A

Mini Project Report On

# Implementation of ATTACK AND DEFENCE GAME SERVER

**Aditya Kumar Singh(RIT2013016)**

**Akash Sharan (RIT2013034)**

**Vinay Kumar Yadav (RIT2013029)**

**Atul Kumar (RIT2013019)**

**Rinchan Amo (RIT2013073)**

**B.Tech. - 5th Semester (I.T.)**

Under the Guidance of:

**Dr. Jagpreet Singh**
**I.I.I.T.-Allahabad**

## CERTIFICATE

This is to certify that the project work entitled, **“ATTACK AND DEFENCE GAME SERVER”** submitted by

ADITYA KUMAR SINGH(RIT2013016)
AKASH SHARAN (RIT2013034)
VINAY KUMAR YADAV (RIT2013029)
RINCHEN AMO (RIT2013073)
ATUL KUMAR (RIT2013019)

in partial fulfillment of the requirements of B.Tech. (IT) embodies the work done by them under my supervision.

**CHAIRPERSON** :Prof. Anupam Agarwal

SUPERVISOR : Dr. Jagpreet singh

SUPERVISOR : Prof. S. Venkatesan

SUPERVISOR : Dr. Vijay Kumar Chaurasia

SUPERVISIOR : Prof. Satyavani Guttula

# Indian Institute of Information Technology, Allahabad

## Table of Contents

## ACKNOWLEDGEMET

We are grateful to **Dr. Jagpreet Singh** for his guidance and motivation to encourage us to do this project .

Yours Sincerely,

ADITYA SINGH (RIT2013016)
AKASH SHARAN (RIT2013034)
VINAY YADAV (RIT2013029)
RINCHEN AMO (RIT2013073)
ATUL KUMAR (RIT2013019)

## ABSTRACT

Many popular and well-established cyber security Capture the Flag (CTF) exercises are held each year in a variety of settings, including universities and semi-professional security conferences. CTF formats also vary greatly, rang-ing from linear puzzle-like challenges to team-based of-fensive and defensive free-for-all hacking competitions. While these events are exciting and important as contests of skill, they offer limited educational opportunities. In particular, since participation requires considerable a pri-ori domain knowledge and practical computer security expertise, the majority of typical computer science stu-dents are excluded from taking part in these events. Our goal in designing and running the IIITA CTF was to make the experience accessible to a wider community in INDIA by providing an environment that would not only test and challenge the computer security skills of the participants, but also educate and prepare those without an extensive prior expertise. This paper describes our experience in designing, organizing, and running an education-focused CTF, and discusses our teaching methods, game design, scoring measures, logged data, and lessons learned.

## INTRODUCTION

In March of 2015, Cyber security wing of Amritapuri University organized a CTF competition on their campus to promote interest in and educate students about practical computer security. The competition was structured around defending and attacking a web application server. The target system consisted of a LAMP (Linux, Apache, MySQL, PHP) software stack and WordPress, a popular blogging plat-form [1]. In order to familiarize participants with the target system and to provide an opportunity to implement substantial solutions, a virtual machine very similar to one used during the competition was made available to the participants over a month before the competition took place. To help participants prepare for the event, we of-fered evening lectures and labs that discussed defensive and offensive techniques and tools that might be useful during the competition. The competition itself was an eighteen-hour event held over the weekend of July 12-13, during which students worked in teams of three to five to defend their instance of WordPress, while simultaneously attacking those of other teams. A scoring system pro-vided numerical measures of instantaneous and cumula-tive security, including measures of availability, integrity, confidentiality and offense. Carefully crafted but realistic vulnerabilities were introduced into WordPress at the start of the competition via ten plug-ins authored by the Lin-coln team. Since getting a high availability score required a team to run these plug-ins, participants were forced to come to terms with the very real dangers of rapidly deploying untrusted code. WordPress is famous for its extensibility, and plug-in architectures are increasingly common and popular in software engineering. A goal of the INCTF was to explore this novel computer security issue.

The event was open to all INDIAN students, without pre-requisites or a qualification round, with main motiva-tion including capturing an actual flag (we made a flag that the winning team took home), learning about practical computer security, and taking home a Rs 25000 first-place prize. Sixty-eight students registered for the event over the course of two weeks in a first-come, first-served basis. Of these, fifty-three actually formed teams, and on the day of the exercise, forty-five showed up in person at 8:30 am on a weekend to compete in the CTF.

**Participants' resp**onse to the INCTF was over-whelmingly positive. After the competition ended, we distributed a survey to ascertain the educational value of this CTF. The survey responses indicate that students learned much about practical computer security both be-fore the competition (in lectures and labs, self-study, and group activities), and during the competition itself (where the time pressures of the competition bring into sharp fo-cus theoretical computer security lessons).

## Project Outline

During the course of this project, we will do the following:

- Implement services which will contain vulnerabilities from SQL-INJECTION, XSS etc .
- Implement a ATTACK and DEFENCE GAME-SERVER which can communicate to **other team's servers.**

## Motivation

Recently we have attended two CTF events one at Microsoft-Hyderabad and other at Amritapuri University from there we get idea to host same type of event in our college which would be a great exposure to all of IIITIANS to the world of Cyber security.

## PROBLEM DEFINITION

To develop an attack and defense server which can communicate to all vulnerable image provided by us through which all teams can attack each others server which have vulnerable services through which they are going to access a string called FLAG and submit it to the GAME-SERVER which give them **offensive points as well as the team which are attacking to other team's services must have their service** up which would be handle by the game server which checks it. You attack other teams server only after you are able to up your service in the Game Arena.

## SCOPE

**It offers lessons that can't effectively be taught in a classroom. A CTF event is a playground in** which students can fail or succeed safely at computer defense, and where it is permissible to engage in attack, without fear of consequences or reprisal. We believe it is crucial for CTF events to include an offensive component, not only because students find it exhilarating, but because it also challenges flawed reasoning and assumptions in tools, techniques, and systems, and leads to a deeper understanding of computer science in general.

## LITERATURE SURVEY

Since our goal was to create not only another CTF ex-ercise, but also a pedagogic tool for teaching computer security, we incorporated several educational components, in the form of lectures and labs, into the IIITA CTF. In total, we offered five classes in the month preceding the competition.

An overview of the CTF game, its mechanics and rules. As part of this description, we presented the game platform and architecture (Linux, x86), as well as the intended target – the WordPress con-tent management system. We also explained and justified the scoring system, with suitable measures of confiden-tiality, integrity, availability and offense (see Section 5). This meeting allowed those who had not taken part in a CTF exercise before to understand the game better and ask questions.

We present the basics of web applications, the WordPress API, and some of the funda-mental ways in which its design makes computer security difficult. We did not teach PHP, JavaScript or SQL, even though WordPress makes use of all three, as these details could easily be mastered by the general computer sci-ence student in self-study. The intent was not to educate students to the point that they might go off and write a web application; rather, we hoped to orient them in this (perhaps unfamiliar) terrain, providing an overview of the target and sketching the security issues for them to consider on their own.

We also cover various aspects of Linux server security, also in lecture form. Topics ranged from high-level concepts, including the principle of least privilege, multi-layer defense and attack surface.

## EXERCISE DESIGN

This section covers design decisions made while planning the CTF and its component challenges.

### Target Selection

In order to design a CTF that carried an academic flavor, we realized that challenges based on compiled binaries would require an unacceptably large amount of prior knowledge and thus contradict our pedagogical goals laid out in Section 2. As such, we chose a CTF setting that would naturally allow the participants access to the source code of the system. An easy way to do this was to focus on web application security.

Having chosen the game genre, the next decision was selecting an open source or custom-written web application framework. We believed that the game would be more meaningful to the participants if we used realis-tic, commercial off-the-shelf (COTS) software during the CTF, since it would allow them to build reusable expertise for a popular software package that they are likely to encounter again elsewhere. With this in mind we set out to select a common web application framework that would enable our CTF to be educational, well-designed, and fun to play. After considering several candidates, the PHP-based Content Management System (CMS) Word-Press [1] was selected as the **CTF's base architecture.**

### Modular Game Design

One of the main requirements in selecting a web application framework was modularity. We needed a robust way to introduce new vulnerabilities that could be exploited by competition participants that could not be discovered by **simple source code "diff". A plug-**in architecture, especially one as flexible and extensively used as in Word-Press, allowed us to create new functionality that featured carefully crafted but realistic vulnerabilities. At the same time, this architecture enabled us to provide the participants with the basic framework (i.e., LAMP server with WordPress) ahead of the competition without revealing any details of the plug-ins we were building. Finally, separating our challenges into different plug-ins enabled easy division of labor.

Plug-ins are used extensively, particularly in web applications. We felt that the dynamics of acquiring untrusted code, examining it for potential flaws, fixing the ones that can be easily found and providing some kind of sandboxing or code isolation as a fail-safe was a realistic strategy that system administrators might employ. Formulating a game around this dynamic enabled participants to practice several important practical computer security skills, including source code auditing, fuzzing or web application penetration testing to find vulnerabilities, patching code without removing functionality, and configuring appropriate sandboxing mechanisms.

### Flag-based Metrics

Every 15 minutes, flags (128-character alphanumeric strings) were deposited into the file **system and database on each team's server. If opposing teams captured these flags, they** could submit them to the scoreboard system. Flags were assigned a point value corresponding to the perceived difficulty and level of access needed to acquire the flag. By providing flags of varying difficulty, we hoped that teams try to escalate privilege to gain higher levels of access than those afforded by the more basic exploits available in the game. Following the insertion of flags into each system, the scoring bot would wait a random period and check whether the flags were unaltered.

### Selecting Participants

Given the open nature of the CTF, we did not require any qualifications of our participants, aside from being enrolled in an undergraduate or graduate level pro-gram at a Boston-area university and willingness to spend the weekend competing in the CTF. We encouraged participants to form teams of at least three members, as we felt that competing with fewer people would put the team at a significant disadvantage. Our resulting participant pool was comprised of undergraduates from Indian Colleges, divided into (some multi-institutional) teams of three to five members.

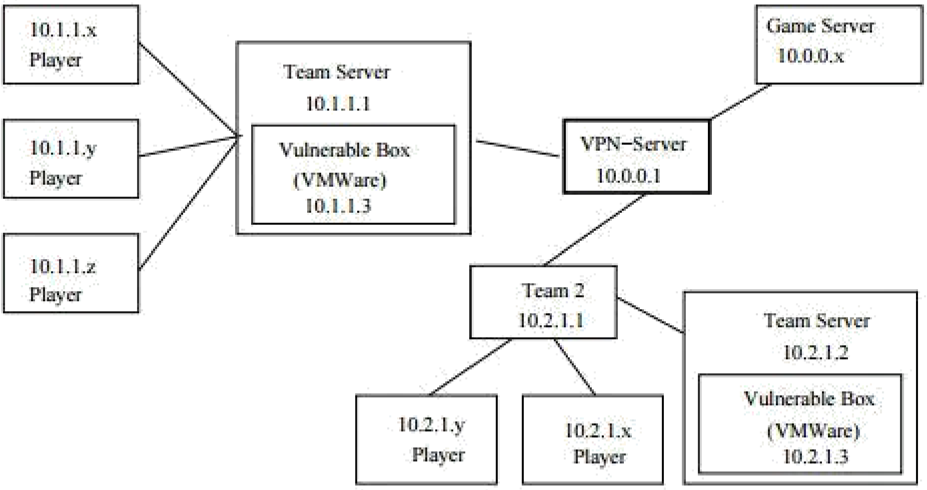


**Fig. 1.** An example network layout, using a central VPN-node

## Hardware and Software Components

Hardware : Computer Systems

Software : Operating System (Linux: Ubuntu)

Language : C language, Socket Programming

Libraries : ISO C library (C standard library), socket libraries.

## ACTIVITY TIME CHART

| Activity | Start-Date | End-Date |
|---|---|---|
| Project start | 8-11-2015 | 18-11-2015 |
| Discuss with other team mate | 9-11-2011 | 18-11-2015 |
| Write three services | 12-11-2015 | 12-11-2015 |
| Make virtual machine of Services | 13-11-2015 | 13-11-2015 |
| write code of scoreboard and submission of flag | 14-11-2015 | 14-11-2015 |
| write report | 18-11-2011 | 18-11-2015 |

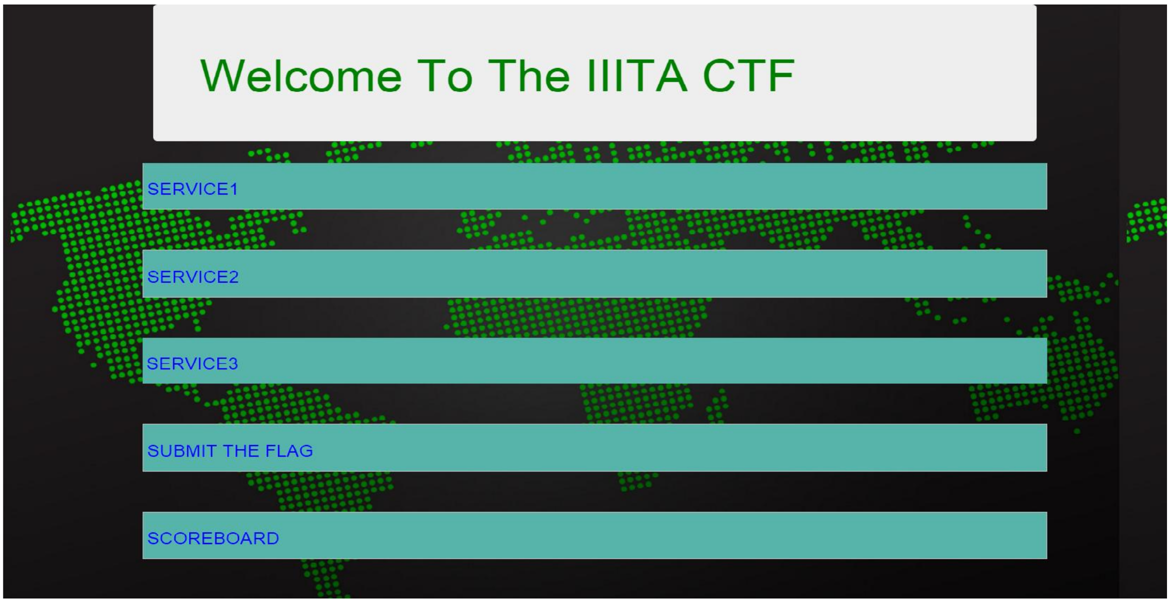
## Submission Of Flags (source code of webpage)

```
<?php
error_reporting(E_ALL ^ E_DEPRECATED);
$servername ="localhost"
```

```
$password = "";
$database="game_server";
$tbl_name="flag";
$conn=mysql_connect($servername , $username , $password);
if(!$conn)
{
        echo "DATABASE ERROR";
}
$db=mysql_select_db($database, $conn);
session_start();
// Include database connection settings
if($db)
{
       $a=$_POST['team_no'];
       $b = $_POST['flag'];
      $login = mysql_query("SELECT * FROM flag WHERE  flag_1 = '$b'");
if (mysql_num_rows($login) == 1)
 {
       $query=" UPDATE score SET service_1 = 100 WHERE team_no ='$a';";
       $result=mysql_query($query);
       $e1 = mysql_query("select service_1 where team_no = '$a';");
      $e2 = mysql_query("select service_2 where team_no = '$a';");
      $e3 = mysql_query("select service_3 where team_no = '$a';");
      $q=" UPDATE score SET total = service_1 +  service_2 + service_3 WHERE team_no
='$a';";
      $r=mysql_query($q);
 echo "<h1>connected</h1>";
 header('Location: scoreboard.php');
 }
```

```
$login = mysql_query("SELECT * FROM flag WHERE  flag_2 = '$b'");
if (mysql_num_rows($login) == 1)
 {
      $query=" UPDATE score SET service_2 = 100 WHERE team_no ='$a';";
      $result=mysql_query($query);
      $e1 = mysql_query("select service_1 where team_no = '$a';");
      $e2 = mysql_query("select service_2 where team_no = '$a';");
      $e3 = mysql_query("select service_3 where team_no = '$a';");
     $q=" UPDATE score SET total = service_1 + service_2 + service_3 WHERE team_no
='$a';";
   $r=mysql_query($q);
echo "<h1>connected</h1>";
header('Location: scoreboard.php');
 }
 $login = mysql_query("SELECT * FROM flag WHERE  flag_3 = '$b'");
if (mysql_num_rows($login) == 1)
 {
    $query=" UPDATE score SET service_3 = 100 WHERE team_no ='$a';";
    $result=mysql_query($query);
   $e1 = mysql_query("select service_1 where team_no = '$a';");
   $e2 = mysql_query("select service_2 where team_no = '$a';");
   $e3 = mysql_query("select service_3 where team_no = '$a';");
   $q=" UPDATE score SET total = service_1 + service_2 + service_3 WHERE team_no ='$a';";
   $r=mysql_query($q);
   echo "<h1>connected</h1>";
  header('Location: scoreboard.php');
 }
}
if (mysql_num_rows($login) != 1)
{
```

```
                                        header('Location: error.html');

}

?>
```

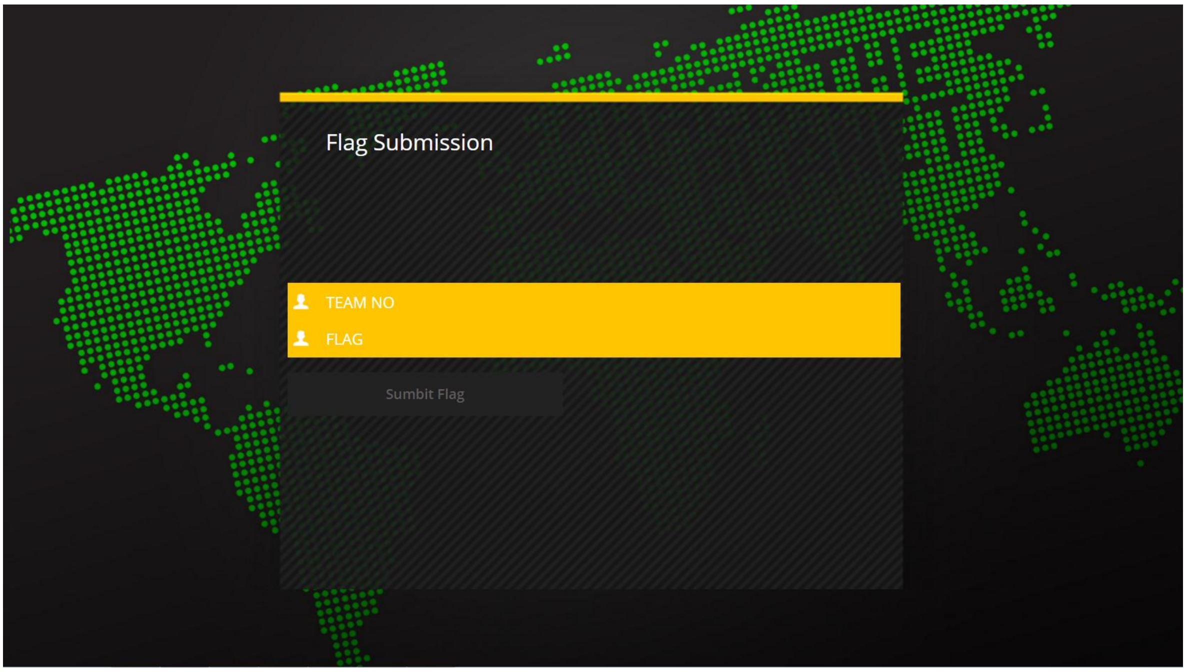


Welcome To The IIITA CTF

## Index (source code of webpage)

```
<!DOCTYPE html>

<html>

<head>

<title>Flag Submission</title><meta charset="utf-8"><link href="css/style.css" rel='stylesheet'
type='text/css' />

<meta name="viewport" content="width=device-width, initial-scale=1">

<script type="application/x-javascript"> addEventListener("load", function()

{

 setTimeout(hideURLbar, 0); }, false); function hideURLbar()

{

 window.scrollTo(0,1);

 }
 </script>
<!--webfonts-->
<link
href='http://fonts.googleapis.com/css?family=Open+Sans:600italic,400,300,600,700'rel='stylesheet'
type='text/css'>
<!--//webfonts-->
</head>

<body><!-----start-main----><div class="login-form">
<h1>Flag Submission</h1>
<form method="post" action="submit_flag.php">
<li>
<input type="text"  name ="team_no" class="text" value="TEAM NO" onfocus="this.value = '';"
onblur="if (this.value == '') {this.value = 'TEAM NO';}" >
<a href="#" class=" icon user">
</a>
 <input type="text"  name ="flag" class="text" value="FLAG" onfocus="this.value = '';" onblur="if
(this.value == '') {this.value = 'FLAG';}" ><a href="#" class=" icon user">
</a>
</li>
<input type="submit" onclick="myFunction()" value="Sumbit Flag" >
</h4>
 </form>
 </div>
<!--//End-login-form-->
<div class="ad728x90" style="text-align:center">
<script async src="//pagead2.googlesyndication.com/pagead/js/adsbygoogle.js">
</script>
<!-- w3layouts_demo_728x90 -->
<ins class="adsbygoogle" style="display:inline-block;width:728px;height:90px" data-ad-client="ca-
pub-9153409599391170" data-ad-slot="8639520288">
</ins>
<script>
```

```
(adsbygoogle = window.adsbygoogle || []).push({});
</script>
 </div>
  <!-----start-copyright---->
<!-----//end-copyright---->


</body>
</html>
```

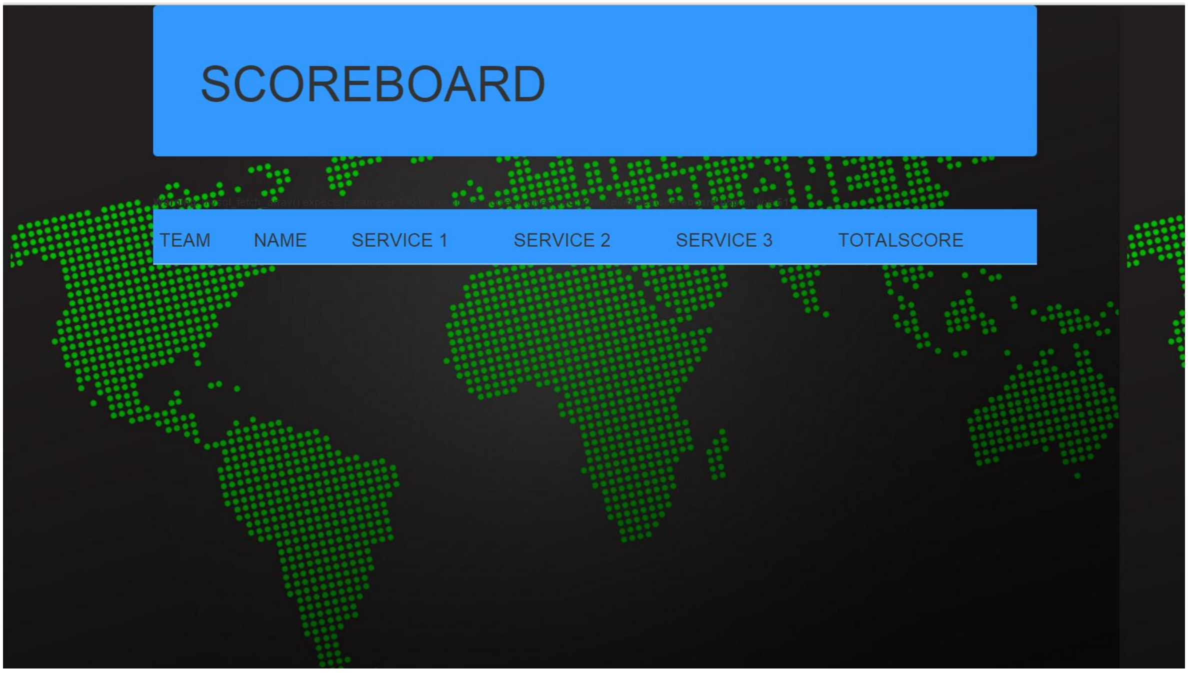


# Scoreboard (source code of webpage)

```
<!doctype html>

<html lang="en">

<head>

  <meta charset="UTF-8">

  <link href="css/table.css" rel='stylesheet' type='text/css' />

   <meta charset="utf-8">

  <meta name="viewport" content="width=device-width, initial-scale=1">

  <link rel="stylesheet" href="http://maxcdn.bootstrapcdn.com/bootstrap/3.3.5/css/bootstrap.min.css">

  <script src="https://ajax.googleapis.com/ajax/libs/jquery/1.11.3/jquery.min.js"></script>

  <script src="http://maxcdn.bootstrapcdn.com/bootstrap/3.3.5/js/bootstrap.min.js"></script>

<style>

.jumbotron {

    position: relative;

    background: #3399FF url("jumbotron-bg.png") center center;

    width: 100%;

    height: 100%;

    background-size: cover;

    overflow: hidden;

}

.table {

    position: relative;

    background: #3399FF url("jumbotron-bg.png") center center;

    width: 100%;

    height: 100%;

    background-size: cover;

    overflow: hidden;

}
```

```
</style>

</head>
<body background="images/bg.jpg">

<div class="container">
 <div class="jumbotron">
  <h1 col>SCOREBOARD</h1>
 </div>
  <?php
              echo "<table class= 'table' >

  <thead>
   <tr>
    <th><h3>TEAM</h3></th>
    <th><h3>NAME </h3></th>
    <th><h3>SERVICE 1</h3></th>
    <th><h3>SERVICE 2</h3></th>
               <th><h3>SERVICE 3</h3></th>
    <th><h3>TOTALSCORE</h3></th>
   </tr>
  </thead>";

              error_reporting(E_ALL ^ E_DEPRECATED);
   $connection = mysql_connect('localhost', 'root', ''); //The Blank string is the password
mysql_select_db('game_server');

$query = "SELECT * FROM score  ORDER BY total DESC"; //You don't need a ; like you do in SQL
$result = mysql_query($query);
echo "<div class='table-responsiv'> ";
//echo "<table class = 'table'>"; // start a table tag in the HTML
```

```
while($row = mysql_fetch_array($result)){   //Creates a loop to loop through results

echo "<tr class='danger' bordercolor= '#000000'  ><td>" . $row['team_no'] . "</td><td>" .
$row['name'] . "</td><td>" . $row['service_1'] . "</td><td>" . $row['service_2'] . "</td><td>" .
$row['service_3'] . "</td><td>" . $row['total'] . "</td></tr>";  //$row['index'] the index here is a field
name

}


echo "</table>"; //Close the table in HTML

echo "</div>";

mysql_close(); //Make sure to close out the database connection

?>

</table>

   </body>

   </html>
```



SCOREBOARD

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in C:\xampp\htdocs\[illegible]scoreboard.php on line 61

| TEAM | NAME | SERVICE 1 | SERVICE 2 | SERVICE 3 | TOTALSCORE |
|---|---|---|---|---|---|

## CONCLUSION

The CTF competition would be a great learning experience both for the students involved and for the organizers. We believe that this exercise helped the students understand the intricacies of practical computer security, highlighted their strengths and weaknesses in computer security skills and generally increased their interest and desire to learn more about this area. We plan to continue fostering this community by encouraging creation of read-ing groups focused on practical computer security and by running similar CTF competitions in **the upcoming years, incorporating the feedback from this year's participants**

## REFERENCES

We would like to thank the anonymous reviewers and INCTF team who inspires us for such a great project which involve learning, fun and hacking skills too.

### References

[1] WordPress: Blog tool and publishing platform. http://www.wordpress.org.

[2] **S. Bratus. What hackers learn that the rest of us don't: Notes on hacker curriculum. IEEE Security** and Privacy, 5(4):72–75, 2007.

[3] http://inctf.in

[4] https://buildtheshield.microsoft.com/

[5] https://people.csail.mit.edu/nickolai/papers/werther-llctf.pdf

[6] https://events.ccc.de/congress/2005/fahrplan/attachments/562-Paper_HostingAHackingChallenge.pdf