

Cybersecurity

Project Week: Attacking the Web Application

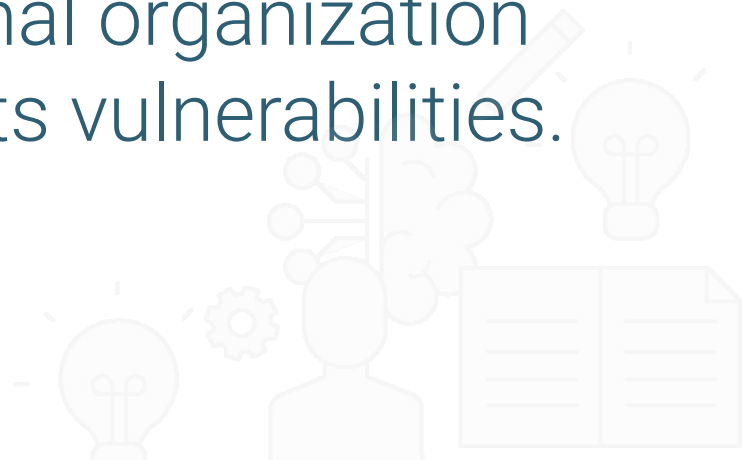
Project Week Day 1

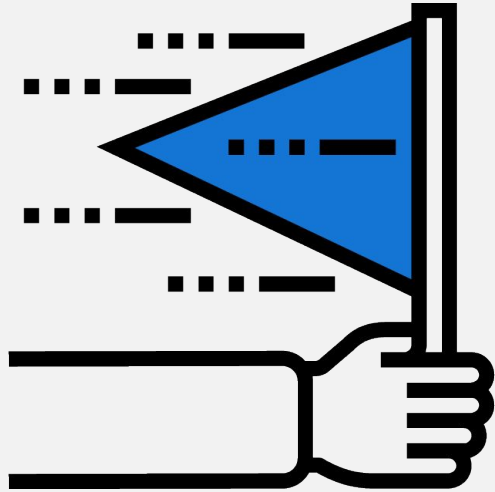


Welcome



This week, you will use the skills that you've learned in the **Offensive Security** unit to attack a fictional organization and discover its vulnerabilities.





As you do so, you'll look for "flags" within the organization's web application and operating systems that you'll collect in a competitive **Capture the Flag (CTF)** game.



Offensive Security Unit

Web application vulnerabilities

- Injection vulnerabilities
 - SQL injection
 - XSS (stored / reflected)
- Back-end component vulnerabilities
 - Directory traversal
 - LFI / RFI

Authentication vulnerabilities

- Session management
- Brute force attacks

Web application testing tools

- Burp Suite

Penetration testing topics

- OSINT
- MITRE framework
- Enumeration
- Port scanning
- Exploitation
- Shells (bind / reverse)
- Lateral movement
- Persistence

Penetration testing tools

- Metasploit / Meterpreter
- Nmap
- Recon-ng
- Shodan.io
- SearchSploit
- Netcat



You'll apply all of these
skills in the second
project!



Project Scenario

For this week's project, you'll work in groups and play the role of penetration testers hired by Rekall Corporation to conduct a penetration testing engagement.

01

Rekall has a brand-new web application and several Linux and Windows servers that manage its businesses.

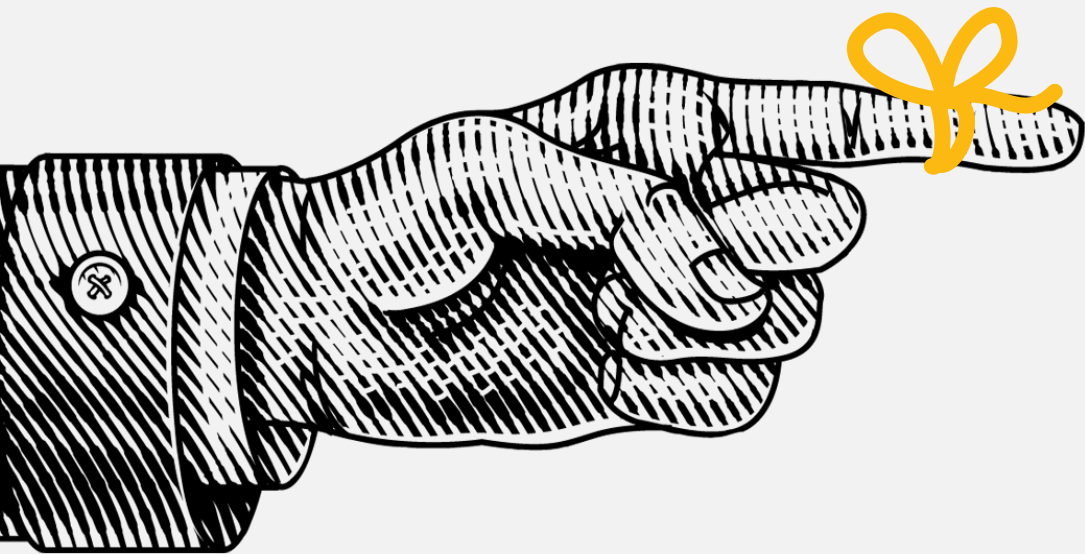
02

You will use your offensive security skills to uncover Rekall's vulnerabilities and summarize the appropriate mitigations.

03

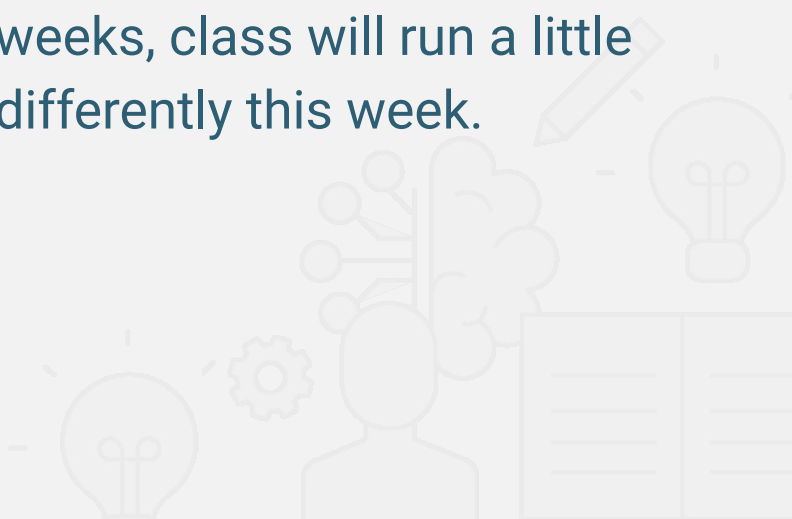
Rekall is ready to bring its business live, and it is counting on your great work this week to protect its organization!

Daily Schedules, Objectives, and Deliverables



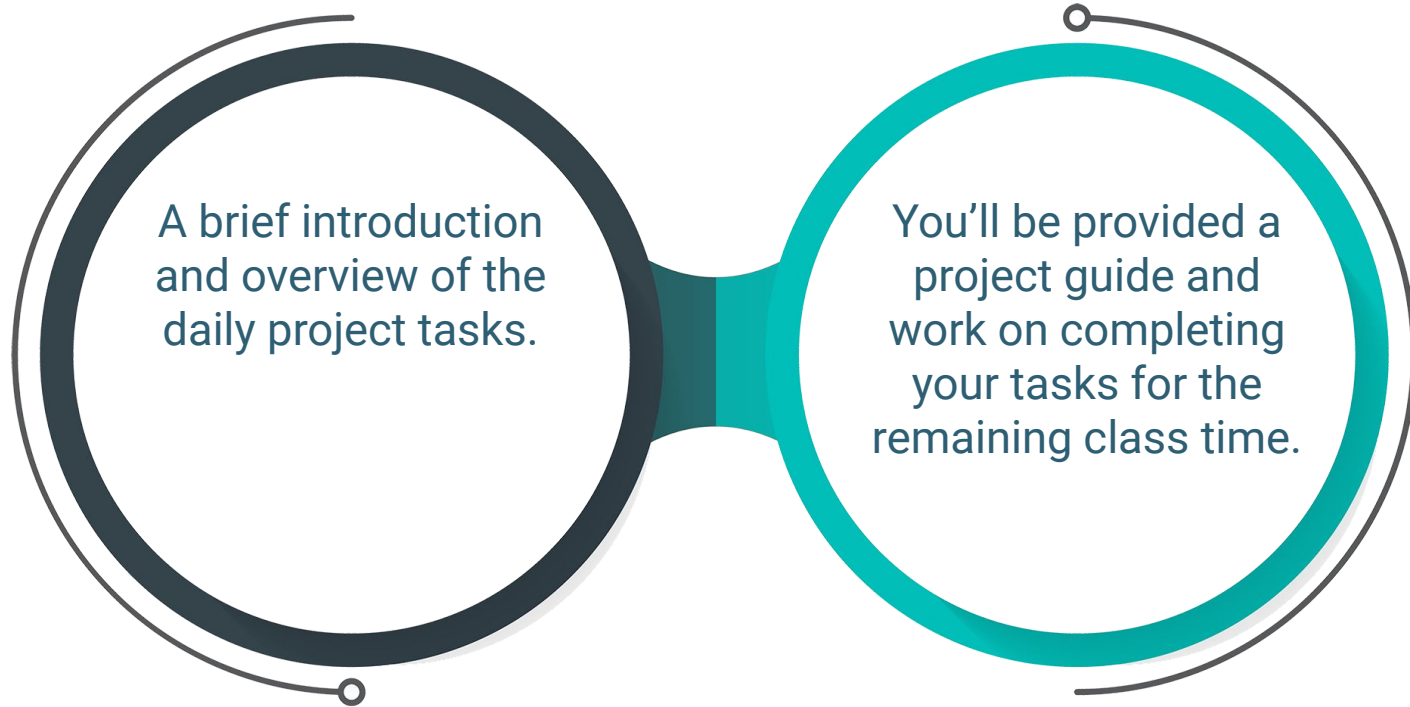
Remember,

As in previous project weeks, class will run a little differently this week.



Daily Schedules, Objectives, and Deliverables

Each day will proceed as follows:



Capture the Flag (CTF)

Each day this week will also be a CTF-style competition.



Your tasks this week include finding vulnerabilities.



You'll be rewarded with a "flag" for each vulnerability you discover and successfully exploit.



You'll receive points for each "flag" that you find.



The team with the most points at the end of class wins!

Daily Objectives and Milestones

Day 1:

Pen test Rekall's **web application**, which has a variety of vulnerabilities, and find flags as you exploit these vulnerabilities.

Day 2:

Continue to exploit Rekall's technical infrastructure, focusing on the organization's **Linux servers** and vulnerabilities related to Linux operating systems. Continue finding flags during your exploitation.

Day 3:

Continue to exploit Rekall's technical infrastructure, focusing on the organization's **Windows servers** and vulnerabilities related to Windows operating systems. Continue finding flags during your exploitation.



Project Deliverables

Summarize your findings and recommended mitigations in a penetration testing report that will become your final deliverable.



A framework for this report will be provided.



Don't forget to include screenshots of your exploits!



Tip: You can take this deliverable with you after graduating and discuss it during job interviews.



Important

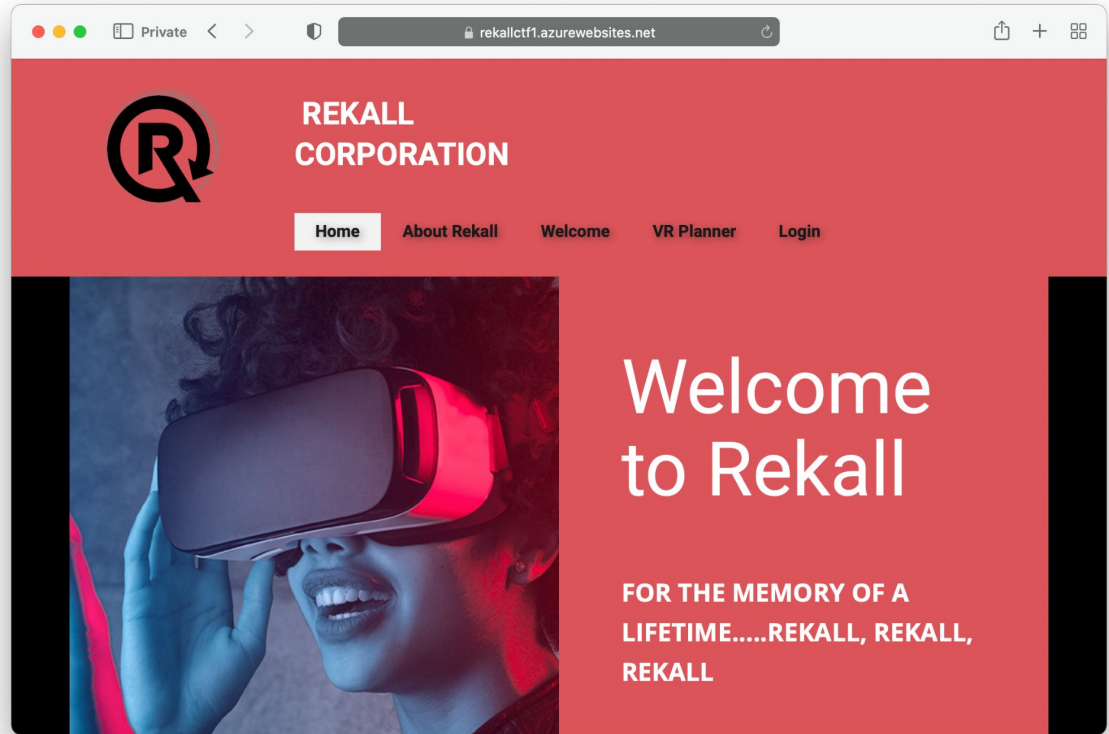


While this is a group activity and you can share findings among group members, every student must submit this deliverable in order to receive credit for Project 2!

Day 1 Project Overview

Project Resources and Setup

Rekall's Web Application
You will access the
Rekall web application
for today's activity within
your Project 2 Lab.





Project Resources and Setup

CTF Flag Submission Page



You'll also access your CTF page within your Lab.



You'll be provided a custom website for your class's CTF when it's time to begin.



Once you have access to the page, register for an account.



Remember your password in case you need to log back in!

CTF Instructions



As penetration testers, you are tasked with finding all vulnerabilities in Rekall's new web application.



There are 15 "flags" hidden across the web application, and a flag will display once you successfully exploit a vulnerability.



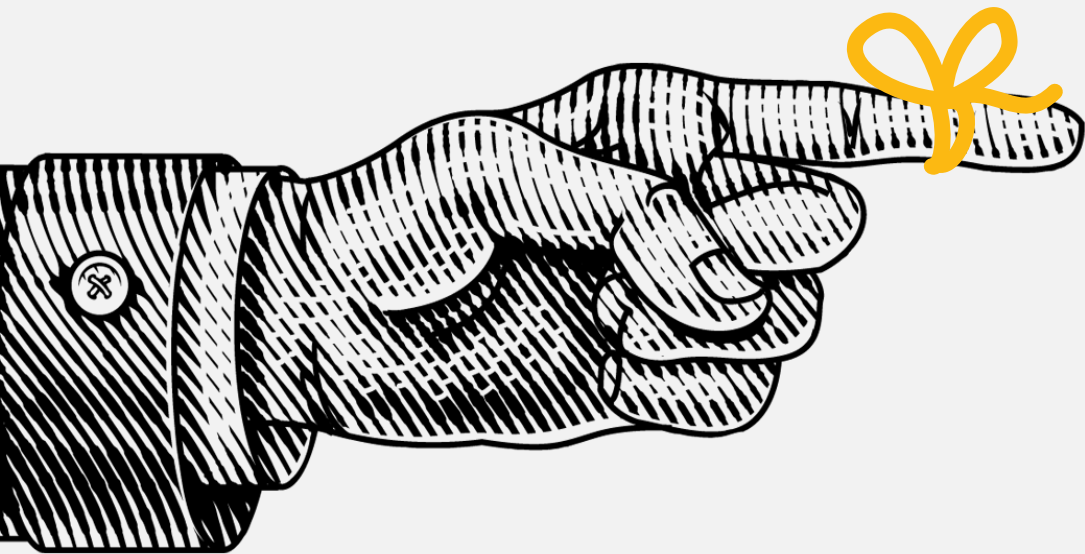
Note that some flags will display on the webpage as soon as you conduct an exploit, while some are hidden in other places.



Each flag is composed of a string of letters and numbers, and is identified by a number (e.g., Flag 1: d8sksydasksd).

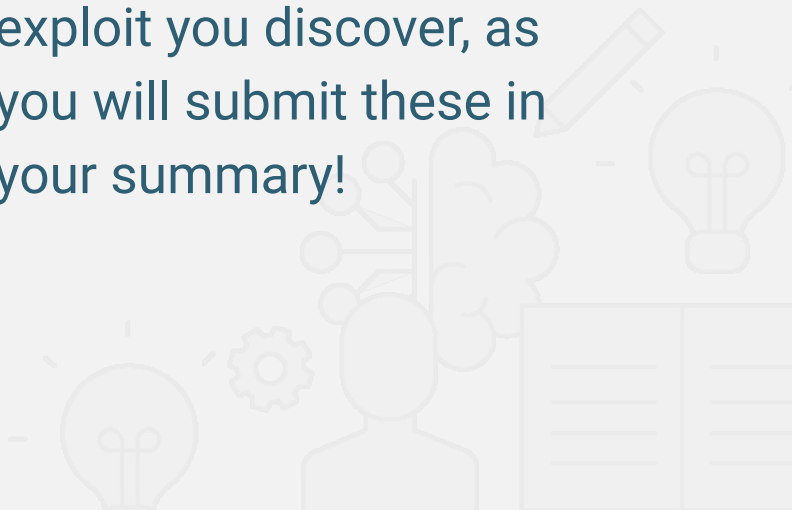


Once you find a flag, enter it on the CTF flag submission page.



Remember,

Take a screenshot of each exploit you discover, as you will submit these in your summary!



CTF Flag Submission Page

- The “Challenges” tab on the CTF page contains the 15 available flags hidden across the web application.
- The flags are categorized by challenge level, including expert, advanced, intermediate, and easy.
- Each flag box indicates the points awarded for that flag. The more challenging a flag, the more points awarded for finding it.

Expert

Flag 13
80

Flag Number

Points Awarded

Advanced

Flag 4
50

Flag 12
50

Flag 15
50

Flag 7
60

Flag 14
60



CTF Flag Submission Page

Selecting a flag will display important information for finding that flag, such as the vulnerability associated with that flag or guidance on where the flag is located.

Challenge

0 Solves

×

Flag 1

30

Reflected XSS

vulnerability

Unlock Hint for 10 points

Unlock Hint for 15 points

Flag

Submit



CTF Flag Submission Page

Once you have found a flag, select the box with that flag number, and enter the flag.

Challenge

0 Solves

×

Flag 13
80



PHP Injection

Unlock Hint for 30 points

Unlock Hint for 20 points

Flag

Submit





CTF Hints

This CTF provides you an option to “pay” for hints with points.

Clicking on a flag will also display any available hints for that flag and the points it costs to unlock those hints.



Note: You must already have been awarded the points before you can use them to “pay” for hints.

Challenge

0 Solves

×

Flag 13

80

PHP Injection

Unlock Hint for 30 points

Unlock Hint for 20 points

Flag

Submit

Hints for Success



To make all the web application pages accessible, click the following buttons:

- The “Get Started” button on the “Home” page.
- The “Click Here to Begin” button on the “About Rekall” page.



Certain flags are protected via input validation; try to find methods to bypass them.

- Think like a hacker!



Use the internet to help figure out methods to exploit these vulnerabilities.



Feel free to use tools such as Burp Suite (installed within your VM) to help with your exploits.



Certain exploits can be used to find information that will help you find other flags.



Most of the exploits that you’ll use were covered in class, but there are some new exploits which will require additional research.

CTF Rules

Rules for today's activity:



Each group will start at the same time once the URL for the CTF has been provided.



The team with the most points at the end of the allotted time will win.



You can use all available resources to assist you: class notes, slides, internet resources, tools such as Burp Suite, etc.



If you are able to exploit a vulnerability and a flag does not display, please contact your instructor or TA to receive the flag.



Your instructor or TA can assist with technical or lab access issues, but will not be able to provide guidance for finding the flags.



Questions?





Activity:

Attacking the Web Application

In this activity, you'll work toward completing the project's Day 1 tasks.

Suggested Time:

2 hours 20 minutes





Time's up!
Let's review



Questions?





The End