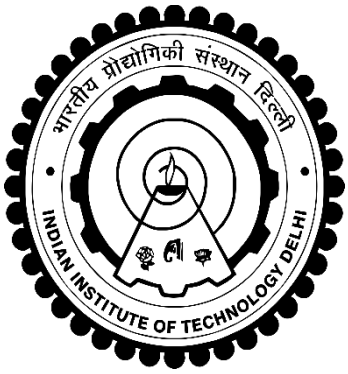
Summer Project Report (2017)

Project Title:

Develop an online System to host capture the flag contest and hackathons

Under

Center of Excellence in Cyber Systems and Information Assurance (CoE-CSIA), IIT Delhi



Duration: 15th May, 2017 to 14th July, 2017

Team Members:

Name	Entry Number
Yash Malviya	2016CS50403
Sumit Kumar Ghosh	2016CS50400
Ayush Patel	2016CS50396
Rudraksh Agarwal	2016PH10549

Supervisor: Prof. Ranjan Bose

Plan of Action

Week1: Learning web technology

- Revising HTML, bootstrap(css), NodeJs
- Practicing framework: EmberJs(Frontend)

Week2: Learning web technology and Learning hacking

- Learning MongoDB
- practicing framework: SailsJs(Backend)
- Hacking: insectechs courses and video tutorials

Week3: Improving CTF specific hacking skills

- Improving CTF specific hacking skills: reverse engineering, cryptography, web vulnerabilities, binary exercises, networking

Week4: Setting capture the flag problems

- First half of the week: taking in always online CTFs.
- Second half of the week: setting up CTF problems

Week5: Implementation of CTF web application

- Implementing frontend by deriving inspiration from famous CTF websites
- Programming scoring, hosting system
- Configuration of database

Week6: deployment CTF web application and Improvisations

- Deploying the website on IITD internal server
- Organising a CTF contest

Develop an online System to host CTF contest and Hackathons

Abstract

Capture the Flag (CTF) is a special kind of information security competitions. There are two common types of CTFs: Jeopardy and Attack-Defence.

This website will be an always online CTF platform. We will primarily focus on developing a jeopardy style CTF hosting site and then extend it to other format CTFs (attack-defense) as well.

Jeopardy-style CTFs will have a couple of questions (tasks) in range of categories. For example, Webapp hacking, Forensic, Cryptography, Binary etc. This type of CTF can be either individual or team-based competition. Participants will gain some points for every solved task. More points will be awarded for more complicated tasks. The next task in chain can be opened only after some team or participant solve previous task. When the game time is over a score bot will show sum of points to declare a CTF winner.

Attack-defence can be another interesting kind of competition to be included. Here every team will have their own network (or only one host) with vulnerable services. One team has time for patching their services and developing exploits. So, then teams are connected and the war game starts! The teams should protect own services for defence points and hack opponents for attack points.

Our Website will have a leader's board showcasing overall ranking of users and teams which will be sum of points they gained during contests. Users too can submit their own contests.

We will use html with bootstrap for frontend. Angular for client side and NoSQL (MongoDB) for database.

Develop an online System to host CTF contest and Hackathons

1st week report (14/5/17-21/5/17)

Further discussion on the structure of the project:

Basically we will be using EmberJs framework for frontend, our backend server will have SailsJs framework integrated with MongoDB (Document based Database Management System).

Starting from basics we will be making a simple EmberJs app which which will contain basic MVC elements i.e. models, views, controllers, templates and routers. It will server as the foundation block of our project. Then we will make migrations on the database using the above models.

We will have an admin panel, a host panel and a client panel. Admin panel will take care of development, bug, security etc. related issues of site. Host panel will be hosting challenges and hackathons on the site. Clients may accept these challenges and then work upon them and submit their responses.

Initially following the jeopardy style, the challenges will be stored in the database with their encrypted and hashed solutions (flags). These will be available in site with proper User Interface (UI), from where the clients can download the challenges (concept of jeopardy style). There will be a portal where the solutions (64bit strings proving the successful completion) of the challenges can be uploaded by the clients and can be evaluated.

The site will thereby be hosted on a paid web server or on the IIT Delhi Intranet Server whichever be more suitable. If the project is accepted by authorities then we will be having an administration unit for maintaining the security of the site so that the site itself is not prone to being “**HACKED”.**

Week 1 Foreseen Objective:

- Revising HTML, bootstrap(css), NodeJs
- Practicing framework: EmberJs(Frontend)

Week 1 Objectives Achieved:

- Attained good enough knowledge of HTML and Bootstrap (js and css) from w3school.
- Learned and practiced JavaScript (from Codecademy and w3school).
- Started learning NodeJs from thenewboston and nodeschool.
- Gained vital knowledge in-built global modules like http and file system. ⌄ Started learning EmberJs, moreover learned to implement custom HTML plugins and js connection libraries and data transfer libraries.

Develop an online System to host CTF contest and Hackathons

2nd week report (22/5/17-28/5/17)

Week 2 Foreseen Objective:

- Learning MongoDB
- practicing framework: SailsJs(Backend)
- Learning Hacking: insectechs courses and video tutorials

Week 2 Objectives Achieved:

NodeJs Practice

- Created a basic express app, which had a simple navigation bar with a few links to webpages of the same app (implemented through fs module). Also learned and used important Nodejs modules such as http, connect, fs.

EmberJs: learning and implementation (continued)

- Continued learning EmberJs framework from Treehouse Tutorials.
- Made an Ember Blog App which had dynamically updated posts and comments feature.

Learning and practicing Sails

- Started learning SailsJs framework from Sails casts.
- Created a Demo Sails (backend) app.

Learning MongoDB

- Learnt basics of NoSQL and MongoDB from documentation and various other sources.
- Integrated Sails backend server with mongo DB's database.

Getting more experience in Sails and implementing some necessary features

- Implemented features in a demo app that users will have on the final app. The examples of the features are as follows-
  - Encrypted password (encryption using Bcrypt Node module) getting stored on user creation.
  - Basic user sign-up.
  - Ability to update user information after user creation.
  - Making the app secure to Cross-Site Request Forgery.
  - Client side information validation during sign-up with help of jQuery (addition module: jQuery Validate).

Develop an online System to host CTF contest and Hackathons

3rd week report (29/5/17-4/6/17)

Week 3 Foreseen Objective:

Improving CTF specific hacking skills

- Reverse Engineering
- Cryptography
- Web Vulnerabilities
- Binary Exercises
- Networking

Week 3 Objectives Achieved:

Finishing up Learning Basics of Web Development

Some members of our team were not able to complete learning the basics of Web Development within our pre-planned deadline, so we completed that task in this week.
That involved

- Learning Ember.js development by making a webapp by following any web tutorial.
- Learning the basics of NoSQL databases like MongoDB and implementing them.
- Learning Sails.js development by making a webapp by following any web tutorial.
- Integrating Ember and Sails together in a webapp by using Sails generated REST API as backend and Ember as frontend. Also implementing MongoDB as the database used.
- Also we looked into the SANE stack as a potential framework to work with (http://sanestack.com/).

All members of our team has completed the above objectives by now and we have a basic idea of web development using Node and its various frameworks.

Improving CTF Hacking Skills

Learned about various web vulnerabilities from Insec-Techs videos and implemented them. Some of those web-vulnerabilities are - ⌄ SQL Injection

- Cross Site Scripting
- Cross-Site Request Forgery
- Session Hijacking through arp spoofing

Read about the basics of Cryptography from various web-tutorials.
Looked into various techniques and tools used by famous CTF winning groups such as pwntools by Gallopsled (https://github.com/Gallopsled/pwntools).

Researching about Already Existing Open-source CTF Frameworks

CTF frameworks can help us in hosting a CTF contest with just a few configurations. We will just have to add the problems in the CTF, not worrying about the other parts of the program.

Searched the Internet for all available open-source CTF frameworks that can be used to host a CTF contest easily. Compiled the found data as a list which is stored at https://github.com/SkullTech/CTF-Resources .

Develop an online System to host CTF contest and Hackathons

4th week report (5/6/17-11/6/17)

Week 4 Foreseen objectives

Setting capture the flag problems

- First half of the week: taking in always online CTFs.
- Second half of the week: setting up CTF problems

Week 4 Objectives Achieved

Learn about various disciplines related to CTF problems

Forensics

- Analysing packet capture dumps using Wireshark.
- Extracting plaintext passwords (or base64 encoded) from pcap file.
- Learning about User-Agent strings. Extracting browser info from pcap file.

Cryptography

- Basics of how cryptography works. Symmetric key cryptography, public key cryptography and logging in using public keys through SSH.
- Basic symmetric key cryptography algorithms: Substitution algorithms such as Caesar cipher, Vigenère cipher, monoalphabetic substitution cipher.
- Learn in detail about Base64 encryption. Learn basic details about RSA and AES encryption.
- Learn about Hash Functions (MD5).
- Cracking common hashes using various web-services.

Web Exploitation

- Executing javascript in chrome developer console to exploit.
- SQL Injection:
  - Cracking login form by submitting SQL through login form.

Miscellaneous

- Using netcat(nc) command to connect to arbitrary machine at an arbitrary port.
- Using basic linux commands such as find and grep.

Practicing in Always Online CTFs

- Picoctf (https://picoctf.com/)
- Setted MCQ questions for the first round (https://github.com/SkullTech/SuperLeet-CTF)