

## PRAKTIKUM 2



### FortifyTech

Anda adalah seorang ahli keamanan yang ditugaskan oleh perusahaan konsultan keamanan CyberShield untuk melakukan penetration testing terhadap infrastruktur perusahaan FortifyTech. FortifyTech adalah startup perusahaan teknologi dan mereka telah menyewa layanan CyberShield untuk mengevaluasi keamanan sistem mereka.

Temukan kerentanan pada perusahaan FortifyTech dengan menerapkan prinsip Ethical Hacking dan buatlah laporan pada setiap kerentanan yang telah anda temukan, dengan begitu celah kerentanan tersebut dengan cepat bisa diproses oleh mereka.

#### Scope:

- 10.15.42.36
- 10.15.42.7

#### Notes:

Pengerjaan hanya bisa menggunakan jaringan ITS (gunakan vpn ITS atau wifi ITS).

#### Rules:

Hindari hal - hal yang melanggar etika atau Anda akan dimarahi (diberi nilai 0) oleh Project Manager 😊.

## IP 10.15.42.36

### 1. Reconnaissance

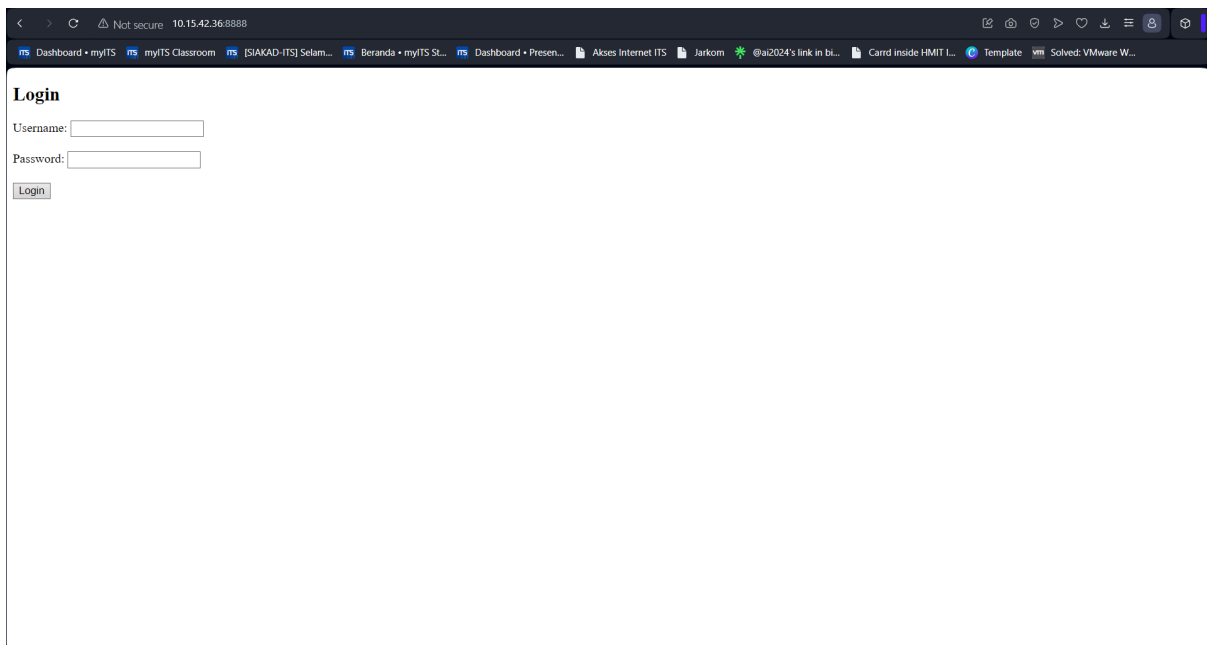
- Nmap

Dengan menggunakan **nmap -p- 10.15.42.36**, didapatkan beberapa open port seperti pada gambar berikut.

```
(root@kali)-[/home/aveee]
# nmap -p- 10.15.42.36
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-07 10:21 EDT
Nmap scan report for 10.15.42.36
Host is up (0.00042s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
8888/tcp  open  sun-answerbook

Nmap done: 1 IP address (1 host up) scanned in 128.73 seconds
```

Kemudian saat dilakukan percobaan pada open portnya didapatkan login page sebagai berikut.



Memanfaatkan adanya info tcp dengan mengeksekusi command ftp 10.15.42.36. Kemudian terdapat backup.sql di dalamnya ketika sudah tersambung.

```

(root@kali)-[/home/aveee]
# ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:aveee):
530 This FTP server is anonymous only.
ftp> close
221 Goodbye.
ftp> ftp 10.15.42.36
Connected to 10.15.42.36.
220 FTP Server
Name (10.15.42.36:aveee): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (||65511|)
150 Here comes the directory listing.
-rwxrwxr-x  1 ftp      ftp      1997 May 04 15:40 backup.sql
226 Directory send OK.
ftp> mget *
mget backup.sql [anpqy]? y
229 Entering Extended Passive Mode (||65503|)
150 Opening BINARY mode data connection for backup.sql (1997 bytes).
100% |*****| 1997      20.24 KiB/s   00:00 ETA
226 Transfer complete.
1997 bytes received in 00:00 (9.91 KiB/s)
ftp> exit
221 Goodbye.

```

Setelah didownload, didapatkan beberapa informasi berikut di dalam backup.sql.

```

(root@kali)-[/home/aveee]
# cat backup.sql
-- MySQL dump 10.13  Distrib 8.0.36, for Linux (x86_64)
--
-- Host: localhost    Database: db
--
-- Server version      8.0.36-0ubuntu0.22.04.1

/*!40101 SET @OLD_CHARACTER_SET_CLIENT=@@CHARACTER_SET_CLIENT */;
/*!40101 SET @OLD_CHARACTER_SET_RESULTS=@@CHARACTER_SET_RESULTS */;
/*!40101 SET @OLD_COLLATION_CONNECTION=@@COLLATION_CONNECTION */;
/*!50503 SET NAMES utf8mb4 */;
/*!40103 SET @OLD_TIME_ZONE=@@TIME_ZONE */;
/*!40103 SET TIME_ZONE='+00:00' */;
/*!40014 SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0 */;
/*!40014 SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0 */;
/*!40101 SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='NO_AUTO_VALUE_ON_ZERO' */;
/*!40111 SET @OLD_SQL_NOTES=@@SQL_NOTES, SQL_NOTES=0 */;

--
-- Table structure for table `users`
--

DROP TABLE IF EXISTS `users`;
/*!40101 SET @saved_cs_client      = @@character_set_client */;
/*!50503 SET character_set_client = utf8mb4 */;
CREATE TABLE `users` (
  `id` int NOT NULL,
  `username` varchar(255) DEFAULT NULL,
  `password` varchar(255) DEFAULT NULL,
  PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4 COLLATE=utf8mb4_0900_ai_ci;
/*!40101 SET character_set_client = @saved_cs_client */;

--
-- Dumping data for table `users`
--

LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES (1,'admin','$2y$10$RwYNURXBmYscv9UyfuRDleF8ML0tjn.Ft5lUKwTWiavJOJhM56d0K');
/*!40000 ALTER TABLE `users` ENABLE KEYS */;
UNLOCK TABLES;
/*!40103 SET TIME_ZONE=@@OLD_TIME_ZONE */;

```

- Gobuster

```
(root@kali)-[/home/aveee]
# gobuster dir -u http://10.15.42.36:8888 -w big.txt

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

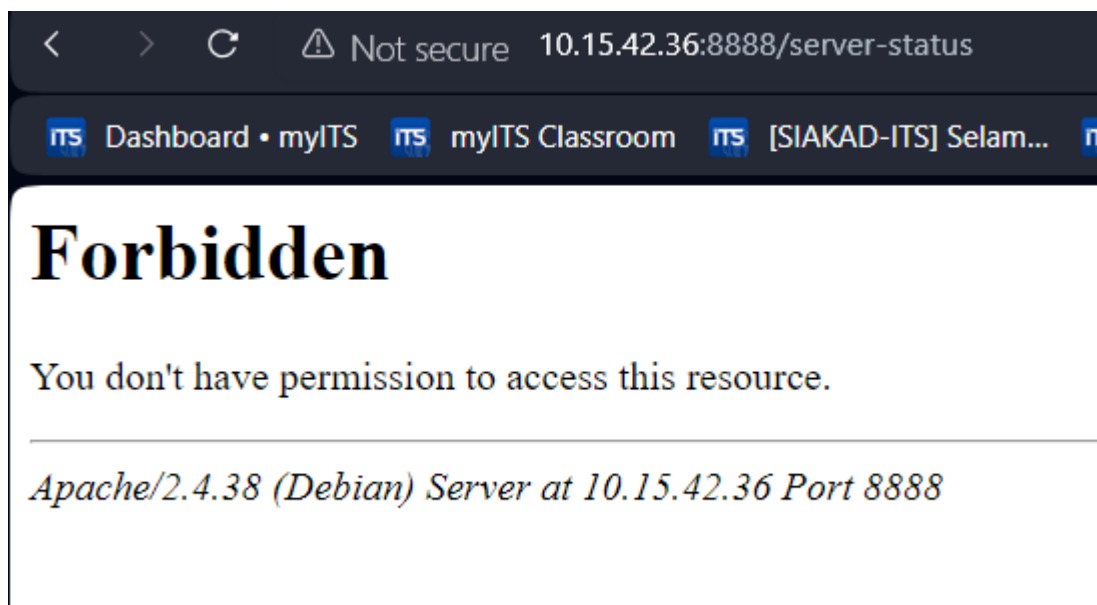
[+] Url: http://10.15.42.36:8888
[+] Method: GET
[+] Threads: 10
[+] Wordlist: big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/.htpasswd (Status: 403) [Size: 278]
/.htaccess (Status: 403) [Size: 278]
/server-status (Status: 403) [Size: 278]
Progress: 20476 / 20477 (100.00%)

Finished
```

Terdapat endpoint `/server-status`. Ketika dibuka ternyata diperlukan permission access terlebih dahulu.



## 2. Vulnerability Assessment

### Nikto IP 10.15.42.36:8888

```
(root@kali) ~/home/aveee
# nikto -h 10.15.42.36:8888

- Nikto v2.5.0

+ Target IP:      10.15.42.36
+ Target Hostname: 10.15.42.36
+ Target Port:    8888
+ Start Time:     2024-05-07 11:50:50 (GMT-4)

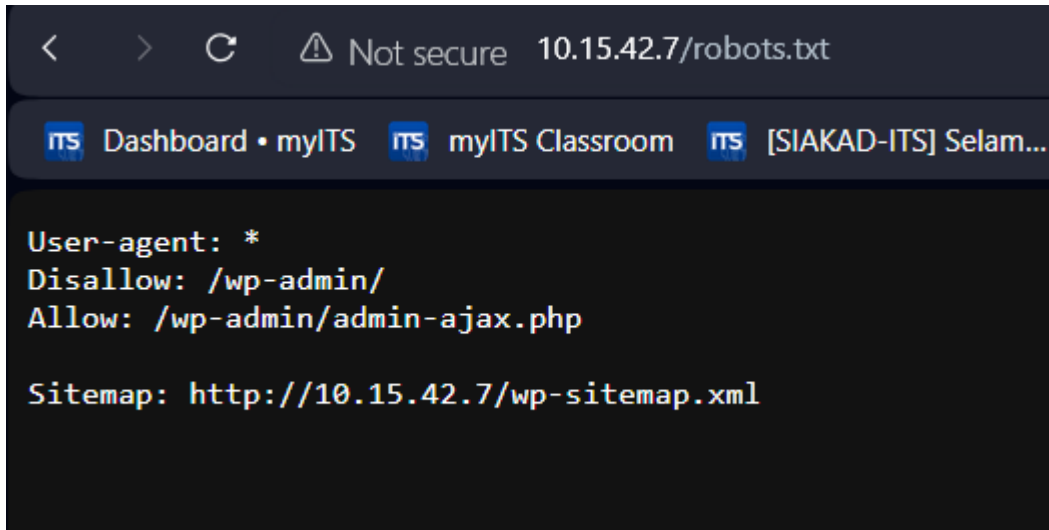
+ Server: Apache/2.4.38 (Debian)
+ /: Retrieved x-powered-by header: PHP/7.2.34.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-c all' to force check all possible dirs)
+ Apache/2.4.38 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ /: Web Server returns a valid response with junk HTTP methods which may cause false positives.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ 8192 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time:     2024-05-07 11:57:38 (GMT-4) (408 seconds)

+ 1 host(s) tested
```

## IP 10.15.42.7

### 1. Reconnaissance

Pada hasil nikto -h 10.15.42.7 pada bagian 2. Vulnerability Assessment, terdapat sebuah endpoint /robots.txt yang dapat diakses.



### 2. Vulnerability Assessment

