Consider the four PHP programs below. Each program contains some form of security vulnerability (please, don't code like that!). Let's see how we could find these vulnerabilities automatically using static analysis.

```php
<?php
  $name = $_GET['name'];
  echo $name;
?>
```

Figure 1: `echo` prints a string into the webpage.

```php
<?php
  $filename = $_GET['filename'];
  system("/usr/bin/file $filename");
?>
```

Figure 2: `system` runs a shell command.

```php
<?php
  $filename = $_GET['filename'];
  include($filename);
?>
```

Figure 3: `include` pastes the code of the file into the calling program.

```php
<?php
  $filename = $_GET['filename'];
  unlink($filename);
?>
```

Figure 4: `unlink` deletes a file.

UFMG

DCC

DEPARTAMENTO DE CIÊNCIA DA COMPUTAÇÃO

Compilers Laboratory

1. Can you explain what is the problem with each program above?

2. Can you think about an attack vector for each vulnerability? Think about a URL that could compromise the program. It does not have to be something as detailed as `http://example.com/index.php?filename=../../../../etc/passwd`. Just approximate this URL.

3. All these vulnerabilities have points in common. Could you list some of these commonalities?

4. Could you think about a static analysis to detect this kind of vulnerability automatically?