

Oxymoron, right? Well for somebody who loves perl so much, it is. Anyway here it is...

te=0x84a51080 [0,0]

Contents: [Dobrica Pavlinu's random unstructured stuff]

- [Dobrica Pavlinu's random unstructured stuff \(One-liners\)](#)
 - ◆ [Dobrica Pavlinu's random unstructured stuff \(show phpinfo from shell\)](#)
- [Dobrica Pavlinu's random unstructured stuff \(Security scanning\)](#)
 - ◆ [Dobrica Pavlinu's random unstructured stuff \(Spike PHP Security Audit Tool\)](#)
 - ◆ [Dobrica Pavlinu's random unstructured stuff \(Pixky\)](#)
 - ◆ [Dobrica Pavlinu's random unstructured stuff \(phc\)](#)
- [Dobrica Pavlinu's random unstructured stuff \(Links\)](#)

One-liners

show phpinfo from shell

```
echo '<? phpinfo() ?>' | php5
```

Security scanning

Spike PHP Security Audit Tool

<http://developer.spikesource.com/projects/phpsecaudit/>

```
sudo apt-get install php5-xslt
```

Small list of checked expressions, quite difficult to browse.

Pixky

<http://pixybox.seclab.tuwien.ac.at/pixy/>

Enables taint analysis of code. Doesn't handle ISO-8859-2 chars well, and breaks with terrifying error, but it's a very promising tool (in Java, sigh)

phc

<http://www.phpcompiler.org/>

Great tool to get php's AST tree. Used by [Plumhead](#)

Links

fetchrss: <http://del.icio.us/rss/dpavlin/php+security>

- There was an error: 500 Server closed connection without sending any data back