| Cybersecurity |
| --- |
| Day 1 Activity Guide |

## Attacking the Web Application CTF

### 

### Project Scenario

For this week’s project, Project 2, you will play the role of penetration testers hired to conduct a penetration testing engagement by Rekall Corporation.

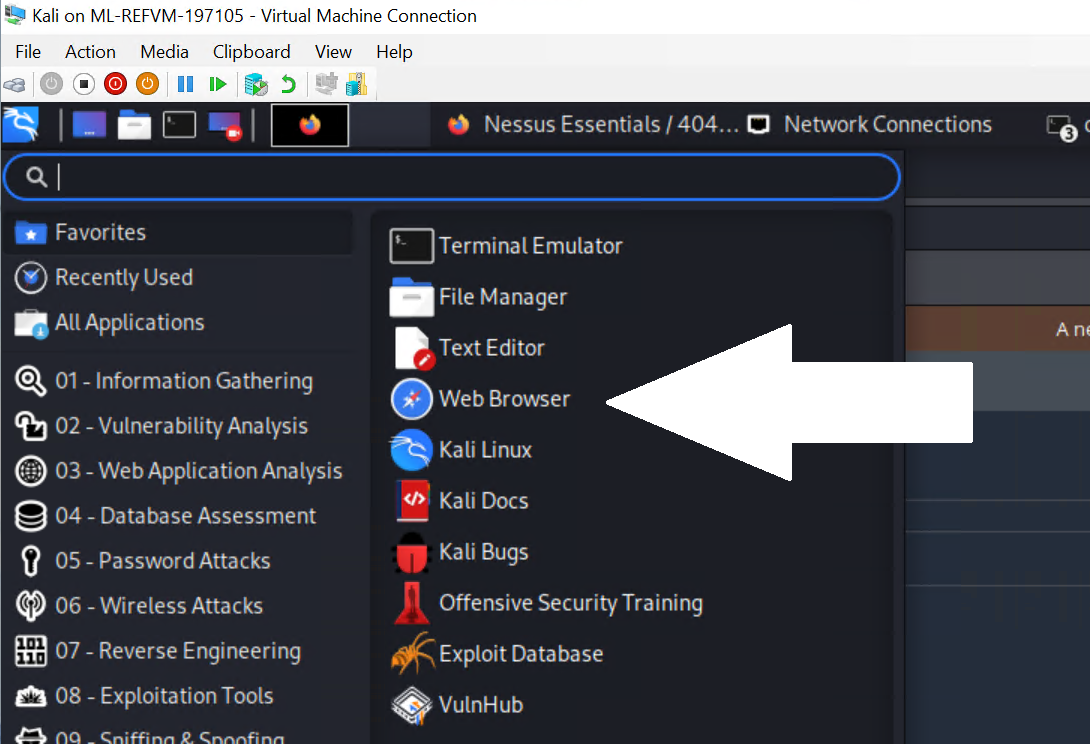
* **Rekall Corporation** is a fictional company that specializes in offering virtual reality experiences based on images that customers upload.
  + These experiences could include dream vacations, adventures, or even secret missions.
  + Rekall guarantees that these virtual reality experiences will feel real.
* Rekall is about to go live with their business, and they need penetration testers to find any vulnerabilities within their technical systems.
  + Rekall has a brand new web application and several Windows and Linux servers that manage their businesses.
* You are tasked with using the offensive security skills that you’ve learned over the last couple of weeks to find any vulnerabilities in Rekall’s technical infrastructure and summarize the appropriate mitigations.
* As you go through this week’s activities, be sure to update this [penetration testing summary report](https://docs.google.com/document/d/1Kz1sOwmb82uNXJyZlox9cP7tPvDpNNcvkxREuCFBVLM/edit#), which you’ll submit upon completion of Project 2.
  + Remember to take screenshots of your exploits, as you’ll include those in your report.

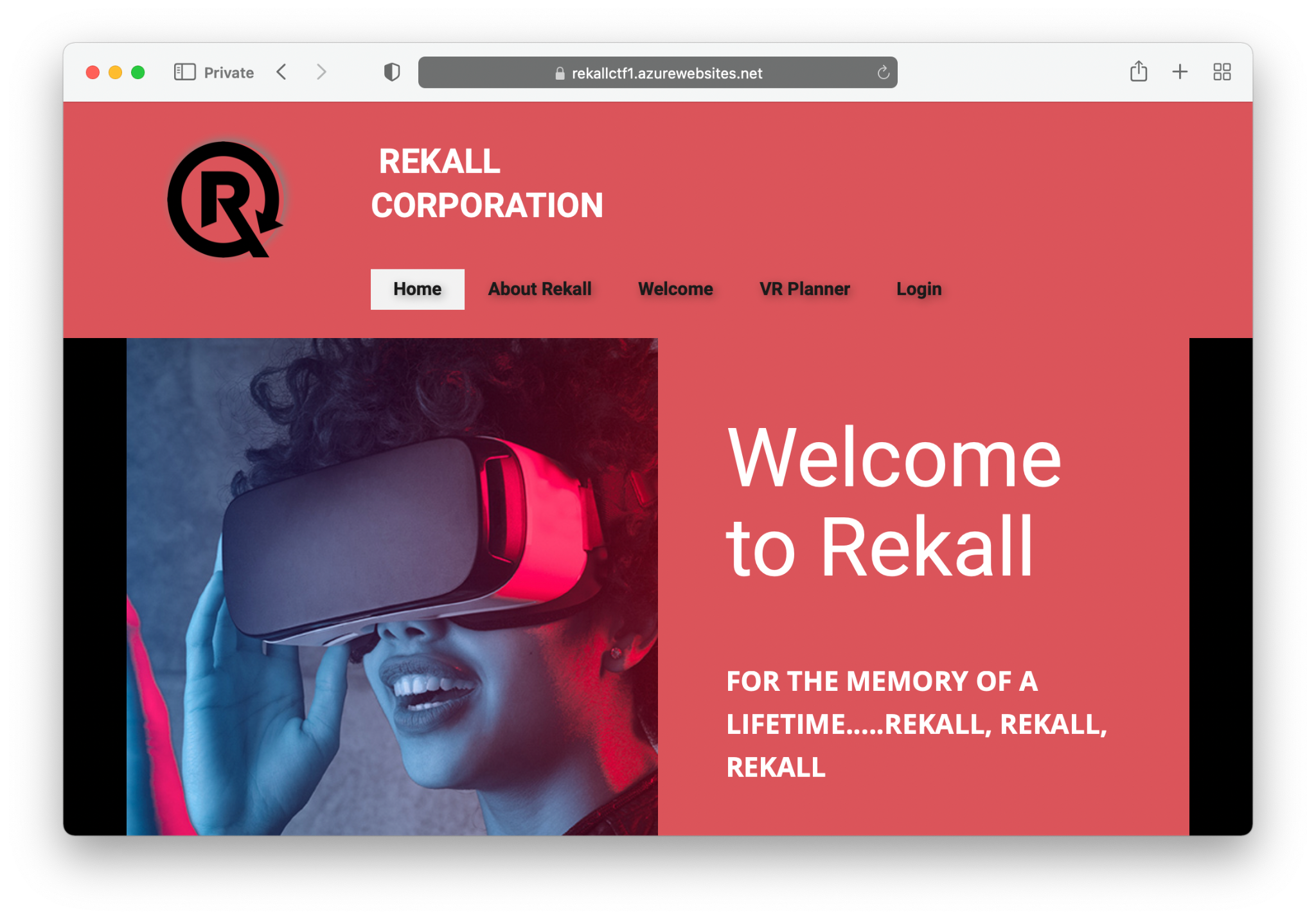
Rekall is ready to bring their business live, and they are counting on your great work this week to protect their organization!

### Project Resources and Setup

You’ll use the following resources to complete today’s project:

1. **Rekall’s web application**

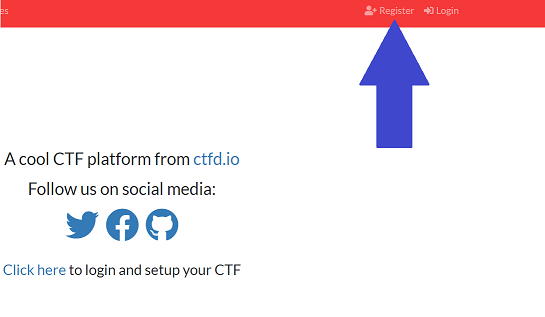
* You will access today’s activity within your Project 2 Lab.
* Once you have logged into the Lab from your Hyper-V, select the “Kali” machine.
* Log in to Kali with the following credentials:
  + User: root
  + Password: kali
* Open a terminal, and cd over to: /root/Documents/day\_1
  + Type: docker-compose pull and press Enter, then...
  + Type: docker-compose up and press Enter.
  + Leave this window open.
* Now, open a browser window, as the following image shows:  
  
* **Important:** To make all the pages of the web application accessible, you must complete the next 3 steps:
  + Once the browser opens, access the web application at http://192.168.14.35. The webpage should resemble the following image:



* + Once the web page loads, click the "Get Started" button. You will be notified via a popup that the CTF is ready.
  + Select "Click Here to Begin" on the "About Rekall" page.
  + **Note:** If any pages are not accessible within your web application, complete the above steps from part 1 again.

2. **CTF flag submission page**

* Within your Lab browser, open a second tab and access your CTF page.
  + Your instructor will provide the custom website for your CTF when you are ready to begin.
* Once you have accessed this page, select “Register” on the top right to register your account, as the following image shows:



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

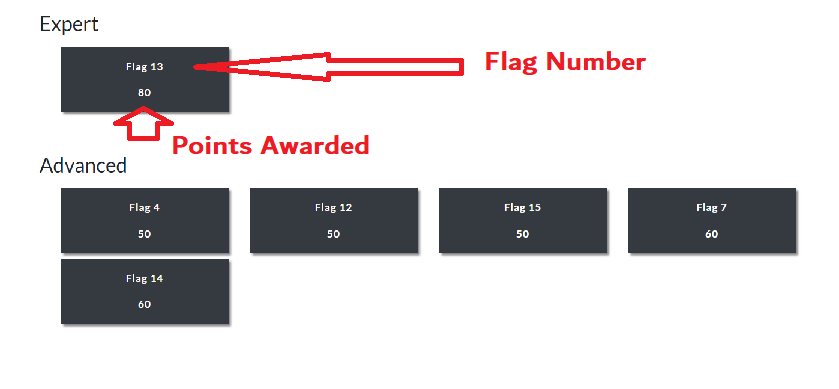
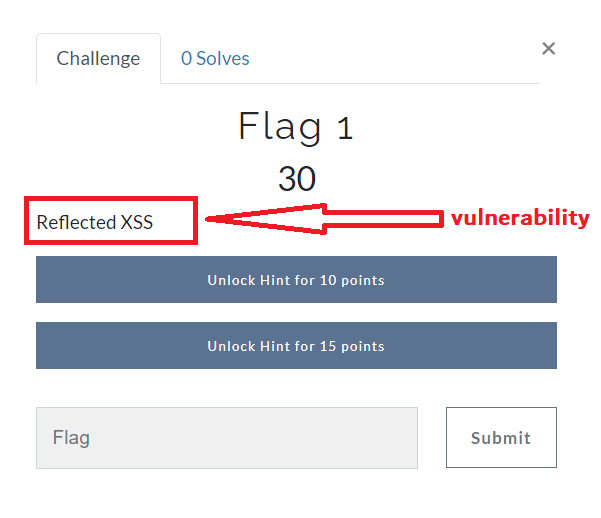
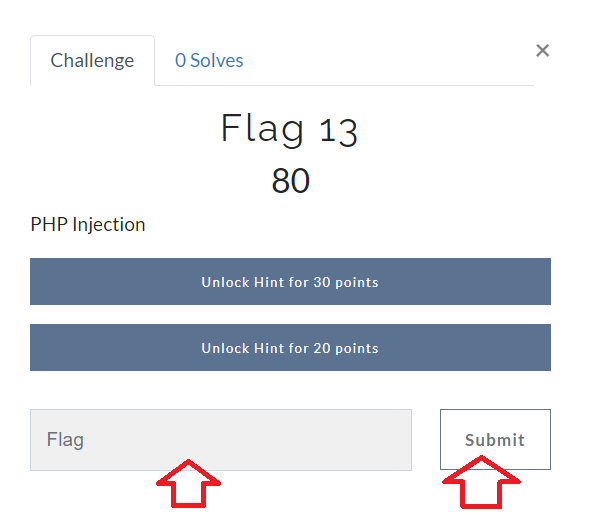
| ⚠️ **Important**: Since you are competing in groups, select one team captain to choose a group name and password and share it amongst the team members when registering. As the following image shows, the team captain will select the “Create Team” option, and the rest of the team will select the “Join Team” option:  A screenshot depicts the "Join Team" and "Create Team" buttons. |
| --- |

### CTF Instructions and Rules

#### Instructions

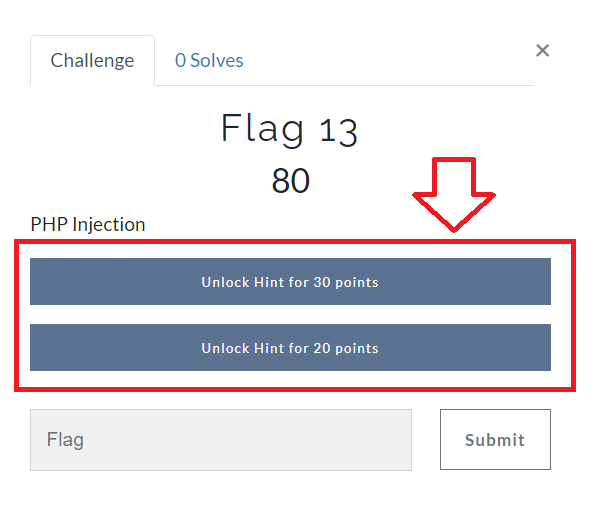
* As penetration testers, you are tasked with finding all vulnerabilities in Rekall’s new web application.
* Fifteen “flags” are hidden across the web application, and a flag will display once you successfully exploit a vulnerability.
  + Note that some flags will display on the webpage as soon as you 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: d8sksydasksdy”.
* Once you find a flag, enter it on the CTF flag submission page.
* Remember to take a screenshot of each exploit you discover, as you will submit these in your summary!

#### CTF Flag Submission Page

* After accessing the CTF website, select the “Challenges” tab.
* This webpage contains the 15 available flags hidden across the web application.
* The flags are categorized by challenge level, including:
  + Expert
  + Advanced
  + Intermediate
  + Easy
* The points awarded for a flag are indicated in the flag box. The more challenging the flag, the more points will be awarded for finding it, as the following image shows:  
  
* 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, as the following image shows:  
  
* Once you have found a flag, select the box with that flag number, and enter in the flag, as the following image shows:  
  
* You can view your team point total by selecting the “Scoreboard” option at the top of the page.

#### 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, as the following image shows:



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

#### Additional 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.
  + Note that you will need to add a Proxy such as “Foxy Proxy” to your browser
  + **Hint**: Use Port 8081 if port 8080 isn’t available.
* 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

* 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.

© 2023 edX, a 2U, Inc. brand. All Rights Reserved.