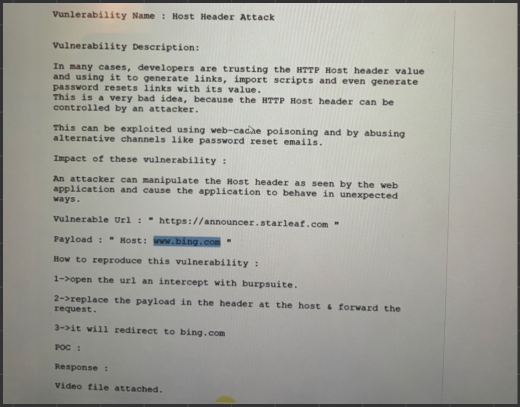
1

Reports

2



Vunlerability Name : Host Header Attack

Vulnerability Description:

In many cases, developers are trusting the HTTP Host header value and using it to generate links, import scripts and even generate password resets links with its value.
This is a very bad idea, because the HTTP Host header can be controlled by an attacker.

This can be exploited using web-cache poisoning and by abusing alternative channels like password reset emails.

Impact of these vulnerability :

An attacker can manipulate the Host header as seen by the web application and cause the application to behave in unexpected ways.

Vulnerable Url : " https://announcer.starleaf.com "

Payload : " Host: www.bing.com "

How to reproduce this vulnerability :

1->open the url an intercept with burpsuite.

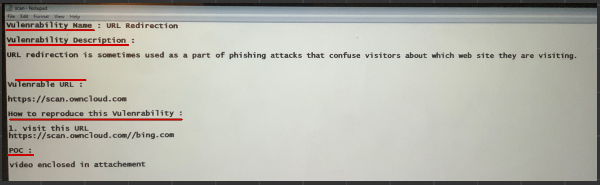
2->replace the payload in the header at the host & forward the request.

3->it will redirect to bing.com

POC :

Response :

Video file attached.



Vulenrability Name : URL Redirection

Vulenrability Description :

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Vulenrable URL :

https://scan.owncloud.com

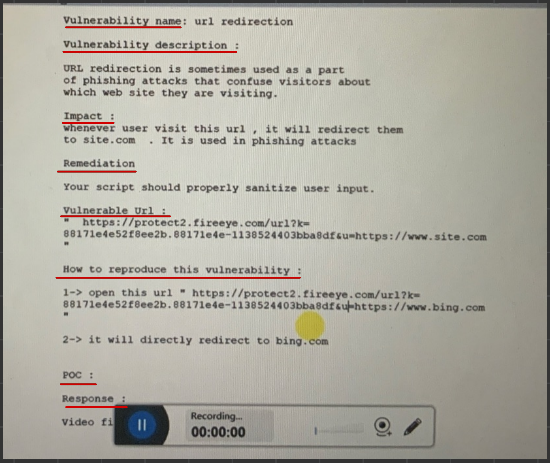
How to reproduce this Vulenrability :

1. visit this URL
https://scan.owncloud.com//bing.com

POC :

video enclosed in attachement

3


Recording...
00:00:00

Vulnerability name: url redirection

Vulnerability description :

URL redirection is sometimes used as a part of phishing attacks that confuse visitors about which web site they are visiting.

Impact :
whenever user visit this url , it will redirect them to site.com . It is used in phishing attacks

Remediation

Your script should properly sanitize user input.

Vulnerable Url :
" https://protect2.fireeye.com/url?k=88171e4e52f8ee2b.88171e4e-1138524403bba8df&u=https://www.site.com "

How to reproduce this vulnerability :

1-> open this url " https://protect2.fireeye.com/url?k=88171e4e52f8ee2b.88171e4e-1138524403bba8df&u=https://www.bing.com "

2-> it will directly redirect to bing.com

POC :

Response :

Video fi