CPTC Week 3 Homework

Web Apps

Part 1: Questions (50pts)

1. (50pts) Compare and contrast your choice of any 2 (or more) web app vulnerabilities. You may choose from the list below, or pick your own. DO NOT SELECT 2 FROM THE HIGHLIGHTED POOL. Some things to consider are:
    a. Prerequisites
    b. Tooling/techniques used
    c. Impact
    d. Remediations

SQL Injection	Cross Site Scripting	Command Injection
Mass Assignment	Deserialization	Server Side Template Injection
Prototype Pollution	Type Juggling	Client Side Request Forgery

Part 2: Lab (50pts)

Access Kamino (kamino.calpolyswift.org) and deploy the template 'CPTC-Web'. Answer the following questions once the application is deployed. If you need help finding the IP address of the web application, refer to the very end of the document.

1. (30pts) Redemption.nft questions. Questions are graded on a mix of both accuracy and effort.
   a. What is the purpose of this web application (What kind of service is the app providing)?
   b. What backend language is the web application using? Explain how you figured that out.
   c. Are there any inherent capabilities tied to the kind of service this app provides that you can take advantage of?
   d. Do a little bit of outside research based on the type of web app this is (your answer to Part 2, 1a). Write about some kinds of vulnerabilities it is known for.
   e. Based on what you see, what are some possible attacks to carry out on this application. Explain your reasoning.
2. (20pts) Perform a web application penetration test against your personal instance of Redemption NFT. Write up about 2 distinct web application vulnerabilities tied to the web application.

Deliverables

1. Submit a PDF with all of the following:
   a. Answers to all the questions
2. Make sure all sections are labeled.
3. Name the file with the following format: FirstLast_CPTCHomework3.pdf

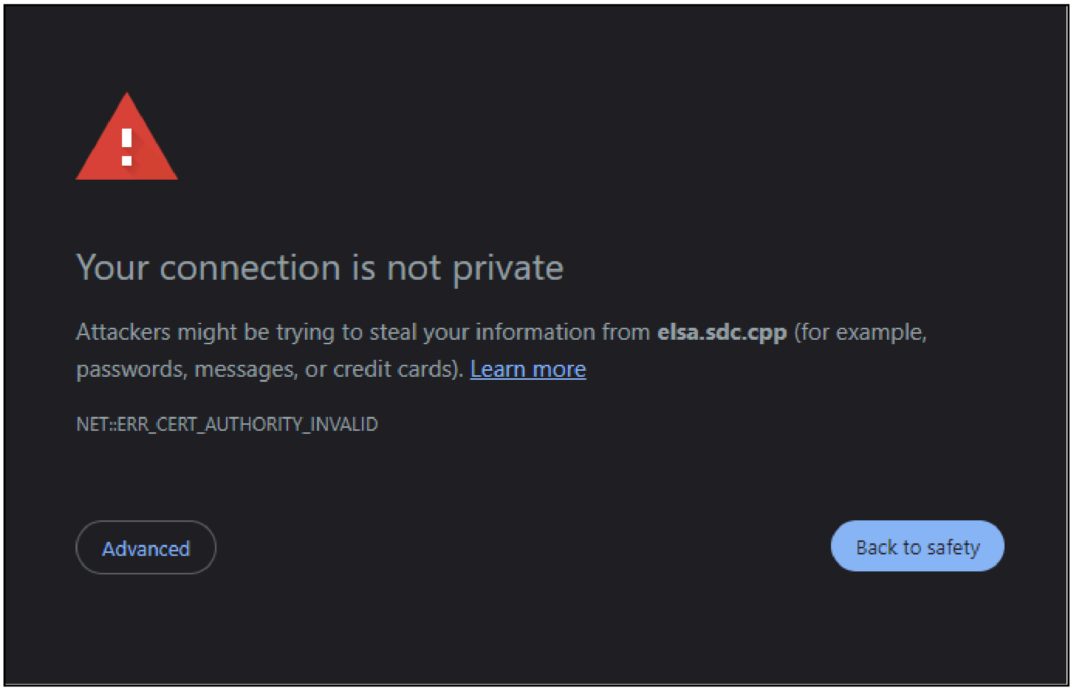
If you are trying out for the team, make sure you submit your PDF in Canvas.

Slides

https://jessh.zip/cptc3slides

VPN Access

1. Download a VPN client. This can be Pritunl or OpenVPN
2. Download the VPN profile here
    - Username: vpn
    - Password: 141252
3. Browse to https://elsa.sdc.cpp. If you see something like the following, you are good.



Your connection is not private

Attackers might be trying to steal your information from **elsa.sdc.cpp** (for example, passwords, messages, or credit cards). Learn more

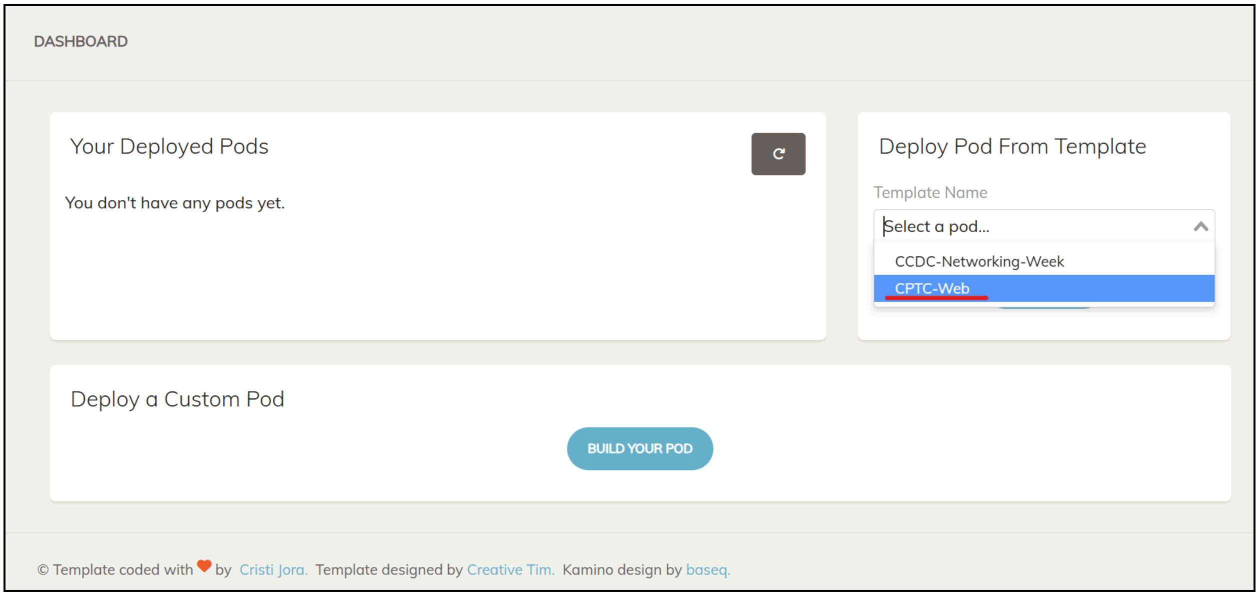
NET::ERR_CERT_AUTHORITY_INVALID

4. Hit advanced and proceed to elsa.sdc.cpp (Browsers other than Chrome may differ slightly)

Accessing Kamino

The link to Kamino is at https://kamino.calpolyswift.org. Note that you need to be on VPN provided in the earlier section to access the pods later on. We are aware of a current issue with the 'Register' function and is currently inoperable. If you need an account, contact Marshall @hgwj on Discord.

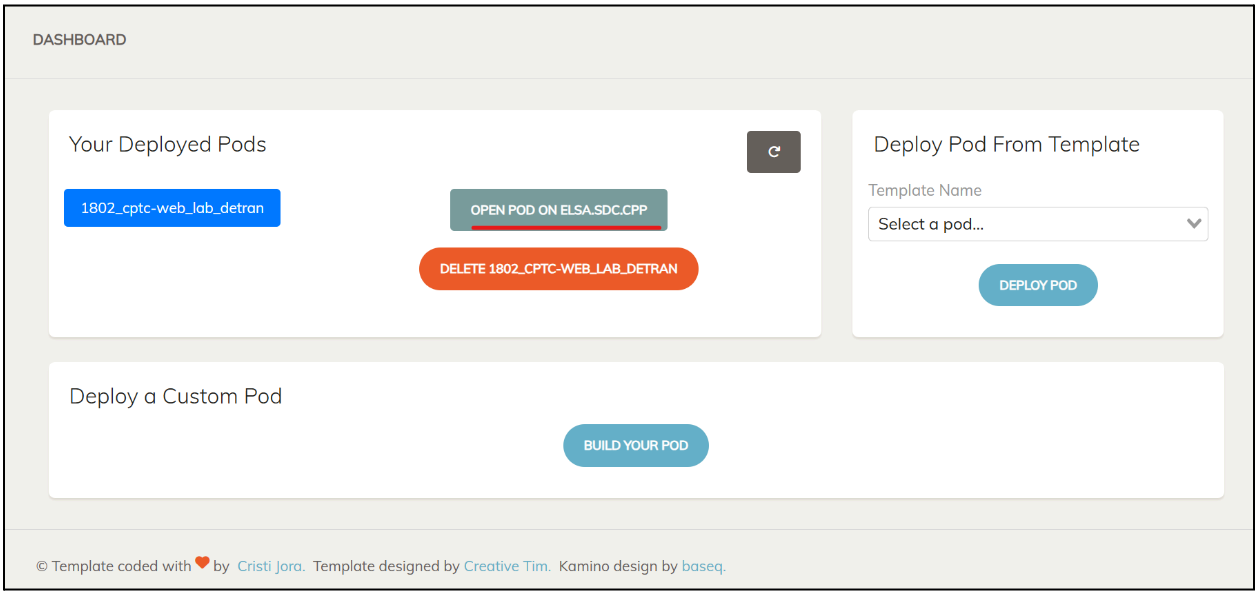
Upon logging in, press the 'Deploy Pod From Template' and select CPTC-Web and then hit 'Deploy'.



You don't have any pods yet.

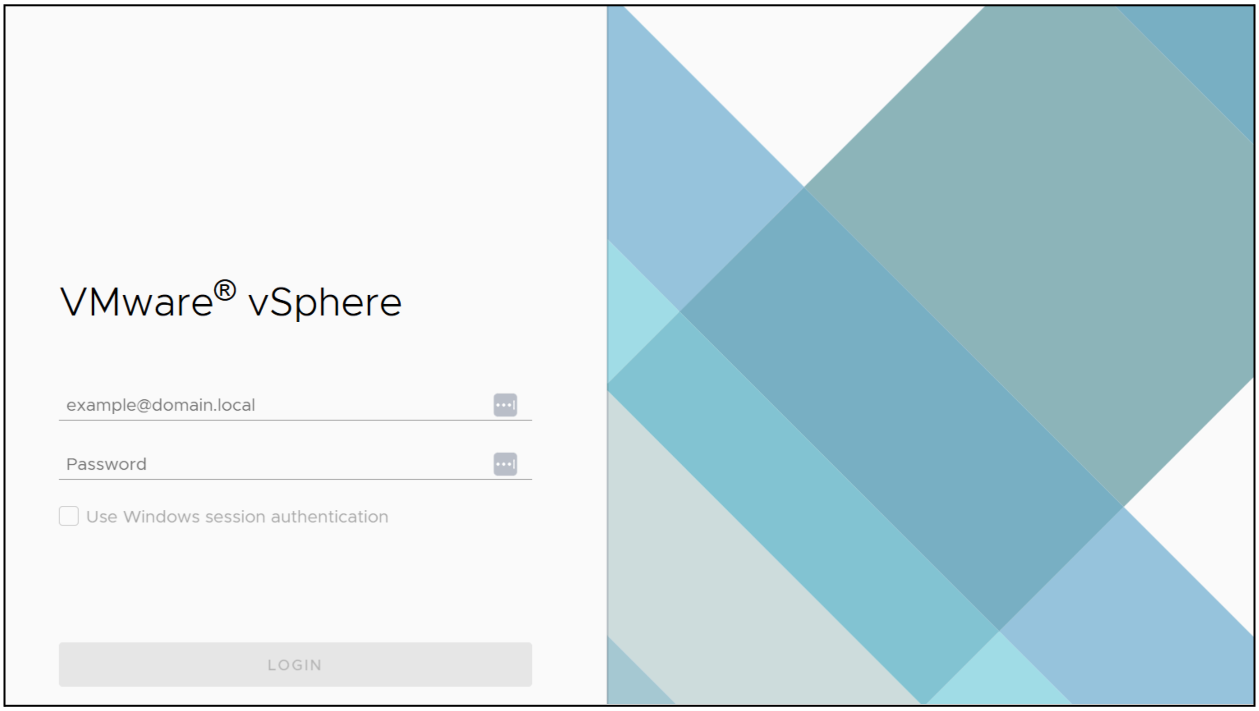
© Template coded with ❤ by Cristi Jora. Template designed by Creative Tim. Kamino design by baseq.

Once the pod is deployed, click the link highlighted below to access the resource on vSphere. You need to be on the VPN in order to open up this page.

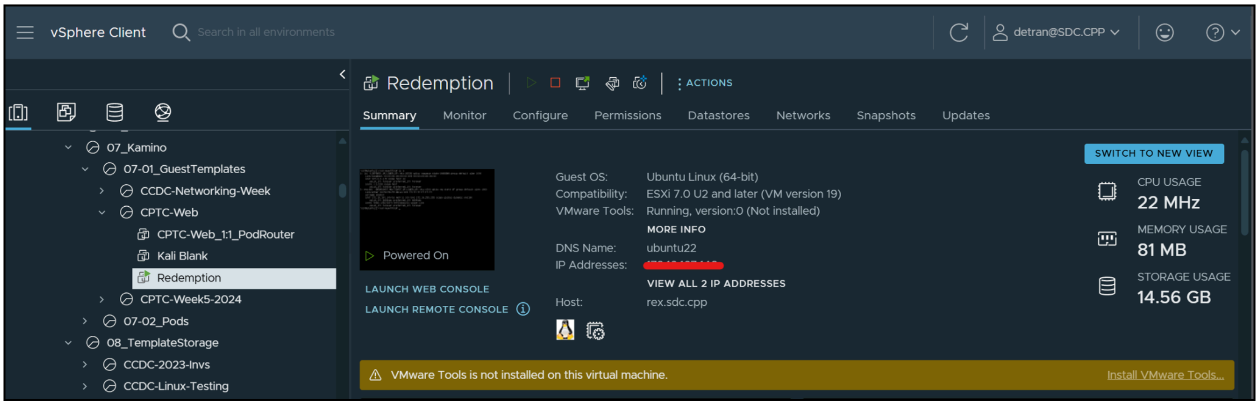


© Template coded with ❤ by Cristi Jora. Template designed by Creative Tim. Kamino design by baseq.

Login with the same credentials you have used for Kamino here.



Once logged in, view your pod and ensure that all of the VMs are online as indicated by the green arrow. The IP of your machine is found under the red line. Most people will have different IPs. There are two ways to access the web application as the machine has their IP Natted. If you are accessing the machine internally, you can use the IP address that you see. Internally in this case means from the Kali machine as they lie on the same network.



Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Running, version:0 (Not installed)
DNS Name: ubuntu22
IP Addresses: [redacted]
Host: rex.sdc.cpp

CPU USAGE 22 MHz
MEMORY USAGE 81 MB
STORAGE USAGE 14.56 GB

⚠ VMware Tools is not installed on this virtual machine.

If you want to access the website externally, from an outside network such as your own host machine, you need to use its external address which can be calculated by the following. In this example, I will use pod 1802, with a listed IP of 192.168.1.15. The external address of this machine always starts with 172.16. The third octet is going to be the last two digits of your pod. Since my pod is 1802, the last two digits are 02 and thus, .2 is my 3rd octet. The last octet of the machine is the same one from the internal address.
TLDR:
Internal address - 192.168.1.15 > External address - 172.16.2.15