iNURTURE
Education Solutions
TOMORROW'S HERE

Chapter 4.2

Mitigation of Vulnerabilities

Aim

To elaborate on how vulnerabilities are mitigated using various tools and techniques

Instructional Objectives

After completing this chapter, you should be able to:

- Discuss how vulnerabilities are exploited along with its consequences, with practical examples
- Explain how vulnerabilities are mitigated using various tools and techniques

Learning Outcomes

At the end of this chapter, you are expected to:

- Demonstrate how vulnerabilities are exploited
- Provide various countermeasures used to mitigate vulnerabilities

Vulnerabilities

Demonstration of Vulnerabilities

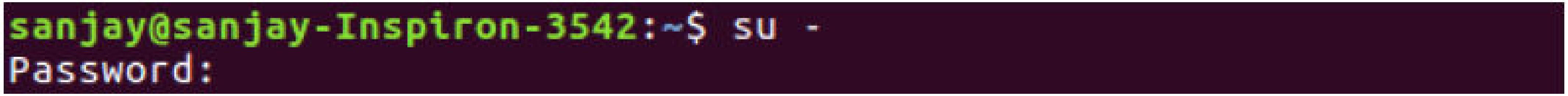
Information systems are constantly exposed to risks, which in simple terms, is the likelihood of a threat exploiting a vulnerability that exists in a system

The penetration test is very helpful for thoroughly investigating a system and to find out vulnerabilities that could be exploited by hackers.

‘Risk management’, is a branch of information security that deals with the various aspects of evaluating risks, while identifying procedures that avoid the impact due to these risks.

Example of a Vulnerability Exploitation

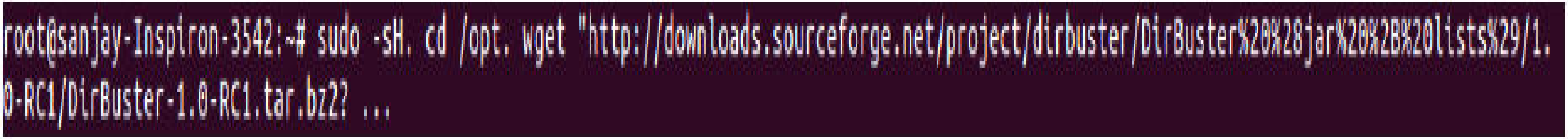
- Any desktop/laptop needs to be checked for vulnerabilities at the root directory as shown in Figure below.



```
sanjay@sanjay-Inspiron-3542:~$ su -
Password:
```

Command to Enter to Root

Once the password is entered, the root@xyz will be available for the user as shown below and to get the DirBuster software one could type the line as shown in Figure

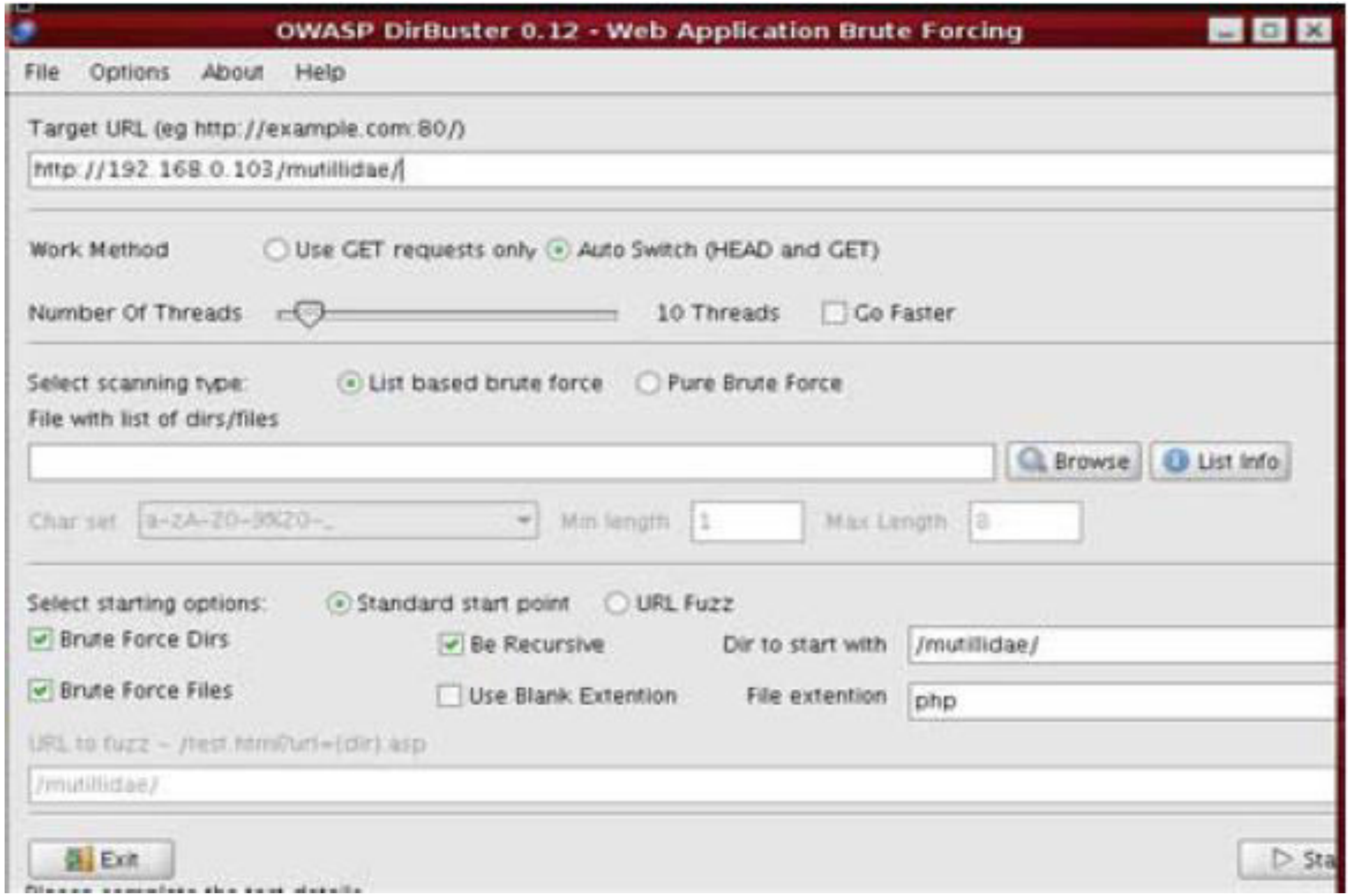


```
root@sanjay-Inspiron-3542:~# sudo -sH. cd /opt. wget "http://downloads.sourceforge.net/project/dirbuster/DirBuster%20%28jar%20%2B%20lists%29/1.
0-RC1/DirBuster-1.0-RC1.tar.bz2? ...
```

The DirBuster is used with the help of this command.

```
sudo -sH
cd /opt/DirBuster
./DirBuster-1.0-RC1.sh
```

After this has been completed, a new popup window with the IP address and the directory name is seen, as shown



OWASP DirBuster 0.12 - Web Application Brute Forcing

Target URL (eg http://example.com:80/)
http://192.168.0.103/mutillidae/

Work Method ○ Use GET requests only ● Auto Switch (HEAD and GET)

Number Of Threads 10 Threads □ Go Faster

Select scanning type: ● List based brute force ○ Pure Brute Force

File with list of dirs/files

Char set a-zA-Z0-9%20-_ Min length 1 Max Length 8

Select starting options: ● Standard start point ○ URL Fuzz

☑ Brute Force Dirs ☑ Be Recursive Dir to start with /mutillidae/

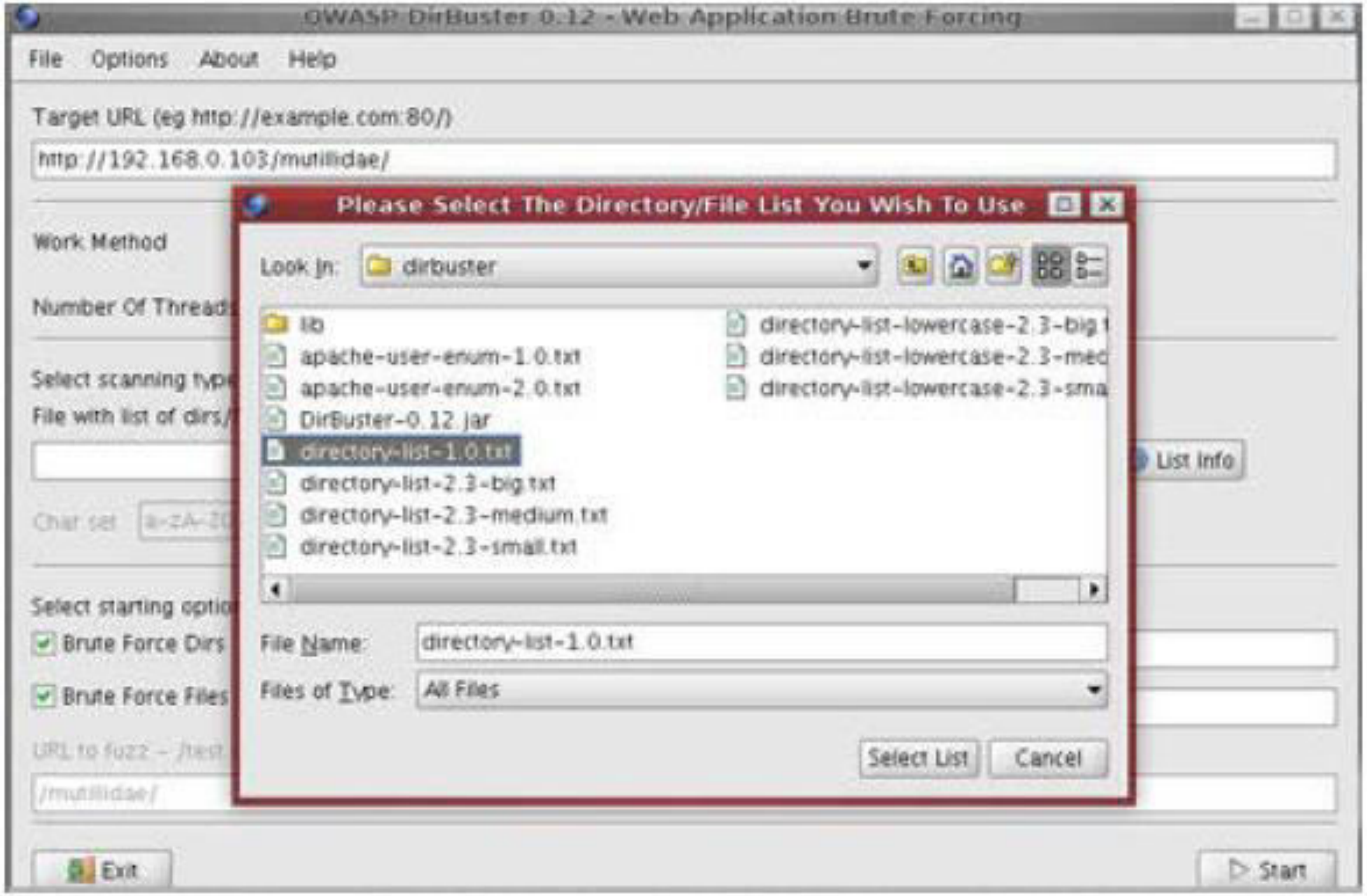
☑ Brute Force Files □ Use Blank Extention File extention php

URL to fuzz - /test.html?url={dir}.asp

/mutillidae/

Please complete the test details

An arbitrary directory is selected, which is present in the DirBuster directory for illustration


OWASP DirBuster 0.12 - Web Application Brute Forcing
File
Options
About
Help
Please Select The Directory/File List You Wish To Use
List Info
Exit
Start
Select List
Cancel

Target URL (eg http://example.com:80/)

http://192.168.0.103/mutillidae/

Work Method

Number Of Thread

Select scanning type

File with list of dirs/

Char set a-zA-Z0

Select starting optio

☑ Brute Force Dirs

☑ Brute Force Files

URL to fuzz - /test

/mutillidae/

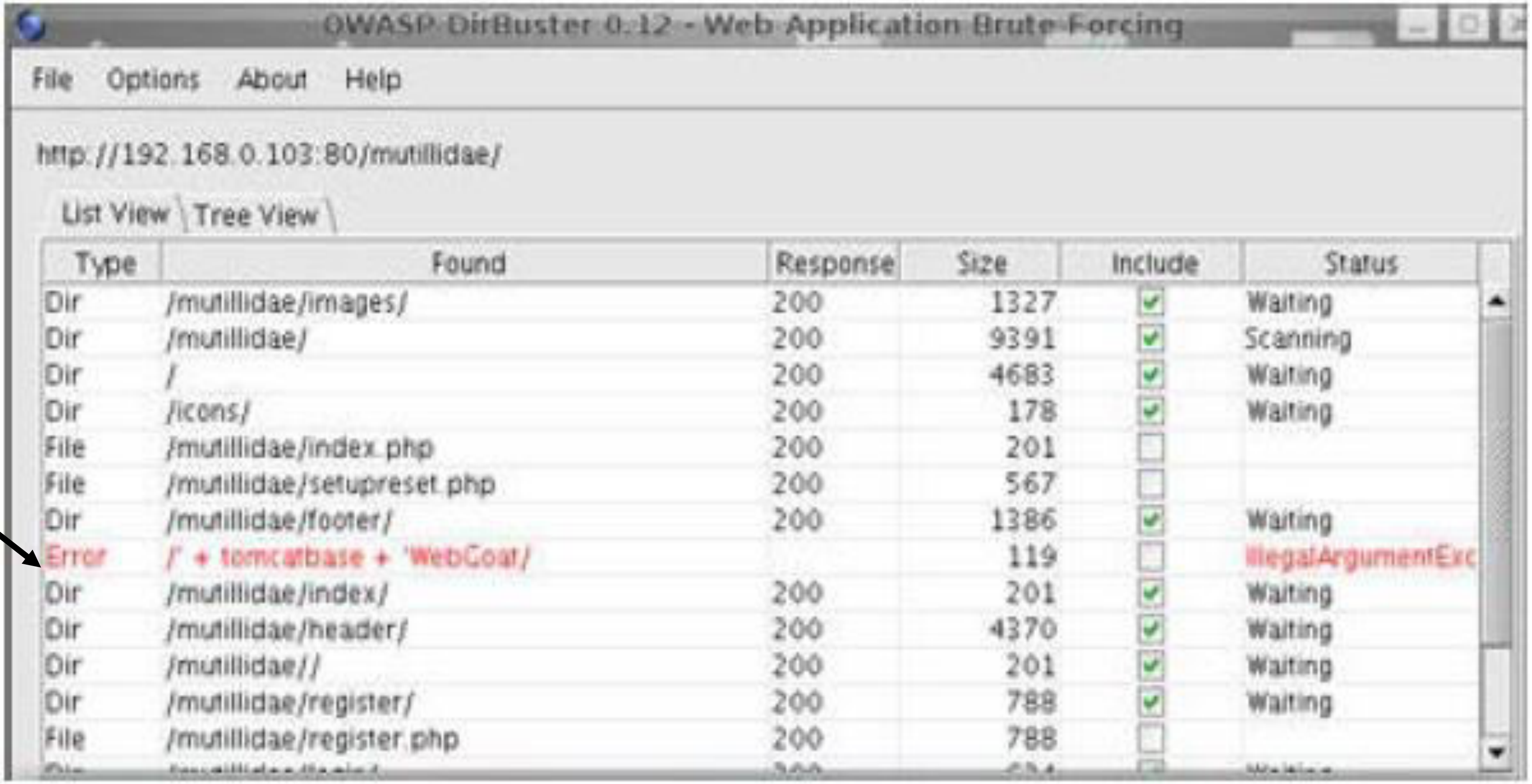
Look In: dirbuster

lib
apache-user-enum-1.0.txt
apache-user-enum-2.0.txt
DirBuster-0.12.jar
directory-list-1.0.txt
directory-list-2.3-big.txt
directory-list-2.3-medium.txt
directory-list-2.3-small.txt
directory-list-lowercase-2.3-big.t
directory-list-lowercase-2.3-med
directory-list-lowercase-2.3-sma

File Name: directory-list-1.0.txt

Files of Type: All Files

Once the arbitrary folder is selected as shown in previous slide, an error is generated giving rise to the html file that contains the password as shown

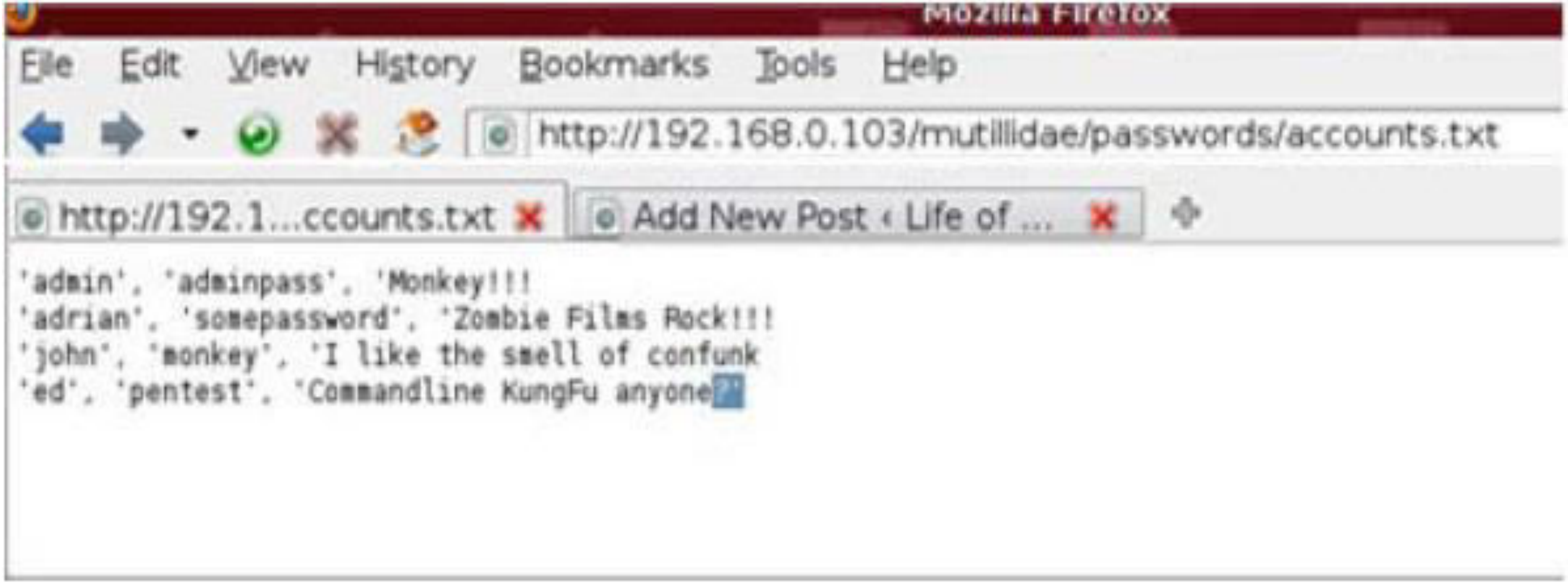


Error

http://192.168.0.103:80/mutillidae/

Type	Found	Response	Size	Include	Status
Dir	/mutillidae/images/	200	1327	☑	Waiting
Dir	/mutillidae/	200	9391	☑	Scanning
Dir	/	200	4683	☑	Waiting
Dir	/icons/	200	178	☑	Waiting
File	/mutillidae/index.php	200	201	□	
File	/mutillidae/setupreset.php	200	567	□	
Dir	/mutillidae/footer/	200	1386	☑	Waiting
Error	/' + tomcatbase + 'WebGoat/		119	□	IllegalArgumentExc
Dir	/mutillidae/index/	200	201	☑	Waiting
Dir	/mutillidae/header/	200	4370	☑	Waiting
Dir	/mutillidae//	200	201	☑	Waiting
Dir	/mutillidae/register/	200	788	☑	Waiting
File	/mutillidae/register.php	200	788	□	

Html File Containing the Password of the Admin

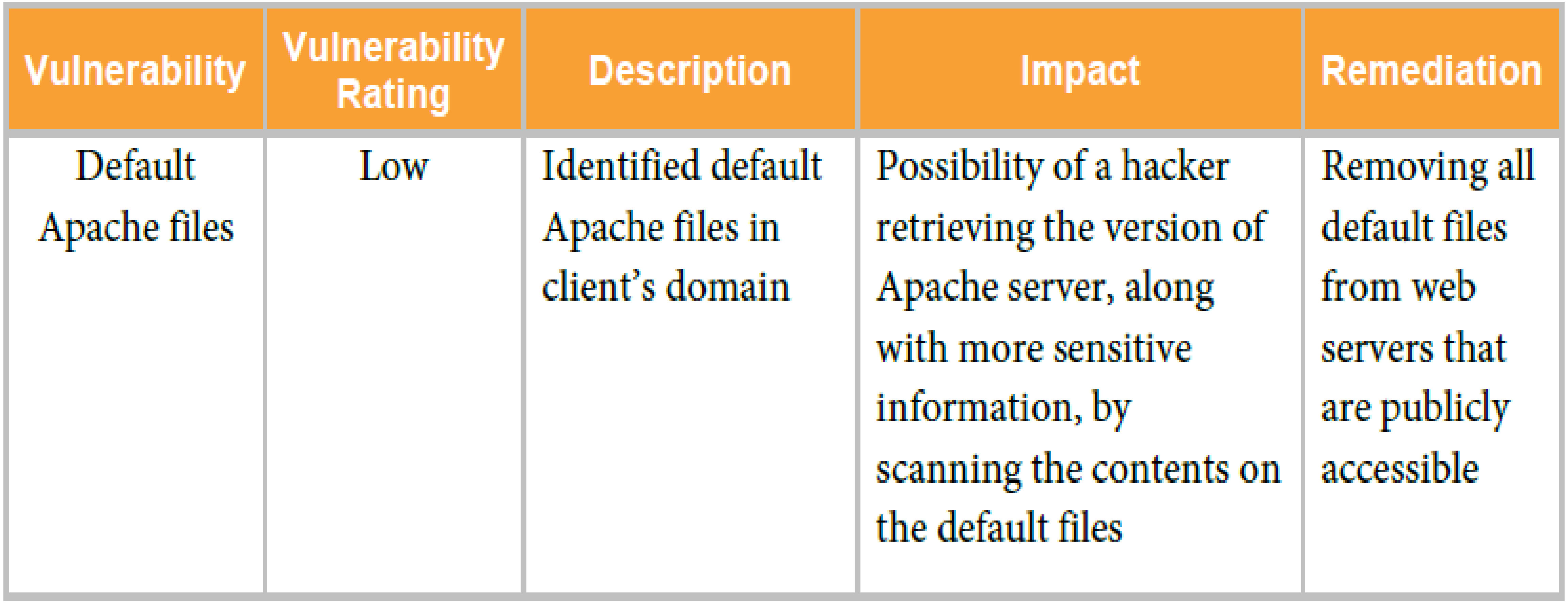

Mozilla Firefox
File
Edit
View
History
Bookmarks
Tools
Help
http://192.168.0.103/mutillidae/passwords/accounts.txt
http://192.1...ccounts.txt
Add New Post ‹ Life of ...

```
'admin', 'adminpass', 'Monkey!!!
'adrian', 'somepassword', 'Zombie Films Rock!!!
'john', 'monkey', 'I like the smell of confunk
'ed', 'pentest', 'Commandline KungFu anyone?'
```

Consequences

- This is most likely how a hacker would exploit this specific vulnerability and gain access to the /admin folder to retrieve further information such as the version of web server, by scanning the contents of the /admin folder.
- The above information can be conveyed in a tabular format in the penetration test report.

Vulnerability Mitigation



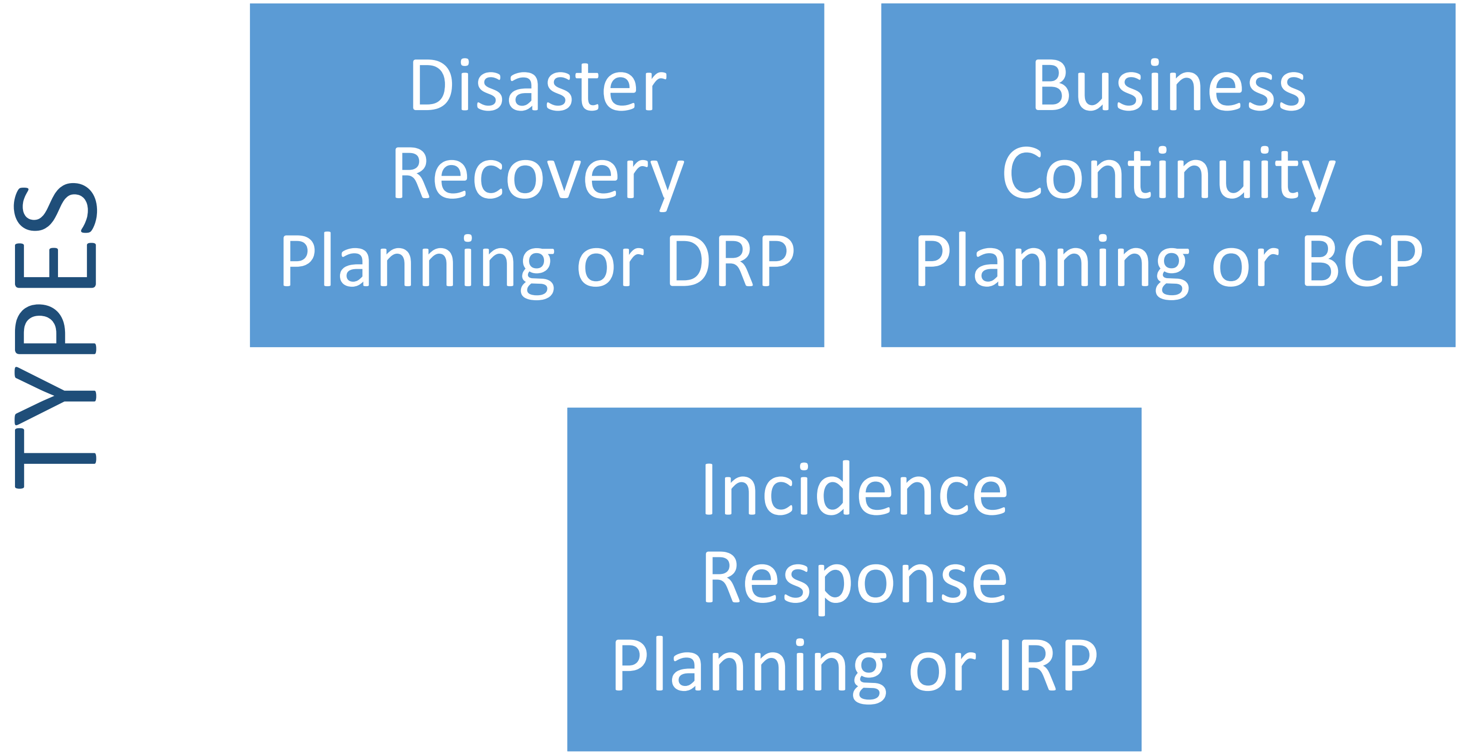
Vulnerability	Vulnerability Rating	Description	Impact	Remediation
Default Apache files	Low	Identified default Apache files in client's domain	Possibility of a hacker retrieving the version of Apache server, along with more sensitive information, by scanning the contents on the default files	Removing all default files from web servers that are publicly accessible

Quiz / Assessment

<table>
<tr><td colspan="4">1) The process in which primary and secondary name servers in a domain update their DNS data, is called</td></tr>
<tr><td>a) DNS poisoning</td><td>b) DNS lookup</td><td>c) DNS zone transfer</td><td>d) None of the above</td></tr>
<tr><td colspan="4">2) Which of these is a method used in the mitigation of a certain vulnerability?</td></tr>
<tr><td>a) Installing software patches</td><td>b) Enforcing strong password policies</td><td>c) Training and building awareness in people about information security</td><td>d) All of the above</td></tr>
</table>

Mitigation

In the instance of a vulnerability discovered in a system through penetration testing, the next step is to avoid the impact of such vulnerability, through thorough planning and preparation. This process is called 'mitigation'.



TYPES

Disaster Recovery Planning or DRP

Business Continuity Planning or BCP

Incidence Response Planning or IRP

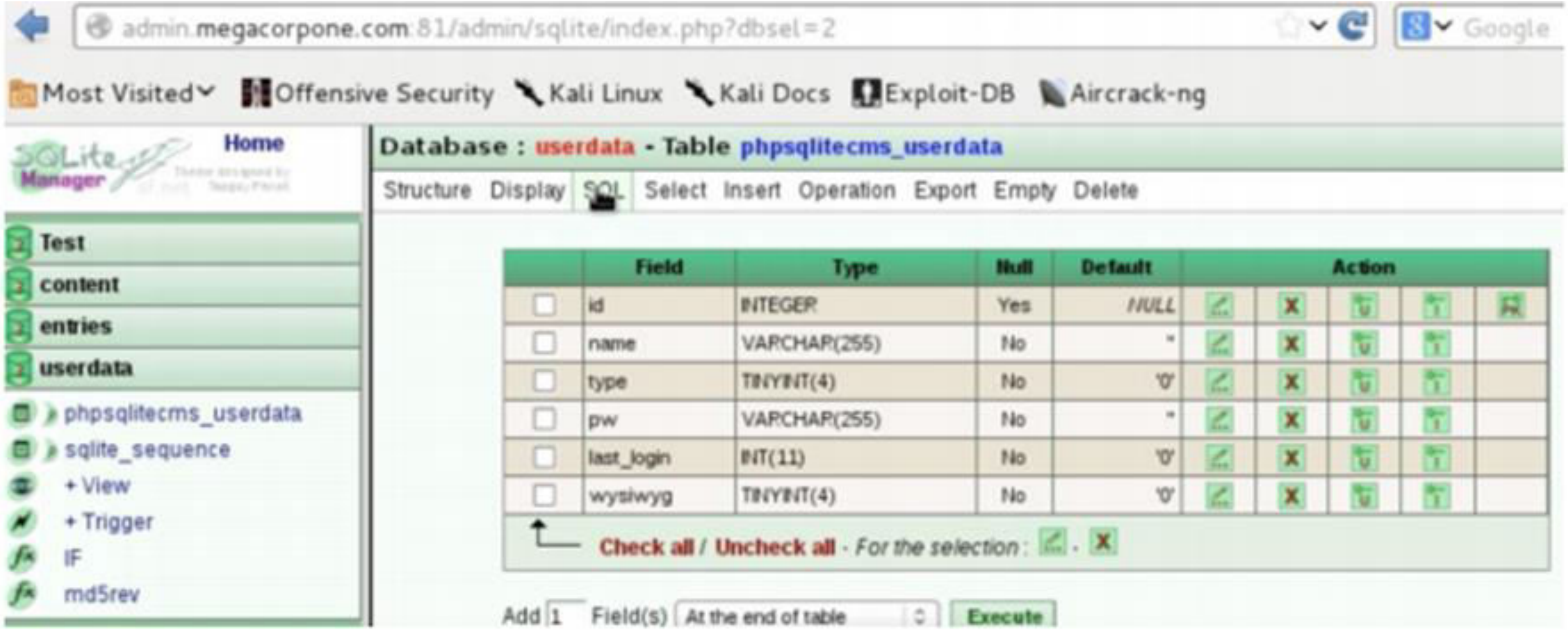
Comparison of the Types of Mitigation Plans

Plan type	Description	Steps include	Deployment	Execution time
Incidence Response Plan	Includes methods taken by organisation during attacks (incidents)	• Intelligence gathering • Information analysis	Unveiling of an attack	Immediate. Works in real-time environment
Disaster Recovery Plan	Includes methods to recover of data and to bring system to normalcy, in case of a disaster. Also aims at minimising the losses during the disaster	• Methods to recover lost data • Methods to reinstall disrupted or suspended services • Methods to shut-down system completely (if none of the other methods work)	Once the attack has been declared as disaster, owing to its severity and impact level	Short term recovery
Business Recovery Plan	Consists of methods that must be implemented in order to keep the business processing running, when a disaster disrupts the entire system	• In case it demands relocating the business operation, secondary datacentres must be activated • Immediately establishing a remote site that can handle business operations	When it is realised that the disaster it going to hit the continuity of business operations	Long-time recovery

Scenario

To discuss mitigation in greater detail, let us go back to the previous example of penetration testing on a network.

Website showing an instance of SQLite Manager



Database : userdata - Table phpsqlitecms_userdata

	Field	Type	Null	Default	Action
☐	id	INTEGER	Yes	NULL	X
☐	name	VARCHAR(255)	No	''	X
☐	type	TINYINT(4)	No	'0'	X
☐	pw	VARCHAR(255)	No	''	X
☐	last_login	INT(11)	No	'0'	X
☐	wysiwyg	TINYINT(4)	No	'0'	X

Algorithm

```
function generate_pw_hash($pw)
{
$Salt=random_String(10,’0123456789abcdef’);
$Salted_hash=sha1($pw.$Salt);
$hash_with_salt=$salted_hash.$salt;
Return $hash_with_salt;
}
```

Mitigation Report

Vulnerability	Vulnerability rating	Description	Impact	Remediation
Password reuse	High	The user 'mike' belonging to MegaCorp one domain has been found reusing credentials for SQLite Manager application and his Windows domain	In this case, as the user was using his password for SQLite Manager for his windows login, attacker indirectly got access to internal Windows domain controllers, which could cost the company very dearly.	Organisation should enforce password policy that prevents users from reusing their passwords as it increases the probability of attacks. One way of doing this is by using Password managers.

Quiz / Assessment

3) One of the options given below is not a mitigation planning type			
a) Disaster Recovery Planning	b) Vulnerability Assessment	c) Incidence Response Planning	d) Business Continuity Planning
4) An organisation has come under an unexpected disaster and facing uncertainties to operate from its premises and the management is keen on relocating with immediate effect. Which is the most appropriate mitigation plan that must be followed.			
a) Disaster Recovery Planning	b) Business Continuity Planning	c) Incidence Response Planning	d) None of the above

e-References & External Resources

- *A case study of Penetration test and vulnerability assessment report-* https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf
- *Risk Mitigation Planning, Implementation and Progress Monitoring-* https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring
- *The Mitigation Strategy: Goals, Actions, Action Plan*-http://mitigationguide.org/task-6/the-mitigation-strategy-goals-actions-action-plan/. This source also gives numerous example of mitigation plans that you can refer
- *Mitigation techniques for Password threat vulnerability-* https://msdn.microsoft.com/en-us/library/windows/desktop/ms717803(v=vs.85).aspx

External Resources

1. Kimberly Graves. Official Certified Ethical Hacker Review Guide
2. Patrick Engebretson. The Basics of Hacking and Penetration Testing, (Second edition)
3. Gregg, Certified Ethical Hacker(with CD), Pearson Education India

Activity

Online Activity
(30min)

Description :

Write a short note on vulnerability management and policy related to vulnerability management.

Thank You