CMS HELL

Pedro Worcel – OWASP AKL
Security-Assessment.com

dimension data

security-assessment.com

About me

- More than five years of experience in IT.
- Security Consultant at Security-Assessment.com.
- Originally from Uruguay.

dimension data

security-assessment.com

TL;DR

- I scanned NZ for out-dated CMSs, found a lot.
- This talk revolves around “Using Components with Known Vulnerabilities” from the OWASP Top 10.

What is a CMS?

- Stands for Content Management System.
- They are pre-made, pre-packaged web applications.

- Drupal is a very popular CMS worldwide.
- SilverStripe is a NZ-Made one, pretty popular in the country.

Is this kind of scanning “legal”?

- Of course, otherwise I would not do it.
- Tool made for non-malicious usage only.
- Scanning machine was in Romania (paid using Bitcoin.)

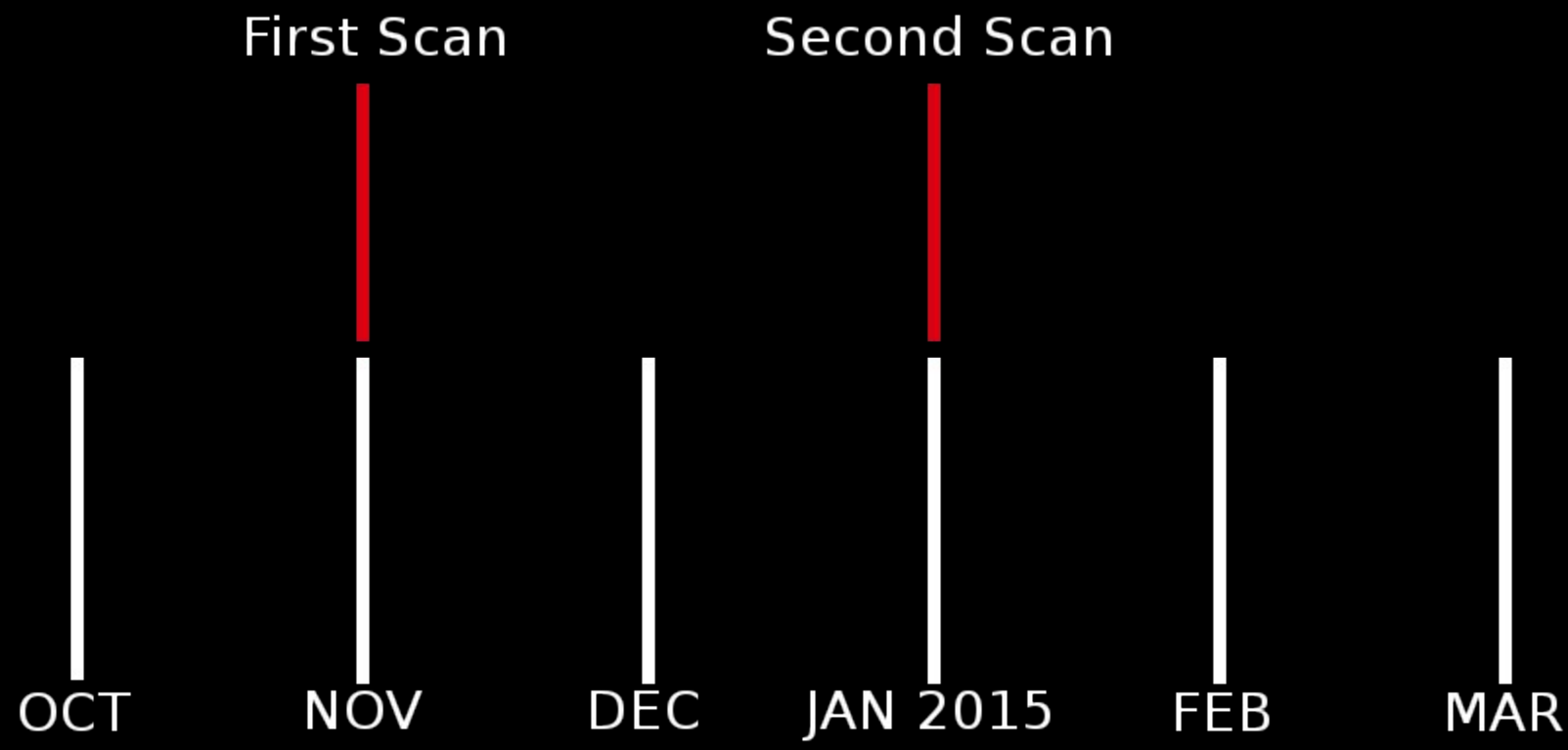
Methodology (TL;DR)

1. Get a list of all HTTP Servers in New Zealand (with the help of Rapid 7’s Sonar project & MaxMind.)
2. Get “domain names” which live in each host using robtex (VirtualHosts is another term.)
3. Scan using droopescan.

The Results

Two scans ran, November 2014 and January 2015.

- Approx 115.000 domains scanned.
- 2492 Drupal installations.
- 2271 SilverStripe installations.



dimension data

security-assessment.com

About Drupaggedon

- SQL injection on the login screen!
- Disclosed by Stefan Horst on the 2014-10-15.
- But...

Previously Reported on public tracker (Open for 7 months)

Database ExpandArguments placeholder naming issues when using array

Posted by david_garcia on *November 29, 2013 at 5:18pm*

[3] Posible door open for SQL injection?

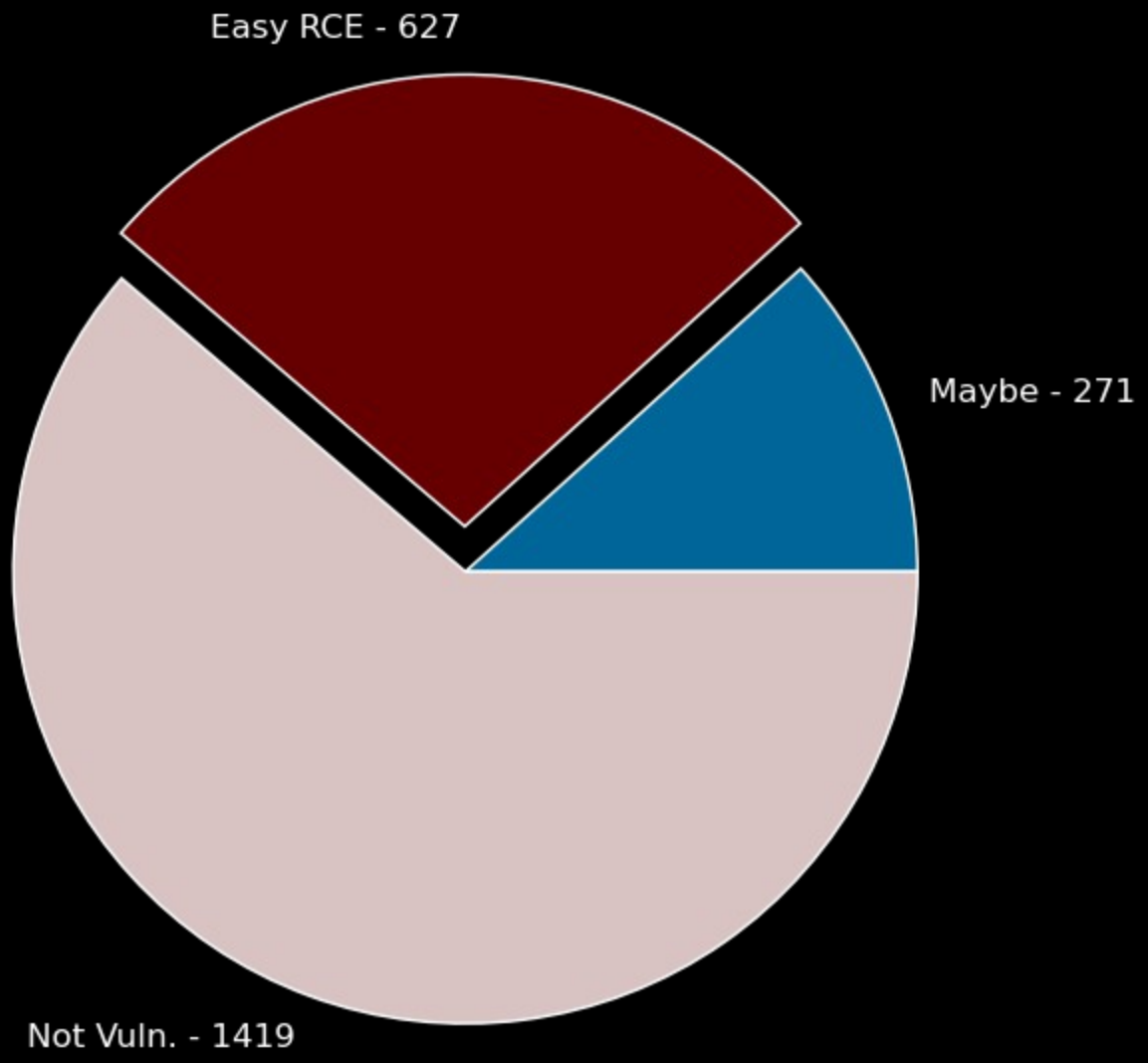
I've tried for a while with someting like this:

```
$params[':nids'] = array(
'ok' => 5,
'ok2) OR (1=1) OR 5 IN (5' => 6,
'ok2' => 7
);

db_query('SELECT UID FROM USERS WHERE USERS.UID IN (:nids)', $params);
```

But I am running SQL Server and the only why I can think of exploiting this would be using duplicate placeholder, wich MySQL swallows but SQL Server complains about. Maybe someone with MySQL can give a try and see if it can make it work.

Drupal (First Scan)



Vulnerable installations in red:

- Between 7.0 and 7.31
- Super easy Remote Code Execution (Drupaggedon)

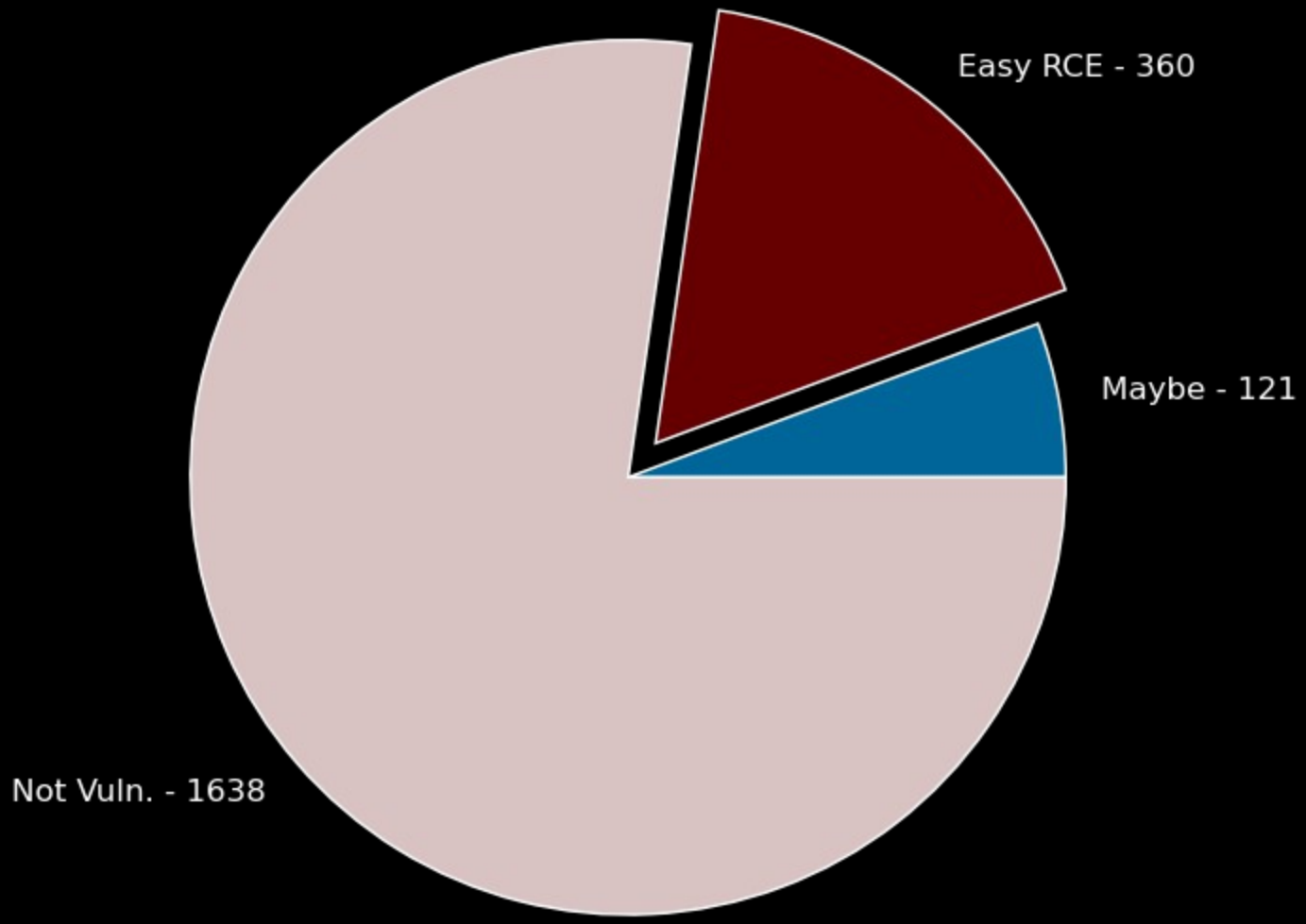
Blue:

- Maybe 7.31, maybe 7.32

dimension data

security-assessment.com

Drupal (Second Scan)

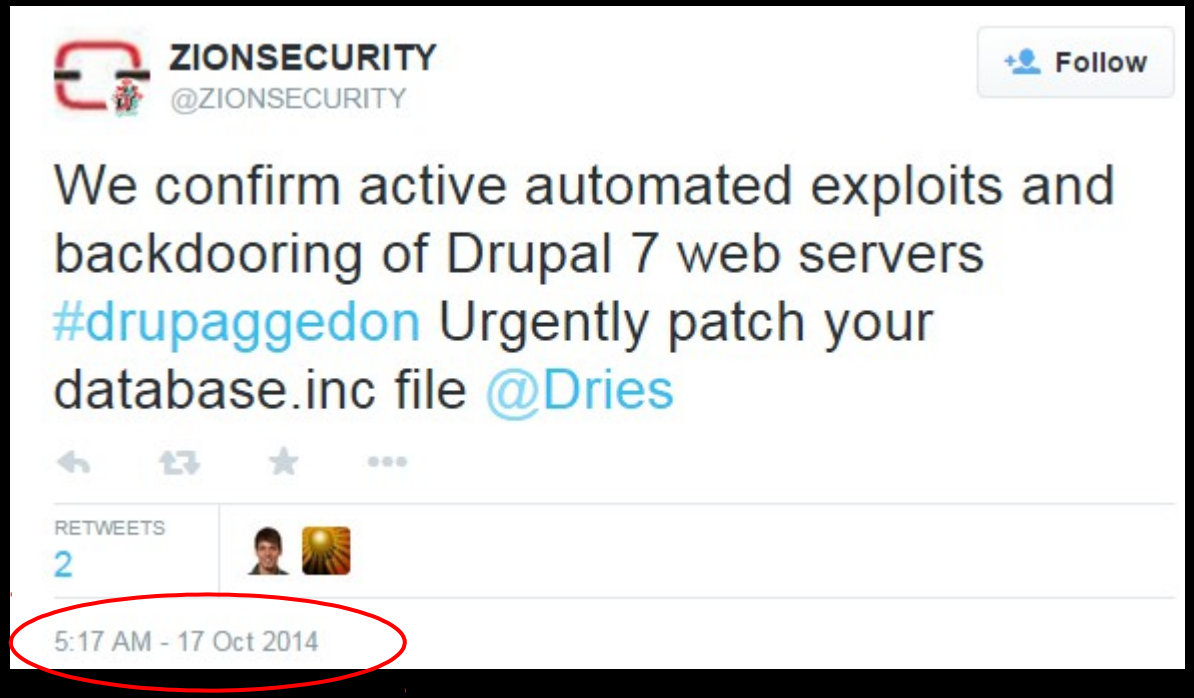


- People patch their stuff! Only took four months for them to get around to it.
- Sites go offline (which makes my numbers not add up)

dimension data

security-assessment.com

Four Months Too Late



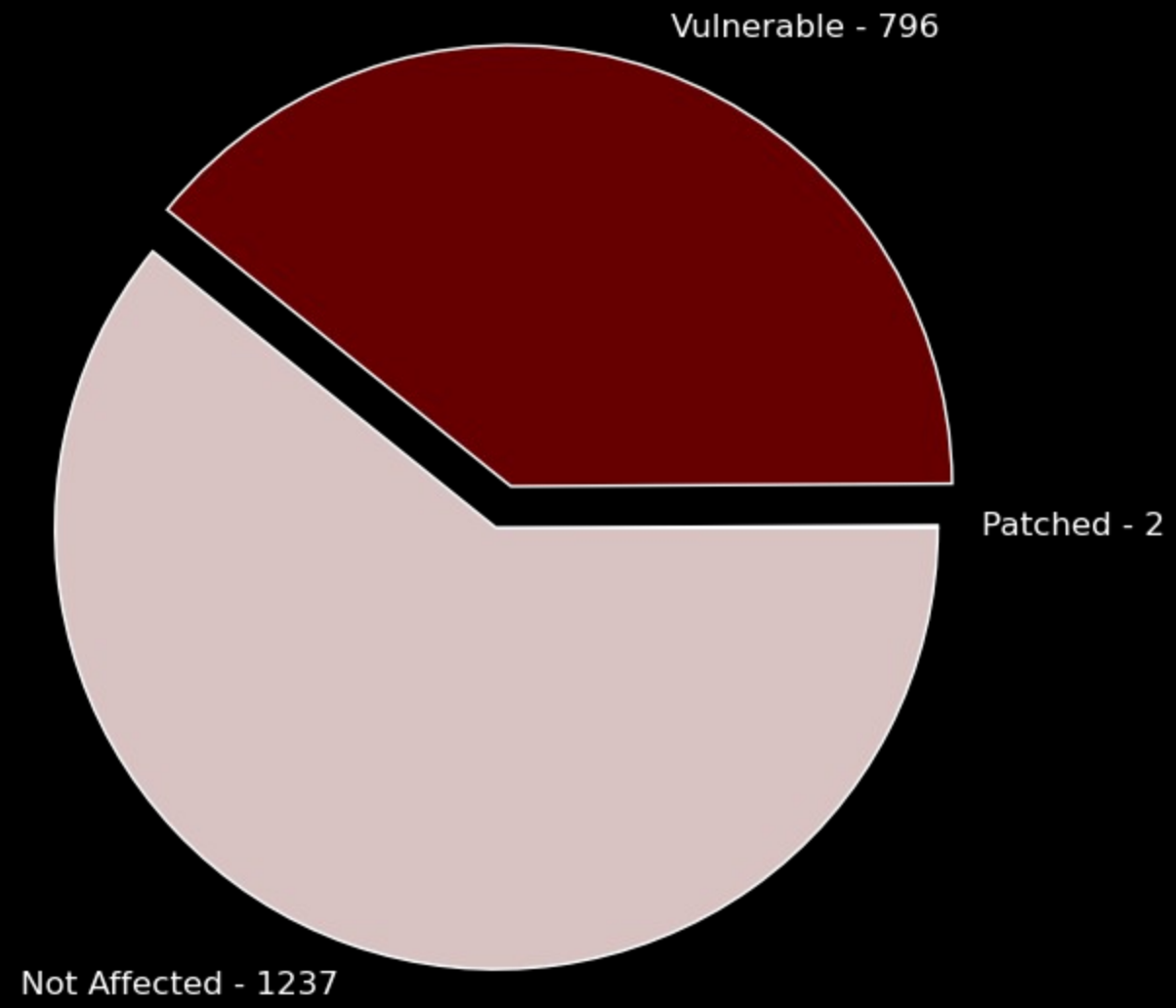
- Acquia confirmed attacks on the same day as Drupal advisory.
- Other people reported automated attacks two days later..

SilverStripe®

dimension data

security-assessment.com

SilverStripe (First Scan)



At time of first scan:

- Username bruteforce vuln disclosed, but no official release from SS.
- Only two domains updated to the release candidate.

dimension data

security-assessment.com

Advisory on 8th, stable release on 14th

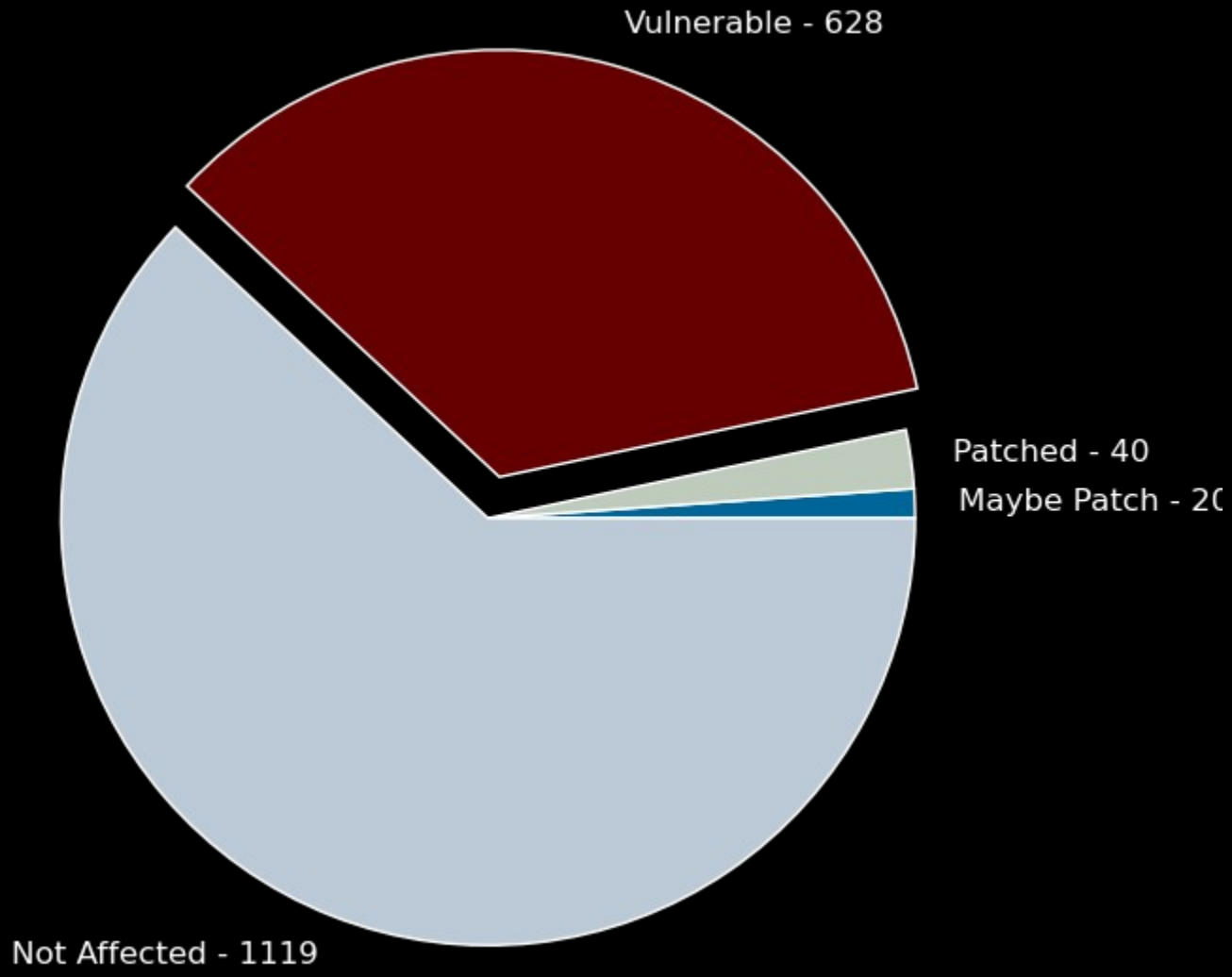
SS-2014-016: Login count is not updated properly when basicauth is used.

Severity:	Low (?)
Identifier:	SS-2014-016
Versions Affected:	3.1
Versions Fixed:	3.1.7
Release Date:	2014-11-08

Login count is not updated properly when basicauth is used, leading to a viable bruteforce attack.

```
2014-11-14 15:38:19 +1300  (tag: 3.1.7)
2014-11-08 18:50:54 +1300  (tag: 3.1.7-rc1)
2014-08-25 11:25:01 +1200  (tag: 3.1.6)
```

SilverStripe (Two Months Later)



- People do not patch their SS.
- This is very bad.

dimension data

security-assessment.com

New bug!

SS-2014-018: Open file permissions vulnerability

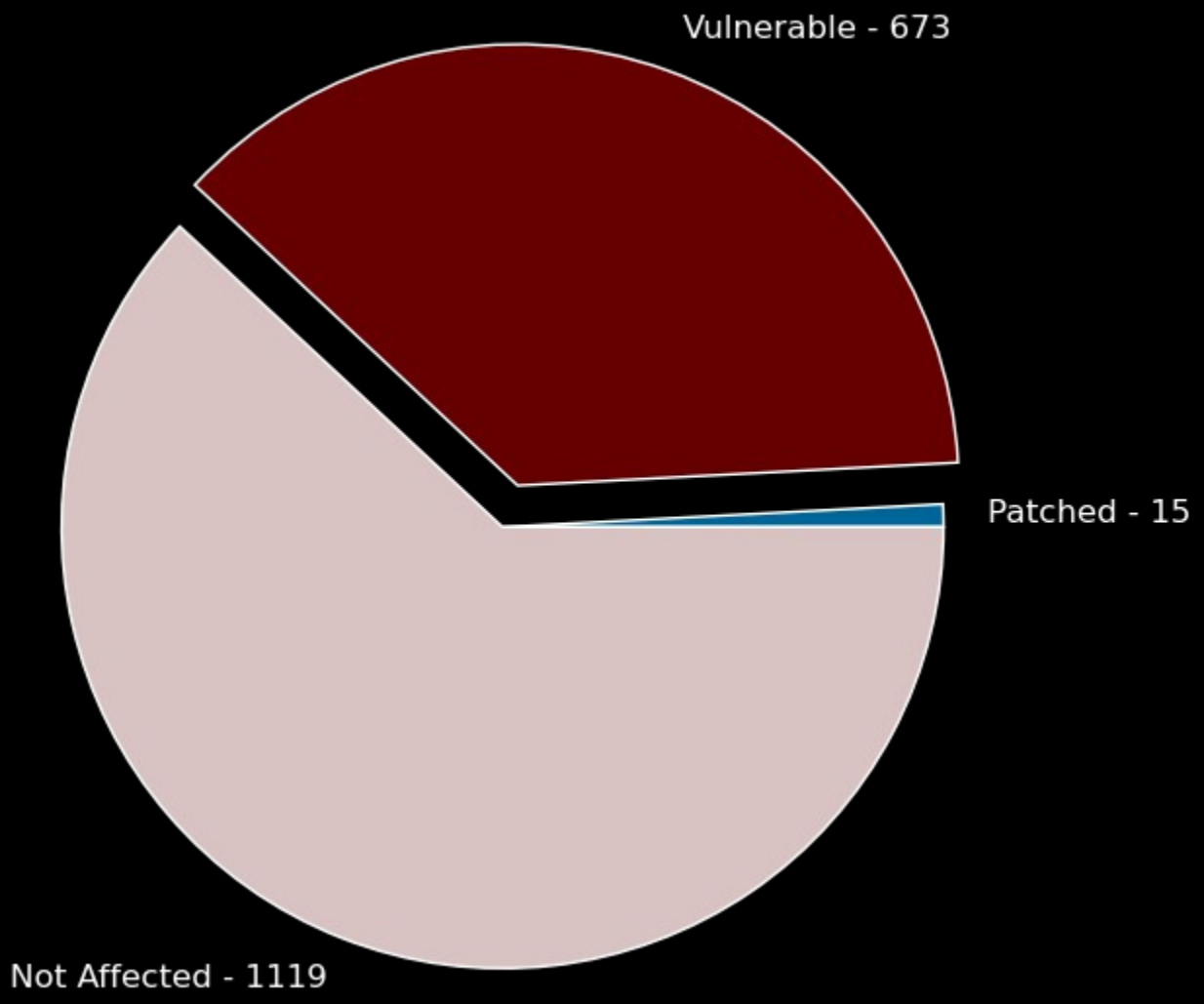
Severity:	Important (?)
Identifier:	SS-2014-018
Versions Affected:	3.1
Versions Fixed:	3.1.9
Release Date:	2015-01-15

The 'edit' & 'delete' actions of UploadField are accessible by unauthenticate

This allows the user unrestricted access to;

- Alter the file or folder name
- Alter the parent folder
- Rename the file
- Change the file owner
- Delete the file or folder

SilverStripe (Third Run)



- AGAIN! No patching.

dimension data

security-assessment.com

About droopescan.

- Written by me while on research time at Security Assessment.
- You can use it for single websites (e.g. your own website or sets of websites.)
- It’s pretty great, I personally recommend it.

https://github.com/droope/droopescan

Demo

Conclusion

- It is important to update.
- Failure to do so could be catastrophic.
- SilverStripe vulnerabilities last for a long time.

Conclusion II

- droopescan is pretty great.
- You can use it to scan your own installation of SilverStripe or Drupal.
- It’s pretty easy to install.

`pip install droopescan`

Q?