# Computer Security HW3 Write-Up

Account: soyccan
Name: 陳正康
Student ID: B07902143

## Unexploitable

**FLAG{baby_recon_dont_forget_to_look_github_page}**

1. Problem URL: http://unexploitable.kaibro.tw/ (http://unexploitable.kaibro.tw/)
2. Try: http://unexploitable.kaibro.tw/87 (http://unexploitable.kaibro.tw/87)
   - see GitHub 404 page
   - guess it's build by github page
   - may be: custom domain -> CNAME -> xxx.github.io (http://xxx.github.io)
3. `dig unexploitable.kaibro.tw`

```
;; ANSWER SECTION:
unexploitable.kaibro.tw. 3599   IN      CNAME   bucharesti.github.io.
```

4. visit his github page and found a commit "delete secret file"
   - https://github.com/Bucharesti/Bucharesti.github.io/commit/c2dc70b0a5031aa396a2ae9ed7fdf6d8e1506462#diff-29710728b7ff4a4ffbe358d2b5670d69 (https://github.com/Bucharesti/Bucharesti.github.io/commit/c2dc70b0a5031aa396a2ae9ed7fdf6d8e1506462#diff-29710728b7ff4a4ffbe358d2b5670d69)
5. Voila!

## Safe R/W

**FLAG{w3lc0me_t0_th3_PHP_W0r1d}**

### Observe: Behaviour

1. write `$c` as file content to the path `$f/meow`
2. include the path `$i`

### Observe: Vulnerabilities

1. a controllable file content `$c` , and its path `$f`
2. a controllable include path `$i`
3. Local File Inclusion

### Observe: Security Check

1. `file_get_content($i)` should not contain '<'
   - this is checked before `include($i)`

2. some WAF check on `$i, $f` , and length limit for `$c`

## Attack Strategy

1. bypass the '<' symbol check
2. obtain RCE by LFI

## Exploit: Symbol Check Bypass

1. It'll be good if `file_get_content()` does not see the '<', but `include()` sees
   - PHP wrapper is used to create different behaviour
   - but `php` is blocked by WAF check
   - use `data://` for safe
2. Attempt: pass `i=data:,ImHACKER`
   - "Here is your file content:" is shown, but nothing are displayed
     $\Longrightarrow$ `include()` doesn't recognize PHP wrapper (since disabled by default)
     $\Longrightarrow$ '<' check is not triggered
   - we know that: `file_get_content()` sees `$i` as a data wrapper, but `include()` sees it as a regular pathname
3. use `data:,ImHACKER` as a dirname
   - pass `f=data:,ImHACKER`
   - and `i=data:,ImHACKER/meow`
   - and `c=` + my PHP code (length limit: 19 bytes)
   - thus RCE is obtained

## Exploit: RCE

1. runs `<?php echo`ls /`;` to list root files
   - `/flag_is_here`
2. runs `<?php echo`cat /f*`;`
   - Voila!