Заметил, что в error.log web сервера массово сыпятся сообщения с ошибками. Смысл сообщений был в том, что кто-то очень настойчиво ломится по адресу *http://site.ru/**al_profileEdit.php?__query=edit&al=-1&al_id=vk***. Этого файла на сайте нет, поэтому сообщение попадает в лог ошибок. До кучи все эти запросы присутствуют в access.log. Все это создает лишнюю нагрузку на сервер, поэтому решил разобраться, как заблокировать этот спам.

Первым делом решил, что сайт взломали и понаоткрывали дырок. Но более внимательное изучение вопроса не показало никаких признаков взлома. Все запросы идут снаружи и обращаются к файлу, которого на сервере нет. Мониторинг не показывал никакой подозрительной активности. В логах ничего подозрительного тоже не обнаружил.

Бегло посмотрел в поиске. Нашел пару упоминаний о такой же проблеме, но простого и надежного решения не увидел. Предлагают сделать редирект куда-нибудь по этому адресу, либо закрыть файл через .htaccees. Но все это полумеры, которые не блокируют полностью запросы, а просто на них каким-то образом реагируют с наименьшими потерями.

На ум пришел простой и надежный **fail2ban**. Ранее я уже рассказывал о настройке fail2ban для защиты админки wordpress. В статье подробно все рассказано, как установить и настроить фильтры. Не буду подробно на этом останавливаться сейчас. Я просто добавлю новый фильтр, который будет навечно блокировать тех, кто будет обращаться к файлу **al_profileEdit.php** на веб сервере. Я сначала оставил дефолтные настройки блокировки на 10 минут вроде бы. Но долбили так часто, что с момента выхода из бана и до новой блокировки боты все равно успевали прилично наспамить в логи. Решил их блокировать навечно.

Создаем новый фильтр fail2ban:

```
# mcedit /etc/fail2ban/filter.d/wp-al-profileEdit.conf
```

```
[Definition]
```

```
failregex = ^<HOST> .* "GET /al_profileEdit.php
```

Этот фильтр вычленяет ip адреса всех, кто будет обращаться к файлу al_profileEdit.php на веб сервере. Данные будет брать из лог файла access.log.

Добавляем новый jail в /etc/fail2ban/jail.conf

```
[wp-al-profileEdit]
enabled = true
port = http,https
action = iptables[name=WP, port=http, protocol=tcp]
filter = wp-al-profileEdit
logpath = /web/sites/site.ru/log/access.log
maxretry = 1
bantime = -1
```

Перезапускаем fail2ban:

```
# systemctl restart fail2ban
```

и проверяем в логе как отработал. Он должен сразу забанить тех, кто успел отметиться в лог файле. Посмотреть список этих ip можно в правилах iptables:

```
# iptables -L -v -n
```

В логе самой программы тоже можно увидеть эту информацию. Теперь тот, кто обратиться к указанному файлу, тут же получит вечный бан в iptables и не будет нагружать web сервер бесполезными запросами.