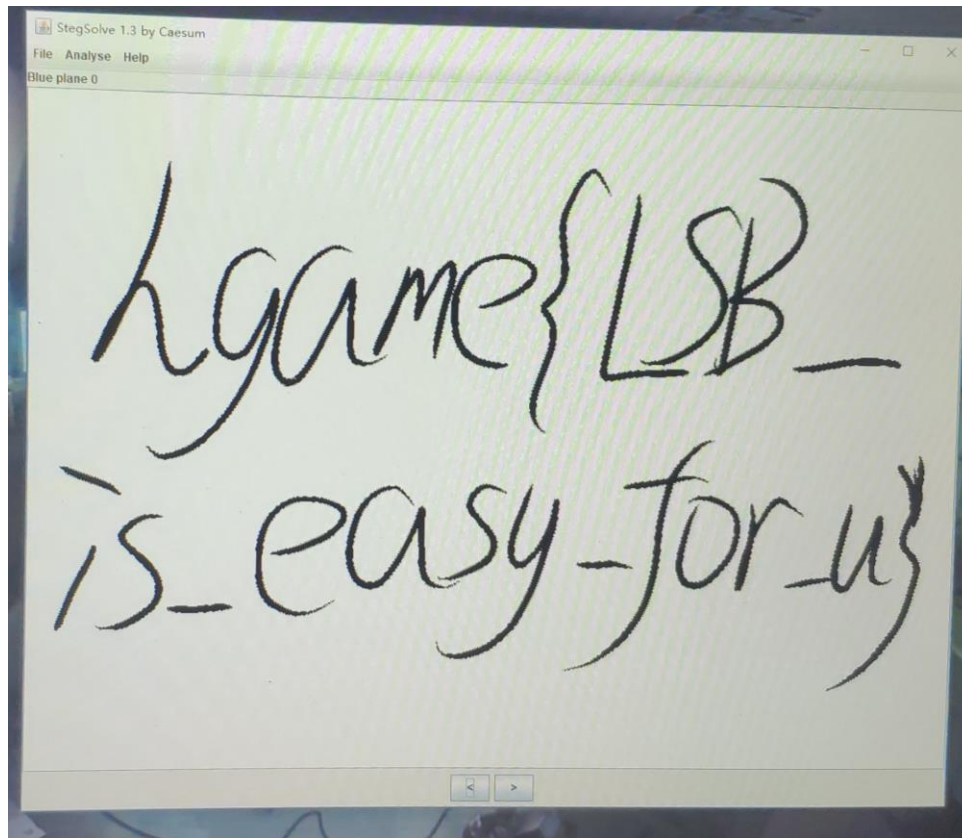


MISC: Hidden Image in LSB

利用软件 stegsolve, 便可以得到 flag



打字机：



Пyλnα{Λr_∀ι0Lαι_ιrDα//Pιιαρ}

根据上图可以确定 hgame 的各个小写字母

1: 通过第一个特征, 我们观察字形, 可以进行这样的猜测:



得到了W, R, A, S, L, X, V, N, M的小写字母可能的对应关系。

最终得出:

abcdefghijklmnop

λϭοδϭογ Πι κL ηγ

opqrstuvwxyz

υρ ϭει οϣ/Π ϩΥ

谁吃了我的 flag:

根据题干可以猜测是意外关机 vim 产生了 swp 文件，我们通过 index.html.swp 下载后得到 flag

```
hgame{3eek_diSc10Sure_fRom+  
wEbsit@}    </br>    <p>fine,
```

换头大作战:

按照要求改 http header 即可得到 flag

```
Cookie: admin=1  
X-Forwarded-For: 127.0.0.1  
Connection: close  
Content-Type: application/  
  
want=1  
  
<body>  
<form action="index.php" metho  
    想要flag嘛 : <input name="v  
    <input type="submit" valu  
</form>  
</body>  
</html>  
  
<br/>hgame{hTTp_HeaDeR_iS_Ez}
```

very easy web:

可以得知这个是一个二次编码的题目

要转的:	vidar
URL编码:	%76%69%64%61%72

要转的:	%76%69%64%61%72
URL编码:	%25%37%36%25%36%39%25%36%34%25%36%31%25%37%32

← → ↻ ⓘ 不安全 | 120.78.184.111:8080/week1/very_ez/index.php?id=%2576%2569%2564%2561%2572

```
hgame{urlDecode_Is_GoOd} <?php
error_reporting(0);
include("flag.php");

if(strpos("vidar", $_GET['id'])!==FALSE)
    die("<p>干巴爹</p>");

$_GET['id'] = urldecode($_GET['id']);
if($_GET['id'] === "vidar")
{
    echo $flag;
}
highlight_file(__FILE__);
?>
```

can u find me?

```
<html>
  <head>...</head>
  <body> == $0
    <p>the gate has been hidden</p>
    <p>can you find it? xixixi</p>
    <a href="f12.php"></a>
  </body>
</html>
```

Target: http://47.107.252.171:8080

Request

Raw Headers Hex

GET /f12.php HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: zh-CN
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 47.107.252.171:8080
Connection: close

Response

Raw Headers HTML Render

Name	Value
HTTP/1.1	200 OK
Server	nginx/1.15.8
Date	Wed, 30 Jan 2019 13:44:46 GMT
Content-Type	text/html; charset=UTF-8
Connection	close
X-Powered-By	PHP/7.2.14
password	woyaoflag
Content-Length	242

<!DOCTYPE html>
<html>
<head>
 <title>can u find me?</title>
</head>
<body>
 <p>yeah!you find the gate</p>
 <p>but can you find the password?</p>
 <p>please post password to me! I will open the gate for you!</p>
</body>
</html>

Done 447 bytes | 264 millis

```
password: woyaoflag
Content-Length: 302

<!DOCTYPE html>
<html>
<head>
  <title>can u find me?</title>
</head>
<body>
  <p>yeah!you find the gate</p>
  <p>but can you find the password?</p>
  <p>please post password to me! I will open the gate for
you!</p>
  <p>right!</p><a href='iamflag.php'> click me to get
flag</a></body>
</html>
```