Week 10 Assessment 20 of 20 points

KYC - Know Your Content for the week. This week's topic -**Capture The Flag** !

All the Best !

✓ Which of the following attack vector is involved in first section of the Capture the Flag? * 1/1

- ○ Cross-Site Scripting
- ◉ SQL Injection ✓
- ○ Insecure Direct Object Reference
- ○ Cross Site Request Forgery

✓ Identify the payload or the step to solve the first attack vector of Capture the Flag? * 1/1

- ○ "/><img scr=x onload=confirm(1) >
- ○ Delete the CSRF tokens to assure success
- ○ Change the values of id parameter
- ◉ ") || (1")=("1 ✓

✓ Which of the following attack vector help you to solve the second section to achieve the flag? * 1/1

- ◉ SSRF ✓
- ○ Open Redirect

- [ ] CORS
- [ ] Cross Site Scripting

✓ Choose the correct payload which helped you to capture the flag? * 1/1

- [ ] Redirect the URL parameter to evil.com
- [x] http://[::]:8000 ✓
- [ ] "/><h1>Flag Captured</h1>
- [ ] 1" or "1"="1

✓ Which of the following port helped you to gain the flag? * 1/1

- [ ] 441
- [ ] 80
- [x] 8000 ✓
- [ ] 5000

✓ Which of the following two attack vectors solved the CTF? * 1/1

- [ ] SQLI,CSRF
- [ ] XSS, Open Redirect
- [ ] CORS, HTML Injection

SQLI,SSRF ✓

✓ Which of the following injection attacks leads a malicious user for retrieving information by querying the SQL databases. * 1/1

- ○ LDAP Injection
- ◉ SQL Injection ✓
- ○ HTML Injection
- ○ Command Injection

✓ In SSRF attack, the attacker might cause the server to make a connection to _____ services of the organization's infrastructure * 1/1

- ◉ Internal ✓
- ○ External
- ○ Public
- ○ None of the Above

✓ For identifying SQL Injection and SSRF based vulnerabilities onto a web application which of the following is a important entity? * 1/1

- ○ URLs
- ○ Response

- ( ) Request
- (•) Parameters ✓

✓ SQL Injection and OS command injection when performed combinedly the resultant attack is called as _____. * 1/1

- ( ) Cross-Site Scripting
- (•) Accellion Attack ✓
- ( ) HTML Injection
- ( ) Server Side Request Forgery

✓ _____ attack is used target internal systems behind the Web Application Firewall, that are unreachable to an attacker from the external network. * 1/1

- ( ) CSRF
- ( ) XSS
- ( ) SSRF
- (•) Open Redirect ✓

✓ What does the batch command in sqlmap mean? * 1/1

- ( ) Identifies the version of database
- (•) It answers YES to all questions ✓

- [ ] It answers YES to all questions
- [ ] Identifies Tables
- [ ] Identifies Databases

✓ In some exceptional cases the SSRF based vulnerabilities can also lead to which of the following vulnerability. * 1/1

- [ ] LDAP Injection
- [ ] SQL Injection
- [x] Remote Code Execution ✓
- [ ] All of the Above

✓ The impact of the SQL Injections can be escalated to compromise the underlying server and can also perform which of the following attack ? * 1/1

- [ ] SSRF attack
- [x] Denial of Service ✓
- [ ] Phishing Attack
- [ ] None of the Above

✓ What are the possible ways to prevent SSRF attack? * 1/1

- [ ] Disable all user inputs
- [ ] Enable Authentication on all Services
- [ ] Whitelist Domain in DNS

Both B and C ✓

✓ Select the custom injection marker to point each potential vulnerable parameter while using sqlmap. * 1/1

- (•) * ✓
- ( ) /
- ( ) ;
- ( ) :

✓ Which of the following is a Time-Based SQL Injection attack? * 1/1

- ( ) Error-Based SQL Injection
- (•) Blind SQL Injection ✓
- ( ) Union-Based SQL Injection
- ( ) All of the Above

✓ Which of the following is used to along with the technique of filtering the inputs to prevent and mitigate SQL Injection attack? * 1/1

- ( ) Web Server
- ( ) Load Balancers

- [x] Web Application Firewall (WAF)
- [ ] All of the above

✓ Select the alternatives of Burp Collaborator used for exploiting SSRF vulnerabilities. * 1/1

- [ ] Requestcatcher.com
- [ ] Tinyurl.com
- [ ] Webhook.site
- [x] Both A and C

✓ Which of the following special character is used to indicate a URL fragment while performing SSRF Attacks with white list based input filters? * 1/1

- [x] #
- [ ] @
- [ ] *
- [ ] &