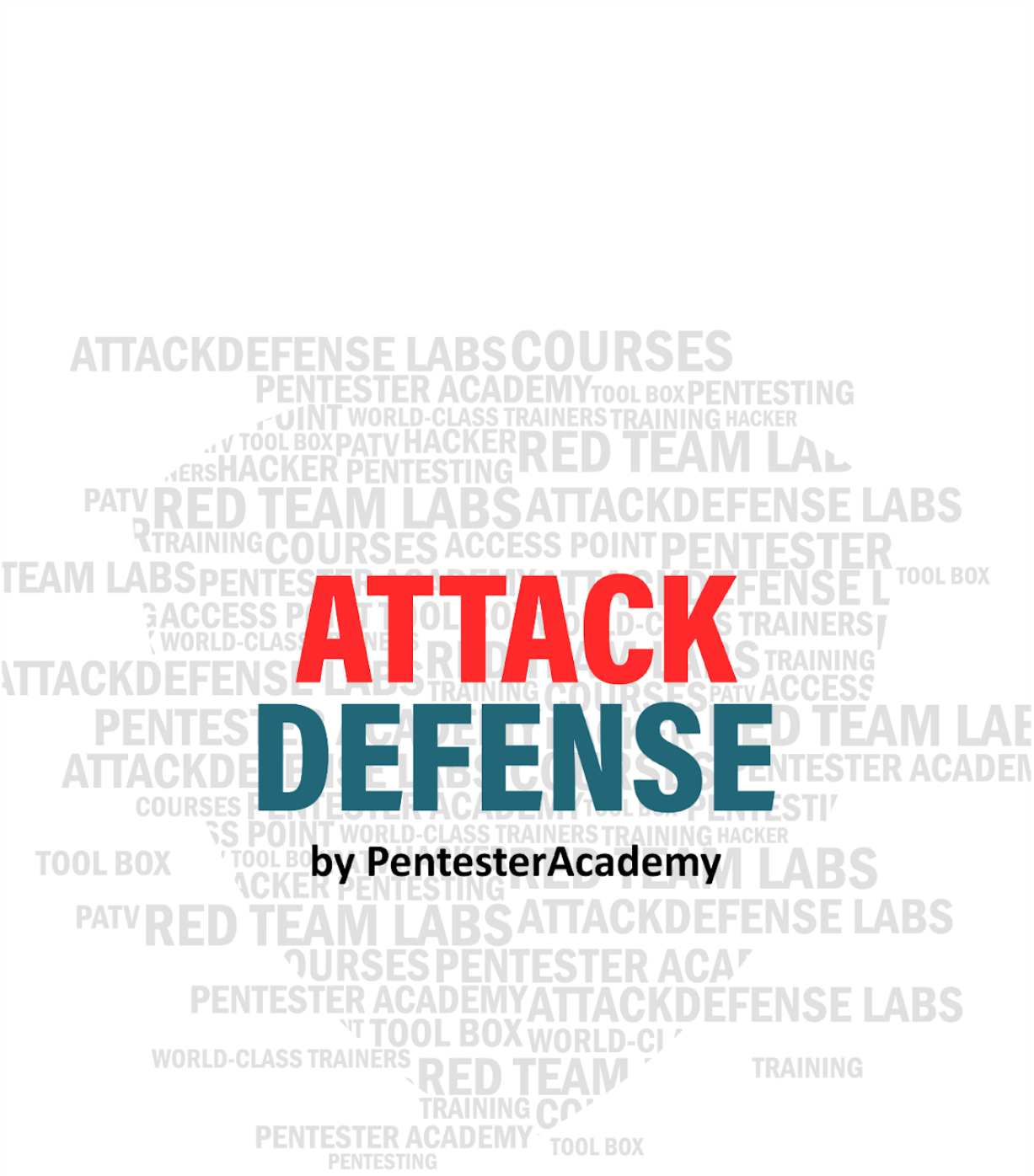

ATTACK
DEFENSE
by PentesterAcademy

| Name | Directory Enumeration with Burp Suite |
|---|---|
| URL | https://attackdefense.com/challengedetails?cid=1886 |
| Type | Webapp Pentesting Basics |

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Step 1:** Start the terminal and check the IP address of the machine.

**Command:** ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
7513: eth0@if7514: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
7516: eth1@if7517: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:1b:68:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.27.104.2/24 brd 192.27.104.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP address of the attacker machine is 192.27.104.2, the target machine will be located at IP address 192.27.104.3

**Step 2:** Run a Nmap scan against the target IP.

**Command:** nmap -sS -sV 192.27.104.3

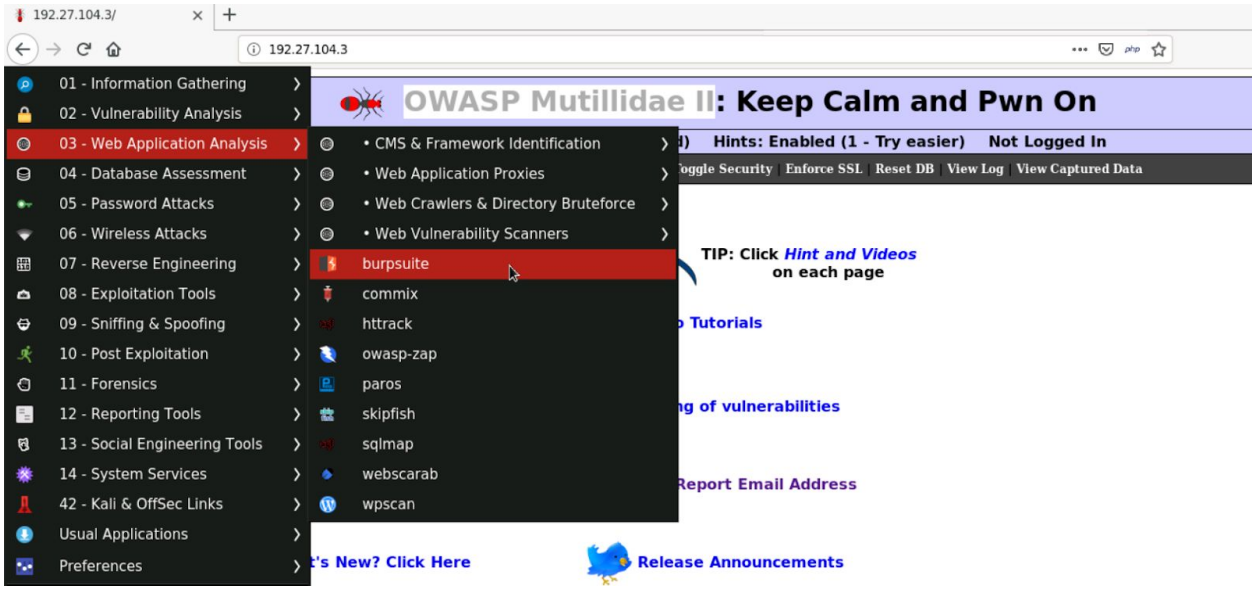
```
root@attackdefense:~# nmap -sS -sV 192.27.104.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-05-22 15:04 IST
Nmap scan report for target-1 (192.27.104.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
3306/tcp open  mysql   MySQL 5.5.47-0ubuntu0.14.04.1
MAC Address: 02:42:C0:1B:68:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.04 seconds
```

Port 80 and 3306 are open.

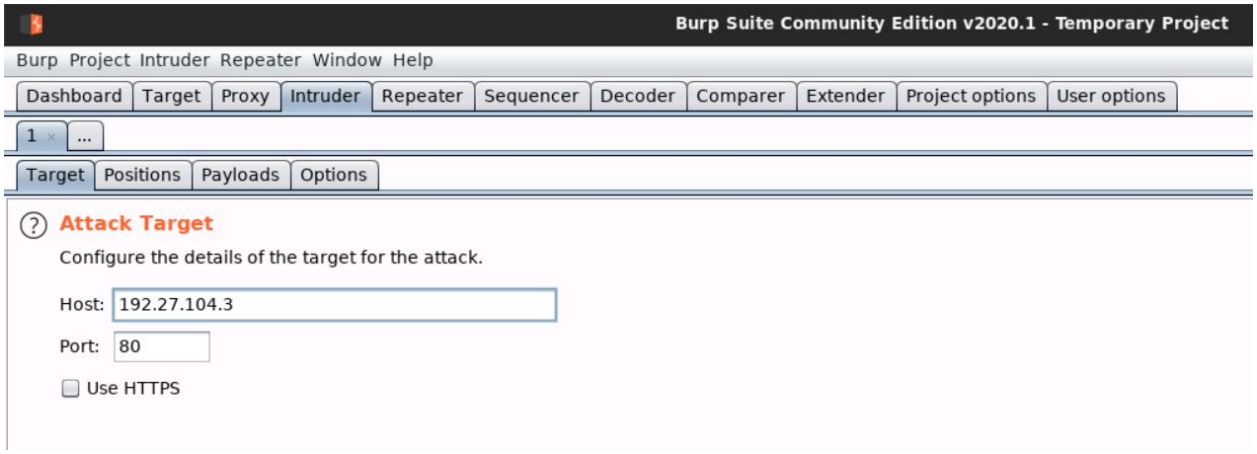
**Step 3:** Access the web application using firefox.

**Command:** firefox http://192.27.104.3


**Step 4:** The target is running OWASP Mutillidae II. Start burp suite.

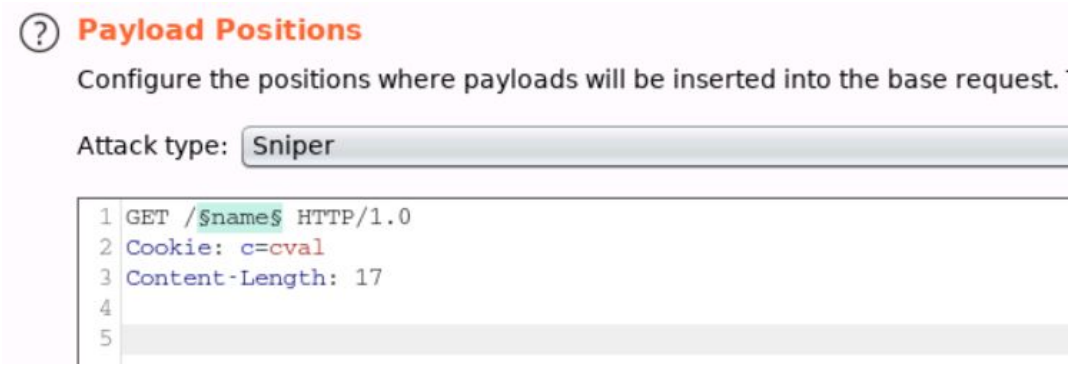


**Step 5:** Navigate to the **intruder tab** and set the target machine IP address.



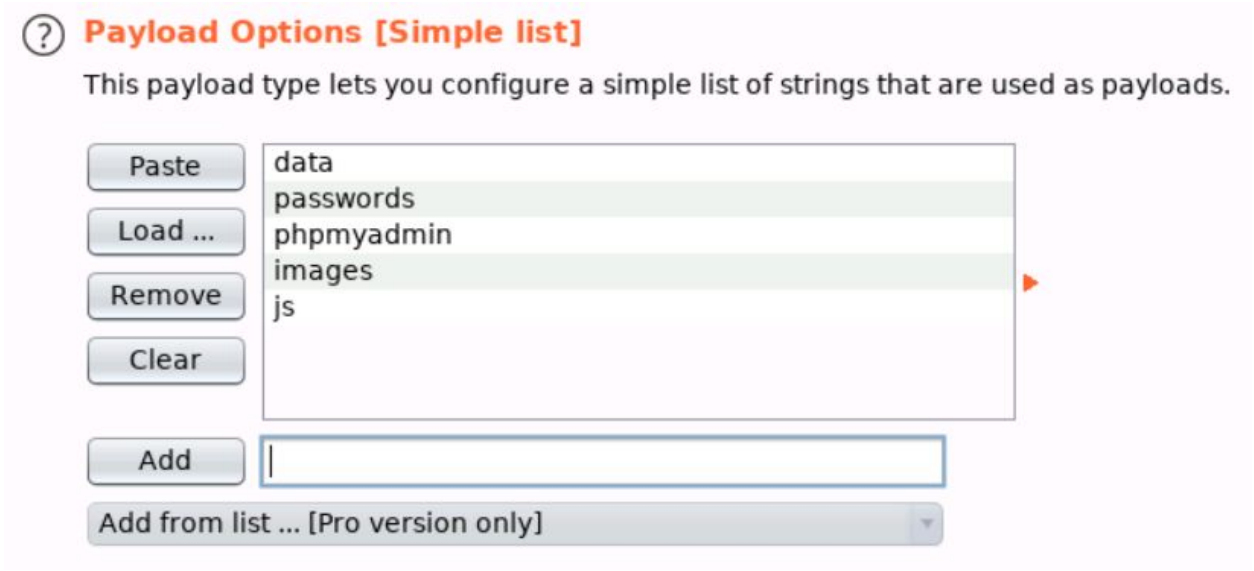

**Step 6:** Configure the Payload positions. The payload position can be set by selecting the text and click on the add button.

GET /§name§ HTTP/1.0
Cookie: c=cval
Content-Length: 17



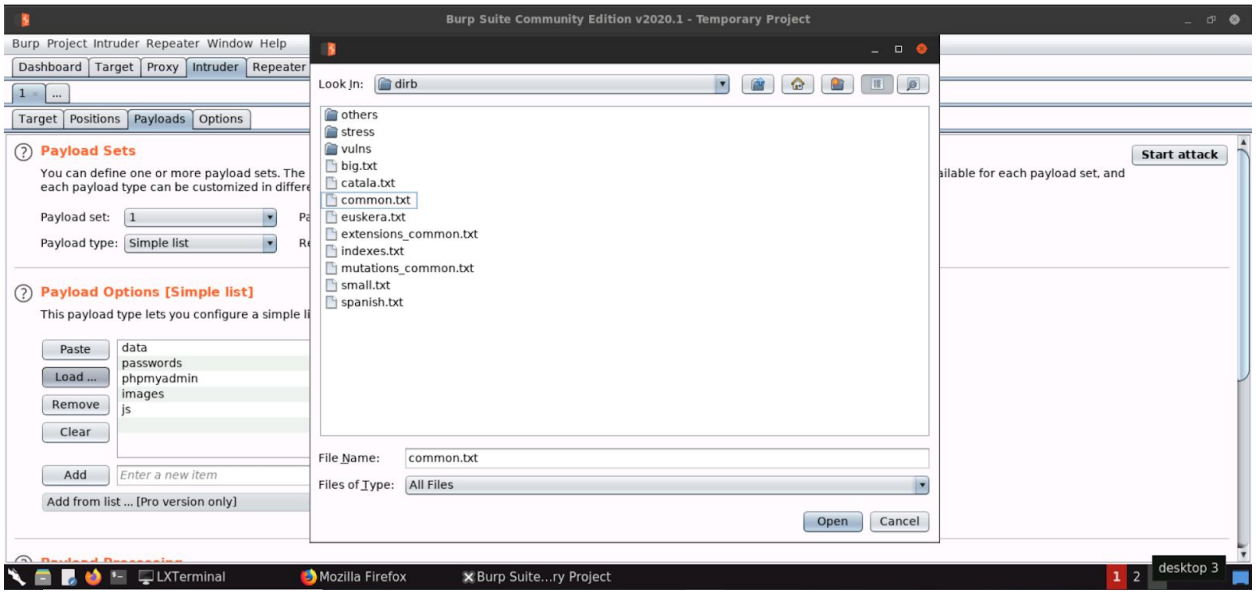

**Step 7:** Since the Burp Suite Community edition, time throttles requests, Add known words to the payload list.

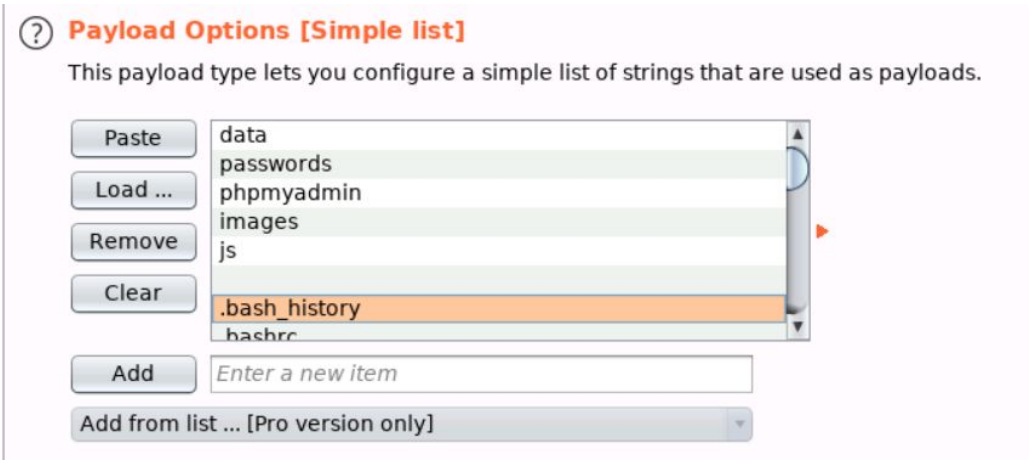
data
passwords
phpmyadmin
images
js



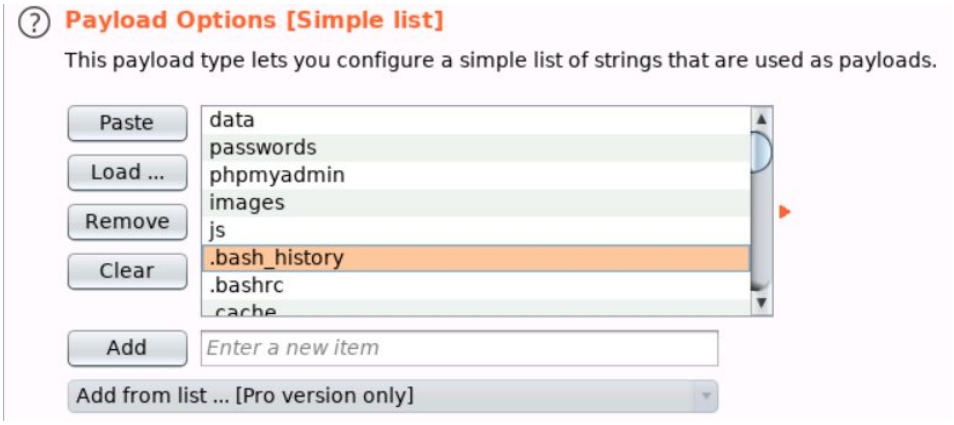

**Step 8:** Click on "**Load ..**" and navigate to common.txt file then click open.

**Path:** /usr/share/wordlists/dirb/common.txt



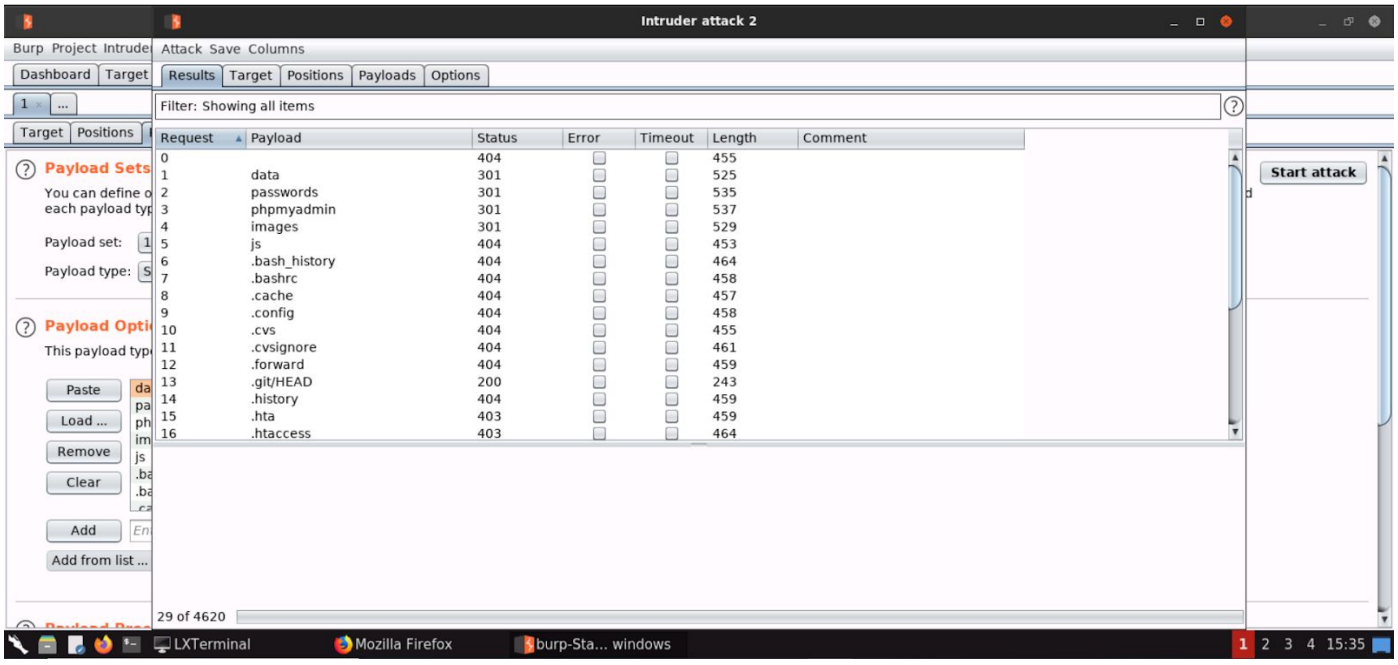



Also, remove the empty entry by selecting the empty space and click on “Remove”




**Step 9:** Click on “**Start Attack**” and check the status code for the payloads.

404 Status Code - Not Found
200/301 Status Code - Directory exists (Moved Permanently)




## References

1. Burp Suite (https://portswigger.net/burp)
2. Mutillidae II (https://sourceforge.net/projects/mutillidae/)