Название задания: Insp3ct0r

Категория:Веб эксплуатация

Автор: ZARATEC/DANNY

Описание

Кишор Балан оповестил нас, что нужно проверить следующий код
Проверить: https://jupiter.challenges.picoctf.org/problem/51418/

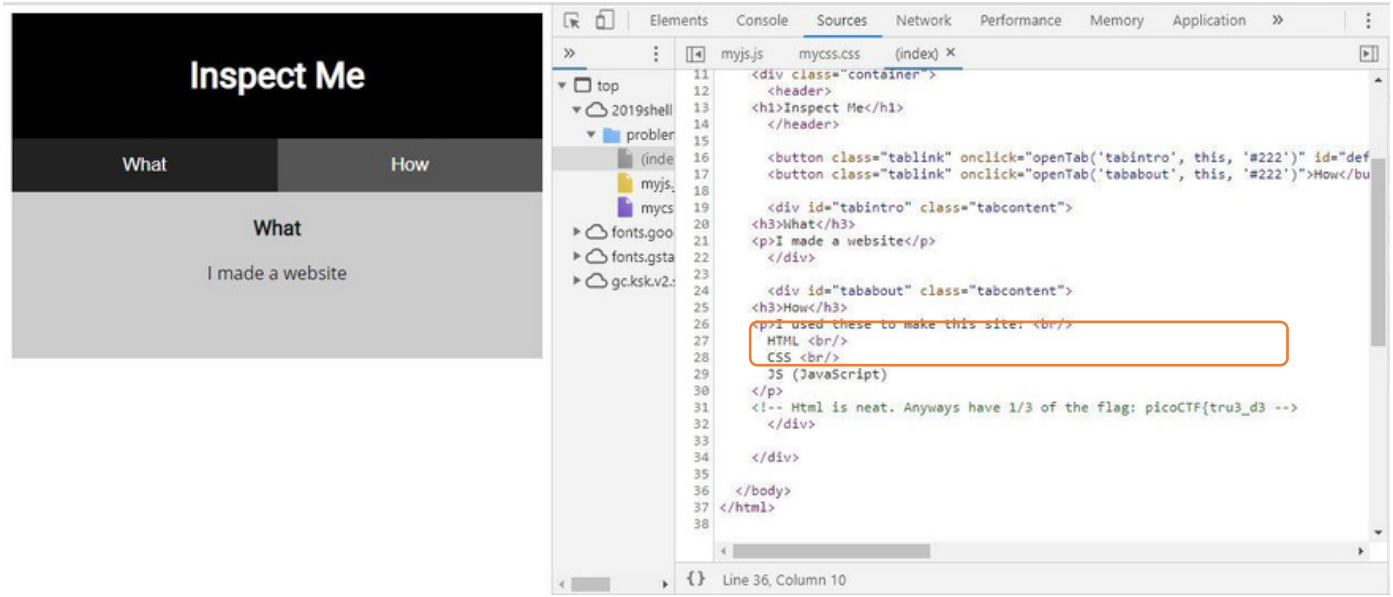
Подсказка 1: Как вы проверяете веб-код в браузере?

Подсказка 2: Здесь три части

Результат обучения: Веб-программирование и инструмент для отладки

Как правило, веб-страница включает в себя файлы 3 типов, например html (контент), css (презентация) и js (повышение интерактивности). Это задание требует от студента понимания концепции веб-программирования и того, как использовать исходный код для отладки в браузере

Решение



1. Используйте опцию проверки элемента в Chrome браузере
2. Перейдите на вкладку Source и просмотреть index.html, mycss.CSS и myjs.js файлы
3. Каждый из них содержит часть флага.

Ответ таков:

“**picoCTF{tru3_d3t3ct1ve_0r_ju5t_lucky?9df7e69a}**”

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

Название задания: Irish-Name-Repo 1

Категория: Веб эксплуатация

Автор: CHRIS HENSLER

Описание

Есть веб-сайт, работающий по адресу https://jupiter.challenges.picoctf.org/problem/51593/. Как вы думаете, сможете ли вы авторизоваться на нас? Попробуйте проверить!

Подсказка 1: Похоже, существует не так много способов взаимодействия с этим. Интересно, хранятся ли пользователи в базе данных?
Подсказка 2: Попробуйте подумать о том, как веб-сайт проверяет ваш логин.

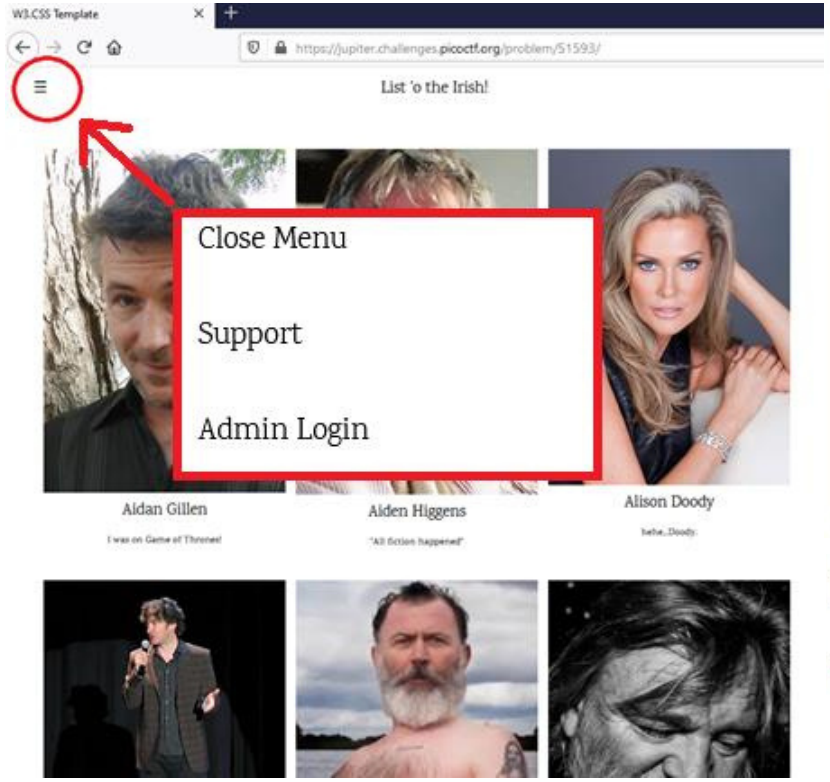
https://play.picoctf.org/practice/challenge/80?category=1&page=1

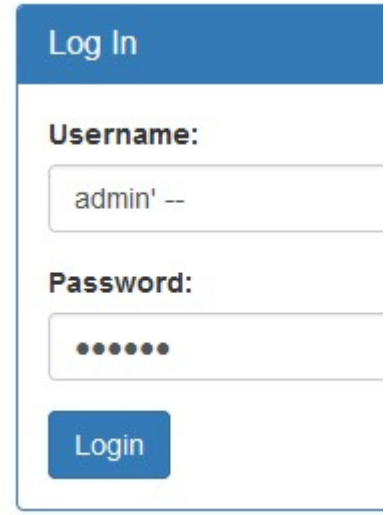
Результат обучения: Навыки анализа и SQL-инъекции

Какой-нибудь программист может завершить программу без тестирования, это может привести к какой-нибудь ошибке

Решение

1. **Проанализируйте веб-страницу,** и вы можете заметить , что в опции скрыт “вход администратора” (красный кружок).
2. Используйте атаку **SQL-инъекцией** (введите “admin’ - -” в имени пользователя и в любом другом месте, где вы вводите пароль.)
3. Вы можете войти в систему как администратор и получить флаг.





Logged in!

Your flag is: picoCTF{s0m3_SQL_fb3fe2ad}