2A

ANITS

ANIL NEERUKONDA INSTITUTE OF TECHNOLOGY AND SCIENCES
(*Approved by AICTE, Affiliated to Andhra University& Accredited by NBA*)
Sangivalasa-531 162, Bheemunipatnam Mandal, Visakhapatnam Dt.
Phone Nos:08933 225083,225084,225087,226131 Fax No 226395
Website : www.anits.edu.in **e-mail: principal@anits.edu.in**

DEPT OF COMPUTER SCIENCE AND ENGINEERING

Ref : ANITS/CSE/Faculty Seminar/2017-18/05 Date: 15-02-2018

CIRCULAR

All the students of 2/4 CSE – A are informed that there will be a seminar titled **"Web Technologies and Cyber Security"** by A. Aditya of 2/4 CSE-B 316126510122 on 16th Feb, 2018. The venue is E-Classroom at 1:40PM.

All the students must attend the seminar. Attendance will be taken during the event.

Faculty Seminar Club

15/2/18

15/2/18

Head of the Department of
Computer Science & Engineering
Anil Neerukonda Institute of
Technology & Sciences
Sangivalasa, Visakhapatnam Dist.

Student Name	Roll No	II/IV CSE-A	Signature
1. Menaka	316126510002		Menaka
P. Gayatri	316126510038		Gayatri
A. chaitanya	316126310046		chaitanya
K. Vastu	316126510022		Vastu
B. Srikanth	316126510124		Srikanth
R. Jayachandra	316126510067		Jayachandra
N. Saipranav	316126510035		N. Saipranav
M.VR Nithil	316126510029		Nithil
K.T Trinikunta	316126510020		K.T Trinikunta
G. Manoj	316126510013		G. Manoj
G. Satish	316126510010		G. Satish
K. Sai Sankar	316126510023		K. Sai Sankar
A. Ravikiran	316126510062		Ravikiran
P.B. Sravan Sai	316126510043		P.B. Sravan Sai
N. Amrutha Lakshmi	316126510032		Amrutha
B Sri Vidya	316126510005		Vidya
B Ashok Kumar	316126510004		Ashok
S. Sai Tej	316126510052		Sai Tej
D. Tarakeswara Rao	316126510138		D. Tarakeswara Rao
Ch. Hemanth Kashyap	316126510132		Hemanth

Student Name	Roll NO	Signature II/IV CSE
G Harsha Vardhan	316126510016	G. Harsha
M. Sohil Roy	316126510025	
SHIVSHANKAR SINGH	316126510050	
M. Raghu	316126510031	
V.S.R. Sagar	316126510057	Sagar
J. Likith	316126510017	
B. Vaishnavi	316126510068	
M. Sravani	316126510024	M. Sravani
K. Alekhya	316126510021	K Alekhya
S. Dinisha	316126510053	S Dinisha
B. Jyothirmayi	316126510065	B. Jyothi
D.L. Sai Sravani	316126510070	Sravani
B. Kanthi	316126510007	
A Tejaswini. A	316126510054	Tejaswini
V Nitesh	316126510059	
B. Rohith	316126510003	Rohith
R. John Wesley	316126510045	
G. Eshlar Sai kumar	316126510011	G. Eshar.
P Suryaja	316126510037	P Suryaja
G. Sandhya	316126510015	G. Sandhya
N. Mounica	316126510053	Mounica
V. Roseline	316126510047	Roseline
M Sushma	316126510027	
P.L Harika	316126510036	Harika
U. Bhavana	316126510056	Bhav
P. Krishna Priya	316126510042	

(1-72 BA (73- B)

Seminar on Web Technologies and Cyber Security

yber Security or information technology Security is a field within information technology nvolving the protection of computer systems and the prevention of unauthorized use or changes r access of electronic data. It deals with the protection of software, hardware, networks and its nformation. Due to the heavy reliance on computers in the modern industry that store and ransmit an abundance of confidential information about people, cyber security is a critical unction and needed insurance of many businesses. It also protects computer systems from theft or damage.

Common Vulnerabilities

Vulnerabilities in Cybersecurity system can come from many different factors. Most of these center around any inherent faults within the system itself, how easy it would be for a cyber attacker to break through any securities the system may have set up, and/or how easy it is for the cyber attacker to use the fault in the system to their advantage. One of the most common faults found in systems that can be abused by attackers is when a system is too complex. The more detailed a system becomes, the harder it is for cybersecurity to cover all the flaws. Thus, creates more opportunities for attacks to make their mark. Also, whenever user input is a variable, there can be ways into a system. This is because it is difficult for a programmer to predict and account for all possible inputs from a user. Attackers could affect the system depending on their inputs which would allow them to exploit the system further.

Denial of service attacks

Denial of service (DoS) attack is a type of cyber attack that floods a network with multiple requests of information with the purpose of shutting down or disrupting services of a host connected to the internet. It may also prevent users of a service running through the targeted server or network.

Direct-access attacks

This form of vulnerability is when a system is physically accessed by an unauthorized user. This allows the user to make modifications or attach backdoor hardware or software in order to access the system remotely. The unauthorized user can also make complex changes to the system due to having direct access to the hardware.

Pharming

Pharming is a form of online fraud that redirects users from legitimate website's traffic to another fake site. Hackers can use pharming by using tools that redirects users to a fake site. The victimized

users will go to a fake website without noticing it is fake. Hackers use this method to steal personal data from users' computer. Hackers exploits the DNS server or called DNS poisoning that makes users think the fake sites are legitimate.

Phishing

Phishing is an email that claims to be a genuine business in an attempt to swindle the user into surrendering sensitive information. The personal information that they receive is then used to steal their identity and can result in a loss of financial freedom.

Social Engineering

Social engineering involves human interaction and the manipulation of people to give up confidential information. The purposes for this technique include fraud, system access or information gathering. It is easier for someone to fool you into giving them a password or bank information than it is for someone to try hacking in order to get the information.

Other Vulnerabilities

There are other vulnerabilities and ways that hackers can gain access of a system. They can use backdoors which is a different method of accessing a computer or network that bypass the authentication and security. Spoofing can also be used to trick a receiver by pretending to be a known source to the receiver. Private escalation can be used to elevate an attacker's access level which will give them access to every file on a computer just like a root user can. A more complicated one is clickjacking. This is when an attacker inverts the user's clicks to buttons or links that take the user to another website.

The Author discussed the above topics and the seminar ended with thanks.

Head of the Department of
Computer Science & Engineering
Adi Kavikunjar Institute of
Technology & Science
Sangivalasa, Visakhapatnam Dist.