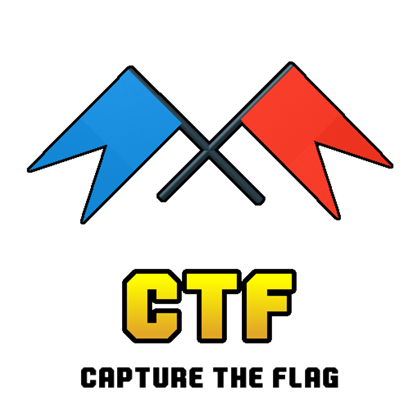
**IE3092**

**Information Security Project**

**CTF**

Project Proposal



**Student Details**

|  |  |
| --- | --- |
| Student Number | Student Name |
| IT18032666 | Wishvajith B. L. D. V |
| IT18021912 | Ramanayaka A. M |

Links –

Youtube : <https://youtu.be/OadvFDJMlRM>

GitHub : [github.com/VimukthiW/CryXSS-CTF](https://github.com/VimukthiW/CryXSS-CTF)

**Introduction**

****

What is E-commerce?

E-commerce can be defined in simpler terms as buying and selling of goods or services over internet. According to recent statistics out of all the possible e-commerce solutions out there, use of web applications/websites for e-commerce businesses takes about 64% out of all the options. It is also estimated that by 2021, worldwide e-commerce retail sales will reach $4.9 trillion. Also due to these recent covid 19 pandemic situation majority of local businesses in our country have also either already converted or considering converting their businesses online. This sudden change resulted in lots of unsecure practices among online e-commerce retailers hence increasing cyber-attacks against e-commerce businesses. Therefore for e-commerce businesses/retailers, web application security plays a crucial role in maintaining a successful online presence. But the problem arises, where most businesses do not have the resources or a safe environment to test and practice as well as train their employees about current e-commerce specific vulnerabilities.

What is the solution?

To provide a solution to these challenges we decided to do some research on industry incidents to get an overall idea about the current trends among attackers and identified why and where most of e-commerce businesses fail in terms of securing their businesses online. We created a safe environment in an exciting way to train current employees/security professionals of e-commerce businesses as a capture the flag event.

Brief introduction

CryX33 CTF is a Jeopardy style capture the flag competition hosted to improve the skills of security professionals in e-commerce sector where participants are presented with challenges in security areas which are critical to the e-commerce businesses like Crypto, Web application security where they get the chance to improve and expand their knowledge on common identified vulnerabilities which have led to attacks in major businesses and also get exposed to tools used to detect and exploitation part and gain overall experience about how CTF events can be used to learn new skills and clarify security needs relevant to the industry.

**Architecture**

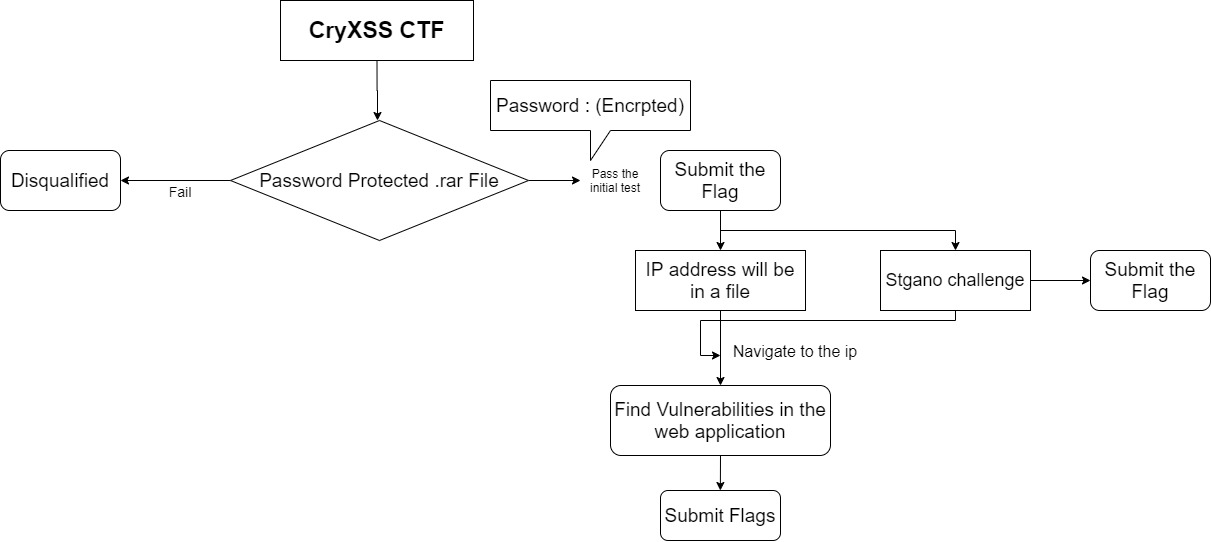
**Level 01 – Preliminary challenges**

The Competition can be deployed as an event within the organization and the event begins when the announcement is given and after the timer starts, competitors will be provided with an encrypted passcode that needs to be decrypted as part of a crypto challenge and will be used to extract the .rar file which will be the first thing a competitor will get when they register for the competition. Proper submission of this first flag will be counted as 5 points and most importantly it is a preliminary challenge which will decide if the player gets the access to the rest of the CTF levels.

Then the attacker will be given several files upon the extraction of the given .rar file. Among files will be a file containing a hidden ip address, several files and a vm file. Alternatively there will be a stegano challenge with a flag and the ip address attached to that file. Submission of that flag would count as an additional 5 points to the team. Both the above challenges are there to make the competition an enjoyable experience.

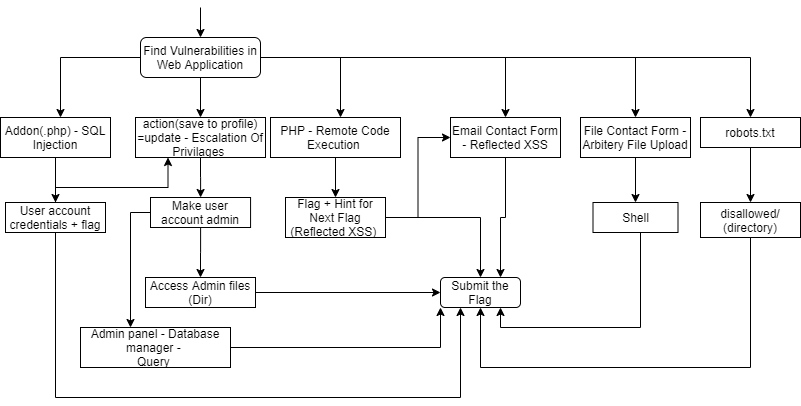
**Level 02 – Web application challenge**

Attackers will be presented with a front end e-commerce web application developed with PHP and js, host - apache containing several vulnerabilities containing 7 flags. Each flag submission will be counted as 10 points.  
  
The team who submit all the flags under 6 hours will receive additional 10 points.



Web application architecture

In level 02, the attacker will be presented with a working web application. Application will have 07 total vulnerabilities leading to 07 flags to be found and submitted.



Robots.txt – robots.txt tells search engine crawlers what directories are allowed and disallowed. Disallowed directories usually have sensitive information. Look through the directories list to find the flag.

Contact Form.php - Contact form will have several bugs which will lead to two flags. One is a simple reflected XSS and second option is to upload a script file to gain a shell and finding the flag.

|  |  |
| --- | --- |
| **Flag Challenge** | **Points upon successful submission** |
| 1.Crypto – Password Decryption | 05 |
| 2. Stegano Challenge | 05 |
| 3 – 9 Web | 10 each - (max 70) |

**Maximum flag points - 80**

**Maximum points attainable – 80 from flags + 10 points from time bonus = 90**

**Flag format – Flag{RaNd0m\_f1ag}**

**Drill Plan**

* All the CTF players must completely fill the form and download the given **.rar** file from the GitHub Repository Link to their machines.
* All the laptops of players will be inspected before the event for modified .rar files and tools.  
  Competitors will be given total of 8 hour time to complete all the challenges.
* Evaluation of all the scores will be done and the scores will be finalized by the organizers of the event.
* The team who score the highest scores will be selected as the winning team and will receive the rewards.

**Audience**

CryX33 CTF is aimed at security professionals / employees in e-commerce industry to train, learn and create awareness on securing e-commerce web applications.

**Budget**

|  |  |
| --- | --- |
|  | **Cost LKR** |
| Cash Prizes | 15,000 |
| Hosting Venue Fees | 2,500 |
| Internet and Setting Up Costs | 5,000 |
| Marketing Cost | 10,000 |
| **TOTAL** | **32,500** |

**Business Value**

The purpose of hosting this Capture the Flag event is to ensure and test the security team within the organization as well as to spread awareness in an enjoyable way and to bring knowledge and real life experience on how to identify, handle vulnerabilities residing in e-commerce web applications by providing a safe simulation environment with vulnerable web applications which have been made specifically for e-commerce sector unlike other CTFs. This event can also pave a way to better understand security risks which could have been already residing within the organization or will help prevent future attacks and this event will also be a great opportunity to gather data and test results.

**Timeline**

