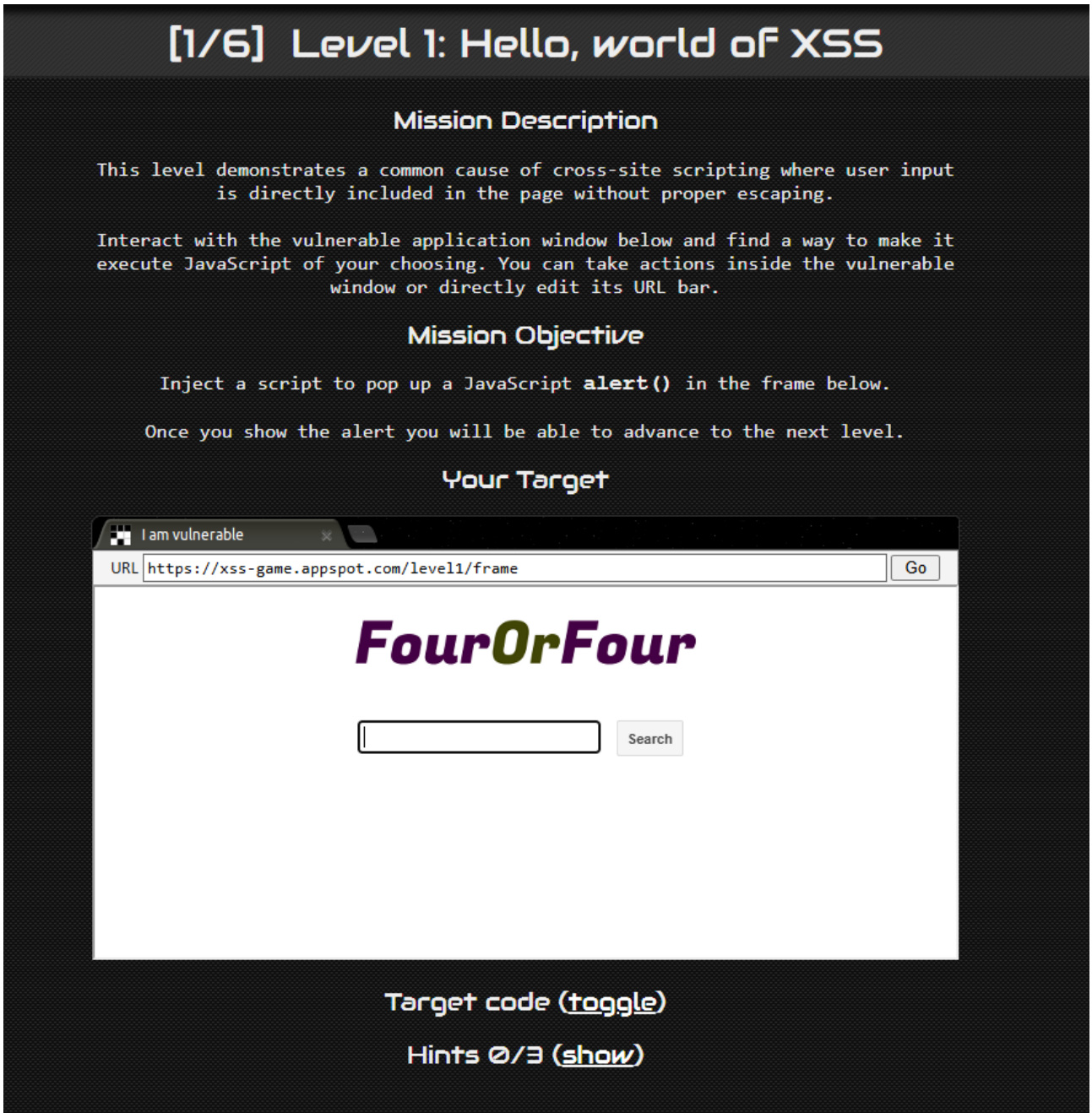
Esercizio extra attacchi XSS (Cross-Site Scripting)

Livello 1

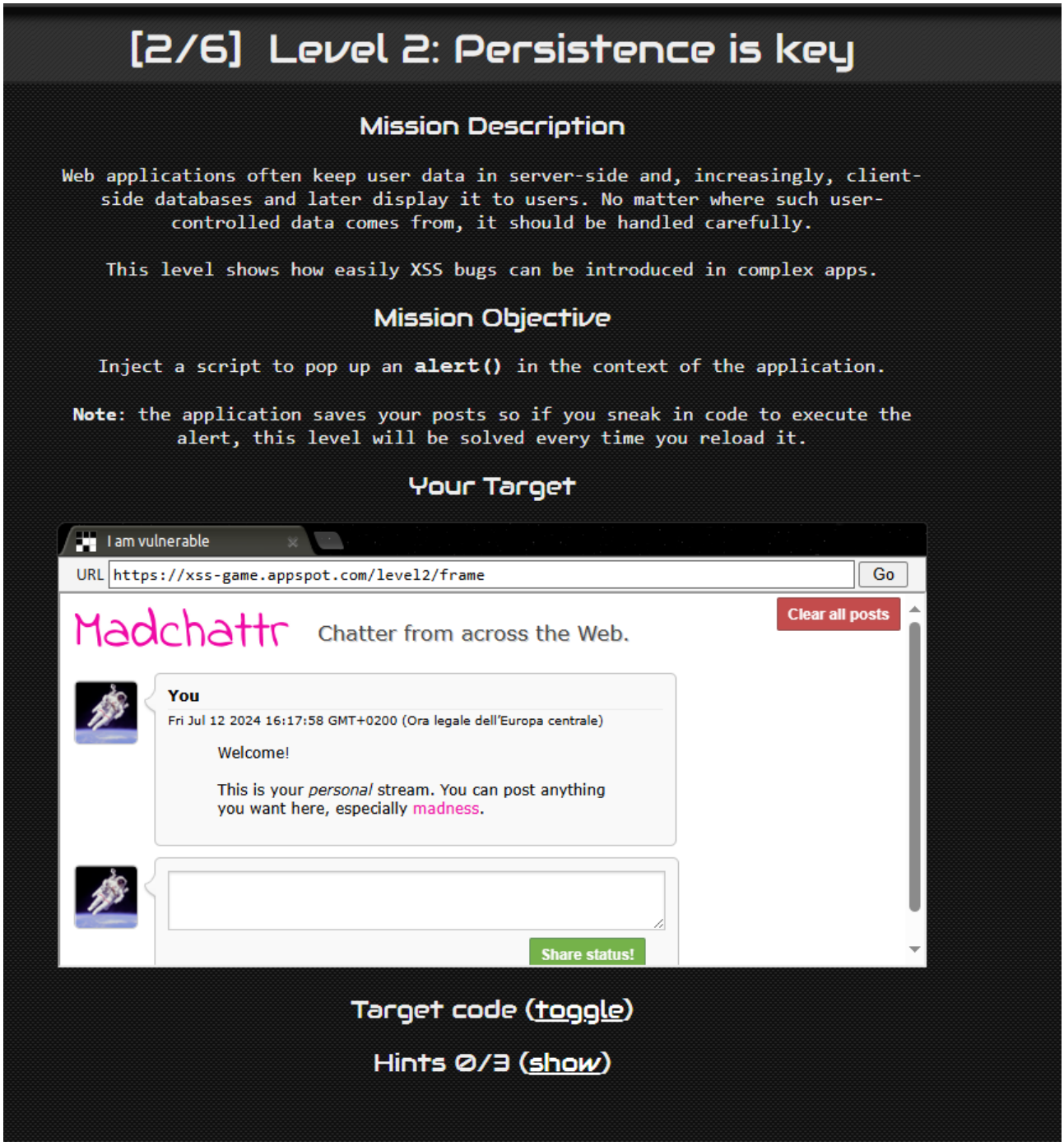


Per superare questo livello basta semplicemente scrivere un piccolo script come:

<script> alert('attacco in corso')</script>

Nella barra di ricerca e l'attacco xxs andrà a buon fine

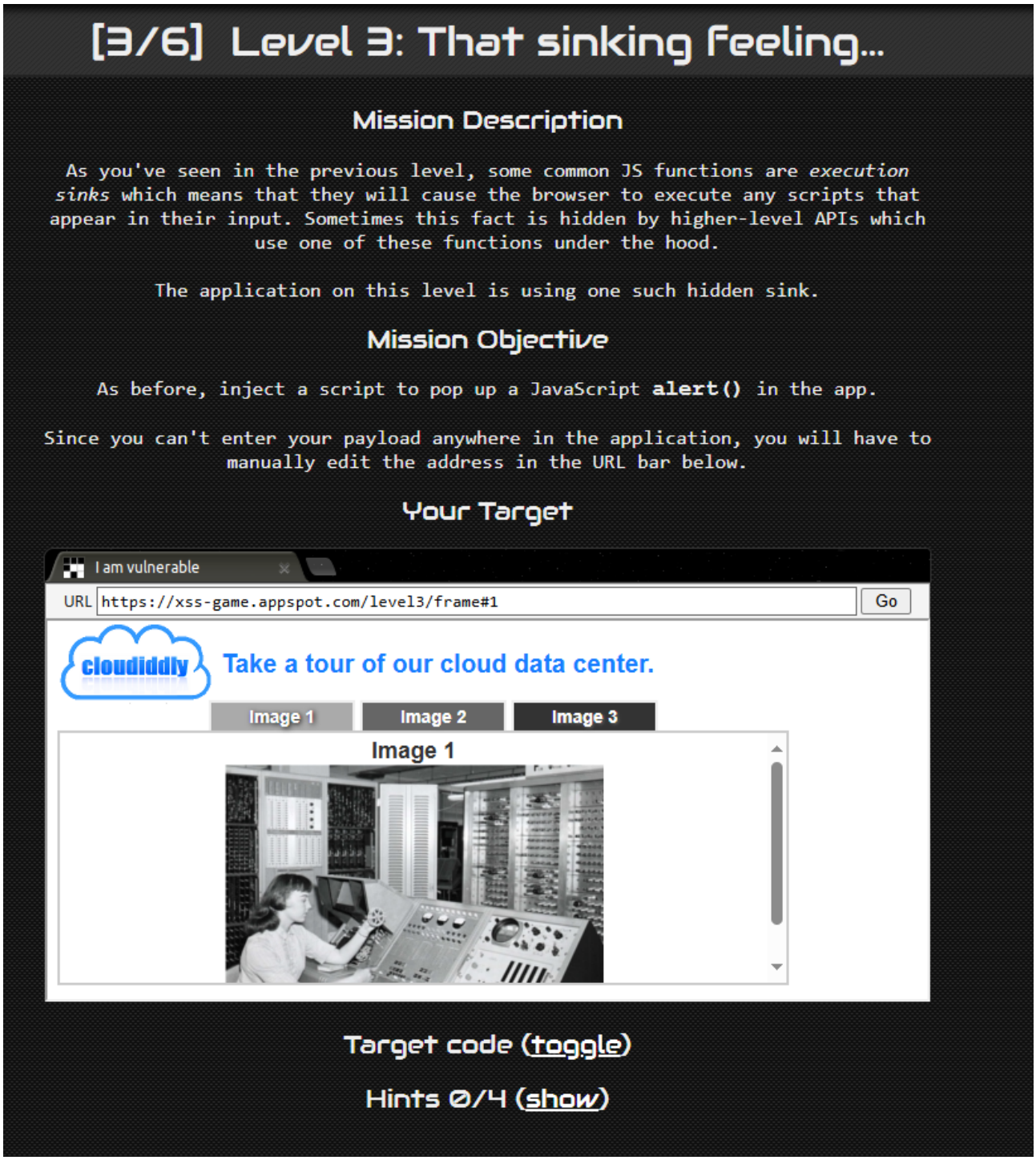
Livello 2



Per superare il secondo livello non basta un semplice script come prima ma bisognerà cambiare tattica useremo “img” questa tecnica sfrutta il fatto che un browser eseguirà il codice JavaScript associato all'attributo “one error” quando non riesce a caricare l'immagine specificata. Possiamo infatti superare il livello usando una stringa del tipo:

<img src='immagine' onerror="alert('attacco in corso")">

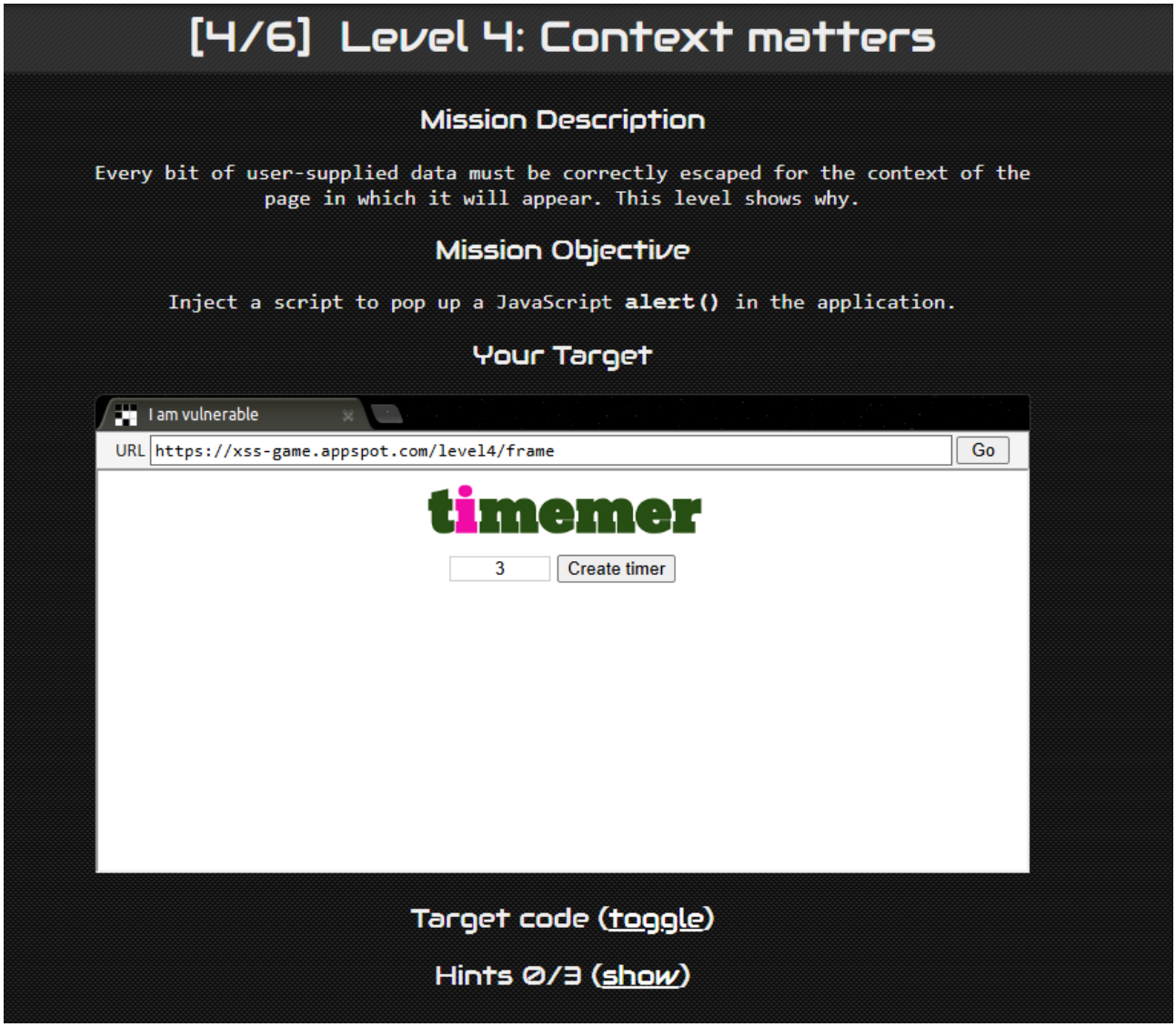
Livello 3



Per superare questo livello dobbiamo procedere in modo simile al precedente. Come possiamo vedere, ci sono già delle immagini caricate sul sito e dall'URL possiamo vedere che sono divise da un #. Possiamo sfruttare questa debolezza per far caricare al sito il nostro script attraverso l'URL inserendolo dopo il # al posto del numero dell'immagine con un codice come:

https://xss-game.appspot.com/level3/frame#<img src='immagine' onerror="alert('XSS Attack!')">

Livello 4


[4/6] Level 4: Context matters
Mission Description
Every bit of user-supplied data must be correctly escaped for the context of the page in which it will appear. This level shows why.
Mission Objective
Inject a script to pop up a JavaScript alert() in the application.
Your Target
I am vulnerable
URL
https://xss-game.appspot.com/level4/frame
Go
timemer
3
Create timer
Target code (toggle)
Hints 0/3 (show)