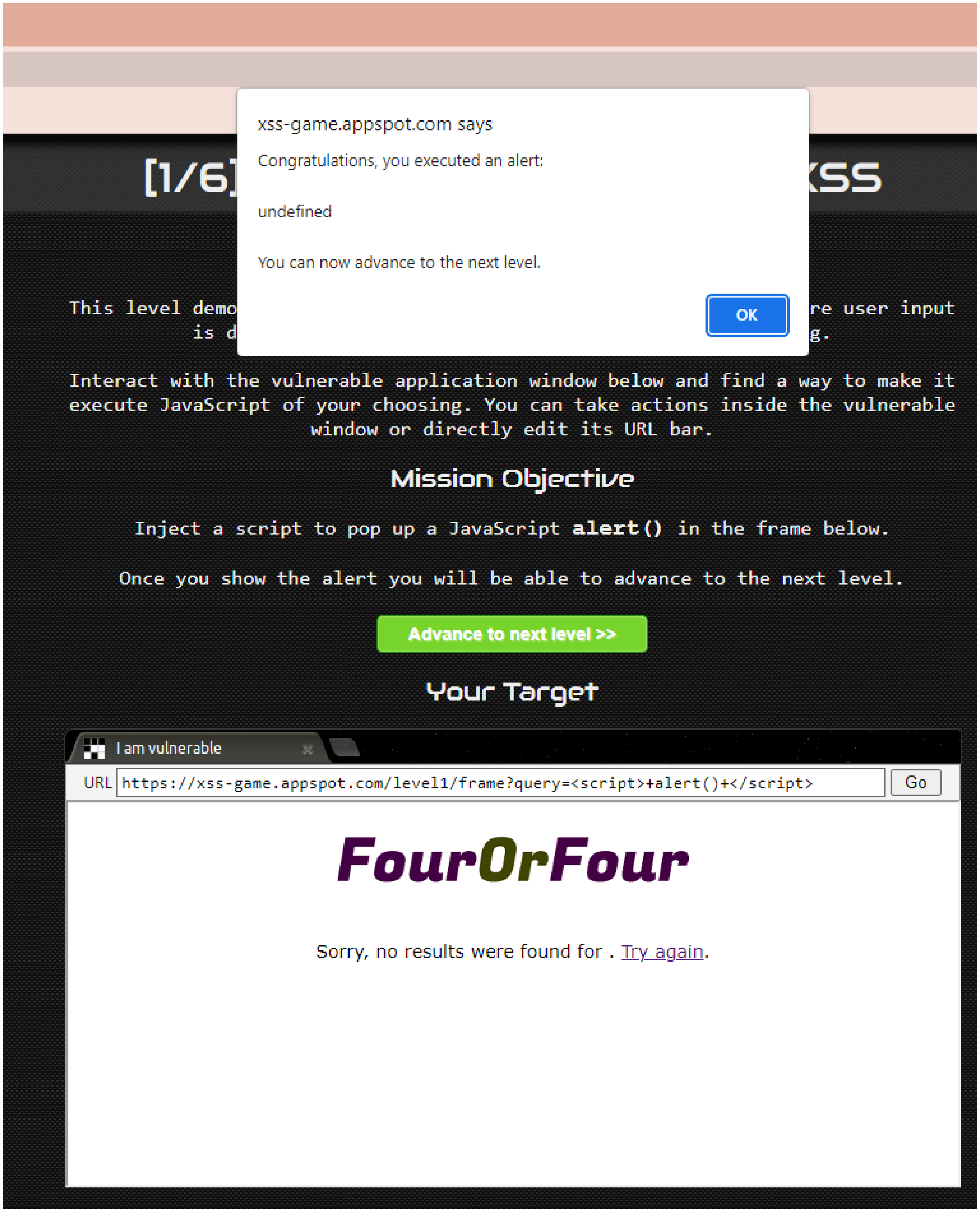
David Thomsen
SEC-260

1. Brief explanation of Reflective XSS and how it works in your own words
    a. Reflective XSS is a type of XSS that uses HTTP requests in order to inject the website with code. In our example, we put a script in a search bar, and the server responded back with an alert after receiving the code.

2. Brief explanation of Stored XSS and how it works in your own words
    a. Stored XSS is done through the use of submissions within a webserver. By adding a script within a comment box, when the comment is received, it is stored in the comment so it can become harmful when someone clicks on the post or it can be harmful to the site.



xss-game.appspot.com says

Congratulations, you executed an alert:

undefined

You can now advance to the next level.

[1/6]

XSS

This level demo re user input
is d g.

Interact with the vulnerable application window below and find a way to make it execute JavaScript of your choosing. You can take actions inside the vulnerable window or directly edit its URL bar.

Mission Objective

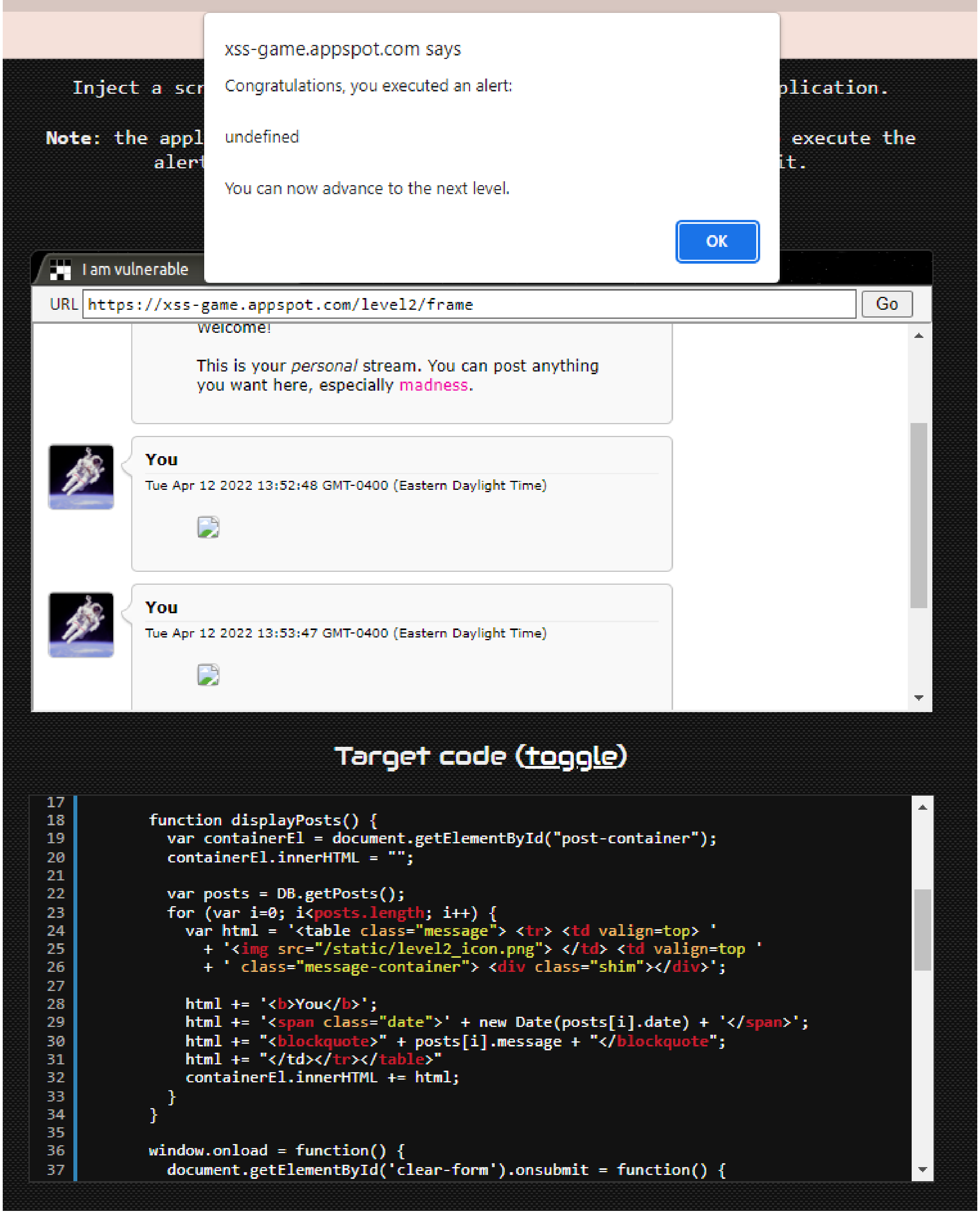
Inject a script to pop up a JavaScript **alert()** in the frame below.

Once you show the alert you will be able to advance to the next level.

Your Target

URL `https://xss-game.appspot.com/level1/frame?query=<script>+alert()+</script>`

Sorry, no results were found for . Try again.



Inject a scr plication.

Note: the appl execute the alert it.

xss-game.appspot.com says

Congratulations, you executed an alert:

undefined

You can now advance to the next level.

URL https://xss-game.appspot.com/level2/frame

Welcome!

This is your *personal* stream. You can post anything you want here, especially madness.

You

Tue Apr 12 2022 13:52:48 GMT-0400 (Eastern Daylight Time)

You

Tue Apr 12 2022 13:53:47 GMT-0400 (Eastern Daylight Time)

Target code (toggle)

```

function displayPosts() {
  var containerEl = document.getElementById("post-container");
  containerEl.innerHTML = "";

  var posts = DB.getPosts();
  for (var i=0; i<posts.length; i++) {
    var html = '<table class="message"> <tr> <td valign=top> '
      + '<img src="/static/level2_icon.png"> </td> <td valign=top '
      + ' class="message-container"> <div class="shim"></div>';

    html += '<b>You</b>';
    html += '<span class="date">' + new Date(posts[i].date) + '</span>';
    html += "<blockquote>" + posts[i].message + "</blockquote";
    html += "</td></tr></table>"
    containerEl.innerHTML += html;
  }
}

window.onload = function() {
  document.getElementById('clear-form').onsubmit = function() {
```