MAJOR – SEP

Name – Anjali Kuamri

Email – anjalirajwar101@gmail.com

College Name – BIT Sindri

Cyber Security Major Project

6. Write an Article on cybersecurity and recent attacks which you came across in media and news and research on that news, and explain the any topic which you learned in this course and mention what you learned

Article on cybersecurity

Article on and recent attacks

Explain XSS attack

Summary

CyberSecurity

Cyber security is the **practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks**. It's also known as information technology security or electronic information security.

Cybersecurity is important **because it protects all categories of data from theft and damage**. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

we will observe five types of cybersecurity techniques

- Critical Infrastructure Cybersecurity. ...
- Network Security. ...
- Cloud Security. ...
- Internet of Things Security. ...
- Application Security.

Examples of Network Security includes **Antivirus and Antispyware programs**, Firewall that block unauthorized access to a network and VPNs (Virtual Private Networks) used for secure remote access

Who needs cyber security?

Now, from social media to online banking to digital hospital records, every piece of our lives are available on the internet. Hackers and other nefarious characters can fight to gain access to this information and use it for their own purposes. In essence, **everyone needs cyber security**

The CIA Triad is a security model developed to ensure the 3 goals of cybersecurity, which are **Confidentiality, Integrity, and Availability of data and the network**.

The Top 10 Personal Cyber Security Tips

1. Keep Your Software Up to Date

2. Use Anti-Virus Protection & Firewall

3. Use Strong Passwords & Use a Password Management Tool

4. Use Two-Factor or Multi-Factor Authentication

5. Learn about Phishing Scams – be very suspicious of emails, phone calls, and flyers

6. Protect Your Sensitive Personal Identifiable Information (PII)

7. Use Your Mobile Devices Securely

8. Backup Your Data Regularly

9. Don’t Use Public Wi-Fi

10. Review Your Online Accounts & Credit Reports Regularly for Changes

What is history of cyber security?

Cybersecurity proper **began in 1972 with a research project on ARPANET** (The Advanced Research Projects Agency Network), a precursor to the internet. ARPANET developed protocols for remote computer networking

What is cyber safety?

Cybersafety is **the safe and responsible use of Information and Communication Technologies (ICT)**. ... Encouraging the public to identify the risks associated with ICT. Putting in place strategies

to minimise and manage risks. Recognising the importance of effective teaching and learning programmes

15 Common Cybersecurity Risks

1 – Malware

2 – Password Theft

3 – Traffic Interception

4 – Phishing Attacks

5 – DDoS

6 – Cross Site Attack

7 – Zero-Day Exploits

8 – SQL Injection

9 – Social Engineering

10 – MitM Attack

11 – Ransomware

12 – Cryptojacking

13 – Water Hole Attack

14 – Drive-By Attack

15 – Trojan Virus

SQL injection flaw in billing software app tied to US ransomware infection

John Leyden 26 October 2021 at 14:54 UTC
Updated: 26 October 2021 at 15:26 UTC

BQE Software's BillQuick Web Suite versions earlier than 22.0.9.1 allows SQL injection that gives rise to an even more serious remote code execution (RCE) risk.

The CVE-2021-42258 vulnerability was patched on October 7 (PDF) but a number of systems nonetheless remain vulnerable.

Huntress Threat Ops team reports that the vulnerability was exploited to get initial access onto the systems of a US engineering company prior to a ransomware attack.

Active exploitation

BQE boasts a user base of 40,000 of mostly small to medium-sized organizations worldwide, and the need for those behind the curve of patching or remediating this actively exploited vulnerability could hardly be more pressing.

The vulnerability enables blind SQL injection via the application's main login form. this opens the door to both stealing data from vulnerable systems without authentication (by dumping SQL database contents) as well as planting malicious code, a detailed technical analysis by Huntress outlines:

Cross Site Scripting (XSS)

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious content.

XSS attacks can generally be categorized into two categories: stored and reflected. There is a third, much less well-known type of XSS attack called DOM Based XSS

How to Determine If You Are Vulnerable

XSS flaws can be difficult to identify and remove from a web application. The best way to find flaws is to perform a security review of the code and search for all places where input from an HTTP request could possibly make its way into the HTML output. Note that a variety of different HTML tags can be used to transmit a malicious JavaScript. Nessus, Nikto, and some other available tools can help scan a website for these flaws, but can only

scratch the surface. If one part of a website is vulnerable, there is a high likelihood that there are other problems as well.

How to Protect Yourself

XSS Using Script in Attributes

XSS Using Script Via Encoded URI Schemes

XSS Using Code Encoding

Attack Examples

Example 1: Cookie Grabber

Error Page Example

what I learned:-

1. Basics of EH
2. Basics of NW
3. Footprinting
4. Scanning
5. Phishing
6. Vulnerability Assessment
7. website Hacking
8. firewalls
9. system hacking
10. IOT & Cloud
11. virus & Trojans

TOP 20 NETWORK SCANNING TOOLS

1. SolarWinds Network Performance Monitor
2. Advanced IP Scanner
3. Acunetix
4. Paessler PRTG Network Monitor
5. OpenVAS
6. Intruder
7. Wireshark
8. Skyboxsecurity
9. Thousandeyes
10. Spiceworks IP Scanner
11. Angry IP Scanner
12. GFI LANGuard
13. Nagios
14. Capsa Free
15. Open NMS
16. Retina
17. Snort
18. NetworkMiner
19. Splunk
20. Icinga 2

a target during footprinting:

- Domain name
- Network blocks
- Network services and applications
- System architecture
- Intrusion detection system
- Authentication mechanisms
- Specific IP addresses
- Access control mechanisms
- Phone numbers
- Contact addresses

Some of the common tools used for footprinting and information gathering are as follows:

- Whois
- NSlookup
- Sam Spade
- SuperScan
- Nmap
- TcpView
- My ip Suite
- Dns enumerator
- Spider Foot
- Nessus
- Zone Transfer
- Port Scan
- HTTP Header Grabber
- Honeypot Detector

Top 10 Phishing Tools

Evilginx2
SEToolkit
HiddenEye
King-Phisher
Gophish
Wifiphisher
SocialFish
BlackEye

Shellphish

zphisher

Top 13 Vulnerability Scanner Tools

1. Qualys Vulnerability Management
2. AT&T Cybersecurity
3. Tenable Nessus
4. Alibaba Cloud Managed Security Service
5. Netsparker
6. Amazon Inspector
7. Burp Suite
8. Acunetix Vulnerability Scanner
9. Intruder
10. Metasploit
11. Nmap
12. IBM Security QRadar
13. Rapid7 InsightVM (Nexpose)

List of virus maker tools:

- DELmE's Batch Virus Generator

- JPS Virus Maker Tool

Thank You…