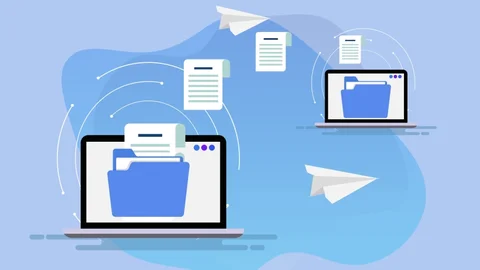
# **CTF Topic: Uploading Files**



# **Introduction**



Users can upload files to a website if there is no proper validation in place to prevent the user from executing code in the website. In this CTF you will be asked to execute a code in the victim website which eventually plays an audio in the victim website.

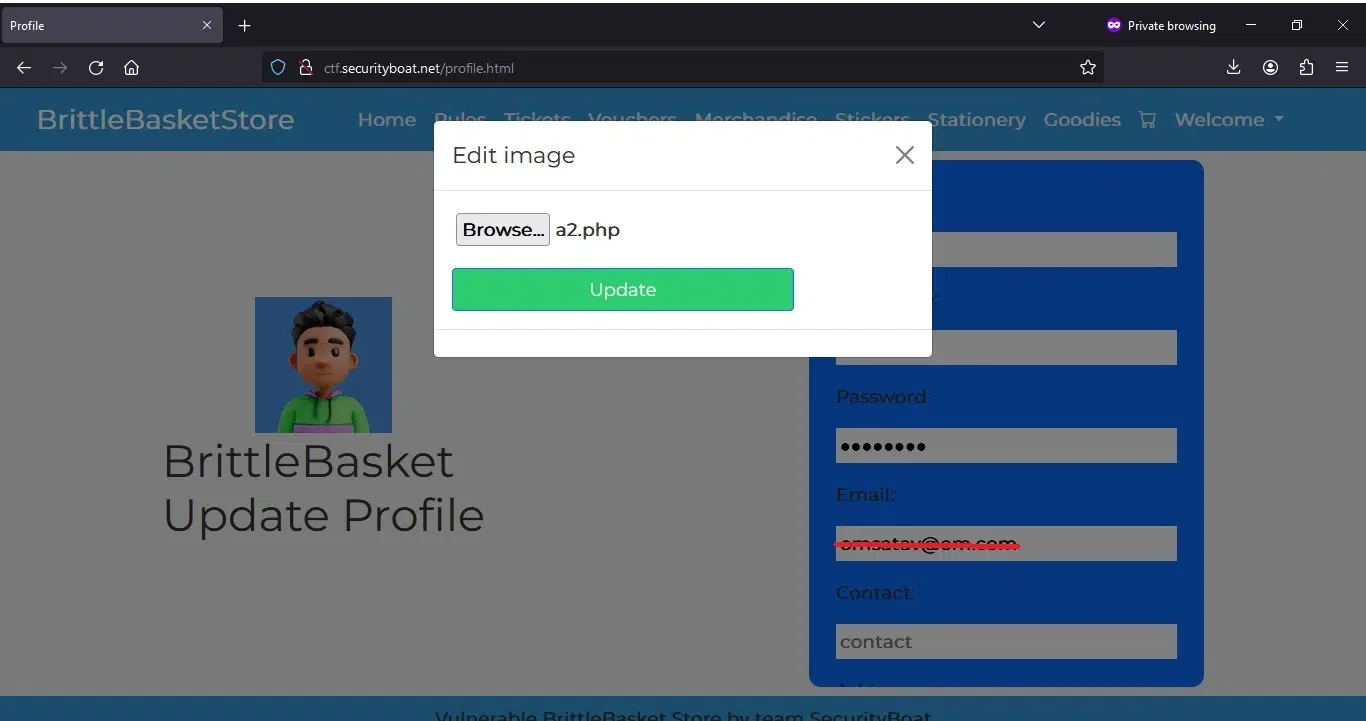
**Tools and requirement**

* Juice Shop
* File Uploading Payload knowledge

# **Link**

<https://juice-shop.herokuapp.com/#/search>

# **Scenario**



You are required to inject an audio file : OWASP Juice Shop Jingle into the OWASP Juice Shop website using javascript.

# **Process**

Step 1: Goto the owasp juice shop website: <https://juice-shop.herokuapp.com/#/>

Step 2: Tap on the search bar and paste this: <iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="<https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true>"></iframe>

# **Question**

Flag 1 : What HTML tag is the code written in?

Answer : iframe

Flag Captured

Flag 2 : Where did you insert the javascript code?

Answer : SearchBar

Flag Captured.

Flag 3 : What syntax was used to declare the source of the audio file?

Answer : src

Flag Captured.

# **Hint**

<iframe width="100%" height="166" scrolling="no" frameborder="no" allow="autoplay" src="<https://w.soundcloud.com/player/?url=https%3A//api.soundcloud.com/tracks/771984076&color=%23ff5500&auto_play=true&hide_related=false&show_comments=true&show_user=true&show_reposts=false&show_teaser=true>"></iframe>



