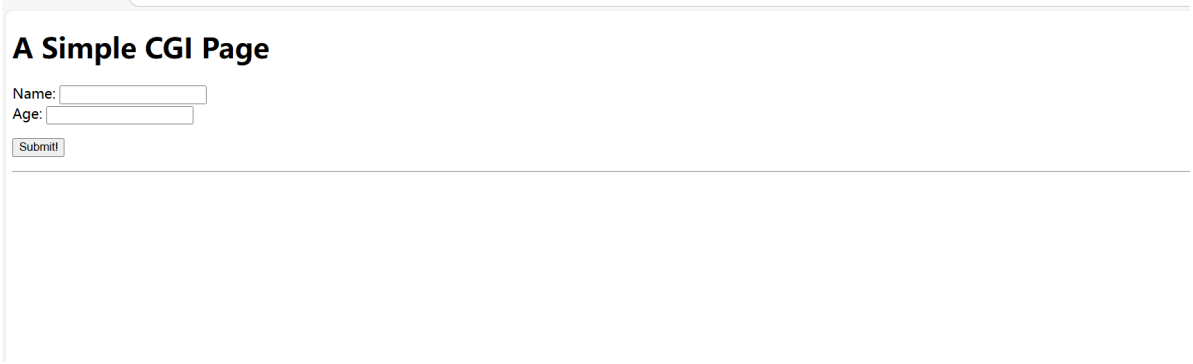
i-got-id-200-adworld

首先点开页面，发现三个子目录，首先还是进行一个目录爆破吧，没有什么信息

点开hello world，发现是一个pl语言，比较小众



首先打开这个貌似是个登陆页面？尝试一下sql注入，原本以为是pl/sql什么的，结果发现完全不是这个东西

然后搜索一下perl的文件上传漏洞，，，怎么打开都是这个题的wp，这怎么搞

猜测该文件上传后台的代码：

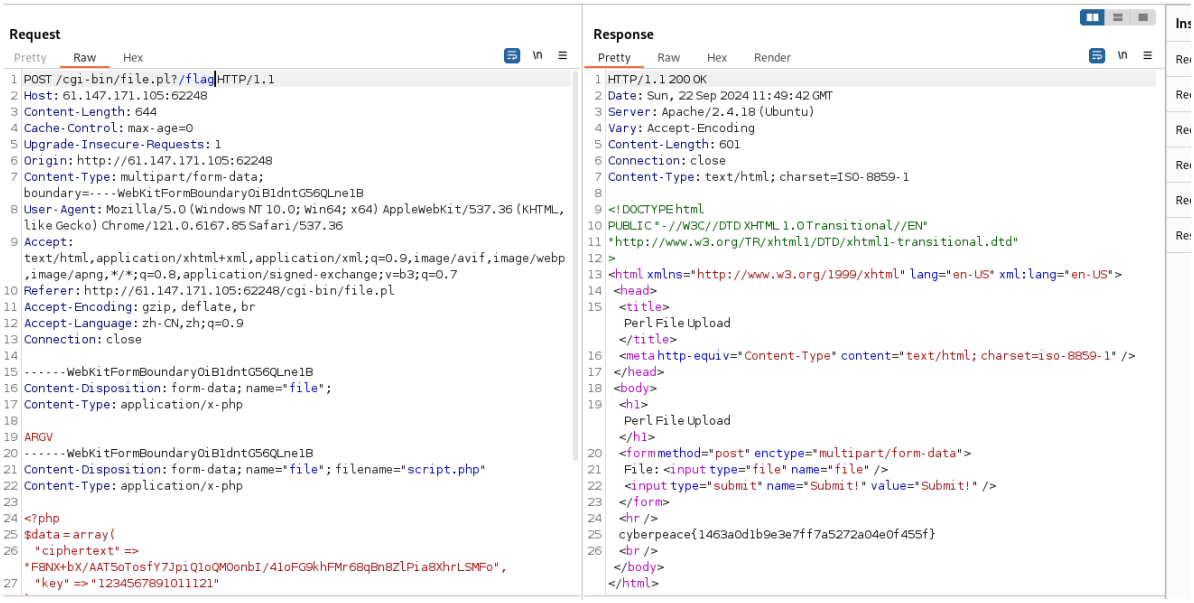
```
my $cgi= CGI->new;
if ( $cgi->upload( 'file' ) )
{
my $file= $cgi->param( 'file' );
while ( <$file> ) { print "$_"; } }
```

param()函数会返回一个列表的文件但是只有第一个文件会被放入到下面的接收变量中。如果我们传入一个ARGV的文件，那么Perl会将传入的参数作为文件名读出来。对正常的上传文件进行修改,可以达到读取任意文件的目的。

这里就是在原有上传文件的基础上多构造一个文件格式，删除filename，内容修改为ARGV

直接访问/flag

得到flag



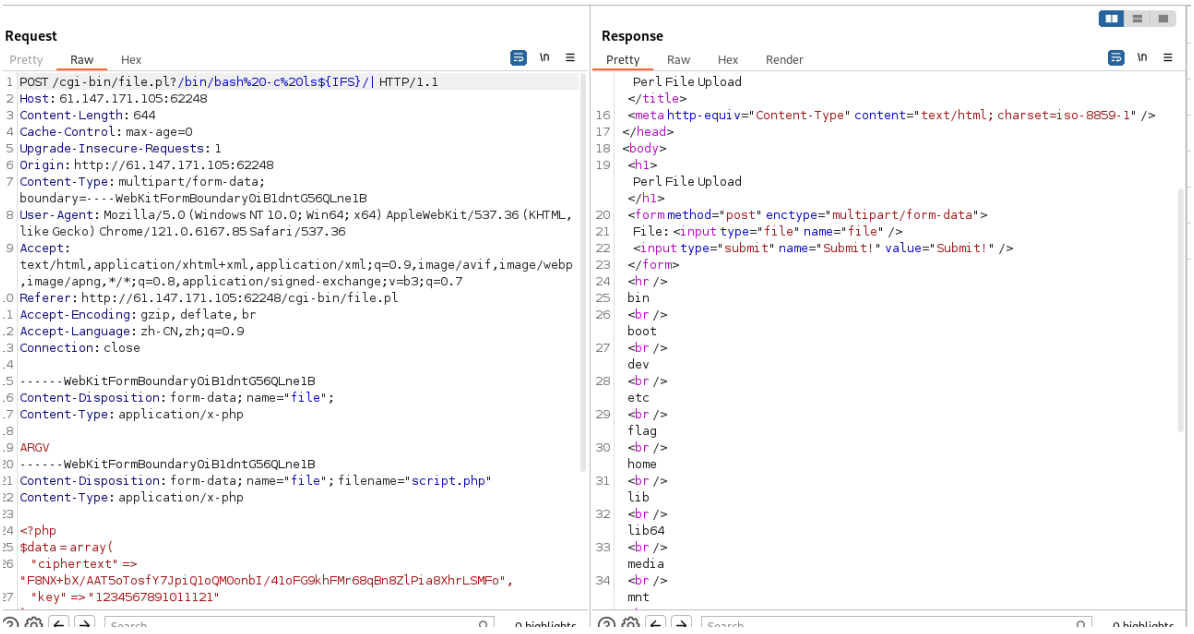
或者构造rce，执行远程代码，最开始我构造/bin/bash的ls去访问根目录却没有回显

```
/bin/bash%20-c%20ls%20/
```

，看了别人的思路才明白要加上`/|`的管道符，其输出结果用管道传输到读入流中

但是继续执行又发现ls的不是根目录而是当前目录，最后发现最后一个命令间的空格不能用url编码因为是作为linux输出，应该加入linux的空格绕过，或者16进制。最后利用如下

```
/bin/bash%20-c%20ls${IFS}/|
```



总结：这道题就是考的搜索能力，是非常规语言的文件上传漏洞。。但是语言比较小众，加上网上相关信息很少只有一个题的wp，感觉没有什么实战价值