B.Sc. Engg. CSE 5th Semester **09 December 2023 (~~Morning~~)**

23

ISLAMIC UNIVERSITY OF TECHNOLOGY (IUT)

ORGANISATION OF ISLAMIC COOPERATION (OIC)

Department of Computer Science and Engineering (CSE)

SEMESTER FINAL EXAMINATION **WINTER SEMESTER, 2022-2023**
DURATION: 3 HOURS **FULL MARKS: 150**

CSE 4531: E-Commerce and Web Security

Programmable calculators are not allowed. Do not write anything on the question paper.
Answer **all 6 (six)** questions. Figures in the right margin indicate full marks of questions whereas corresponding CO and PO are written within parentheses. The symbols have their usual meanings.

1. a) Let's assume 'atiqBored.com' has path traversal vulnerability. Now if you search for this URL `https://atiqBored.com/loadImage?filename=218.png` it will execute this : `<img src="/loadImage?filename=218.png">` html tag and retrieve an image from the directory `./img/api/international/218.png`. 4 (CO3) (PO1)

   As an attacker, you have inside information that admin's credentials are in `./misc/cred/adm/pwd.txt` directory. Demonstrate the approach you can take to get the credentials of admin.

   b) Public key cryptography is more secure but computationally slower than symmetric key cryptography. However, the symmetric key must be sent to the recipient over insecure transmission. Propose a solution where you can get both faster computation than public key cryptography and more security than symmetric key cryptography. Describe each step of the solution by drawing a diagram depicting the entire process. 1 + 3 + 3 (CO2) (PO2)

   c) If an attacker searches for `https://shoeMaker.com/login/home.jsp?admin=true` instead of `https://shoeMaker.com/login/home.jsp?admin=false` the server of 'shoeMaker.com' will reply with the admin page. Define the type of server-side vulnerabilities the website has and determine which type of privilege escalation the attacker is going for. 2 × 2 (CO4) (PO2)

   d) Describe three approaches an attacker can take to exploit authentication vulnerabilities using brute force attacks. 6 (CO3) (PO1)

   e) Any user can put a comment like "This is a very helpful post" in scrollToKnow website. And scrollToKnow will save this comment in its database without checking if it is really a string or some malicious java script. Now an attacker have put a comment with some java script command under a post called "Beautiful Cats". Now whenever a user trying to open "Beautiful Cats" post he/she is seeing a prompt box, asking his/her password. Define the aforementioned attack and describe some preventive measures against it. 1 + 6 (CO4) (PO2)

2. a) WonderfulBakery.com has SQL injection vulnerability. If anyone searches for the URL '`https://WonderfulBakery.com/products?category=Vanilla`', the server will run the SQL command '`SELECT * FROM products WHERE category='Vanilla' AND released=1`'. This will show all the released products under the vanilla category. 4 × 2 (CO3) (PO1)

   Now, write the necessary SQL commands for the following URLs, along with the consequences:

   i. `https://WonderfulBakery.com/products?category=Vanilla'- -`

   ii. `https://WonderfulBakery.com/products?category=Vanilla'+OR+1=1- -`

   b) Write short notes on the following topics: 4 × 2 (CO1) (PO1)

   i. Keyword Advertising

   ii. Affiliate Marketing

c) Inexperienced developers might give access to the admin page if someone searches for the URL '`https://insecure-website.com/admin`'. The solution to this problem is to use an uncommon URL extension for the admin page URL. Explain how an application can still leak the admin page URL to users with a code example. 5 (CO4) (PO2)

3. a) Developers try their best to shield their websites from file upload vulnerabilities; however, there are some unforeseen circumstances that eventually make their websites vulnerable to file upload attacks. Describe those unforeseen circumstances. 4 (CO3) (PO1)

   b) Write short notes on the following topics: 4 × 2 (CO3) (PO1)
      i. Pivot Attack
      ii. REST API

   c) SHA-256 defines two functions σ_1 and Maj. Evaluate $\sigma_1(z)$ and $\text{Maj}(x, y, z)$ functions utilizing the following hexadecimal numbers: 9 + 4 (CO1) (PO1)
      - $x =$ DABBADAB
      - $y =$ BADDABAD
      - $z =$ DEADBEEF

4. a) While scrolling through 'scrollToKnow' (a new social media platform), you found a post discussing the ways to maintain a high CGPA. At the end of the post, you found a link to a website claiming to have more information on the same topic. Since you were interested, you clicked on that link, and some absurd-looking web page appeared with the heading "Hello darkness, my good old friend, I have come to talk with you again". You became so disturbed that you closed both the absurd web page and scrollToKnow. After several hours, you tried to log in to the srollToKnow website, but it showed that your credentials were incorrect despite of giving the correct credentials. 3 + 12+3 (CO4) (PO2)

   Considering the attack mentioned in the scenario, answer the following:
      i. Describe the conditions an attacker needs to maintain to initiate the attack.
      ii. Explain each of the steps taken by the intruder to deliver the attack and draw a diagram to depict the entire process.
      iii. Describe some common defenses that can be taken against the attack.

   b) Define Username Enumeration. Let's say an attacker is going to exploit a login page that is vulnerable to brute force attacks. Discuss three types of Username Enumeration to which the attacker should pay attention to. 1 + 6 (CO3) (PO1)

5. a) Selina was surfing the internet to download some free software called 'MagicOfMizu'. After downloading that free software, she found out that another program called 'atiqPopAds' automatically got installed which was very hard to remove. Define the aforementioned security threat and discuss its types. 6 (CO2) (PO2)

   b) Write six reasons for which consumers would choose the online channel. 6 (CO1) (PO1)

   c) Describe the process of online credit card transactions with an appropriate diagram. 6 (CO1) (PO1)

   d) 'ProteinShake.com' does not check what sort of parameter is going through its interface and finally to its server. Assuming the website uses `productId` and `storeId` parameters to locate a particular product from a specific store. Demonstrate the process an attacker can utilize to check the network configuration of the server that is running on the Linux operating system. 8 (CO4) (PO2)

6. a) 'BatteryHIGH Inc.' has three departments 'HR & Managers', 'Developers & Engineers', and 'Testers & Debuggers'. At present, the company has sufficient funding and connections. The employer recently wants to get into 'VR Technology' and has planned with the managers, chief developers, and engineers to analyze the feasibility of the idea. At last, they concluded that this is a promising idea since Bangladesh is rapidly developing in the domain of digital technology. It is not far that citizens will stop using our mobile phones or laptops and start using only VR to attend online classes, meetings, play games, and so on. They also discussed that their product will be free for the first three weeks, then they will charge their customers per hour. 10 (CO2) (PO2)

   Considering the scenario, identify the elements of the business model with appropriate justification.

   b) The owner of 'petAnimals.com' has found out his customers are unable to access the website. Upon investigation, the server team informed him that some sort of attack had been going on, resulting in the frozen state of the servers. Define the attack and describe some preventive measures against this sort of attack. $1+8$ (CO4) (PO2)

   c) Answer the followings: $3+3$ (CO1) (PO1)

      i. Write six key dimensions of E-commerce security.

      ii. Draw a diagram depicting vulnerable points in an E-commerce transaction.