CTF uppgift: The Cryptic Website

Gustav Löfqvist V210S

Uppgiften utmanar deltagarna att ‘hacka’/modifiera en webbplats för att hitta ett doldt python-skript. Deltagarna måste använda ledtrådar på webbsidan och sina kunskaper inom webbhantering och Python-programmering för att lösa de olika stegen och avslöja den gömda flaggan. Genom att inspektera källkoden, identifiera en nyckel och använda den för att dekryptera en gömd Python-kod, kommer deltagarna närmare lösningen på uppgiften. Uppgiften är utformad för att vara en lagom utmaning för nybörjare inom säkerhet och CTF.

**Lösningsförslag:**

Uppgiften går själklart att lösa på flera olika sätt men här är ett förslag:

1. Deltgarana besöker webbsidan och tar hjälp utav ledtrådarna för att ta sig vidare till nästa steg.
2. Med hjälp av ledtrådarna listar deltagarna ut att de beöhver besöka hemsidans källkod och de öppnar ‘inspect element’.
3. Efter att ha letat runt i inspectelement och hittat meddelanden I bland annat <Head> och <Body> så borde deltagarna hittat en python-script alt ‘banana’ class.
4. Studerar vi den här klassen kan vi modifera dess css och därmed extrahera ett python script. Python scriptet kommer gå att köra utan bekymmer men för att kunna hämta ut flaggan behöver deltagaren identifiera en key.
5. Scriptets key är ‘banana’ och det hintas på överallt i hemisdan. Efter att ha matat in det så går deltagaren ut rätt flagga.

**Svårighetsgrad:** 0.7 (ca 70% som borde kunna lösa uppgiften)

Uppgiften kräver grundläggande kunskaper inom python och webbhanterring. Det är något som alla borde ha bemästrat. Det kårngliga skulle kunna vara kombinationen av dessa kunskaper. Uppgiften är lagom för nybörjare inom säkerhet och CTF.

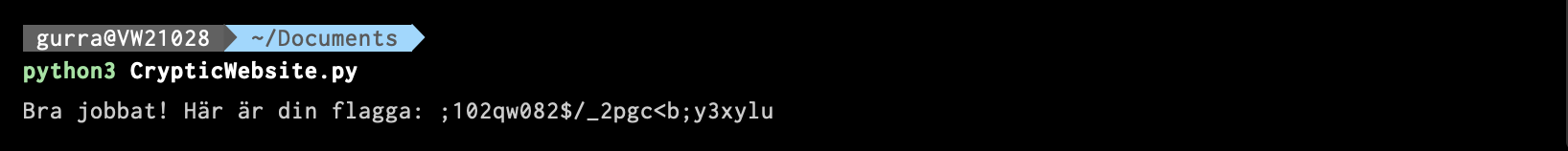
A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Här kan vi se hur man exempelvis skulle kunna manipulera hemsidans källkod för att få fram den gömda python koden. Om vi kör pythonprogramet får vi outputen nedan:



Vi behöver justera python kodens secret till ‘banana’. A computer screen shot of a code

Description automatically generated

Genom att ta hjälp från hemisdans hints får vi fram key till banana och därmed printar pythonkoden ut rätt nyckel.

A screenshot of a computer program

Description automatically generated