



honeyapps
Inc

**The Search For Intelligent Life
OWASP Philadelphia**





honeyapps
Inc

Or.....

The 4 Stages of Security Intelligence





About Me

CoFounder HoneyApps

Former CISO Orbitz

Contributing Author
Beautiful Security

CSO Magazine/Online Author

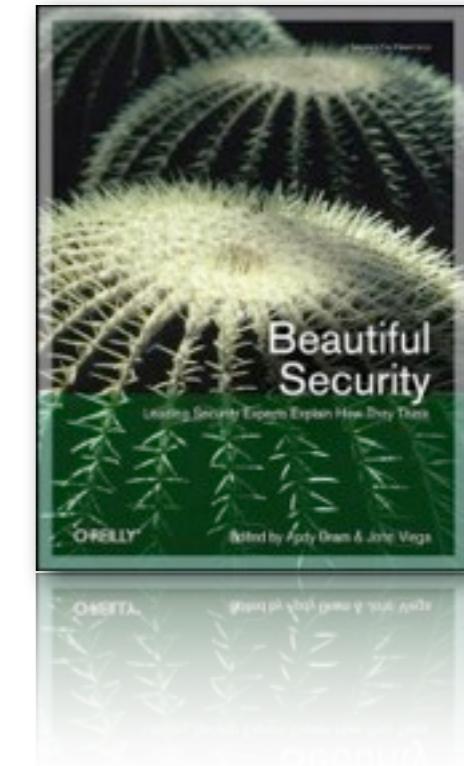
HoneyApps

Vulnerability Management as a Service

16 Hot Startups - eWeek

3 Startups to Watch - Information Week

Nice To Meet You



Stage I: Ignorance is Bliss





Stage 2: Where are all of my vulnerabilities?

Back in my Yahoo days I performed hundreds of web application vulnerability assessments. To streamline the workload, I created an assessment methodology consisting of a few thousand security tests averaging 40 hours to complete per website. Yahoo had over 600 websites enterprise-wide. To assess the security of every website would have taken over 11 years to complete and the other challenge was these websites would change all the time which decayed the value of my reports.

Jeremiah Grossman
Founder, WhiteHat Security





Stage 3: Scan & Dump or...

“thanks for the 1000 page report,
now what?!”



honeyapps
Inc

Why This Occurs

Lack of Communication

Lack of Data

Lack of Coordination

Silos, Silos, Everywhere



Stage 4: A New Beginning

Or.....

Using What You Already Have.



Vulnerability Management: A Case Study

Building the Warehouse

WebApp Vulnerability

Type: XSS

Severity

Threat

Subtype: (persistent, reflected, etc)

Asset URL/URI

Confirmed?

Dates Found/Opened

Dates Closed

Description

Attack Parameters



Vulnerability Management: A Case Study

Building the Warehouse

WebApp Vulnerability

Type: XSS
Severity
Threat
Subtype: (persistent, reflected, etc)
Asset URL/URI
Confirmed?
Dates Found/Opened
Dates Closed
Description
Attack Parameters

Asset: URL

Platform / Code
Web Server Version
Application Server Version
Database Version



Vulnerability Management: A Case Study

Building the Warehouse

WebApp Vulnerability

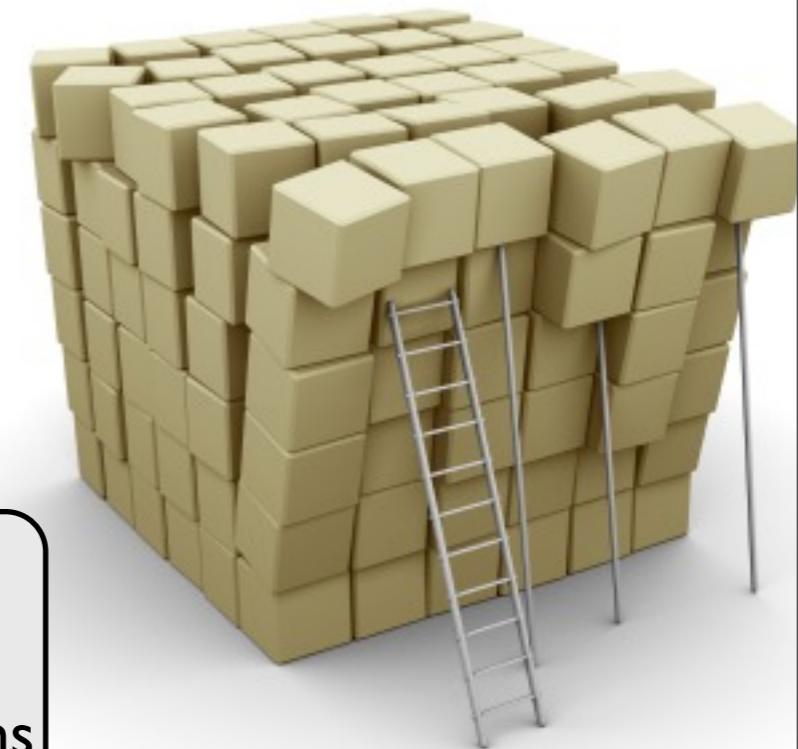
Type: XSS
Severity
Threat
Subtype: (persistent, reflected, etc)
Asset URL/URI
Confirmed?
Dates Found/Opened
Dates Closed
Description
Attack Parameters

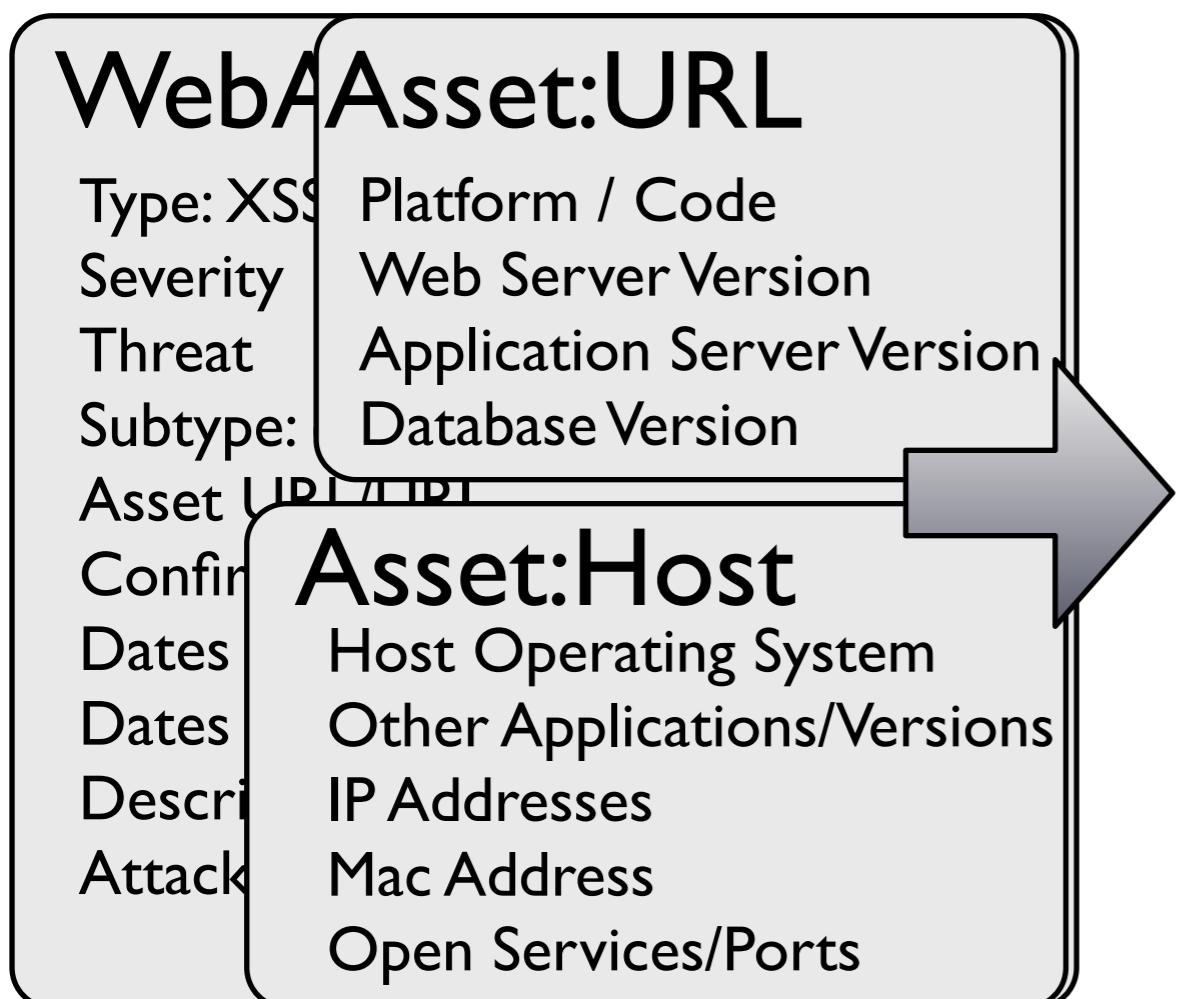
Asset: URL

Platform / Code
Web Server Version
Application Server Version
Database Version

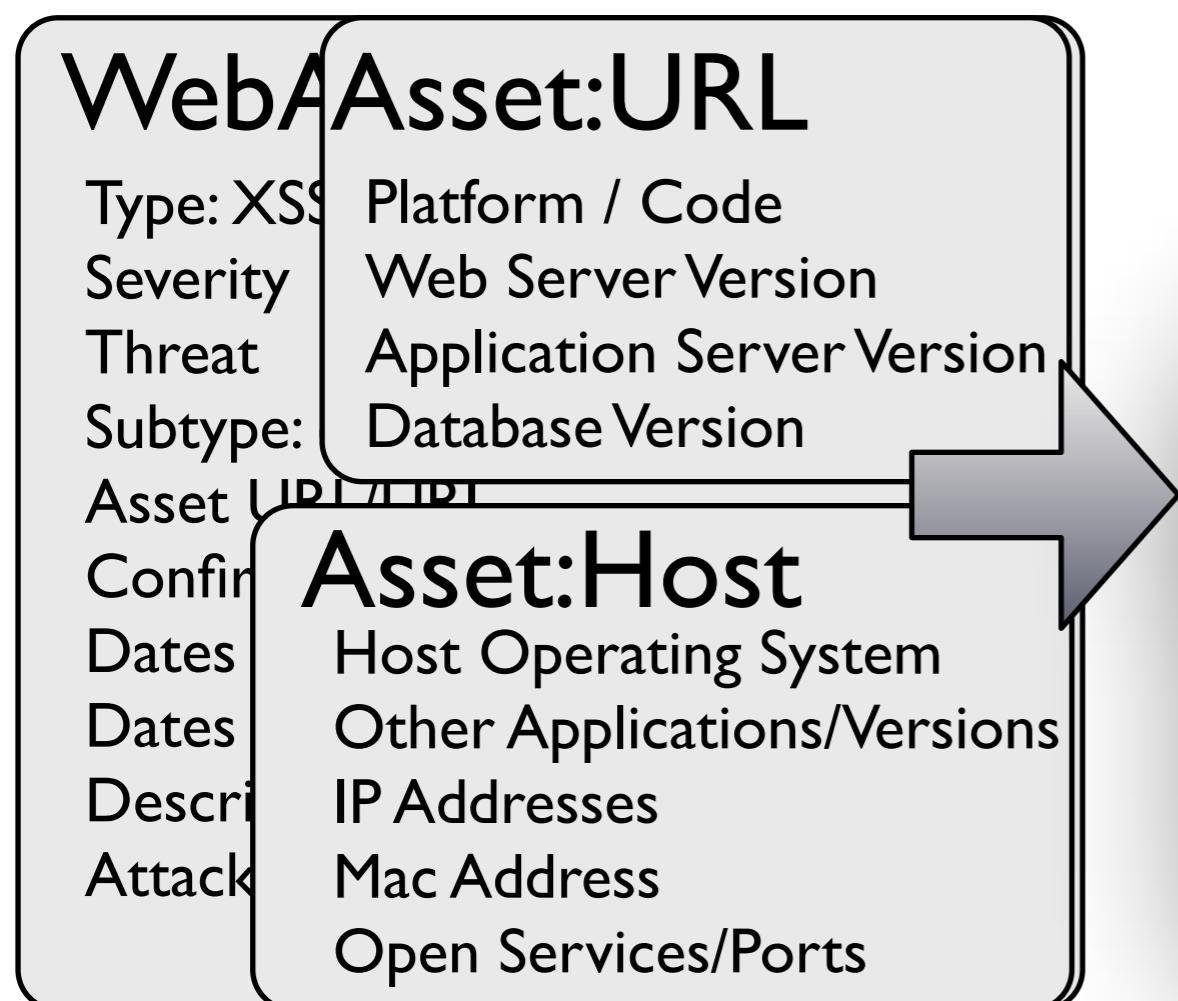
Asset: Host

Host Operating System
Other Applications/Versions
IP Addresses
Mac Address
Open Services/Ports





Vulnerability Management: A Case Study



Meta Data





Vulnerability Management: A Case Study

Web Asset: URL

Type: XSS Platform / Code
Severity
Threat
Subtype: Database Version

Asset URL / IP

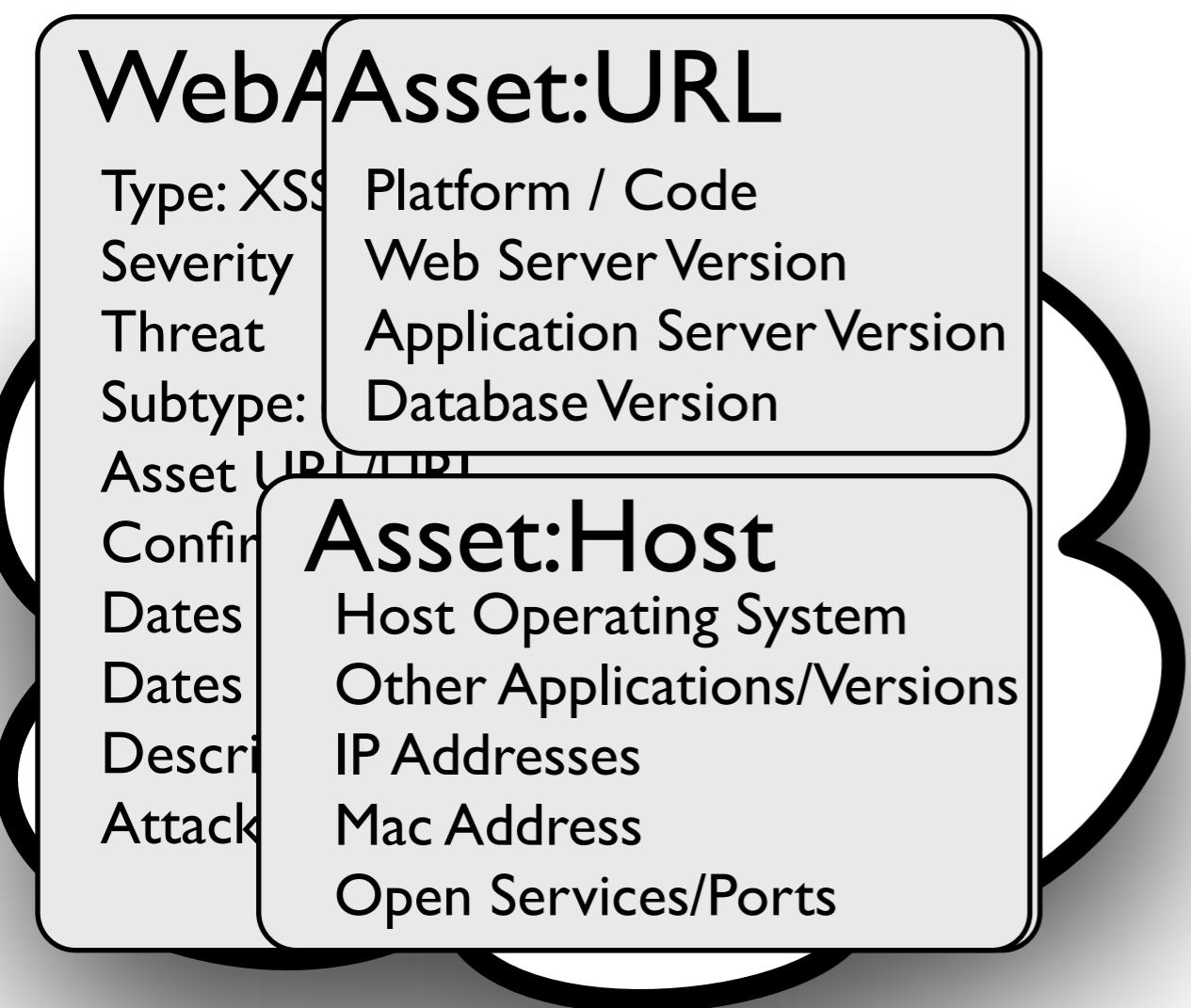
Confir

Asset: Host

Dates Host Operating System
Dates Other Applications/Versions
Descri IP Addresses
Attack Mac Address
Open Services/Ports



Vulnerability Management: A Case Study



Apply Internal Threat Data





Vulnerability Management: A Case Study

Web Asset: URL

Type: XSS Platform / Code
Severity
Threat Web Server Version
Subtype: Application Server Version
Database Version

Asset URL / IP

Confir

Asset: Host

Dates Host Operating System
Dates Other Applications/Versions
Descri IP Addresses
Attack Mac Address
Open Services/Ports



Web Asset: URL

Type: XSS Platform / Code
Severity Web Server Version
Threat Application Server Version
Subtype: Database Version

Asset URL / IP

Asset: Host

Dates Host Operating System
Dates Other Applications/Versions
Descri IP Addresses
Attack Mac Address
Open Services/Ports

Apply External Threat Data





Vulnerability Management: A Case Study

Web Asset: URL

Type: XSS Platform / Code
Severity Web Server Version
Threat Application Server Version
Subtype: Database Version

Asset URL / IP

Asset: Host

Dates Host Operating System
Dates Other Applications/Versions
Description IP Addresses
Attack Mac Address
Open Services/Ports

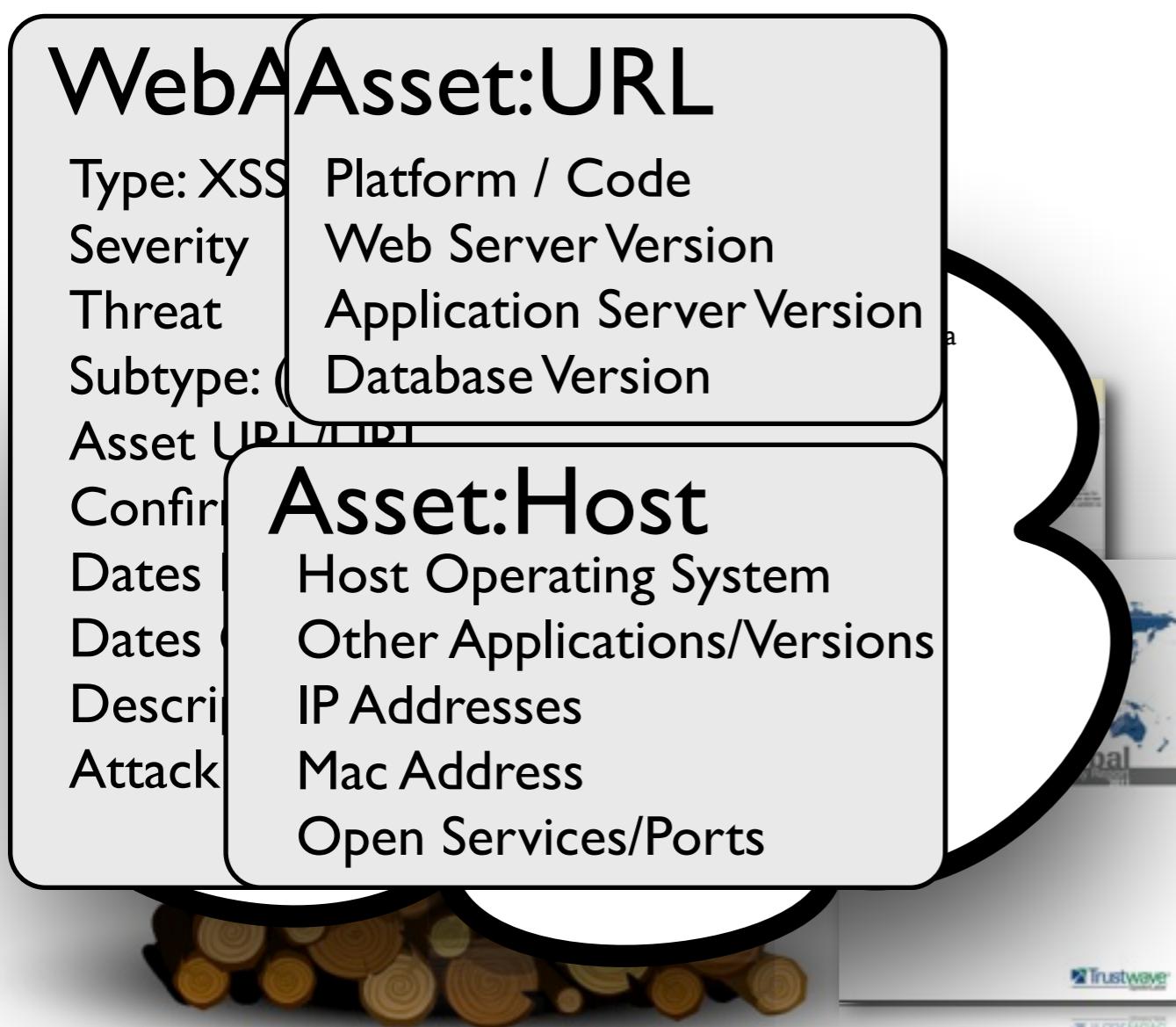
Apply External Threat Data

Example Data Sources

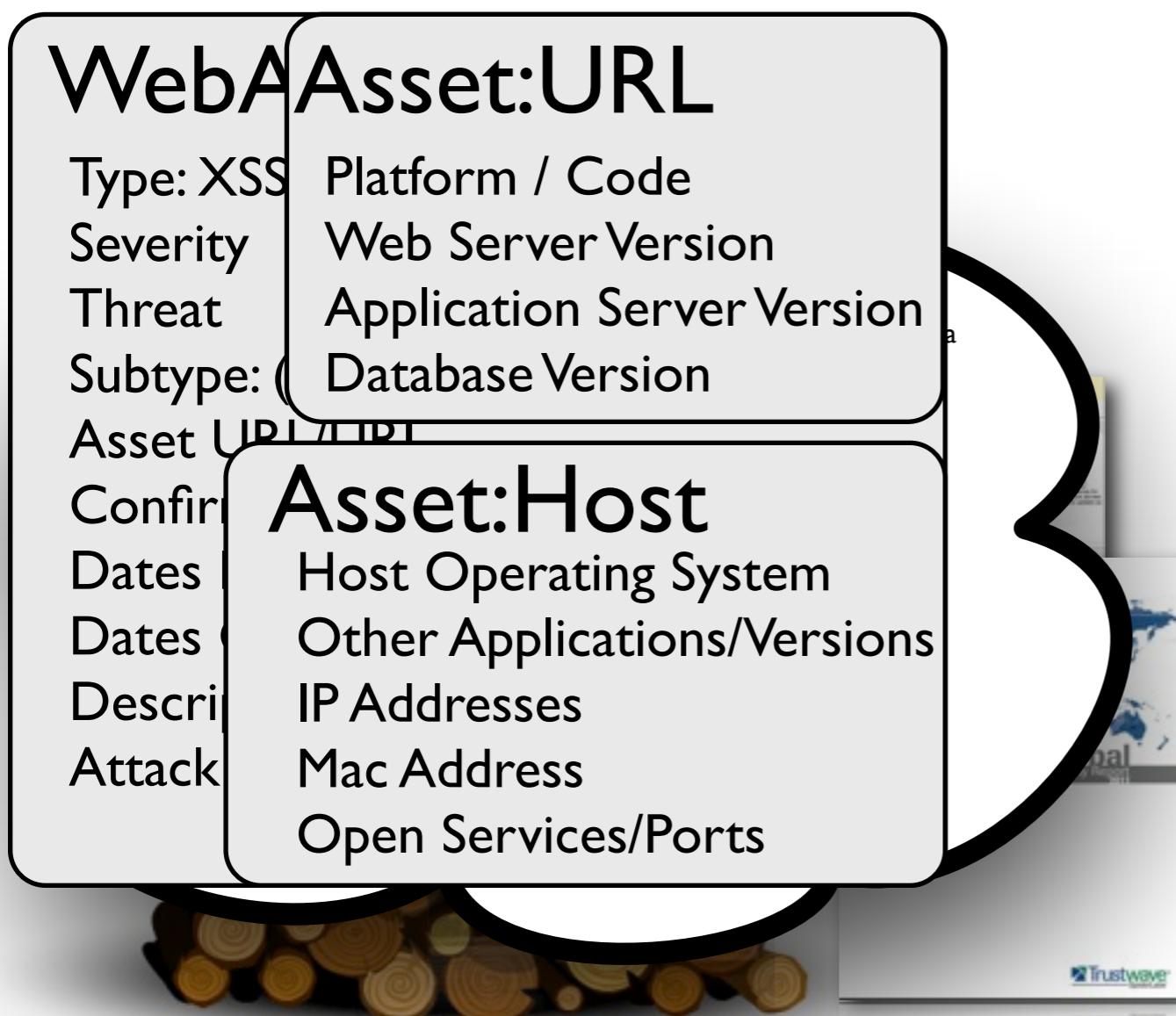
- ❖ DataLossDB
- ❖ Verizon DBIR
- ❖ Trustwave Global Security Report
- ❖ FS-ISAC
- ❖ SANS ISC
- ❖ Symantec DeepSight
- ❖ IBM XForce



Vulnerability Management: A Case Study



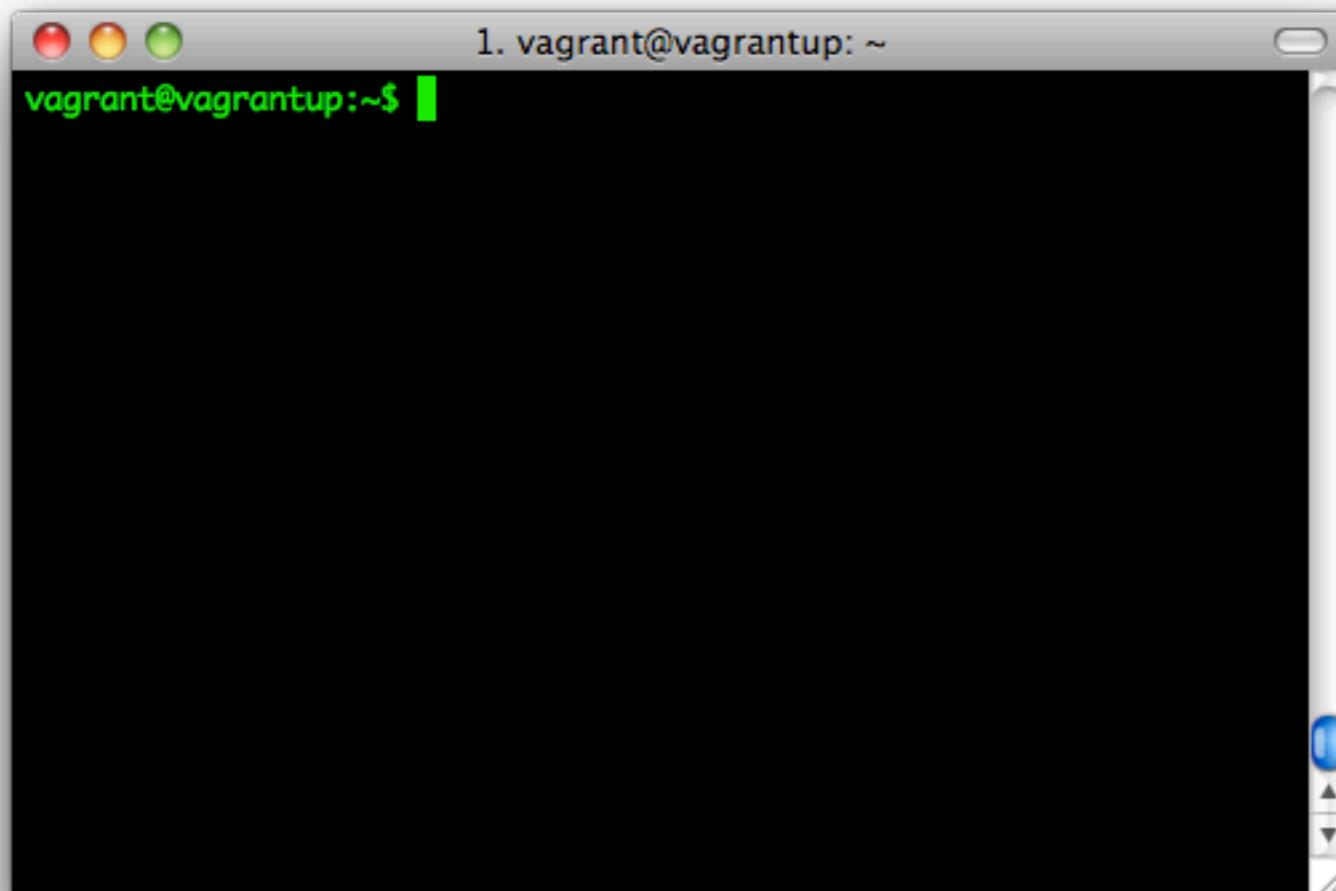
Vulnerability Management: A Case Study



- Remediation Statistics
- Internal Bug Tracking Reports
- Denim Group Remediation Study
- Build and Development Process

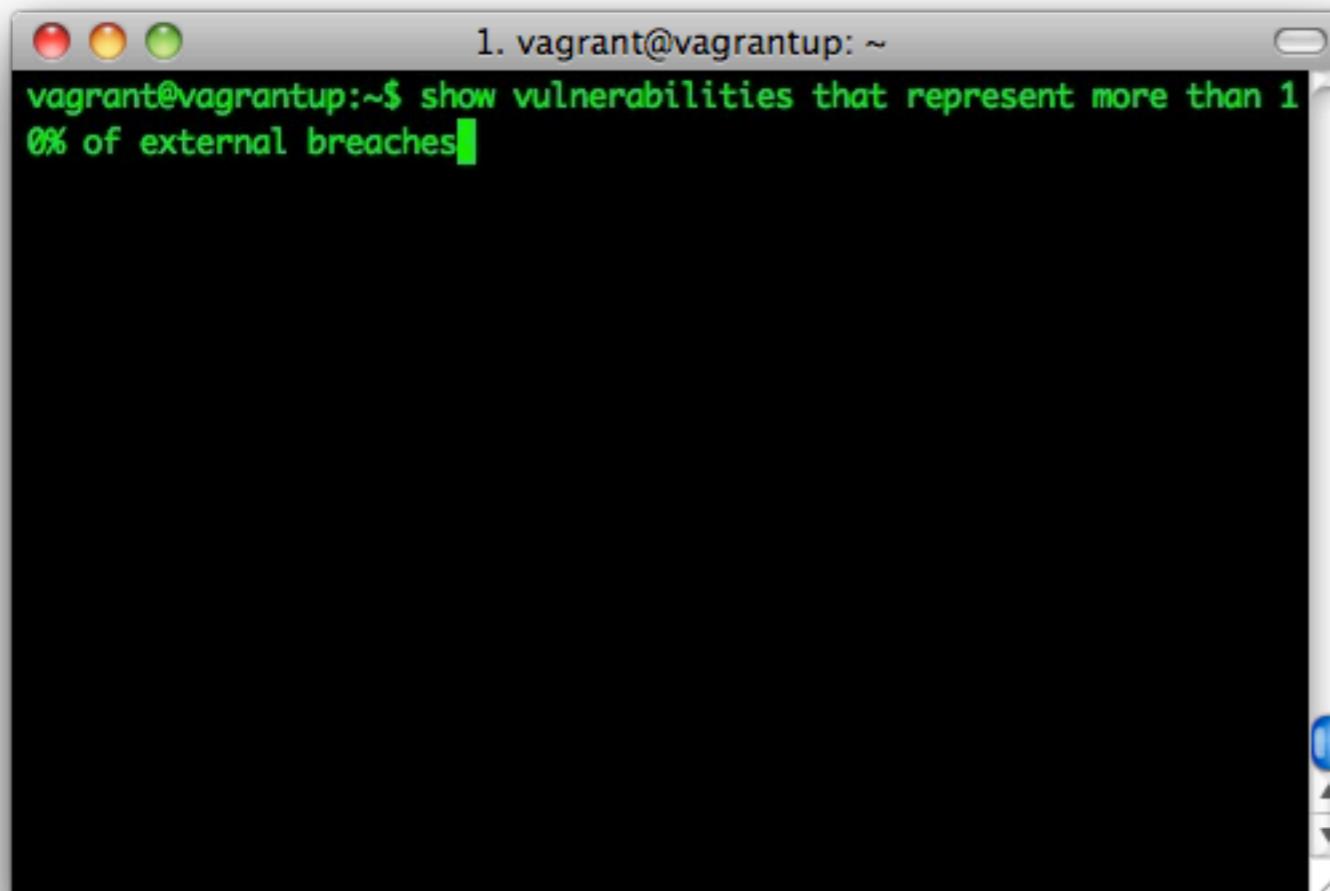
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

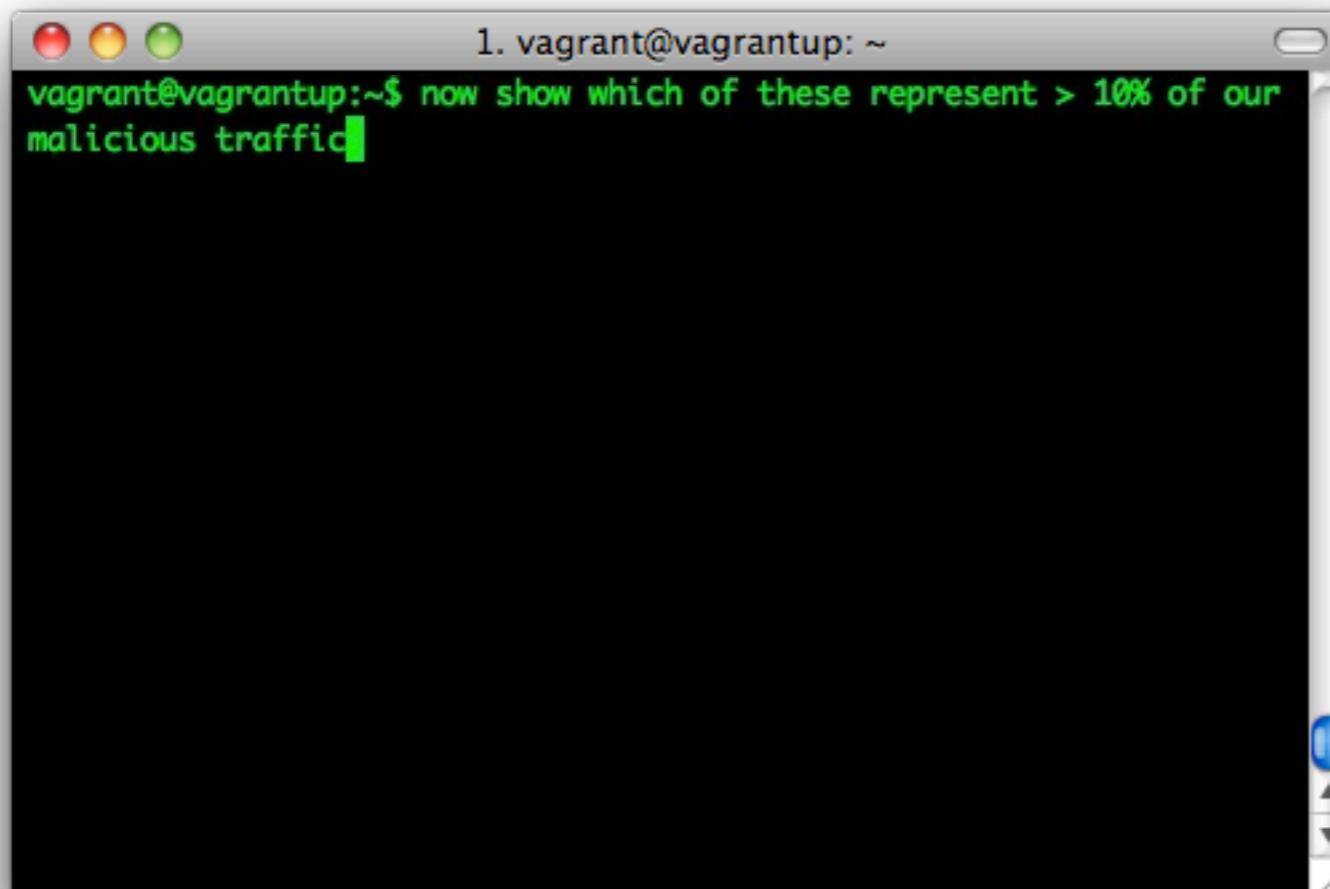


1. vagrant@vagrantup: ~
vagrant@vagrantup:~\$ show vulnerabilities that represent more than 1
0% of external breaches



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

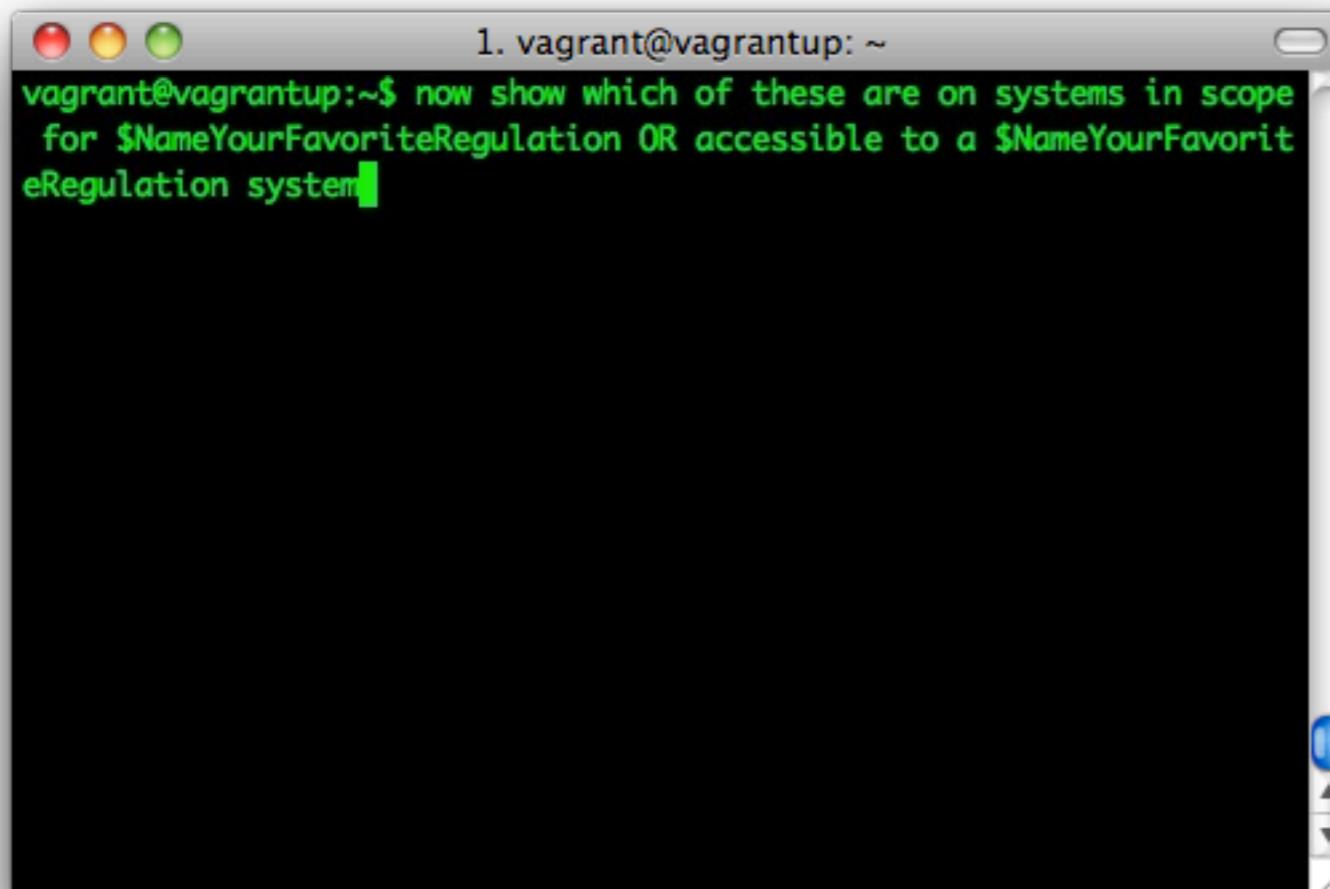


```
1. vagrant@vagrantup: ~
vagrant@vagrantup:~$ now show which of these represent > 10% of our
malicious traffic
```



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

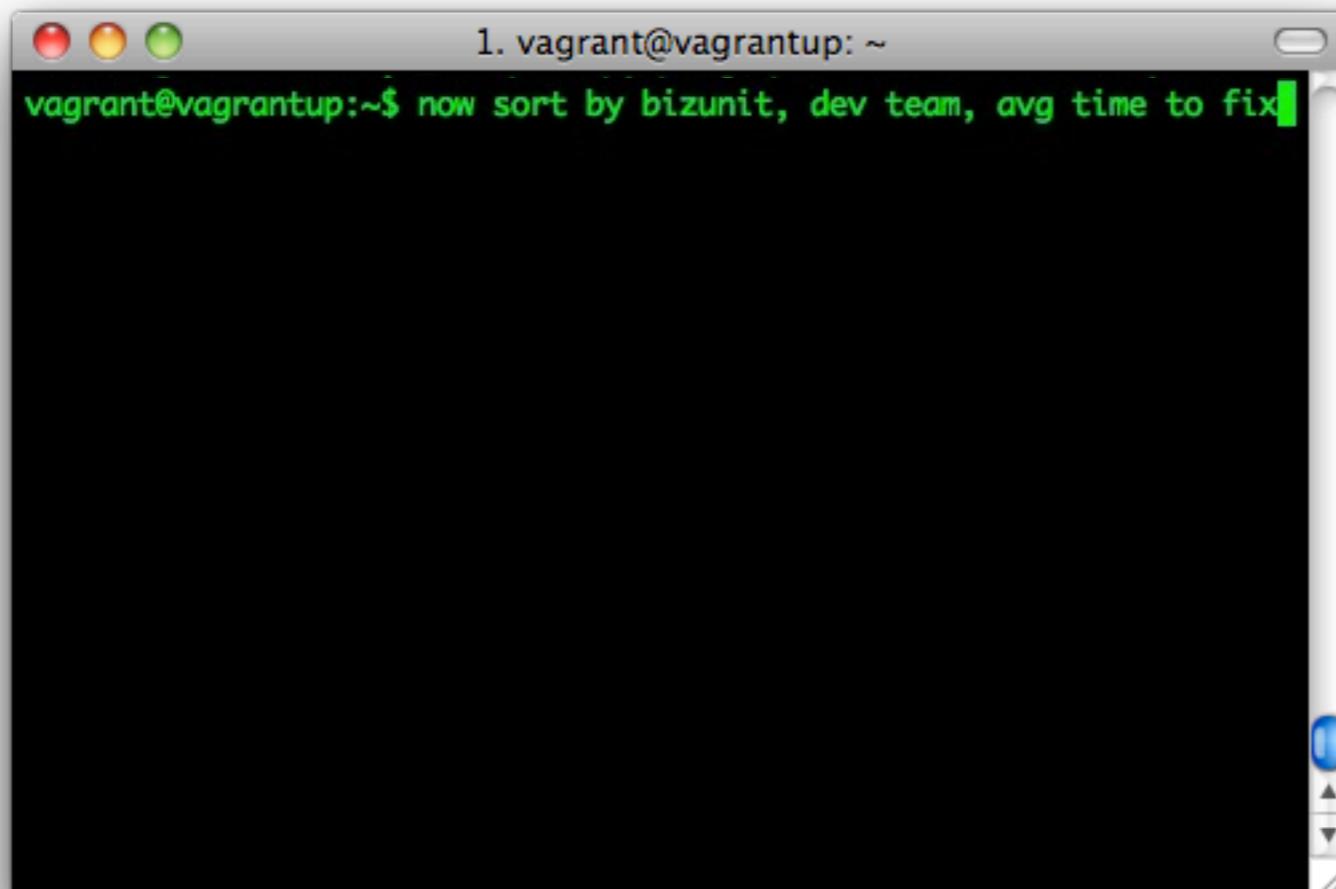


1. vagrant@vagrantup: ~
vagrant@vagrantup:~\$ now show which of these are on systems in scope
for \$NameYourFavoriteRegulation OR accessible to a \$NameYourFavorit
eRegulation system



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

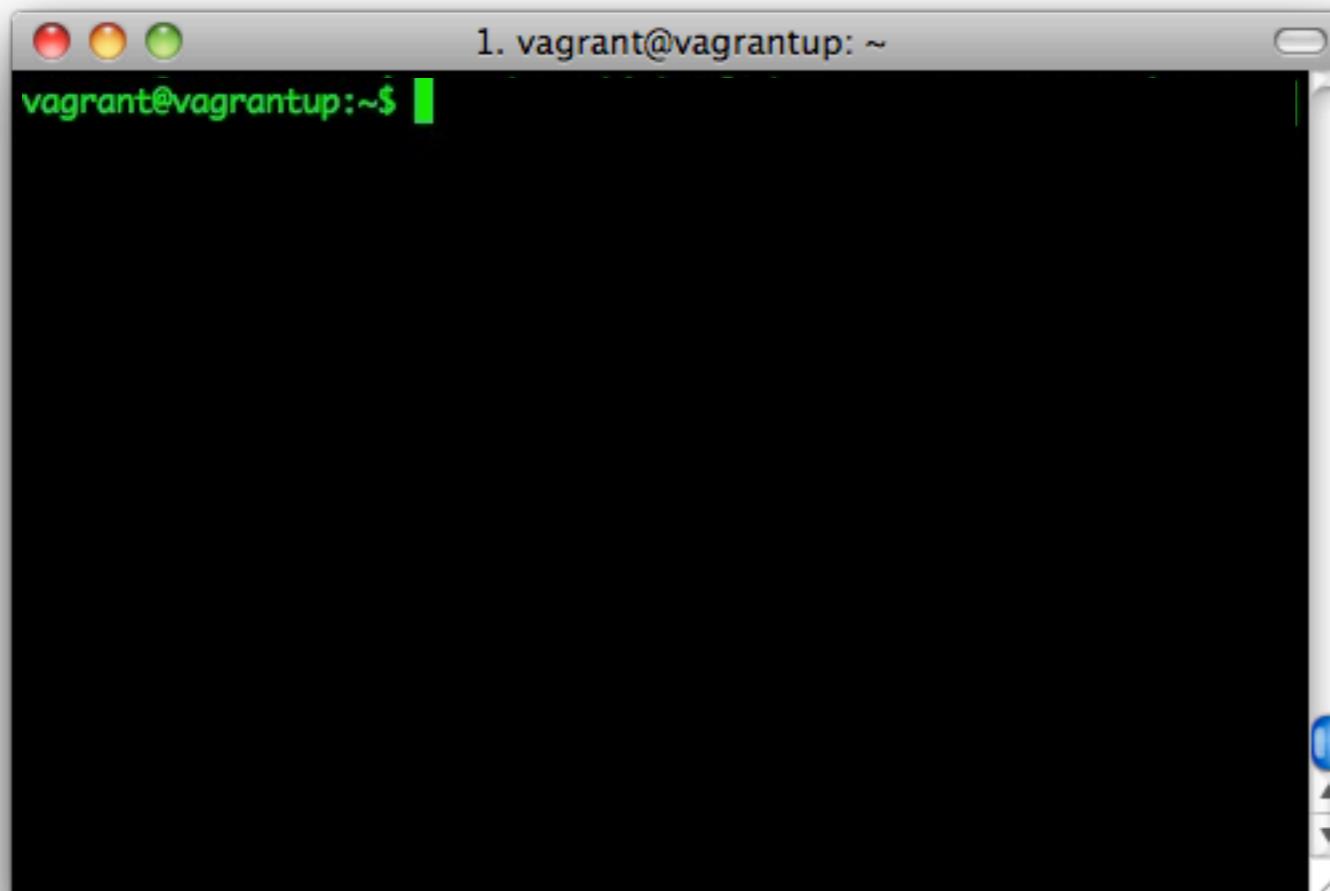


```
1. vagrant@vagrantup: ~
vagrant@vagrantup:~$ now sort by bizunit, dev team, avg time to fix
```



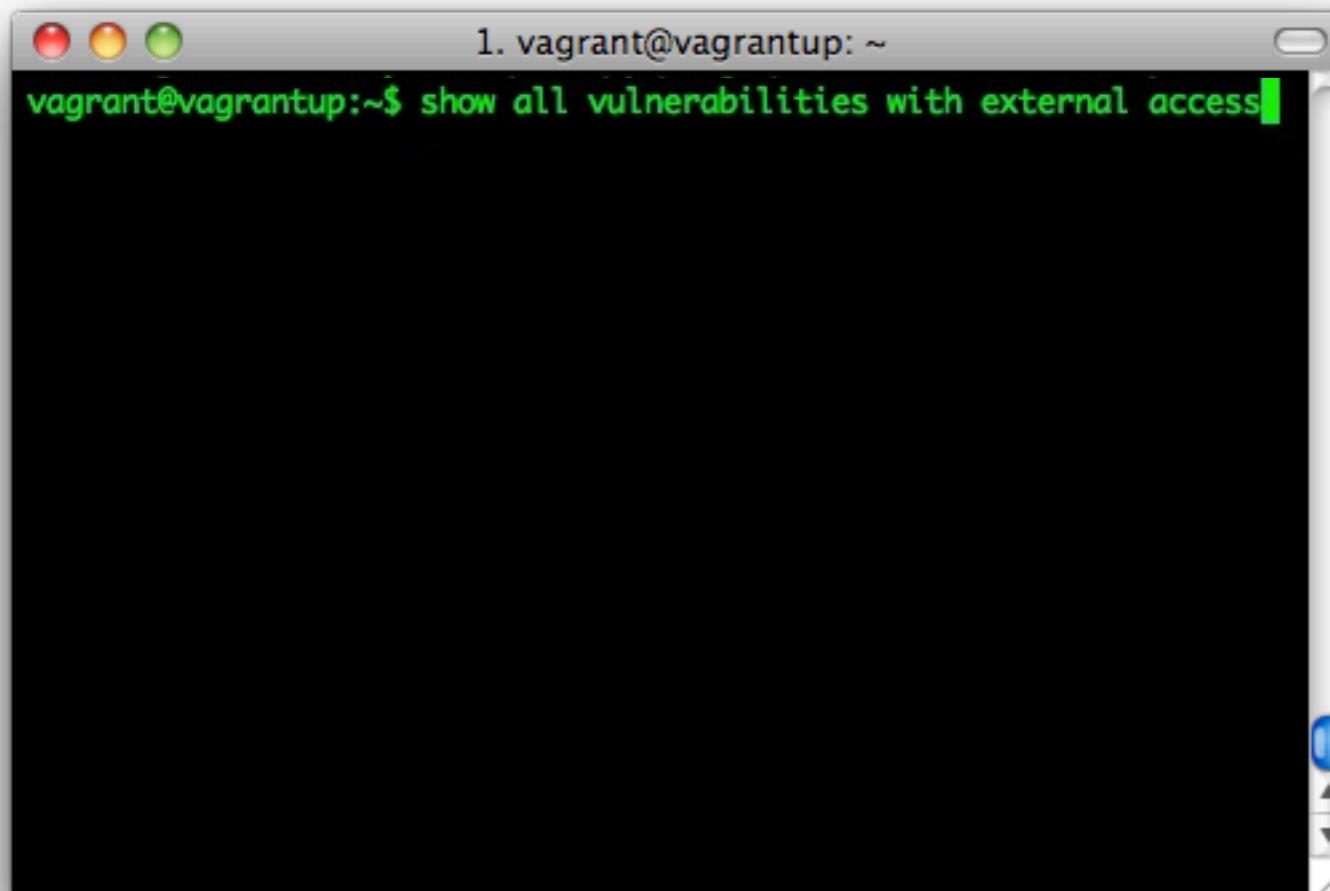
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

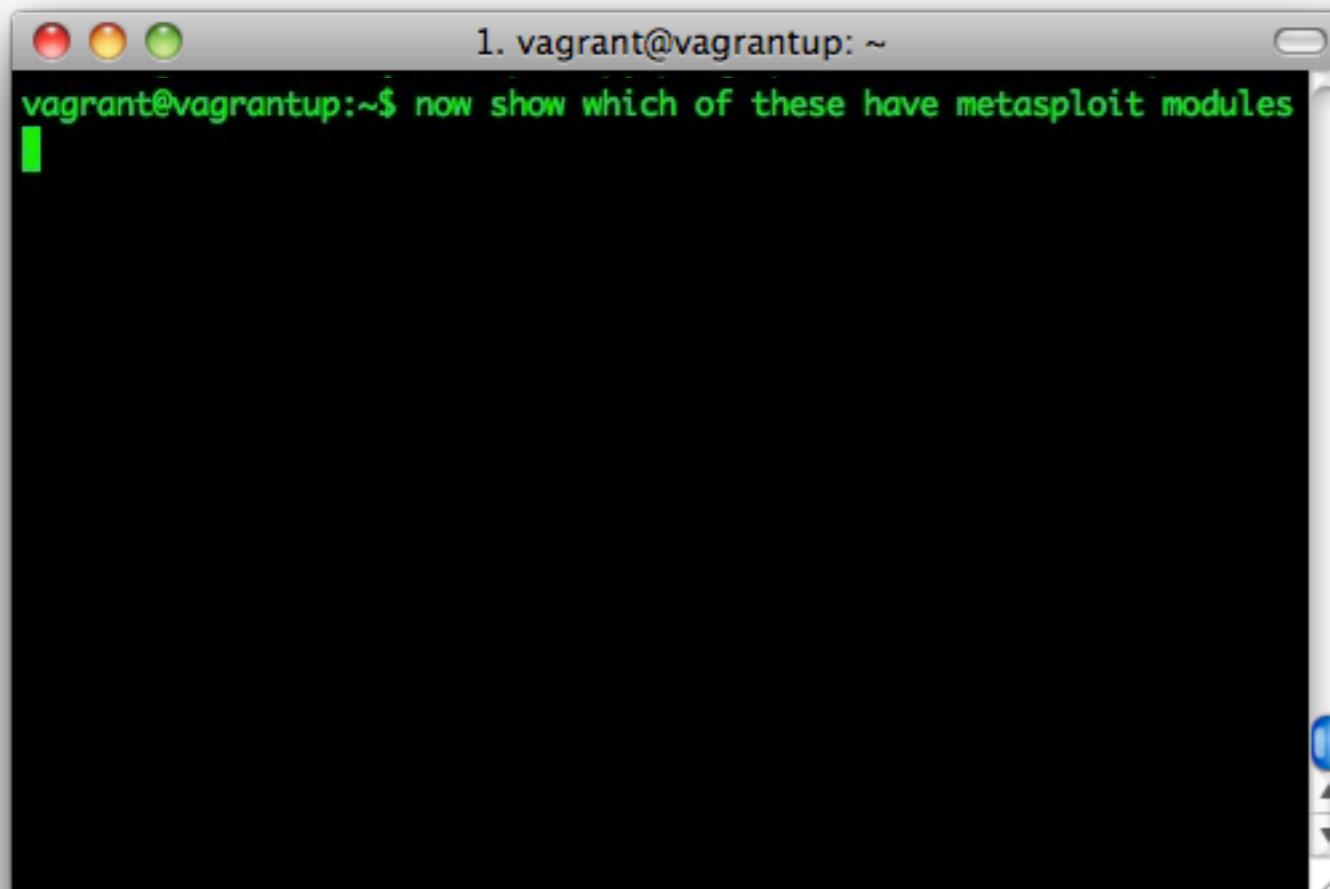


1. vagrant@vagrantup: ~
vagrant@vagrantup:~\$ show all vulnerabilities with external access



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

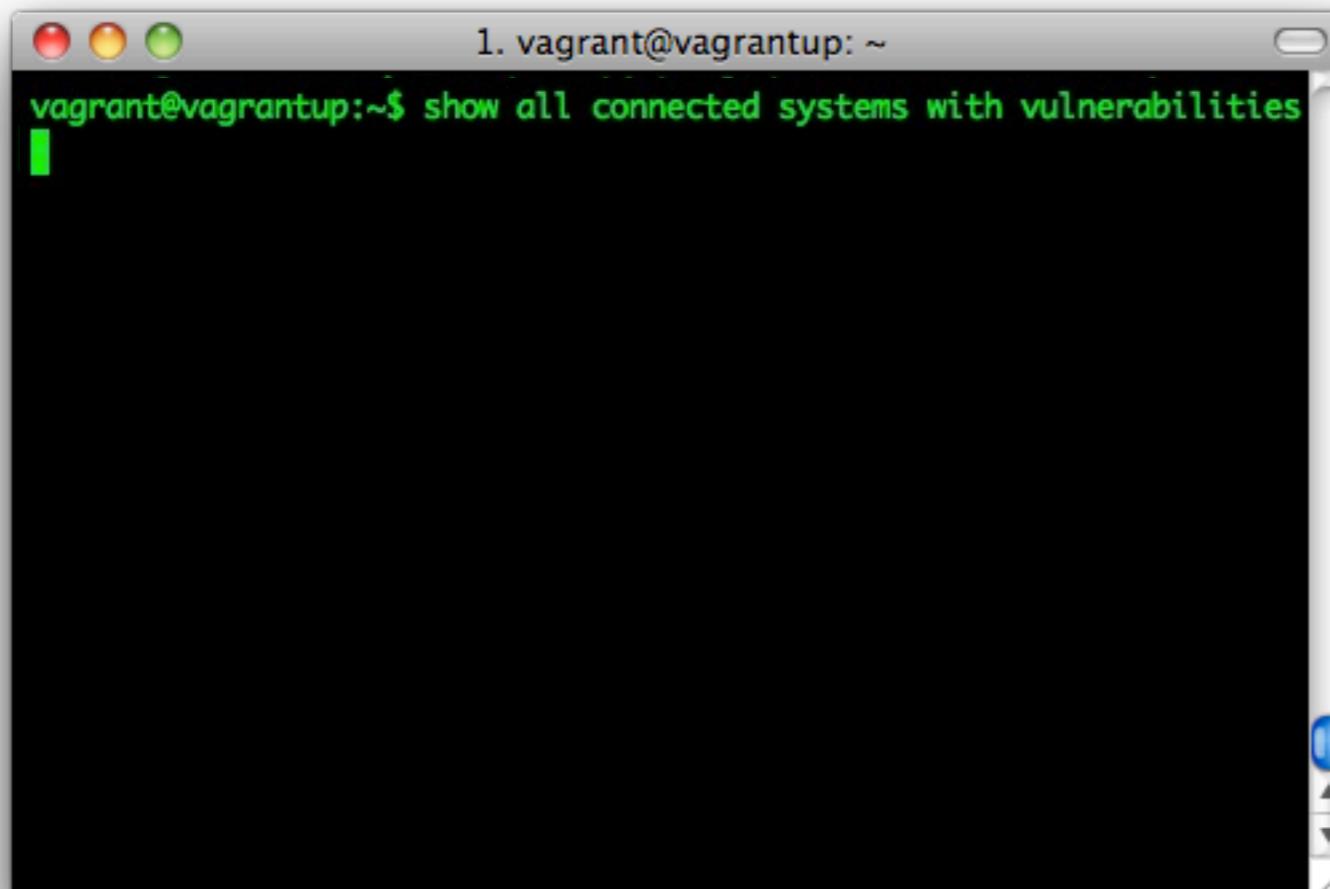


1. vagrant@vagrantup: ~
vagrant@vagrantup:~\$ now show which of these have metasploit modules



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

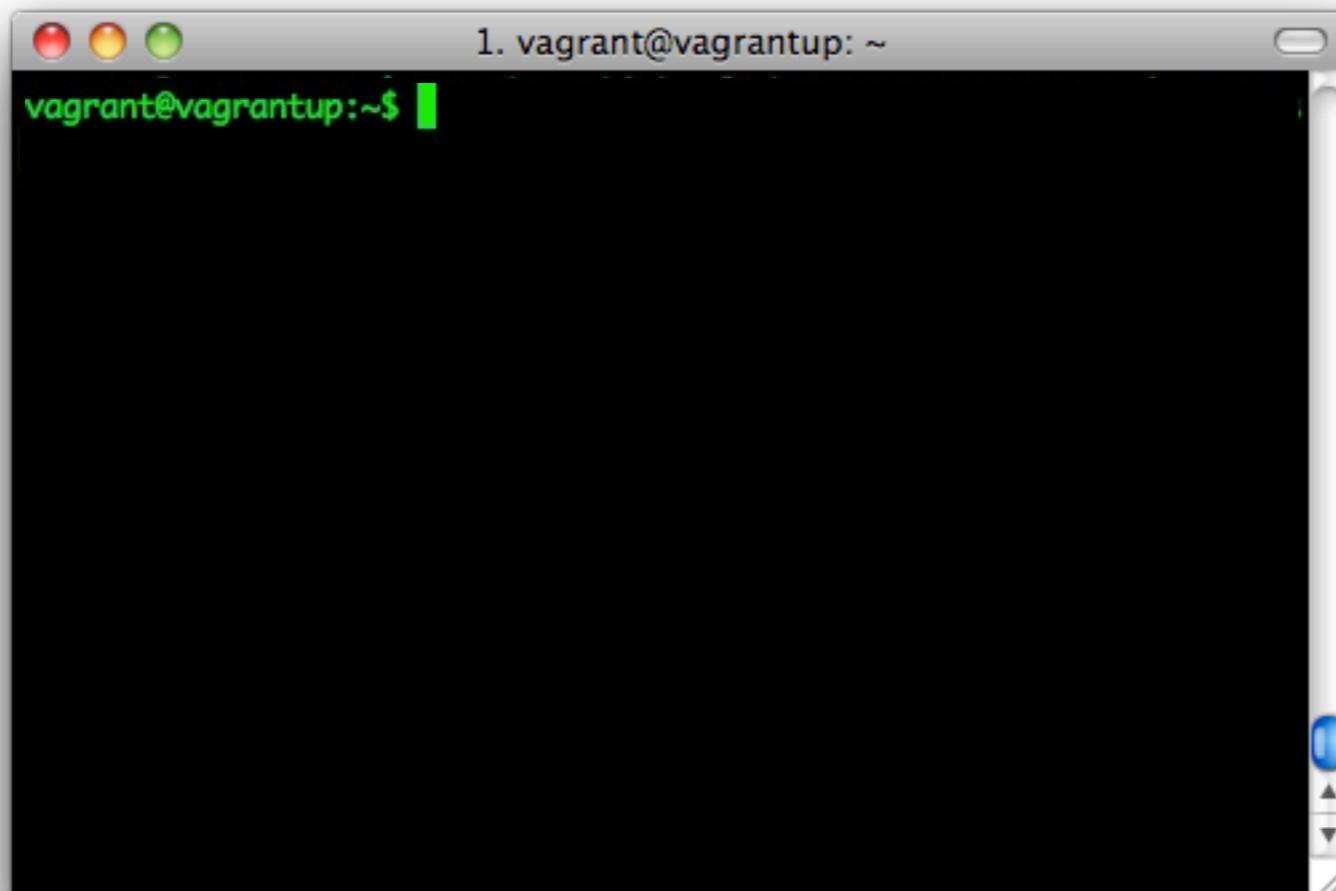


1. vagrant@vagrantup: ~
vagrant@vagrantup:~\$ show all connected systems with vulnerabilities



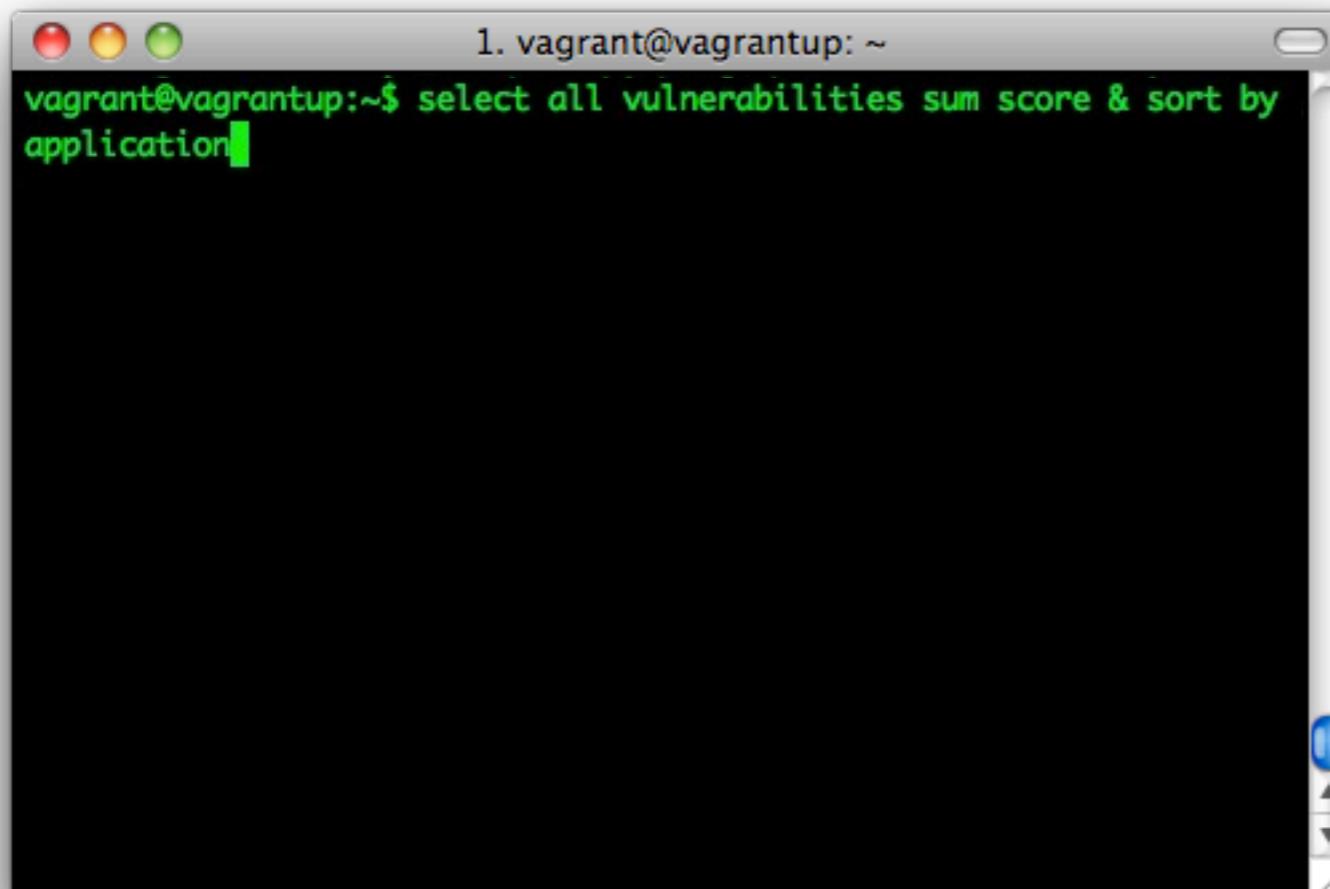
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information

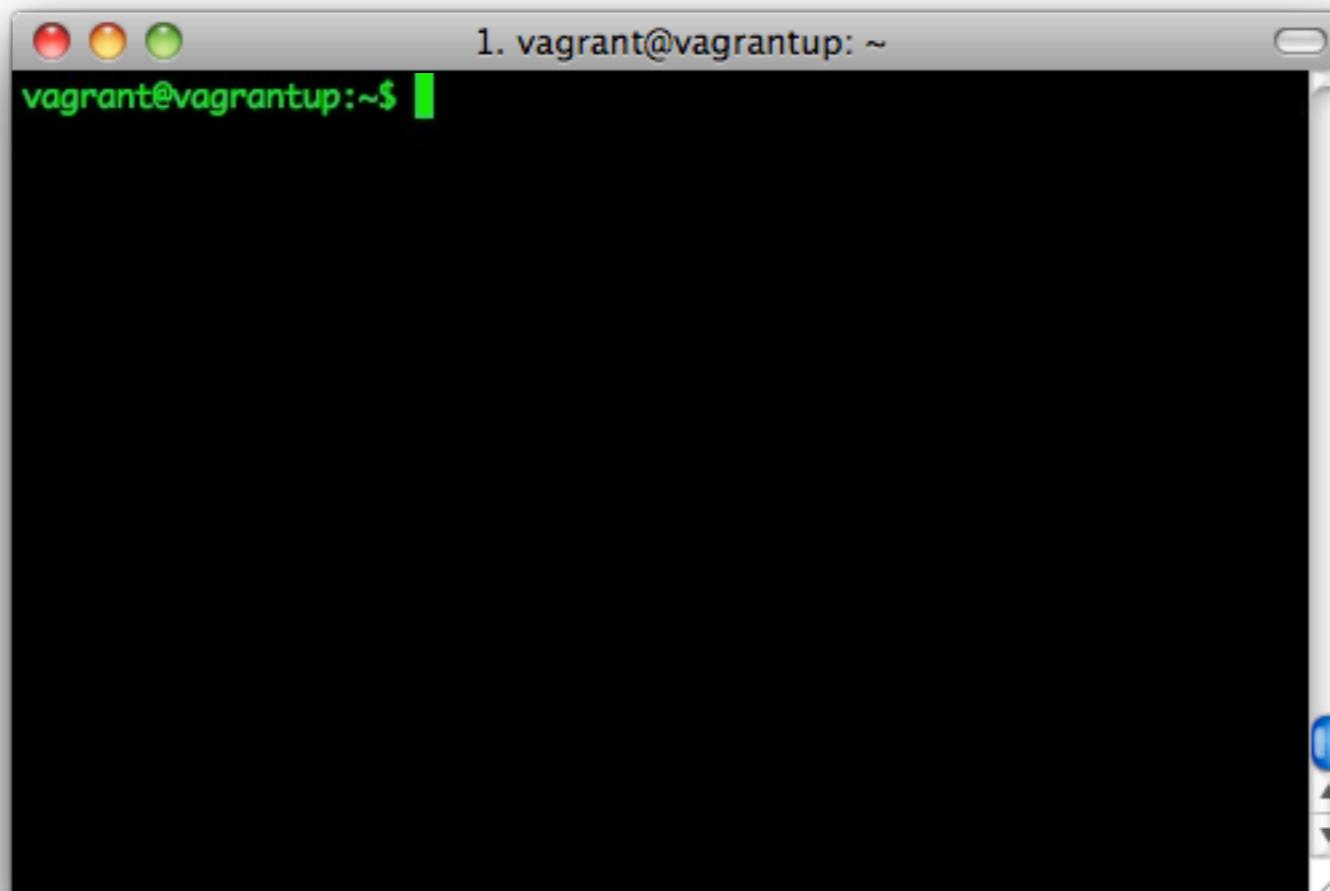


1. vagrant@vagrantup: ~
vagrant@vagrantup:~\$ select all vulnerabilities sum score & sort by application



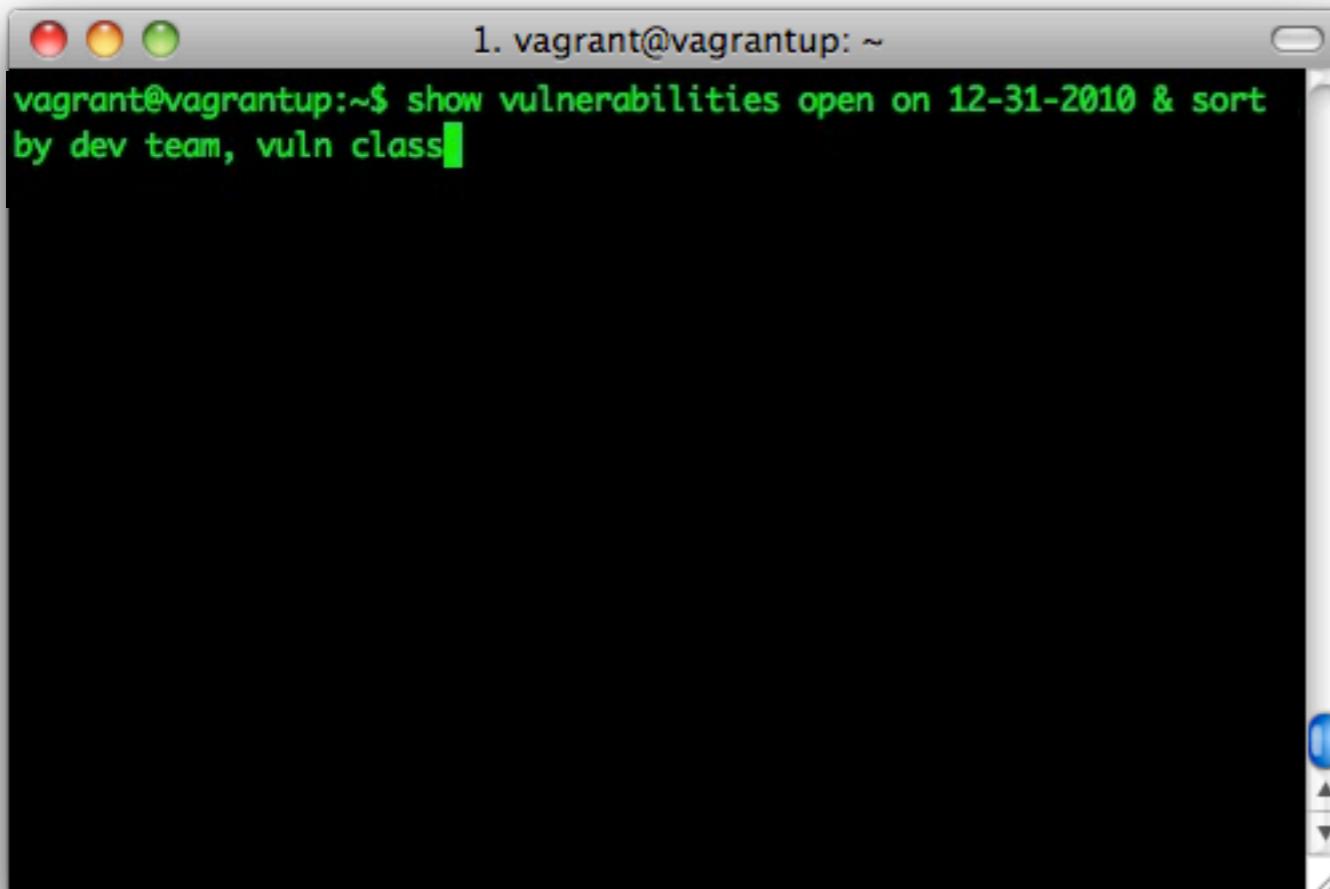
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



1. vagrant@vagrantup: ~

```
vagrant@vagrantup:~$ show vulnerabilities open on 12-31-2010 & sort
by dev team, vuln class
```



Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



```
1. vagrant@vagrantup: ~
vagrant@vagrantup:~$ show open vulnerabilities created after 2-1-201
1 & sort by dev team, vuln class
```





The Twitter Poll



@Beaker

Christofer Hoff

RT [@ebellis](#): . @securitytwits what non-security tools are you using for security purposes? < I carry this-here big stick.

10 May via [Tweetie for Mac](#) [Favorite](#) [Retweet](#) [Reply](#)



@thrashor

C Hammond-Thrasher

@ebellis: . @securitytwits what non-security tools are you using for security purposes >> perl

10 May via [Twitter for iPhone](#) [Favorite](#) [Retweet](#) [Reply](#)



@digininja

Robin

@ebellis ssh - port forwarding, tftp, MSSQL console, web browser, ftp/vnc/rdp clients

10 May via [Seesmic twirl](#) [Favorite](#) [Retweet](#) [Reply](#)



@robtdew

Rob Dewhurst

@ebellis grep, awk, sed, gnuplot

10 May via [web](#) [Favorite](#) [Retweet](#) [Reply](#)



@dfranke

Daniel Franke

@securitytwits @ebellis For quick tests, Firebug's DOM-editing features make it a nice lazy alternative to Burp Proxy.

10 May via [web](#) [Favorite](#) [Retweet](#) [Reply](#)



@innismir

Ben Jackson

@ebellis perl :)



@Clint326

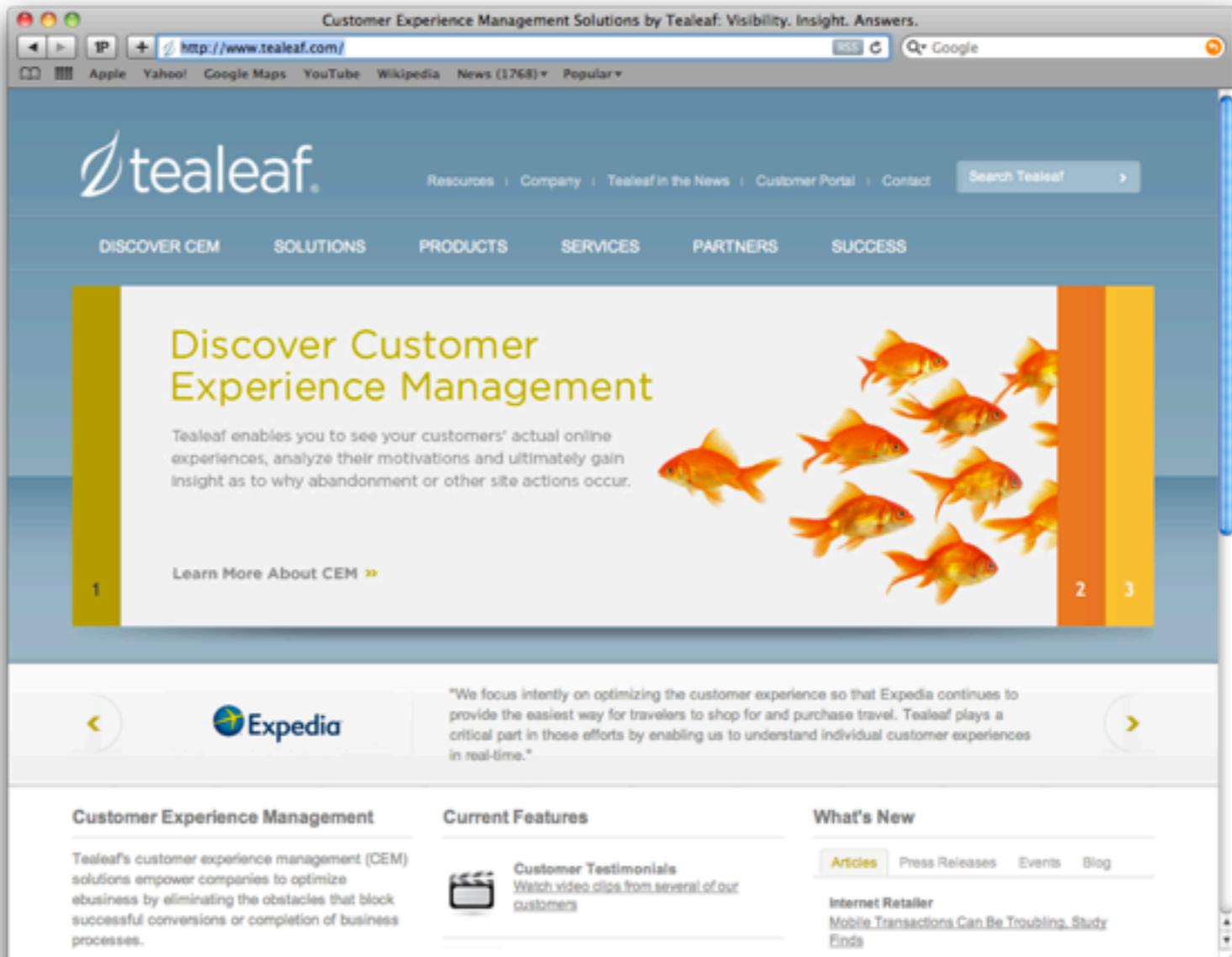
Clint Laskowski

@ebellis @securitytwits I use Text Filter (<http://www.musetips.com/text-filter.html>) all the time for search logs, lists, etc. Very fast.

10 May via [web](#) [Favorite](#) [Retweet](#) [Reply](#)

My Favorite Non-Sec Tools

■ TeaLeaf



The screenshot shows the homepage of the Tealeaf website. The header reads "Customer Experience Management Solutions by Tealeaf: Visibility. Insight. Answers." with a sub-header "http://www.tealeaf.com/". The main navigation menu includes "Resources", "Company", "Tealeaf in the News", "Customer Portal", and "Contact". A search bar is also present. Below the header, a main banner features the Tealeaf logo and the text "Discover Customer Experience Management". It includes a subtext: "Tealeaf enables you to see your customers' actual online experiences, analyze their motivations and ultimately gain insight as to why abandonment or other site actions occur." A call-to-action button "Learn More About CEM >" is visible. To the right of the text is a graphic of several goldfish swimming. The footer contains a testimonial from Expedia: "We focus intently on optimizing the customer experience so that Expedia continues to provide the easiest way for travelers to shop for and purchase travel. Tealeaf plays a critical part in those efforts by enabling us to understand individual customer experiences in real-time." Below the testimonial, there are sections for "Customer Experience Management", "Current Features", and "What's New".

■ GreenPlum

■ Ruby



Resources Referenced

Verizon DBIR <http://www.verizonbusiness.com/dbir/>

VERIS Framework <https://www2.icsalabs.com/veris/>

Denim Group - Real Cost of S/W Remediation

<http://www.slideshare.net/denimgroup/real-cost-of-software-remediation>

DataLoss DB <http://datalossdb.org/>

TrustWave Global Security Report

<https://www.trustwave.com/GSR>

Symantec DeepSight <https://tms.symantec.com/>

WASC Web App Security Stats
<http://projects.webappsec.org/w/page/13246989/Web-Application-Security-Statistics>

FS-ISAC <http://www.fsisac.com/>

SANS Internet Storm Center
<http://isc.sans.org/>

XForce <http://xforce.iss.net/>



Q & A

follow us

the blog

<http://blog.honeyapps.com/>

twitter

@honeyapps

@ebellis

