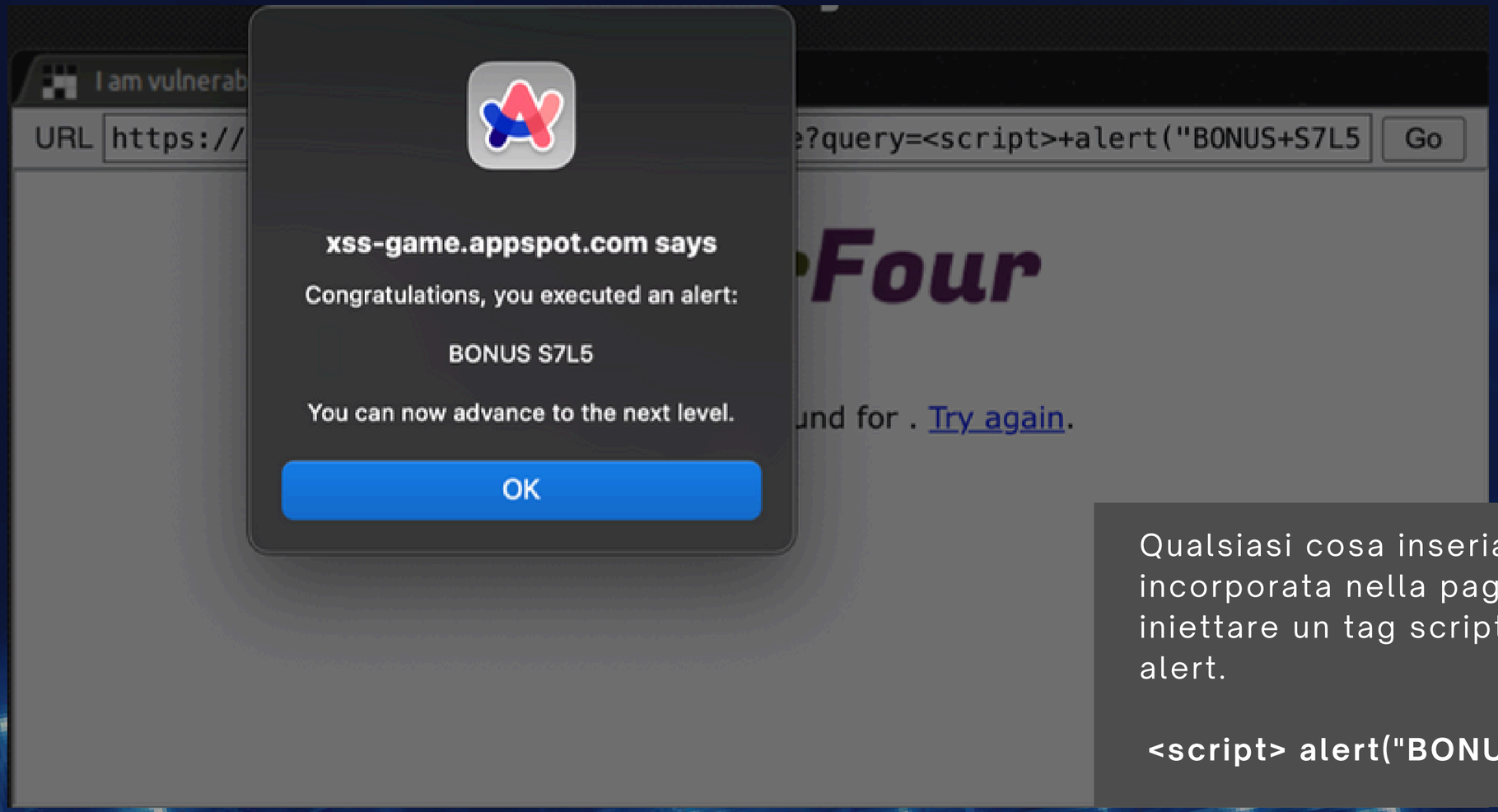
BONUS PROJECT REPORT

S7L5
CS0424IT

SIMONE LA PORTA

Livello 1



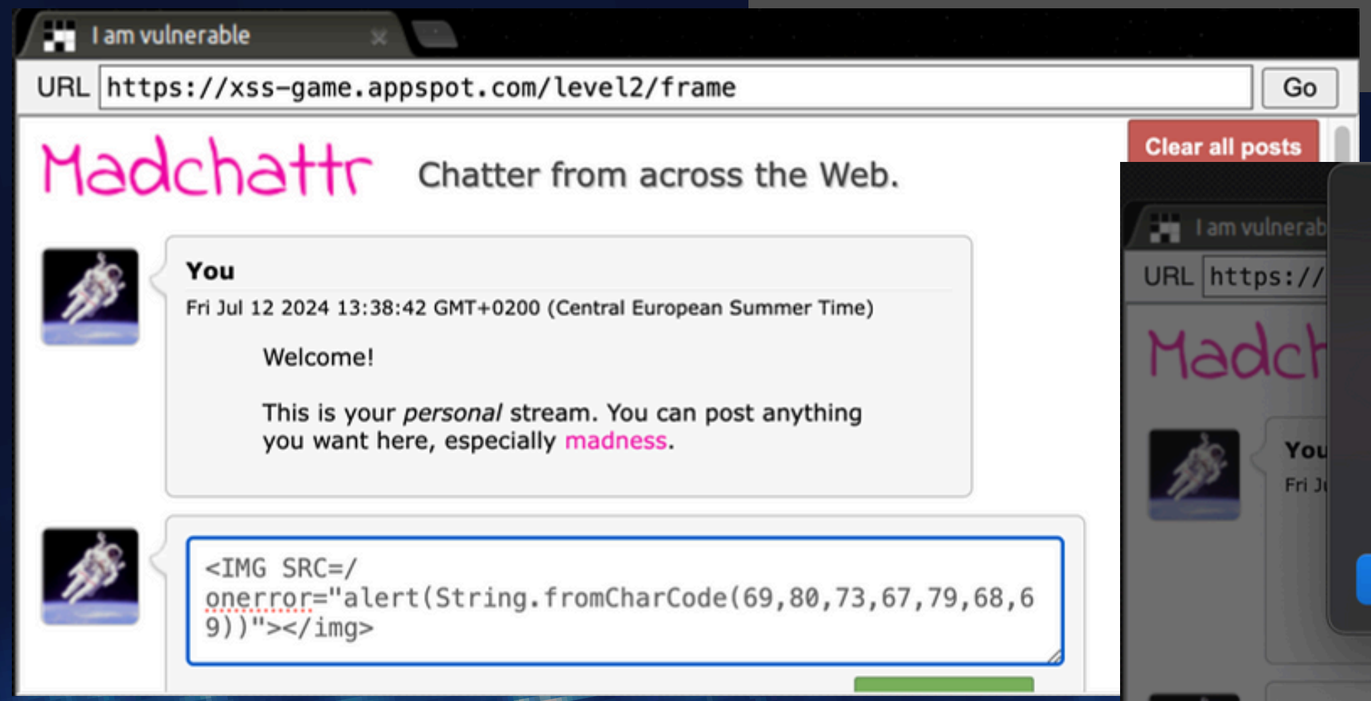
Qualsiasi cosa inseriamo viene incorporata nella pagina. Pertanto, basta iniettare un tag script con un codice di alert.

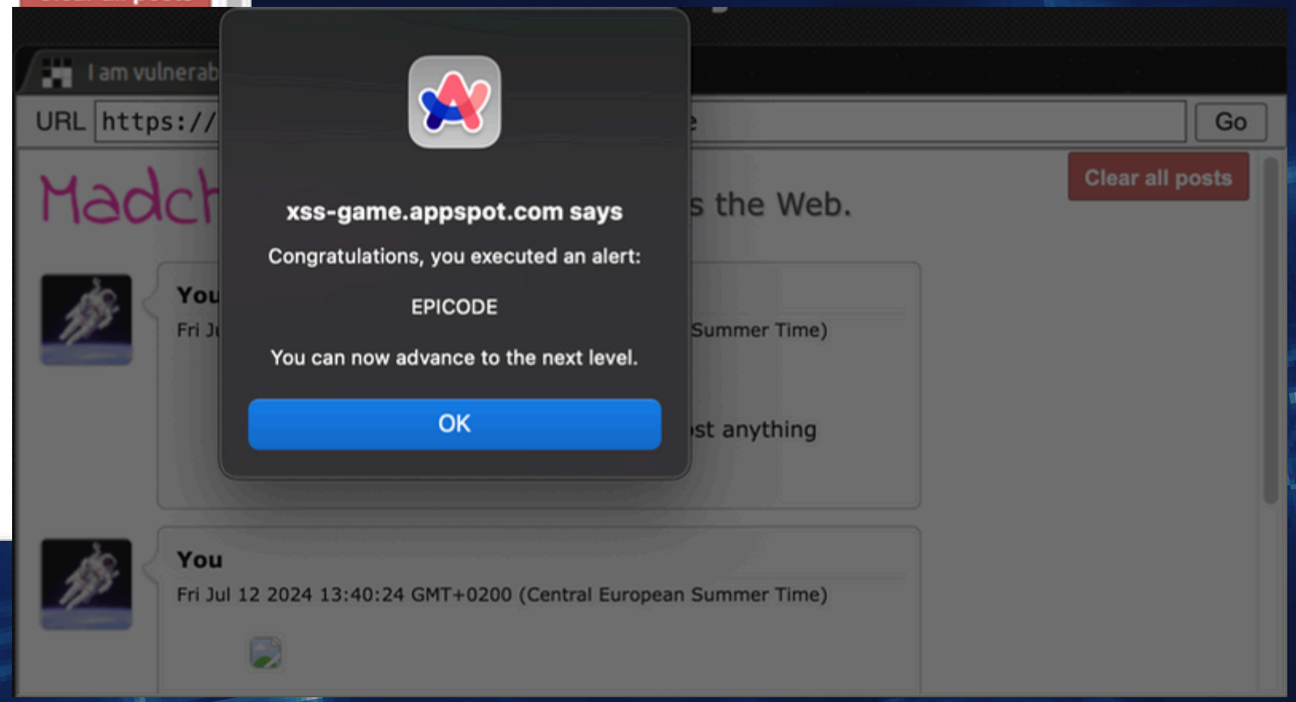
<script> alert("BONUS S7L5") </script>

Livello 2

Questa volta c’è una validazione che ci impedisce di usare il tag script. Per aggirarla, possiamo inserire un tag immagine con un URL non valido e un attributo onerror che eseguirà un avviso JavaScript.

<IMG SRC=/ onerror="alert(String.fromCharCode(69,80,73,67,79,68,69))">

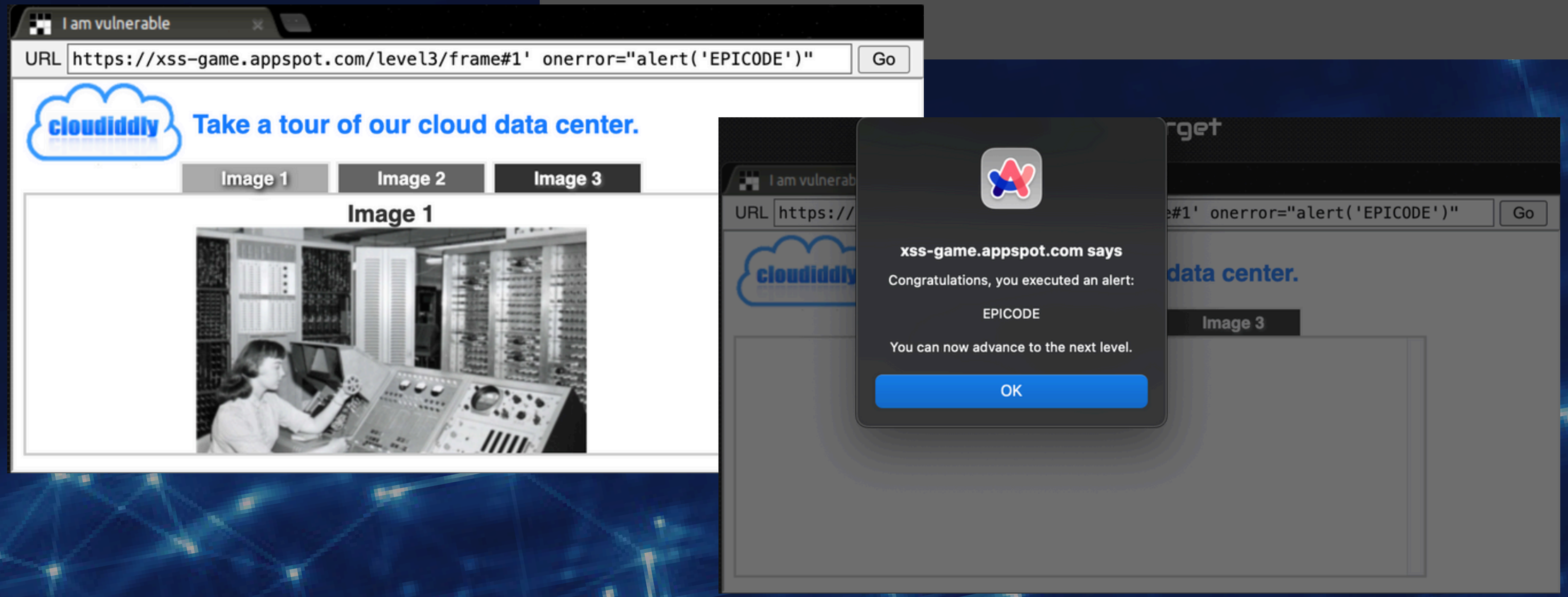




Livello 3

La pagina web incorpora direttamente il frammento di URL dopo il simbolo # come parte del contenuto della pagina, senza sanitizzare correttamente il contenuto.

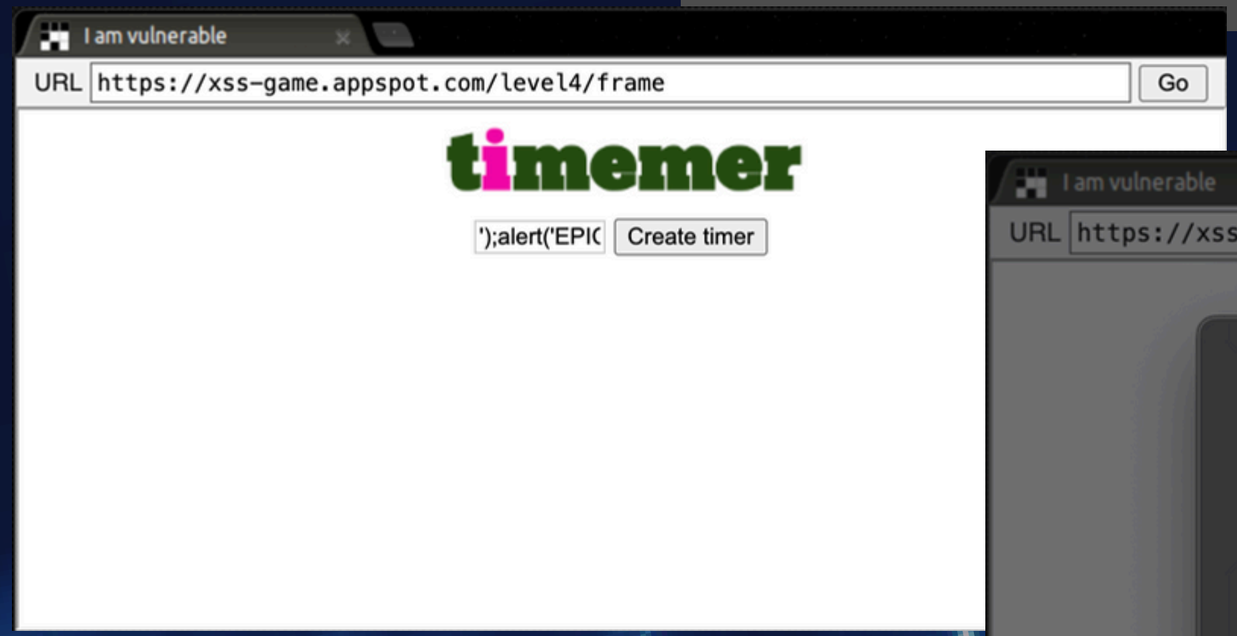
https://xss-game.appspot.com/level3/frame#1' onerror='alert('EPICODE')'

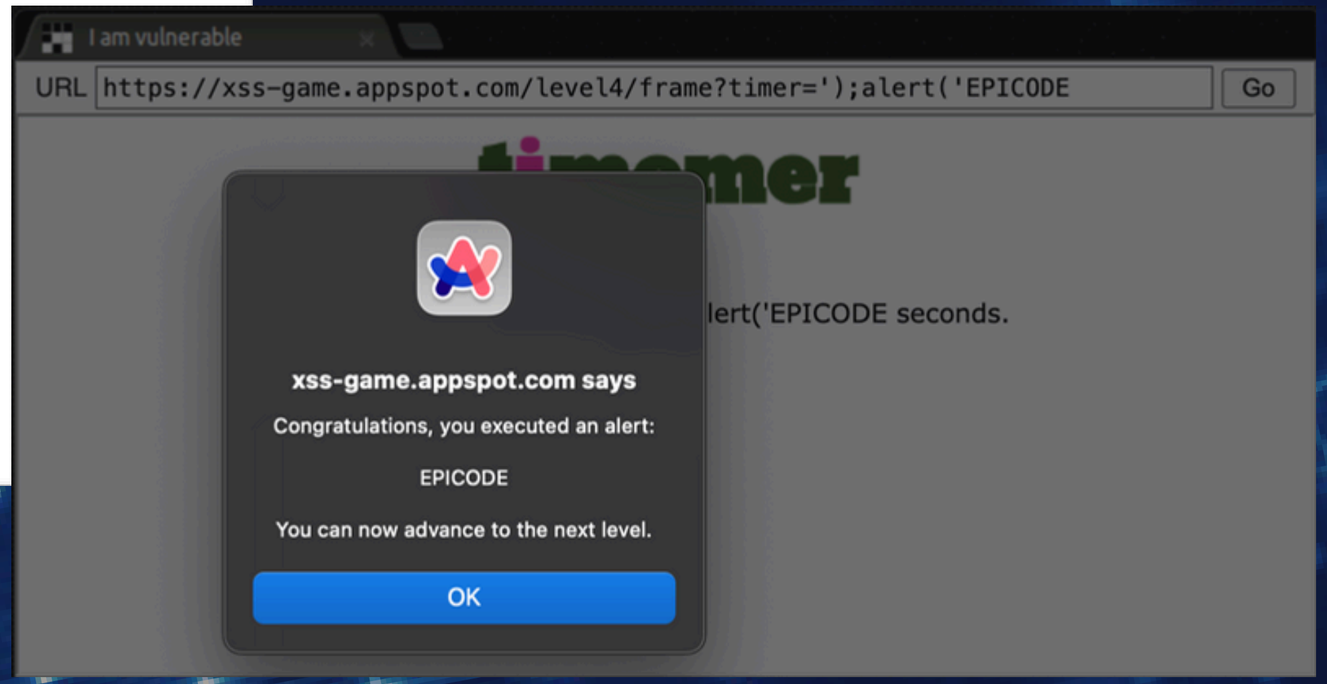


Livello 4

La vulnerabilità in questo livello sfrutta il fatto che l'input dell'utente viene inserito direttamente in una funzione JavaScript senza una corretta sanitizzazione. L'obiettivo è manipolare l'input per chiudere l'istruzione esistente e aggiungere un nuovo comando, in questo caso un avviso (alert).

');alert('EPICODE

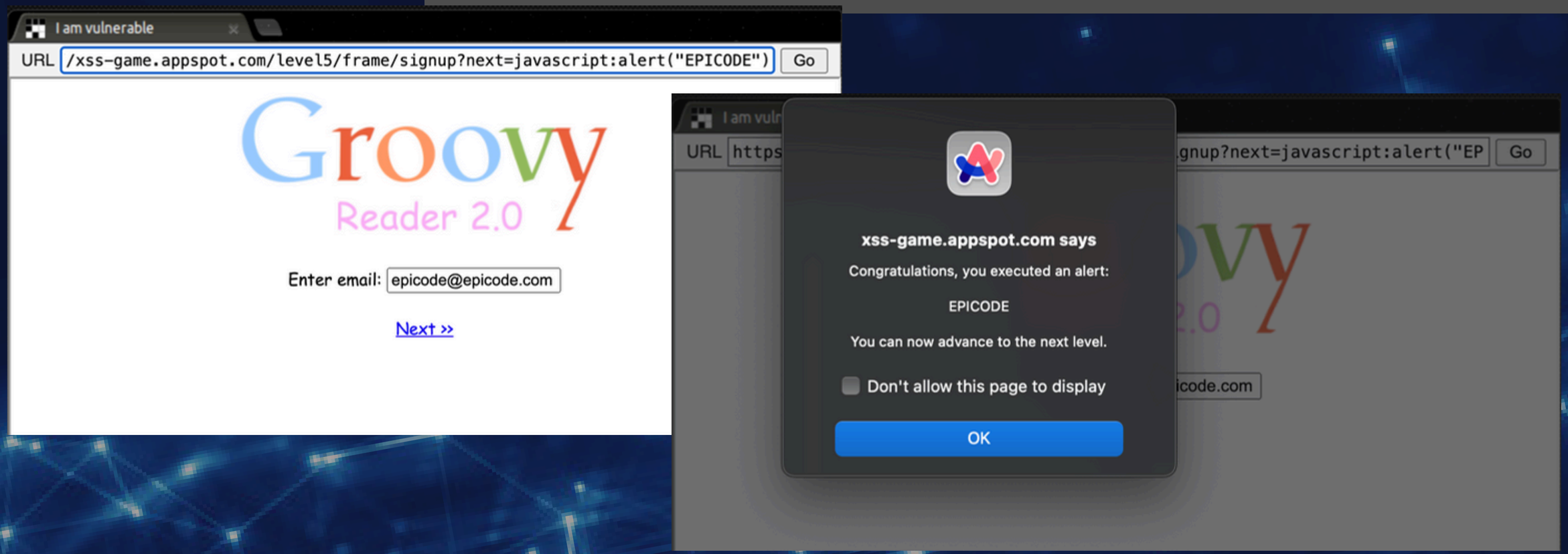




Livello 5

Vulnerabilità in cui un parametro URL (next) viene utilizzato direttamente come valore per l'attributo href di un link senza corretta sanitizzazione. Questo permette di inserire codice JavaScript che viene eseguito quando il link viene cliccato.

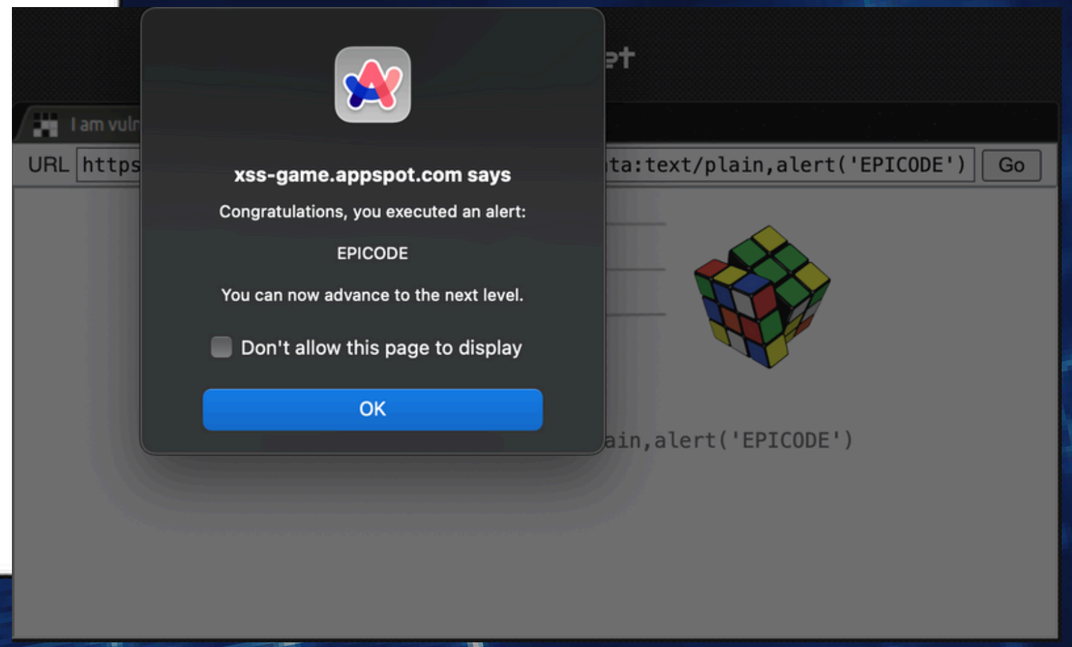
https://xss-game.appspot.com/level5/frame/signup?next=javascript:alert("EPICODE")



Livello 6

In questo livello, la vulnerabilità risiede nel fatto che la pagina aggiunge un tag <script> con un attributo src che punta al valore del frammento dell'URL (la parte dopo #). La pagina verifica che il frammento inizi con "http" o "https" per prevenire il caricamento di file esterni, ma possiamo bypassare questa validazione utilizzando lo schema data per eseguire JavaScript.

https://xss-game.appspot.com/level6/frame#data:text/plain,alert('xss')



Congratulations!

You have successfully completed the game!

Thanks!

Thanks!

While breaking things is fun, it is also important to know how to prevent XSS. For a gentle introduction to the topic of XSS, take a look at our documentation.

Thanks for playing!

THANK YOU!