UNIVERSITY OF GHANA

B.SC INFORMATION TECHNOLOGY, FIRST SEMESTER

EXAMINATIONS: 2016/2017

CSIT309: DATA NETWORK SECURITY I

INSRUCTIONS

*ANSWER **ALL** QUESTIONS IN **SECTION A***

*ANSWER **QUESTION ONE** AND ANY OTHER QUESTION IN **SECTION B***

TIME ALLOWED:

TWO AND A HALF (2½) HOURS

[50 MARKS TOTAL]

[SECTION A 30 MARKS]

1. Which of The following is correct about Open Web Application Security Project (OWASP)?

a. They are dedicated to finding and fighting the causes of insecure software
b. They are dedicated to allowing users to be the causes of insecure software
c. They are used to make businesses operate in and insecure environment
d. They are firewalls and intrusion detection systems to monitor traffic

1. The following are some of the myth that IT managers think: “Our site is safe” which one is wrong?

a. “We use network vulnerability assessments”

- This approach neglects the security of the software on the network or Web server

a. “We have firewalls in place”

- Port 80 & 443 are open for the right reasons

a. “We encrypt our data with SSL”

- This only protects data between site and user, not the Web application itself

a. “We have a policy in place”

- But we know our system can be vulnerable to threats and attack

1. The following are some of what can happen to the Web application security attacks and vulnerabilities?

a. Sensitive data leakage: Customer, partner, or company data
b. Identity theft: Hacker impersonates a trusted user
c. Application shutdown (site available), Access cannot cause major loses
d. Defacement: content modification, Hurts brand, misleads customers, and so on

1. Threats against Web applications (WASC) includes all the following apart from?

a. Authentication: Attacks that target a Web site's method of validating the identity of a user, service, or application
b. Authorization: Attacks that target a Web site's method of determining if a user, service, or

application has the necessary permissions to perform a requested action

c. Physical-side attacks: Attacks that abuse or exploit a Web site user's system

d. Command execution: Attacks designed to execute remote commands on the Web site

1. The following are some Computer Security Challenges that indicates Security is not simple besides?

a. Potential attacks on the security features need to be considered not often as an afterthought
b. Procedures used to provide particular services are often counter-intuitive
c. It is not necessary to decide where to use the various security mechanisms
d. Requires constant monitoring

1. Passive Attacks includes all except?

a. The release of message contents is a Passive Attacks
b. Goal of the Passive Attacks is not to obtain information that is being transmitted
c. Traffic analysis is a Passive Attacks
d. Passive Attacks are in the nature of eavesdropping on or monitoring of transmissions

1. The protection of traffic flow from analysis: This requires that an attacker will not be able to view all characteristics of the traffic on a communications facility apart from?

a. Observe the source and destination
b. Frequency of traffic
c. Series of the traffic
d. Length of traffic

1. The following explains Web site and Web application Components vulnerability apart from?

a. Web site provides access to static documents and user input does affects business functionality

b. Web site provides access to dynamic documents and user input does affects business functionality

c. Web application builds on a Website and takes user i put that affects back end business logic

d. The Web server typically interacts with other back end servers, such as an application server or a database server

1. The client tier side of Web Application Components vulnerability includes all except?

a. Client tier: Is the HTML side, A textual representation of a graphical page

b. Client tier: Consists of tags, attributes, and values

c. Most injection attacks involve breaking out of the current context and starting a new context

d. More common attacks may involve creating a sub-context with in the current context, or directly into the current context which is possible to stop

1. In the Client tier Scripting capabilities, A script has the following capabilities except?

a. Implement user interactions with the hackers

b. Interact seamlessly with the Website

c. Perform any action that is related to the Website

d. Launch signed and safe Active X controls

1. In the Client tier Scripting capabilities, same origin policy includes all except?

a. A script loaded from one origin can get or set properties of a document from a different origin

b. The term origin is defined using Domain name, Protocol and the Port as the values

c. Scripts can access other frames only from the same origin

d. Scripts can issue requests to documents from a different origin, but cannot view the corresponding responses

1. The Middle tier presentation components vulnerability in web applications includes all apart from?

a. Generates and presents Web pages via Web server such as Apache, IIS and so on

b. Generates and presents Web pages via Web server such as google chrome and so on

c. Middle tier presentation Can also generate “dynamic” content based on as Active Server Pages (ASP) and Java™ Server Pages (JSP) technology

d. Middle tier presentation Can be part of an “application server” implementation IBM® WebSphere® Application Server

1. The Data tier components vulnerability in web applications includes all apart from?

a. Data tier is Sometimes referred to as the “back end” tier

b. Data tier controls access to user and application specific data and corporate data

c. Data tier controls access to user and system specific data and corporate data

d. Data tier is usually based on Relational Database Management Systems (RDBMS) technology.

1. The most common example of an injection attack is “SQL injection” includes all except?

a. SQL Injection has been successfully exploited by hackers for well more than a decade

b. SQL injection involves an attacker appending SQL database commands within an input field.

c. If the web application code does not filter (sanitize) the input, SQL commands could be executed on the web server, allowing an attacker to bypass network DMZ security, and directly interrogate the back-end database.

d. With SQL injection, an attacker is not able to return and steal tables of information, make change store cords, or even delete the entire database.

1. In SQL injection flaws and Vulnerability, the following are correct apart from?

a. SQL (Structured Query Language) is a programming language for querying databases.

b. An attacker provides malicious data to your application and that data is concatenated to a (D B) query.

c. The implications includes Information leakage through DB error messages

d. Take complete control of your DB but does not allow insert data, delete tables.

1. The following explains HTTP: Hypertext Transfer Protocol apart from?

a. HTTP is a communications protocol used to transfer information on intranets and the World Wide Web

b. Versions:0.9,1.0,1.1

c. RFCs (request for comments): 1945,2068,2616

d. Describes the internet connection used by browsers and Web servers

1. The following are all HTTP request methods (basics) except?

a. GET: retrieve a document

b. HEAD: retrieve header information

c. POST: collects data from the server

d. PUT: DELETE: store an entity-body at the URL, and delete a URL

1. HTTP response codes includes all the following apart from?

a. 1XX: Informational. The client should cancel request.

b. 2XX: Successful. The client's request was successfully received, understood, and accepted.

c. 3XX: Redirection. Further action needs to be taken by the user agent in order to fulfill the request.

d. 4XX:Client Error.

1. The HTTP Client state management process includes all the following apart from?

a. HTTP is stateless: no continuity from one request to the next

b. Maintaining state is a responsibility of the Web Server

c. Session: putting individual user requests in context

d. Session management mechanisms Cookies and Get / Post query parameter

1. The following are the implications of Injection Flaws apart from?

a. Information leakage through DB error messages

b. Data extracted from your DB

c. Take complete control your DB (insert data, delete tables, and soon)

d. Execute commands on your browser

1. The following are ways of Fixing SQL Injection except?

a. Input validation as often as possible, only accept known good values, rather than sanitizing

b. Never use dynamic queries

c. Use parameterized query APIs: APIs encode the user input, and make sure that it doesn't break the SQL statements

d. Use encrypted procedures as they are generally safe from SQL Injection

1. In Broken authentication and session management, Session hijacking includes all except?

a. An attacker may seek to steal (hijack) a web session by learning a victim's secret session ID.

b. Knowing a user's session ID cannot allow an attacker to impersonate the user's authenticated connection with the web server, compromising the user account.

c. If the web app manages session ID's poorly, such as displaying a session ID within a URL instead of using a cookie, it can be a fairly simple for an attacker to obtain the session ID by tricking the user.

d. Even when web apps use cookies to store session IDs, attackers still seek to obtain session ID's directly from the user's locally stored cookie files, by tricking users into running covert scripts.

1. Broken authentication and session management, Session Fixation includes all except?

a. Session fixation is another type of attack that can be performed on the web server

b. The attacker accesses the target Web site and obtains the session ID

c. The attacker sometimes has to repeatedly access the site to keep the session alive

d. The attacker gets the victim to access the target Web site with the session id value

1. In Session Fixation, If session ID expiration on a Web site isn't timely, all the following may happen except?

a. It increases the chances for an attacker to perform a session prediction or session fixation attack by allowing them more time to guess a value or perform a brute force attack

b. It increases the number of concurrent open sessions, which increases the pool of numbers that a hacker can guess

c. In a shared work environment, you cannot access a Web site in another user's session

d. The browser's back button can be used to access previous pages accessed by the victim

1. In a Weak Session Management, credential or session prediction methods includes all apart from?

a. Web applications often use session management to track a user when communication is first established

b. Users does not have to prove their identity to the site with login credentials

c. A unique session id is then supplied to the user, rather than require the user to constantly log in

d. Subsequent communication between the user and the site is then tagged with the session id as proof of the authenticated session

1. In Weak Session Management, credential or session prediction vulnerability includes all apart from?

a. If an attacker can guess the value of the session ID, they can access the site as that user and impersonate them Attacker first accesses the application to determine the session ID and where it is stored

b. Attacker predicts the next session ID and switches the current session ID value and is logged in as the identity of the next user

c. This cannot be done by brute force as well

1. Fixing a weak authentication in broken authentication and session management includes all apart from?

a. Password strength: Restrict passwords to a minimum size and complexity

b. Password strength: Require a combination of alphabetic, numeric, or non-alphanumeric characters

c. Password storage and protection: Should not be stored as a hash or encrypted value with decryption keys strongly protected

d. Password storage and protection: The entire login transaction should be sent through SSL

1. Fixing a weak authentication in broken authentication and session management includes all apart from?

a. Password use: Restrict to a defined number of login attempts (for example, three)

b. Password use: Keep a log of any failed attempts, log the actual password

c. Password use: Provide a generic error message for a failed log in attempts

d. Password use: Do not allow a user to use previous passwords

1. Preventing Session Hijacking in broken authentication and session management includes

all apart from?

a. Do not combine the source IP address of the user with the session ID

b. Ensure user re-authentication before allowing any changes to key account details, such as changes to passwords and email addresses.

c. Changes to Passwords and personal details are a common first action by hackers upon hijacking a web session

d. Forcing re-authentication terminates the hijacked session a simple coding technique to reduce risk.

1. Fixing weak session management in broken authentication and session management includes all apart from?

a. Permanent cookies should be used to store session values

b. Session ID should be protected via SSL so that the value can’t be stolen over the network

c. Session ID should be long, complicated, random numbers that cannot be guessed

d. Session ID should be set to expire after a certain period of time, and expire after logging out

[SECTION B]

ANSWER QUESTION ONE <u>COMPULSERY</u> AND ANY OTHER QUESTION FOR 10 MARKS EACH

[20 MARKS TOTAL]

1. With the aid of a diagram, explain the vulnerabilities that may exist on the Web application components from Client Tier, Middle tier and the Data tier? [6Marks]

B. Define HTTP and explain the following HTTP request methods? [4 Marks]

1. With the aid of a diagram explain why it is essential to incorporate security in Security in the software development lifecycle SDLC? [5 Marks]

B. Explain the following HTTP response codes? [5 Marks]

1. With examples explain the concepts of Injection Flaws attacks and how it can be initiated by a hacker [2 Marks].

B. Explain SQL Injection vulnerabilities and its implications when initiated by a hacker? [4 Marks]

B. Conduct a SQL Injection attack from a hacker's point of view. Include the codes used to carry out the exploits? Using AturoMutual.com Online Banking as the interface? [4 Marks]

1. With the aid of a diagram and examples explain Cross-site Scripting (XSS), its implications and how to prevent XSS attacks and exploits? [5 Marks]

B. Conduct an XSS attack methods from a hacker's point of view using the GET, POST strings AltoroMutual.com online Interface? [5 Marks]