

Домашнее задание:

1. Составьте отчет об уязвимости, которая рассмотрена в примере 1 методички и позволяет залить шелл на удаленный сервер.
2. Составьте отчет об уязвимости, рассмотренной в одном из примеров предыдущего урока.
3. Изучите описание и условия bug-bounty программы компании mail.ru и ответьте на вопрос: «Принимаются ли отчеты об уязвимостях, которые позволят реализовать атаку, требующую полного доступа к локальному аккаунту или профилю браузера»? Ответ обоснуйте.

Домашнее задание (повышенная сложность):

1. * Изучите внимательно пример 2 методички. К раскрытию какой конфиденциальной информации может привести такая атака? Ответ обоснуйте.
2. * Сможет ли злоумышленник найти список пользователей bwarrr, используя только сканер nikto? И если «ДА», то позволит ли найденная информация войти в систему? Ответ обоснуйте.

1.

1) Исследуемая страница <http://192.168.56.11>

2) Описание уязвимости

Имя найденной уязвимости	URL	Описание и последствия
УЯ1	http://192.168.56.11	На сайте http://192.168.56.11 есть открытые порты, что позволяет получить доступ к информации о приложениях. Уязвимость позволяет развить вектор атаки
УЯ2	http://192.168.56.11	На сайте http://192.168.56.11 разрешено индексирование каталогов. Это позволяет получать доступ к информации, хранящейся в каталогах на сервере. Уязвимость позволяет получить доступ к конфиденциальной информации. Не требует дополнительных уязвимостей для эксплуатации.
УЯ3	http://192.168.56.11/uploads	Для каталога разрешен метод PUT, что позволяет загрузить шелл на сервер.

3) Технические детали обнаружения и воспроизведения.

Уязвимости расположены по адресу <http://192.168.56.11>

Наименование продукта: Metasploitable 3 Linux virtual machine.

УЯ1 можно обнаружить, просканировав URL сканером nmap. Информацию о приложениях можно получить, просканировав порты сканером nikto.

```
(kali㉿kali)-[~]
└─$ nmap 192.168.56.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 03:20 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00076s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql
6666/tcp  open  irc
6667/tcp  open  irc
8080/tcp  open  http-proxy
8181/tcp  open  intermapper
10010/tcp open  rxapi
```

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-01 03:08 EDT
Nmap scan report for 192.168.56.11
Host is up (0.00068s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11 (Ubuntu Linu
x; protocol 2.0)
80/tcp    open  http         Apache httpd
111/tcp   open  rpcbind      2-4 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp          CUPS 1.7
3306/tcp  open  mysql        MySQL (unauthorized)
6666/tcp  open  ftp          vsftpd 3.0.2
6667/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.7 (2018-03-28))
10010/tcp open  rxapi?
listing when /s are requested.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing My
SQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3092: /phpmyadmin/README: phpMyAdmin is for managing MySQL database
s, and should be protected or limited to authorized hosts.
+ 8727 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:      2021-04-01 03:31:05 (GMT-4) (55 seconds)
```

УЯ2 и УЯ3 можно обнаружить сканером nikto

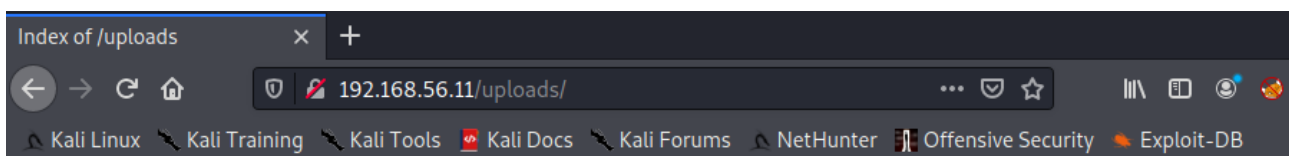
```
+ OSVDB-3268: /./: Directory indexing found.
+ /./: Appending './.' to a directory allows indexing
+ OSVDB-3268: //: Directory indexing found.
+ //: Apache on Red Hat Linux release 9 reveals the root directory listing
by default if there is no index page.
+ OSVDB-3268: /%2e/: Directory indexing found.
+ OSVDB-576: /%2e/: Weblogic allows source code or directory listing, upgra
de to v6.0 SP1 or higher. http://www.securityfocus.com/bid/2513.
+ OSVDB-3268: ///: Directory indexing found.
+ OSVDB-119: /?PageServices: The remote server may allow directory listings
through Web Publisher by forcing the server to show all files via 'open di
rectory browsing'. Web Publisher should be disabled. http://cve.mitre.org/c
gi-bin/cvename.cgi?name=CVE-1999-0269.
+ OSVDB-119: /?wp-cs-dump: The remote server may allow directory listings t
hrough Web Publisher by forcing the server to show all files via 'open dire
ctory browsing'. Web Publisher should be disabled. http://cve.mitre.org/cgi
-bin/cvename.cgi?name=CVE-1999-0269.
+ Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.26
+ OSVDB-3092: /phpmyadmin/ChangeLog: phpMyAdmin is for managing MySQL datab
ases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting ...
+ OSVDB-3268: //////////////////////////////////////
////////////////////////////////////
////////////////////////////////////
////////////////////////////////////: Directory indexing found.
+ OSVDB-3288: //////////////////////////////////////
```

```
ype
+ OSVDB-3268: /uploads/: Directory indexing found.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ OSVDB-397: HTTP method 'PUT' allows clients to save files on the web serv
er.
```

Далее с помощью curl шелл загружается в каталог *uploads*.

4) Демонстрация возможностей эксплуатации.

См. выше плюс:



Index of /uploads

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
msf_http_put_test.txt	2019-02-01 21:45	13	
shell.php	2018-12-17 22:36	22	
shell2.php	2018-12-17 22:43	1.1K	
shell21.php	2018-12-17 22:43	1.1K	
test	2018-12-15 18:51	9	
test.php	2018-12-15 18:52	9	

5) Выводы и рекомендации по устранению

Запретить просмотр каталогов, закрыть порты, запретить метод PUT.

6) При тестировании использовались Kali Linux, включенные в его сборку сканеры nmap и nikto, Firefox web browser.

2. Возьмем для примера из предыдущего урока уязвимость weak password в bWapp.

1) Исследуемая страница <http://192.168.56.11/bwapp/login.php>

2) Описание уязвимости


Имя найденной уязвимости	URL	Описание и последствия
УЯ1	http://192.168.56.11/bwapp/ba_weak_pwd.php	На сайте http://192.168.56.11/bwapp установлены пароли не соответствующие требованиям безопасности. Уязвимость позволяет быстро и просто подобрать пароль брутфорсом.

3) Технические детали обнаружения и воспроизведения.

Уязвимости расположены по адресу http://192.168.56.11/bwapp/ba_weak_pwd.php

Наименование продукта: Metasploitable 3 Linux virtual machine.

Как критерий для выявления нужной пары логин/пароль можно использовать сообщение о неверном вводе данных.



Broken Auth. - Weak Passwords

Enter your credentials.

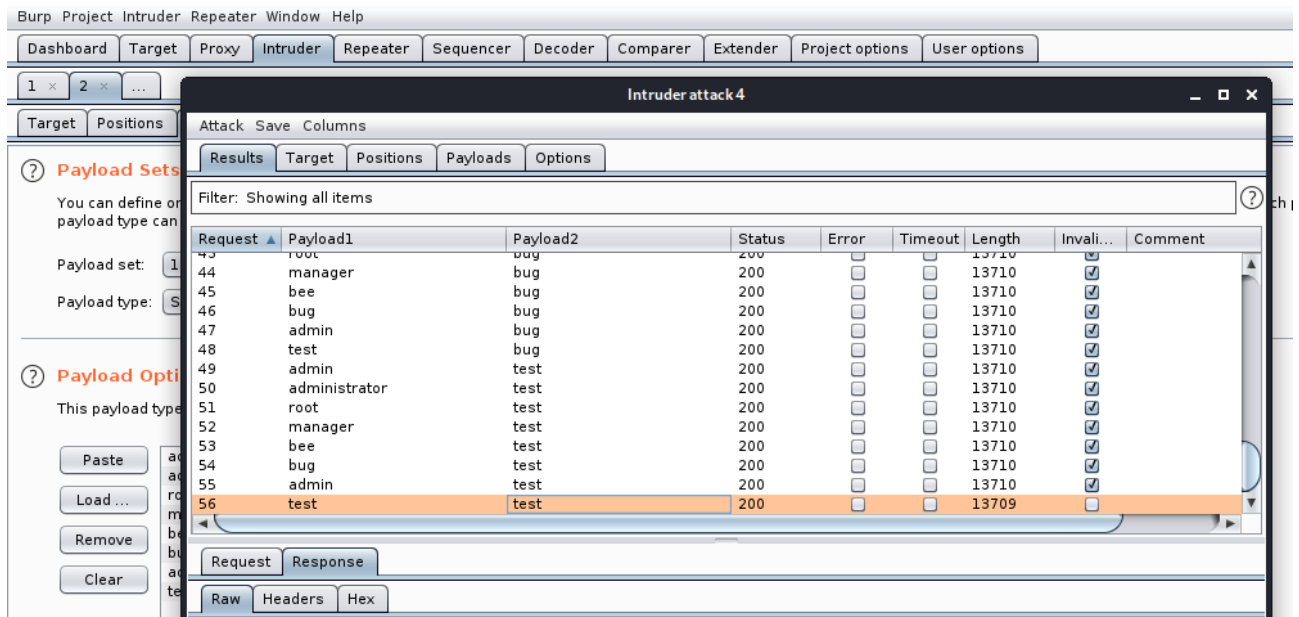
Login:

Password:

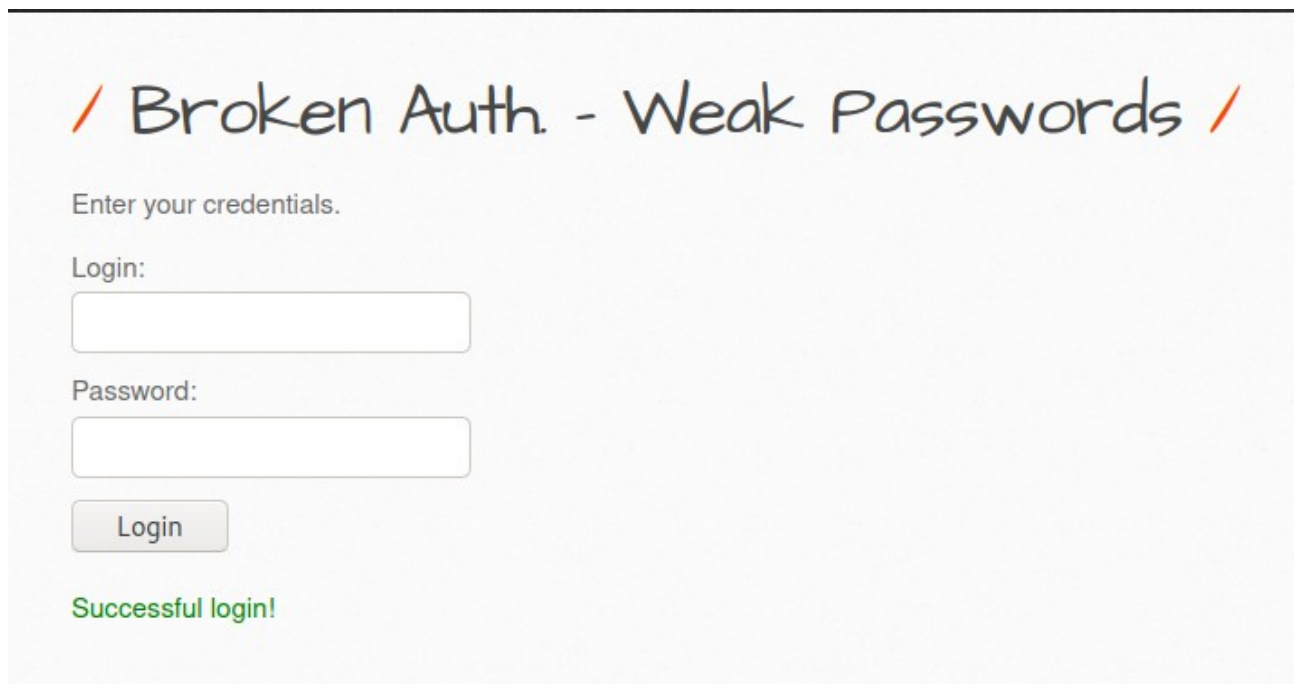
Login

Invalid credentials!

Далее запускаем брутфорс с помощью burp suite. Кстати словари для логинов и паролей есть в стандартной сборке kali linux в файле /usr/share/wordlists/rockyou.txt.gz.



4) Демонстрация возможностей эксплуатации



5) Выводы и рекомендации по устранению

Установить пароль соответствующий стандартным требованиям безопасности. Пароль должен содержать буквы в разных регистрах, числа, спецсимволы и быть длиной 10 или более символов.

6) При тестировании использовались Kali Linux, burp suite community edition.

3. Вознаграждения за такой тип атаки получить не удастся. Об этом написано:

We will not pay a reward (and we will be really upset) if we detect:
Attempt to access arbitrary user's account or data or another vulnerability post-exploitation not required to demonstrate the bug presence

И далее:

Please **use your own accounts, phone numbers, etc** to conduct your research. Do not try to gain access to others' accounts or any confidential information.

2*. Достаточно nikto и браузера(или командной строки).

А можно и без браузера, используя опцию -output (nikto -host http://192.168.56.11:80/bwapp/admin/index.php -Format txt -output /bwappadmin.txt).





```
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS
+ Cookie PHPSESSID created without the httponly flag
+ OSVDB-3092: /bwapp/web.config: ASP config file is accessible.
+ OSVDB-9216: /bwapp/test.php?%3CSCRIPT%3Ealert('Vulnerable')%3C%2FSCRIPT%3E=x: OmniHTTPD's test.php is vulnerable to Cross Site Scripting (XSS). http://www.cert.org/advisories/CA-2000-02.html.
+ /bwapp/phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-3092: /bwapp/admin/: This might be interesting...
+ OSVDB-3268: /bwapp/apps/: Directory indexing found.
+ OSVDB-3092: /bwapp/apps/: This might be interesting...
+ OSVDB-3268: /bwapp/db/: Directory indexing found.
+ OSVDB-3092: /bwapp/db/: This might be interesting...
+ OSVDB-3268: /bwapp/logs/: Directory indexing found.
+ OSVDB-3092: /bwapp/logs/: This might be interesting...
+ OSVDB-3092: /bwapp/passwords/: This might be interesting...
+ OSVDB-3268: /bwapp/stylesheets/: Directory indexing found.
+ OSVDB-3092: /bwapp/stylesheets/: This might be interesting...
+ OSVDB-3093: /bwapp/admin/index.php: This might be interesting... has been seen in web logs from an unknown scanner.
+ OSVDB-3233: /bwapp/phpinfo.php: PHP is installed, and a test script which runs phpinfo() was found. This gives a lot of system information.
+ /bwapp/admin/phpinfo.php: Output from the phpinfo() function was found.
+ OSVDB-35877: /bwapp/admin/phpinfo.php: Immobilier allows phpinfo() to be run.
+ OSVDB-5092: /bwapp/config.inc: DotBr 0.1 configuration file includes user names and passwords.
+ Cookie admin created without the httponly flag
```

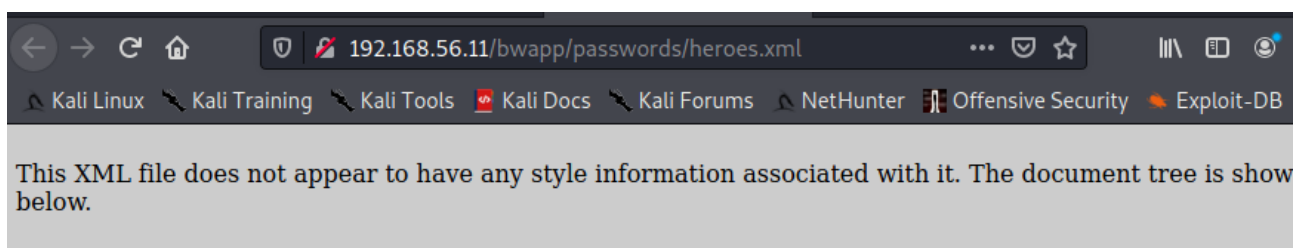
/bwapp/admin/

/ Settings /

Setting	Value	Description
Security Level	low	Possible values: low - medium - high
SMTP Server		Used for e-mail functionality
A.I.M. IP Address	6.6.6.6	A no-authentication mode, for testing web scanners and crawlers
Evil Bee Mode	0	All security levels are bypassed in this mode
Credentials	bee/bug	Static credentials used on some pages

/bwapp/passwords/

<u>name</u>	<u>last modified</u>	<u>size</u>	<u>description</u>
 Parent Directory	-		
 heroes.xml	2018-10-19 22:53	1.2K	
 web.config.bak	2018-10-19 22:53	7.4K	
 wp-config.bak	2018-10-19 22:53	1.5K	



```
-<heroes>
  -<hero>
    <id>1</id>
    <login>neo</login>
    <password>trinity</password>
    <secret>Oh why didn't I took that BLACK pill?</secret>
    <movie>The Matrix</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    <id>2</id>
    <login>alice</login>
    <password>loveZombies</password>
    <secret>There's a cure!</secret>
    <movie>Resident Evil</movie>
    <genre>action horror sci-fi</genre>
  </hero>
  -<hero>
    <id>3</id>
    <login>thor</login>
    <password>Asgard</password>
    <secret>Oh, no... this is Earth... isn't it?</secret>
    <movie>Thor</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    <id>4</id>
    <login>wolverine</login>
    <password>Log@N</password>
    <secret>What's a Magneto?</secret>
    <movie>X-Men</movie>
    <genre>action sci-fi</genre>
  </hero>
  -<hero>
    ...
  </hero>
```

```
<?php

/*
bwAPP, or a buggy web application, is a free and open source deliberately insecure web application.
It helps security enthusiasts, developers and students to discover and to prevent web vulnerabilities.
bwAPP covers all major known web vulnerabilities, including all risks from the OWASP Top 10 project!
It is for security-testing and educational purposes only.

Enjoy!

Malik Mesellem
Twitter: @MME_IT

bwAPP is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License
(http://creativecommons.org/licenses/by-nc-nd/4.0/). Copyright © 2014 MME BVBA. All rights reserved.

*/

// Connection settings
$server = "localhost";
$username = "alice";
$password = "loveZombies";
$database = "bwAPP_BAK";

?>
```

Логин/пароль для основного входа есть в админке.

Логин/пароль alice судя по всему для БД.

Другие логины и пароли не подходят на основной странице но возможно используются где-то еще.

В web.config.bak можно найти вот такую вещь:

```
856AD364E35" requirePermission="false" allowDefinition="MachineToApplication" />
<section name="roleService" type="System.Web.Configuration.ScriptingRoleServiceSection, System.Web.Extensions, Version=3.5.0.0, Culture=neutral, PublicKeyToken=31BF3856AD364E35" requirePermission="false" allowDefinition="MachineToApplication" /></sectionGroup></sectionGroup></configSections><appSettings>
  <connectionStrings>
    <add name="bwAPPConnectionString" connectionString="Data Source=bee-box;Initial Catalog=bwAPP;Persist Security Info=True;User ID=wolverine;Password=Log@N" />
  </connectionStrings>
  <system.web>
    <globalization culture="nl-BE" uiCulture="nl-BE" />
    <!--
    Set compilation debug="true" to insert debugging
```

И тд. тп.

1*. Как я понял в примере 2 из методички сканируются каталоги, в которые можно зайти и посмотреть там логи и конфиги приложений и выудить из них логины и пароли. Например для MySQL или админки PHP. По аналогии с заданием 2*.