Tushar Follow
Mar 2, 2021 · 2 min read · Listen

Authenticated Blind & Error based SQL injection on Local Services Search Engine Management System -v 1.0

Product: LSSMES-V1.0

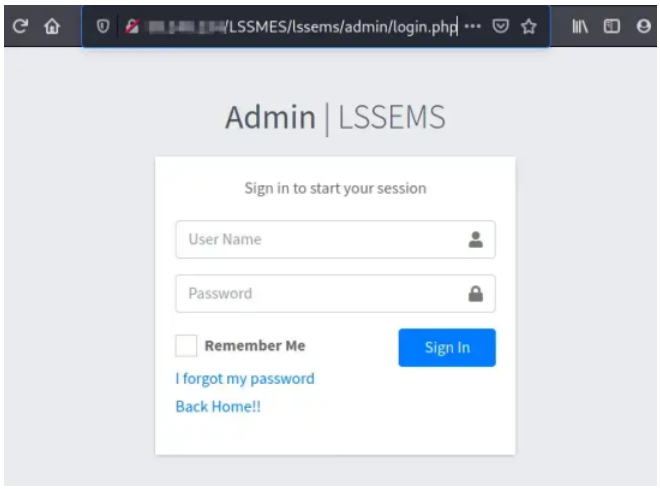
Vulnerability Title: Authenticated Blind & Error SQLi

Identifier: Owasp Top 10: Injection

Detailed description: It was found that when we update Category using the admin login, edit-category-detail.php is given a GET request containing **editid** and with all other parameters. Whereas, **editid** is the parameter that is vulnerable to SQLi. As an admin, a user can dump all the data from the database.

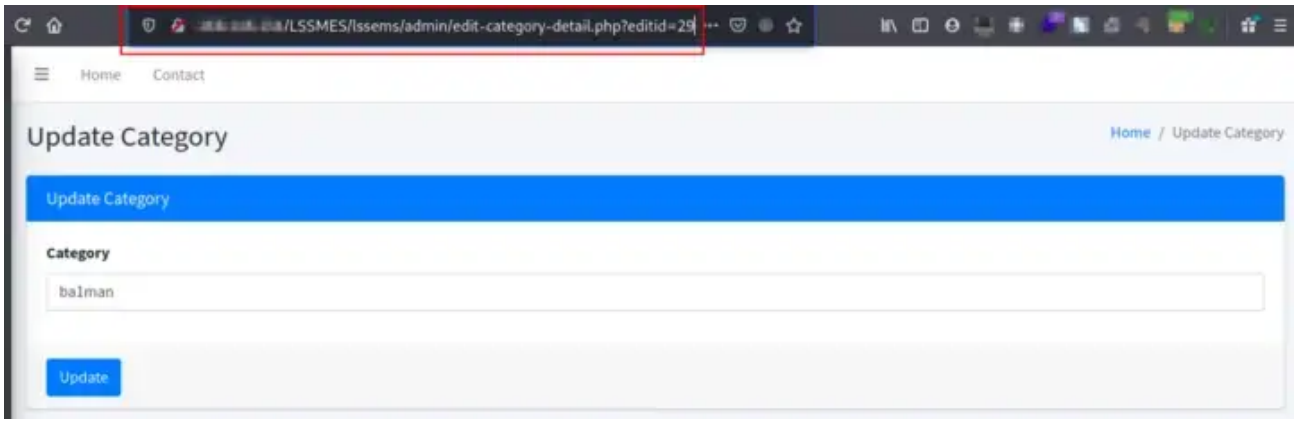
Steps to reproduce:

1. Login to the admin page of LSSMES-V1.0, which is http://server_ip/LSSMES/lssems/admin/login.php



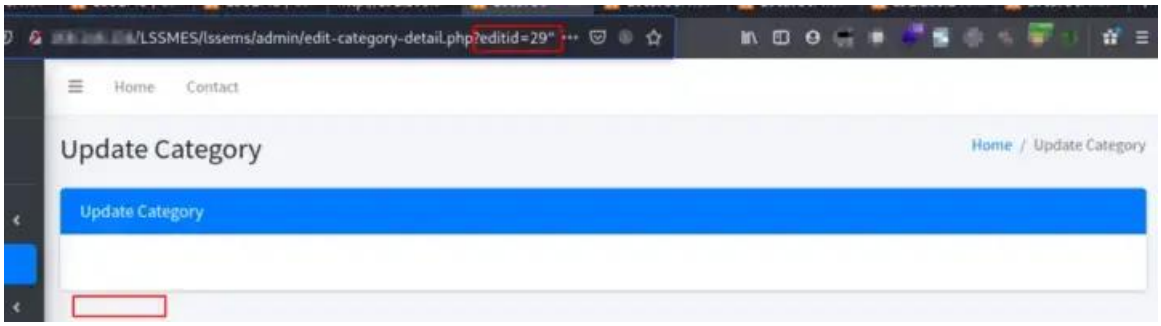
Admin login page

2. Click on, Service Category → Manage Category to update presence data.



Normal respond

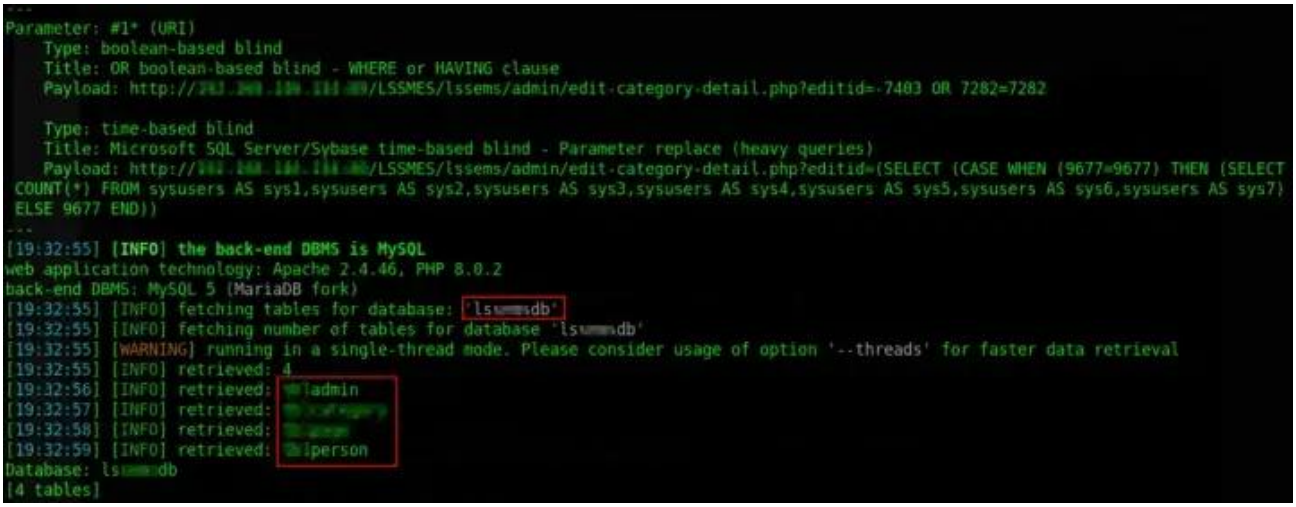
3. Just a double quote on **editid** parameter will confirm the SQL injection as below shown image. Update button disappears.



Application misbehaviour

4. After confirming that **editid** is vulnerable to SQL injection feeding the request to SQLMAP will do the rest of the work for us 😊

The result of SQLMAP against the **editid** parameter



Boom!!!

Linkedin Profile: https://www.linkedin.com/in/tushar-vaidya-2111s5/

Sql Injection Sqlmap Projects