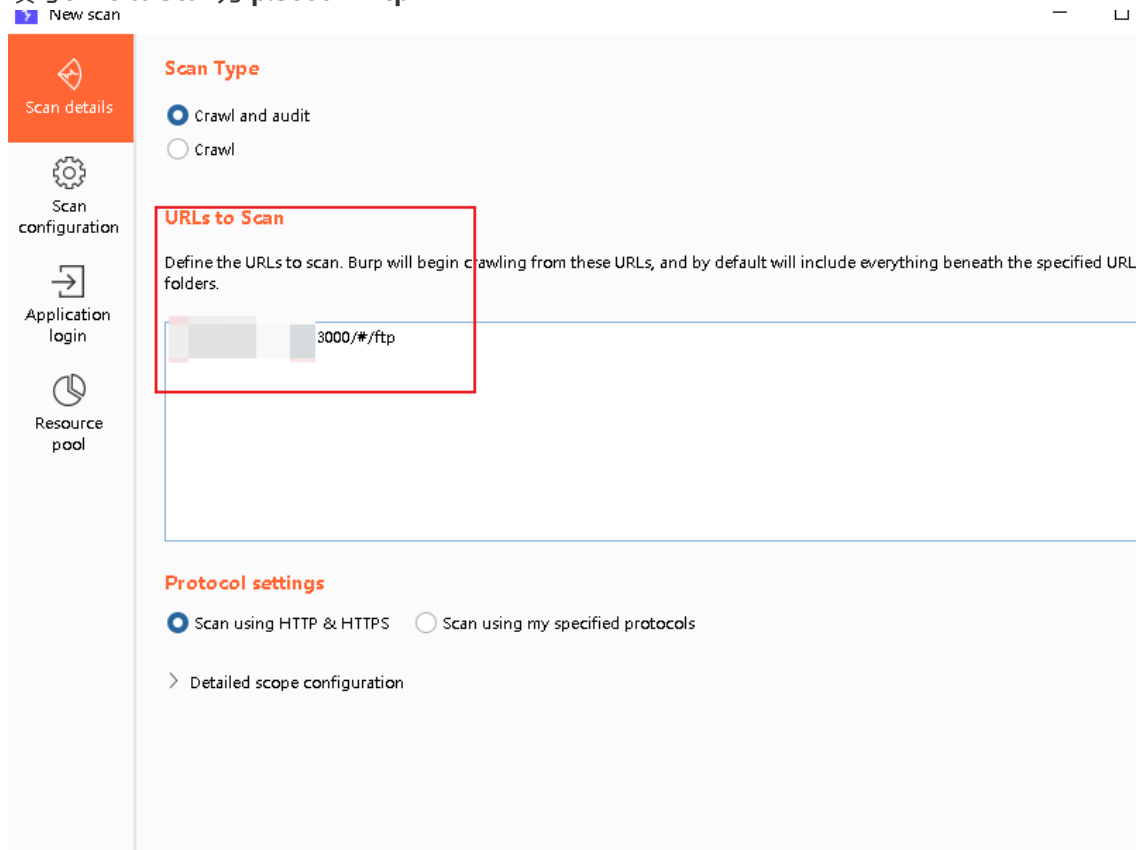
4. 在activity scan过程中，Error handling挑战成功

Confidential Document

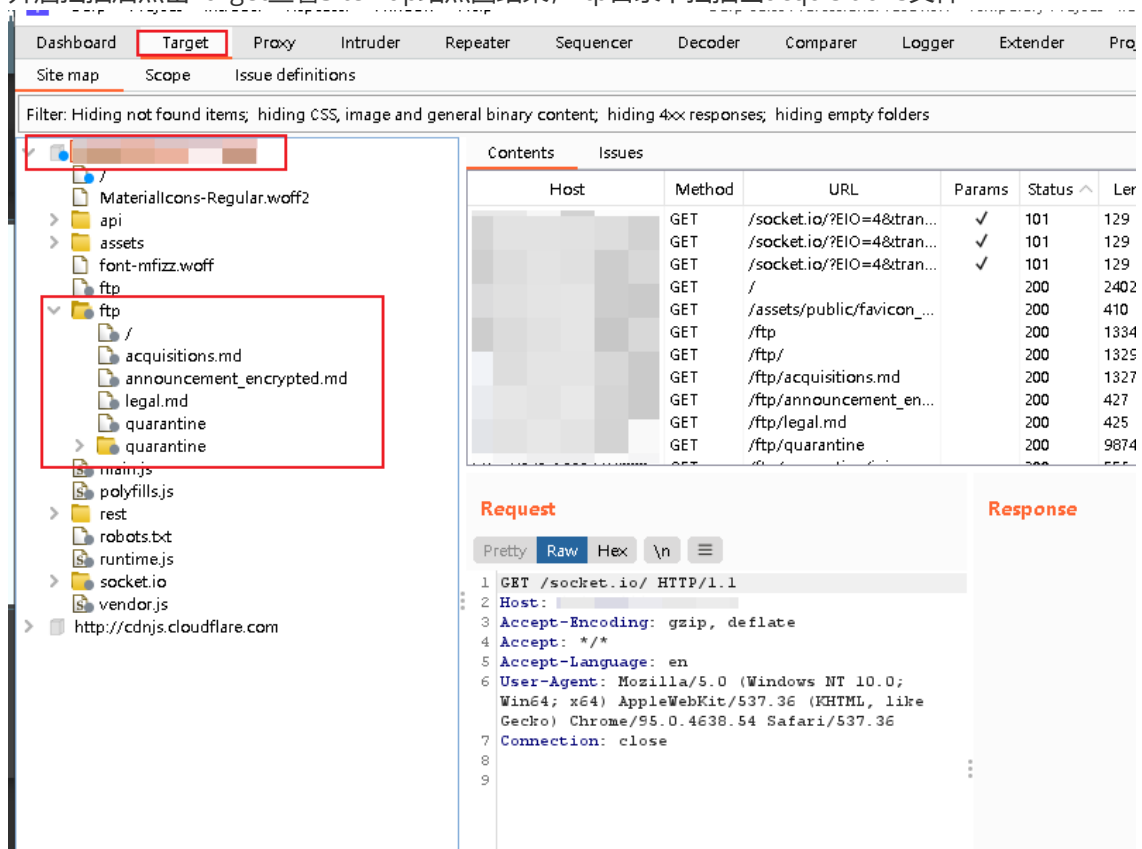
1. 在DashBoard中新建Scanner扫描



2. 填写URLs to Scan为ip:3000/#/ftp



3. 开启扫描后点击Target查看SiteMap站点图结果，ftp目录下扫描出acquisitions文件



4. 访问文件后，Confidential Document挑战成功