# 411: A Framework for Managing Security Alerts

Kai Zhong
@sixhundredns

Ken Lee
@kennysan

# 411: A Fr[illegible]rk for Ma[illegible] Security Alerts

OPEN SOURCE!

Kai Zhong
@sixhundredns

Ken Lee
@kennysan

# Who Are We?

# KZER

Kai Zhong

Product Security Engineer @ Etsy

I wear many hats

Twitter: @sixhundredns





# KLEE

Ken Lee

Senior Product Security Engineer @ Etsy

Spoke at Defcon 21 about Content Security Policy

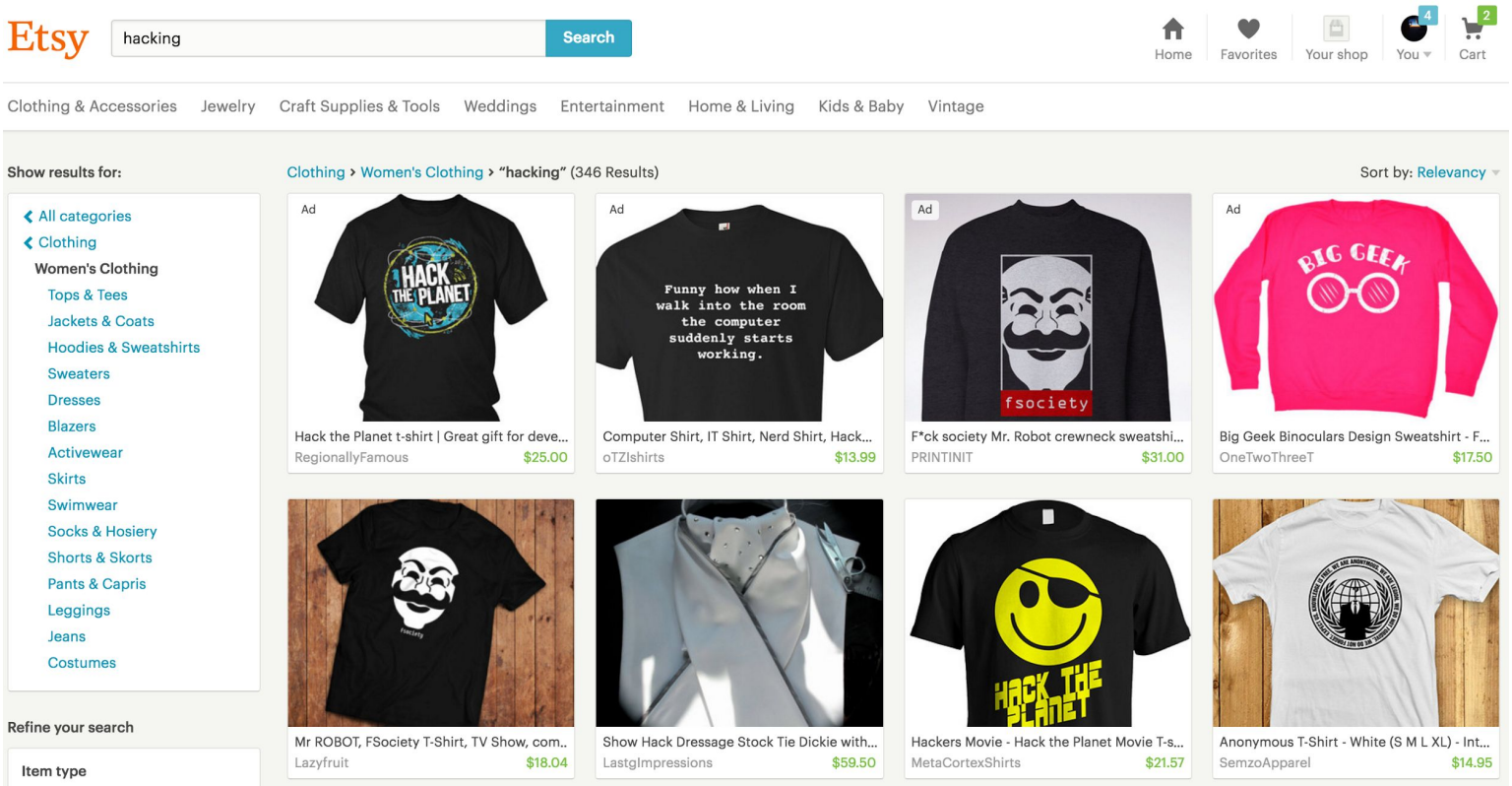
Loves funny cat gifs

Twitter: @Kennysan





# What is Etsy?


Etsy
hacking
Search
Home
Favorites
Your shop
You
Cart
Clothing & Accessories
Jewelry
Craft Supplies & Tools
Weddings
Entertainment
Home & Living
Kids & Baby
Vintage
Show results for:
All categories
Clothing
Women's Clothing
Tops & Tees
Jackets & Coats
Hoodies & Sweatshirts
Sweaters
Dresses
Blazers
Activewear
Skirts
Swimwear
Socks & Hosiery
Shorts & Skorts
Pants & Capris
Leggings
Jeans
Costumes
Refine your search
Item type
Clothing › Women's Clothing › "hacking" (346 Results)
Sort by: Relevancy
Ad
Hack the Planet t-shirt | Great gift for deve...
RegionallyFamous $25.00
Ad
Funny how when I walk into the room the computer suddenly starts working.
Computer Shirt, IT Shirt, Nerd Shirt, Hack...
oTZIshirts $13.99
Ad
fsociety
F*ck society Mr. Robot crewneck sweatshi...
PRINTINIT $31.00
Ad
BIG GEEK
Big Geek Binoculars Design Sweatshirt - F...
OneTwoThreeT $17.50
Mr ROBOT, FSociety T-Shirt, TV Show, com..
Lazyfruit $18.04
Show Hack Dressage Stock Tie Dickie with...
LastgImpressions $59.50
HACK THE PLANET
Hackers Movie - Hack the Planet Movie T-s...
MetaCortexShirts $21.57
Anonymous T-Shirt - White (S M L XL) - Int...
SemzoApparel $14.95


SECURITY
Etsy

# What Are We Covering?



# History

# The Problem(s)

# Our Solution

# Alert Management @ Etsy

# More Examples

# Demo

# But First, Some Terminology



# Logs

```
[Sun Jul 24 06:29:39.622074 2016] [ssl:warn] [pid 10539] AH02292: Init: Name-based SSL virtual hosts only work for clients with TLS server name indication support (RFC 4366)
[Sun Jul 24 06:29:39.622234 2016] [mpm_prefork:notice] [pid 10539] AH00163: Apache/2.4.7 (Ubuntu) PHP/5.5.9-1ubuntu4.17 OpenSSL/1.0.1f configured -- resuming normal operations
[Sun Jul 24 06:29:39.622252 2016] [core:notice] [pid 10539] AH00094: Command line: '/usr/sbin/apache2'
[Sun Jul 24 16:14:27.487249 2016] [:error] [pid 19397] [client 127.0.0.1:61356] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fplugin-install.php&reauth=1
[Sun Jul 24 16:14:27.560486 2016] [:error] [pid 19398] [client 127.0.0.1:61357] Duo cookie with name: duo_secure_wordpress_auth_cookie not found. Start two factor authentication.
SSL: 1, referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fplugin-install.php&reauth=1
[Sun Jul 24 16:14:27.563980 2016] [:error] [pid 19397] [client 127.0.0.1:61356] Duo cookie with name: duo_secure_wordpress_auth_cookie not found. Start two factor authentication.
SSL: 1, referer: https://wp.fouroneone.io/wp-admin/admin.php?page=wsal-auditlog
[Sun Jul 24 16:14:37.642356 2016] [:error] [pid 19401] [client 127.0.0.1:61362] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-admin/plugin-install.php
[Sun Jul 24 16:14:53.421014 2016] [:error] [pid 19398] [client 127.0.0.1:61376] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fplugins.php&reauth=1
[Sun Jul 24 16:14:53.492853 2016] [:error] [pid 19398] [client 127.0.0.1:61376] Duo cookie with name: duo_secure_wordpress_auth_cookie not found. Start two factor authentication.
SSL: 1, referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fplugins.php&reauth=1
[Sun Jul 24 16:15:01.952409 2016] [:error] [pid 20146] [client 127.0.0.1:61388] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-admin/plugins.php
[Sun Jul 24 16:15:27.429473 2016] [:error] [pid 19400] [client 127.0.0.1:61392] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fadmin.php%3Fpage%3Dwsal-
settings&reauth=1
[Sun Jul 24 16:15:27.491539 2016] [:error] [pid 19400] [client 127.0.0.1:61392] Duo cookie with name: duo_secure_wordpress_auth_cookie not found. Start two factor authentication.
SSL: 1, referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fadmin.php%3Fpage%3Dwsal-settings&reauth=1
[Sun Jul 24 16:15:37.433204 2016] [:error] [pid 19412] [client 127.0.0.1:61398] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-admin/admin.php?page=wsal-settings
[Sun Jul 24 16:18:16.853434 2016] [:error] [pid 21242] [client 127.0.0.1:61516] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fedit.php&reauth=1
[Sun Jul 24 16:18:16.916996 2016] [:error] [pid 21242] [client 127.0.0.1:61516] Duo cookie with name: duo_secure_wordpress_auth_cookie not found. Start two factor authentication.
SSL: 1, referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2Fedit.php&reauth=1
[Sun Jul 24 16:18:26.072769 2016] [:error] [pid 20146] [client 127.0.0.1:61520] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1] data
[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[127.0.0.1] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-admin/edit.php
[Mon Jul 25 10:24:16.648713 2016] [:error] [pid 19423] [client 216.0.145.50:52878] dbg [NONE] SELECT * FROM `sites` WHERE `host` IN (?) AND `archived` = ? 0:[demo.fouroneone.io] 1:
[0], referer: https://demo.fouroneone.io/login?redirect=/alerts
[Mon Jul 25 10:24:16.649246 2016] [:error] [pid 19423] [client 216.0.145.50:52878] dbg [NONE] SELECT `value` FROM `config` WHERE `site_id` = ? AND `key` = ? 0:[1] 1:[cookie_secret],
referer: https://demo.fouroneone.io/login?redirect=/alerts
[Mon Jul 25 10:24:16.657020 2016] [:error] [pid 19423] [client 216.0.145.50:52878] dbg [NONE] SELECT * FROM `users` WHERE `user_id` IN (NULL) AND `site_id` = ? AND `archived` = ? 0:
[1] 1:[0], referer: https://demo.fouroneone.io/login?redirect=/alerts
[Mon Jul 25 16:47:40.022210 2016] [:error] [pid 21242] [client 216.0.145.50:46091] [audit] migrated:[] type:[1000] category:[Other User Activity] message:[User logged in] site:[1]
data:[Username:[tango] CurrentUserRoles:[0:[administrator] 1:[superadmin]] ClientIP:[216.0.145.50] UserAgent:[Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36]], referer: https://wp.fouroneone.io/wp-login.php?redirect_to=https%3A%2F%2Fwp.fouroneone.io%2Fwp-admin%2F&reauth=1
[Mon Jul 25 16:47:40.070685 2016] [:error] [pid 21242] [client 216.0.145.50:46091] Duo cookie with name: duo_secure_wordpress_auth_cookie not found. Start two factor authentication.
```

# The ELK Stack



elastic



logstash







# logstash

# Logstash

Data processor and log shipper

# Logstash

Data processor and log shipper

Allows you to break out your log data into separate fields

# Logstash

Data processor and log shipper

Allows you to break out your log data into separate fields

We use it to ship logs into Elasticsearch!



elasticsearch

# Elasticsearch

Distributed, real-time search engine

# Elasticsearch

Distributed, real-time search engine

Allows storing complex, nested documents

# Elasticsearch

Distributed, real-time search engine

Allows storing complex, nested documents

Allows generating statistics over your data

# Elasticsearch

Distributed, real-time search engine

Allows storing complex, nested documents

Allows generating statistics over your data

We use it for analyzing logs!

# Kibana

Data visualization frontend for Elasticsearch

# Kibana

Data visualization frontend for Elasticsearch

Log discovery

# Kibana

Data visualization frontend for Elasticsearch

Log discovery

Visualizations!


Logstash Search
2 days ago to 3 minutes ago
QUERY
bytes:[0 TO 4000000] AND @tags:success
FILTERING
EVENTS OVER TIME
View | Zoom Out | html (ext) (868) php (ext) (659) png (ext) (317) gif (ext) (229) css (ext) (121) count per 30m | (2214 hits)
60
50
40
30
20
10
0
00:00 02-24
04:00 02-24
08:00 02-24
12:00 02-24
16:00 02-24
20:00 02-24
00:00 02-25
04:00 02-25
08:00 02-25
12:00 02-25
16:00 02-25
20:00 02-25
MAP
REVENUE
22%
VOLUME
9%
TOP DESTINATIONS
Other values 42%
CN 19%
IN 16%
TOP SOURCES
Other values 52%
IN 19%
US 10%
GEO PAIRS
100
80
60
40
20
0
ALL EVENTS
0 to 100 of 500 available for paging
Fields
Type to filter...
@message
@tags
@tags
geo.srcdst
extension
clientip
bytes
id
phpmemory
response
success,security MY:VN html 167.12.22.189 8540 1066 200
success,info IT:MM png 164.87.170.73 2045 1903 200
success,info AR:ES html 222.23.102.238 1801 1133 200
success,info IN:DZ html 138.226.66.81 7029 1801 200

# History

# Switching to ELK

Work started in mid 2014

# Switching to ELK

Work started in mid 2014

Finished in mid 2015

# Switching to ELK

Work started in mid 2014

Finished in mid 2015

We learned a lot from the migration

# Switching to ELK

Work started in mid 2014

Finished in mid 2015

We learned a lot from the migration

And got a bunch of great tools out of it

# It Was A Bumpy Road

Hiccups are expected when moving to a new technology

# It Was A Bumpy Road

Hiccups are expected when moving to a new technology

Had to deal with annoying, performance-impacting bugs

# It Was A Bumpy Road

Hiccups are expected when moving to a new technology

Had to deal with annoying, performance-impacting bugs

Security was concerned about the usability of ELK

# It Was A Bumpy Road

Hiccups are expected when moving to a new technology

Had to deal with annoying, performance-impacting bugs

Security was concerned about the usability of ELK

ELK didn’t have functionality to help us monitor attacks in real time

ANANDTECH

Logi

ABOUT B

PC COMPONENTS ▼ SMARTPHONES & TABLETS ▼ SYSTEMS ▼ ENTERPRI

TRENDING TOPICS | GPUS | SMARTPHONES | AMD | MOBILE | STORAGE | RADEON | INTEL | POLARIS

Home > Storage

# Samsung Acknowledges the SSD 840 EVO Read Performance Bug - Fix Is on the Way

116 Comments

+ Add A Comment

by Kristian Vättö on September 19, 2014 3:23 PM EST

Posted in Storage | SSDs | Samsung | TLC | 840 EVO




ANANDTECH

Logi

ABOUT B

PC COMPONENTS ▼ SMARTPHONES & TABLETS ▼ SYSTEMS ▼ ENTERPRI

TRENDING TOPICS | GPUS | SMARTPHONES | AMD | MOBILE | STORAGE | RADEON | INTEL | POLARIS

Home > Storage

# New Samsung SSD 840 EVO Read Performance Fix Coming Later This Month

76 Comments

+ Add A Comment

by Kristian Vättö on April 14, 2015 1:40 PM EST

Posted in Storage | SSDs | Samsung | TLC | 840 EVO



We have some emergency ELK downtime coming in a few minutes.
It seems we've run into a new kernel bug with NFS mounts, which is causing backups to fail, and causing elasticsearch to behave badly :-(

We're going to try and keep this as fast as possible and hopefully we'll be back up and also caught up on replication in a few hours.




Struggle Bus Coffee Mug | Funny Mug Gift

shopHelloGinger $16.00

# The Problem(s)

# Search scheduling?

## Reactive Security Mechanisms

Reactive security mechanisms usually consist of real-time event monitoring and alerting. These security mechanisms focus on events that trigger immediate responses based on regular information querying: they query the same data and they query it often.

Some examples of reactive security mechanisms at Etsy are automated Splunk searches and anomaly detection based on StatsD/Graphite logs.

# No Search Scheduling

Security heavily relied on Splunk scheduled searches for alerting

# No Search Scheduling

Security heavily relied on Splunk scheduled searches for alerting

No equivalent for ES at the time

# No Search Scheduling

Security heavily relied on Splunk scheduled searches for alerting

No equivalent for ES at the time

No web UI for managing searches

# An Unfamiliar Query Language

Our alerts were complex SPL (Splunk Processing Language) queries

# An Unfamiliar Query Language

Our alerts were complex SPL (Splunk Processing Language) queries

ES’s query language is less robust

# An Unfamiliar Query Language

Our alerts were complex SPL (Splunk Processing Language) queries

ES’s query language is less robust

Some things were non-obvious coming from SPL

# The Road to ELK Integration



# The Road to ELK Integration

We needed a query language for building complex queries without code

# The Road to ELK Integration

We needed a query language for building complex queries without code

We needed a mechanism to run and manage these queries

# The Road to ELK Integration

We needed a query language for building complex queries without code

We needed a mechanism to run and manage these queries

Preferably before we turned off Splunk ; )

# ESQuery

# Features

Superset of the standard Lucene syntax

# Features

Superset of the standard Lucene syntax

Syntactically similar to SPL!

# Features

Superset of the standard Lucene syntax

Syntactically similar to SPL!

Supports all the functionality we need!!!

# Syntax

| Command | Syntax |
| --- | --- |
| Inline params | `$size:20 $sort:user_id $fields:[a,b,c]` |
| Joins | `* \| join source:src_ip target:dst_ip` |
| Aggregations | `* \| agg:terms field:src_ip`<br>`  \| agg:terms field:user_id` |
| Variable substitution | `src_ip:@internal_ips` |

# SPL

```
source="/data/syslog/current/web/info.log" log_namespace="login"

reason="wrong password" response=403 | top 10 remote_host
```

```
{  "query": {
    "filtered": {
      "query": {
        "bool": {
          "minimum_number_should_match": 1,
          "should": [
            {
              "query_string": {
                "query": "type:web_info_log log_namespace:login logdata.reason:\"wrong password\" response:403 ",
                "default_operator": "AND",
                "lowercase_expanded_terms": false,
                "allow_leading_wildcard": false
      }}]}},
      "filter": {
        "bool": {
          "must": [
            {
              "range": {
                "event_timestamp": {
                  "from": 1468294422783,
                  "to": 1468295322783
  }}}]}}},
  "size": 0,
  "sort": [
    {
      "event_timestamp": {
        "order": "desc",
        "ignore_unmapped": true
    }},
    {
      "event_timestamp": {
        "order": "desc",
        "ignore_unmapped": true
  }}],
  "aggs": {
    "terms_bucket": {
      "terms": {
        "field": "logdata.remote_host",
        "size": 10
}}}}
```

# ESQuery

```
type:web_info_log log_namespace:login

logdata.reason:"wrong password" -response:403 |

agg:terms field:logdata.remote_host size:10
```

# splogTASH SPL to lucene translator

source="/data/syslog/current/web/info.log" "Response to reCAPTCHA" status="incorrect" | transaction ip | where eventcount > 250

Go

```
type:web_info_log AND "Response to reCAPTCHA" status:"incorrect" | agg:terms field:ip min_doc_count: 250
```

ENTER SPLUNK QUERY. CLICK GO. TEST QUERY ON KIBANA.

411

# Alert Management

Write queries to be automatically executed

# Alert Management

Write queries to be automatically executed

Receive email alerts whenever there are results

# Alert Management

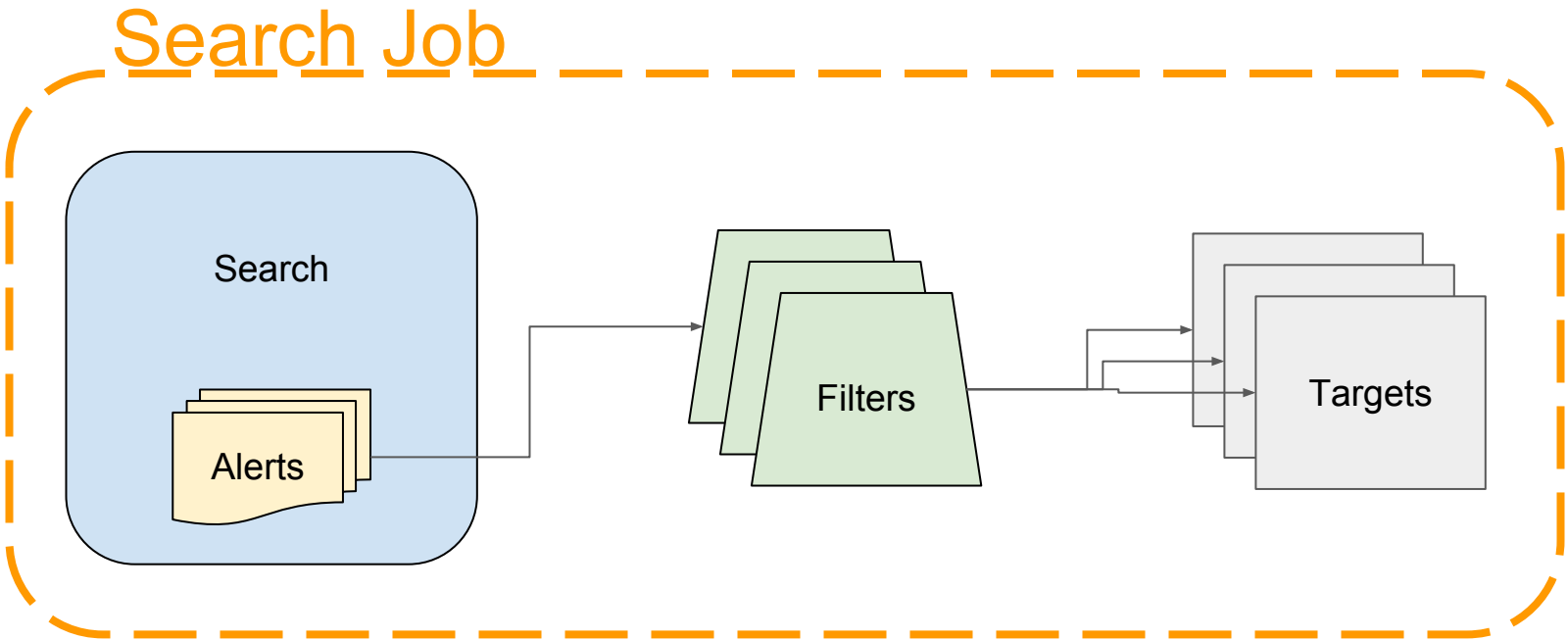
Write queries to be automatically executed

Receive email alerts whenever there are results

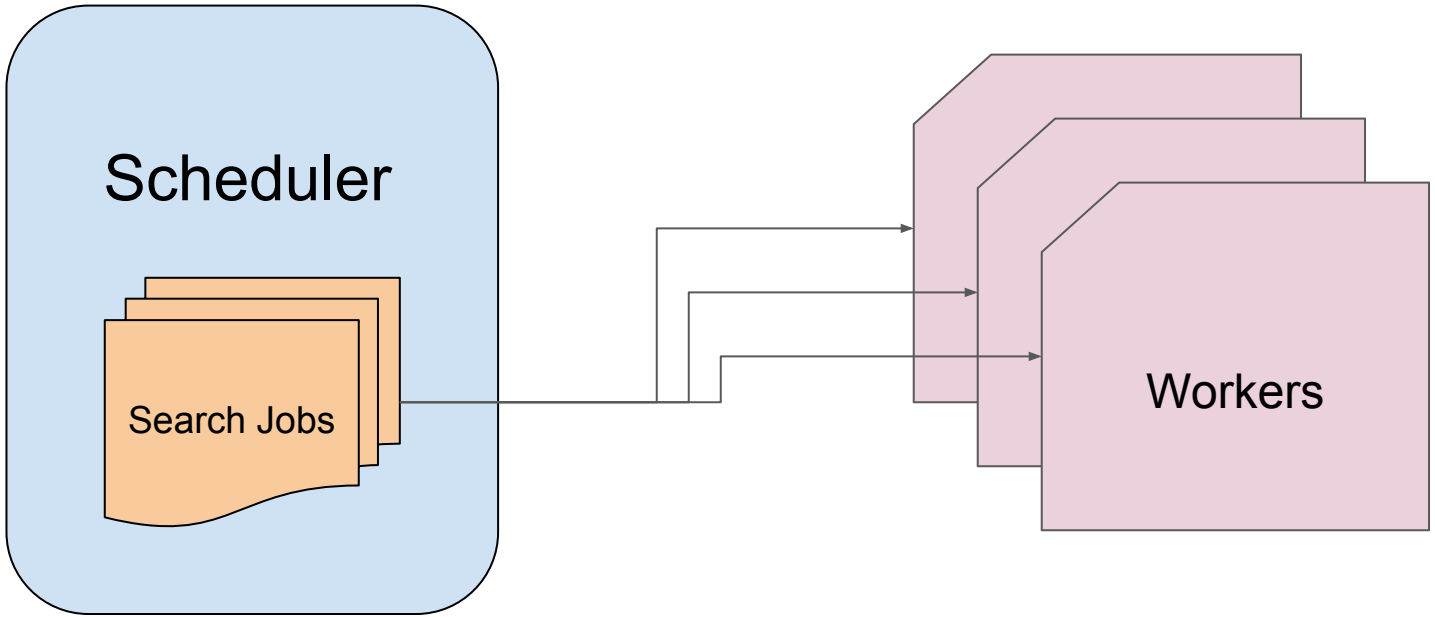
Manage alerts through the web interface

# Scheduling

# Under the Hood



# Under the Hood



# Dashboard

Sec411 / Index

Me

Sec411 | Alerts | Searches | Groups | Lists | Kai Zhong

# Stats

**242** Alerts are active (242 New, 0 In Progress)

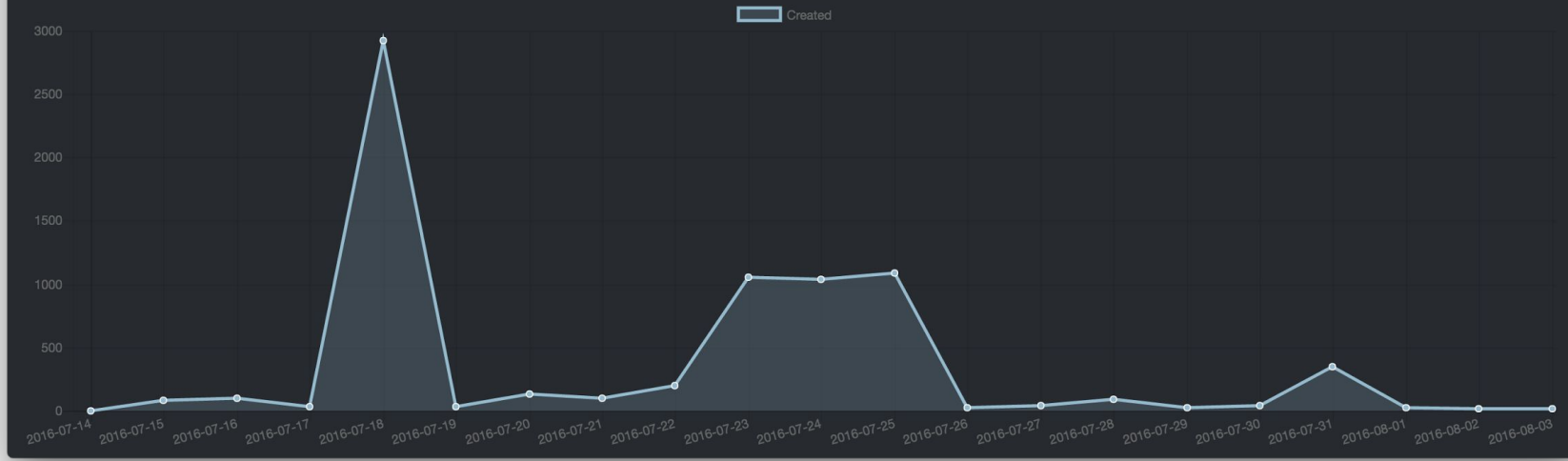
**242** of them are high priority

**0** of them are medium priority

**0** of them are low priority

**0** of them are stale

## Alerts in the last 20 days



Sec411 / Index

Me

Sec411 | Alerts | Searches | Groups | Lists | Kai Zhong

# Stats

**242** Alerts are active (242 New, 0 In Progress)

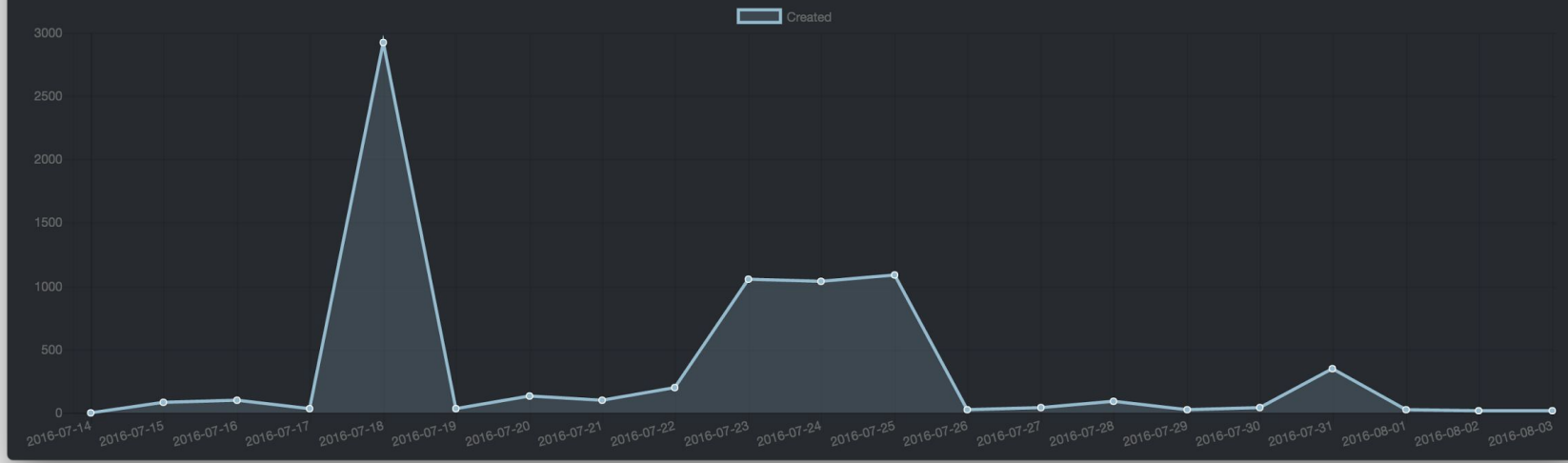
**242** of them are high priority

**0** of them are medium priority

**0** of them are low priority

**0** of them are stale

## Alerts in the last 20 days



Sec411 / Index

Me

Sec411 | Alerts | Searches | Groups | Lists | Kai Zhong

# Stats

**242** Alerts are active (242 New, 0 In Progress)

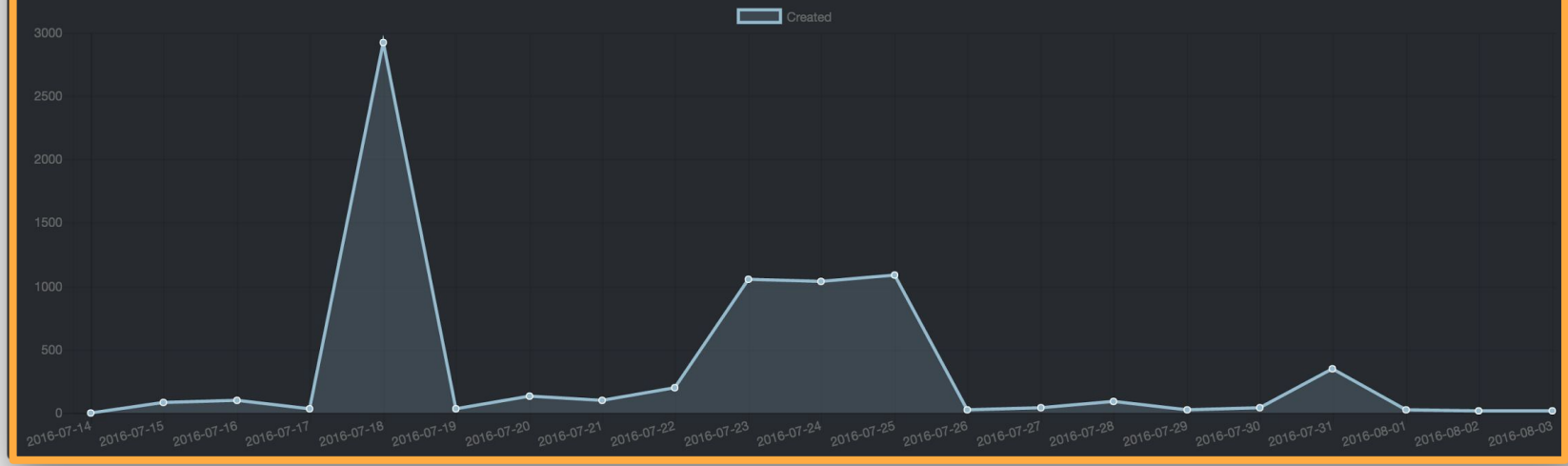
**242** of them are high priority

**0** of them are medium priority

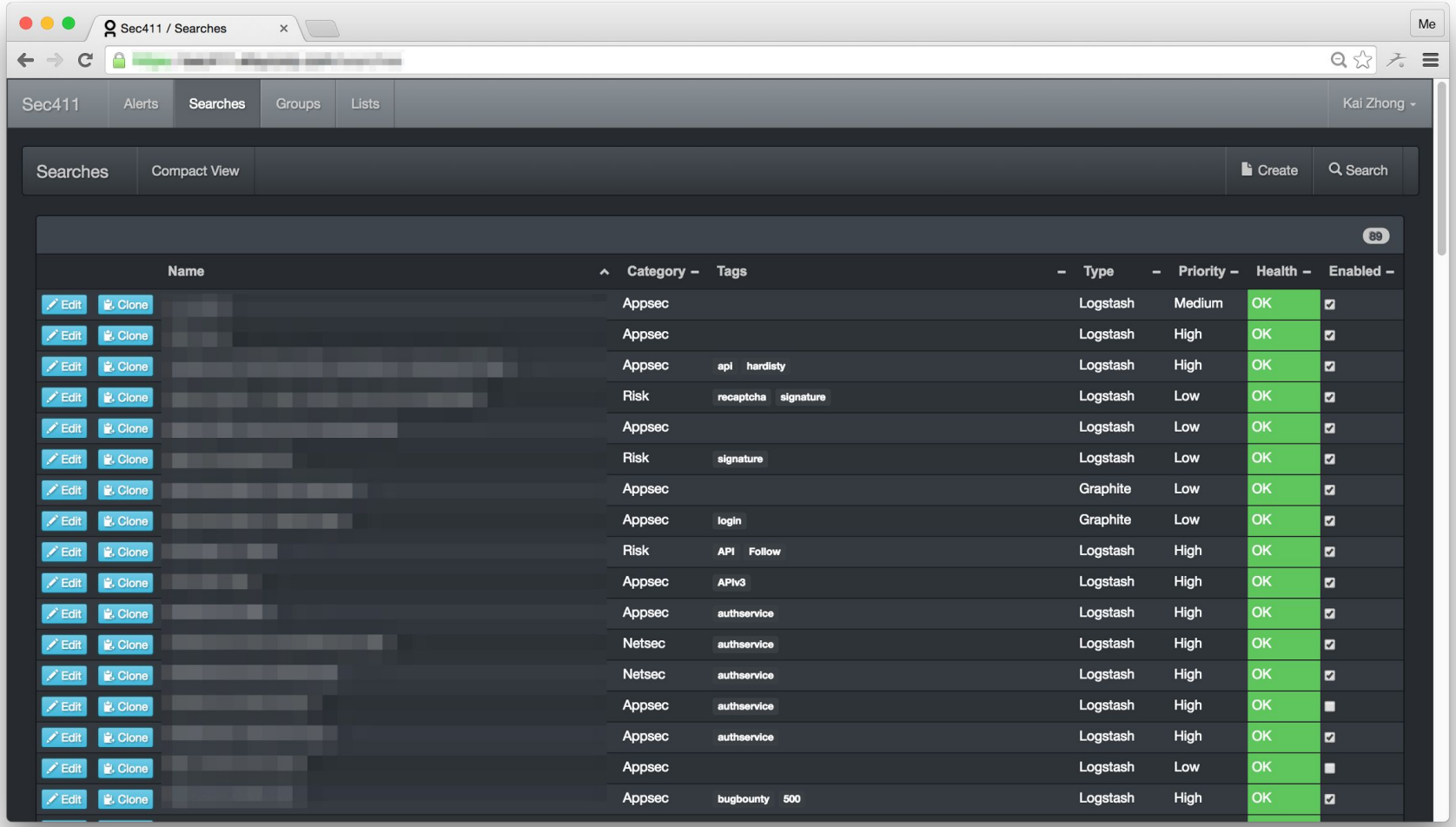
**0** of them are low priority

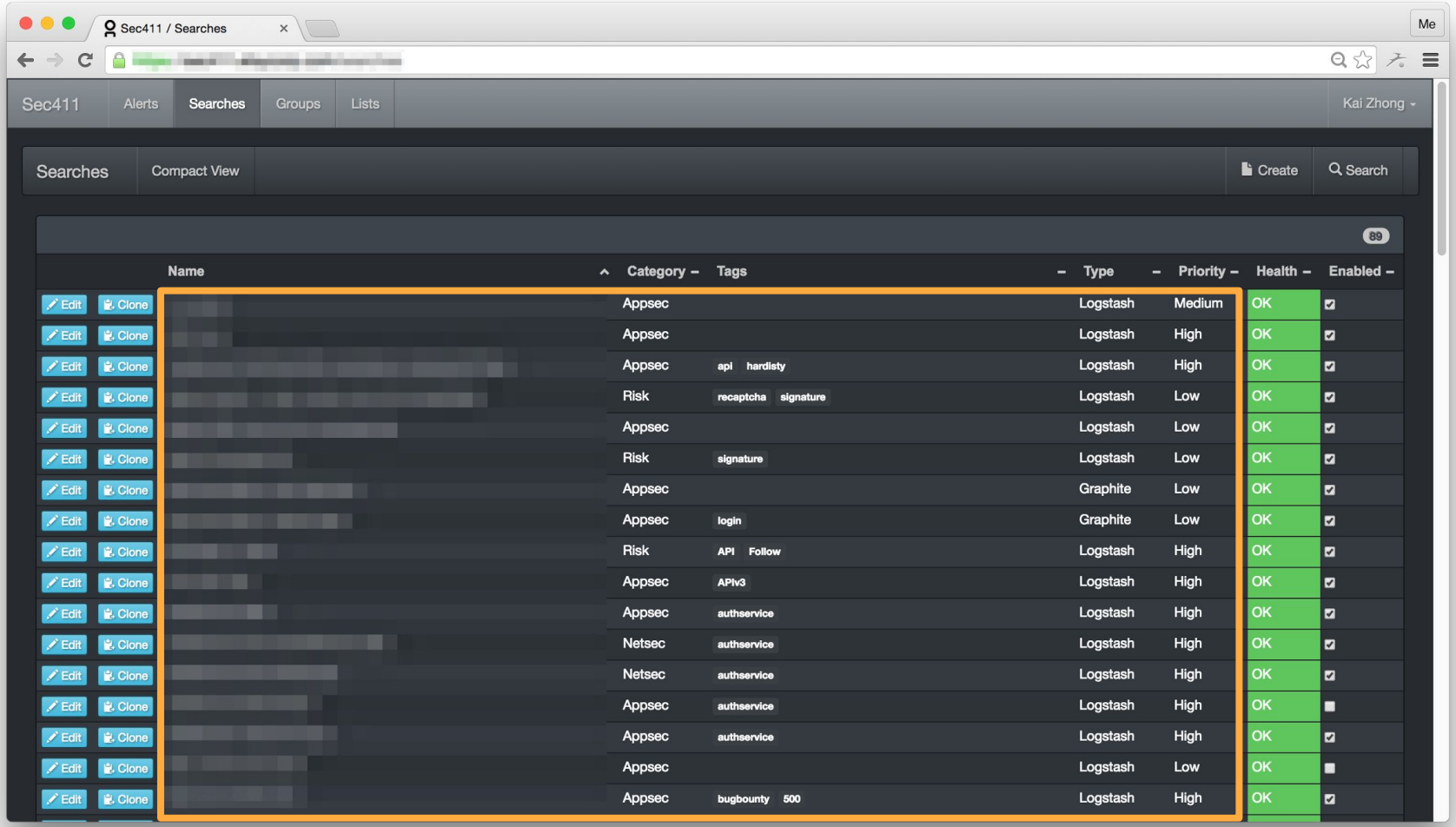
**0** of them are stale

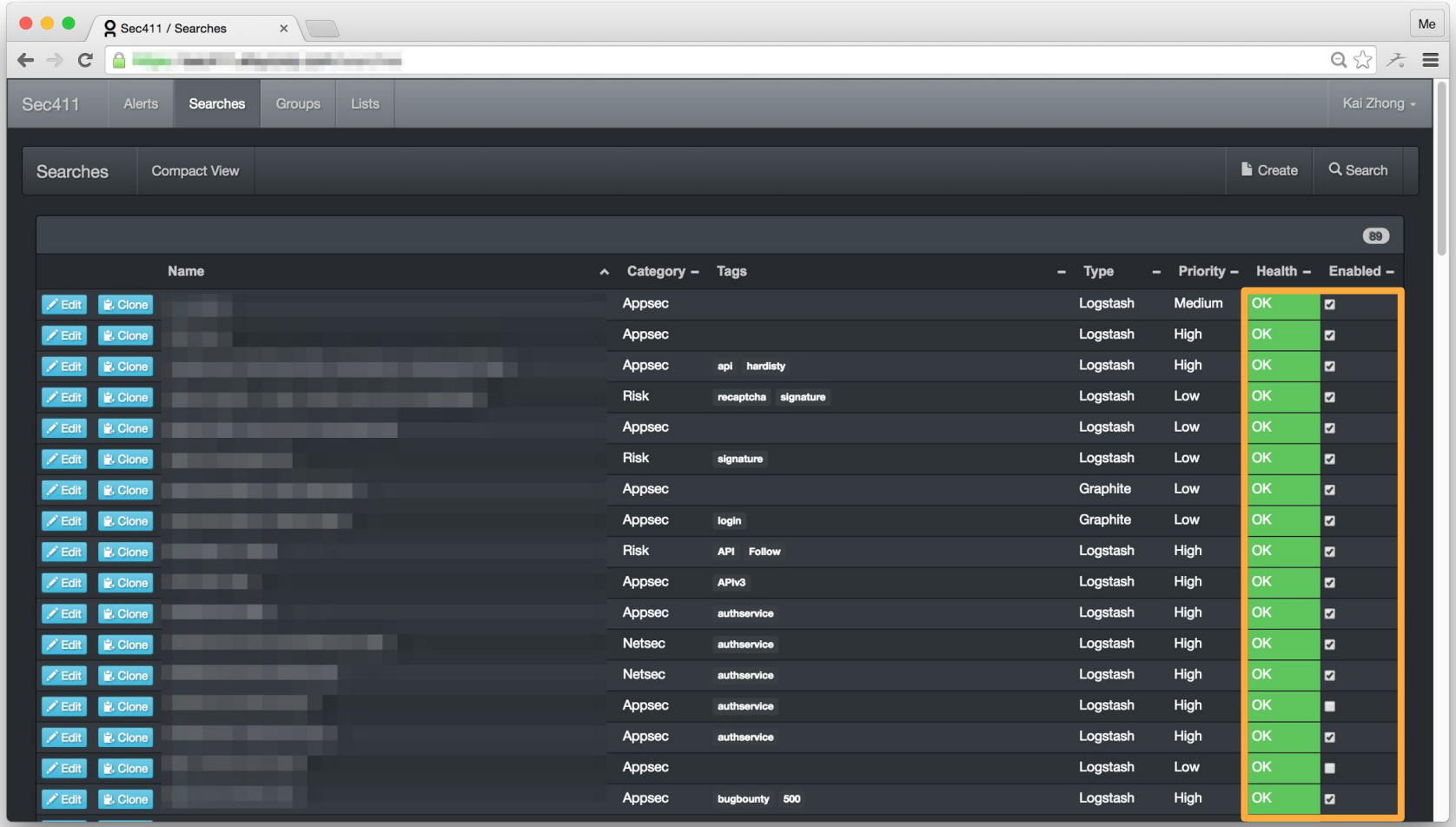
## Alerts in the last 20 days



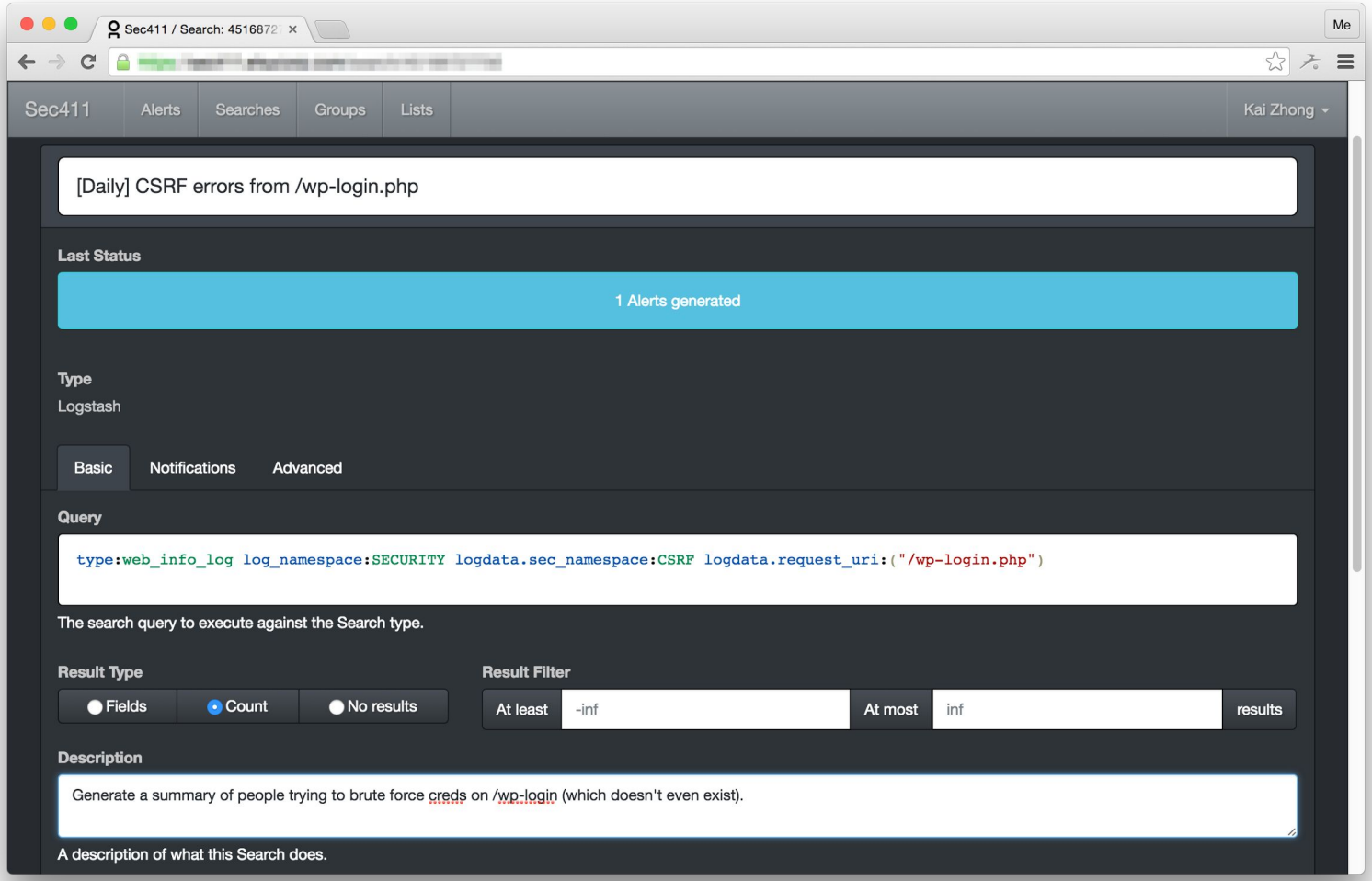
# Managing queries

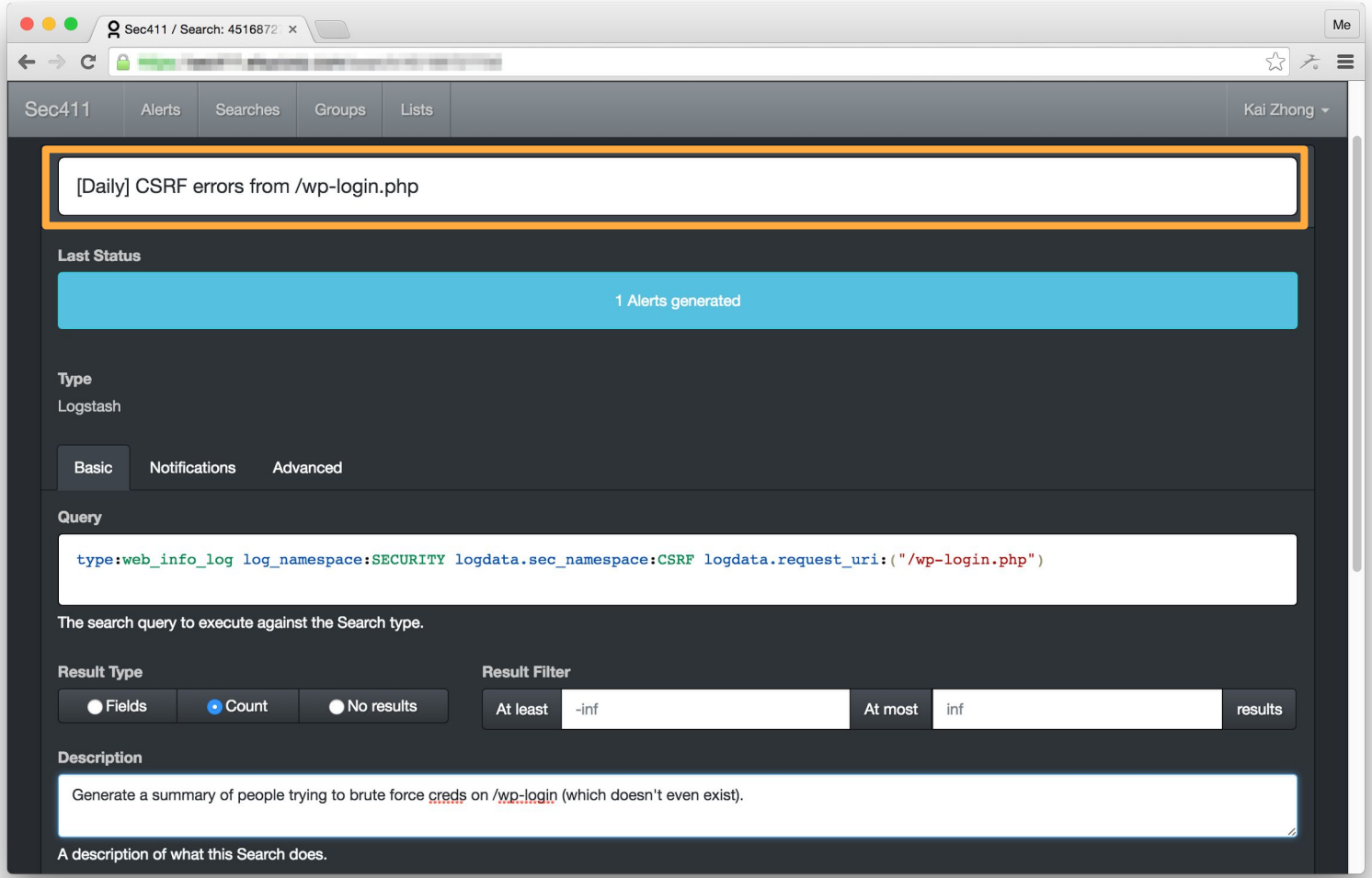

Sec411 / Searches
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Searches
Compact View
Create
Search
89
Name
Category
Tags
Type
Priority
Health
Enabled
Edit
Clone
Appsec
Logstash
Medium
OK
Edit
Clone
Appsec
Logstash
High
OK
Edit
Clone
Appsec
api
hardisty
Logstash
High
OK
Edit
Clone
Risk
recaptcha
signature
Logstash
Low
OK
Edit
Clone
Appsec
Logstash
Low
OK
Edit
Clone
Risk
signature
Logstash
Low
OK
Edit
Clone
Appsec
Graphite
Low
OK
Edit
Clone
Appsec
login
Graphite
Low
OK
Edit
Clone
Risk
API
Follow
Logstash
High
OK
Edit
Clone
Appsec
APIv3
Logstash
High
OK
Edit
Clone
Appsec
authservice
Logstash
High
OK
Edit
Clone
Netsec
authservice
Logstash
High
OK
Edit
Clone
Netsec
authservice
Logstash
High
OK
Edit
Clone
Appsec
authservice
Logstash
High
OK
Edit
Clone
Appsec
authservice
Logstash
High
OK
Edit
Clone
Appsec
Logstash
Low
OK
Edit
Clone
Appsec
bugbounty
500
Logstash
High
OK

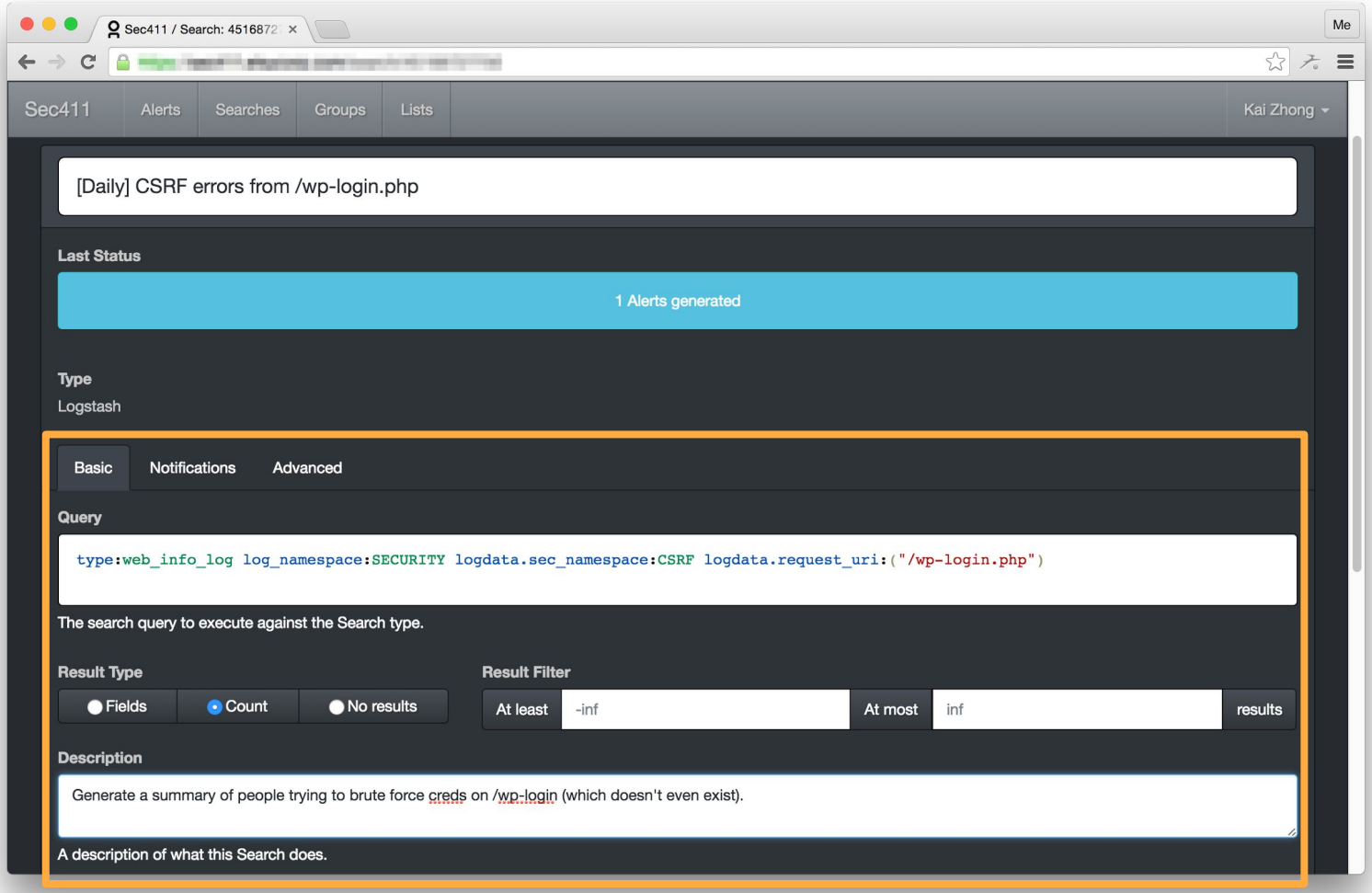

Sec411 / Searches
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Searches
Compact View
Create
Search
89
Name
Category
Tags
Type
Priority
Health
Enabled
Edit
Clone
Appsec
Logstash
Medium
OK
Appsec
Logstash
High
OK
Appsec
api
hardisty
Logstash
High
OK
Risk
recaptcha
signature
Logstash
Low
OK
Appsec
Logstash
Low
OK
Risk
signature
Logstash
Low
OK
Appsec
Graphite
Low
OK
Appsec
login
Graphite
Low
OK
Risk
API
Follow
Logstash
High
OK
Appsec
APIv3
Logstash
High
OK
Appsec
authservice
Logstash
High
OK
Netsec
authservice
Logstash
High
OK
Netsec
authservice
Logstash
High
OK
Appsec
authservice
Logstash
High
OK
Appsec
authservice
Logstash
High
OK
Appsec
Logstash
Low
OK
Appsec
bugbounty
500
Logstash
High
OK

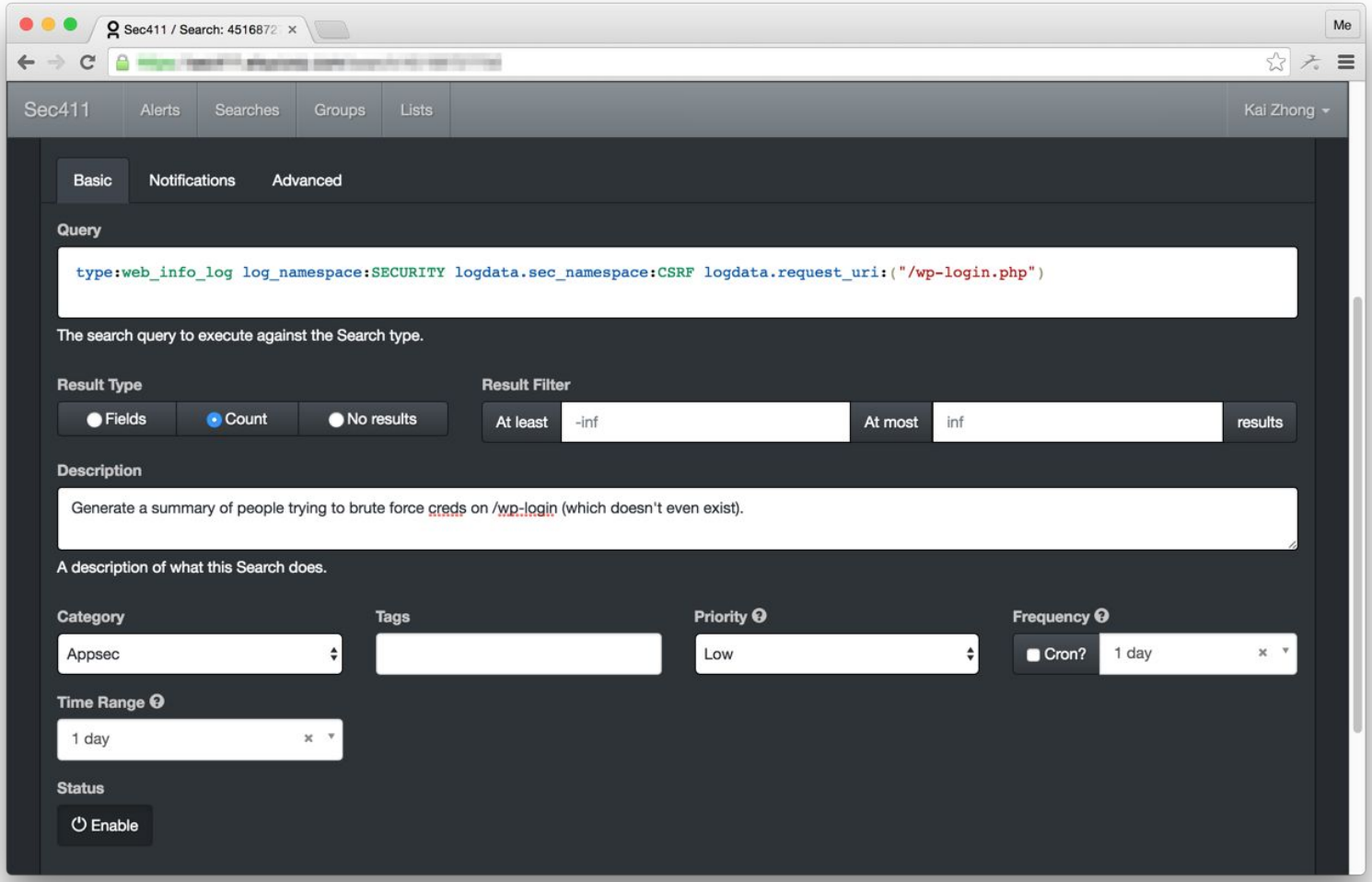

Sec411 / Searches
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Searches
Compact View
Create
Search
89
Name
Category
Tags
Type
Priority
Health
Enabled
Edit
Clone
Appsec
Logstash
Medium
OK
Edit
Clone
Appsec
Logstash
High
OK
Edit
Clone
Appsec
api
hardisty
Logstash
High
OK
Edit
Clone
Risk
recaptcha
signature
Logstash
Low
OK
Edit
Clone
Appsec
Logstash
Low
OK
Edit
Clone
Risk
signature
Logstash
Low
OK
Edit
Clone
Appsec
Graphite
Low
OK
Edit
Clone
Appsec
login
Graphite
Low
OK
Edit
Clone
Risk
API
Follow
Logstash
High
OK
Edit
Clone
Appsec
APIv3
Logstash
High
OK
Edit
Clone
Appsec
authservice
Logstash
High
OK
Edit
Clone
Netsec
authservice
Logstash
High
OK
Edit
Clone
Netsec
authservice
Logstash
High
OK
Edit
Clone
Appsec
authservice
Logstash
High
OK
Edit
Clone
Appsec
authservice
Logstash
High
OK
Edit
Clone
Appsec
Logstash
Low
OK
Edit
Clone
Appsec
bugbounty
500
Logstash
High
OK

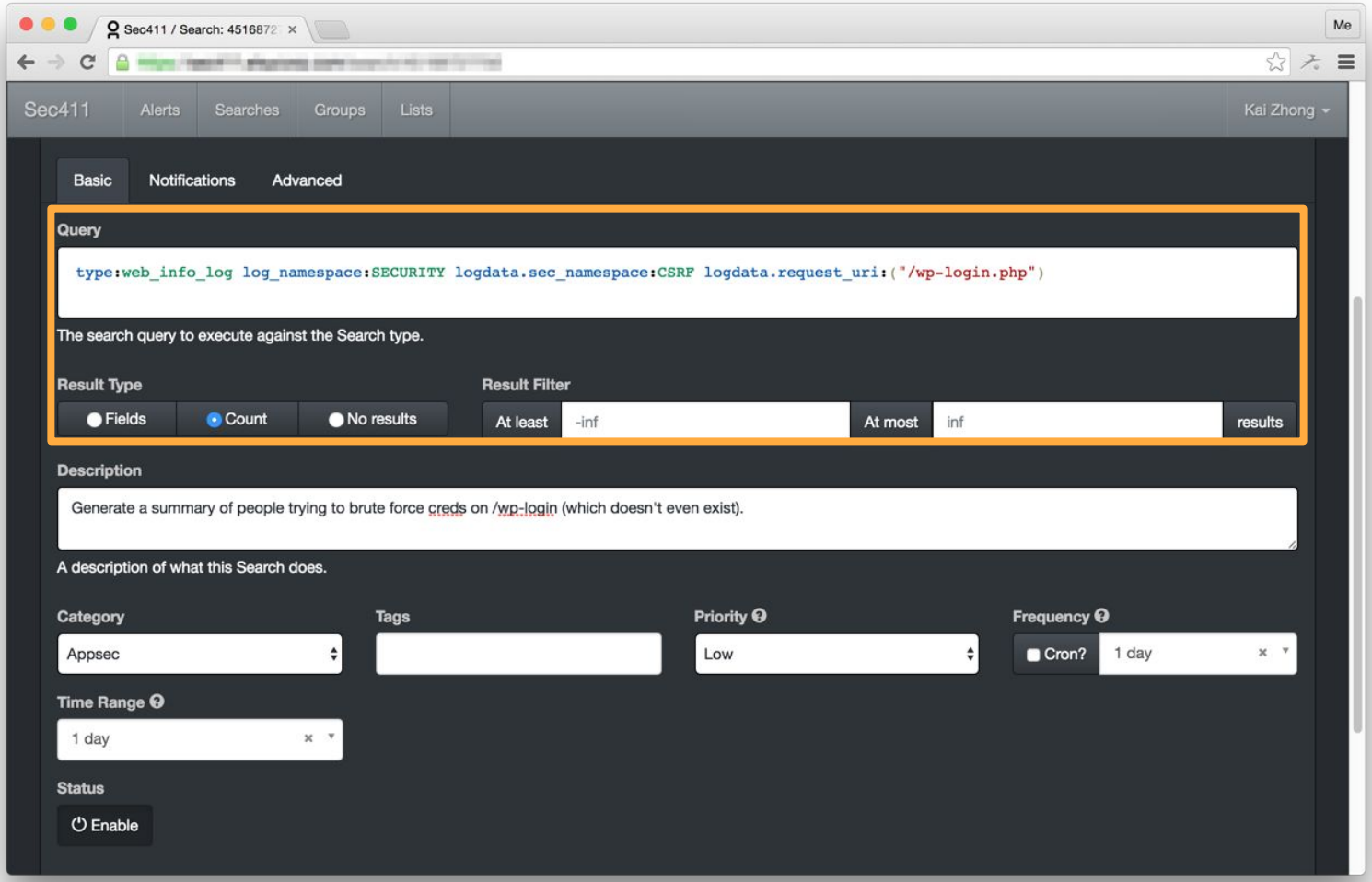
# Configuring a query

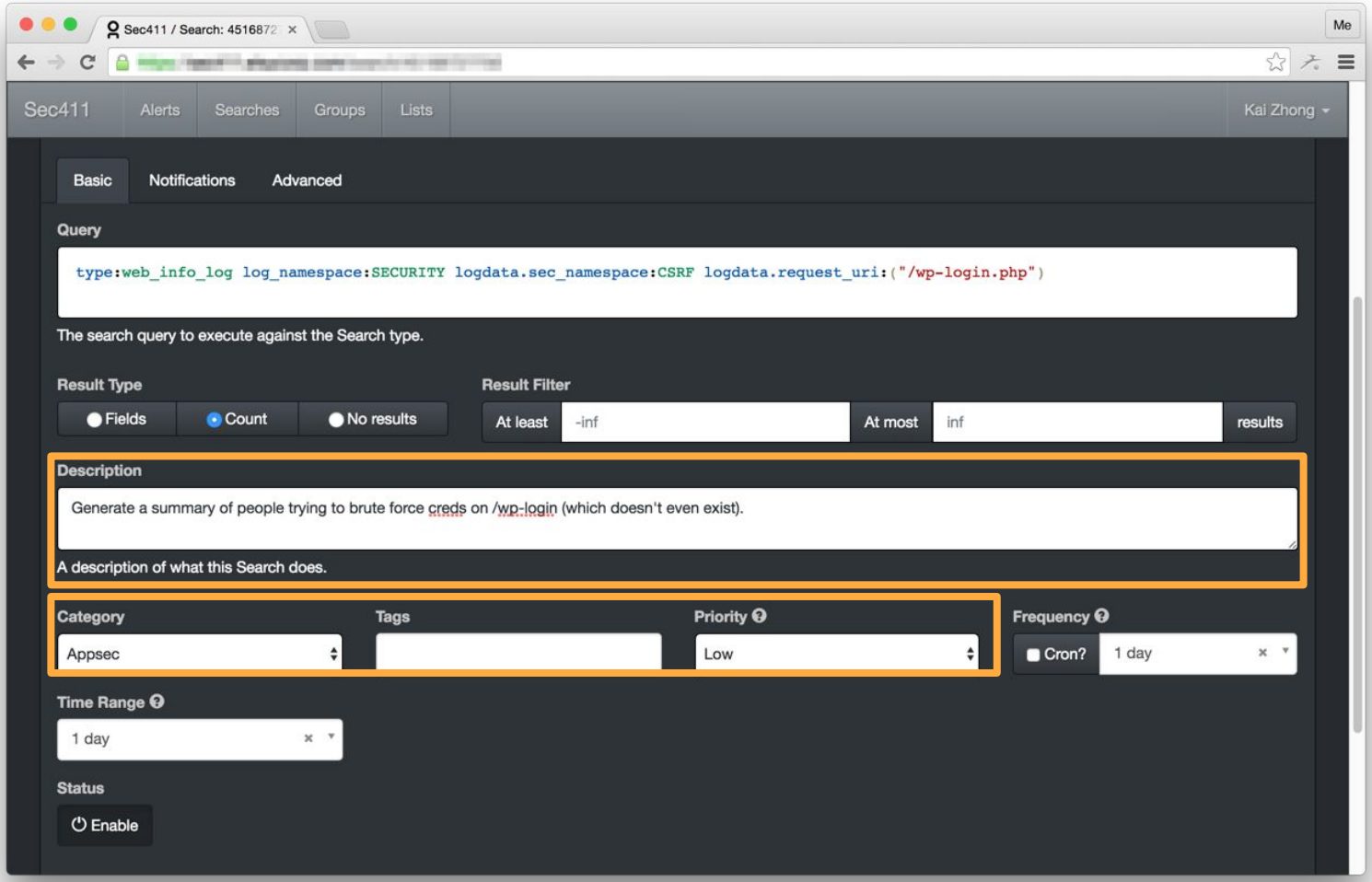

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
[Daily] CSRF errors from /wp-login.php
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.

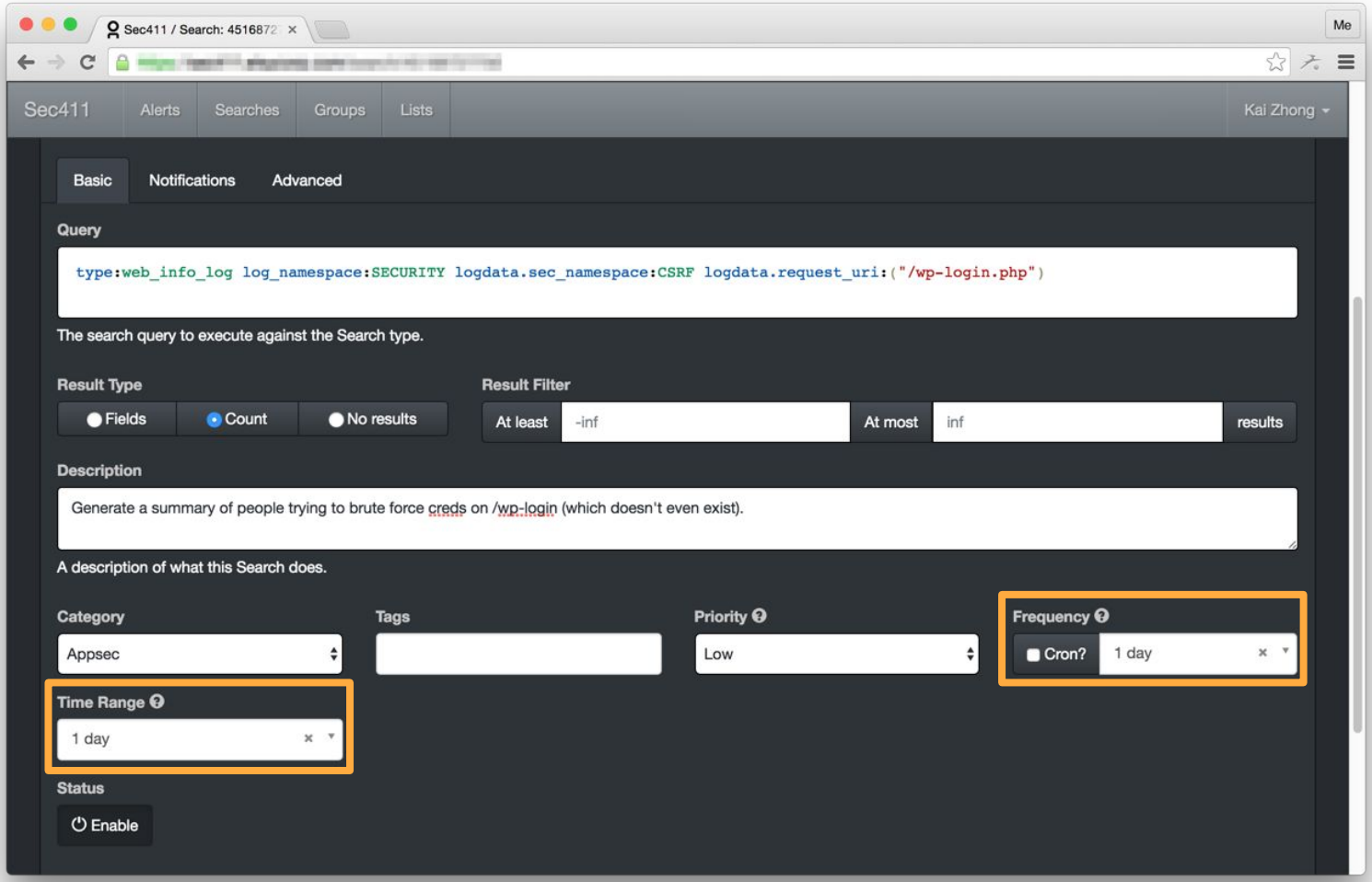

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
[Daily] CSRF errors from /wp-login.php
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.

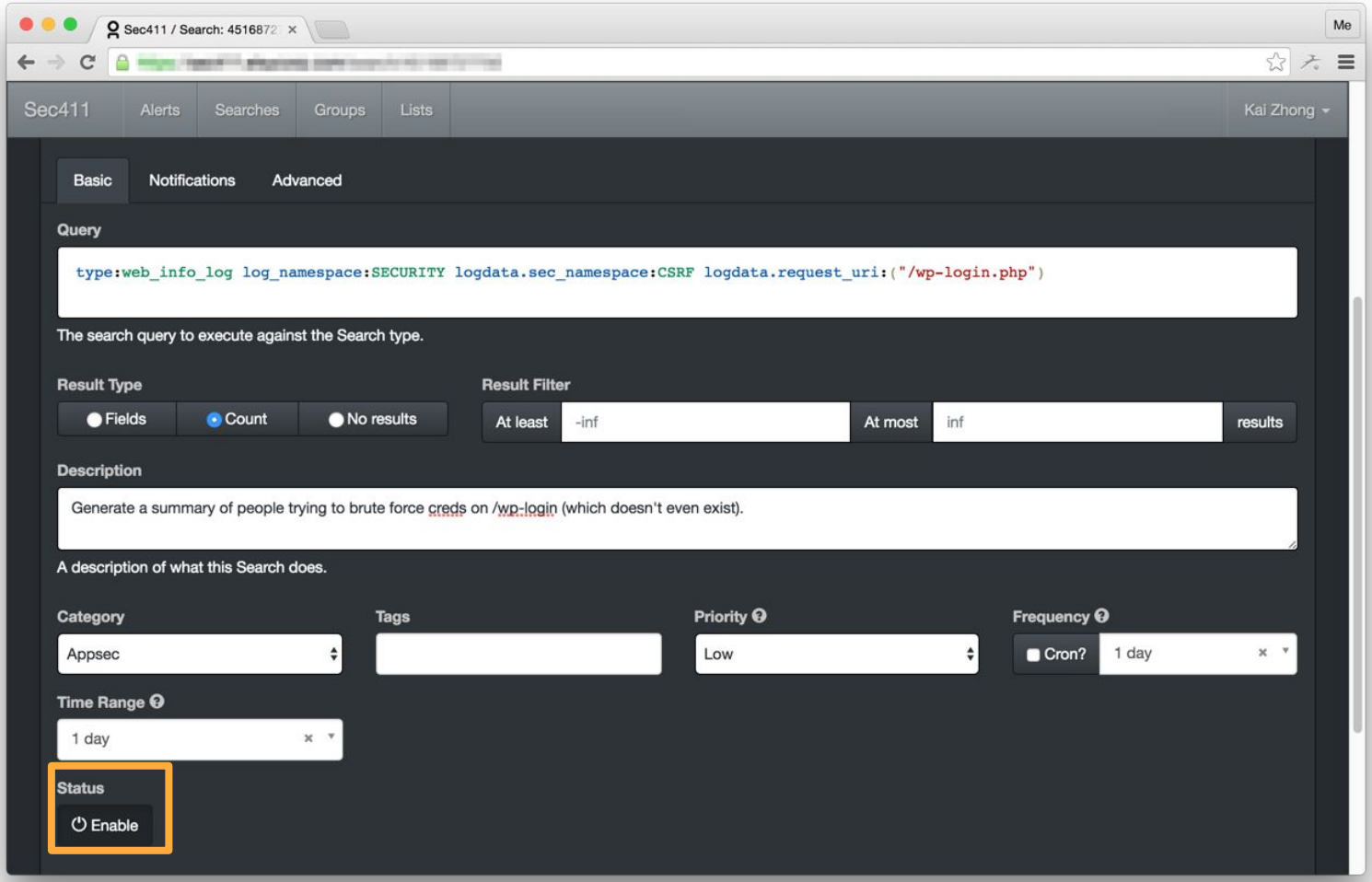

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
[Daily] CSRF errors from /wp-login.php
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.

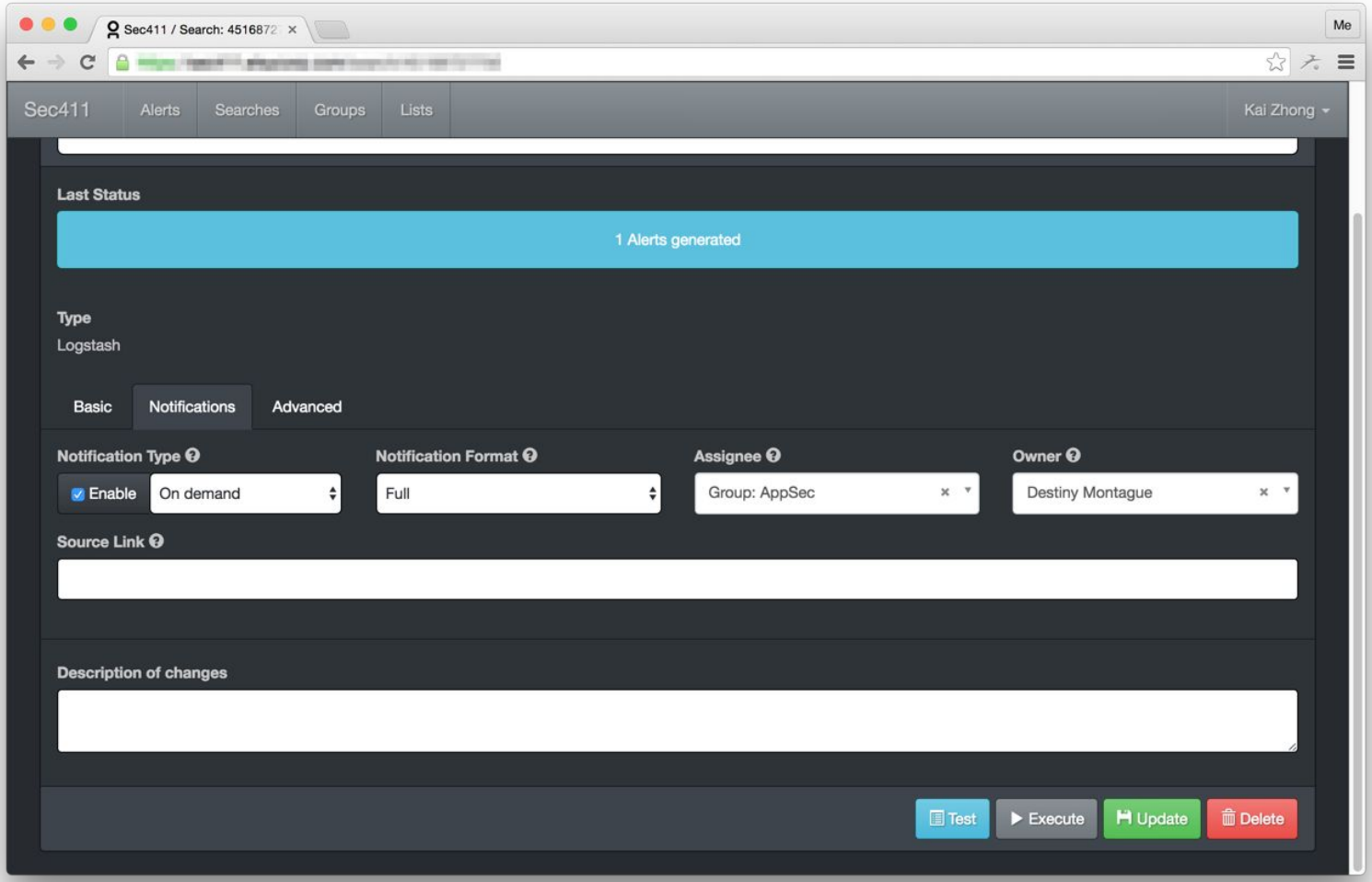

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.
Category
Appsec
Tags
Priority
Low
Frequency
Cron?
1 day
Time Range
1 day
Status
Enable

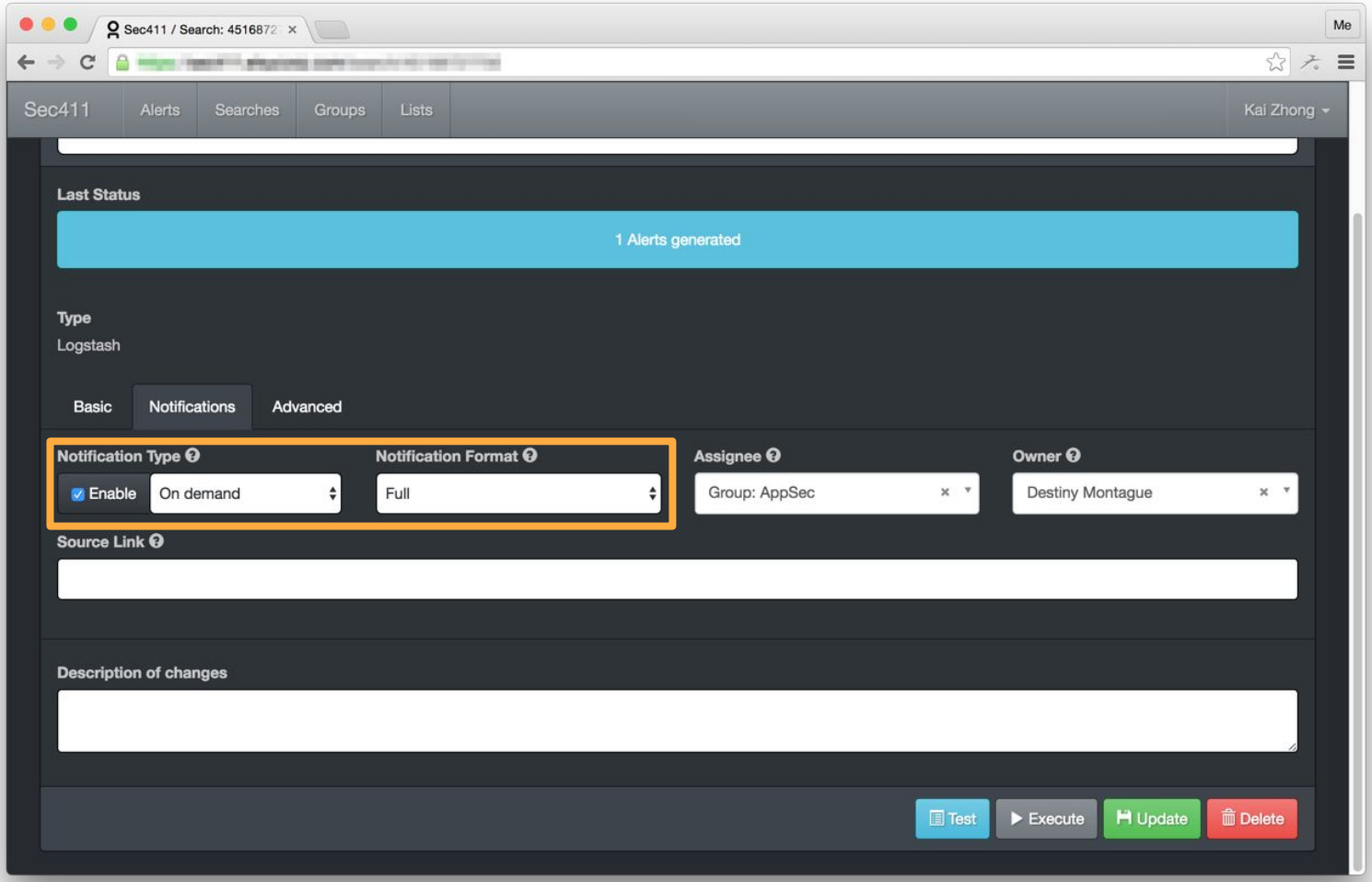

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.
Category
Appsec
Tags
Priority
Low
Frequency
Cron?
1 day
Time Range
1 day
Status
Enable

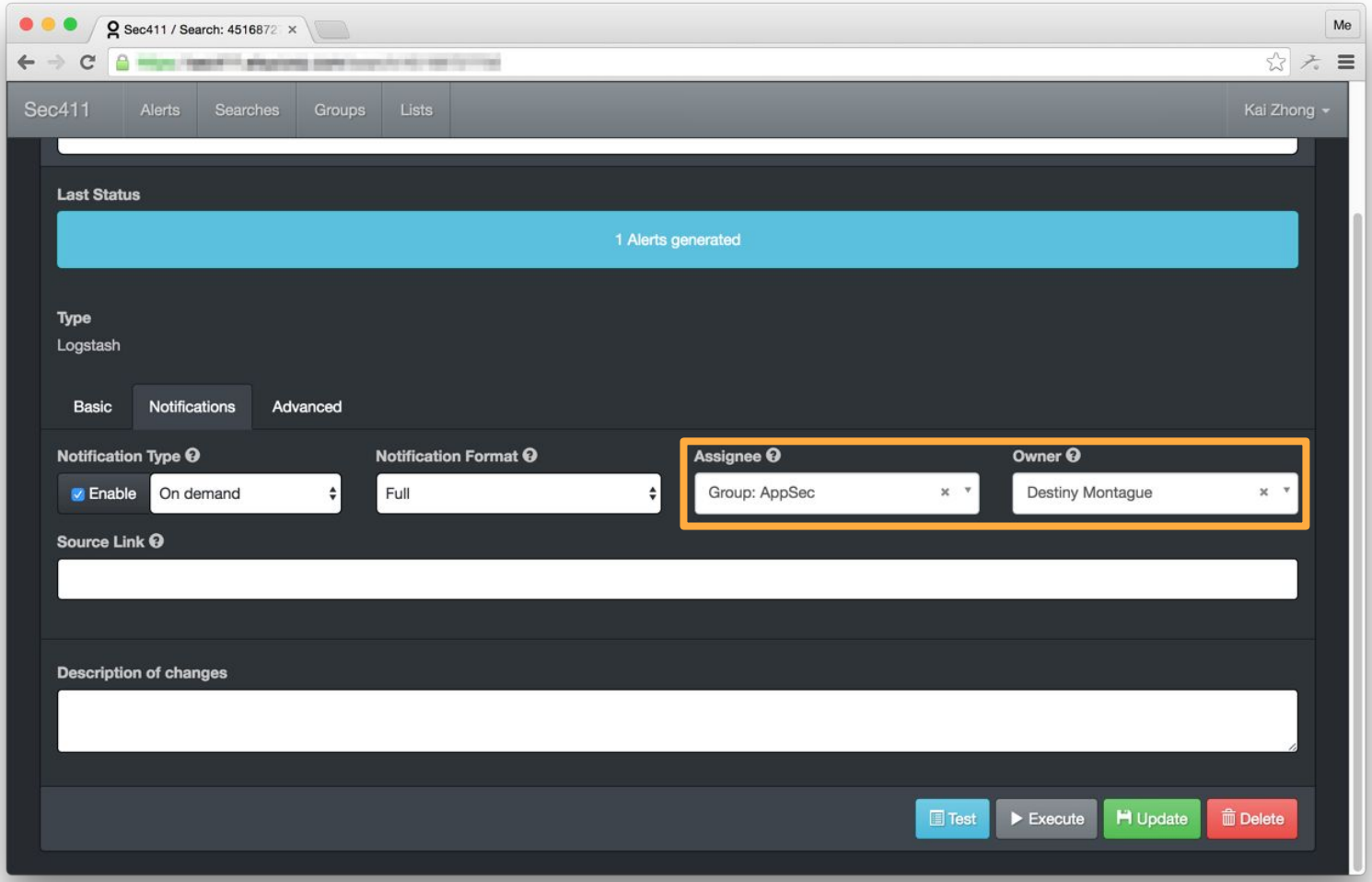

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.
Category
Appsec
Tags
Priority
Low
Frequency
Cron?
1 day
Time Range
1 day
Status
Enable

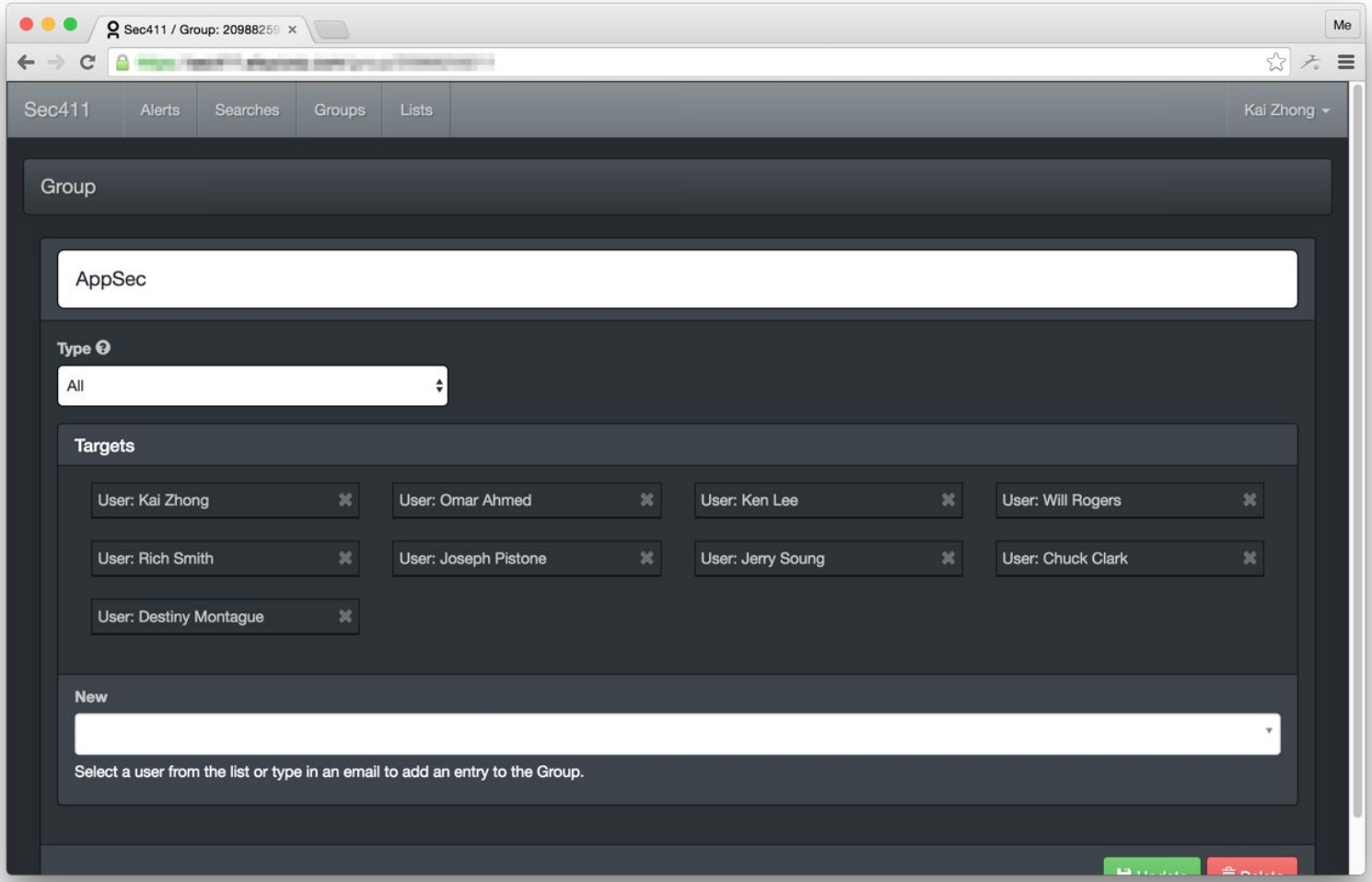

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.
Category
Appsec
Tags
Priority
Low
Frequency
Cron?
1 day
Time Range
1 day
Status
Enable

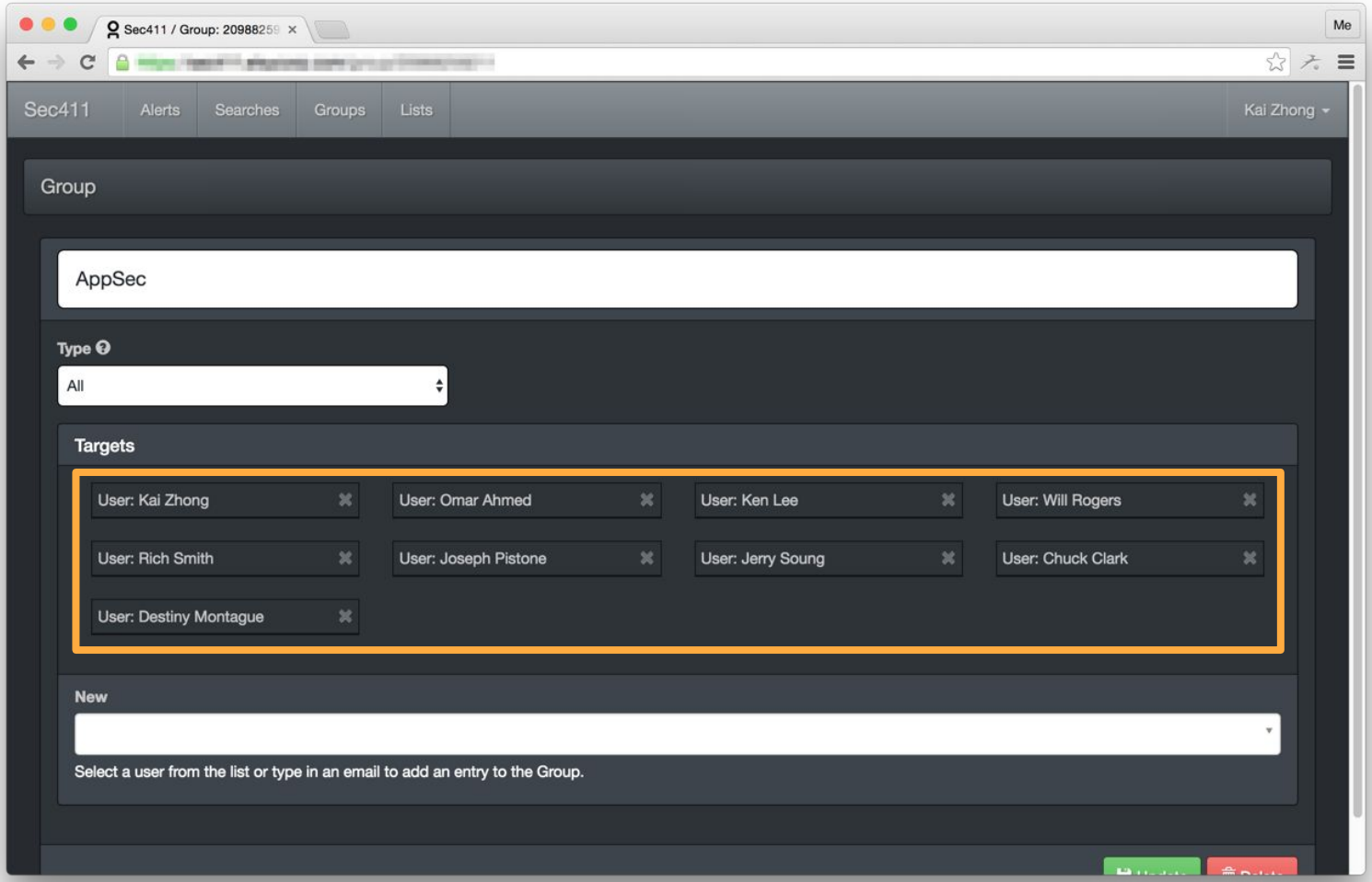

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Basic
Notifications
Advanced
Query
type:web_info_log log_namespace:SECURITY logdata.sec_namespace:CSRF logdata.request_uri:("/wp-login.php")
The search query to execute against the Search type.
Result Type
Fields
Count
No results
Result Filter
At least
-inf
At most
inf
results
Description
Generate a summary of people trying to brute force creds on /wp-login (which doesn't even exist).
A description of what this Search does.
Category
Appsec
Tags
Priority
Low
Frequency
Cron?
1 day
Time Range
1 day
Status
Enable

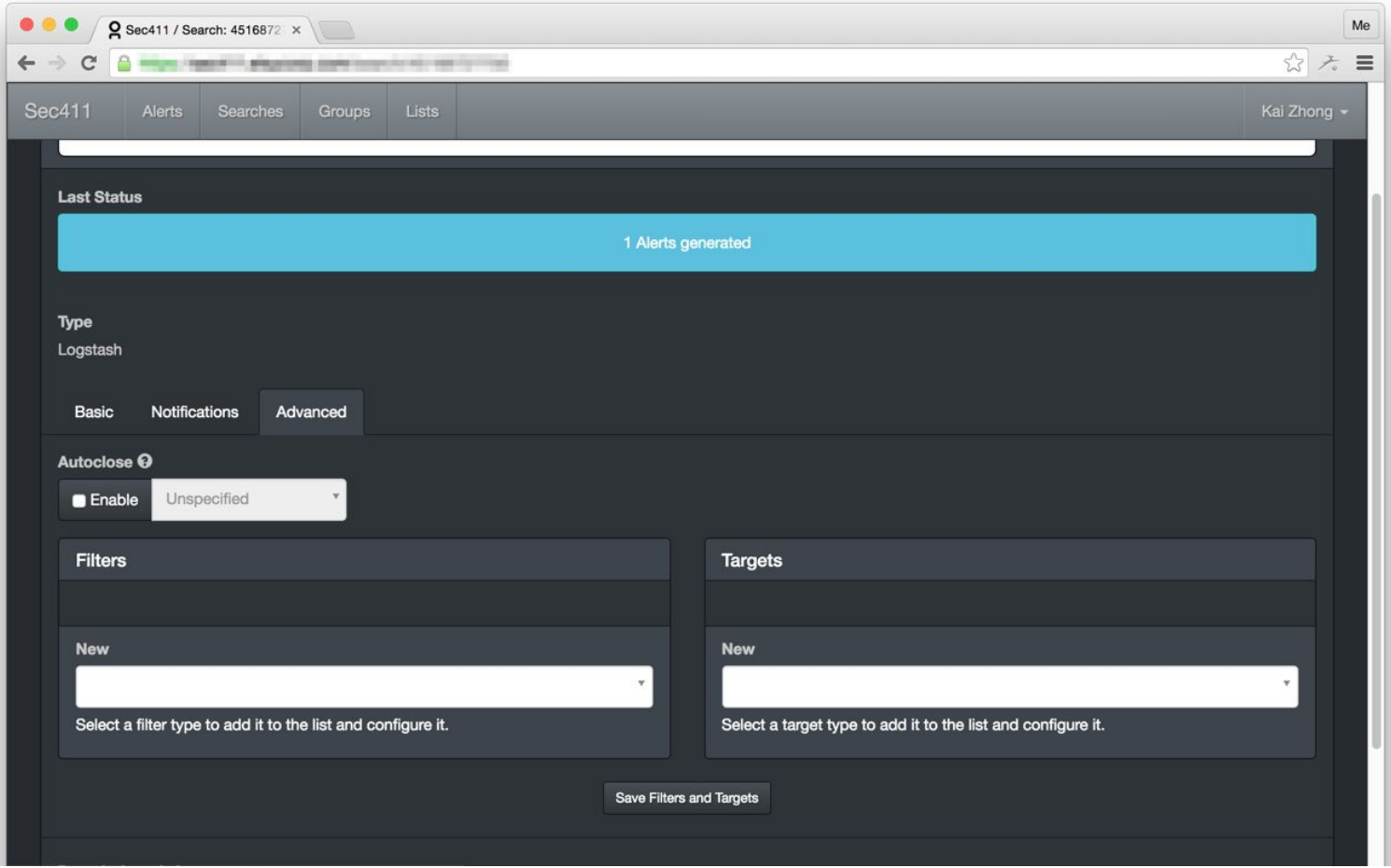

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Notification Type
Enable
On demand
Notification Format
Full
Assignee
Group: AppSec
Owner
Destiny Montague
Source Link
Description of changes
Test
Execute
Update
Delete

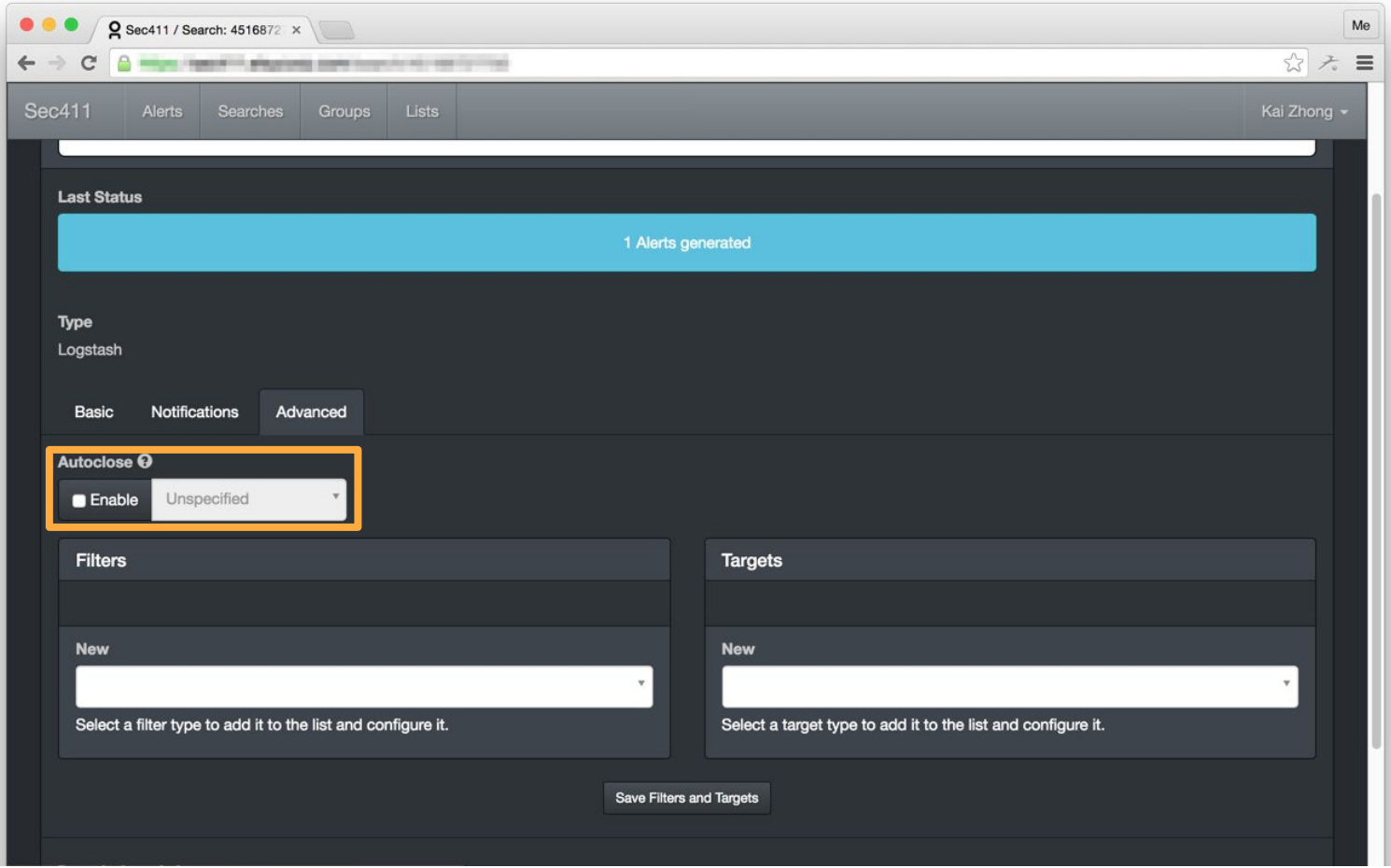

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Notification Type
Enable
On demand
Notification Format
Full
Assignee
Group: AppSec
Owner
Destiny Montague
Source Link
Description of changes
Test
Execute
Update
Delete

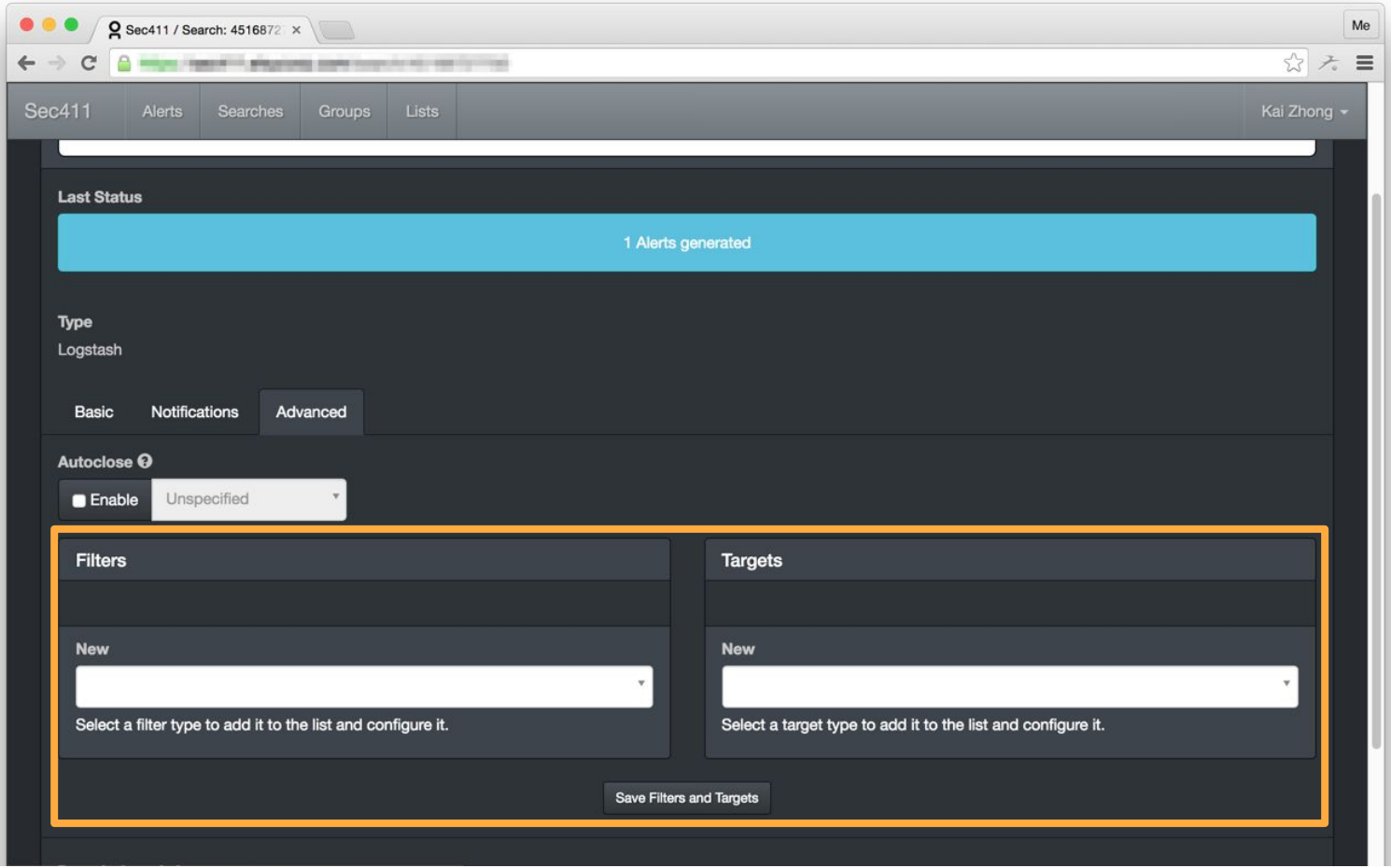

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Notification Type
Enable
On demand
Notification Format
Full
Assignee
Group: AppSec
Owner
Destiny Montague
Source Link
Description of changes
Test
Execute
Update
Delete

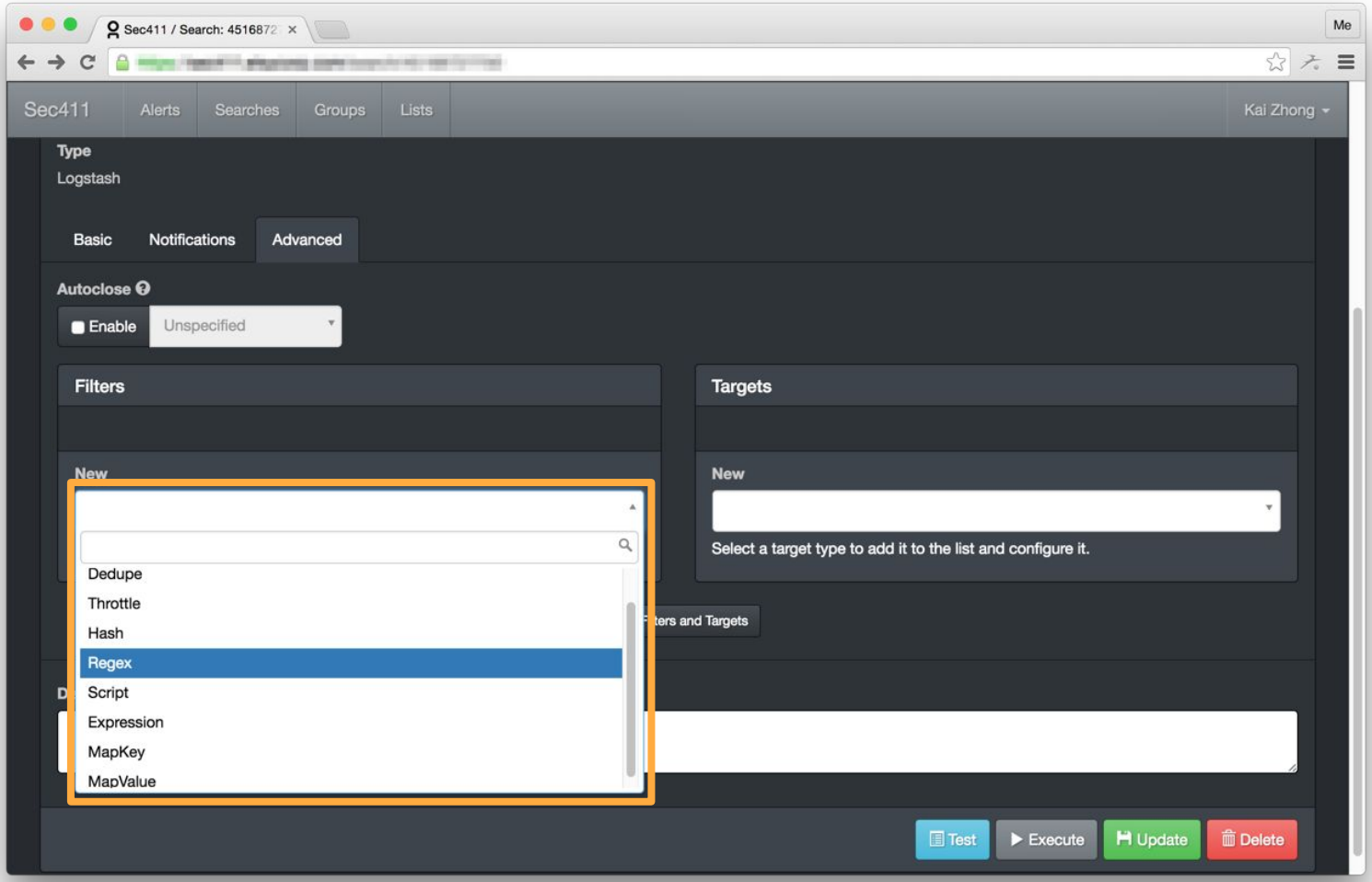

Sec411 / Group: 20988259
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Group
AppSec
Type
All
Targets
User: Kai Zhong
User: Omar Ahmed
User: Ken Lee
User: Will Rogers
User: Rich Smith
User: Joseph Pistone
User: Jerry Soung
User: Chuck Clark
User: Destiny Montague
New
Select a user from the list or type in an email to add an entry to the Group.

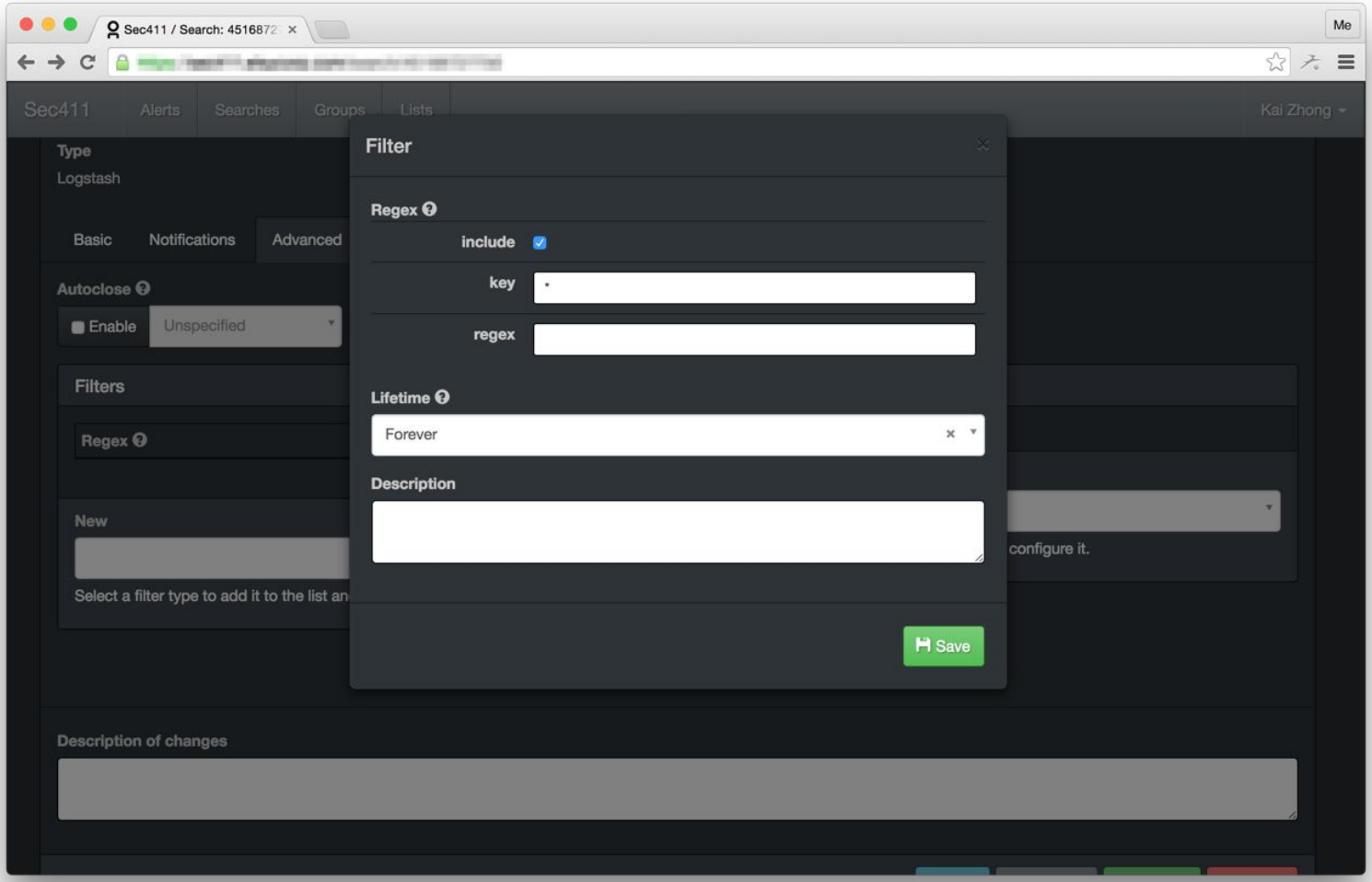

Sec411 / Group: 20988259
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Group
AppSec
Type
All
Targets
User: Kai Zhong
User: Omar Ahmed
User: Ken Lee
User: Will Rogers
User: Rich Smith
User: Joseph Pistone
User: Jerry Soung
User: Chuck Clark
User: Destiny Montague
New
Select a user from the list or type in an email to add an entry to the Group.

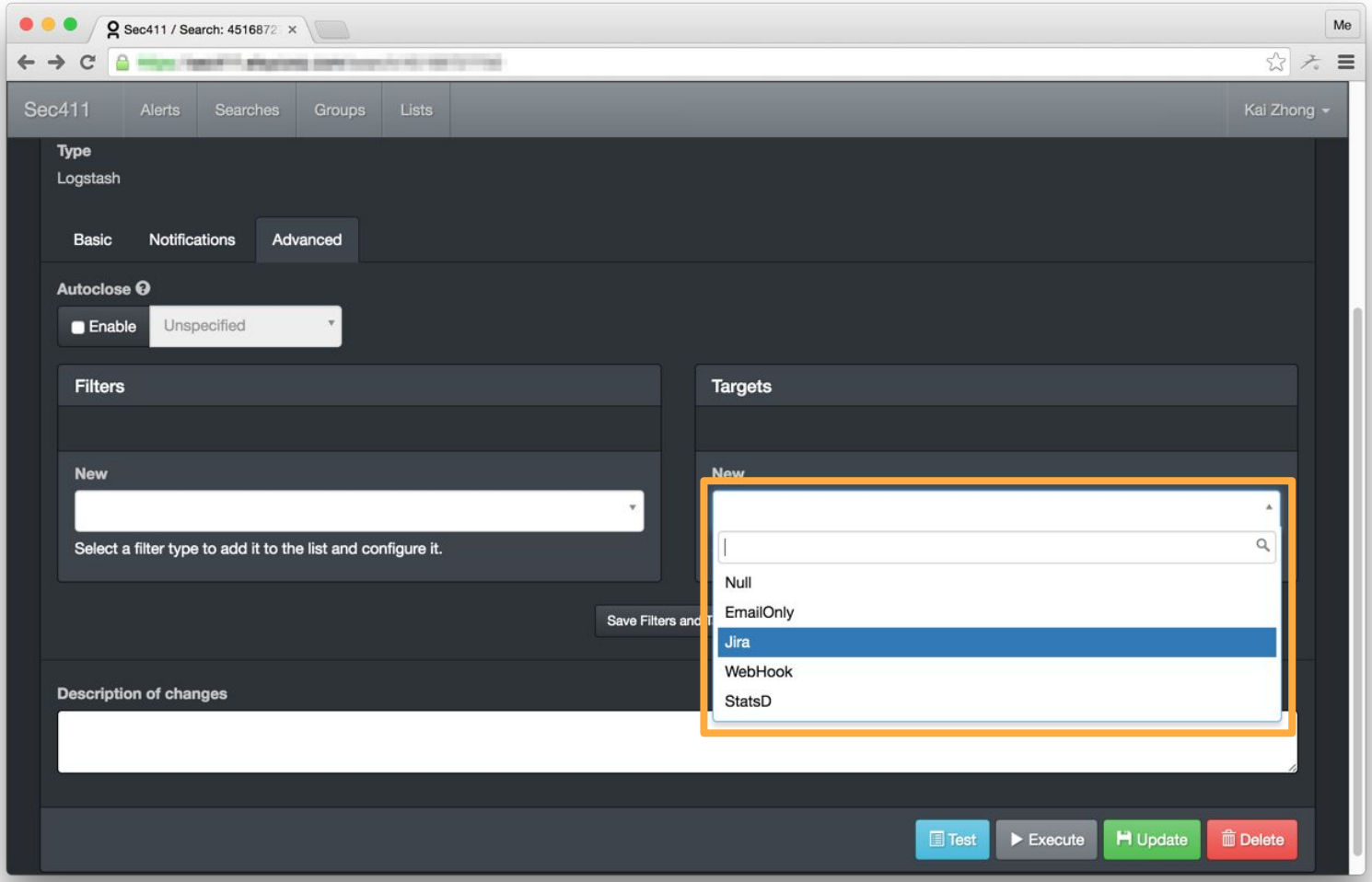

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
New
Select a filter type to add it to the list and configure it.
Targets
New
Select a target type to add it to the list and configure it.
Save Filters and Targets

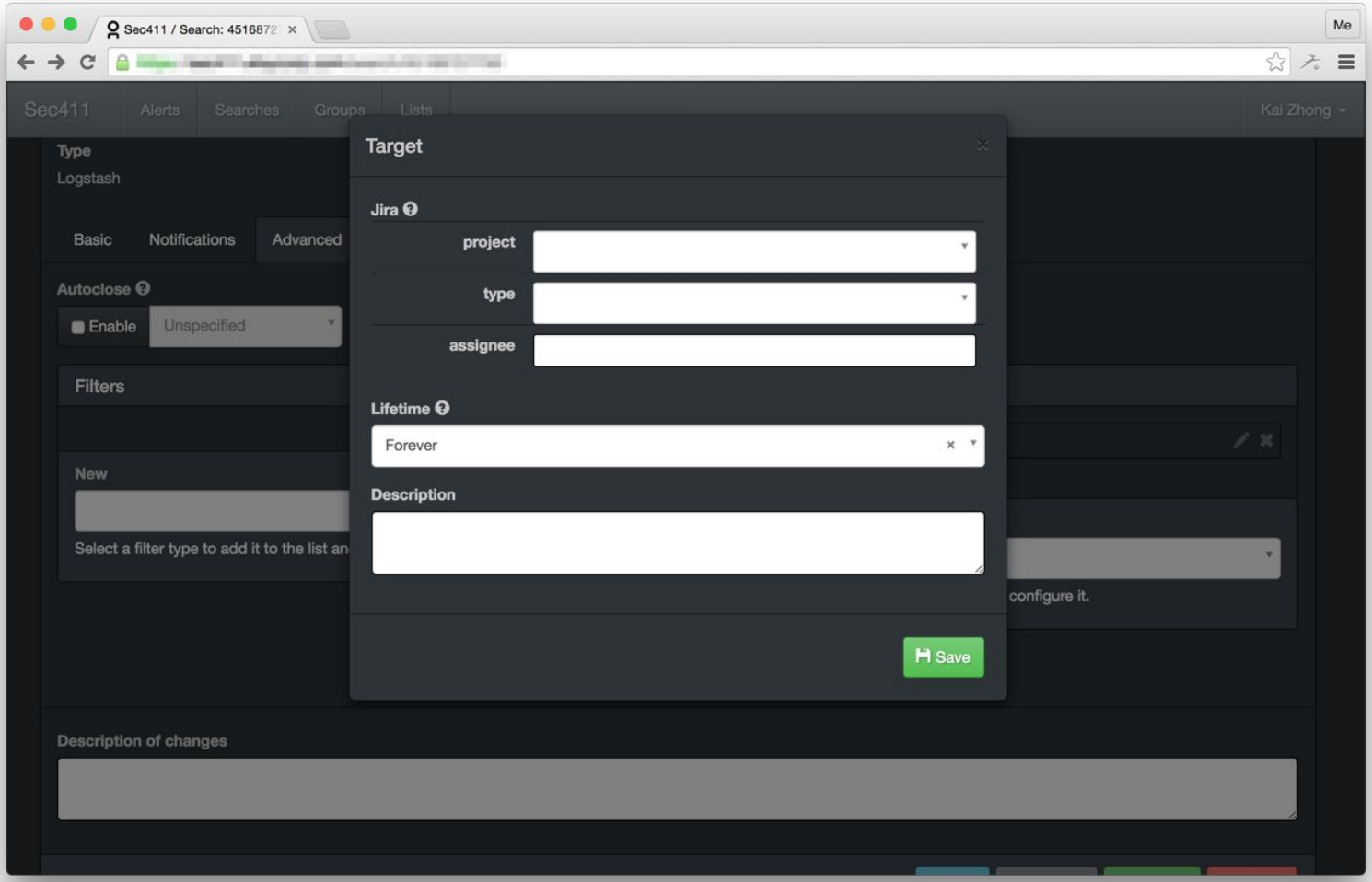

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
New
Select a filter type to add it to the list and configure it.
Targets
New
Select a target type to add it to the list and configure it.
Save Filters and Targets


Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Last Status
1 Alerts generated
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
New
Select a filter type to add it to the list and configure it.
Targets
New
Select a target type to add it to the list and configure it.
Save Filters and Targets

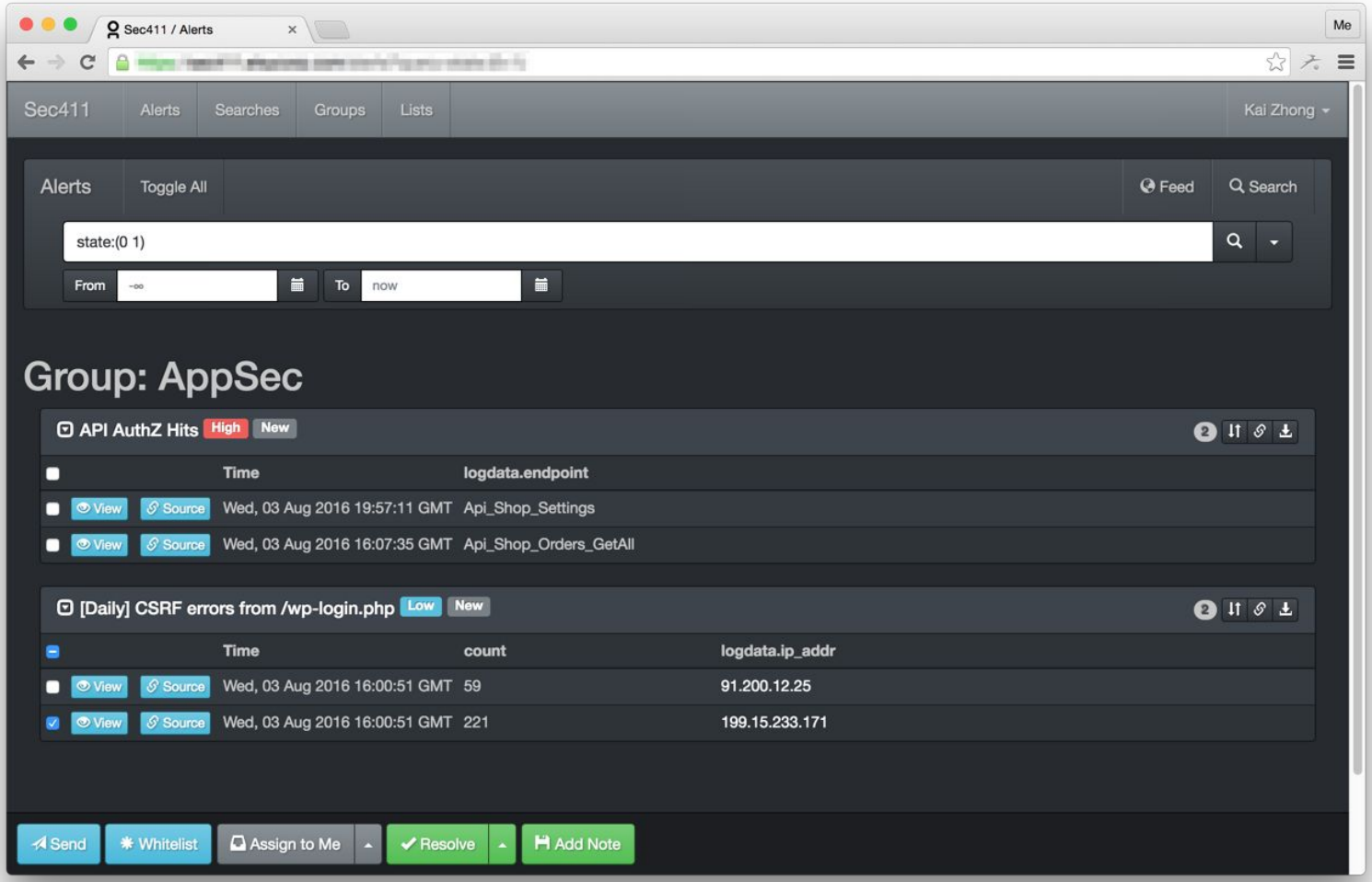

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
New
Dedupe
Throttle
Hash
Regex
Script
Expression
MapKey
MapValue
Targets
New
Select a target type to add it to the list and configure it.
ters and Targets
Test
Execute
Update
Delete

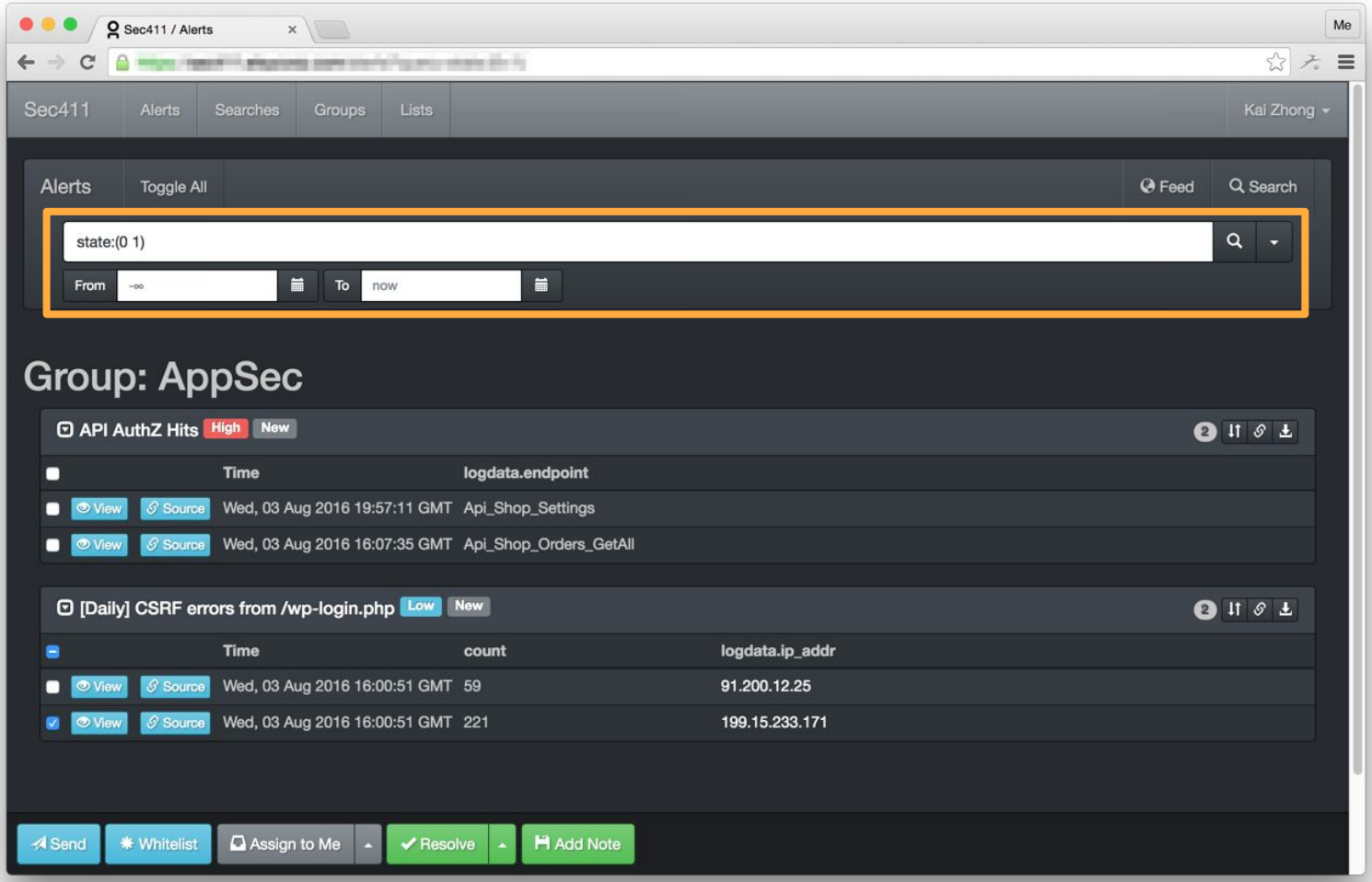

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
Regex
New
Select a filter type to add it to the list an
configure it.
Description of changes
Filter
Regex
include
key
regex
Lifetime
Forever
Description
Save

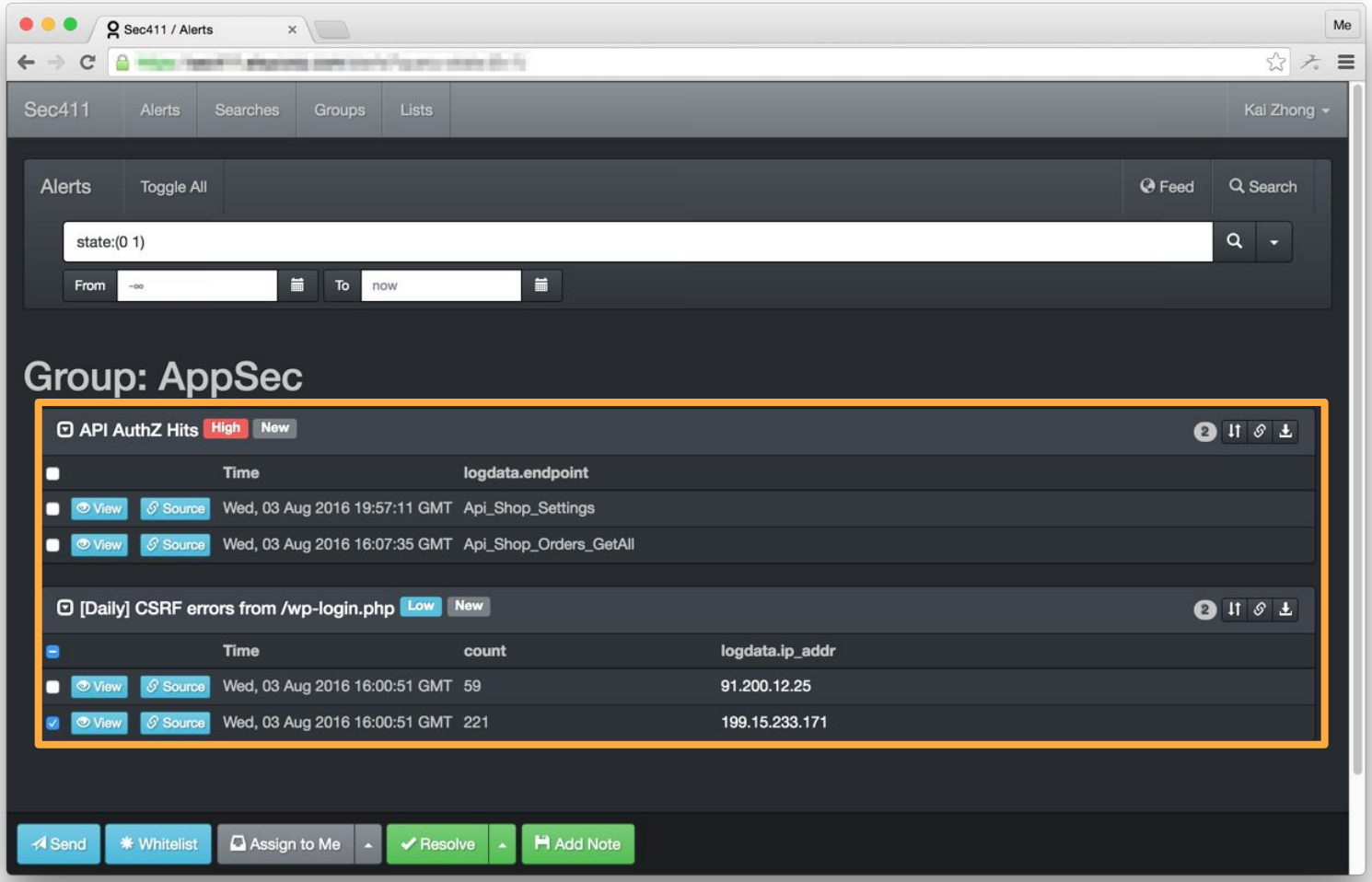

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
New
Select a filter type to add it to the list and configure it.
Targets
New
Null
EmailOnly
Jira
WebHook
StatsD
Save Filters and
Description of changes
Test
Execute
Update
Delete

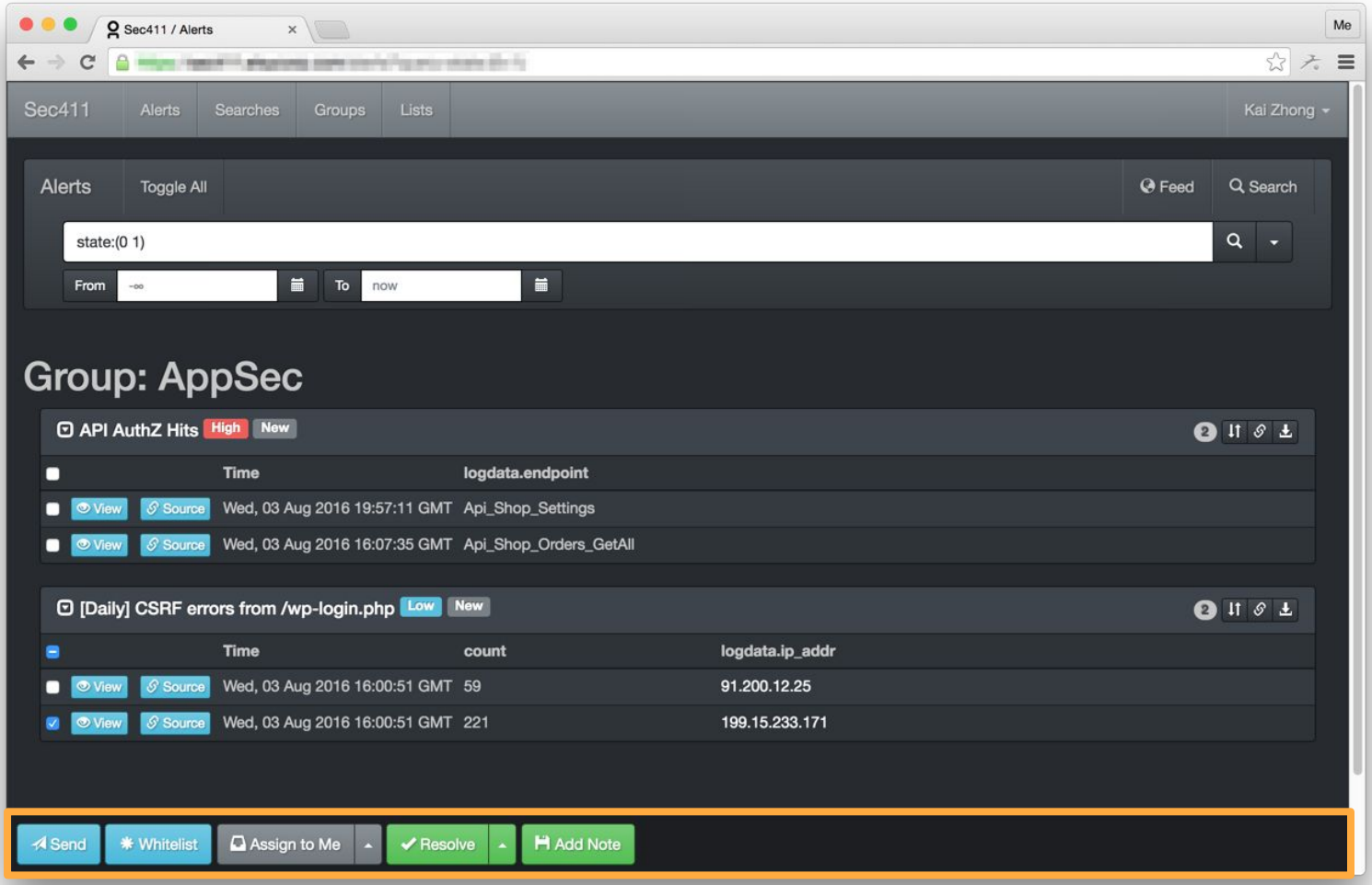

Sec411 / Search: 4516872
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Type
Logstash
Basic
Notifications
Advanced
Autoclose
Enable
Unspecified
Filters
New
Select a filter type to add it to the list an
configure it.
Description of changes
Target
Jira
project
type
assignee
Lifetime
Forever
Description
Save

# Managing alerts

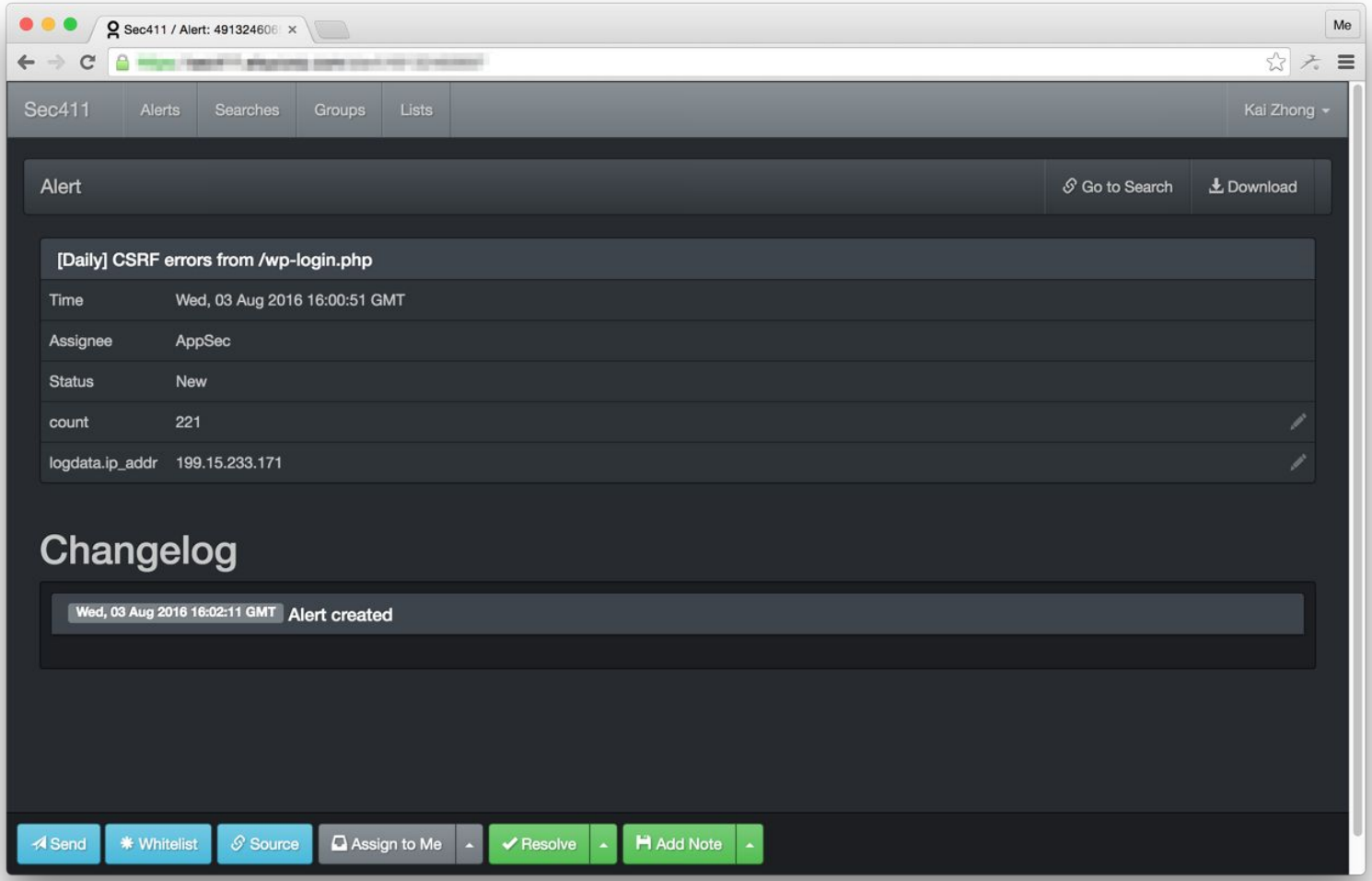

Sec411 / Alerts
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alerts
Toggle All
Feed
Search
state:(0 1)
From
-∞
To
now
Group: AppSec
API AuthZ Hits
High
New
2
Time
logdata.endpoint
View
Source
Wed, 03 Aug 2016 19:57:11 GMT
Api_Shop_Settings
View
Source
Wed, 03 Aug 2016 16:07:35 GMT
Api_Shop_Orders_GetAll
[Daily] CSRF errors from /wp-login.php
Low
New
2
Time
count
logdata.ip_addr
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
59
91.200.12.25
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
221
199.15.233.171
Send
Whitelist
Assign to Me
Resolve
Add Note

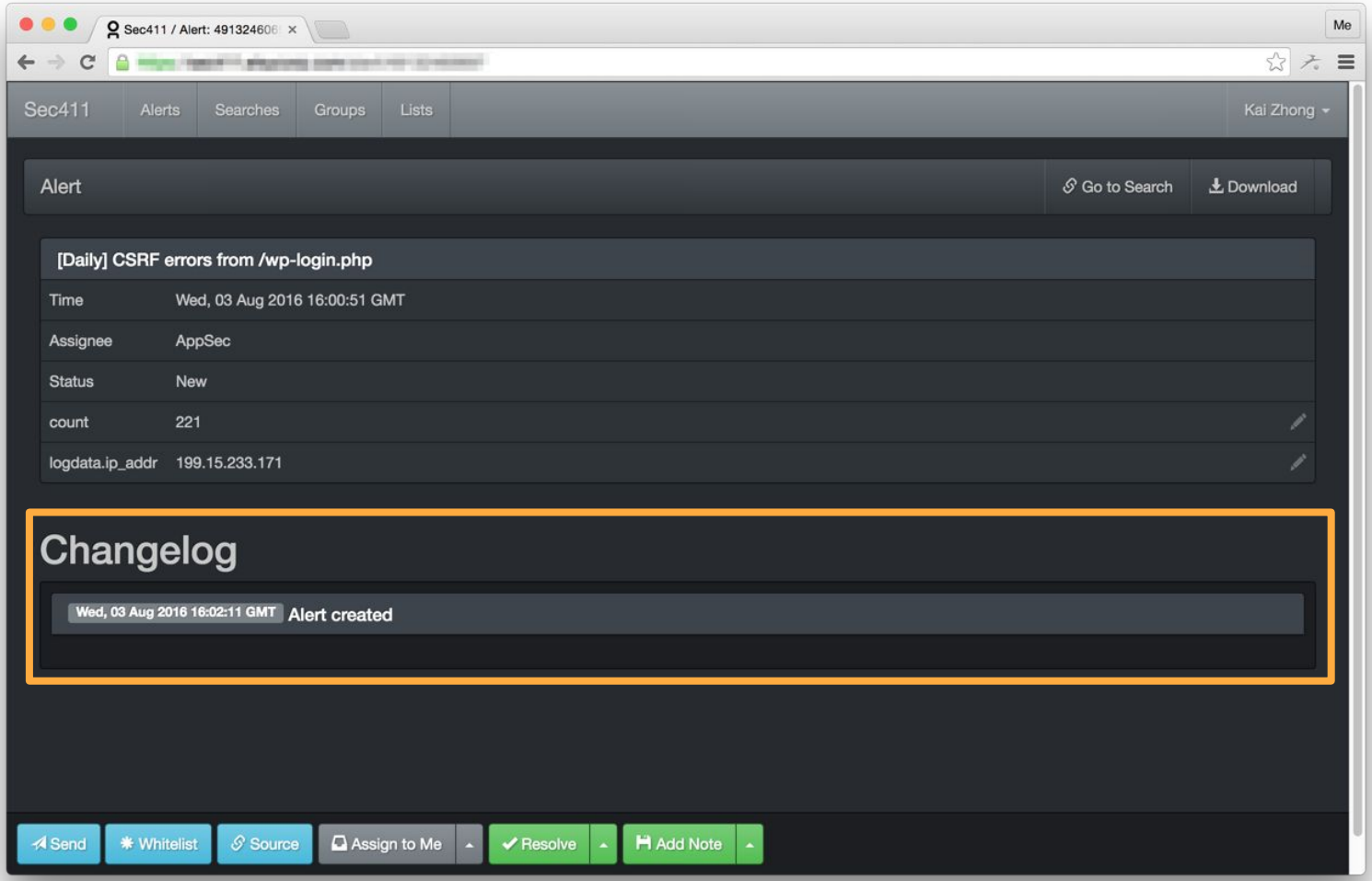

Sec411 / Alerts
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alerts
Toggle All
Feed
Search
state:(0 1)
From
-∞
To
now
Group: AppSec
API AuthZ Hits
High
New
2
Time
logdata.endpoint
View
Source
Wed, 03 Aug 2016 19:57:11 GMT
Api_Shop_Settings
View
Source
Wed, 03 Aug 2016 16:07:35 GMT
Api_Shop_Orders_GetAll
[Daily] CSRF errors from /wp-login.php
Low
New
2
Time
count
logdata.ip_addr
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
59
91.200.12.25
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
221
199.15.233.171
Send
Whitelist
Assign to Me
Resolve
Add Note

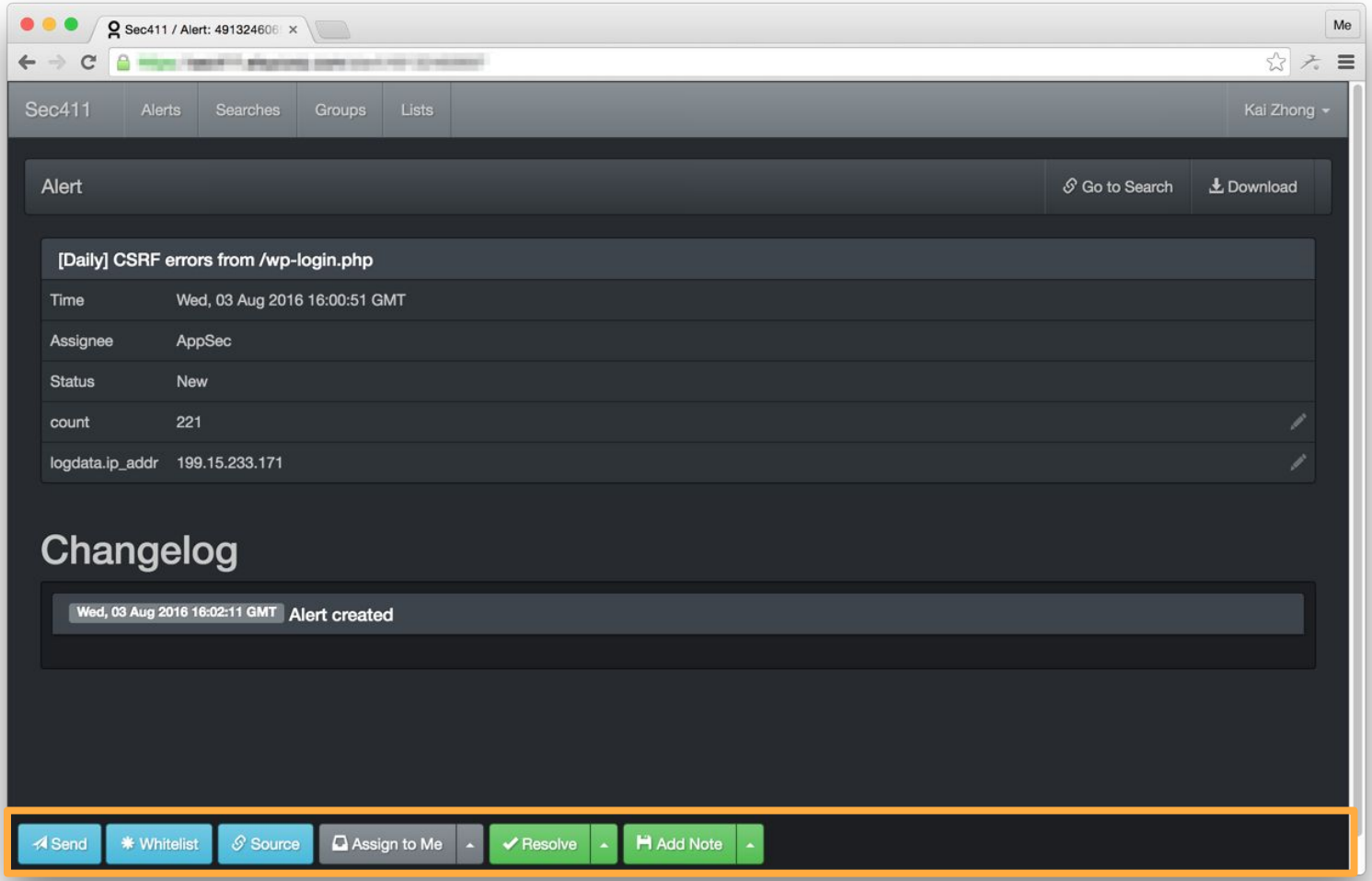

Sec411 / Alerts
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alerts
Toggle All
Feed
Search
state:(0 1)
From
-∞
To
now
Group: AppSec
API AuthZ Hits
High
New
2
Time
logdata.endpoint
View
Source
Wed, 03 Aug 2016 19:57:11 GMT
Api_Shop_Settings
View
Source
Wed, 03 Aug 2016 16:07:35 GMT
Api_Shop_Orders_GetAll
[Daily] CSRF errors from /wp-login.php
Low
New
2
Time
count
logdata.ip_addr
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
59
91.200.12.25
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
221
199.15.233.171
Send
Whitelist
Assign to Me
Resolve
Add Note

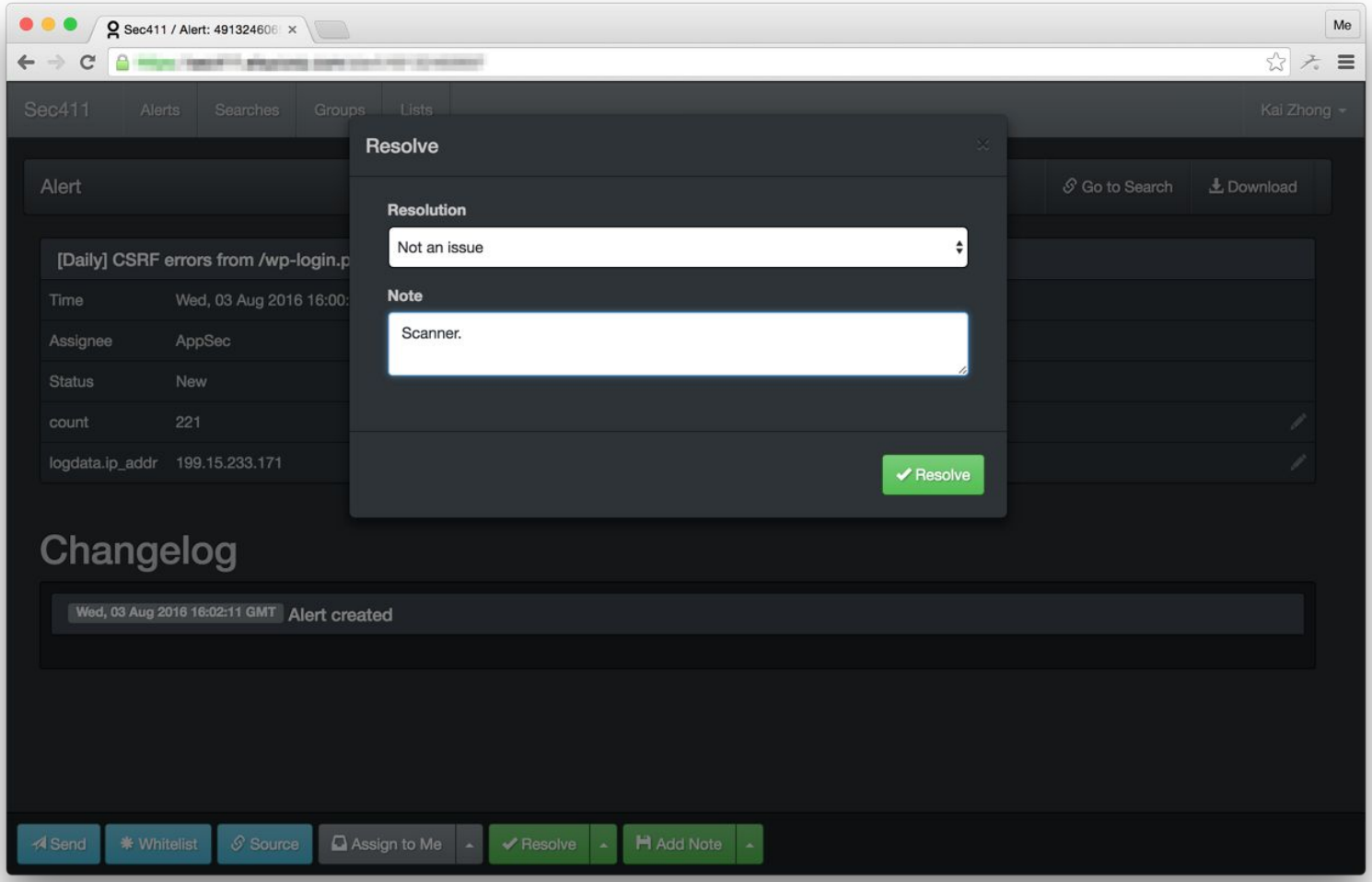

Sec411 / Alerts
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alerts
Toggle All
Feed
Search
state:(0 1)
From
-∞
To
now
Group: AppSec
API AuthZ Hits
High
New
2
Time
logdata.endpoint
View
Source
Wed, 03 Aug 2016 19:57:11 GMT
Api_Shop_Settings
View
Source
Wed, 03 Aug 2016 16:07:35 GMT
Api_Shop_Orders_GetAll
[Daily] CSRF errors from /wp-login.php
Low
New
2
Time
count
logdata.ip_addr
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
59
91.200.12.25
View
Source
Wed, 03 Aug 2016 16:00:51 GMT
221
199.15.233.171
Send
Whitelist
Assign to Me
Resolve
Add Note

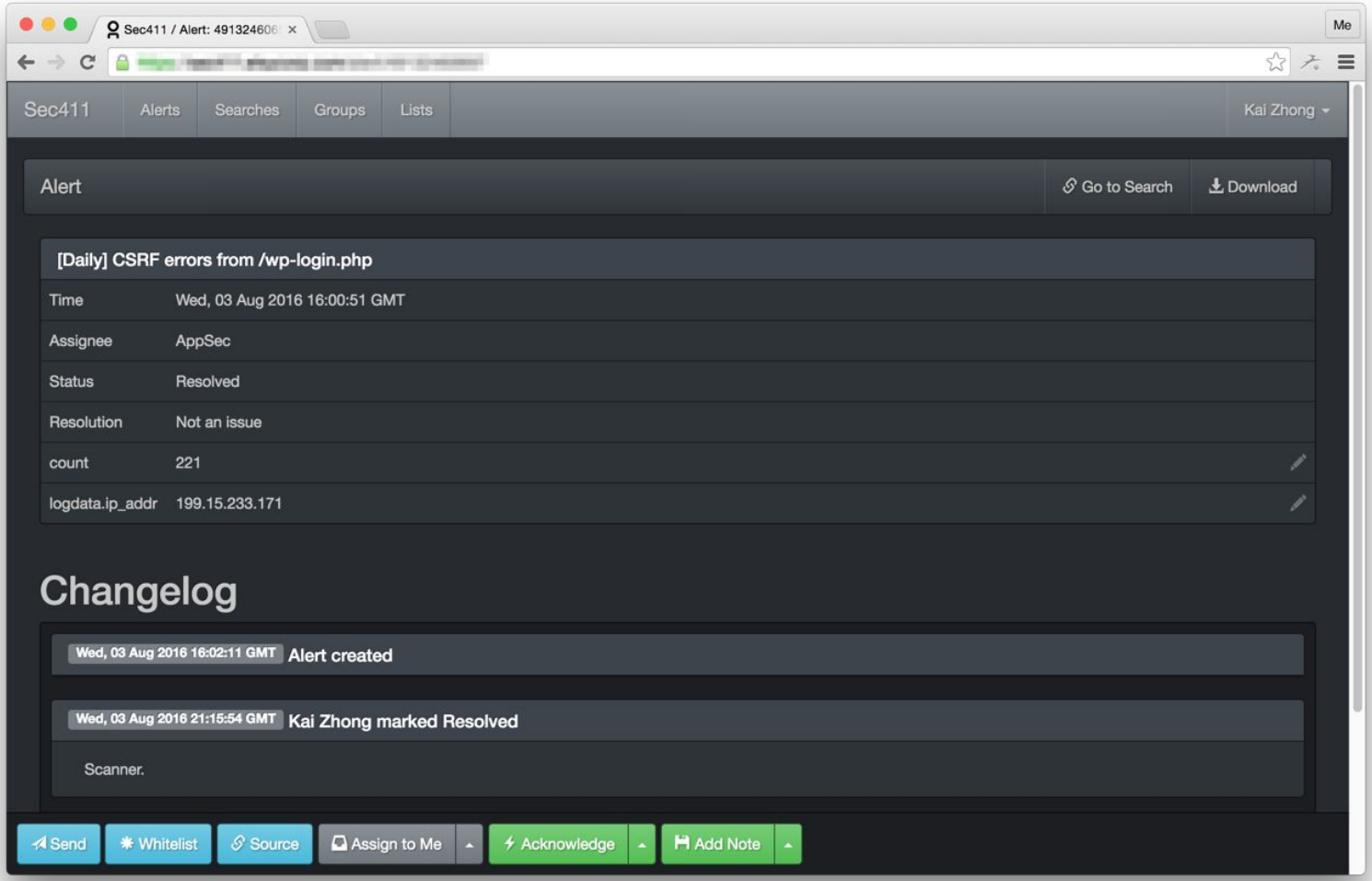
# Reviewing an alert

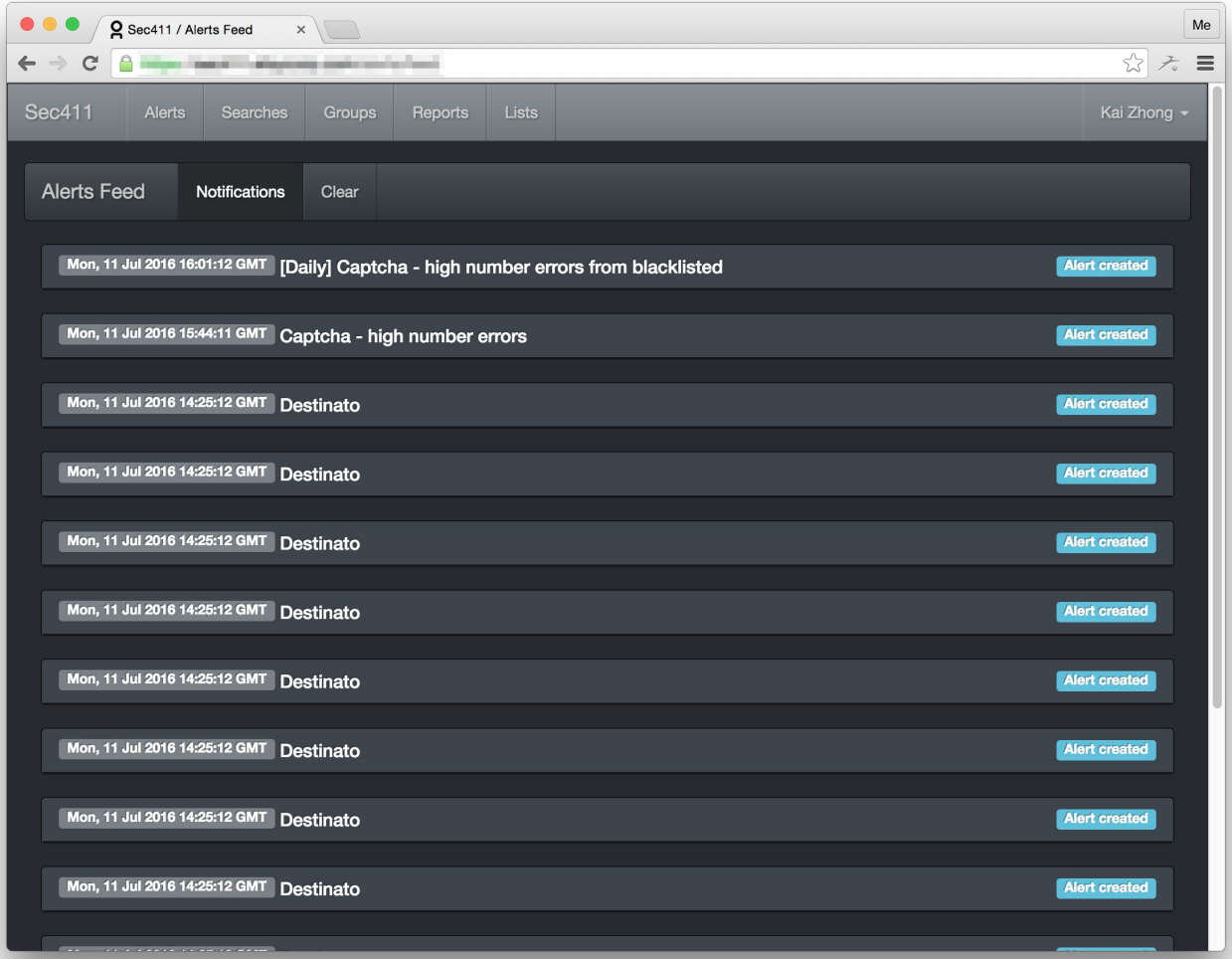

Sec411 / Alert: 491324606
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alert
Go to Search
Download
[Daily] CSRF errors from /wp-login.php
Time
Wed, 03 Aug 2016 16:00:51 GMT
Assignee
AppSec
Status
New
count
221
logdata.ip_addr
199.15.233.171
Changelog
Wed, 03 Aug 2016 16:02:11 GMT
Alert created
Send
Whitelist
Source
Assign to Me
Resolve
Add Note

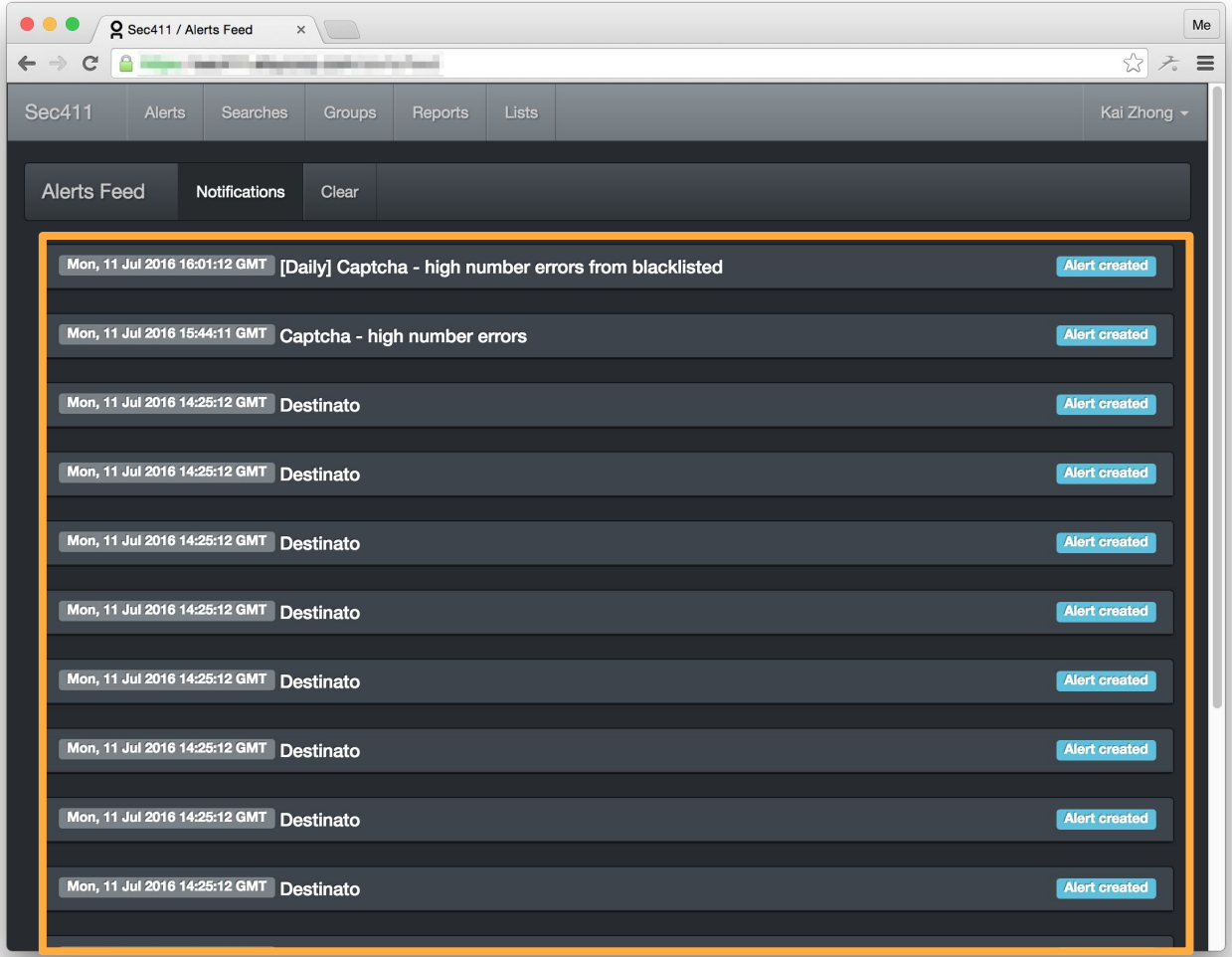

Sec411 / Alert: 491324606
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alert
Go to Search
Download
[Daily] CSRF errors from /wp-login.php
Time
Wed, 03 Aug 2016 16:00:51 GMT
Assignee
AppSec
Status
New
count
221
logdata.ip_addr
199.15.233.171
Changelog
Wed, 03 Aug 2016 16:02:11 GMT
Alert created
Send
Whitelist
Source
Assign to Me
Resolve
Add Note


Sec411 / Alert: 491324606
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alert
Go to Search
Download
[Daily] CSRF errors from /wp-login.php
Time
Wed, 03 Aug 2016 16:00:51 GMT
Assignee
AppSec
Status
New
count
221
logdata.ip_addr
199.15.233.171
Changelog
Wed, 03 Aug 2016 16:02:11 GMT
Alert created
Send
Whitelist
Source
Assign to Me
Resolve
Add Note


Sec411 / Alert: 491324606
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alert
Go to Search
Download
[Daily] CSRF errors from /wp-login.p
Time
Wed, 03 Aug 2016 16:00:
Assignee
AppSec
Status
New
count
221
logdata.ip_addr
199.15.233.171
Resolve
Resolution
Not an issue
Note
Scanner.
Resolve
Changelog
Wed, 03 Aug 2016 16:02:11 GMT
Alert created
Send
Whitelist
Source
Assign to Me
Resolve
Add Note


Sec411 / Alert: 491324606
Me
Sec411
Alerts
Searches
Groups
Lists
Kai Zhong
Alert
Go to Search
Download
[Daily] CSRF errors from /wp-login.php
Time
Wed, 03 Aug 2016 16:00:51 GMT
Assignee
AppSec
Status
Resolved
Resolution
Not an issue
count
221
logdata.ip_addr
199.15.233.171
Changelog
Wed, 03 Aug 2016 16:02:11 GMT
Alert created
Wed, 03 Aug 2016 21:15:54 GMT
Kai Zhong marked Resolved
Scanner.
Send
Whitelist
Source
Assign to Me
Acknowledge
Add Note


Sec411 / Alerts Feed
Me
Sec411
Alerts
Searches
Groups
Reports
Lists
Kai Zhong
Alerts Feed
Notifications
Clear
Mon, 11 Jul 2016 16:01:12 GMT [Daily] Captcha - high number errors from blacklisted
Alert created
Mon, 11 Jul 2016 15:44:11 GMT Captcha - high number errors
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created


Sec411 / Alerts Feed
Me
Sec411
Alerts
Searches
Groups
Reports
Lists
Kai Zhong
Alerts Feed
Notifications
Clear
Mon, 11 Jul 2016 16:01:12 GMT [Daily] Captcha - high number errors from blacklisted
Alert created
Mon, 11 Jul 2016 15:44:11 GMT Captcha - high number errors
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created
Mon, 11 Jul 2016 14:25:12 GMT Destinato
Alert created

# Alert Management @ Etsy

[Sec411] Login 500s

S **sec411** to [redacted] Jul 7

## Login 500s

[1 Alert]

Login 500s investigate!

**Time range:** 5 minute(s)

| | Date | message |
|---|---|---|
| View Source | 2016-07-07 16:47:02 +0000 | [Thu Jul 07 16:47:02 2016] [-:error] [client [REDACTED]] PHP Parse error: syntax error, unexpected end of file, expecting variable (T_VARIABLE) or ${ (T_DOLLAR_OPEN_CURLY_BRACES) or {$ (T_CURLY_OPEN) in connections.php on line 2348 [host [REDACTED]] [request_log_id Co5ub44w/8o] |

Compare alerts

o_O **Omar Ahmed** to [redacted] Jul 7

Ebbo ebbo wauo wauo

Can someone take a look at this file? [redacted]

...

K **Kai Zhong** to [redacted] Jul 7

Asking in #mysql.




i'm sensitive - pinback button badge

beanforest $1.50

# Incident Response

High sensitivity alerts

# Incident Response

High sensitivity alerts

Low alerts don’t generate notification e-mails

# Incident Response

High sensitivity alerts

Low alerts don’t generate notification e-mails

Medium/High alerts generate alerts

# Incident Response

High sensitivity alerts

Low alerts don’t generate notification e-mails

Medium/High alerts generate alerts

Attackers often generate a lot of noise -- can result in numerous alerts firing!

# Responding to an Alert

Is this an alert that can wait till morning?

# Responding to an Alert

Is this an alert that can wait till morning?

How many other related alerts went off during this time period?

# Alert Maintenance

Sometimes certain queries are no longer useful

# Alert Maintenance

Sometimes certain queries are no longer useful

Review noisy alerts

# Alert Maintenance

Sometimes certain queries are no longer useful

Review noisy alerts

Add in other useful fields

# What Deserves an Alert?

Potential error conditions

# What Deserves an Alert?

Potential error conditions

Volume of traffic/Thresholds being hit

# What Deserves an Alert?

Potential error conditions

Volume of traffic/Thresholds being hit

Deprecating old code

# Instances

Sec411

# Instances

Sec411

Netsec411

# Instances

Sec411

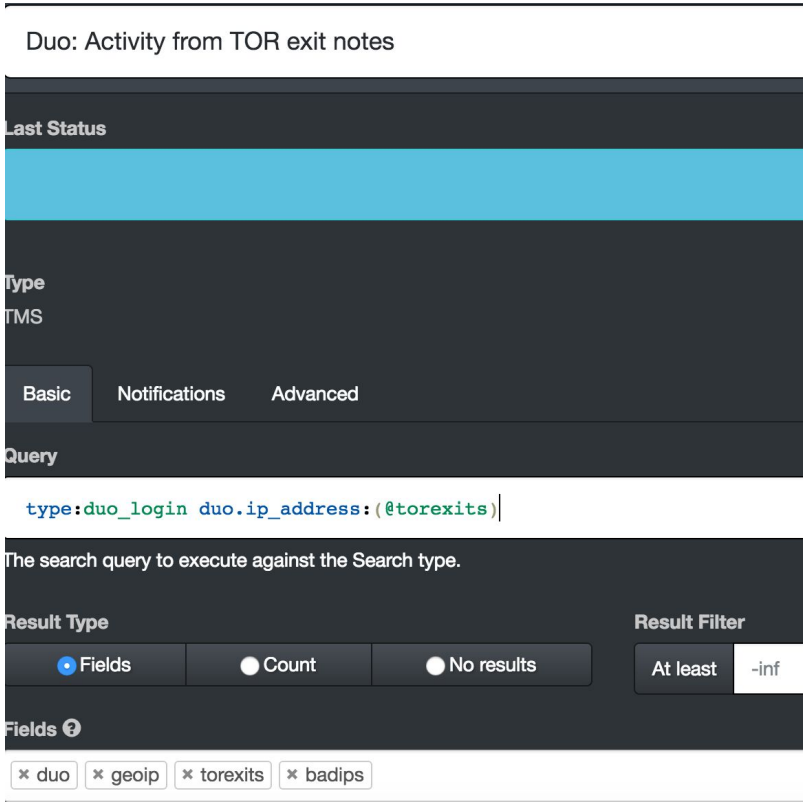
Netsec411

Sox411

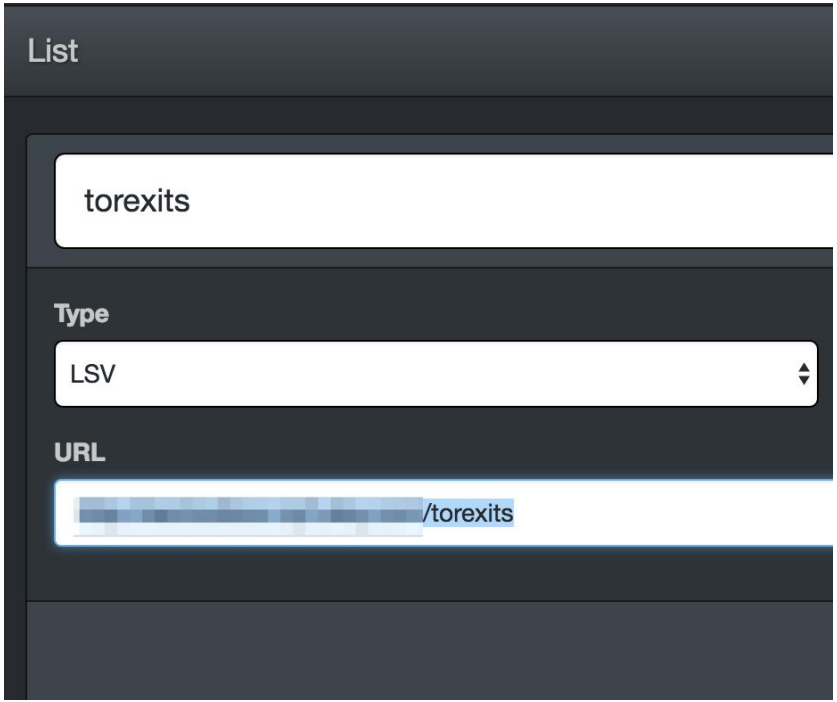
# More Examples

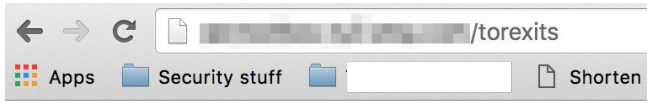

Etsy!

# Better Queries with Lists



# Better Queries with Lists




```
2.111.70.28
2.242.35.6
4.31.64.70
5.9.158.75
5.9.195.140
5.28.62.85
5.34.183.72
5.39.217.14
5.56.133.19
5.79.68.161
5.79.70.174
5.135.85.23
5.135.158.101
5.135.199.14
5.146.204.188
5.165.73.118
5.189.140.238
5.189.146.133
5.189.188.111
5.196.39.57
5.196.39.63
5.196.66.162
5.196.121.161
5.196.143.10
5.199.130.188
5.199.142.195
5.249.145.164
```

# Beyond ELK



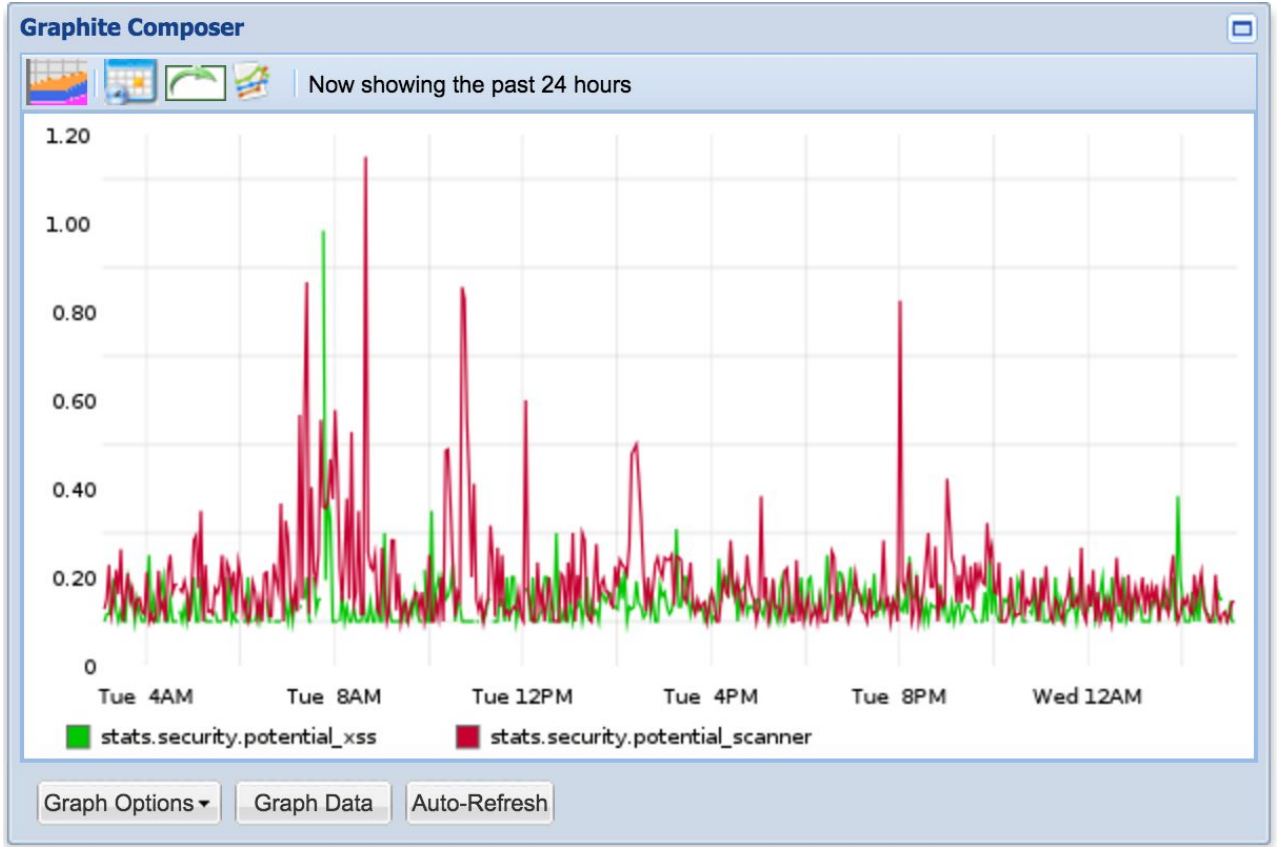

Got Elk? Coffee Mug - Great Birthday Gift f...

SignsMT $15.95



Carbon Sticks 99,9% Graphite for GaNS pr...

LiquidPlasmaFeeding US$13.76


Graphite Composer
Now showing the past 24 hours
1.20
1.00
0.80
0.60
0.40
0.20
0
Tue 4AM
Tue 8AM
Tue 12PM
Tue 4PM
Tue 8PM
Wed 12AM
stats.security.potential_xss
stats.security.potential_scanner
Graph Options
Graph Data
Auto-Refresh

# Graphite

A way to store and graph time series data

# Graphite

A way to store and graph time series data

Best for simple threshold alerting

# Graphite

A way to store and graph time series data

Best for simple threshold alerting

All of Graphite’s data transforms are available




HTTP TCP/IP Cufflinks

cuffcuff US$38.00

# HTTP

Detect when a HTTP endpoint returns an unexpected response

# HTTP

Detect when a HTTP endpoint returns an unexpected response

Useful for web services

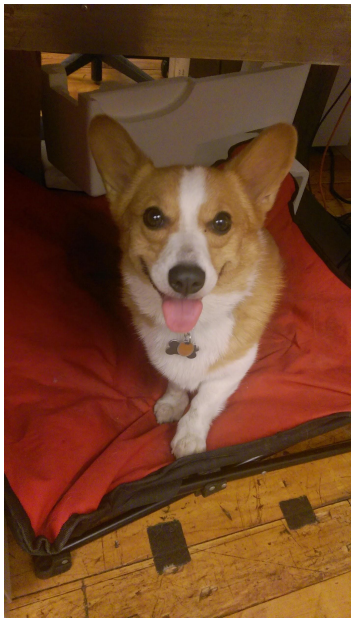
# HTTP

Detect when a HTTP endpoint returns an unexpected response

Useful for web services

Similar in functionality to Nagios

# Demo



# Questions?

## Check out 411 here:

https://fouroneone.io

Kai
@sixhundredns
kai@etsy.com

Ken Lee
@kennysan
ken@etsy.com

