
XSS game과 여름종강 Write up

목차

1. XSS game level 3
2. XSS game level 4
3. XSS game level 5
4. 여름 종강..

XSS game level 3

[3/6] 3단계 : 가라앉는 그 느낌...

미션 설명

이전 레벨에서 보았듯이, 일부 일반적인 JS 함수는 실행 싱크로, 즉 브라우저가 입력에 나타나는 모든 스크립트를 실행하게 합니다. 때때로 이 사실은 이러한 함수 중 하나를 후드 아래에서 사용하는 상위 레벨 API에 의해 숨겨집니다.

이 레벨의 애플리케이션은 그러한 숨겨진 싱크 중 하나를 사용합니다.

임무 목표

이전과 마찬가지로, 앱에 JavaScript를 팝업하는 스크립트를 삽입합니다 alert().

애플리케이션의 어디에도 페이로드를 입력할 수 없으므로 아래 URL 표시줄의 주소를 수동으로 편집해야 합니다.

당신의 목표

I am vulnerable


웹 주소 https://xss-game.appspot.com/level3/frame

가다

cloudiddly

이미지 1 이미지 2 이미지 3

당사의 클라우드 데이터 센터를 둘러보시기 바랍니다.



XSS game은 전반적으로 모두 알맞은 스크립트를 넣어 alert()를 띄우는 형태의 문제

이미지 3개를 각각 누르면, frame#뒤에 있는 숫자들이 바뀜 #뒤로 스크립트를 주입 해야 한다고 생각했음

20240904 SSL 세미나 강혜인

XSS game level 3

주입 지점을 파악했으면 새로운 HTML 요소를 몰래 넣기 위해 무엇을 해야 할지 생각해 보세요.

이전과 마찬가지로, **<script>** ...페이로드로 사용하면 작동하지 않습니다. 브라우저가 페이지가 로드된 후 추가된 스크립트를 실행하지 않기 때문입니다.

주어진 힌트를 보고, HTML 요소가 어떤식으로 전달이 되는지 파악 해야겠다고 생각
-> 소스코드를 보았음

```
<script>
function chooseTab(num) {
  // Dynamically load the appropriate image.
  var html = "Image " + parseInt(num) + "<br>";
  html += "<img src='/static/level3/cloud" + num + ".jpg' />";
  $('#tabContent').html(html);
}
```

소스코드 일부를 보면, #뒤에 어떠한 값을 넣었을 때 html에 더해지는 코드 구조가 이므로, num에 아무 숫자를 넣고, 추가로 스크립트를 넣으면 되지 않을까 하고 생각

XSS game level 3

주입 지점을 파악했으면 새로운 HTML 요소를 몰래 넣기 위해 무엇을 해야 할지 생각해 보세요.

이전과 마찬가지로, **<script>** ...페이로드로 사용하면 작동하지 않습니다. 브라우저가 페이지가 로드된 후 추가된 스크립트를 실행하지 않기 때문입니다.

주어진 힌트를 보고, 일단 xss의 대표 페이로드인 <script>...</script>는 필터링이 되어있다는 것을 확인했고, 소스 코드를 보았음

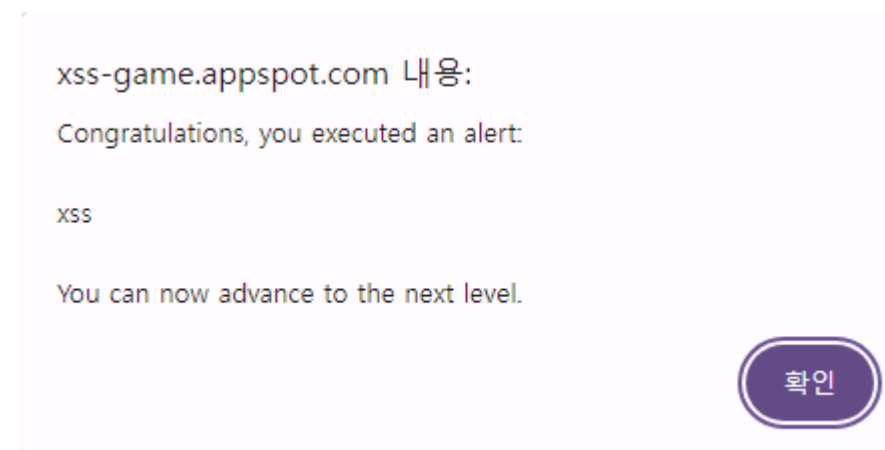
```
<script>
function chooseTab(num) {
  // Dynamically load the appropriate image.
  var html = "Image " + parseInt(num) + "<br>";
  html += "<img src='/static/level3/cloud" + num + ".jpg' />";
  $('#tabContent').html(html);
}
```

소스코드 일부를 보면, #뒤에 어떠한 값을 넣었을 때 html에 더해지는 코드가 형태
이므로, 내가 입력할 num <script>...</script>를 제외한 다른 스크립트를 넣으면 되지 않을까 하고 생각

XSS game level 3

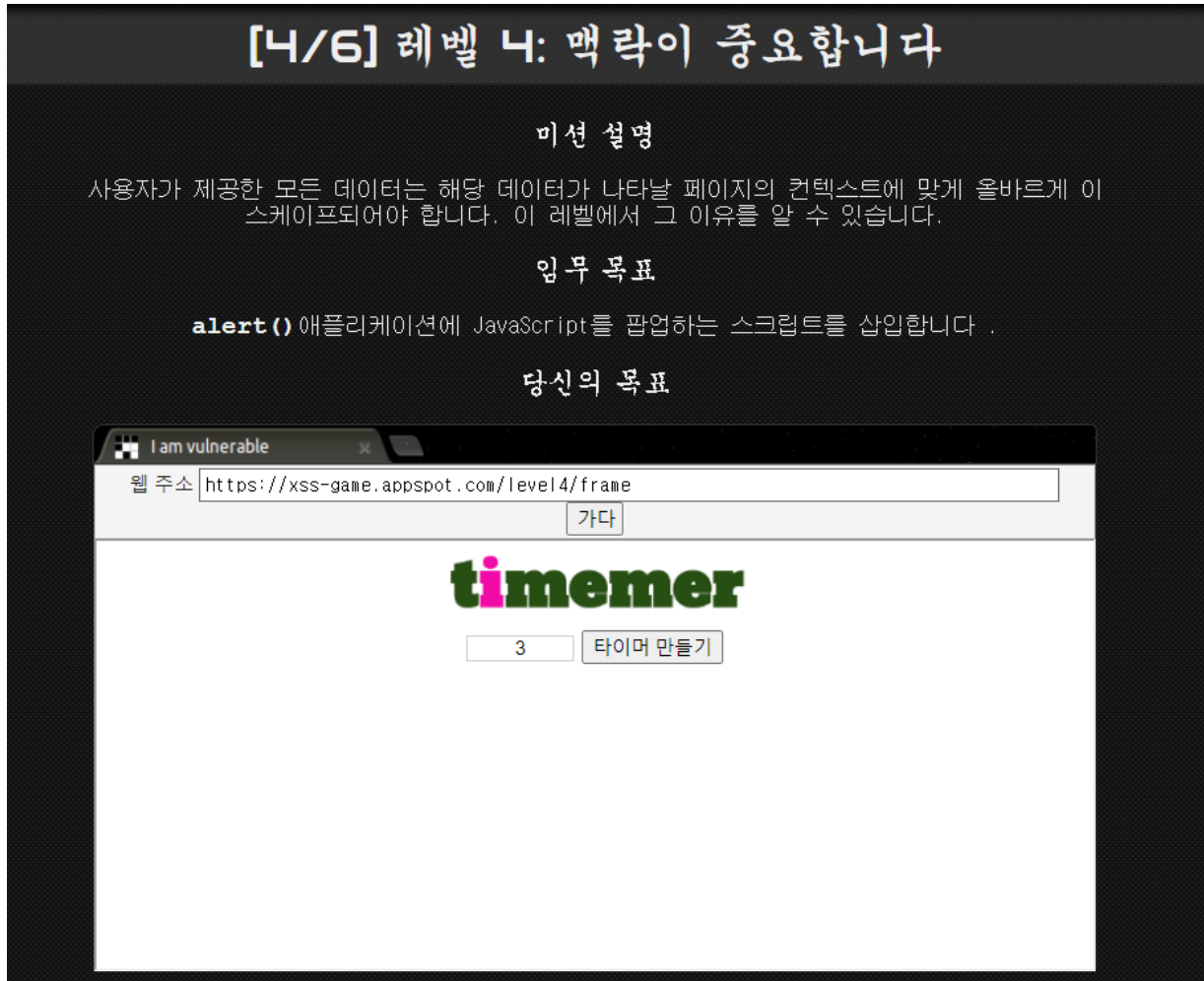


`<script>alert()</script>` 대신 이벤트 속성인 `onerror`를 사용해 `num`에 들어갈 자리에 `onerror` 스크립트를 입력했음

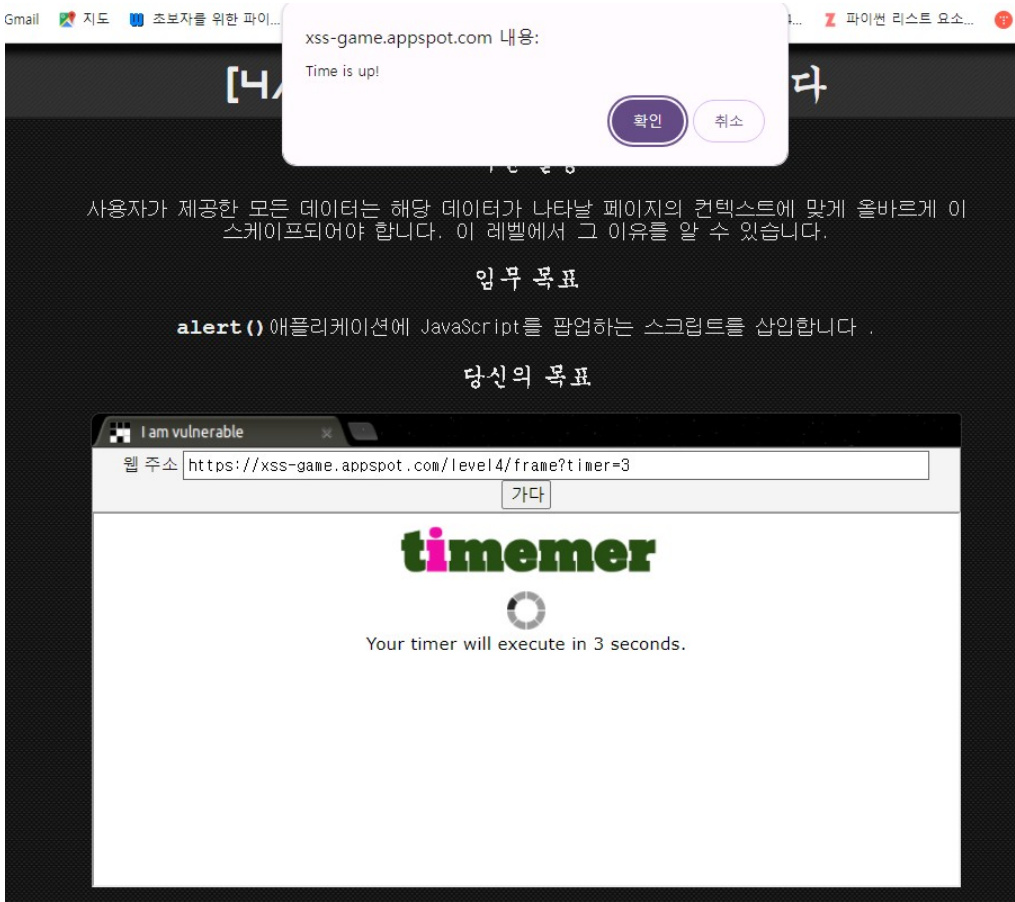


문제에서 요구한 `alert()`를 띄우며 level3 문제가 풀림

XSS game level 4

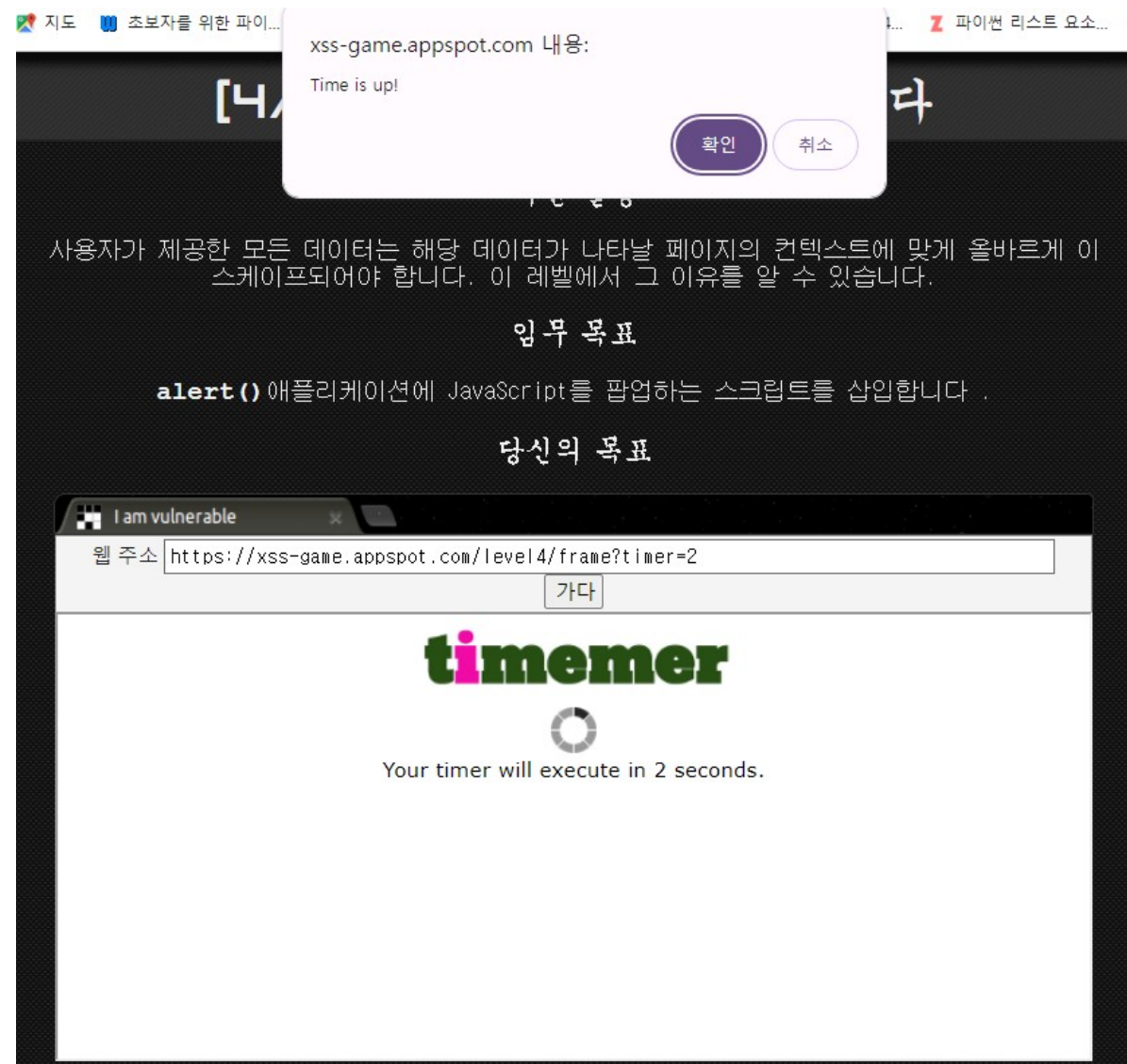


타이머가 실행되면서 alert()팝업창을 띄우게 해야하는 문제



기본값으로 3이 입력되어 있길래, 실행해보니 url에 ?timer=3이 입력되면서 'Time is up!'이라는 팝업창이 뜬

XSS game level 4



그래서 값을 2로 변경하고 실행해보니, 2초뒤에 팝업창이 뜨는 것을 확인함.

여기서 내가 바꿀 수 있는 값은 timer에 입력되는 값 뿐이라고 생각

XSS game level 4

```
<script>
  function startTimer(seconds) {
    seconds = parseInt(seconds) || 3;
    setTimeout(function() {
      window.confirm("Time is up!");
      window.history.back();
    }, seconds * 1000);
  }
</script>
</head>
<body id="level4">
  
  <br>
  
  <br>
  <div id="message">Your timer will execute in {{ timer }} seconds.</div>
</body>
```

소스코드를 살펴보니 onload가 사용되었고, 여기서 내가 입력한 timer 값이 startTimer 함수에 들어가게 되고, startTimer가 실행되는 것을 확인

그렇다면 timer 값에 기존 숫자를 두고, 추가로 javascript 코드를 입력할 수 있는 스크립트 방법을 쓰면 되지 않을까?

XSS game level 4

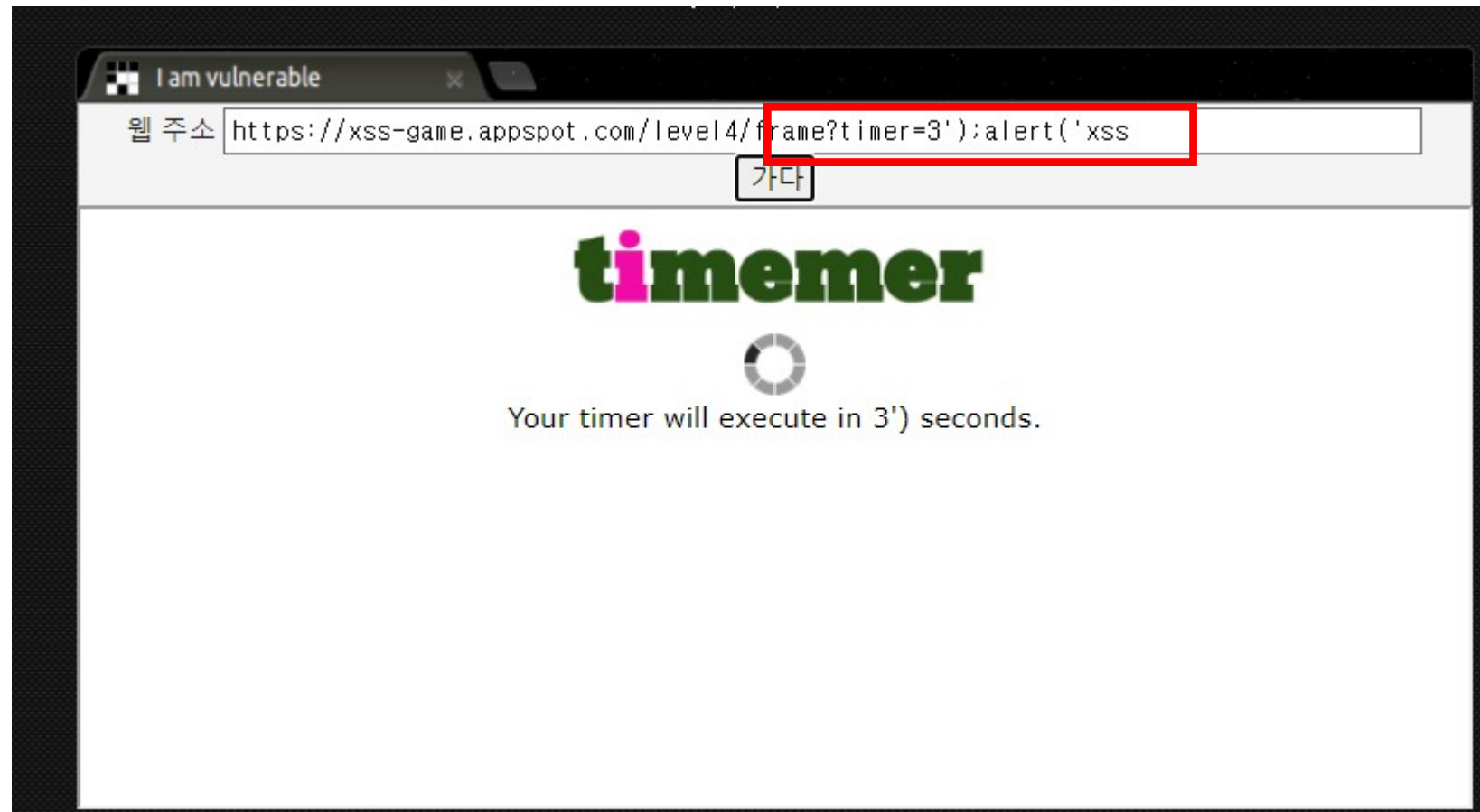
```
<script>
function startTimer(seconds) {
  seconds = parseInt(seconds) || 3;
  setTimeout(function() {
    window.confirm("Time is up!");
    window.history.back();
  }, seconds * 1000);
}
</script>
</head>
<body id="level4">
  
  <br>
  
  <br>
  <div id="message">Your timer will execute in {{ timer }} seconds.</div>
</body>
```

소스코드를 살펴보니 onload가 사용되었고, 여기서 내가 입력한 timer 값이 startTimer 함수에 들어가게 되고, startTimer가 실행되는 것을 확인

그렇다면 timer 값에 기존 숫자를 두고, 추가로 javascript 코드를 입력할 수 있는 스크립트 방법을 쓰면 되지 않을까?

-> SQL Injection과 비슷한 방법

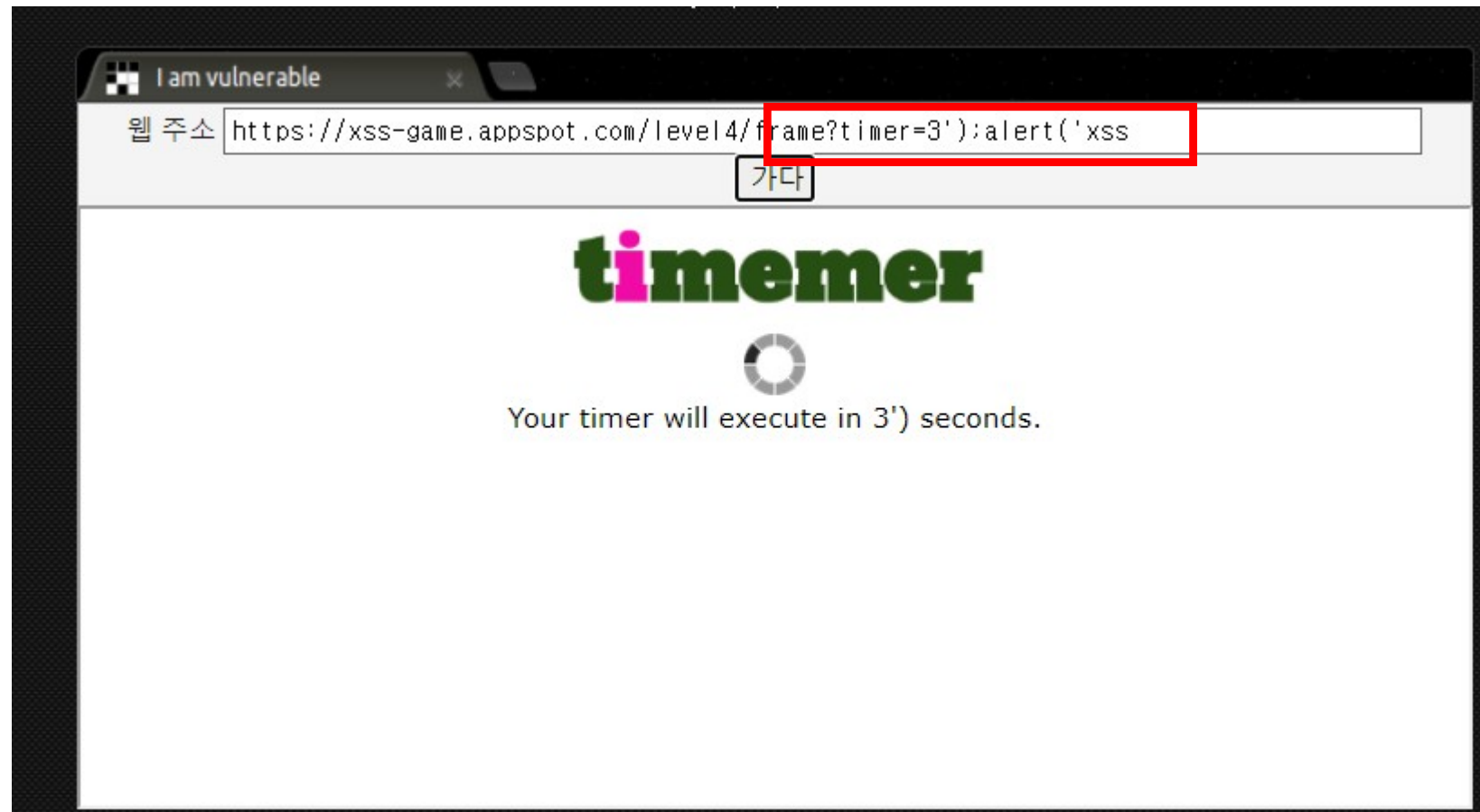
XSS game level 4



그래서 기본으로 설정된 3이라는 값 뒤에 기존 구문을 끝내도록 ');를 입력한 후에 추가로 alert('xss를 추가해봤음

그러나, 무한로딩만 걸림 -> 내가 넣은 timer값이 3') 까지만 입력됨.

XSS game level 4



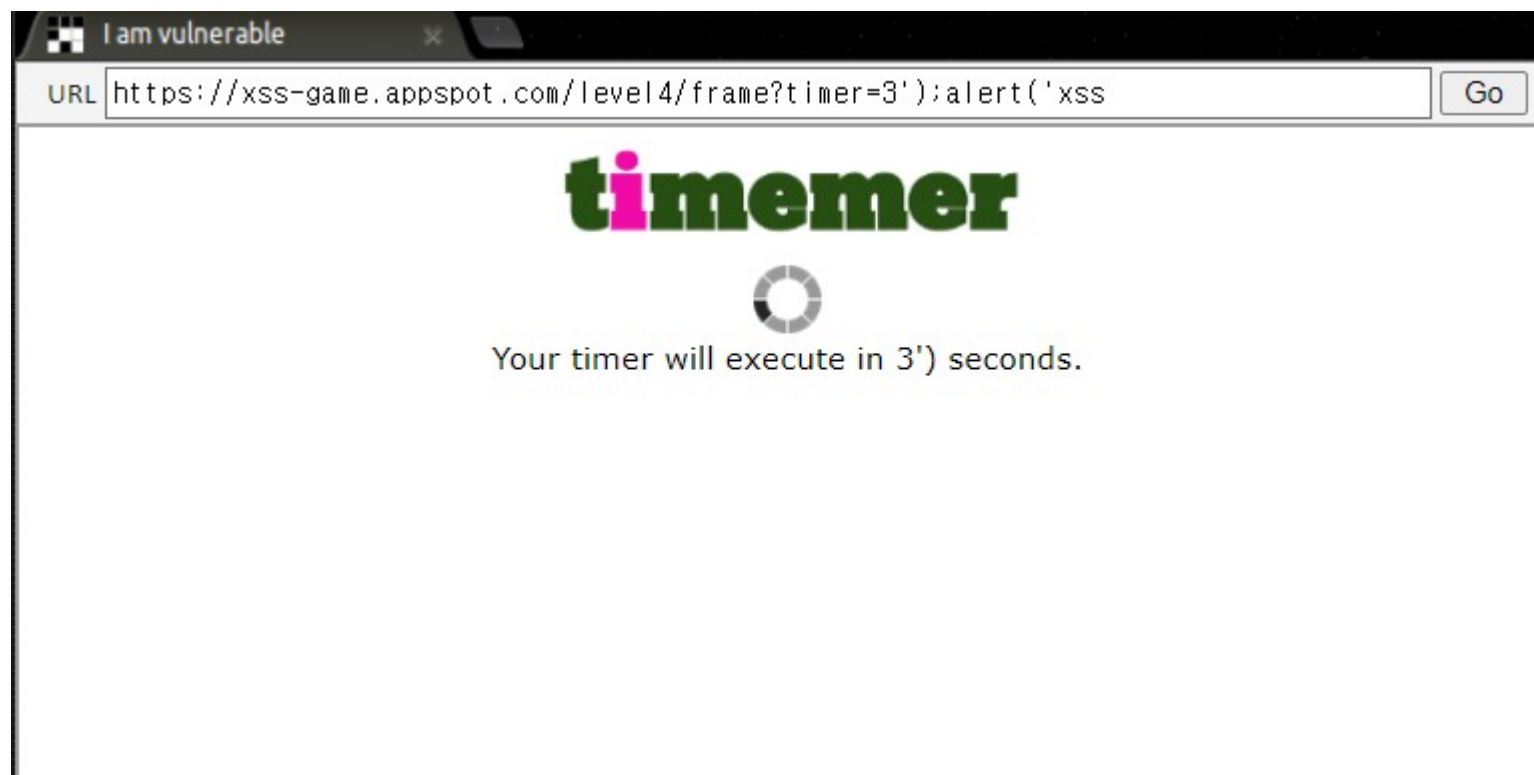
그래서 기본으로 설정된 3이라는 값 뒤에 기존 구문을 끝내도록 ');를 입력한 후에 추가로 alert('xss를 추가해봤음

그러나, 무한로딩만 걸림 -> 내가 넣은 timer값이 3') 까지만 입력됨.

XSS game level 4

```
When browsers parse tag attributes, they HTML-decode their values first. <foo  
bar='z'> is the same as <foo bar='&#x7a;'
```

힌트를 확인하니, 브라우저가 태그 속성을 읽을때, HTML 디코드를 먼저 수행한다고 함



그래서 무한로드 되는페이지를 다시 보니, 3') 까지 입력된 것을 봐선
싱글쿼터와 괄호는 입력이 되는데, 세미콜론이 문제인 것을 파악함

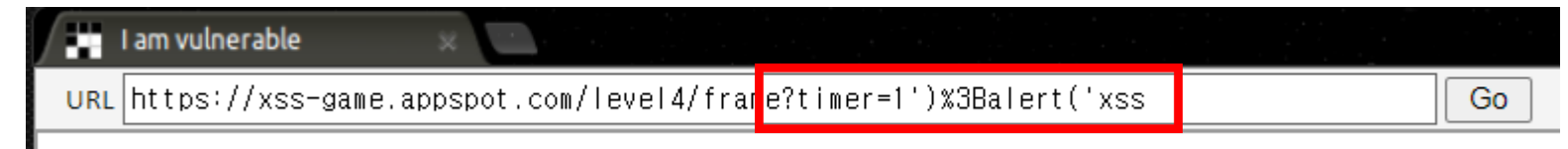
XSS game level 4

세미콜론(`;`)을 URL 인코딩하면 `%3B`가 됩니다.

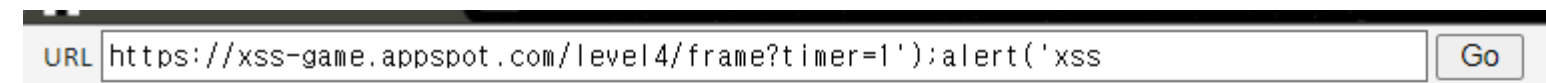


세미콜론이 URL 인코딩 했을 때 값을 잊어버려서...
영원한 나의 친구 gpt에게 물어보았고, %3B라고 답변을 받았다!

;을 URL 인코딩해줘



빨리 실행되라고 기존값 3에서 1로 바꾸고, 세미콜론을 URL 인코딩한 값으로 변경해서 넣어줬더니,



timer



Your timer will execute in 1');alert('xss seconds.

xss-game.appspot.com 내용:

Congratulations, you executed an alert:

xss

You can now advance to the next level.

확인

입력값이 제대로 들어가면서, alert() 팝업이 떴다! 해결!