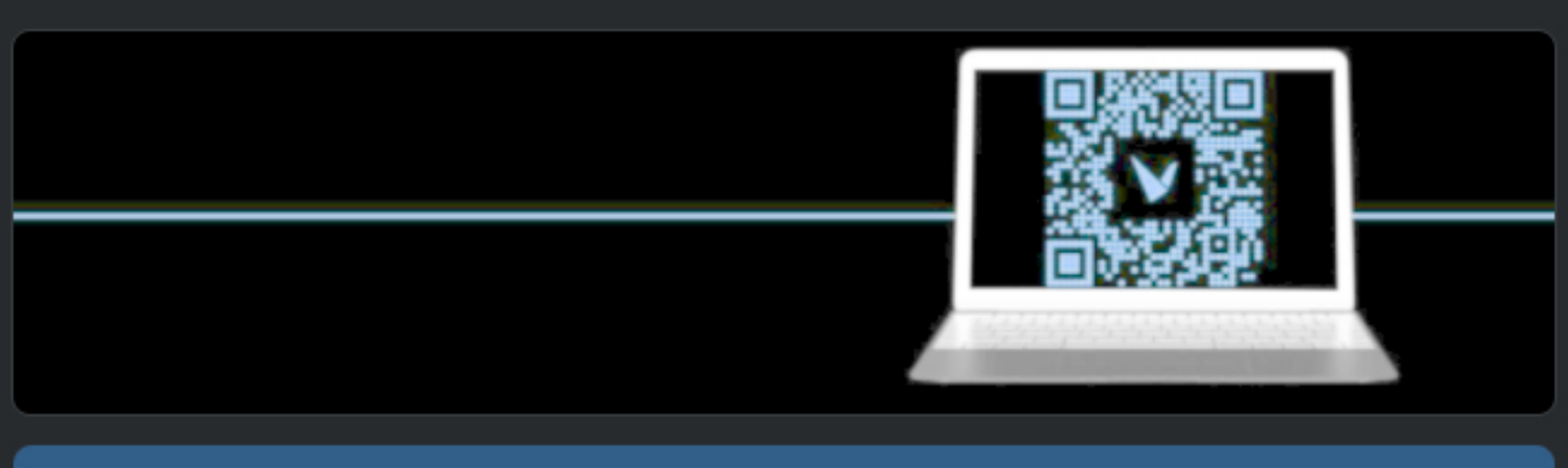

Week 6 - Assignment Submission Form

atharvajagdale45@gmail.com Switch account

Draft saved

* Required

Week 6 Assessment

KYC - Know Your Content for the week. This week's topic - **Cross Site Request Forgery (CSRF)** !

All the Best !

Which of the following is not a tool for generating CSRF Proof of Concept. *

- (●) Sea Surfer
- ( ) CSRF PoC Generator
- ( ) Malidate
- ( ) All of the Above

To prevent CSRF attacks which of the following frameworks have a built-in support. *

- ( ) Joomla
- ( ) Struts
- (●) Laravel
- ( ) Both A and B

Choose the Correct Sequence of steps to be performed for solving the lab Eassyy CSRF: *

(i) Create Two accounts.
(ii) Victim Clicks on the click CSRF attack successful.
(iii) Generate a CSRF PoC.
(iv) Login into the Account and Click on Change Password.
(v) Send the CSRF PoC it to the victim.
(vi) Capture the Request into Burp Suite and right click and select Engagement Tools.
(vii) Victim Clicks on the click CSRF attack successful.

- ( ) (ii), (vi), (iv), (iii), (vii), (i), (v)
- ( ) (ii), (v), (vii), (iii), (iv), (i), (vi)
- (●) (i), (iv), (vi), (iii), (v), (vii), (ii)
- ( ) (i), (iv), (iii), (iv), (v), (vii), (ii)

CSRFProtector Project is used to protect against CSRF attacks against which of the following programming language? *

- ( ) Python
- (●) PHP
- ( ) Java
- ( ) Ruby

Identify the XSS payload used for stealing the session id and the cookies to perform a CSRF attack in lab XSS the Savior! *

- ( ) <script>alert(document.id))</script>
- (●) <script>alert(document.cookie)</script>
- ( ) <script>alert(document.token)</script>
- ( ) None of the Above

Web applications are vulnerable to CSRF attacks when their request method is changed from ______ to ______ and vice versa. *

- (●) GET, POST
- ( ) STORE, RETRIEVE
- ( ) GET, DISPLAY
- ( ) POST, PATCH

CSRF is also known as ________ *

- ( ) SSRF
- ( ) RSRF
- ( ) RCE
- (●) XSRF

CSRF attack means *

- ( ) Attack that can abuse functionality on server to read and update internal resources
- ( ) Attack in which malicious scripts are injected into websites
- ( ) Attacker can remotely execute commands on someone else devices
- (●) Attacks that tricks victim into submitting a malicious request

Some web applications check CSRF Tokens based on ________ length. *

- (●) Request
- ( ) Response
- ( ) Entropy
- ( ) Access

Sometimes removing the ________ parameter from the PoC, can give you a valid CSRF. *

- (●) request
- ( ) token
- ( ) cookies
- ( ) url

If a website is vulnerable to CSRF we can change the Email ID and/or password of the user thus performing a ___________ of the user. *

- ( ) Deleting folders on PC
- (●) Account Take Over
- ( ) SQL injection on browser
- ( ) All of the above

Which of the following tips would help you to solve and perform a CSRF attack on lab rm -rf token *

- ( ) Delete the CSRF token completely
- ( ) Using the Same CSRF token for changing other users Passwords also.
- (●) Both A and B
- ( ) None of the Above

A same-site Cookie is a Cookie which can only be sent, if the request is being made from the ___________ that is related to the Cookie being sent. *

- ( ) Arbitary origin
- ( ) Null origin
- (●) Same origin
- ( ) Cloudfare origin

In a CSRF for a victim it is impossible for a victim to distinguish a legitimate request from a forged one. *

- ( ) TRUE
- (●) FALSE

To remediate CSRF a token that is associated to a particular user can be found as hidden value in evey state changing form present in web application such tokens are called as ________ *

- ( ) Synchronizer Token
- ( ) SSRF Token
- ( ) Session IDs
- (●) Both A and B

________ are intrinsically vulnerable to CSRF because they are automatically sent with each request. *

- ( ) JWT tokens
- ( ) Session IDs
- ( ) Request
- (●) Cookies

A simple payload of getting the _______ using XSS and passing the _________ to CSRF PoC *

- ( ) cookie, cookie
- ( ) cookie, token
- ( ) token, cookie
- (●) token, Session Ids

If a victim with administrative account is compromised through a CSRF attack the entire web application can be compromised. *

- (●) TRUE
- ( ) FALSE

Which of the following sensitive data can be changed through a successful CSRF? *

- ( ) Email id
- ( ) Pssword
- ( ) Username
- (●) All of the Above

What does CSRF stands for ________ *

- ( ) Cross Server Request Forgery
- (●) Cross Site Request Forgery
- ( ) Cross Server Response Forgery
- ( ) Cross Site Reader Forgery

Microsoft refers CSRF attacks as a _________ attack in their threat modelling process. *

- ( ) Hybrid
- ( ) XML-based
- ( ) Double-click
- (●) One-Click

Severity of CSRF attacks varies from ____ to _______ depending on what action is being performed. *

- ( ) P4, P5
- (●) P2, P3
- ( ) P3, P4
- ( ) P2, P4

With a little help of ______________ an attacker may trick the users of a web application into executing actions of the attacker's choosing. *

- ( ) Tampering URL
- (●) Social engineering
- ( ) Executing commands
- ( ) None of the Above

The forged request sent by an attacker to the victim seems to be ___________ request. *

- (●) illegitimate
- ( ) invalid
- ( ) legitimate
- ( ) illegal

Choose the following options to prevent CSRF attacks. *

- [x] Anti-CSRF Token
- [ ] Sanitize the User inputs
- [x] Use the SameSite Flag in Cookies
- [ ] Monitor the server logs

For a CSRF attack to be successful which of the following steps are mandatory. *

- ( ) Inject malicious code into the database.
- ( ) Send Poc (malicious link) to the victim.
- ( ) Victim to interact with the link sent by the attacker.
- (●) Both B and C

Which of the following is the correct sequential order tasks should be performed to achieve a successful CSRF attack on lab Always Validate Tokens. *

(i) Create two accounts. (Attacker and a Victim Account)
(ii) First Login in to attacker account and click on Change the Password.
(iii) Victim's Password changed so CSRF attack was successful.
(iv) Login into Victims Account and now open the CSRF PoC generated onto the browser and Click Submit.
(v) Generate the CSRF PoC for the attacker change password request.
(vi) Capture the request into the Burp Suite identify the CSRF token in the Request.
(vii) Send the request to the repeater tab modify the value of CSRF token to any random value.

- ( ) (vi), (iii), (i), (vii), (iv), (v), (ii)
- ( ) (i), (ii), (iii), (iv), (v), (vii), (vii)
- ( ) (i), (ii), (vii), (vi), (iv), (v), (iii)
- (●) (i), (ii), (vi), (vii), (v), (iv), (iii)

Which of the following approach would you follow to solve the lab GET me or POST me *

- ( ) Modify the value of the CSRF token
- (●) Change the Request method from POST to GET
- ( ) Change the Request method from POST to PATCH
- ( ) Delete the CSRF token from the Request

Which of the following victim's details would be gained by an attacker through a successful CSRF attack? *

- ( ) Victim's email address, passwords
- ( ) Server Configurations
- ( ) Fund Transfers
- (●) Both A and C

Which of the following tips would help you to solve and perform a CSRF attack on lab I hate when someone uses my tokens! *

- ( ) Delete the CSRF token from the Request
- ( ) Modify the value of the CSRF token
- ( ) Using the Same CSRF token for changing other users Passwords also.
- (●) Both B and C

A copy of your responses will be emailed to the address you provided.

Back | Submit | Clear form