



## Week 10 - Assignment Submission Form

atharvajagdale45@gmail.com [Switch account](#)

Draft saved

### Week 10 Assessment

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

Which of the following is a Time-Based SQL Injection attack?

- ☐ Error-Based SQL Injection
- ☒ Blind SQL Injection
- ☐ Union-Based SQL Injection
- ☐ All of the Above

[Clear selection](#)

Select the custom injection marker to point each potential vulnerable parameter while using sqlmap.

- ☐ \*
- ☐ /
- ☒ ;
- ☐ :

[Clear selection](#)

Which of the following port helped you to gain the flag?

- ☐ 441
- ☐ 80
- ☒ 8000
- ☐ 5000

[Clear selection](#)

Select the alternatives of Burp Collaborator used for exploiting SSRF vulnerabilities.

- ☐ Requestcatcher.com
- ☐ Tinyurl.com
- ☐ Webhook.site
- ☒ Both A and C

[Clear selection](#)

SQL Injection and OS command injection when performed combinedly the resultant attack is called as \_\_\_\_\_.

- ☐ Cross-Site Scripting
- ☒ Accellion Attack
- ☐ HTML Injection
- ☐ Server Side Request Forgery

[Clear selection](#)

\_\_\_\_\_ attack is used target internal systems behind the Web Application Firewall, that are unreachable to an attacker from the external network.

- ☐ CSRF
- ☒ XSS
- ☐ SSRF
- ☐ Open Redirect

[Clear selection](#)

What are the possible ways to prevent SSRF attack?

- ☐ Disable all user inputs
- ☐ Enable Authentication on all Services
- ☐ Whitelist Domain in DNS
- ☒ Both B and C

[Clear selection](#)

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

- ☐ #
- ☒ @
- ☐ \*
- ☐ &

[Clear selection](#)

Which of the following two attack vectors solved the CTF?

- ☐ SQL,CSRF
- ☐ XSS, Open Redirect
- ☐ CORS, HTML Injection
- ☒ SQL,SSRF

[Clear selection](#)

Which of the following attack vector help you to solve the second section to achieve the flag?

- ☒ SSRF
- ☐ Open Redirect
- ☐ CORS
- ☐ Cross Site Scripting

[Clear selection](#)

What does the batch command in sqlmap mean?

- ☐ Identifies the version of database
- ☒ It answers YES to all questions
- ☐ Identifies Tables
- ☐ Identifies Databases

[Clear selection](#)

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

- ☐ LDAP Injection
- ☒ SQL Injection
- ☐ HTML Injection
- ☐ Command Injection

[Clear selection](#)

In SSRF attack, the attacker might cause the server to make a connection to \_\_\_\_\_ services of the organization's infrastructure

- ☒ Internal
- ☐ External
- ☐ Public
- ☐ None of the Above

[Clear selection](#)

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

- ☐ Web Server
- ☐ Load Balancers
- ☐ Web Application Firewall (WAF)
- ☒ All of the above

[Clear selection](#)

Which of the following attack vector is involved in first section of the Capture the Flag?

- ☐ Cross-Site Scripting
- ☒ SQL Injection
- ☐ Insecure Direct Object Reference
- ☐ Cross Site Request Forgery

[Clear selection](#)

Identify the payload or the step to solve the first attack vector of Capture the Flag?

- ☐ '><img src=x onload=confirm(1)>
- ☐ Delete the CSRF tokens to assure success
- ☐ Change the values of id parameter
- ☒ ' ) || ('1)=('1

[Clear selection](#)

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

- ☐ URLs
- ☒ Response
- ☐ Request
- ☐ Parameters

[Clear selection](#)

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

- ☐ SSRF attack
- ☒ Denial of Service
- ☐ Phishing Attack
- ☐ None of the Above

[Clear selection](#)

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

- ☐ LDAP Injection
- ☐ SQL Injection
- ☒ Remote Code Execution
- ☐ All of the Above

[Clear selection](#)

Choose the correct payload which helped you to capture the flag?

- ☐ Redirect the URL parameter to [evil.com](#)
- ☒ http://[-]:8000
- ☐ '><h1>Flag Captured</h1>
- ☐ ' or '1'='1

[Clear selection](#)

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

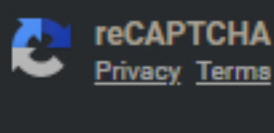
[Back](#)

[Submit](#)

Page 4 of 4

[Clear form](#)

Never submit passwords through Google Forms.



This form was created inside of [VT](#). [Report Abuse](#)

Google Forms