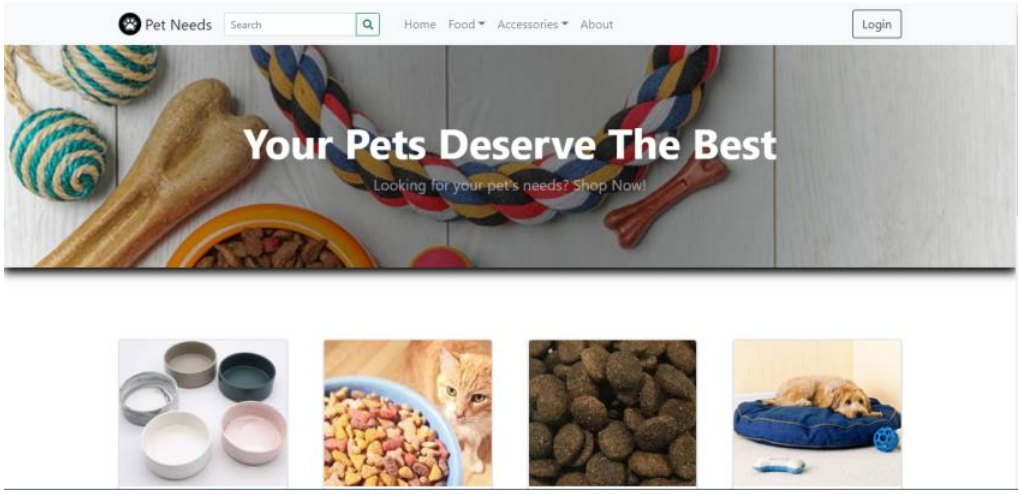
nu11secur1ty Update README.MD ... on Oct 21, 2021 History

..	
docs	last year
PoC-REXSS.py	last year
PoC-SQL.py	last year
README.MD	last year
chromedriver.exe	last year
pet_shop.zip	last year

README.MD

CVE-2021-35458



Description:

The Online Pet Shop We App (by: oretnom23) v1.0 is vulnerable to SQL injection - bypass authentication also Reflected-XSS vulnerability The MySQL vulnerable app to SQL injection is login.php, with parameter: "name="username"" without no sanitizing. After the successful PWNED of the credentials for the admin account. The malicious user can manipulate all information and does malicious stuff with information from customers. Also, this application is vulnerable to Reflected-XSS vulnerability, the malicious user can execute a malicious javascript payload code in the parameter: (name="search") on the general app search form of this application.

Reproduce:

href

Proof:

href