nu11secur1ty / CVE-nu11secur1ty Public

Code Issues Pull requests Actions Projects Security Insights

main

CVE-nu11secur1ty / vendors / oretnom23 / 2022 / Cosmetics-and-Beauty-Product-Online-Store /

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

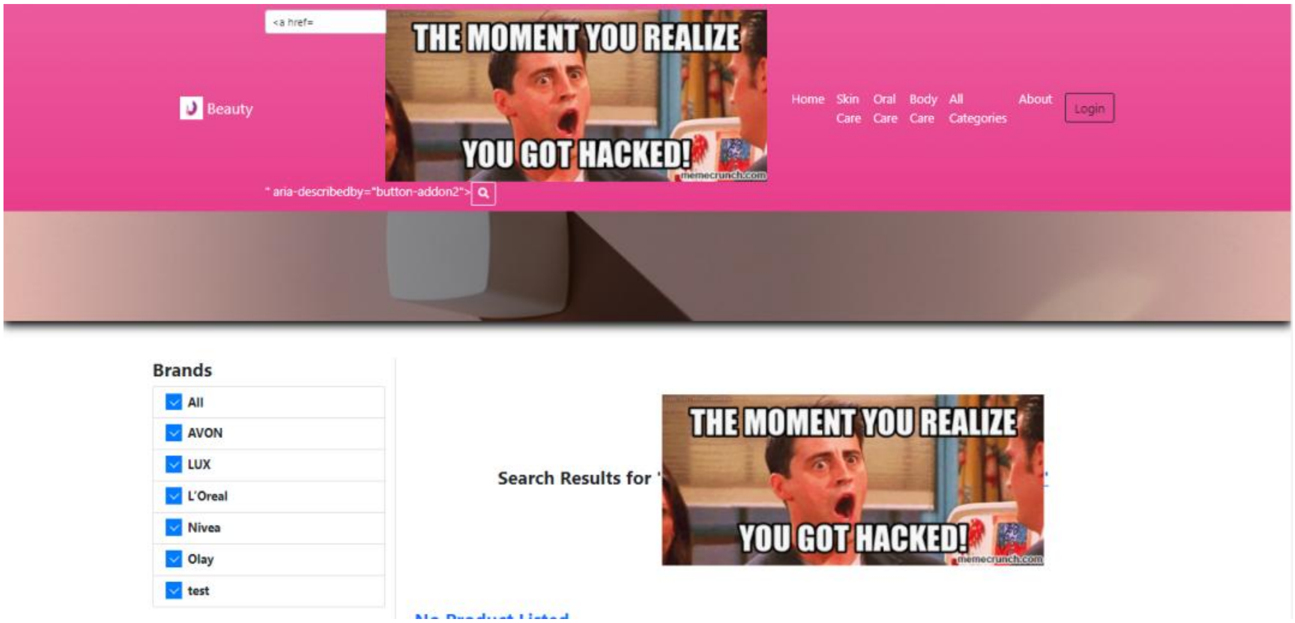
..

Docs	9 months ago
PoC	9 months ago
SQL-Injection	9 months ago
README.MD	9 months ago

README.MD

Cosmetics-and-Beauty-Product-Online-Store

Vendor



Brands

☑ All

☑ AVON

☑ LUX

☑ L'Oreal

☑ Nivea

☑ Olay

☑ test

Search Results for '

No Product Listed

Description:

The `search` parameter from /cbpos/ app on Cosmetics and Beauty Product Online Store v1.0 appears to be vulnerable to multiple XSS-Reflected attacks. The attacker can take very sensitive information from the system and even he can prepare a very dangerous RCE by using this XSS vulnerability.

Status: CRITICAL

[+] Payloads:

```
<a href="https://www.malicious_site.com/">Please visit our beauty store!</a>
<a href="https://www.nu11secur1ty.com/"><img src=https://cdn5-capriofiles.netdna-ssl
```

- RCE example:

```
<a href="http://192.168.1.8/cbpos/uploads/product_4/banner.3.jpg"><img src=https://c
```

Reproduce:

href

Proof and Exploit:

href