Love

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-26 15:15 EDT
Nmap scan report for 10.10.10.239
Host is up (0.088s latency).
Not shown: 993 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
80/tcp   open  http        Apache httpd 2.4.46 ((Win64) OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Voting System using PHP
135/tcp  open  msrpc       Microsoft Windows RPC
139/tcp  open  netbios-ssn Microsoft Windows netbios-ssn
443/tcp  open  ssl/http    Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_ssl-date: TLS randomness does not represent time
| tls-alpn:
|_  http/1.1
|_http-title: 403 Forbidden
| ssl-cert: Subject: commonName=staging.love.htb/organizationName=ValentineCorp/stateOrProvinceName=m/countryName=in
| Not valid before: 2021-01-18T14:00:16
|_Not valid after:  2022-01-18T14:00:16
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
445/tcp  open  EDcr        Windows 10 Pro 19042 microsoft-ds (workgroup: WORKGROUP)
3306/tcp open  mysql?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, FourOhFourRequest, HTTPOptions, Help, LDAPBindReq, LDAPSearchReq, RPCCheck, RTSPRequest, SIPOptions, SMBProgNeg, SSLSessionReq, TLSSessionReq, TerminalServerCookie, X11Probe:
|_    Host '10.10.14.16' is not allowed to connect to this MariaDB server
5000/tcp open  http        Apache httpd 2.4.46 (OpenSSL/1.1.1j PHP/7.3.27)
|_http-server-header: Apache/2.4.46 (Win64) OpenSSL/1.1.1j PHP/7.3.27
|_http-title: 403 Forbidden
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
```

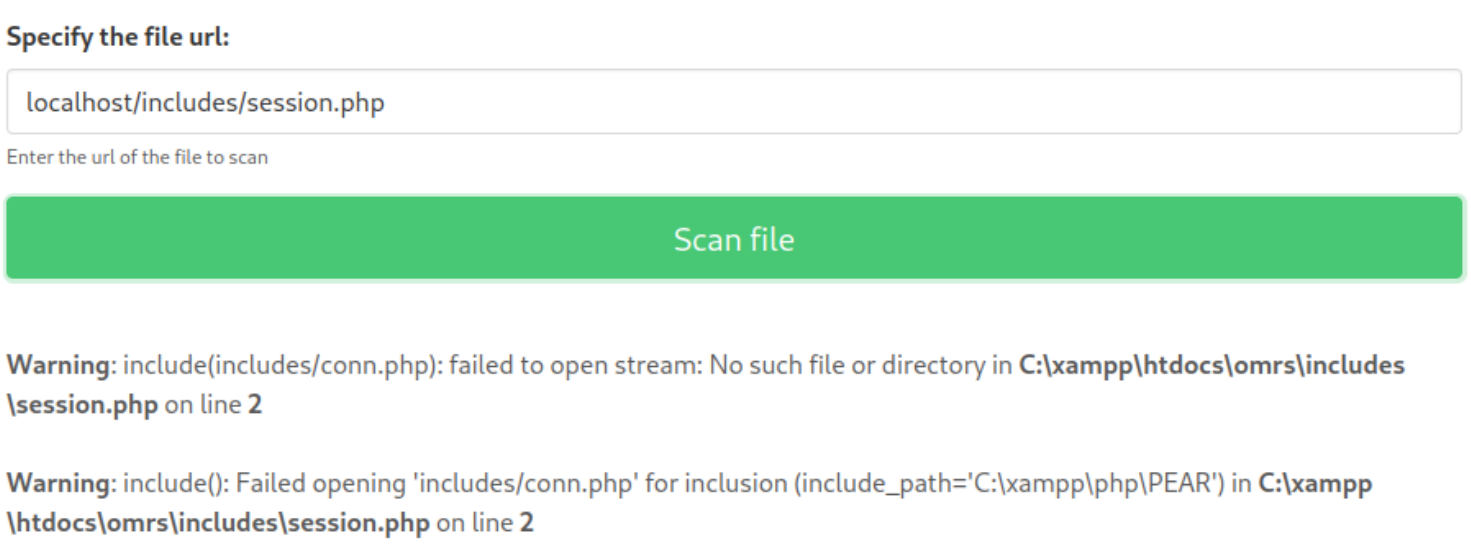
websites

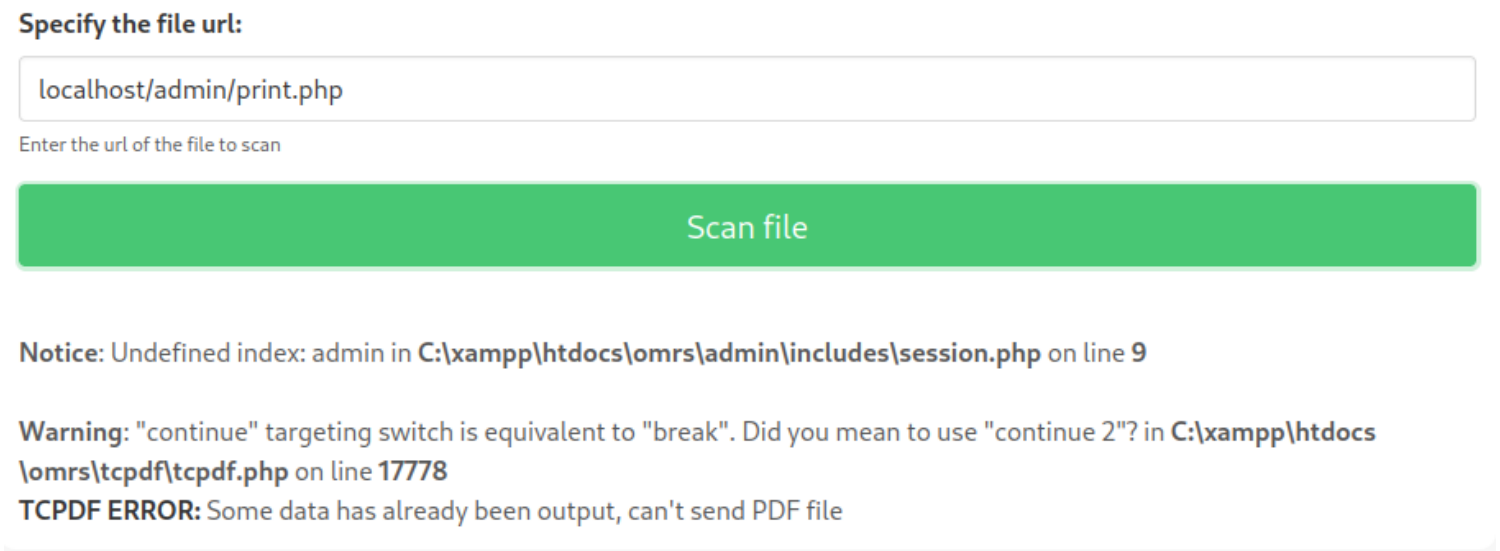
going to port 80, we are greeted with a login prompt for a voting system.
-> /index.php says “Voter's ID” instead of username
-> /admin says “Username”

visiting port 443, the ssl certificate reveals the subdomain staging.love.htb
-> otherwise, nothing to see on 443 as we do not have permission to view any pages

http://staging.love.htb is a free file scanner web app

Looks like there is an SSRF:





Looking back at the nmap scan, there is an unusual port, 5000, which gives a 403 on a http page
Using the SSRF, we can view this page

admin:@LoveIsInTheAir!!!!

We are greeted with an admin panel

we can update our “profile picture” with an msfvenom payload to get ourselves a shell!

priv esc

WINPEAS!!

```
Checking AlwaysInstallElevated
 https://book.hacktricks.xyz/windows-hardening/windows-local-privilege-escalation#alwaysinstallelevated
   AlwaysInstallElevated set to 1 in HKLM!
   AlwaysInstallElevated set to 1 in HKCU!
```

With these registers enabled, any .msi file we run will be run as NT Authority\System
So we can generate a reverse_shell.msi file with msfvenom and get a root shell!

Hacktricks actually suggests a metasploit module which does this for you...