S7/L5 Bonus

XSS GAME

Eleonora Viola

DATASHIELDS

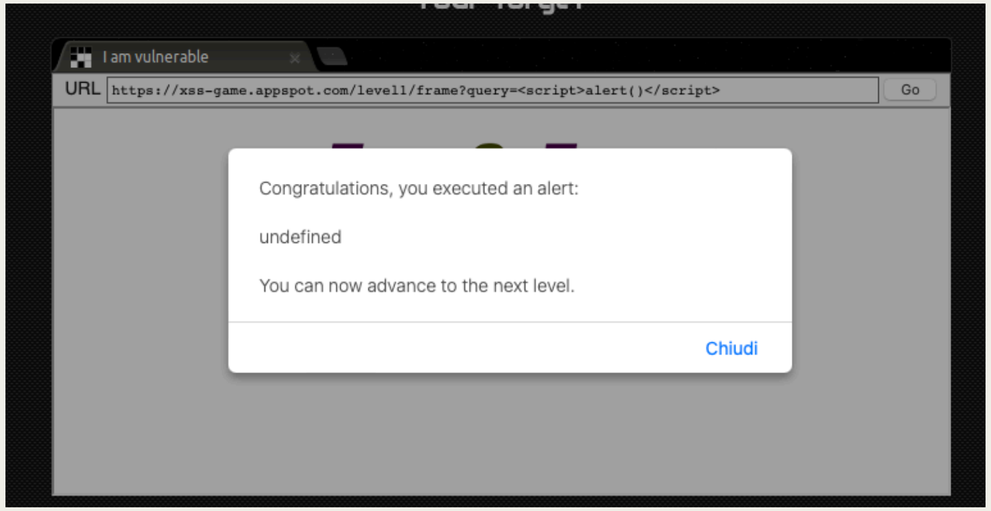
INDICE

LEVEL 1

- Come primo passaggio dobbiamo visualizzare il codice sorgente: usiamo tasto destro e andiamo su view page source, che è anche disponibile sul sito.
- Guardando il codice e scendendo fino a link /level 1/source e troviamo il codice sorgente
- Analizziamo la funzione def(get) qui c'è xss protection()

```
def get(self):
  # Disable the reflected XSS filter for demonstration purposes
  self.response.headers.add_header("X-XSS-Protection", "0")
```

- Questo denota che il sito è sensibile agli attacchi xss quindi proseguiamo immettendo il codice **<script> alert() </script>**

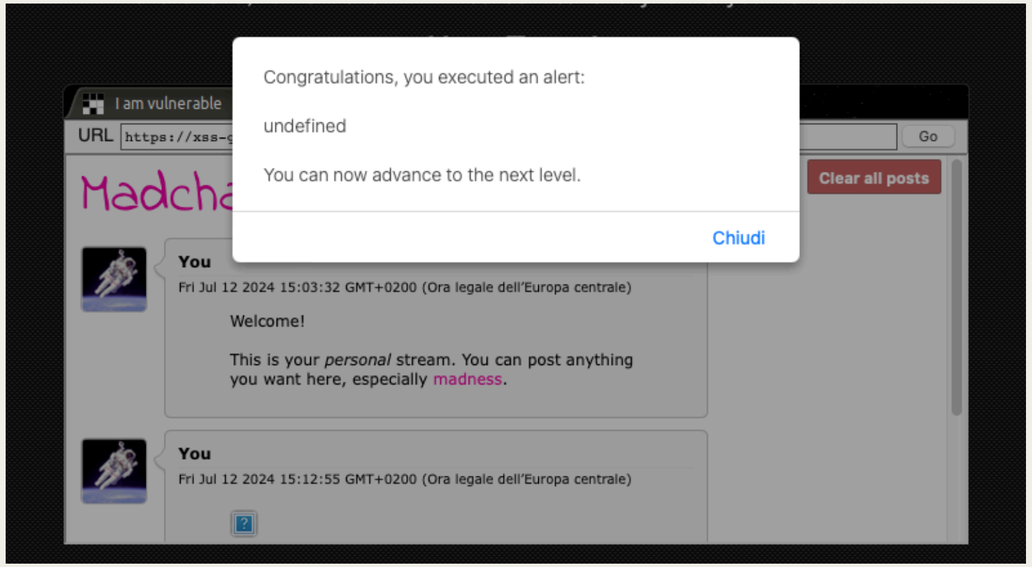


LEVEL 2

- Come prima visualizziamo il codice sorgente
- Analizzando la funzione var post possiamo modificarla al fine di iniettare codice di errore perché nel codice manca la chiusura della virgoletta per l'attributo **valign**:

```
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>';
```

- Dunque inseriamo il codice <**img src "x" onerror=alert()**>



Thank you!