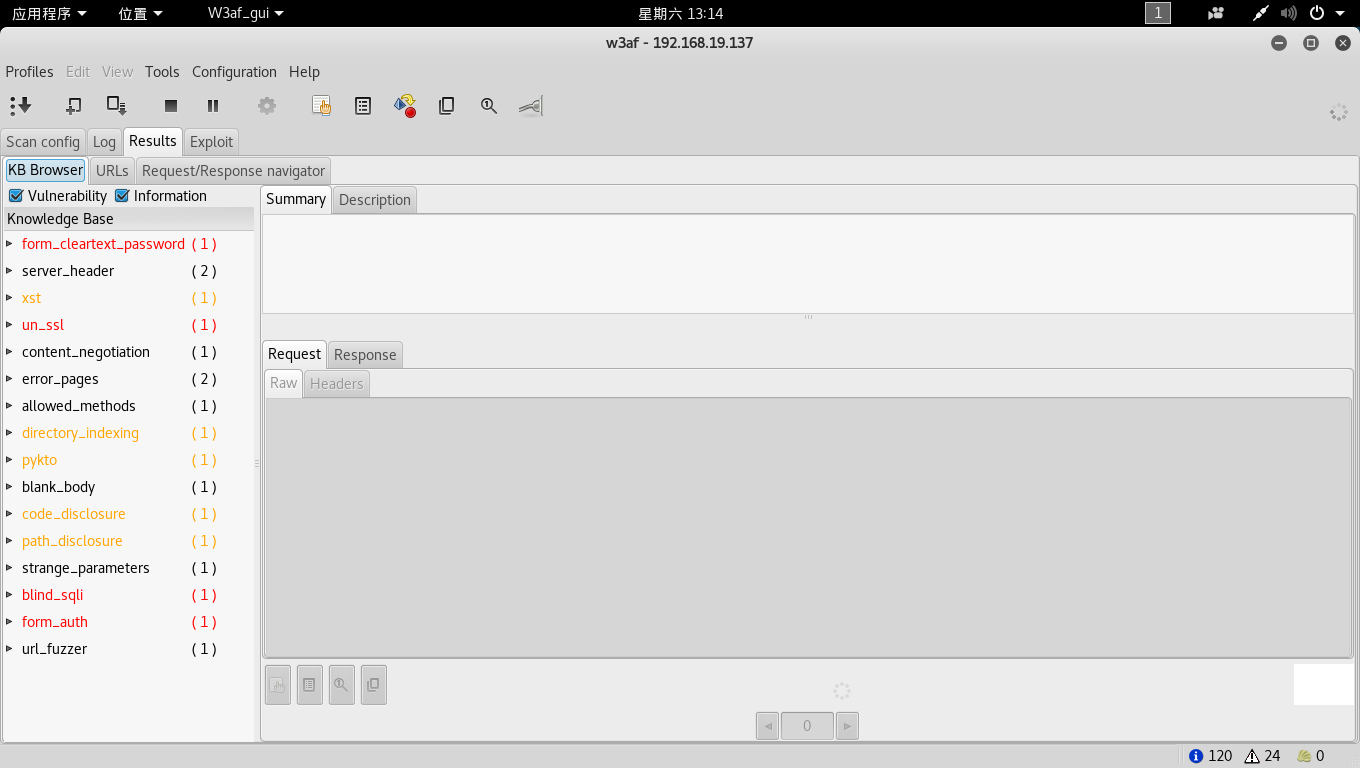
***DVWA:192.168.19.137/dvwa/login.asp***

***级别：low***

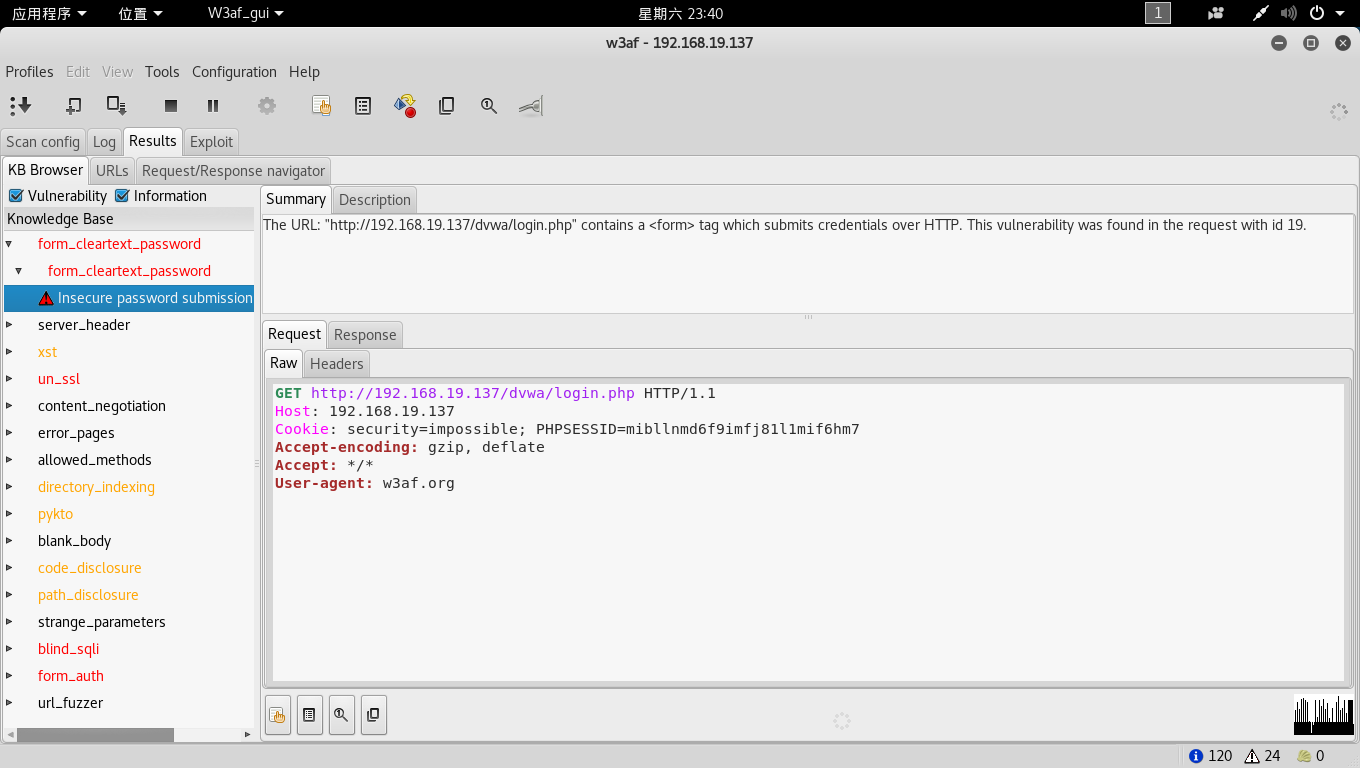
******

***form\_cleartext\_password***

Insecure password submission over HTTP

明文密码漏洞

参考文章：http://blog.csdn.net/owen\_william/article/details/66477384

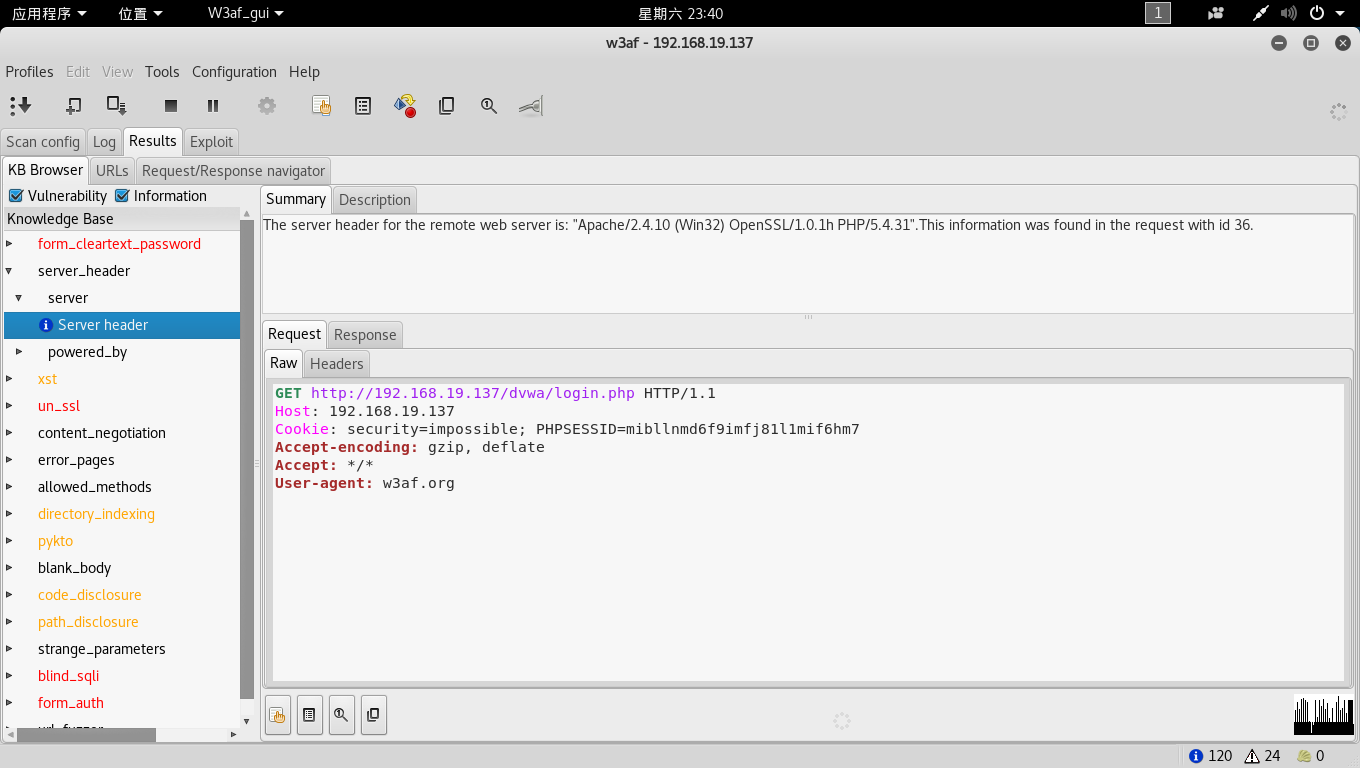


***server\_header***

Server header

http host 头攻击漏洞

参考文章：http://netsecurity.51cto.com/art/201705/539759.htm

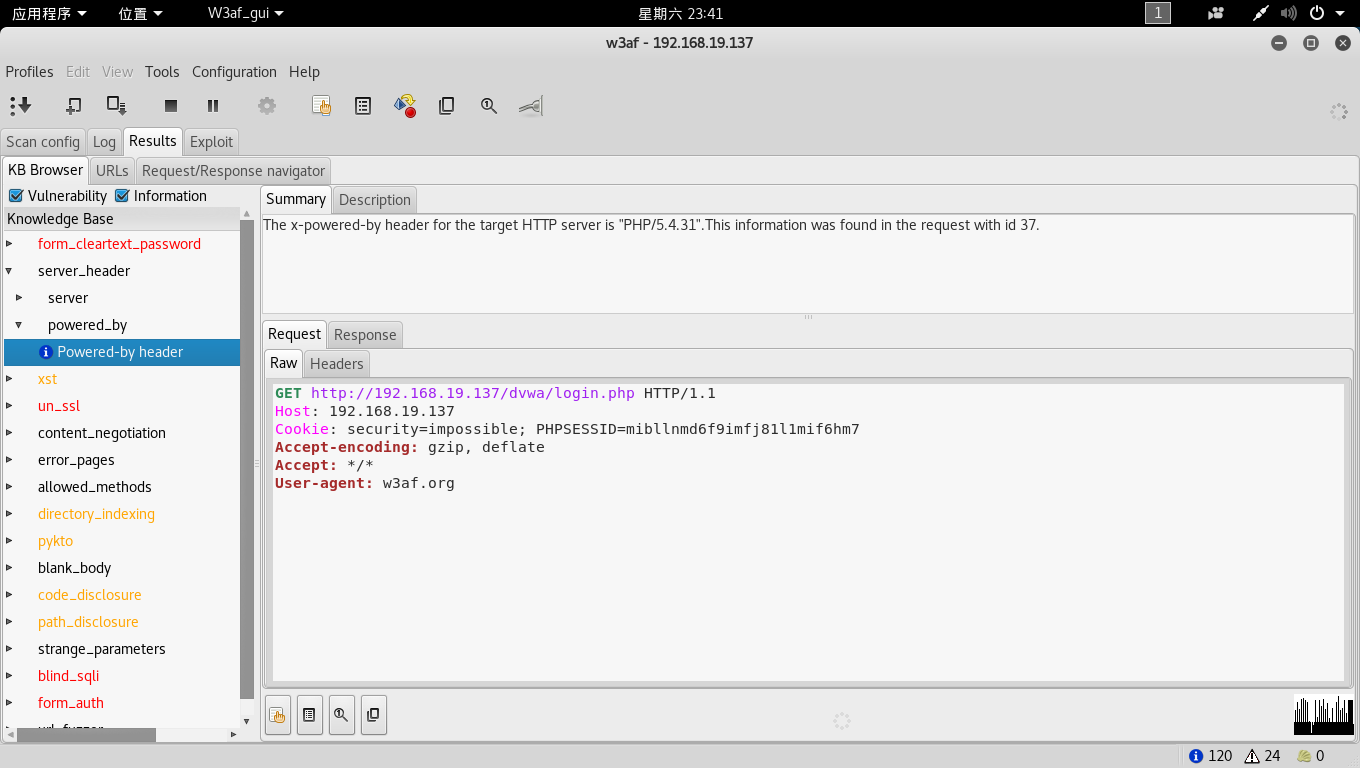


***powered\_by***

Powered-by header

告知网站使用何种语言或框架编写的，有时候会有特定版本网页服务器漏洞进行攻击

解决方法：在php.ini中设定expose\_php = off



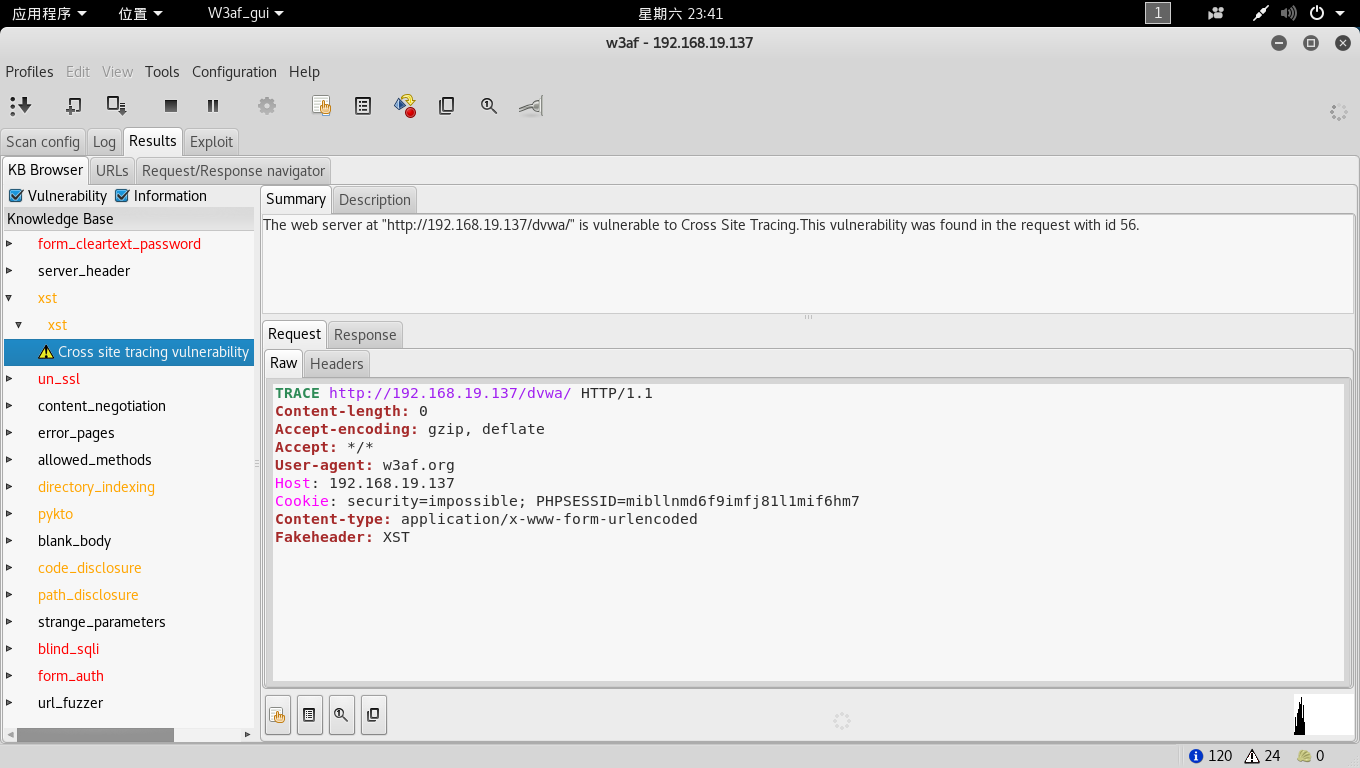
***xst***

Cross site tracing vulnerability

主要利用http的trace（跟踪），原理为返回浏览器发送给服务器的所有请求信息（多见于debug的需求）

例子：在存在XSS漏洞但设置了cookie的httponly属性的时候，结合trace。比如用户点击网站中的一个标签会执行一段脚本，那么该脚本会异步（异步双方不需要共同时钟，也就是接收方不知道发送方什么时候发送，所以在发送的信息中就要有提示接受方开始接受的信息，如开始位，停止位）发起一个trace请求，由于是同域，所以会带上cookie，然后服务器会把请求的信息都返回来，其中包括cookie，可以在回调函数里解析然后上传到我们的服务器上去。

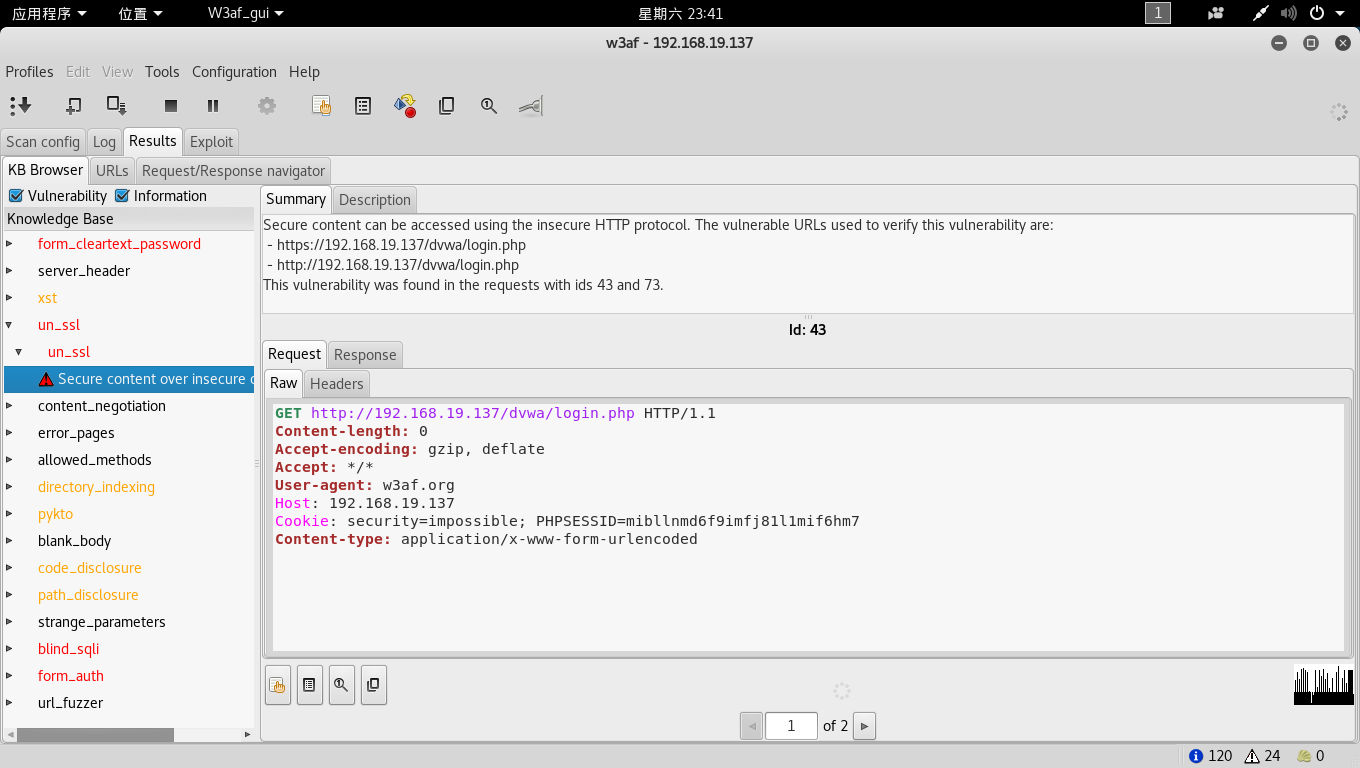
攻击描述：攻击者将恶意代码嵌入一台已经被控制的主机上的web文件，当访问者浏览时恶意代码在浏览器中执行，然后访问者的cookie、http基本验证以及ntlm验证信息将被发送到已经被控制的主机，同时传送Trace请求给目标主机，导致cookie欺骗或者是中间人攻击。



***un\_ssl***

Secure content over insecure channel

未使用ssl协议传输

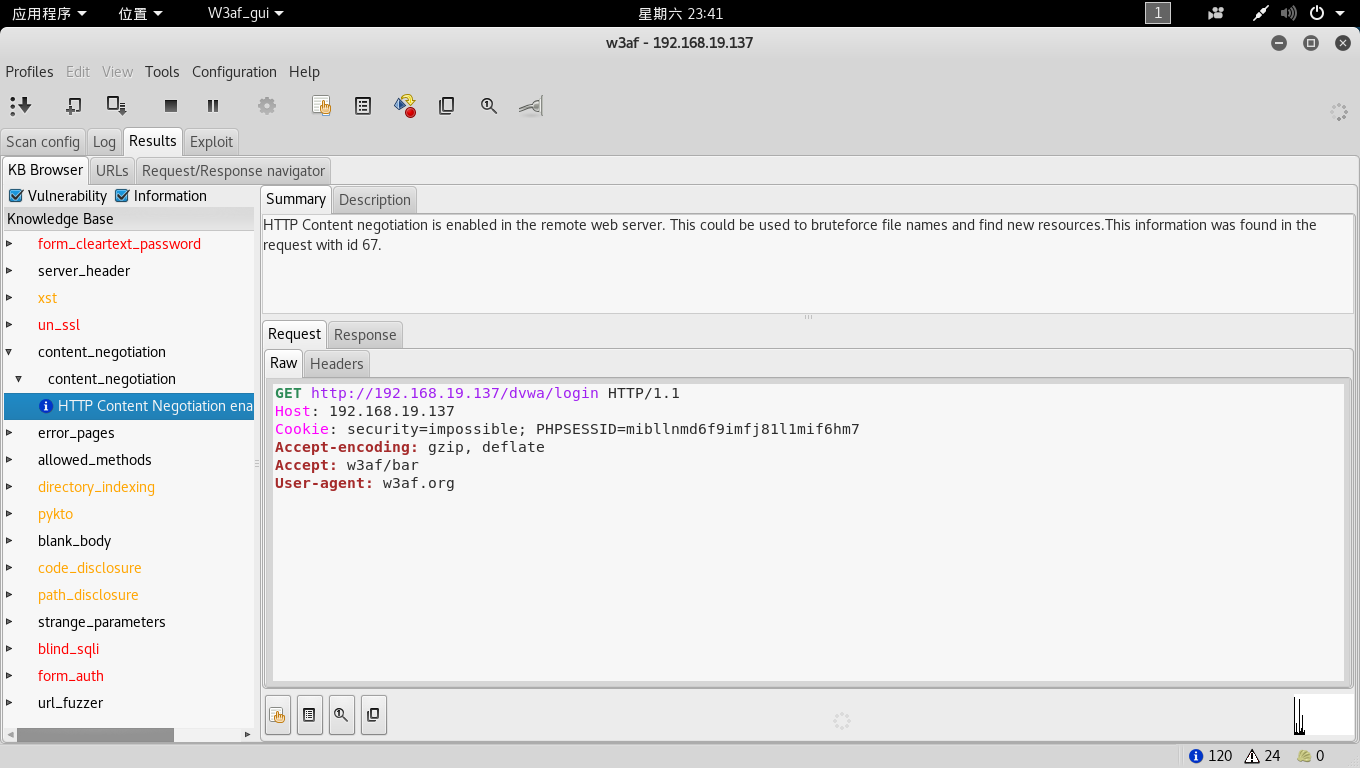


***comtent\_negotiation***

HTTP Content Negotiation enabled

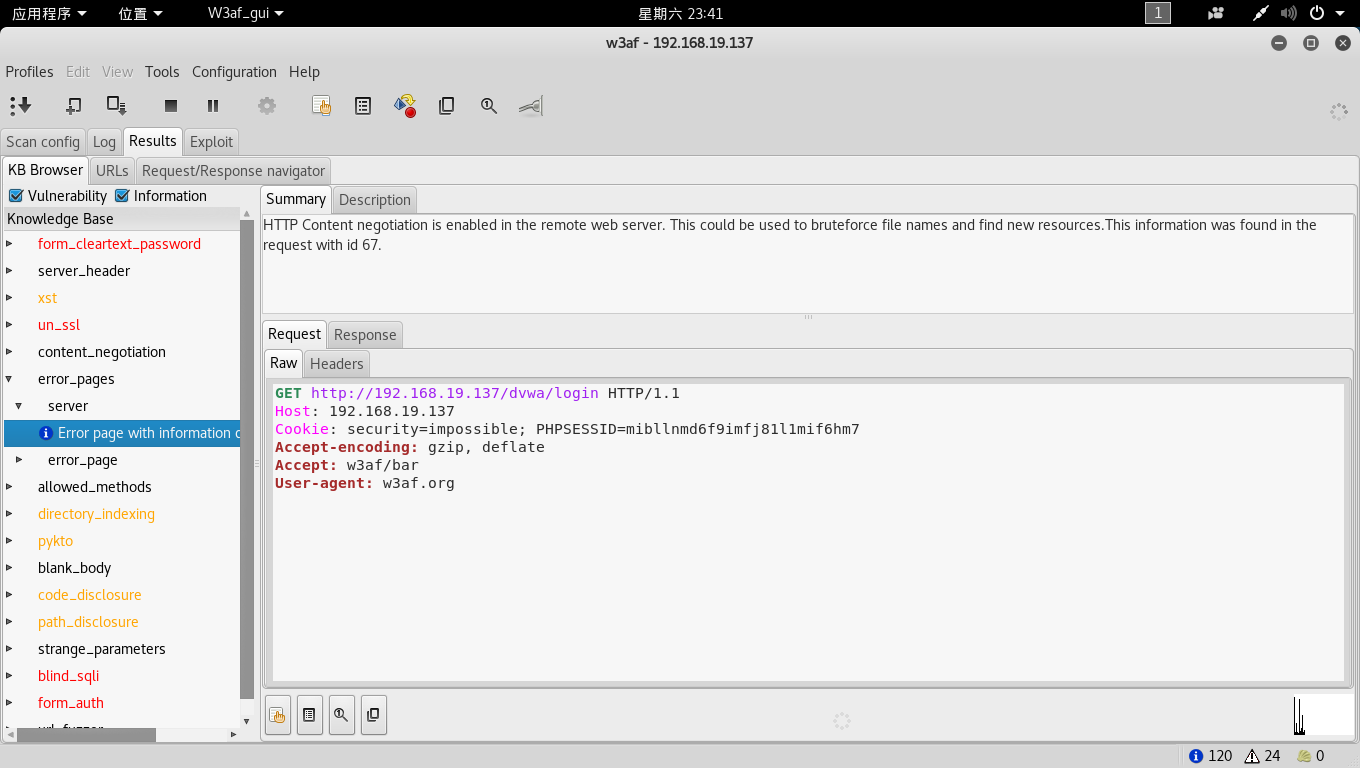
Apache mod\_negotiation模块HTML注入及HTTP响应拆分漏洞。Apache的Mod\_negotiation没有正确地过滤406 Not Acceptable响应和300 Multiple Choices消息体中的文件名，这可能导致跨站脚本攻击；此外由于也未经过滤便发送了文件名列表，因此如果文件名中包含有换行符的话还可能导致HTTP响应拆分。

参考文章：https://www.2cto.com/kf/201601/484917.html



***error\_pages***

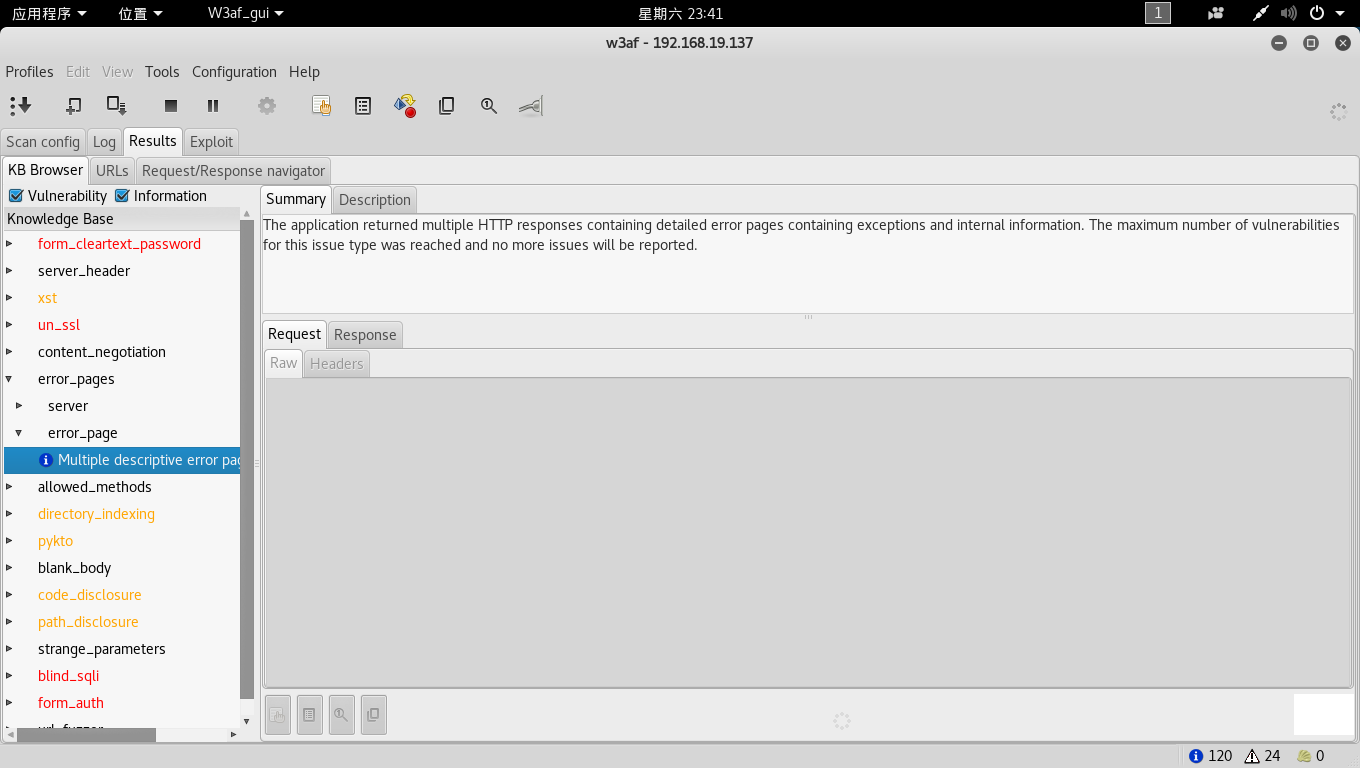
server:Error page with information disclosure



***error\_page***

Multiple descriptive error pages

应用程序返回多个HTTP响应，其中包含异常和内部信息。

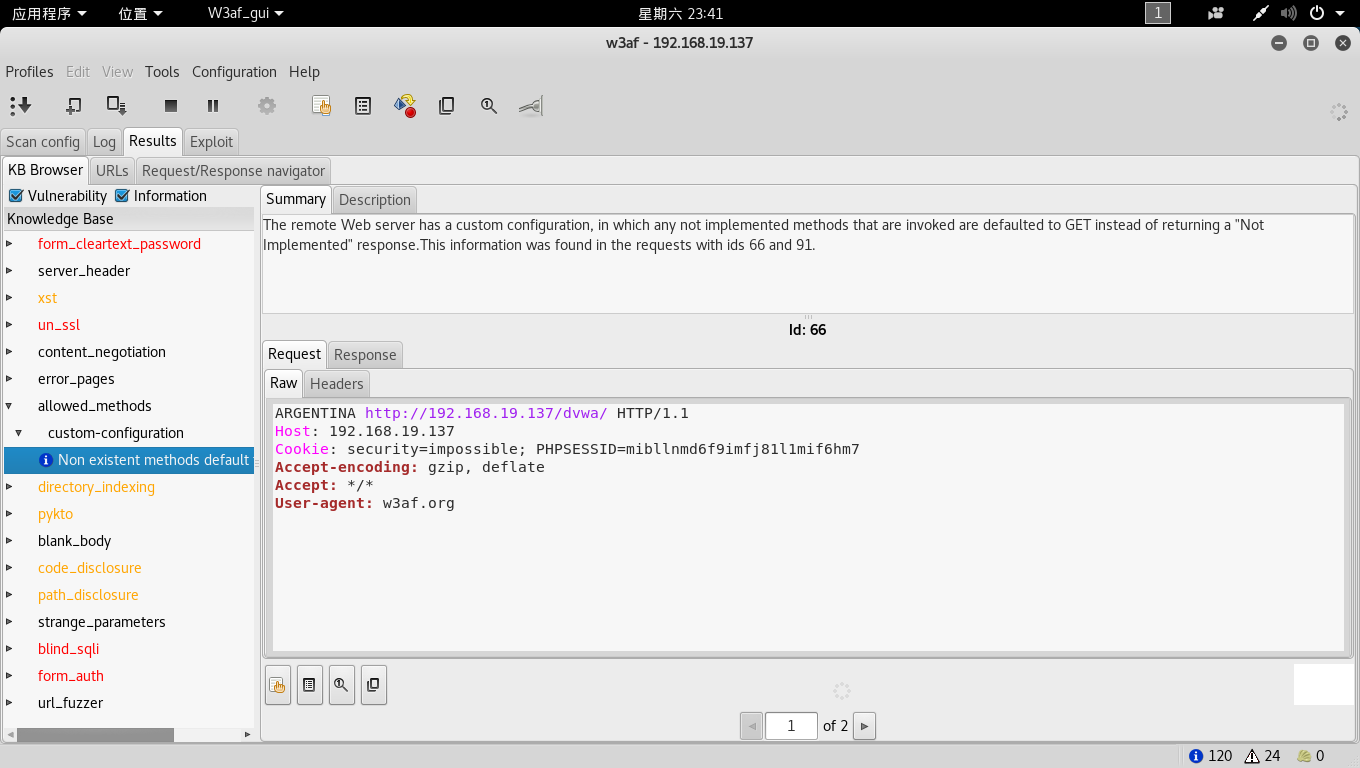


***allowes\_methods***

***custom-configuration***

Non existent methods default to GET

远程Web服务器具有自定义配置，其中未执行的任何被调用的方法都默认GET，而不是返回一个“未实现”的响应



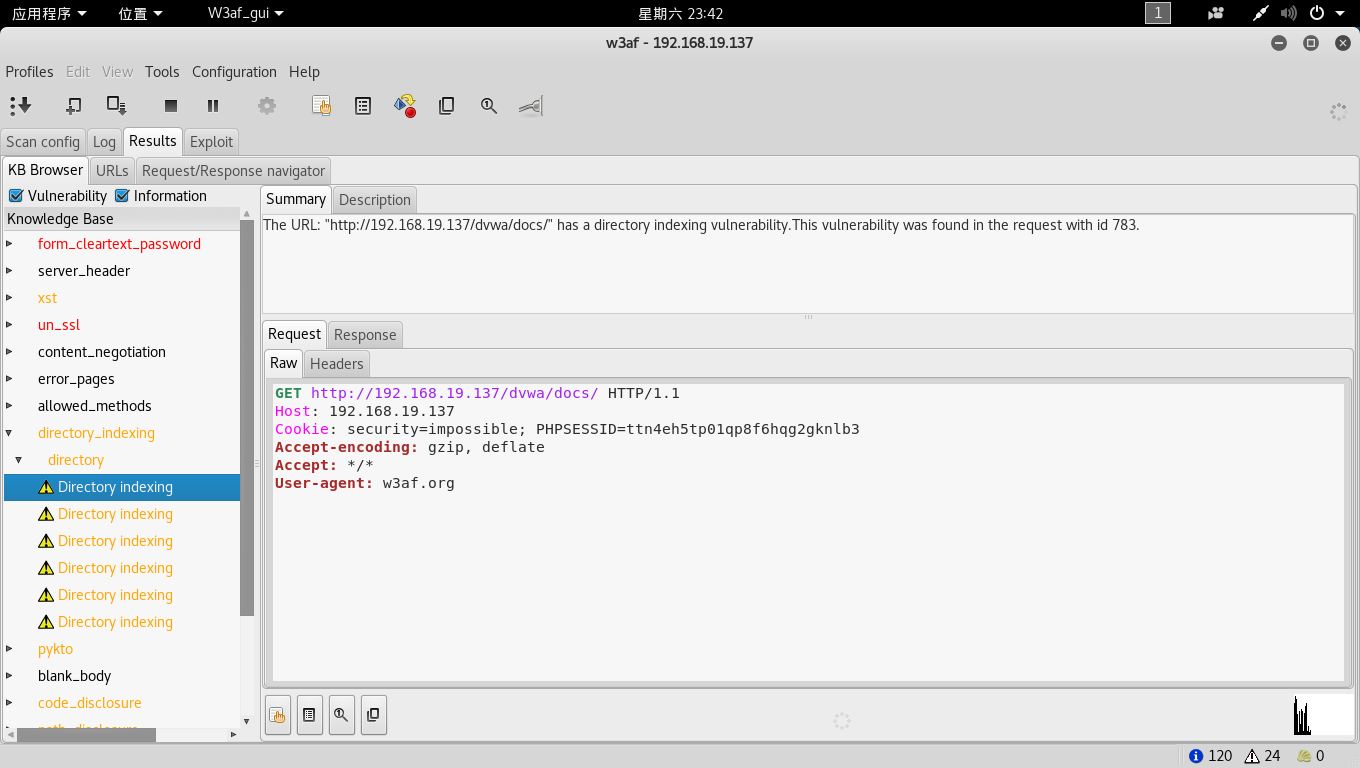
***directory\_indexing***

***directory***

Directory indexing

目录索引漏洞，攻击者可以利用此漏洞在受影响的应用程序上下文中从易受攻击的系统检索任意文件。获得的信息可能有助于攻击者进一步攻击。

在DVWA中包含http://192.168.19.137/icon/s、http://192.168.19.137/dvwa/vulnerabilities/、http://192.168.19.137/dvwa/Docs/、http://192.168.19.137/dvwa/config/、http://192.168.19.137/dvwa/external/、http://192.168.19.137/dvwa/docs/

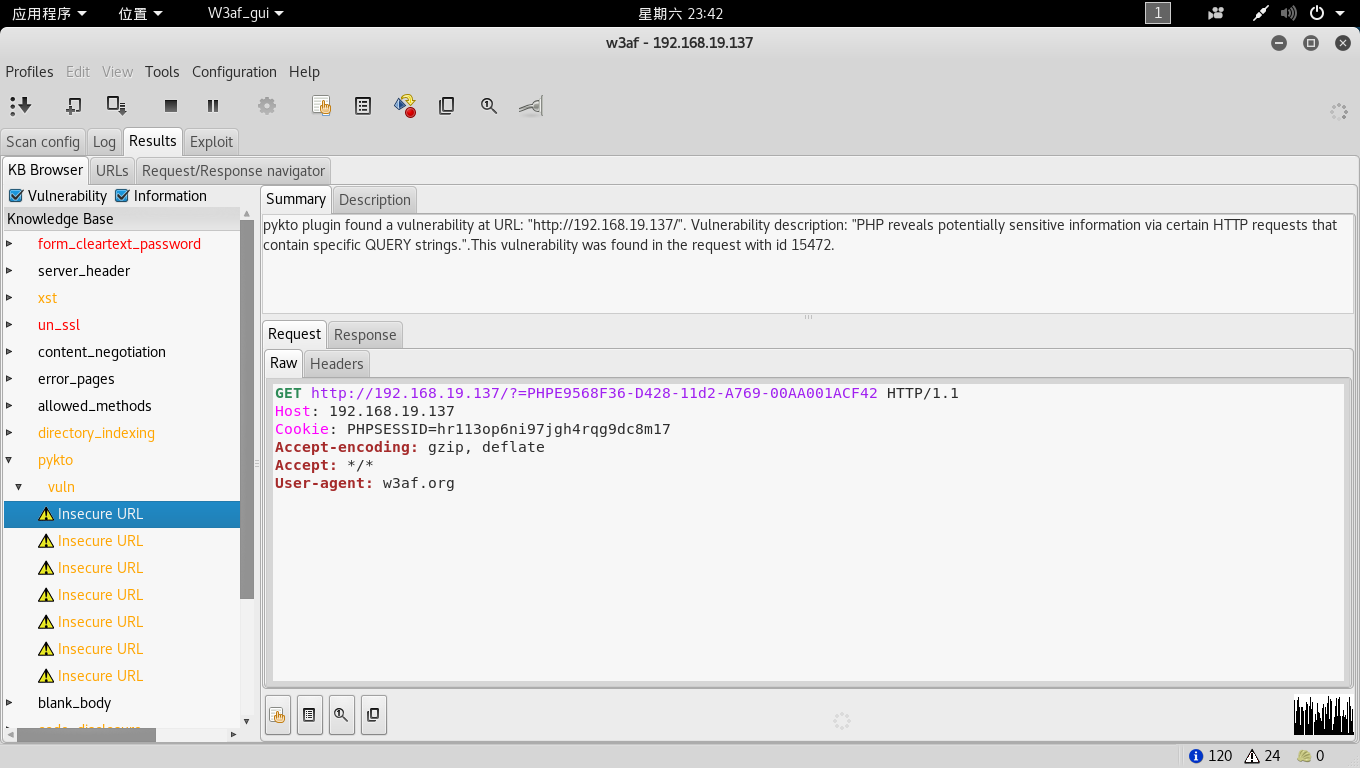


***pykto***(Nikto接口插件)

***vuln***

Insecure URL

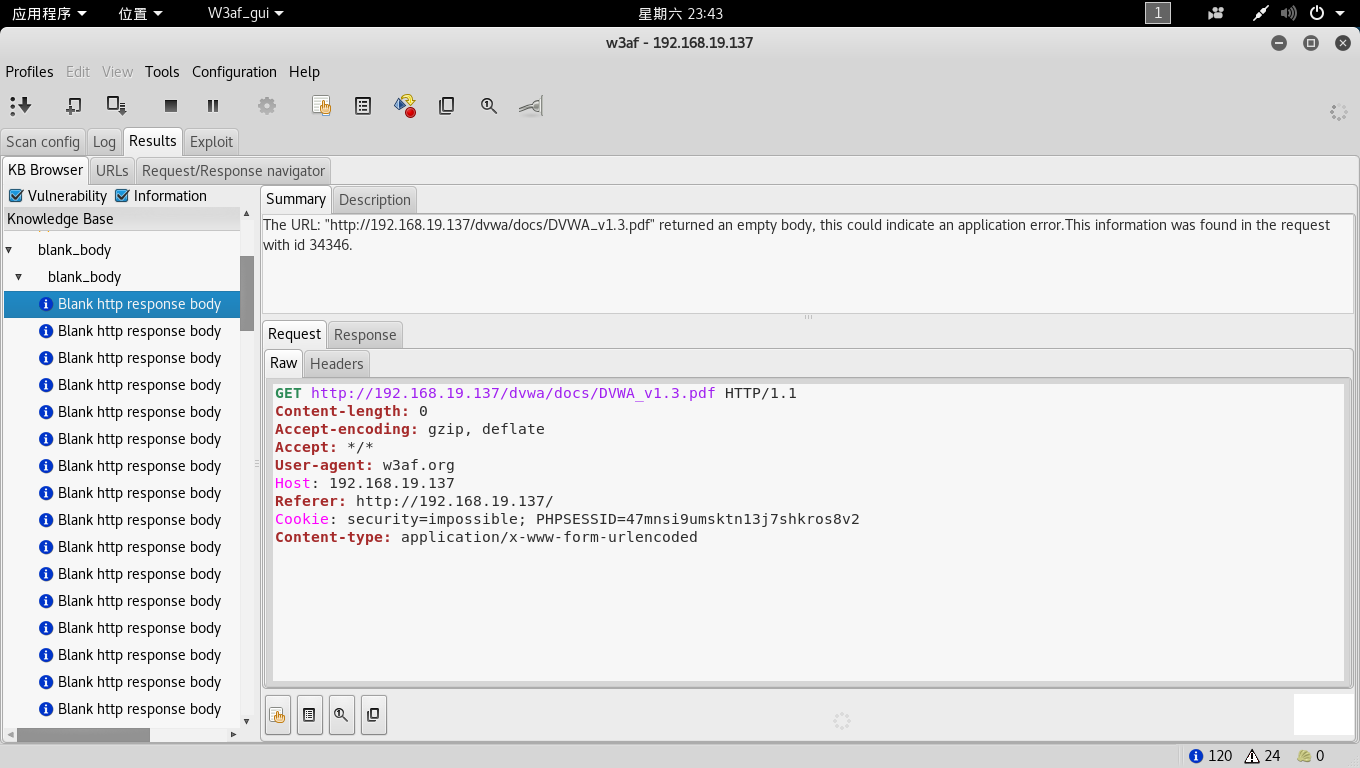
PHP通过包含特定查询字符串的某些HTTP请求揭示潜在的敏感信息。



***blank\_body***

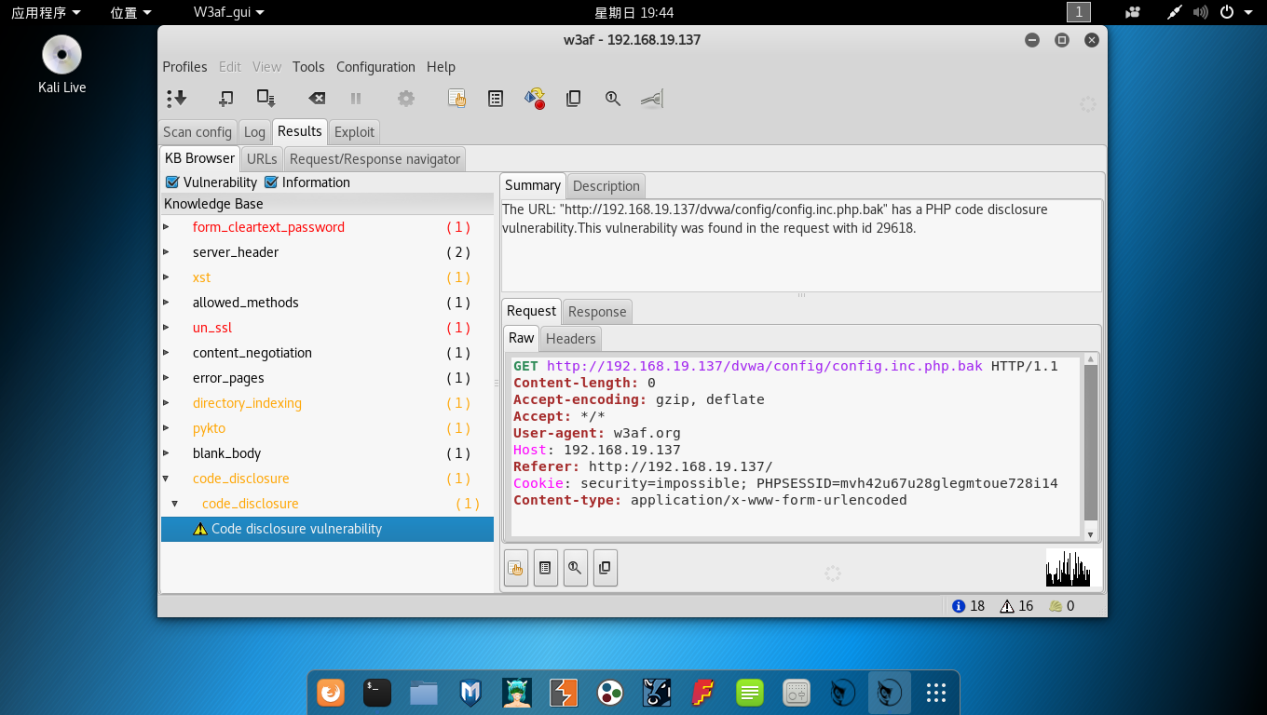
Blank http response body

URL返回空的响应体，可能是一种应用程序错误



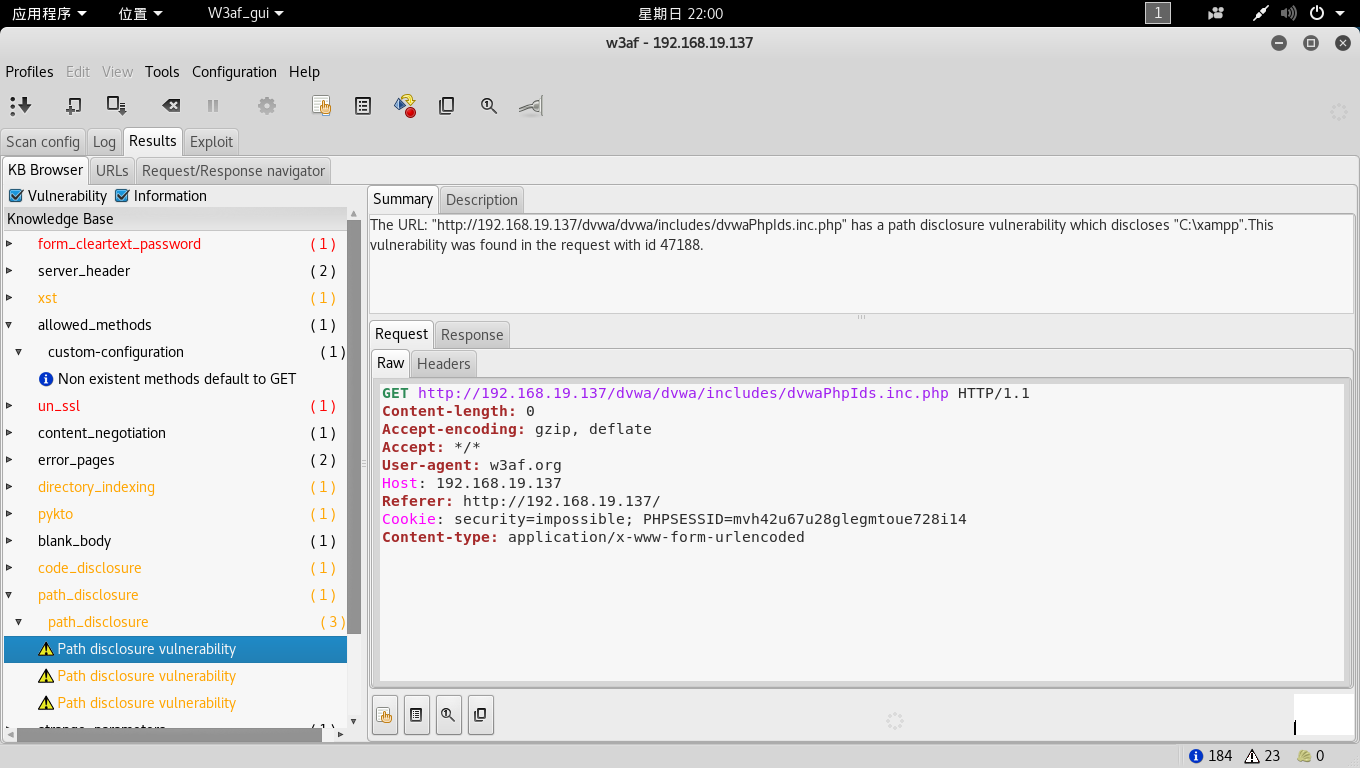
***code\_disclosure***

Code disclosure vulnerability



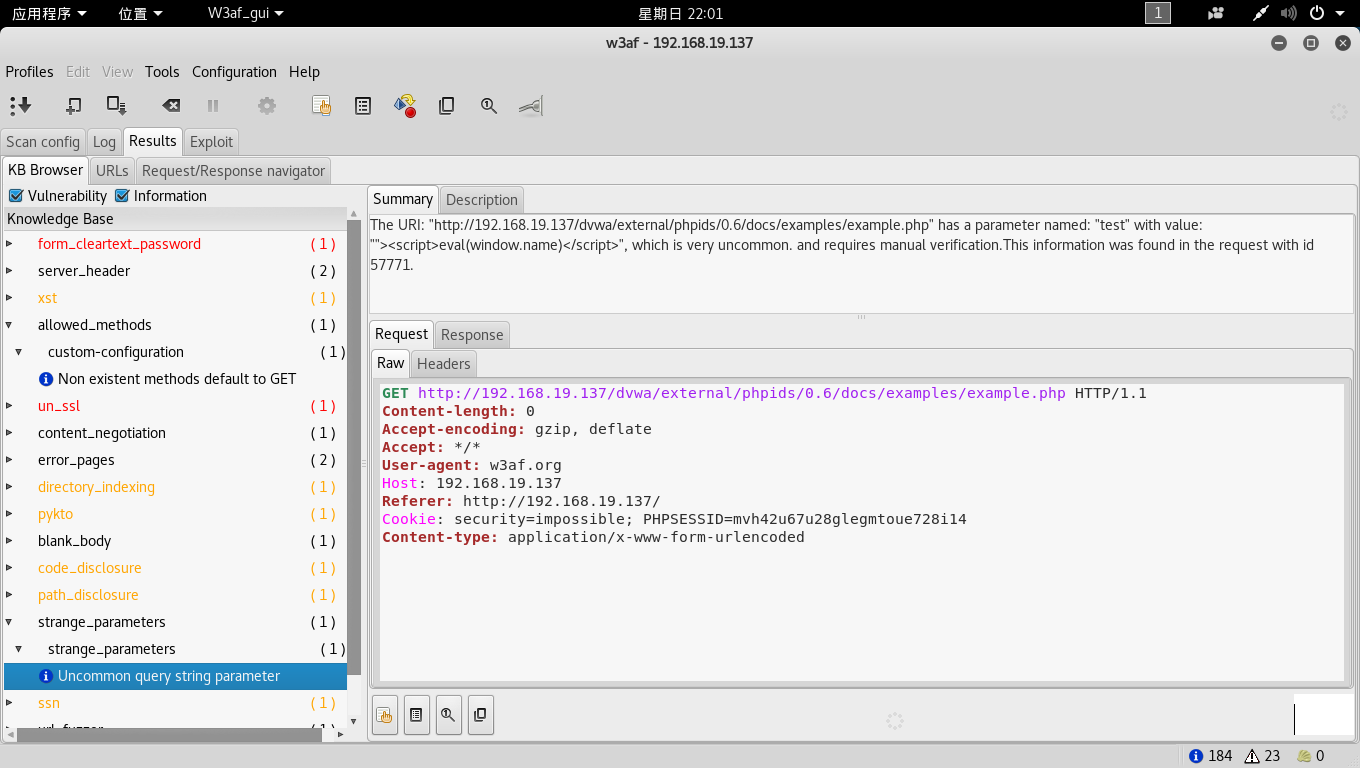
***path\_disclosure***

Path disclosure vulnerability



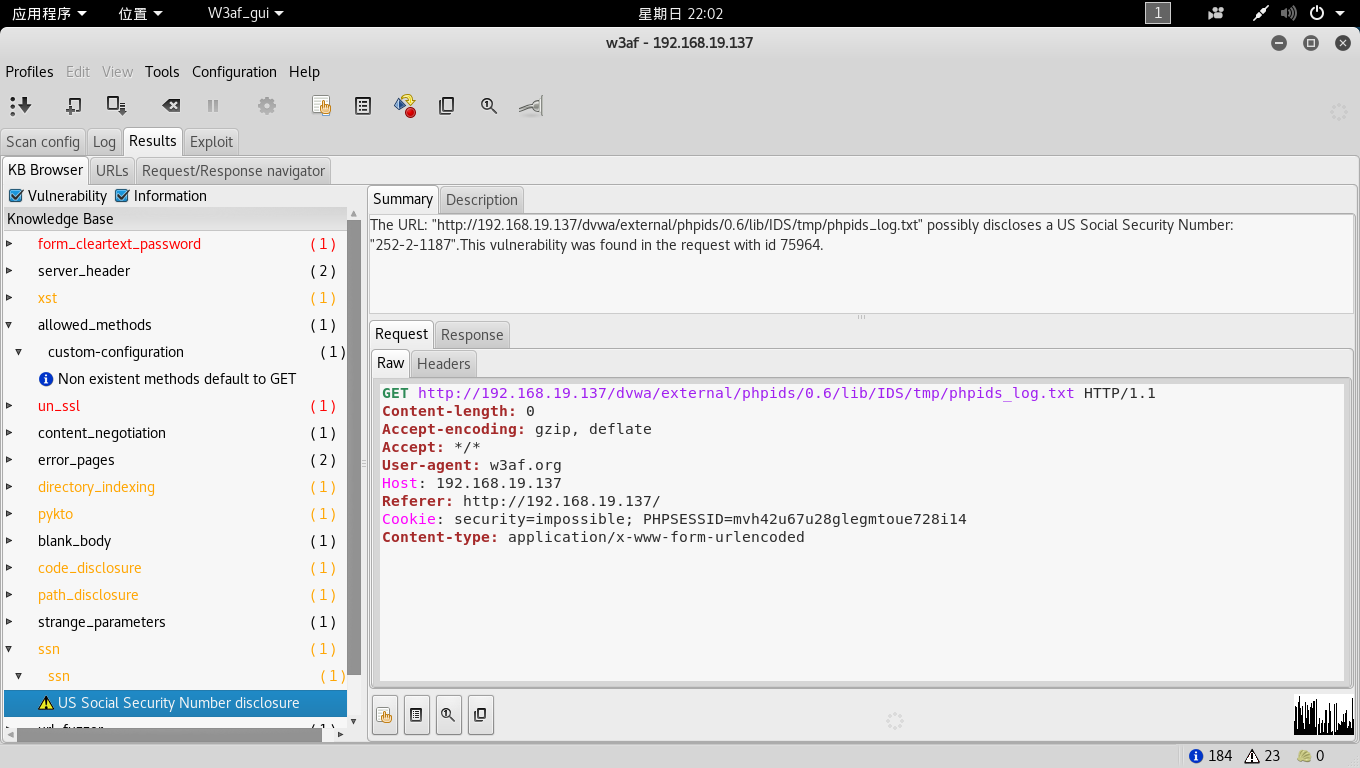
***strange\_parameters***

Uncommon query string parameter



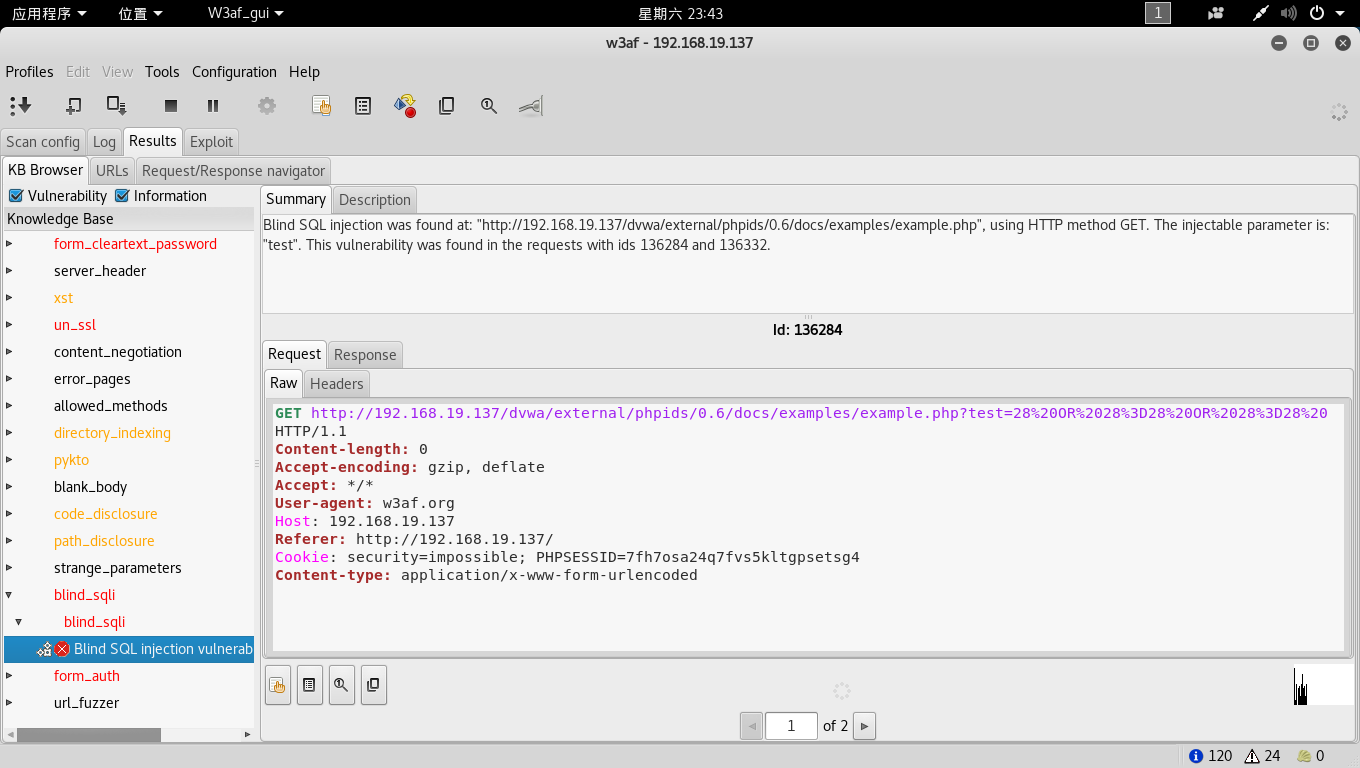
***ssn***

US Social Security Number disclosure



***blind\_sqli***

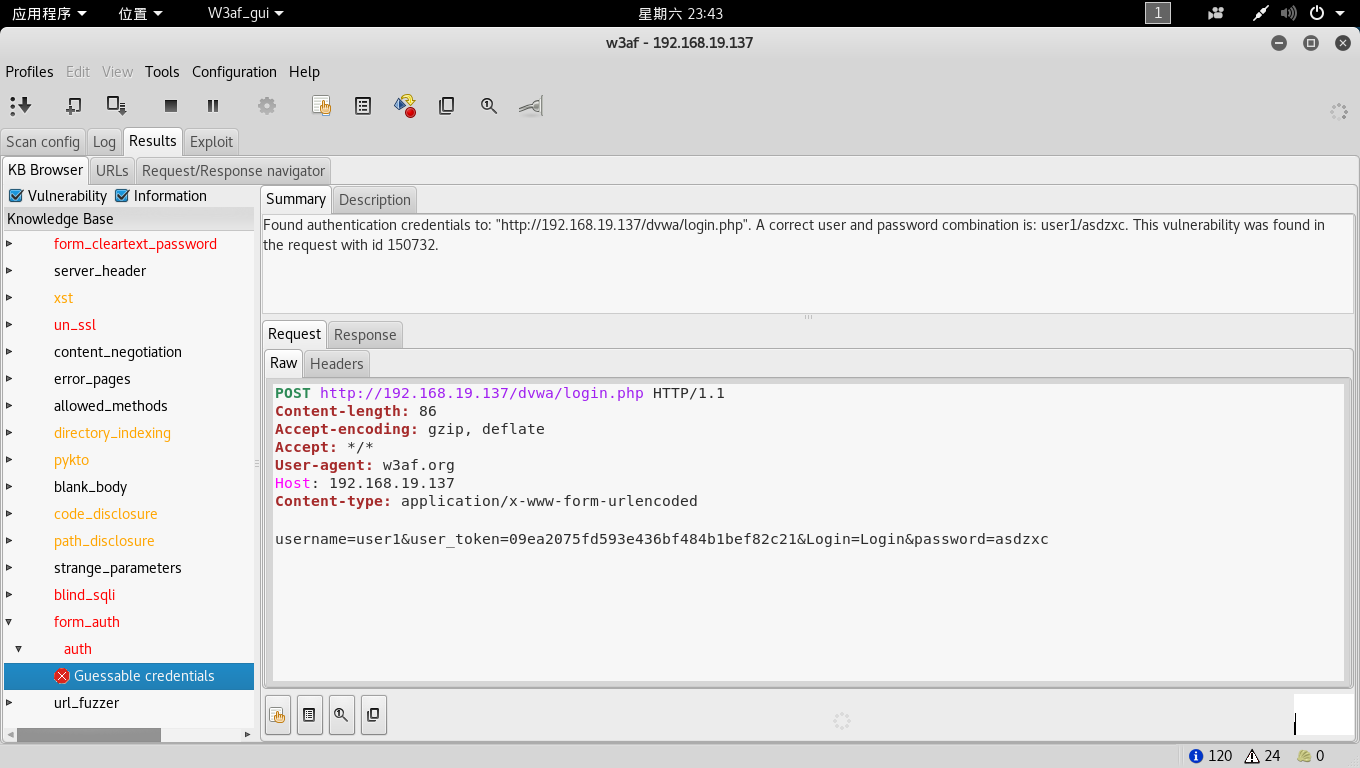
SQL注入攻击



***form\_auth***

***auth***

Guessable credentials



***url\_fuzzer***

***files***

Potentially interesting file

