✓ The following attack can execute scripts in the user's browser and is capable of hijacking user sessions, or redirecting the user to malicious sites? * 1/1

- ○ SQLi
- ◉ XSS ✓
- ○ Open Redirect
- ○ CSRF

✓ IDOR + MFLAC combined together in OWASP 2017 represents * 1/1

- ○ Broken Authentication
- ◉ Broken Access Control ✓
- ○ Security Misconfiguration
- ○ Insufficient Logging and Monitoring

✓ The history of requests can be viewed in * 1/1

- ○ Intercept
- ◉ HTTP History ✓
- ○ Repeater

Intruder

✓ Which tab allows you to decode a string * 1/1

- (●) Decoder ✓
- ( ) Repeater
- ( ) Intruder
- ( ) All of the above

✓ What is the use of Throttle in Burp Suite Intruder tab * 1/1

- (●) Tells Burp Intruder to stop the amount of time between two requests ✓
- ( ) Tells Burp Intruder to send the amount of requests given in 1 millisecond
- ( ) All of the above
- ( ) None of the above

✓ What is Phishing? * 1/1

- ( ) Data Transfer Protocol
- (●) Email Scam ✓
- ( ) Network Scandal
- ( ) Cross Domain Scandal

✓ Which of the following feature is present in Burp Suite Pro but not in Burp Suite Community * 1/1

- ○ Burp Collaborator
- ○ Generate CSRF PoC
- ○ Throttle
- ◉ All of the above ✓

✓ The following statement is false about request manipulation in Burp Suite * 1/1

- ○ Burp Comparer is used to identify the difference between two responses of applications quickly in the context of applications on the web.
- ◉ The Decoder tool is used to identify the differences between failed log in responses using invalid and valid usernames. ✓
- ○ Burp Repeater is used for manually reissuing and modifying individual requests of HTTP.
- ○ Burp proxy is an HTTP/S interactive proxy server for testing and attacking applications on the web.

✓ Which of the following tab is used to compare two requests in Burp Suite * 1/1

- (●) Comparer ✓
- ( ) Collaborator
- ( ) Comparers
- ( ) Sequencer

✓ Burp Spider is replaced by _____ in the newest version of Burp Suite * 1/1

- (●) Burp Crawler ✓
- ( ) Burp Spider Pro
- ( ) Burp Spider++
- ( ) Burp Crawler++

✓ The following is true about Cluster Bomb attack * 1/1

- ( ) It uses multiple payload sets
- ( ) The total number of requests generated by the attack is the product of the number of payloads
- (●) Both A and B ✓

None of the above

✓ Which of the following is/are true about XSS with Burp-Repeater tool? * 1/1

- This tool checks the cross site scripting vulnerability.
- This tool uses a java script syntax like code to check the vulnerability.
- It is used for authentication of the web applications.
- (●) Both A and B ✓

✓ The vulnerability produced when authorization of user for direct reference to restricted data is not validated is? * 1/1

- SQLi
- XSS
- (●) IDOR ✓
- All of the above

✓ example.com changes connection from HTTP to HTTPS. Assume session identifier is not being changed what flaw arises? * 1/1

- (●) Session Replay ✓
- XSS
- Session Hijacking

- [ ] CSRF

✓ Which of the following breaks the trust that a site has in user's browser * 1/1

- [ ] Session Hijacking
- [x] CSRF ✓
- [ ] SQL Injection
- [ ] XSS

✓ Which of the following options provides you with a server? * 1/1

- [ ] Burp Repeater
- [ ] Burp Server
- [x] Burp Collaborator ✓
- [ ] Both B and C

✓ The Action in Intercept tab of Burp Suite is used for * 1/1

- [ ] Abandon the message so that it is not forwarded.
- [ ] Review and edit the message to send the message on to the server or browser.
- [x] Shows a menu of available actions that can be performed ✓
- [ ] Used to check proxy history

✓ What are the resolution steps when Burp does not intercept HTTPS requests? * 1/1

- (●) To check the browser configuration. ✓
- ( ) To install Burp's CA certificate in your browser.
- ( ) To request additional memory for Burp by starting Burp from the command line using the -Xmx argument.
- ( ) Both A and B

✓ Burp Suite is an integrated platform for attack 1/1

- ( ) Client
- ( ) Server
- ( ) Browser
- (●) Web Application ✓

✓ The attack in which web sites are exploited by altering backend database queries through inputting manipulated queries? * 1/1

- ( ) LDAP Injection
- (●) SQL Injection ✓

- XML Injection
- OS Commanding

✓ The role of "Do intercept" is * 1/1

- (●) Responsible for the interception of the request. ✓
- ( ) Allows to quickly add an interception rule to prevent future interception of messages.
- ( ) Displays the HTTP status code of the current request.
- ( ) None of the above

✓ The vulnerability when untrusted user-entered data is entered is * 1/1

- ( ) IDOR
- (●) Injection ✓
- ( ) CSRF
- ( ) Insufficient Transport layer protection

✓ Which of the following can lead to exposure of sensitive data? * 1/1

- ( ) Session Fixation
- (●) Improper Authentication ✓
- ( ) Insecure Cryptographic Storage

- Unvalidated redirects and forwards

✓ Which of the following is used for web application mapping * 1/1

- Proxy
- Spider ✓
- Scanner
- All of the above

✓ Network permissions should be established so that users can accomplish their tasks, but cannot access any system resources that are not necessary so that: * 1/1

- A hacker cannot steal a legitimate user's identity
- Users will not have access to and misuse system resources
- Only the resources authorized for that user will be at risk ✓
- Hackers will not pose as legitimate users

✓ CORS comes under which category * 1/1

- Broken Access Control
- Broken Authentication
- Security Misconfiguration ✓

Insufficient Logging and Monitoring

✓ Which vulnerability is prevented by Role-Based Access Control * 1/1

- (●) Failure to restrict URL Access ✓
- ( ) Unvalidated Redirect or Forward
- ( ) Security Misconfiguration
- ( ) Insufficient Transport Layer Protection

✓ The following vulnerability was added in OWASP 2017 * 1/1

- (●) XXE ✓
- ( ) XSS
- ( ) CSRF
- ( ) MFLAC

✓ OTP Bypass, Captcha Bypass, 2FA Bypass, Common Password brute force are examples of * 1/1

- (●) Broken Authentication ✓
- ( ) Broken Access Control
- ( ) Using Components with known vulnerability

- ( ) Security Misconfiguration

✓ Cookie can be defined as * 1/1

- ( ) Computer Virus
- ( ) Web Application file
- (•) A file that makes it easier to access a Web site and browse ✓
- ( ) A file that hackers use to steal your identity

✓ In this attack a user's session credential or session ID is forced to an explicit value. * 1/1

- (•) Session Fixation ✓
- ( ) Session Hijacking
- ( ) Brute Force Attack
- ( ) Dictionary Attack

✓ What does OWASP stand for? * 1/1

- ( ) Open Web Application Secure Penetration
- ( ) Operational Web Application Secure Project
- (•) Open Web Application Security Project ✓

- ( ) Open Web Assessment Security Project

✓ Which of the following is/are applicable about extending Burp proxy? * 1/1

- ( ) It is used to modify the http request easily.
- ( ) It is better to use in case of web application hacking.
- ( ) For testing multiple extension.
- (•) All of the above ✓

✓ The following vulnerability was removed from OWASP 2013 * 1/1

- (•) Unvalidated redirects and forwards ✓
- ( ) CSRF
- ( ) XXE
- ( ) XSS

✓ Which of the following is/are applicable for 'NoClassDefFoundError' in troubleshooting? * 1/1

- ( ) This may be the problem related to the location of the jar file.
- ( ) To resolve this, it is necessary to run the command java-version and confirm that the version being executed is 1.6 or later.
- (•) All of the above ✓

None of the above

✓ The role of Burp Suite proxy in handing request in web application is ? * 1/1

- Manages the configuration of the application.
- Uses 8080 port by default for handling web apps.
- User need to log into the Burp Suite for the responses and requests that pass through each of the proxies.
- (●) All of the above ✓

✓ The Forward button in Intercept tab of Burp Suite is used to * 1/1

- (●) Edit the message. ✓
- Shows a menu of available actions that can be performed on the currently displayed message
- Used to add a comment to interesting items, to easily identify them later.
- None of the above

✓ You receive an e-mail from evil.com saying that you have won a contest. What should you do? * 1/1

- Claim the prize by providing all the information
- (●) Contact administrator for assistance ✓

- Forward the email to others
- Answer the email to call you back

✓ XXE can be prevented by * 1/1

- Filter Inputs and sanitize them
- Disable DTD ✓
- Apply Rate limiting
- All of the Above

✓ Burp Suite has the wonderful feature to add add-ons. This can be done by * 1/1

- Burp Project Options
- Burp Extender ✓
- Burp User Options
- Burp Logger

✓ What is the role of sequencer in request manipulation in Burp Suite? * 1/1

- This tool is a better choice for application security.
- It defines the application's status in terms of sessions.
- It maintains the application performance for virus security.

- [x] Both A and B ✓

✓ What are not the tasks related to Burp Proxy for intercepting and manipulating the request? * 1/1

- [ ] Intercept and modify all HTTP/S traffic passing in both directions.
- [ ] This tool manage the content and serialization of request.
- [ ] Burp proxy is used to test manually the requests and responses.
- [x] None of the above ✓

✓ If an attacker finds a Zero Day exploit of a vulnerable software which category will it come in * 1/1

- [ ] Insufficient Logging and Monitoring
- [x] Using Component with known Vulnerabilities ✓
- [ ] Security Misconfiguration
- [ ] Sensitive Data Exposure

✓ When HTTP cookies with tokens are not flagged as secured the threat that arises is * 1/1

- [x] Session Hijacking ✓
- [ ] Insecure Cryptographic Storage

- Access Control Violation
- Session Replay

✓ When the web application has poor randomness of session tokens than the flow that happens is * 1/1

- Insecure Direct Object References
- Session Replay
- Session Fixation
- Session Hijacking ✓

✓ The Comment field control in Intercept tab of Burp Suite is used to * 1/1

- Edit the message.
- Shows a menu of available actions that can be performed on the currently displayed message
- Used to add a comment to interesting items, to easily identify them later. ✓
- Both A and C

✓ Which of the following is a tool for mapping web applications and uses various intelligent techniques? 1/1

- Burp Spider ✓
- Burp Intruder

- Burp Repeater
- Burp Proxy

✓ When a browser does not check for proper validations and escaping the attack performed is * 1/1

- (●) Cross Site Scripting ✓
- ( ) Cross Site Request Forgery
- ( ) XML External Entities
- ( ) Sensitive Data Exposure

✓ Following is an example of Sensitive Data exposure * 1/1

- ( ) Github Tokens and API Keys
- ( ) Sensitive Invoices Indexed by Google
- ( ) Internal Jira Dashboards
- (●) All of the Above ✓

✓ Which of the following is/are correct about Burp suite walkthrough step in web application? * 1/1

- ( ) It is used to test the web application.
- ( ) It is used to intercepting and modification of the request.
- ( ) It is used to check the session token management for the users

It is used to check the session token management for the users.

- [x] All of the above

This form was created inside of VT.