GYALPOZHING COLLEGE
OF
INFORMATION TECHNOLOGY

Assignment-II

WEB PROGRAMMING-ITW101

Submitted by:
Dorji Gyeltshen
12190049
Group A

Question1

What is Web Security?

Answer: Web Security is also known as “Cybersecurity”. It basically means protecting the websites or web application by detecting, preventing and responding to Cyber threats. Websites and web application are just prone to security breaches as physical homes, stores, government and locations.

Real time issues of web security are:

1. Injection flaws
2. Broken Authentication
3. Cross Site Scripting (XSS)
4. Insecure Direct Object References
5. Security wrong configuration
6. Sensitive data exposure
7. Missing function level access control
8. Cross site request forgery (CSRF)
9. Using components with known vulnerabilities
10. Invalidated redirects and forwards.

Question2

Aspect of data security: It keeps the sensitive data protected from unauthorized access.

A. Privacy: Branch of data security concerned with proper handling of data(consent, notice and obligations).

Real time issue: vulnerability to fake data generation, problem in protecting cryptography and probability of sensitive information.

Identification of personal information during transmission over the internet. E-banking and e-business portals have multiplies the risk associated with online privacy.

B. Integrity: The process of ensuring and preserving the validity and accuracy of data.

Real time issues: Software bugs, design flaws and human errors (sharing password, fabricating data, etc).

Cybercrime has emerged everywhere making the profitable business for criminals therefore, have to preserve validity through validate and verify all kind of data.

C. Authenticity: Quality of digital object being genuine without corrupted from the original.

Real time issue: Nowadays, most people are dealing with this problem by proposing solutions related to authentication especially in identification of the manipulated data.

Watermarking-based authentication helps in dealing with such issues.

Question3

Web security issues

1. Defacement: Is an attack in which malicious parties penetrate a website and replace content on the site with their own messages.

Real time issues: Unauthorized access, SQL injection and malware infection.

More access of your website leads to more chance for an attacker to do damage.

In 2018, the BBC reported that a website hosting data of patients by UK National health service was defaced by hackers with the defacement message “hacked by Anoa Ghost”

2. Phishing: Type of attack to steal user data, including login credentials and credit card numbers.

Real time issues: Malicious attachments, malicious web links and fraudulent data-entry. Increasingly sophisticated attacks in move from email to alternative attack vectors like social media and messaging. Google and Facebook got duped out of $100 million through email phishing scheme.

3. Privacy violation: Stealing and manipulating or mishandling of private information like passwords or security number which is often illegal.

Real time issues: Spying, snooping and mishandling of information. Millions of people were of victims of identity theft leading to legal and financial problems.

Causes of this issues are:

Unprotected storage of user data.

Misplaced trust and unsafe handling of sensitive information.

Display of sensitive data on end-device.