Pentesting Reconnaissance Vulnerable

This test was conducted for academic and personal use. All exercises were performed in controlled environments using VMs, with an attacker machine like Kali Linux and a vulnerable machine like bWAPP (BeeBox). The following tools were used to scan for vulnerabilities:

- nslookup
- whois
- Sublist3r
- Nikto
- Gobuster
- Dirb

Phase 1:

In this phase, we conducted an IP scan using **Nmap**, which identified the IP address corresponding to our vulnerable bWAPP machine.

Phase 2:

Using **Nmap**, we identified the services running on the IP `192.168.56.106`:

- **FTP (Port 21)**: ProFTPD 1.3.1, a file transfer service.
- **SSH (Port 22)**: OpenSSH 4.7p1, providing remote access to the machine.
- **SMTP (Port 25)**: Postfix, an email service.
- **HTTP (Port 80)**: Apache 2.2.8 web server with mod_fastcgi and PHP.
- **NetBIOS (Ports 139 and 445)**: Samba, used for file sharing in local networks.
- **Multiple HTTP services** on ports 8080, 8443, 9080, and 9443, running web servers like Nginx and Lighttpd.
- **VNC (Port 5901)**: A remote desktop control protocol.
- **MySQL (Port 3306)**: MySQL 5.0.96 database service.
- An **unusual service** was also detected on port 666.

```
└─$ nmap -sV -p- 192.168.56.106
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-12 00:29 EDT
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 41.69% done; ETC: 00:30 (0:00:24 remaining)
Stats: 0:01:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 94.74% done; ETC: 00:31 (0:00:04 remaining)
Stats: 0:03:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 00:32 (0:00:00 remaining)
Nmap scan report for 192.168.56.106
Host is up (0.00072s latency).
Not shown: 65516 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
443/tcp  open  ssl/http    Apache httpd 2.2.8 ((Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: ITSECGAMES)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell?
666/tcp  open  doom?
3306/tcp open  mysql       MySQL 5.0.96-0ubuntu3
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.3 (Ubuntu 4.2.3-2ubuntu7))
5901/tcp open  vnc         VNC (protocol 3.8)
6001/tcp open  X11         (access denied)
8080/tcp open  http        nginx 1.4.0
8443/tcp open  ssl/http    nginx 1.4.0
9080/tcp open  http        lighttpd 1.4.19
9443/tcp open  ssl/http    lighttpd 1.4.19
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port666-TCP:V=7.94SVN%I=7%D=10/12%Time=6709FB61%P=x86_64-pc-linux-gnu%r
SF:(GenericLines,400,"\*\*\*\x20bWAPP\x20Movie\x20Service\x20\*\*\*\nMatch
SF:ing\x20movies:\x200\n\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0
```

Phase 3:

We used the **nslookup** tool to determine the domain name associated with the IP address. In some cases, reverse lookup is performed. In this instance, no domain name was generated since the IP address used does not belong to a domain. Instead, it is publicly accessible and can be used by various devices such as phones, computers, etc.

Phase 4:

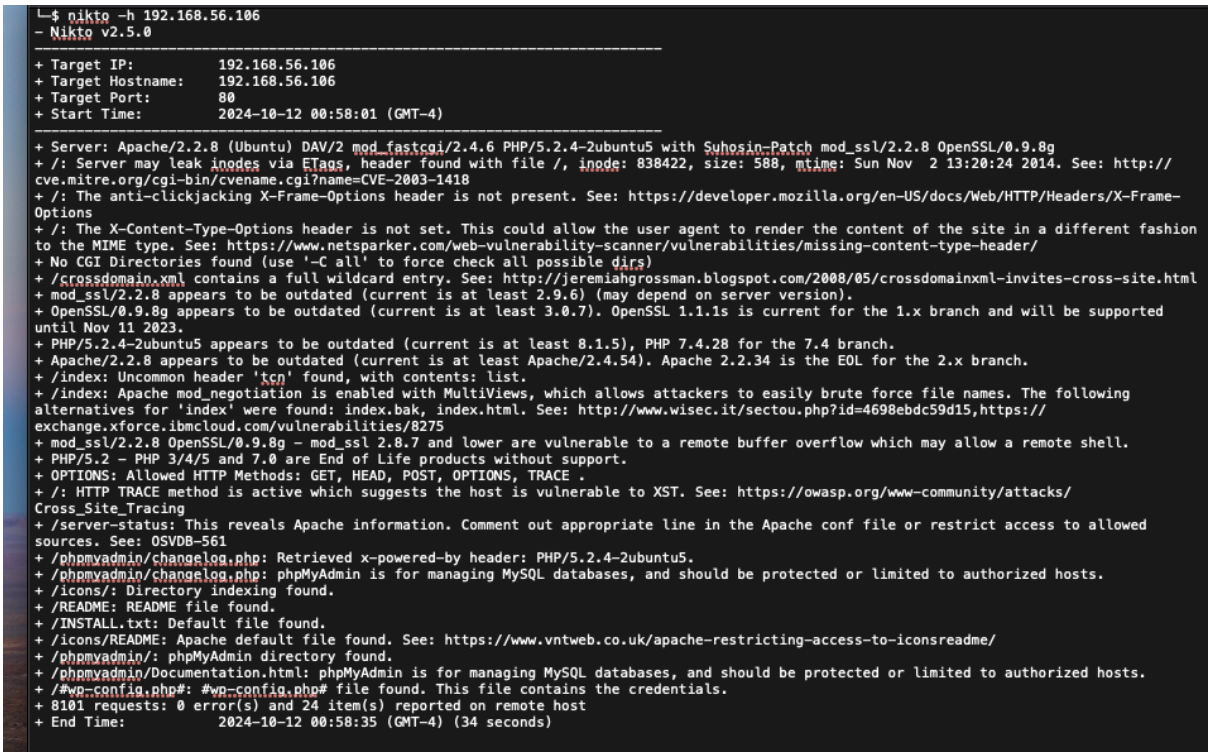
We used **WHOIS**, a protocol used to query databases for information on registered entities or assignees of an internet resource. The IP address belongs to the range `192.168.0.0 - 192.168.255.255`, which is a block of addresses reserved for private networks (RFC 1918). It does not provide specific ownership information since this IP range is intended for use in local networks. These addresses are not routable over the public Internet.

```
NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2024-05-24
Comment:        These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are
automatically configured in hundreds of millions of devices.  They are only intended for use within a private context  and traffic that needs to cross the Internet will need to use a
different, unique address.
Comment:
Comment:        These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry.  The traffic from these addresses does not come from ICANN or IANA.
We are not the source of activity you may see on logs or in e-mail records.  Please refer to http://www.iana.org/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2024-05-24
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN
```

Phase 5:

We assessed vulnerabilities by scanning using **Nikto**. The scan was performed on the web server hosted at IP `192.168.56.106` on port 80.

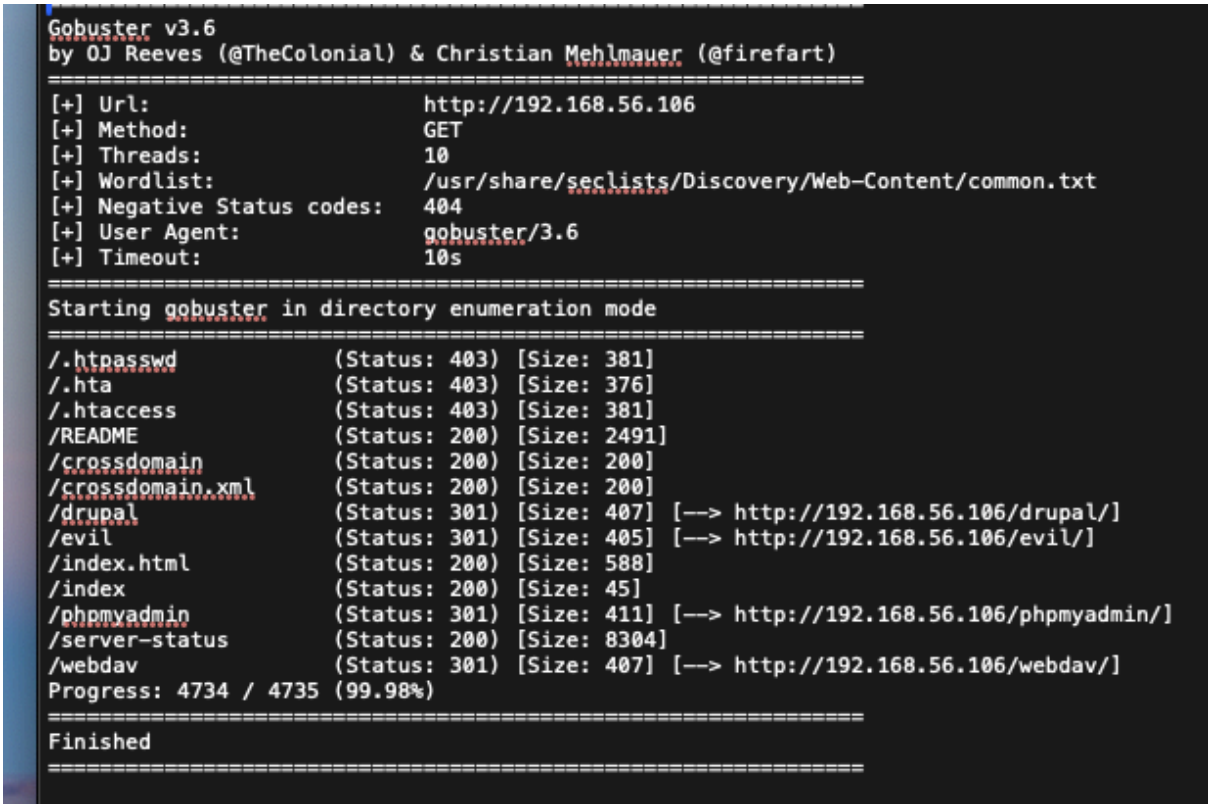
- **Detected Server**: Apache/2.2.8 on an Ubuntu system, with PHP/5.2.4 and OpenSSL/0.9.8g.
- **Vulnerabilities found**:
    - **ETags**: The server may leak inodes through ETag headers, potentially allowing attacks like cache synchronization (CVE-2003-1418).
    - **X-Frame-Options**: The anti-clickjacking header is missing.
    - **X-Content-Type-Options**: This header is missing, which could allow browsers to interpret content in a different MIME type.
    - **crossdomain.xml**: This file allows any domain to make cross-site requests, posing a security risk.
    - **mod_ssl, OpenSSL, PHP, Apache**: These services are outdated, exposing the server to known vulnerabilities.
    - **Allowed HTTP Methods**: GET, HEAD, POST, OPTIONS, and TRACE, with TRACE being a risk for **Cross-Site Tracing (XST)**.
    - **phpMyAdmin**: The MySQL database management tool is exposed without proper protection.
    - **Directory Indexing**: An index of files was found in `/icons/`, allowing access to view the contents of that folder.



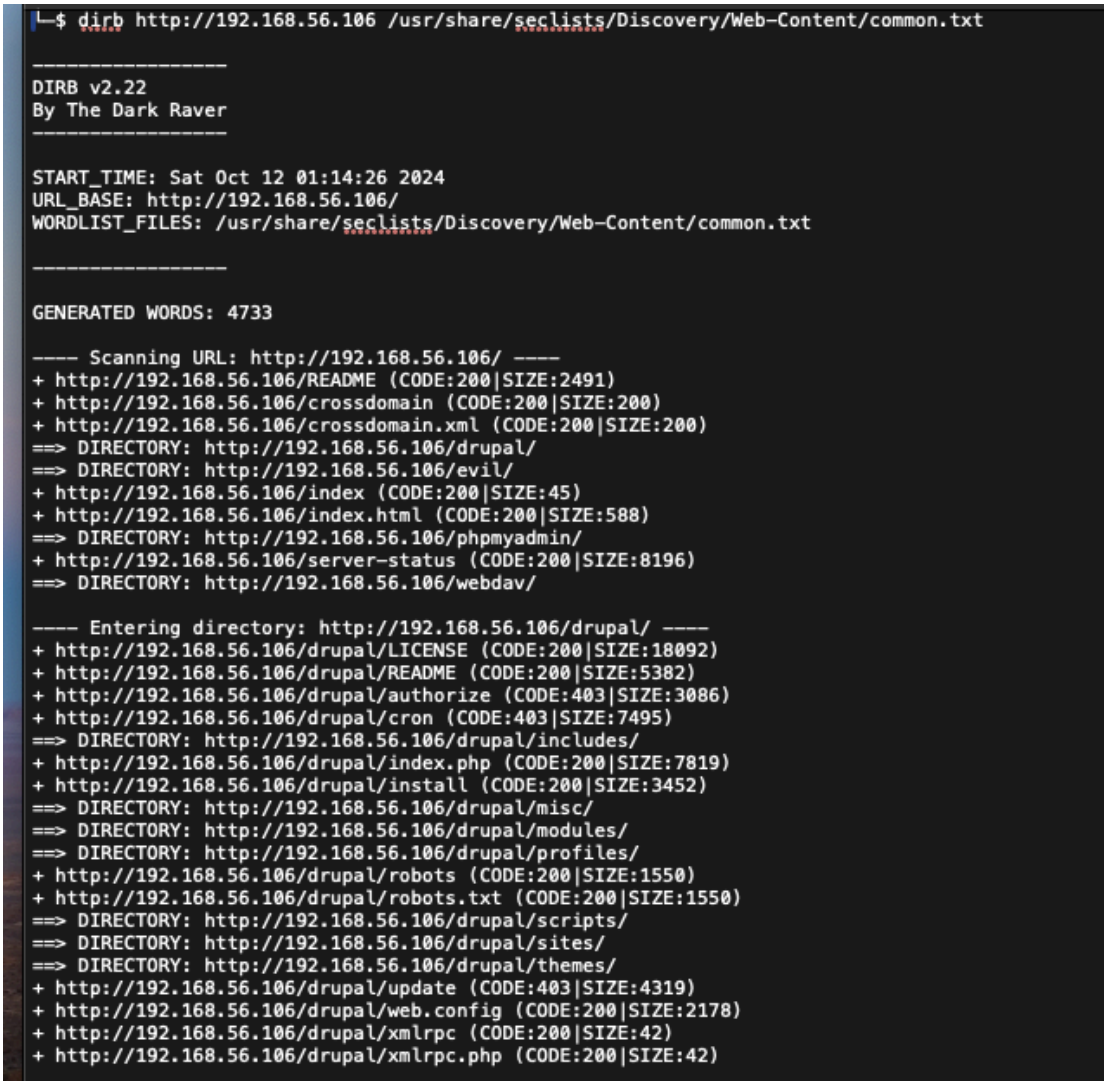
Phase 6:

We used **Gobuster** and **Dirb** to review vulnerable directories and assess which ones might be susceptible to brute-force attacks.

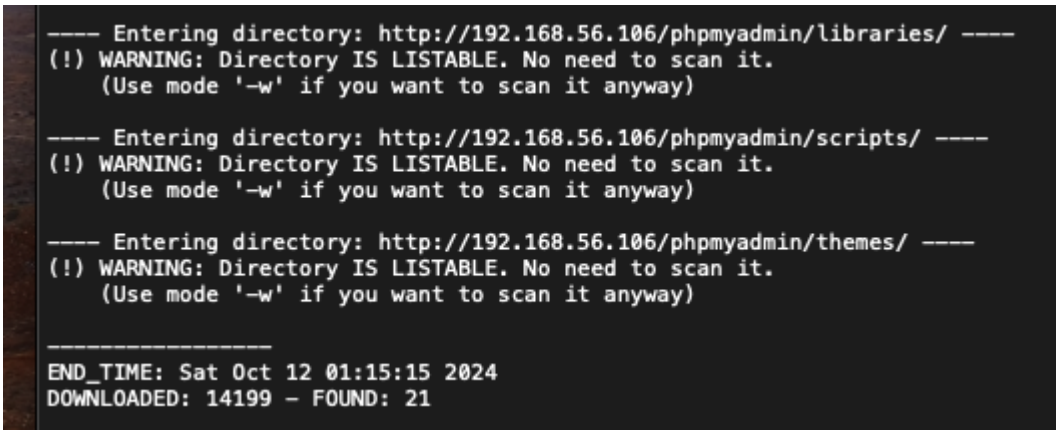
- **Gobuster**: The scan found several interesting paths on the server `192.168.56.106`, including:
  - Sensitive files like `.htaccess` and `.htpasswd`, which are accessible but return HTTP code 403 (forbidden).
  - Directories of interest such as `/drupal/`, `/evil/`, `/phpmyadmin/`, `/webdav/`, and `/server-status/`.
  - Directories where file listing is enabled (such as `/evil/` and `/webdav/`), potentially exposing sensitive information.
  - `/phpmyadmin/` exposes the MySQL database management tool.



- **Dirb**: The results are similar to those found by **Gobuster**, highlighting paths such as:
    - `/drupal/`: A CMS (Content Management System) that could be an attack vector if not properly secured.
    - `/phpmyadmin/`: As with Gobuster, the MySQL management interface is exposed.
    - Several directories where file listing is enabled, meaning users can view the files they contain.




---- Entering directory: http://192.168.56.106/evil/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/phpmyadmin/ ----
+ http://192.168.56.106/phpmyadmin/favicon.ico (CODE:200|SIZE:18902)
+ http://192.168.56.106/phpmyadmin/index.php (CODE:200|SIZE:8132)
==> DIRECTORY: http://192.168.56.106/phpmyadmin/js/
==> DIRECTORY: http://192.168.56.106/phpmyadmin/lang/
==> DIRECTORY: http://192.168.56.106/phpmyadmin/libraries/
+ http://192.168.56.106/phpmyadmin/phpinfo.php (CODE:200|SIZE:0)
==> DIRECTORY: http://192.168.56.106/phpmyadmin/scripts/
==> DIRECTORY: http://192.168.56.106/phpmyadmin/themes/
---- Entering directory: http://192.168.56.106/webdav/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/includes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/modules/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/profiles/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/sites/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/drupal/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/phpmyadmin/js/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)


---- Entering directory: http://192.168.56.106/phpmyadmin/libraries/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/phpmyadmin/scripts/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.56.106/phpmyadmin/themes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
END_TIME: Sat Oct 12 01:15:15 2024
DOWNLOADED: 14199 - FOUND: 21

Recommendations:

Update Services: It is recommended to update Apache, PHP, OpenSSL, Samba, and MySQL to their latest versions to mitigate known vulnerabilities.

Disable Directory Indexing: Disable directory listing on the `/evil/` and `/webdav/` directories to prevent exposure of sensitive files.

Secure phpMyAdmin: Restrict access to phpMyAdmin and sensitive files such as `wp-config.php` and others.

Implement Proper Access Control (Additional Suggestion): Limit access to essential services (such as SSH and FTP) by restricting access through firewalls or using IP whitelisting to reduce exposure to unauthorized users.