Challenge Name: Insp3ct0r

Category: Web Exploitation

AUTHOR: ZARATEC/DANNY

Description

Kishor Balan tipped us off that the following code may need inspection: https://jupiter.challenges.picoctf.org/problem/51418/

Hint 1: How do you inspect web code on a browser?

Hint 2: There's 3 parts

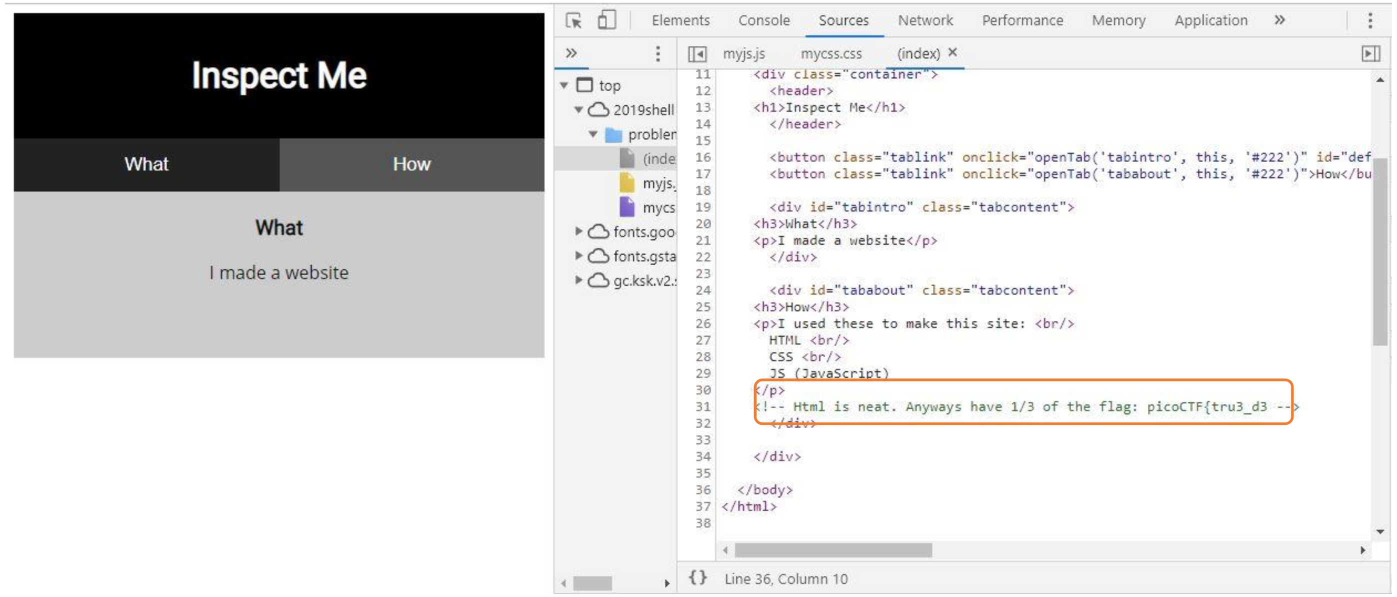
https://play.picoctf.org/practice/challenge/18

Learning outcome : Web Programming and Debug Tool

*In general a web page involves 3 types of files, e.g. html (content), css (presentation) and js (enhance interactive). This challenge require student to understand **web programming concept** and how to use **debug source code** in browser*

Solution

1. Use **Inspect Element** option in Chrome browser
2. Go to the Source tab and view the index.html, mycss.css, and myjs.js files
3. Each containing a part of the flag. The answer is “**picoCTF{tru3_d3t3ct1ve_0r_ju5t _lucky?9df7e69a}**”



Inspect Me

What

How

What

I made a website

```
    <div class="container">
      <header>
    <h1>Inspect Me</h1>
      </header>

      <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="def
      <button class="tablink" onclick="openTab('tababout', this, '#222')">How</bu

      <div id="tabintro" class="tabcontent">
    <h3>What</h3>
    <p>I made a website</p>
      </div>

      <div id="tababout" class="tabcontent">
    <h3>How</h3>
    <p>I used these to make this site: <br/>
      HTML <br/>
      CSS <br/>
      JS (JavaScript)
    </p>
    <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
      </div>

    </div>

  </body>
</html>
```

Line 36, Column 10

https://github.com/kevinjycui/picoCTF-2019-writeup/tree/master/Web Exploitation/Insp3ct0r

挑戰名稱: Insp3ct0r

類別: Web Exploitation

作者: ZARATEC/DANNY

描述

你們可能需要檢示一下以下的代碼：

https://jupiter.challenges.picoctf.org/problem/51418/

提示 1: 您如何在瀏覽器上檢示網頁原始碼？

提示 2: 旗幟共由 3 個部份組成

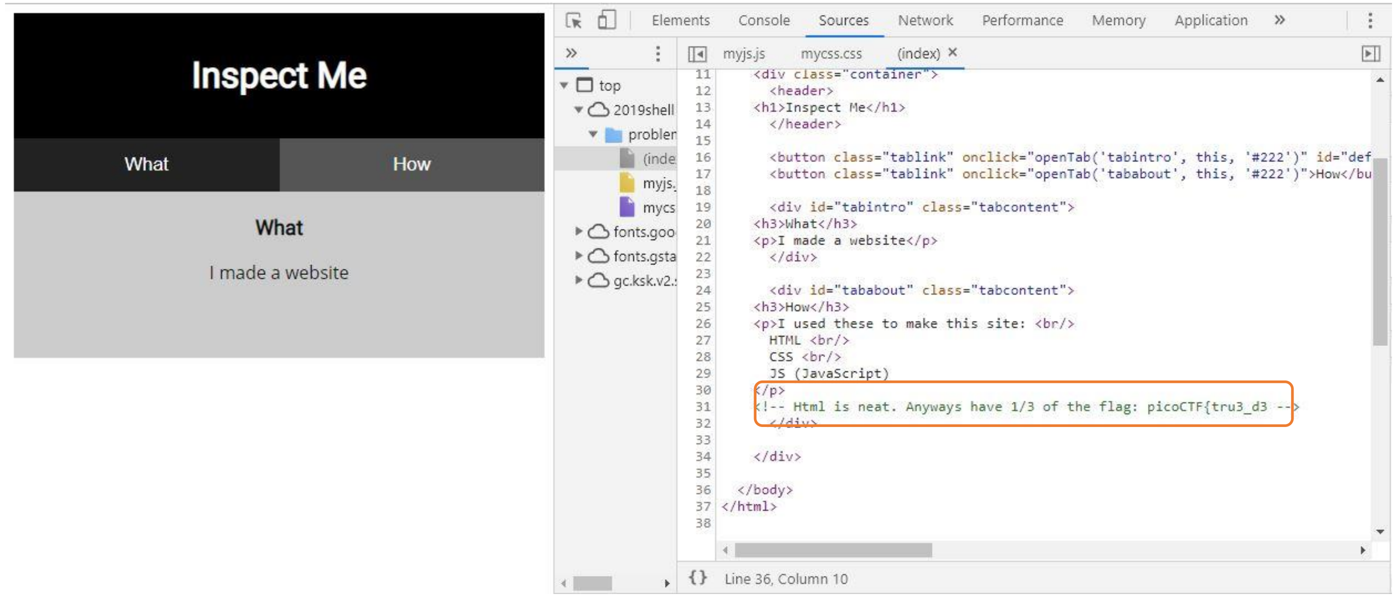
https://play.picoctf.org/practice/challenge/18

可以學習到: 網頁程式 及 除錯工具

*一般來說，網頁包括3 種類型的文件，例如html（內容），css（演示）和js（增強互動性）。 這一個挑戰要求學生了解**網頁編程概念**以及如何在瀏覽器中使用**除錯源代碼工具**。*

解題

1. 在瀏覽器中使用檢示元素選項 或 檢示原始碼
2. 檢示 index.html, mycss.css, 及 myjs.js 文件
3. 每個文件都包含一部份旗幟。所得的旗幟是：“**picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?9df7e69a}**”



```
    <div class="container">
      <header>
    <h1>Inspect Me</h1>
      </header>

      <button class="tablink" onclick="openTab('tabintro', this, '#222')" id="def
      <button class="tablink" onclick="openTab('tababout', this, '#222')">How</bu

      <div id="tabintro" class="tabcontent">
    <h3>What</h3>
    <p>I made a website</p>
      </div>

      <div id="tababout" class="tabcontent">
    <h3>How</h3>
    <p>I used these to make this site: <br/>
      HTML <br/>
      CSS <br/>
      JS (JavaScript)
    </p>
    <!-- Html is neat. Anyways have 1/3 of the flag: picoCTF{tru3_d3 -->
      </div>

    </div>

  </body>
</html>
```

Line 36, Column 10

https://github.com/kevinjycui/picoCTF-2019-writeup/tree/master/Web Exploitation/Insp3ct0r

Challenge Name: Irish-Name-Repo 1

Category: Web Exploitation

AUTHOR: CHRIS HENSLER

Description

There is a website running at https://jupiter.challenges.picoctf.org/problem/51593/. Do you think you can log us in? Try to see if you can login!

Hint 1: There doesn't seem to be many ways to interact with this. I wonder if the users are kept in a database?

Hint 2: Try to think about how the website verifies your login.

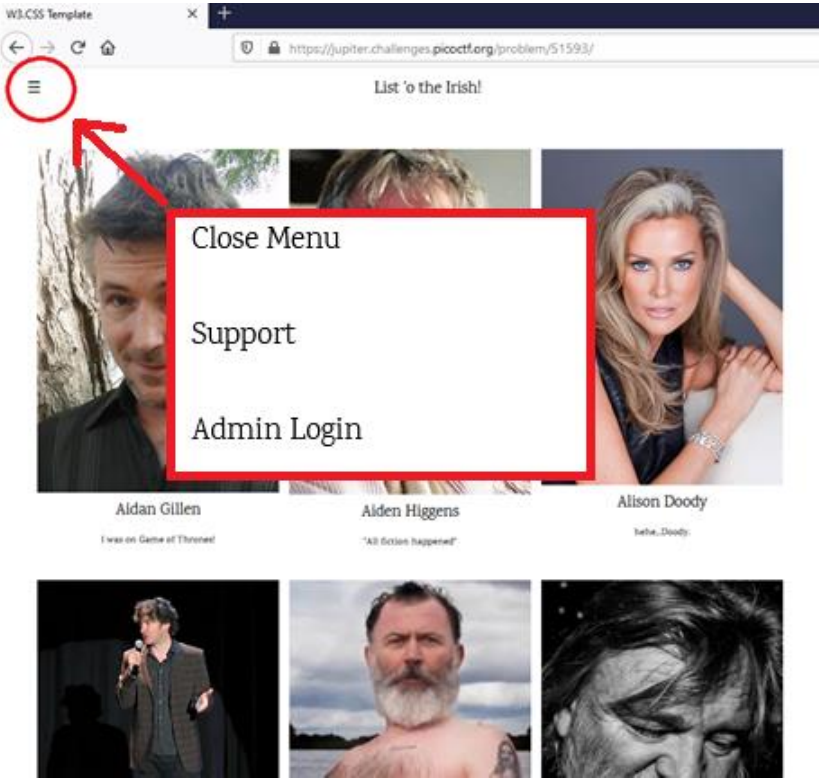
https://play.picoctf.org/practice/challenge/80?category=1&page=1

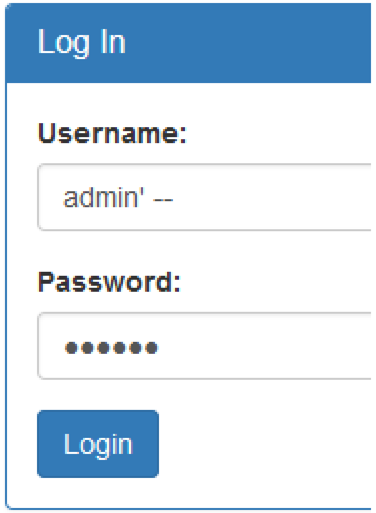
Learning outcome : Analysis skill and SQL injection

Some programmer may finish the program without testing, it may produce some bug

Solution

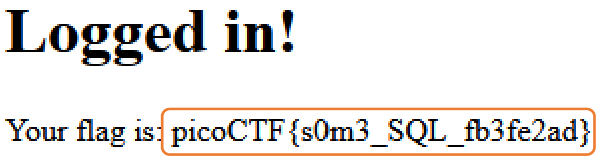
1. **Analysis the webpage**, and you may notice there are a “admin login” hidden in the option (Red circle)
2. Use **SQL injection attack** (Type “admin’ - -” in the username, and what ever you type the password.)
3. You can **login as admin** and get the flag.
4. The answer is “**picoCTF{s0m3_SQL_fb3fe2ad}**”




Log In

Username: admin' --

Password: ••••••


Logged in!

Your flag is: picoCTF{s0m3_SQL_fb3fe2ad}

挑戰名稱: Irish-Name-Repo 1

類別: Web Exploitation

作者: CHRIS HENSLER

描述

這裡有個網站 https://jupiter.challenges.picoctf.org/problem/51593/. 你認為你可以登入到嗎？試一下吧。

提示 1: 網站中好像沒有太多提示，不知用戶資料是否儲存在資料庫呢？

提示 2: 嘗試用網頁的層面思考一下，它是如何認證你的登入？

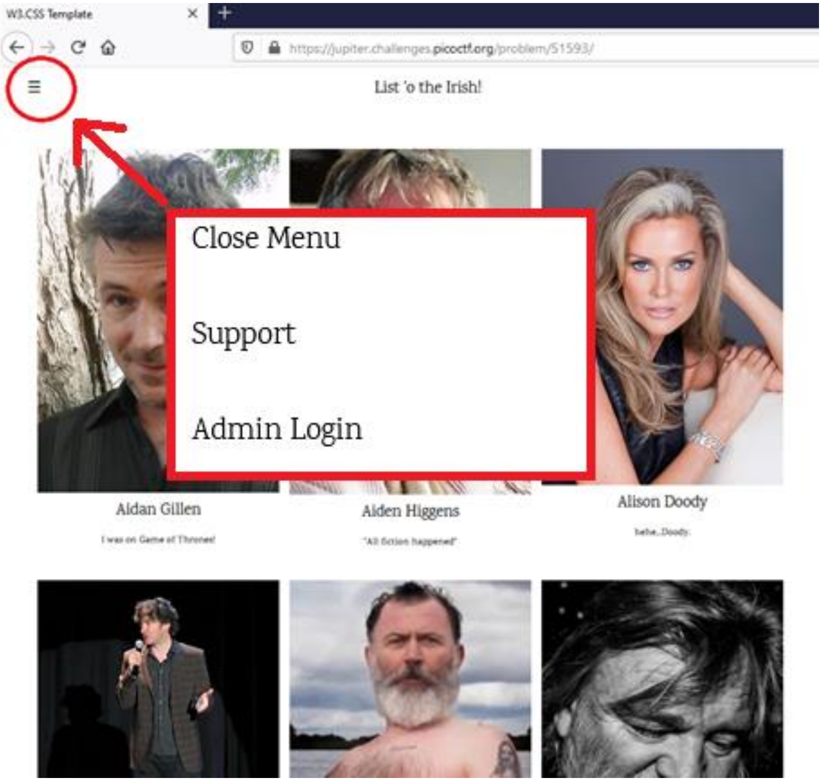
https://play.picoctf.org/practice/challenge/80?category=1&page=1

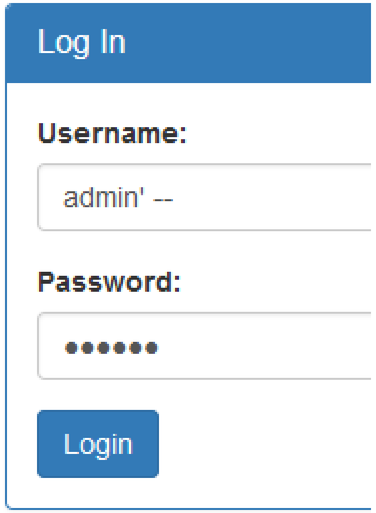
可以學習到: 分析能力 及 SQL 代碼注入

有些程式編寫員在完成程式時沒有進行測試，因而產生一些漏洞

解題

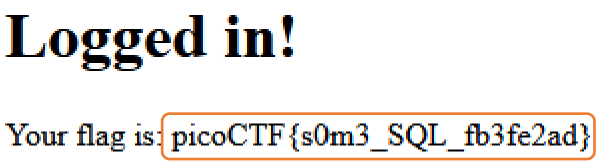
1. **分析網頁**，你應該可以留意到管理員登入是隱藏在選項中（紅圈）
2. 注入 **SQL 代碼**（在登入名種中輸入 “admin’ - -” 並隨便輸入密碼）
3. 你就可以 **登入為管理員**並得到旗幟。
4. 所得的旗幟是：**“picoCTF{s0m3_SQL_fb3fe2ad}”**




Log In

Username: admin' --

Password: ●●●●●●


Logged in!

Your flag is: picoCTF{s0m3_SQL_fb3fe2ad}