Sri Lanka Institute of Information Technology

B.Sc. Special Honours Degree
in
Information Technology
(Software Engineering)

Regular Examination
Year 4, Semester 2 (2018)

SE4030 - Secure Software Development

Duration: 3 Hours

October 2018

Instructions to candidate:

- This paper has 5 questions.
- Answer all questions.
- Marks for each question are given.
- Total mark is 100.
- This paper contains 6 pages including cover page.

Question 1 (20 marks)

a) A software development organization follows the waterfall method in the development process. In each phase of the SDLC, it is important to verify the security for developing vulnerability free software. **List** one recommendation for each phase for integration security into the SDLC.

(5 marks)

b) In a product based software development organization, there are different teams developing the software products and there is a security team to manage the overall security of all the products. When a security vulnerability is reported on a product, the security team might not be able to identify the root cause as they are not aware of the implementation of the product. The product developers also would fail due to the lack of knowledge in security domain. **What** do you propose to address this gap? Briefly **explain**.

(3 marks)

c) "Using components with known vulnerabilities" is included in OWASP Top 10 list of web application security vulnerabilities. If your web application uses such components which are having reported security vulnerabilities, **list** 3 approaches you could follow for eliminating the impact of the vulnerabilities.

(4 marks)

d) **List** the message flow in two-way SSL (mutual SSL) handshake where the client is the browser and the server is Apache tomcat server.

(5 marks)

e) **List** 3 security analysis techniques you could use for identifying security vulnerabilities in web applications.

(3 marks)

Question 2 (20 marks)

a) **What** is the root cause for SQL Injection vulnerability in websites?

(2 marks)

b) **How** to prevent SQL Injection, when comes to writing secure code?

(1 mark)

c) A website is vulnerable to SQL Injection. In the website, it has the search textbox where you can enter a name of a product and the website will display the matching results in tabular manner as following.

Price List

ID	Name	Price
1	USB	35.50
2	Micro USB Cambe	10.23

The SQL query it runs for finding the products is given below.

```
SELECT id, name, price FROM product WHERE name like '%USB%'
```

Note that in above query, % mark is added by code and USB is the user input of the search text box. You have discovered that the table for storing users has the schema user [userid int, username varchar(20), password varchar(20)].

Write a UNION based SQL Injection for retrieving the userid, usrename and password values through the products search page.

Hint: For commenting a SQL command from a given point, # can be used. For concatenating multiple column values, SELECT CONCAT (column1, column2, ...) can be used.

(5 marks)

d) In addition to UNION based SQL Injection, **list** two other types of SQL Injection attacks.

(2 marks)

e) **What** is Cross-Site Scripting (XSS)?

(1 mark)

f) **What** are the two main types of XSS vulnerability?

(2 marks)

g) **What** is the root cause for XSS? **What** are the two main ways for fixing XSS vulnerability in websites in terms of the inputs to the website and outputs from the website?

(2 marks)

h) Read the following scenario and answer the questions.
An attacker found a XSS vulnerability in a website.

Attacker could directly inject the following payload in a query parameter in a URL of the website and the XSS was successful.

```
<script>alert(1);</script>
```

Attacker also found out that the session cookie (and other cookies) used by the website are not protected.

i. **Write** the javascript payload that the attacker could use to steal the cookies from an enduser. Attacker has the URL http://attacker.com/receiver?data=XXXX available in his website that receives the query parameter 'data' where the value is saved in a log file.

Hint: In javascript, document.cookie can be used to retrieve the cookies as a string. Assigning a URL to window.location.href would result the browser in getting redirected to the given URL.

(2 Marks)

ii. In the same website that is vulnerable to XSS, there is a textbox where the end users can provide a URL (of an image) as the value. The HTML page source of the resulting page is as following where the src attribute would have the given URL.

```
<img src="XXXXXX" alt="Smiley face" height="42" width="42">
```

Provide the string that you would enter in the textbox for successfully popping up a javascript alert with the message 'Hello'.

(1 mark)

iii. In the above scenario where the payload is getting added to the img tag, if the server side code is written in Java, the OWASP Java Encoder can be used for converting user input into HTML safe content. This Java library provides various different methods like forHtml(String), forJavaScript(String), forJavaScriptAttribute(String) etc. **What** would be the suitable method to be used in this scenario?

(2 marks)

Question 3 (20 marks)

a) Cross Site Request Forgery (CSRF) was a Top 10 vulnerability in OWASP 2013 list. Briefly **explain** what CSRF is.

(2 marks)

b) As per OWASP recommendation, **list** two security patterns which you can follow for implementing CSRF protection in a website.

(2 marks)

c) Using a diagram, **show** the message/activity flow of **one** security pattern which you listed above, when making a HTTP POST request from browser to web server. Clearly **show** how the CSRF token is included in the request.

(5 marks)

d) If an attacker hosts a website (eg: attacker.com) that sends the same HTTP POST request where the legitimate web page sends for a particular operation, the attacker's HTTP request would fail to bypass the CSRF protection if the website is protected against CSRF. **Explain** why the attacker's request would fail when using each security pattern you listed above?

(3 marks)

e) **List** the two standard flags that can be set in HTTP cookies for protecting the cookies getting exposed to attackers. Briefly **explain** the usage of each flag.

(5 marks)

f) For preventing CSRF, we can use the samesite flag in HTTP session cookies. Although this is not a standard yet, modern browsers already support this flag. This flag can have two values as lax or strict. Briefly explain how CSRF is prevented in the two scenarios where the session cookie has samesite=lax and samesite=strict.

(3 marks)

Question 4 (20 marks)

a) **Explain** the anatomy of a JSON Web Token (JWT).

(3 marks)

b) Briefly **explain** what OpenID Connect (OIDC) protocol is and its usage.

(3 marks)

c) When comparing OAuth access tokens with the id_token in OIDC, **what** is the difference?

(2 marks)

d) An API Management solution uses JSON Web Tokens for authenticating/authorizing the API requests. When a JWT is presented to the resource server, it can validate the signature of the JWT for verifying the authenticity of it. Briefly **explain** how the signature of the JWT is generated and also **how** the signature could be verified.

(8 marks)

e) An OAuth resource server uses JWT for authenticating/authorizing API requests. In a situation where a JWT issued to a client gets exposed to an attacker, **how** can you implement revoking the JWT? Briefly **explain** the functionality you would implement in the authorization server and also in the resource server. For uniquely identifying each JWT, **which** parameter would you use in the body of the JWT?

(4 marks)

Question 5 (20 marks)

a) OAuth 2.0 framework facilitates delegated authorization for 3rd party applications. **List** the 4 main grant types defined in the OAuth 2.0 specification and briefly **explain** in which scenario the particular grant type should be used.

(6 marks)

b) An OAuth client application possesses an access token which is obtained from the authorization server. It presents the token to the resource server and requests for user's profile information. The resource server needs to validate the token for deciding whether to return user profile details to the client. **Explain** how the resource server can validate the access token in this scenario. In OAuth terminology, **what** is the term used to represent this process.

(4 marks)

c) Briefly **explain** the usage of OAuth Token Revocation.

(2 marks)

d) Tickets.LK is a local website that facilitates social login where users can login to the website with their facebook account. It uses OAuth 2.0 to achieve this functionality. First, the website obtains an OAuth access token and then presents it to facebook and obtain the authenticated user's profile information to identify the user. Using a diagram, **show** the message flow in this scenario. Clearly **mention** the OAuth roles and endpoints in the diagram. (Note!: It is **not required** to list the parameters in each HTTP request).

(8 marks)

-- End of the Question Paper --