4.2 wraithmail

Log into this website:

<http://localhost:8080/wraithmail/>

and I found two emails in my inbox. One is “Welcome to wraithmail!”, with no real meaning; another is “track the attacker”, with a important clue that provide a referer(the attack email, send by attacker rwilson to hkoch)

I opened the attack email(http://192.168.1.109:8080/wraithbox/htmlisland.jsp?messageid=2849902671918618960/), finding that the link text and the actual content are different, which is a typical example of a forged link. I clicked on the actual link, nothing happened.

With the hint of IDOR, I also try to change the messageid to some typical number(0, 1, 100, etc.). Nothing happened.

I changed my approach and didn't start by targeting the spam emails. I find that when I was at the inbox page, there are three buttons on the left. I clicked on “login history”, finding that the URL was like” <http://192.168.1.109:8080/wraithbox/history.jsp?id=algo/>”, which was also vulnerable to IDOR attack.

So I try to change id to the attacker’s name. shows that “Header validation failed”. It reminds me of the referer, I changed it’s URL to mail.jsp(or send.jsp).

图形用户界面, 文本

AI 生成的内容可能不正确。

Complete!

4.3 Cloaknet

In 4.2, we found that the attacker used a proxy service called Cloaknet. I logged into the website:

<http://localhost:8080/cloaknet/>

I tried different attack payload in the “username” section and received no vulnerable feedback. The server always send a 200 status back.

So I used the default user and password provided to try. They is only one attack record in the user’s page, no text area. But I found that there are two step with the login operation: POST and GET. Since the POST part is not vulnerable, how about GET?

I separately tested the three cookie parameters of the HTTP request when sending a GET request to the server to retrieve the user's page. I found there is a 500 wrong happened when I attack the userid.

