11

The only service that you have left to attack is the mail server. Your team has suggested that you try to password spray using the contact list from the guest accounts as well as sending phishing emails to the users in the contact list.

Password Spraying Overview
Password spraying is using one password to attempt to log in to a list of users typically with a common weak password. There are many tools to automate password spraying on multiple attack vectors. You can easily test an environment for weak passwords by password spraying a list of all their users.

Common Weak Passwords
In a realistic environment humans are the weakest link, if the environment has a weak password policy then often times you can spray for common weak password based upon various conditions of the year for example if the year was 2020 and the season was Fall then a common weak password that you could spray for would be Fall2020.

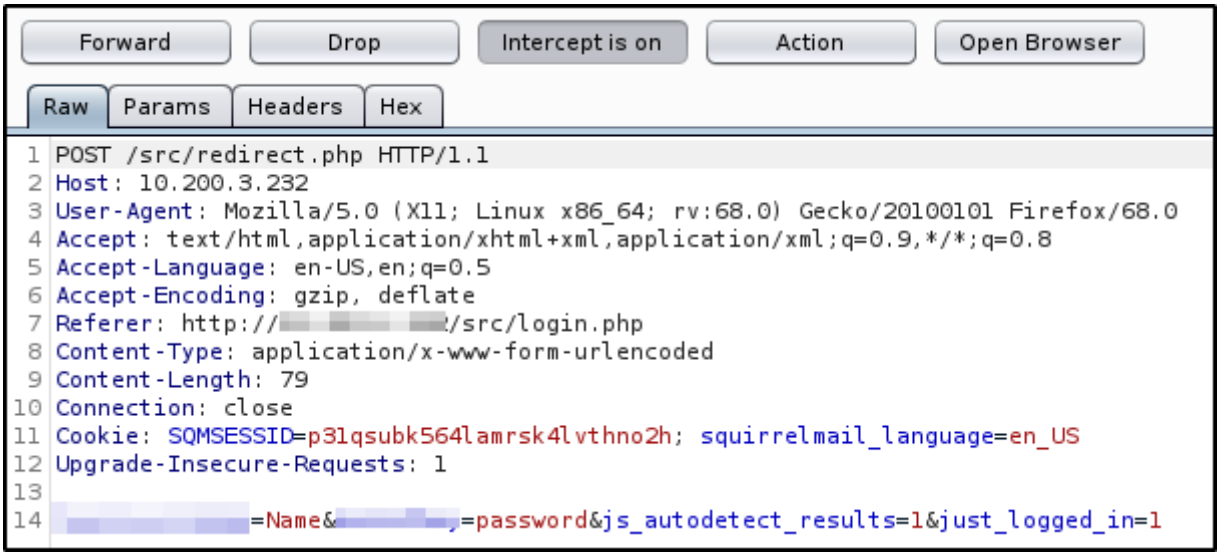
Some examples of weak passwords:

- Summer2020
- Management2020
- Management2018
- Password2020
- 2020
- Password123

Finding the Attack Surface
The attack surface for password spraying is fairly broad, all you need is a field to submit a username and a password and you can password spray against that login. Even if there is not a login portal you can still sometimes password spray against it, for example we can password spray active directory users with kerbrute. Having a broad attack surface makes password spraying a commonly used attack vector in many red team engagements. The only hard part about finding our attack surface is finding

the parameters of the request. This can either be done by submitting a test login and seeing what the parameters are, however, this does not always work so instead what we can do is use burp to intercept our request and see what the request parameters are.

1.) We need to send a request to burp with dummy data in the user and password fields to identify where the request parameters are.



Capturing the request with burp to extract the parameters

We can now use these parameters in hydra to make requests to the website with a user list and a password.
In order to password spray you will need a list of users, you can get the contact list from the guest account and utilize the names from it as a user list.

Password Spraying with Hydra
Hydra is typically used as a web application login portal brute force tool however it can also be used to password spray against a login portal. You only have to supply the IP, Password, and User list. A password list is optional however you can make a small list of common passwords within the company and use it to spray with.
1.) hydra -L users.txt -p MACHINE_IP http-post-form '/src/redirect.php:<user_parameter>=^USER^&<pass_parameter>=^PASS^:F=incorrect' -v

```
cryillic@human-eater:~/Downloads$ hydra -L users.txt -p [redacted] 10.40.119.232 http-post-form '/src/redirect.php:[redacted]=^USER^&[redacted]=^PASS^:F=incorrect'
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-08-13 23:39:53
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:12/p:1), ~1 try per task
[DATA] attacking http-post-form://10.40.119.232:80/src/redirect.php:[redacted]=^USER^&[redacted]=^PASS^:F=incorrect
[80][http-post-form] host: 10.40.119.232   login: [redacted]   password: [redacted]
[80][http-post-form] host: 10.40.119.232   login: [redacted]   password: [redacted]
[80][http-post-form] host: 10.40.119.232   login: [redacted]   password: [redacted]
[80][http-post-form] host: 10.40.119.232   login: [redacted]   password: [redacted]
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-08-13 23:40:01
```

Password spraying the target with Hydra

If you successfully password sprayed you will now have a user account or two that you have fully compromised allowing you to view company emails and potentially gain further access into the network.

Answer the questions below

What is the username parameter in the POST request?

Correct Answer

What is the password parameter in the POST request?

Correct Answer

What username found with hydra starts with an M?

Correct Answer

What is the password found with hydra?

Correct Answer