honeyapps Inc

The Search For Intelligent Life
OWASP Philadelphia

honeyapps Inc

Or.....

The 4 Stages of Security Intelligence

honeyapps Inc

Nice To Meet You

About Me

CoFounder HoneyApps

Former CISO Orbitz

Contributing Author
Beautiful Security

CSO Magazine/Online Author

HoneyApps

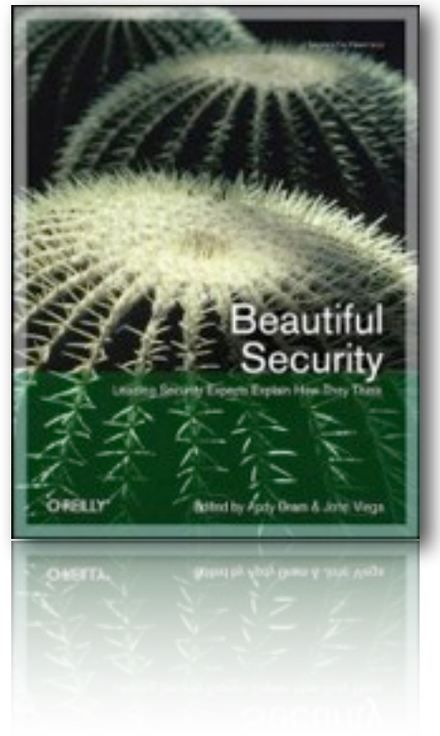
Vulnerability Management as a Service

16 Hot Startups - eWeek

3 Startups to Watch - Information Week

CSO
BUSINESS RISK LEADERSHIP

eWEEK
HOT
STARTUP
2011



InformationWeek
BUSINESS INNOVATION POWERED BY TECHNOLOGY

honeyapps Inc

Stage 1: Ignorance is Bliss

honeyapps Inc

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

honeyapps Inc

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

honeyapps Inc

Stage 4: A New Beginning

Or.....

Using What You Already Have.

honeyapps Inc

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

honeyapps Inc

Vulnerability Management: A Case Study

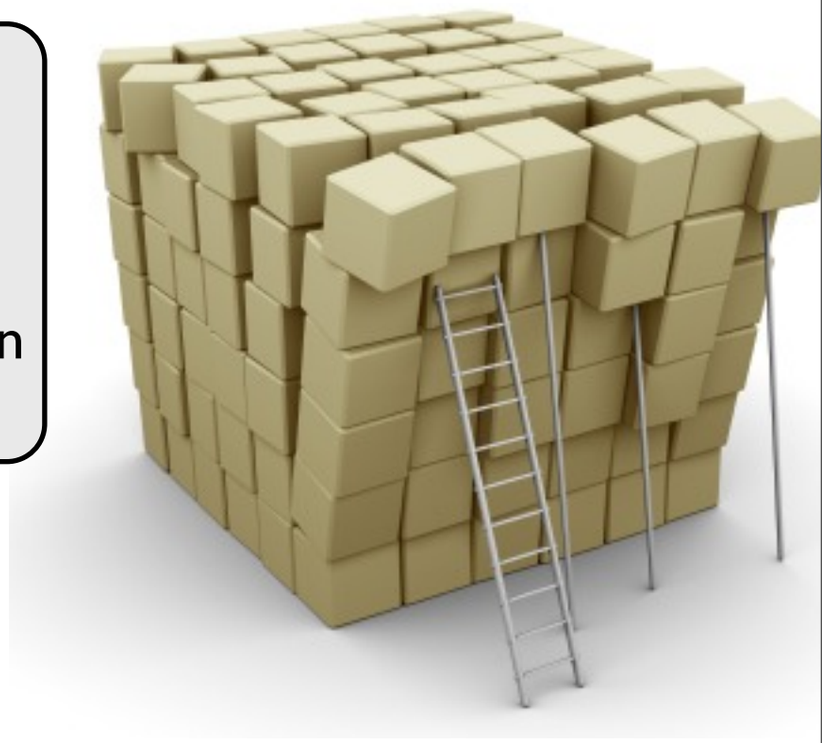
Building the Warehouse

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



honeyapps Inc

Vulnerability Management: A Case Study

Building the Warehouse

WebApp Vulnerability

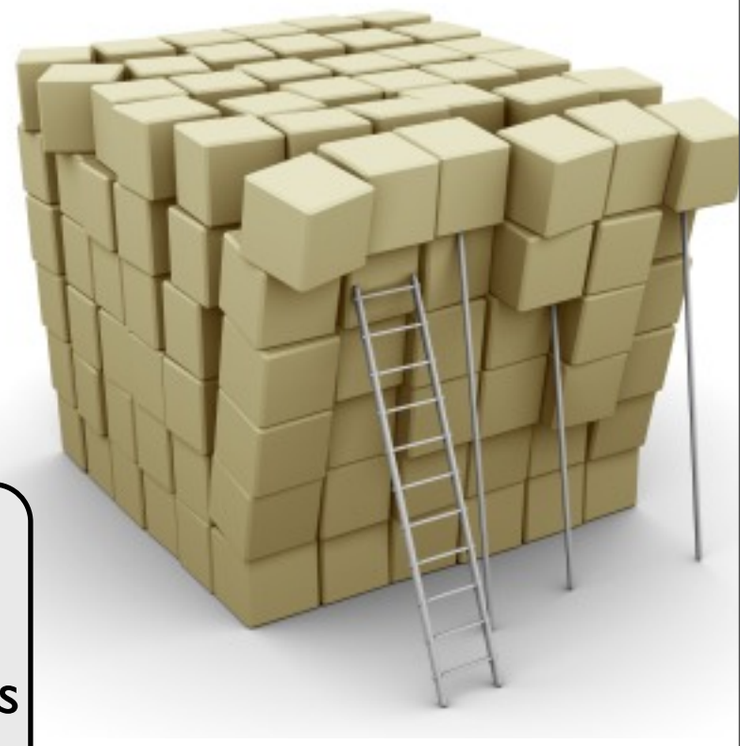
- Type: XSS
- Severity
- Threat
- Subtype: (persistent,reflected,etc)
- Asset URL/URI
- Confirmed?
- Dates Found/Opened
- Dates Closed
- Description
- Attack Parameters

Asset:URL

- Platform / Code
- Web Server Version
- Application Server Version
- Database Version

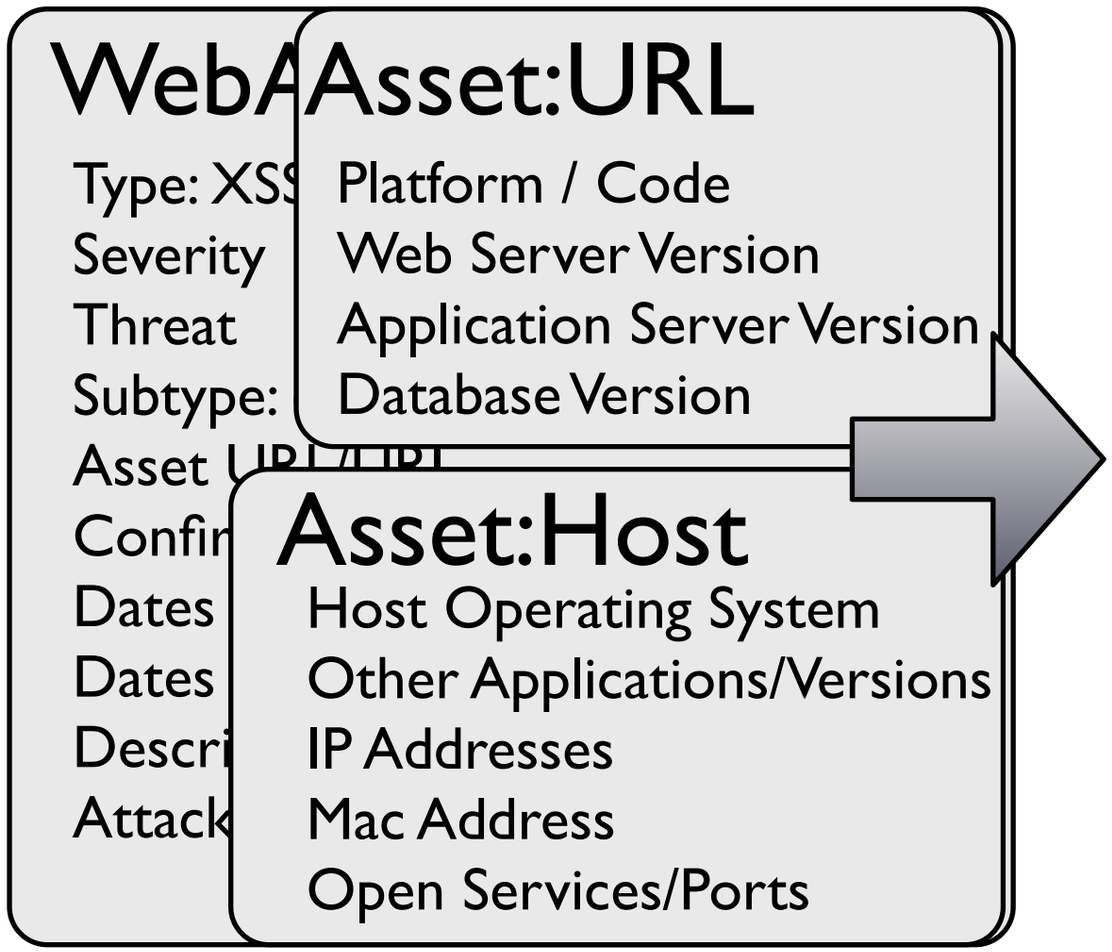
Asset:Host

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



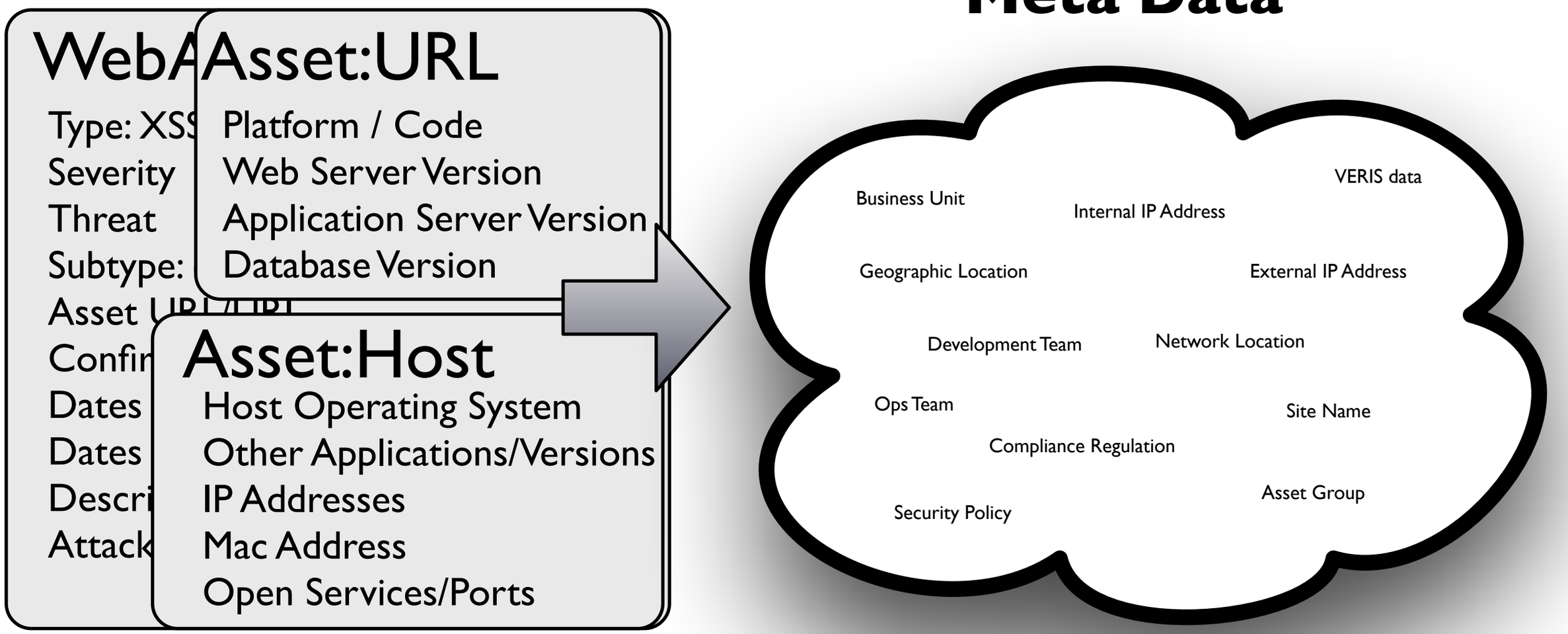
honeyapps Inc

Vulnerability Management: A Case Study



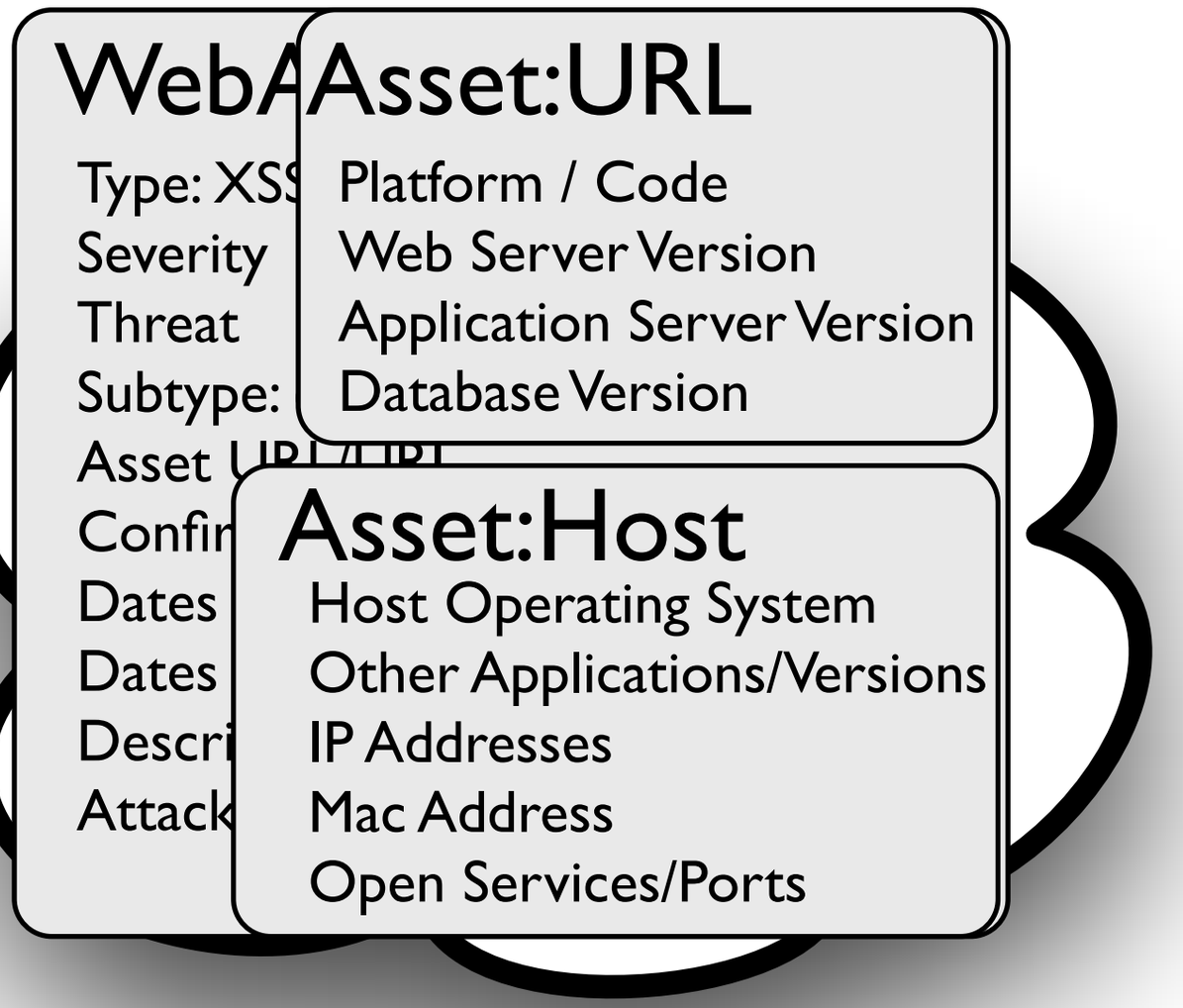
Vulnerability Management: A Case Study

Meta Data

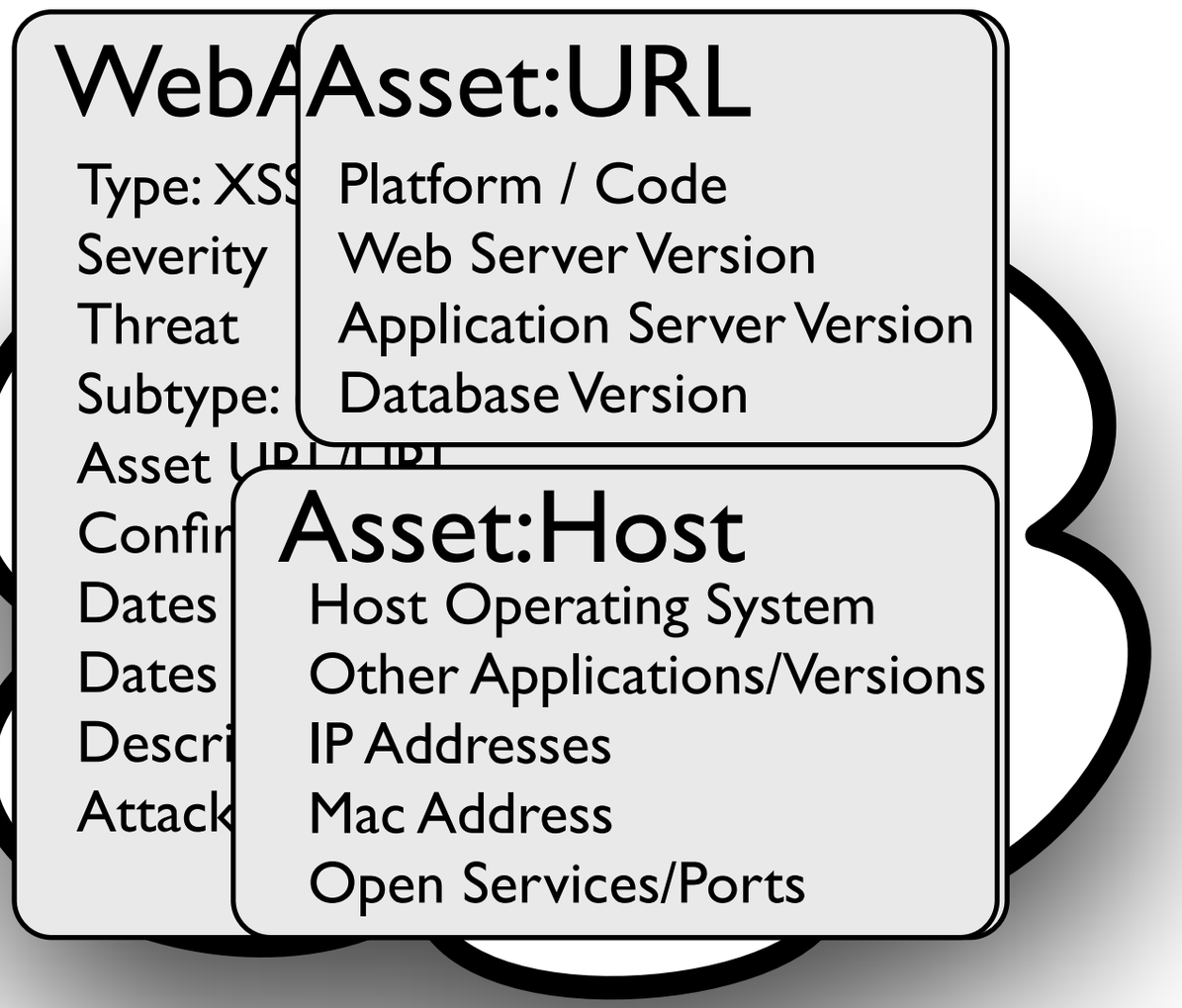


honeyapps Inc

Vulnerability Management: A Case Study



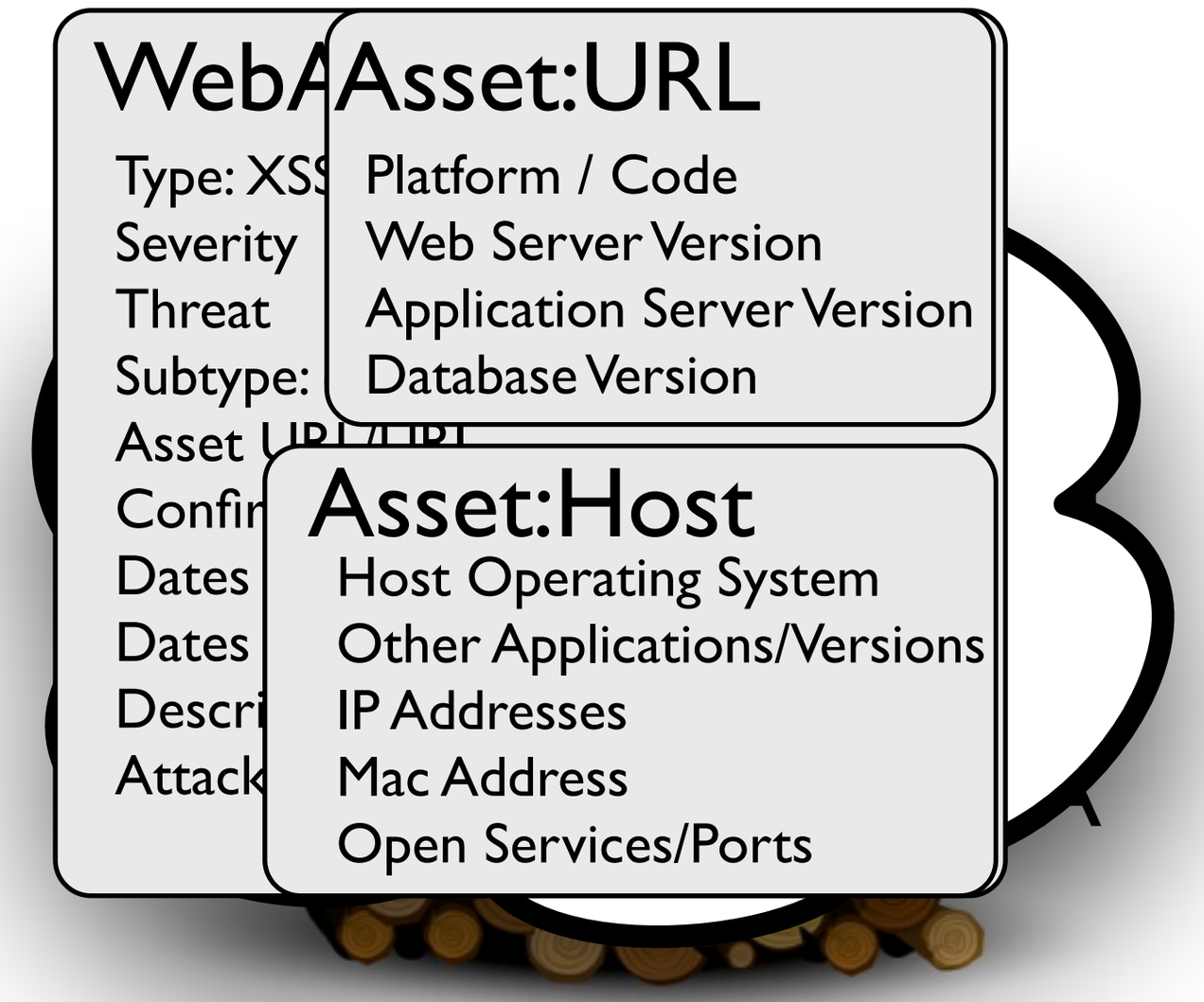
Vulnerability Management: A Case Study



Apply Internal Threat Data

honeyapps Inc

Vulnerability Management: A Case Study



honeyapps Inc

Vulnerability Management: A Case Study

Web A

Type: XSS
Severity
Threat
Subtype:
Asset URL/URI
Confir
Dates
Dates
Descri
Attack

Asset:URL

Platform / Code
Web Server Version
Application Server Version
Database Version

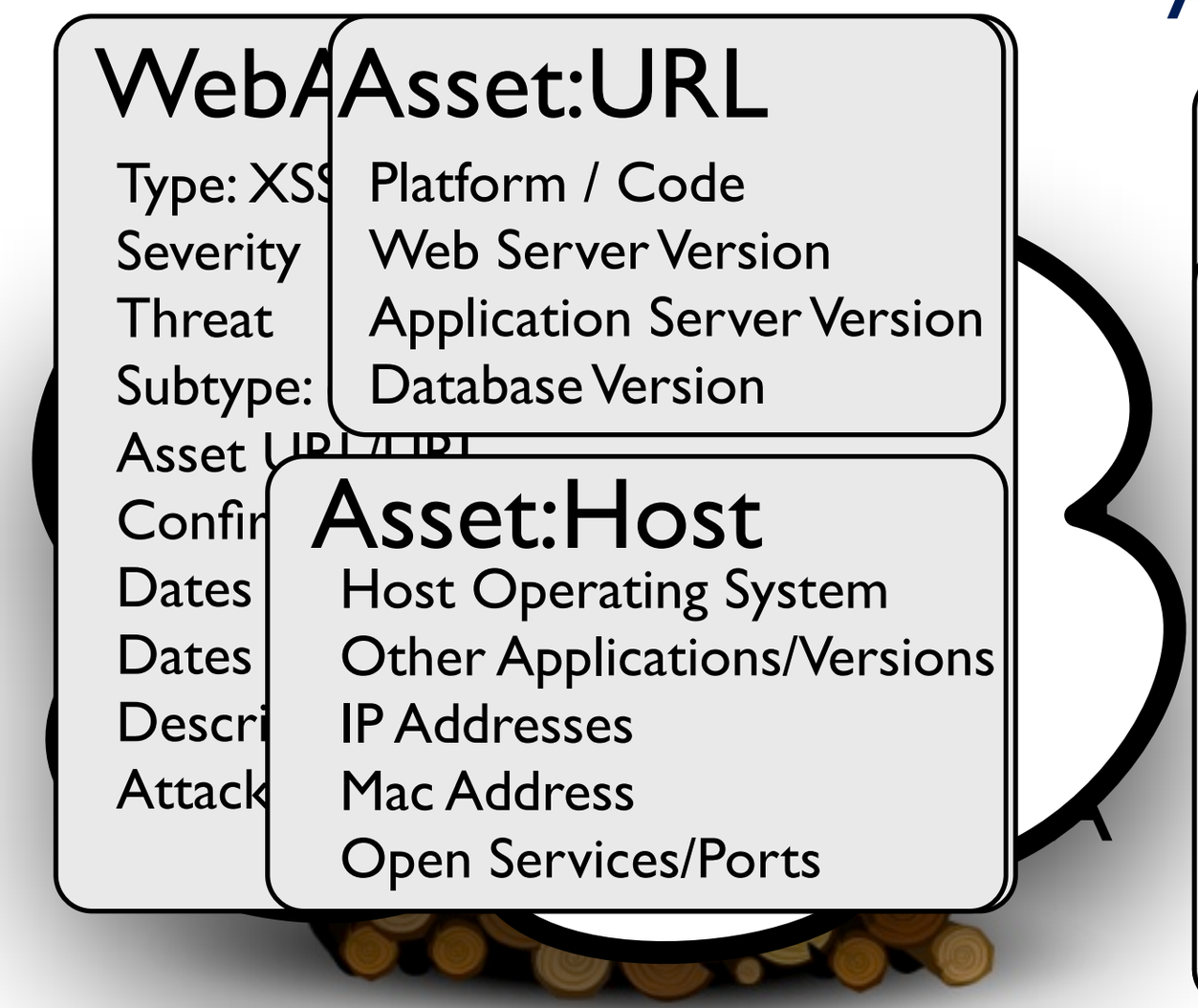
Asset:Host

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

Apply External Threat Data

Vulnerability Management: A Case Study

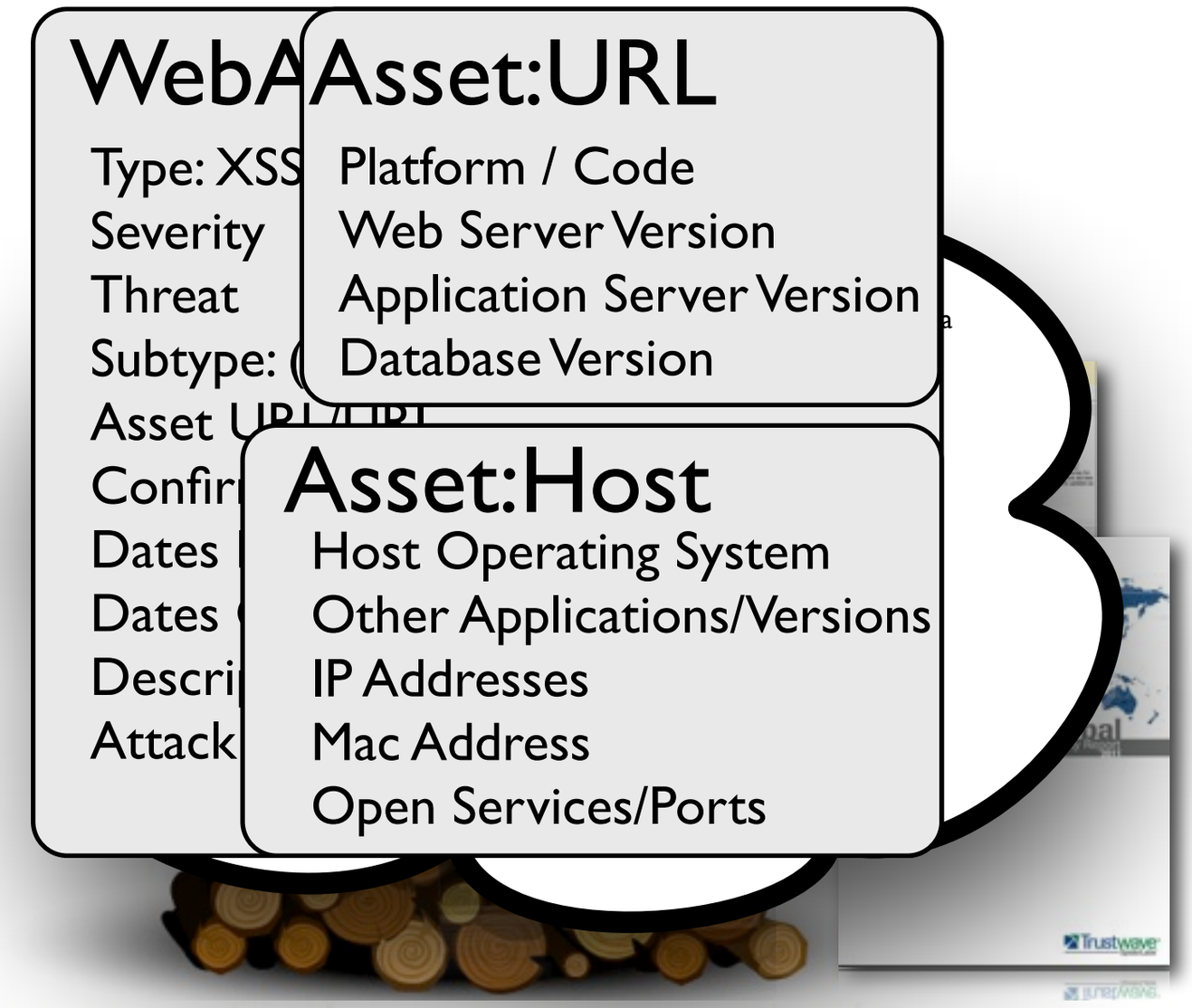
Apply External Threat Data



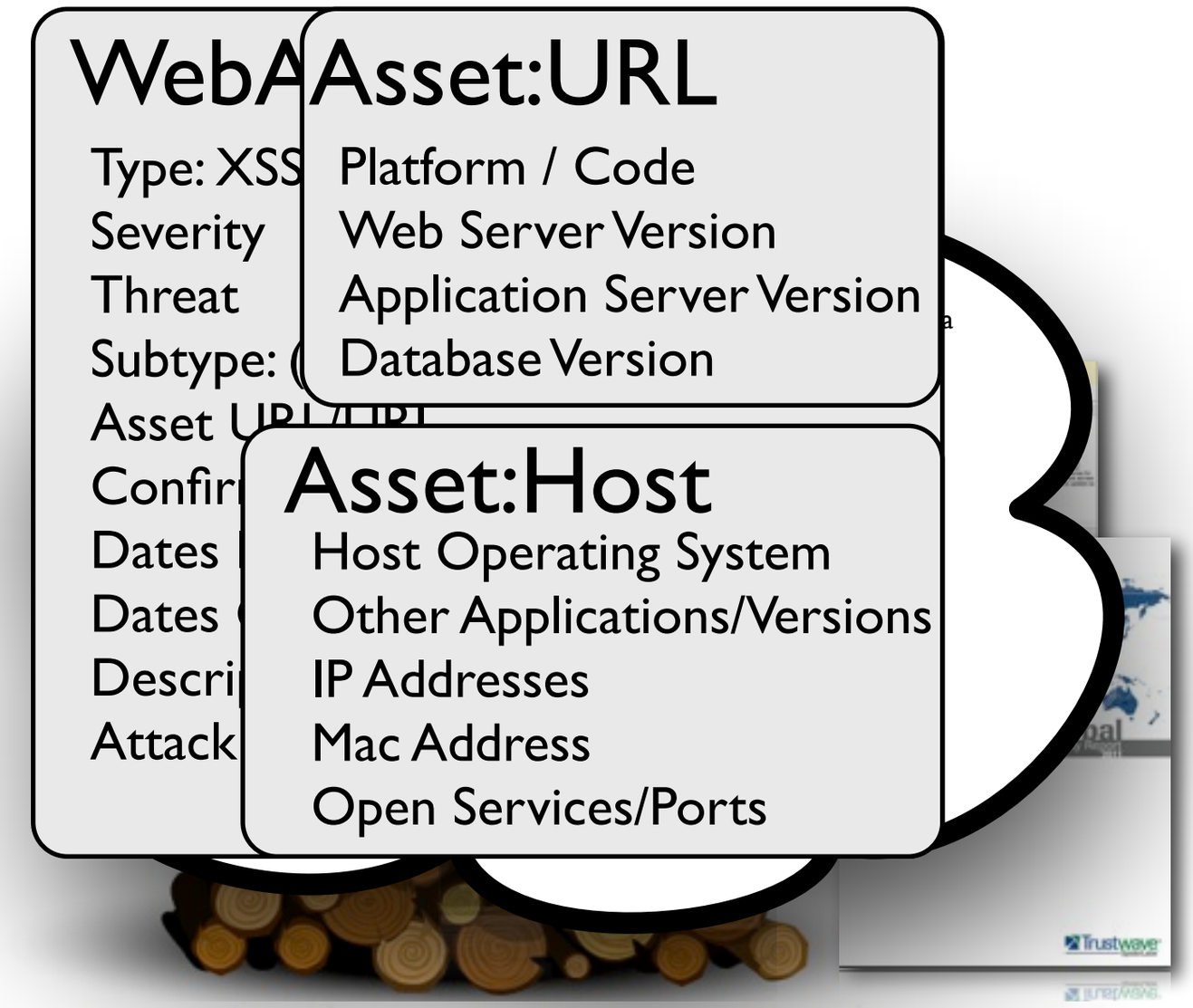
Example Data Sources

- 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

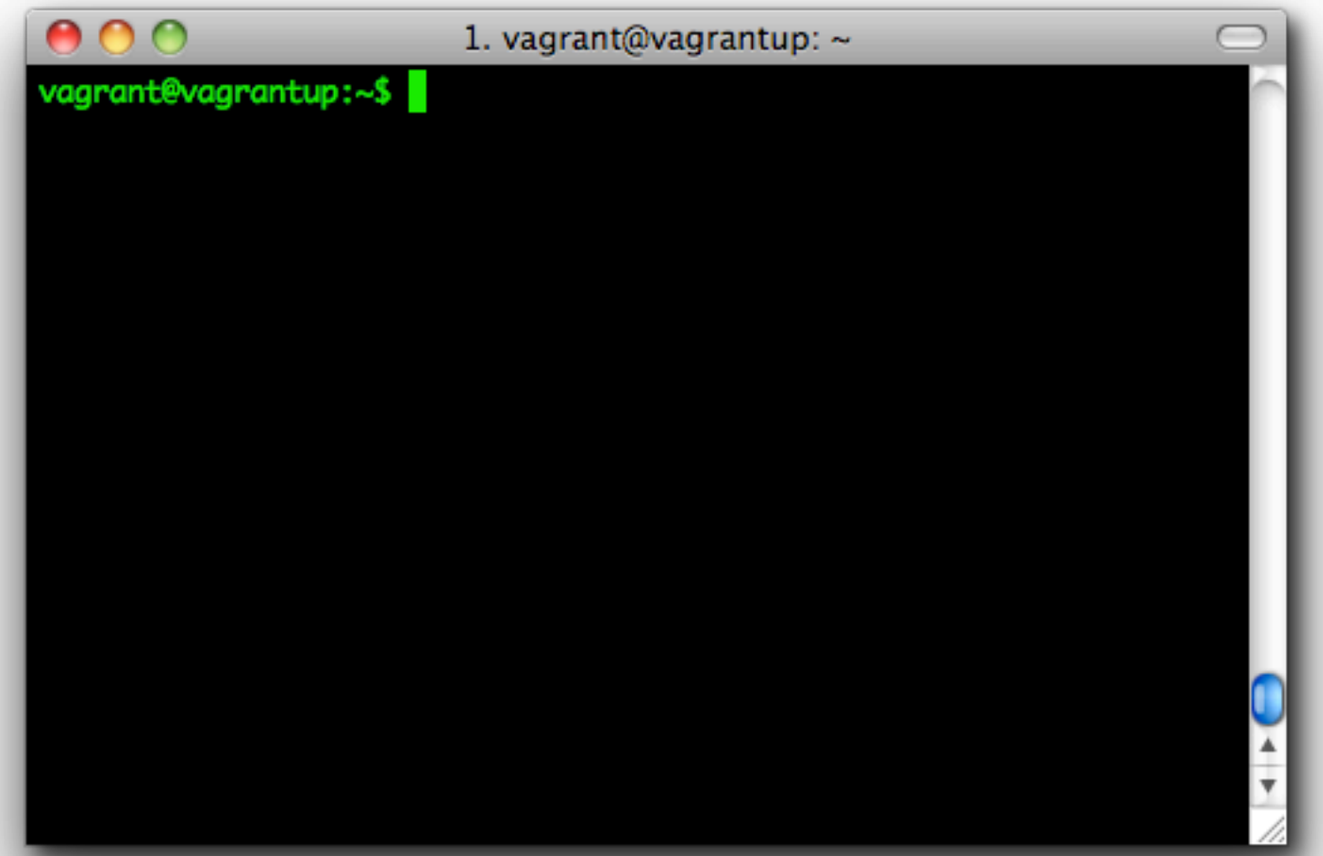


- ☑ Remediation Statistics
- ☑ Internal Bug Tracking Reports
- ☑ Denim Group Remediation Study
- ☑ Build and Development Process

honeyapps Inc

Data Lenses: Views into the Warehouse

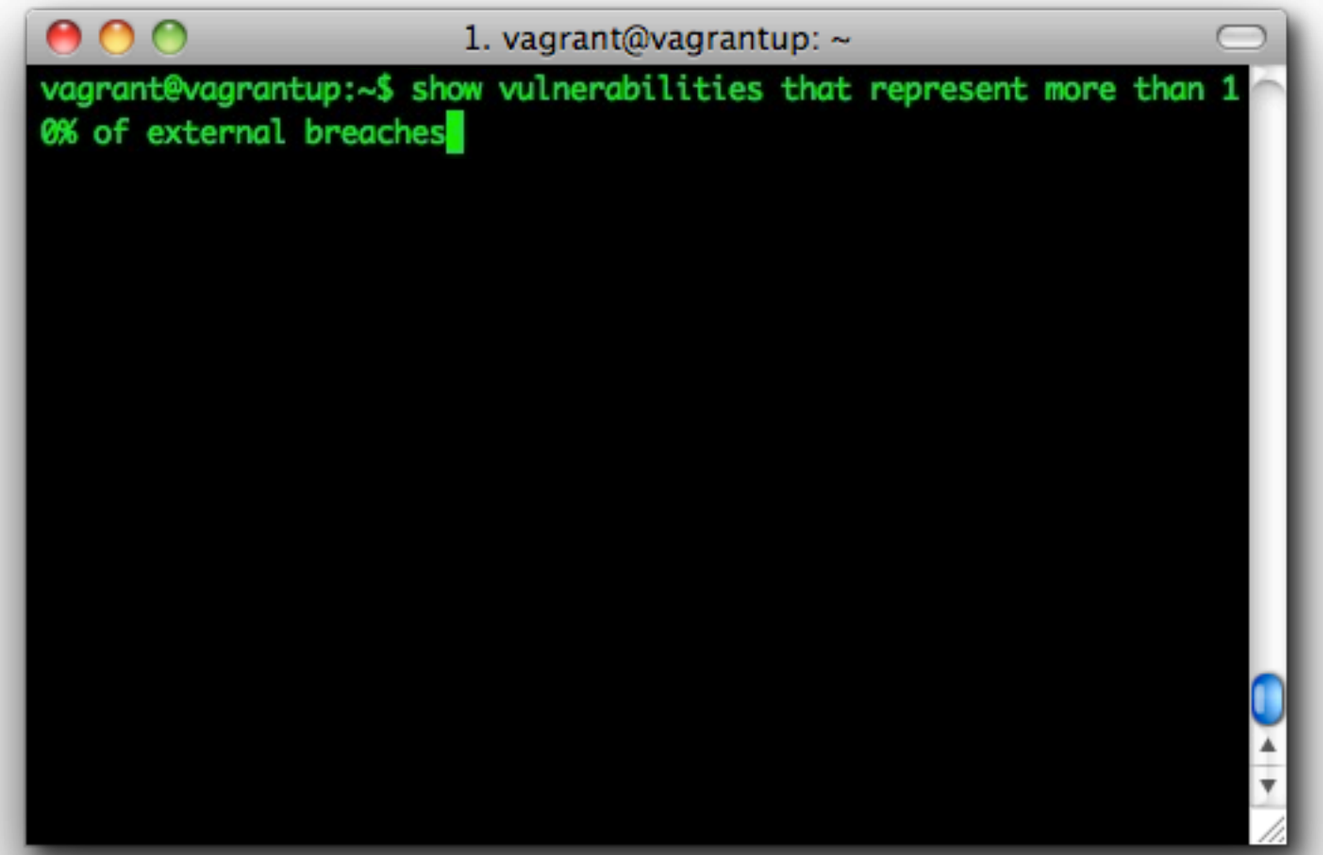
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

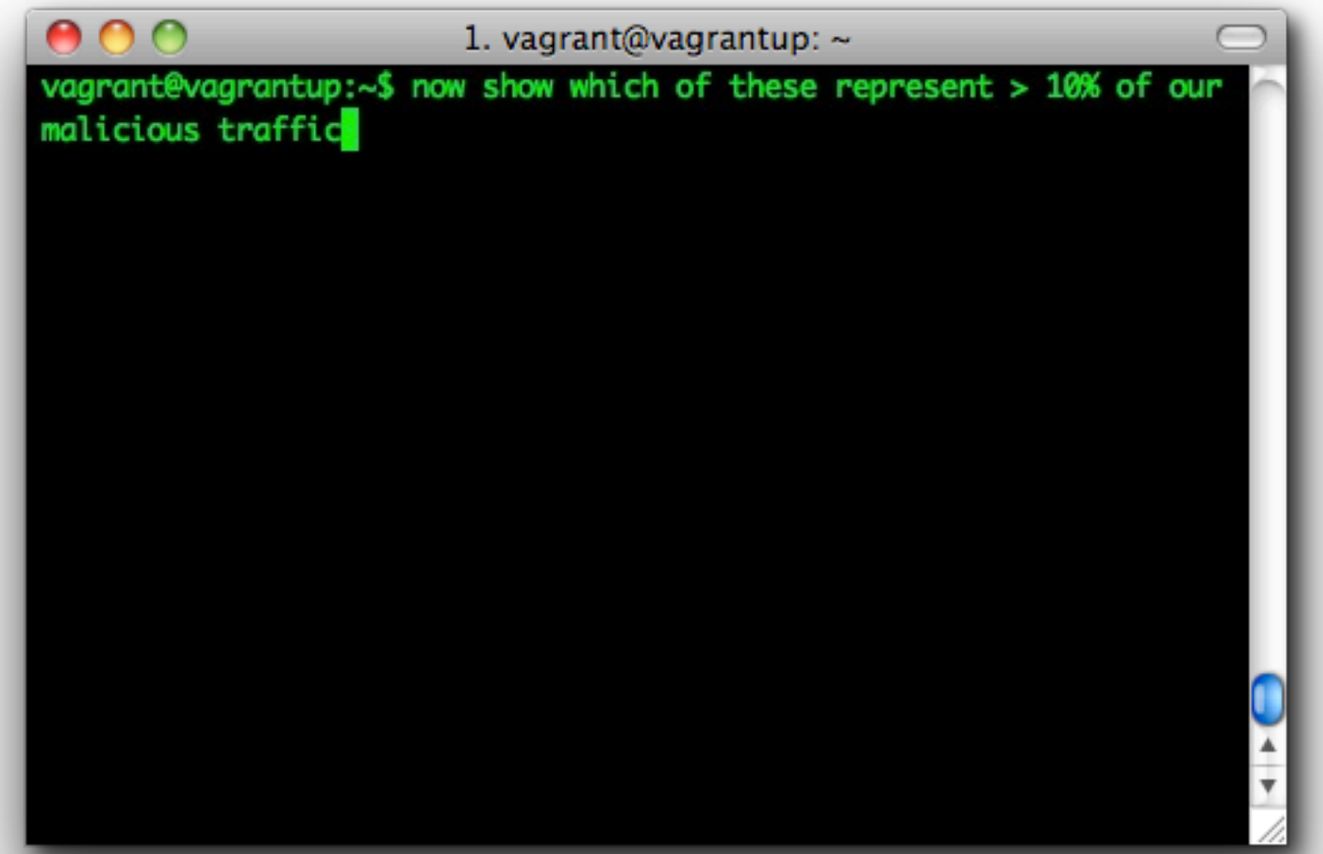
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

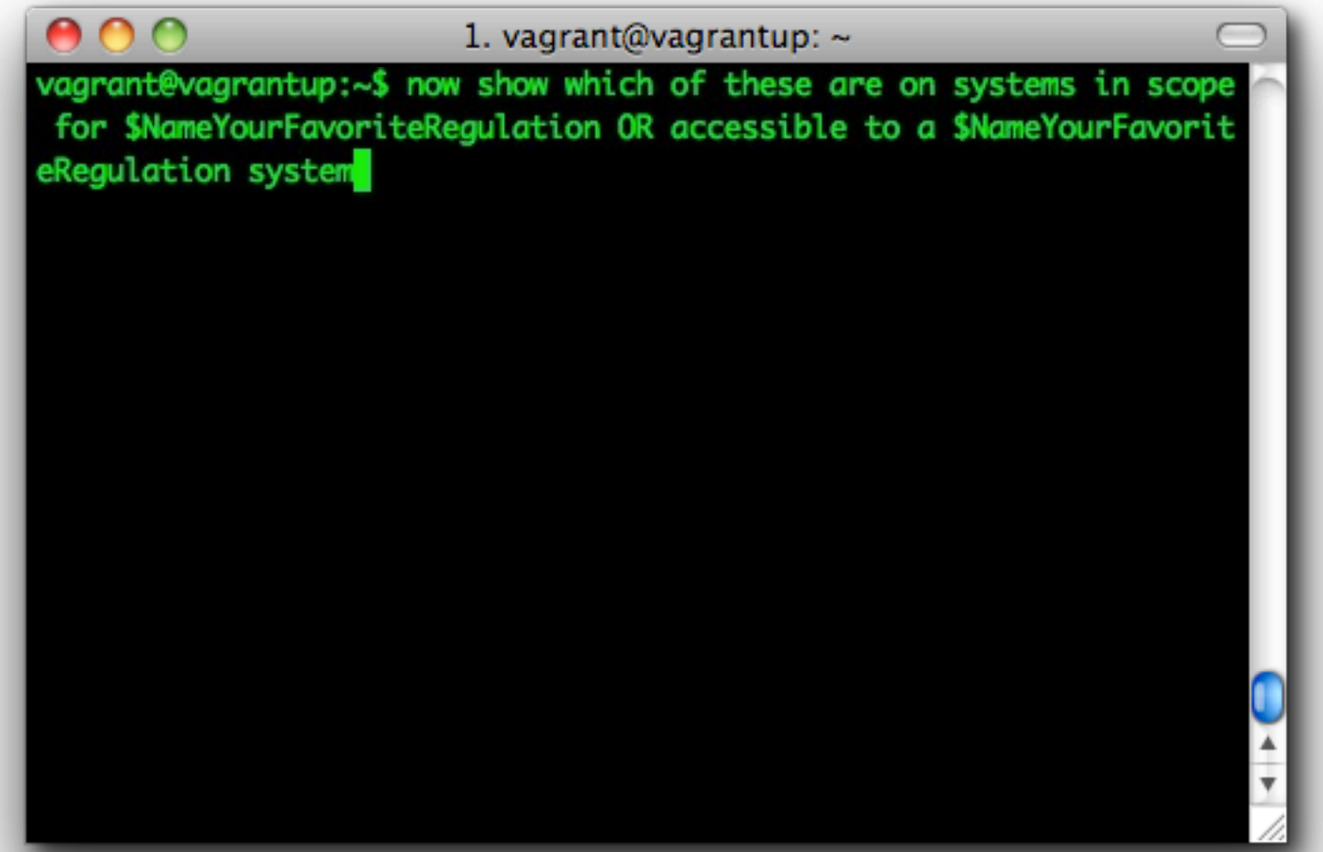
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

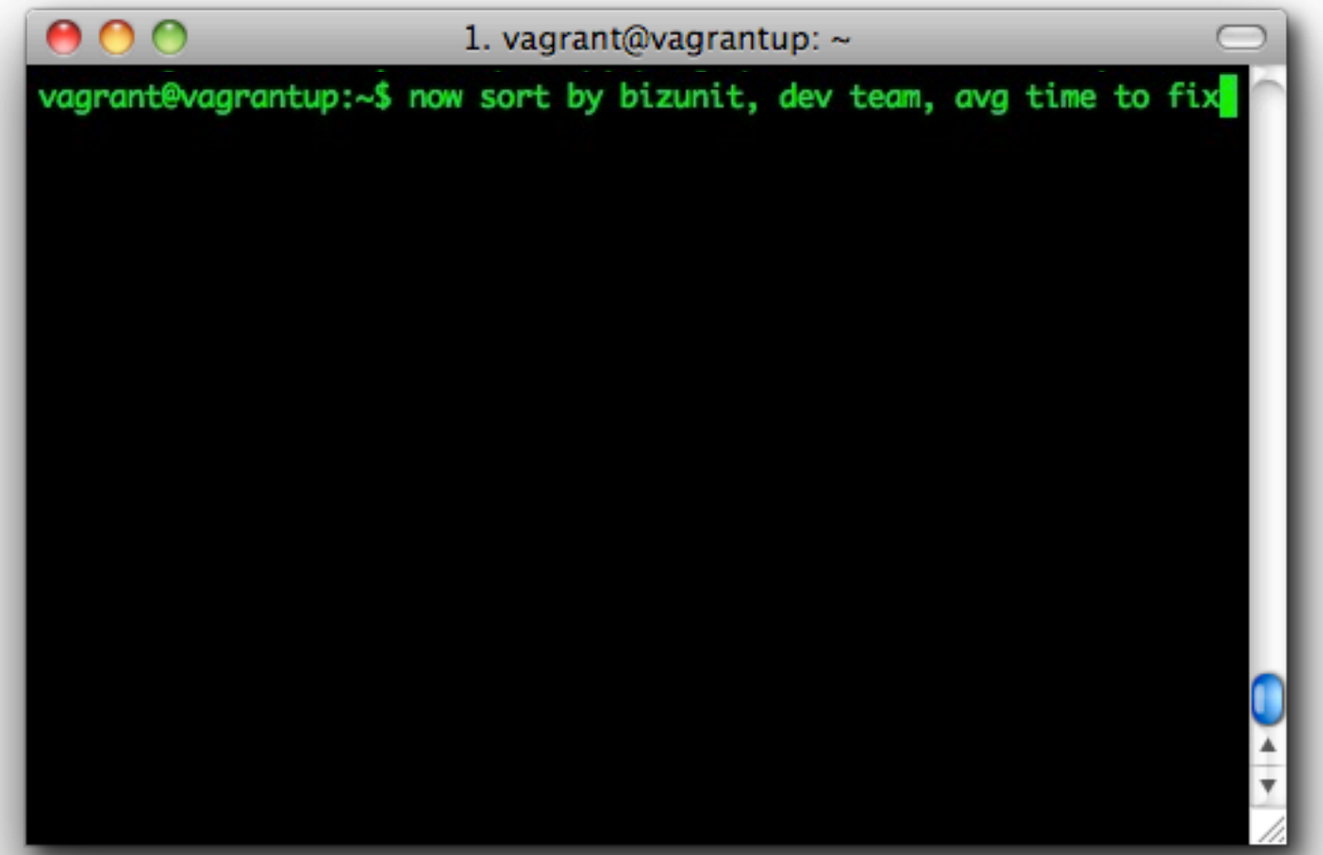
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

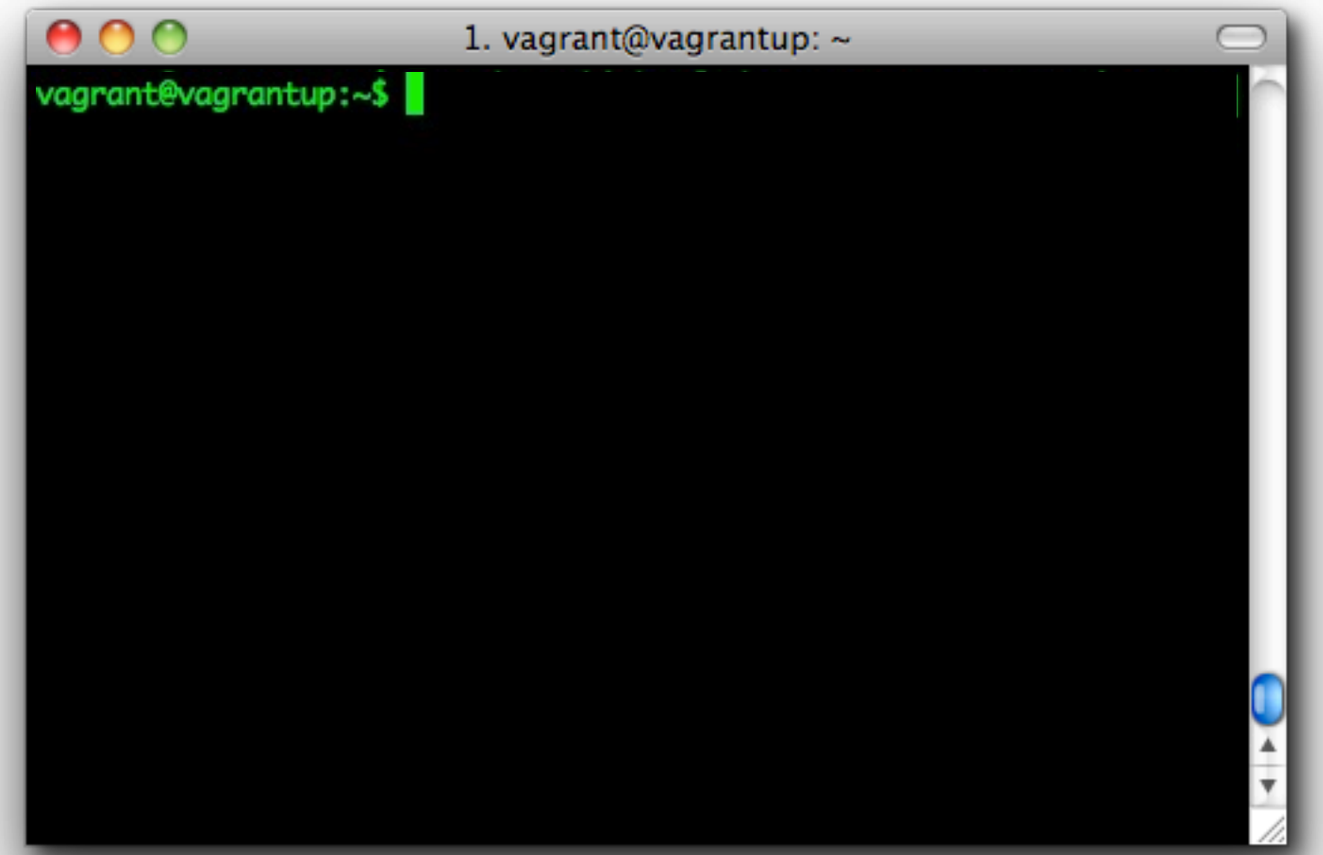
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

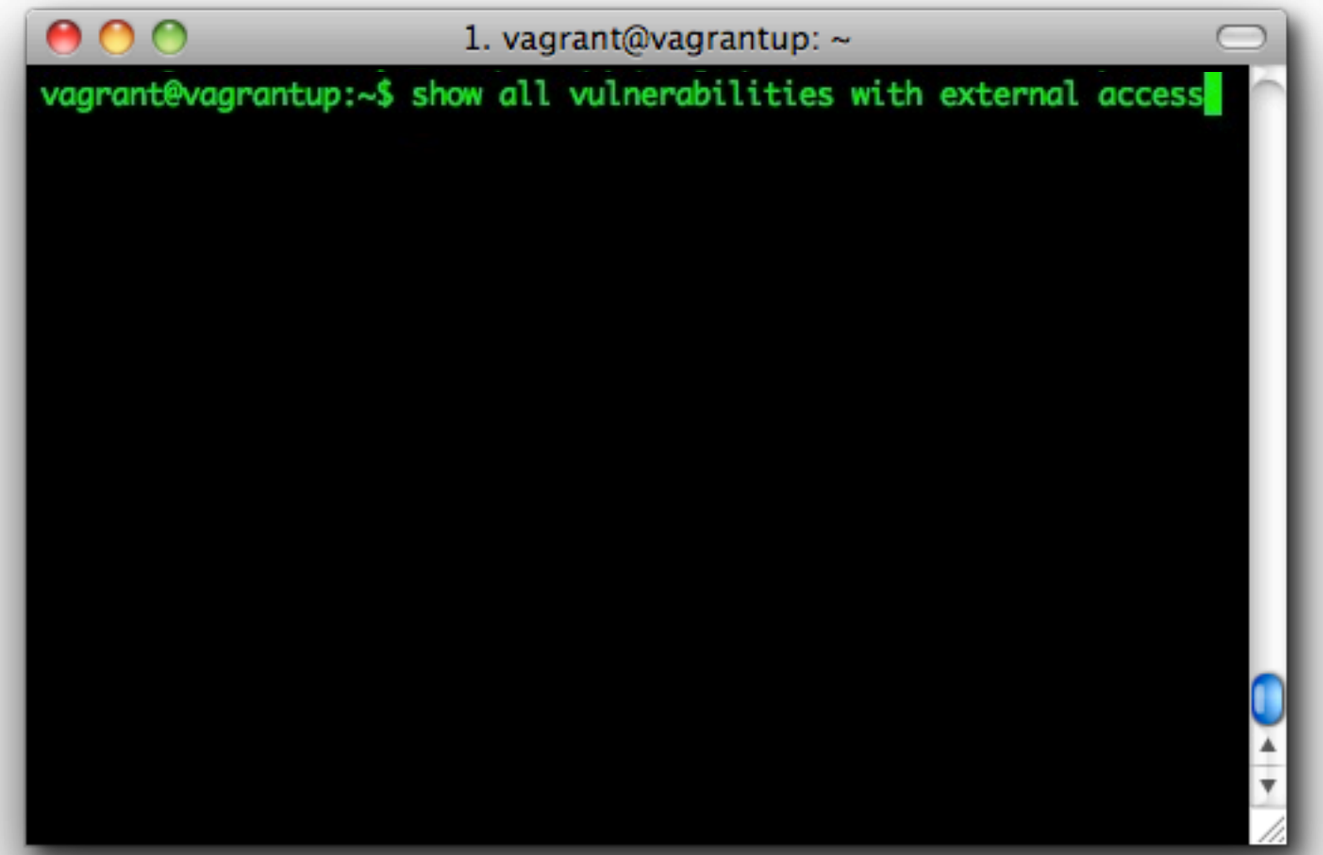
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

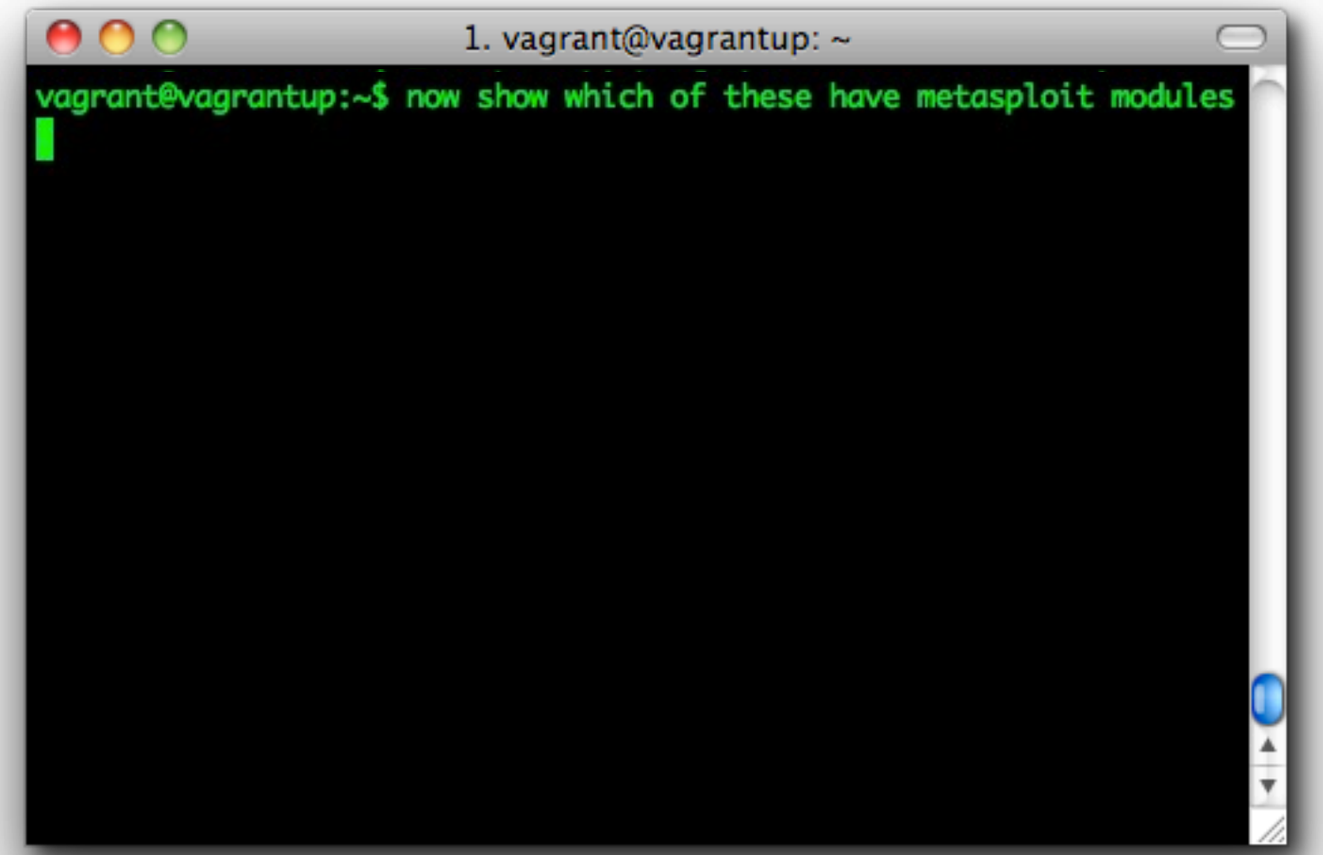
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

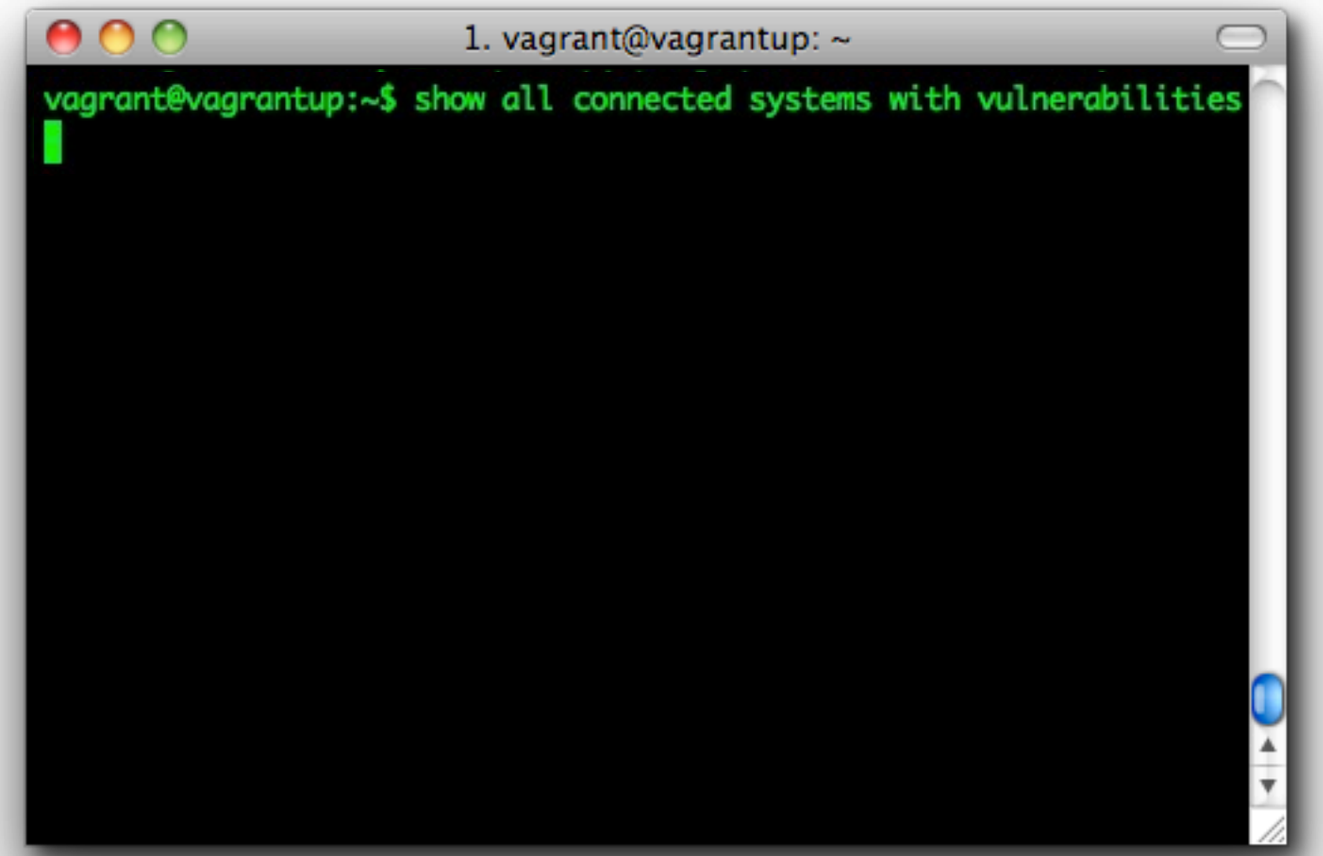
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

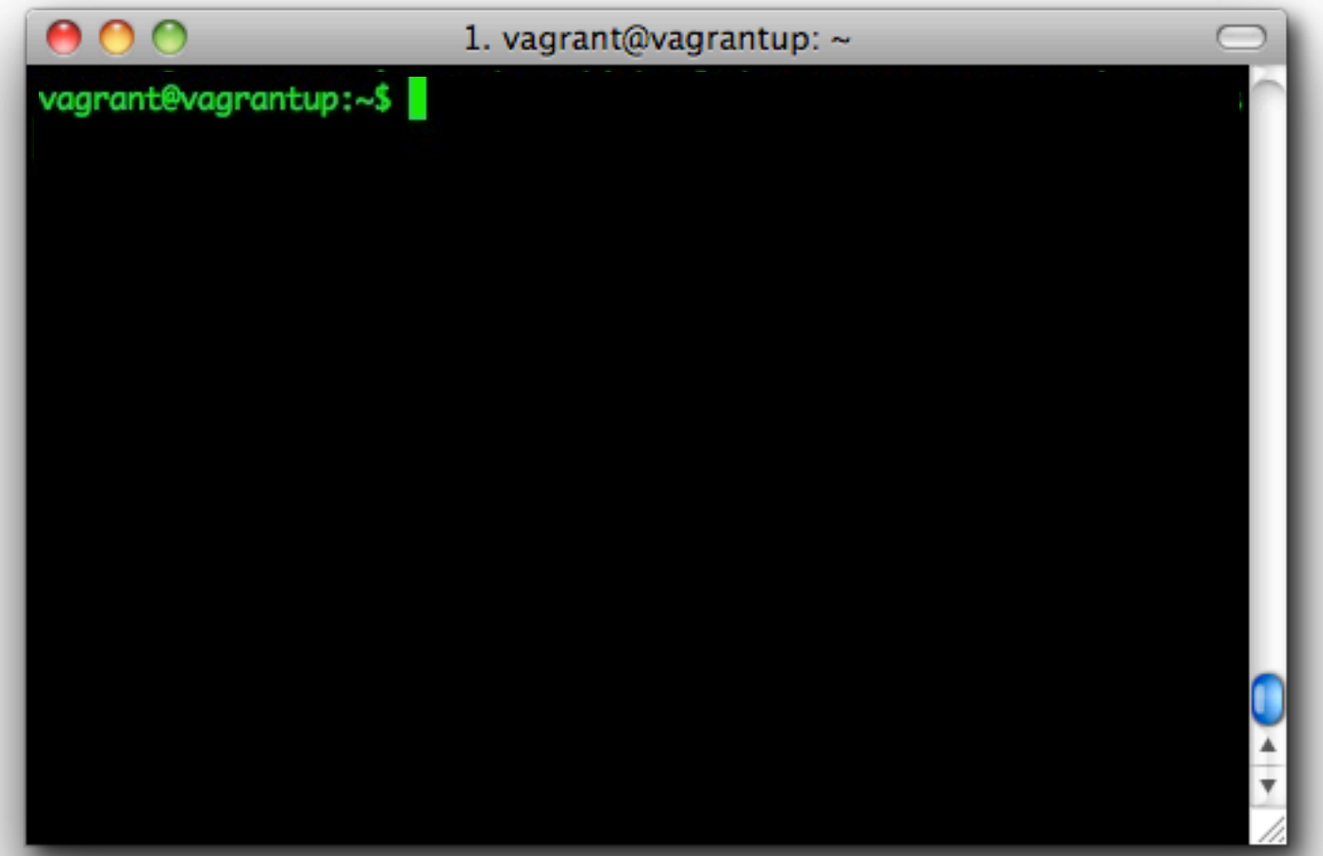
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

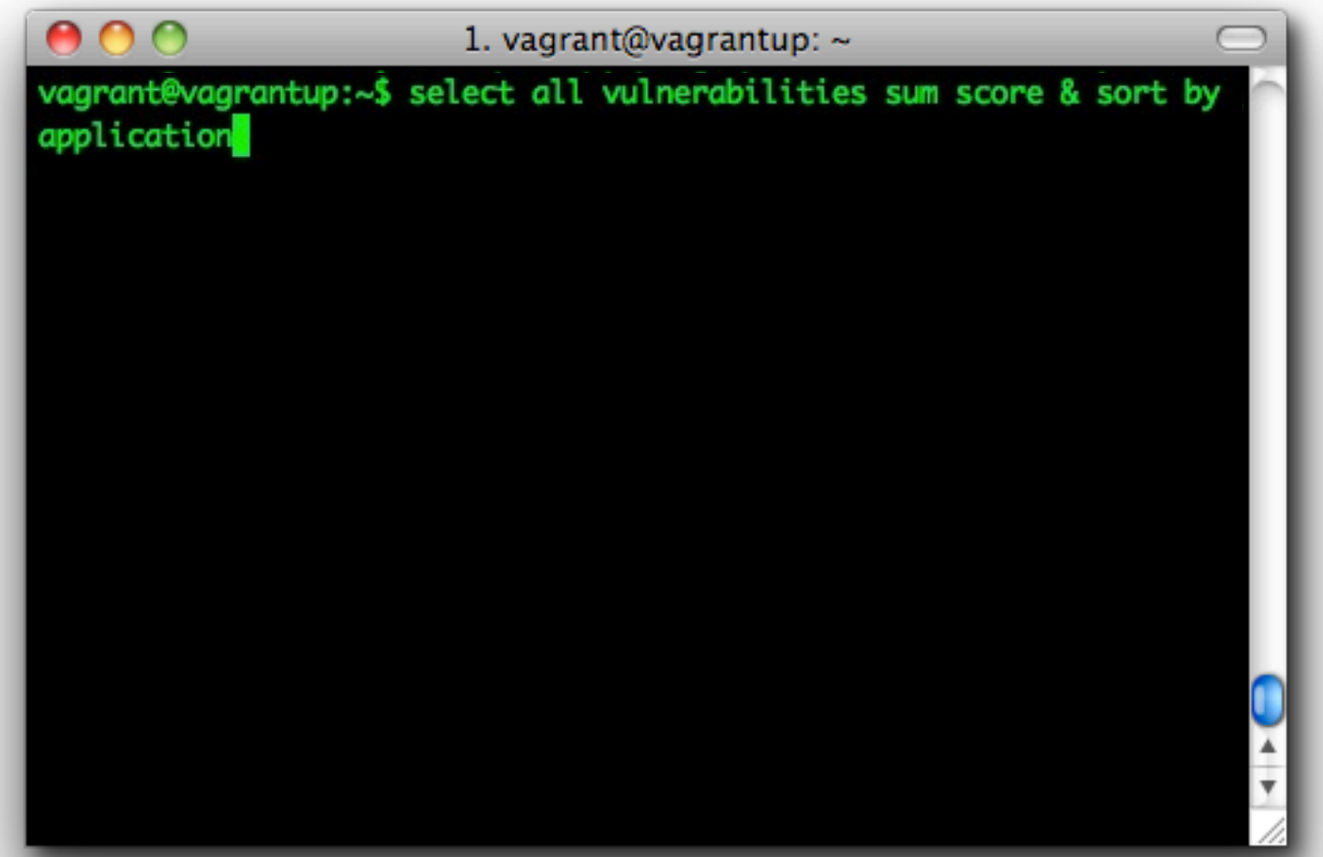
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

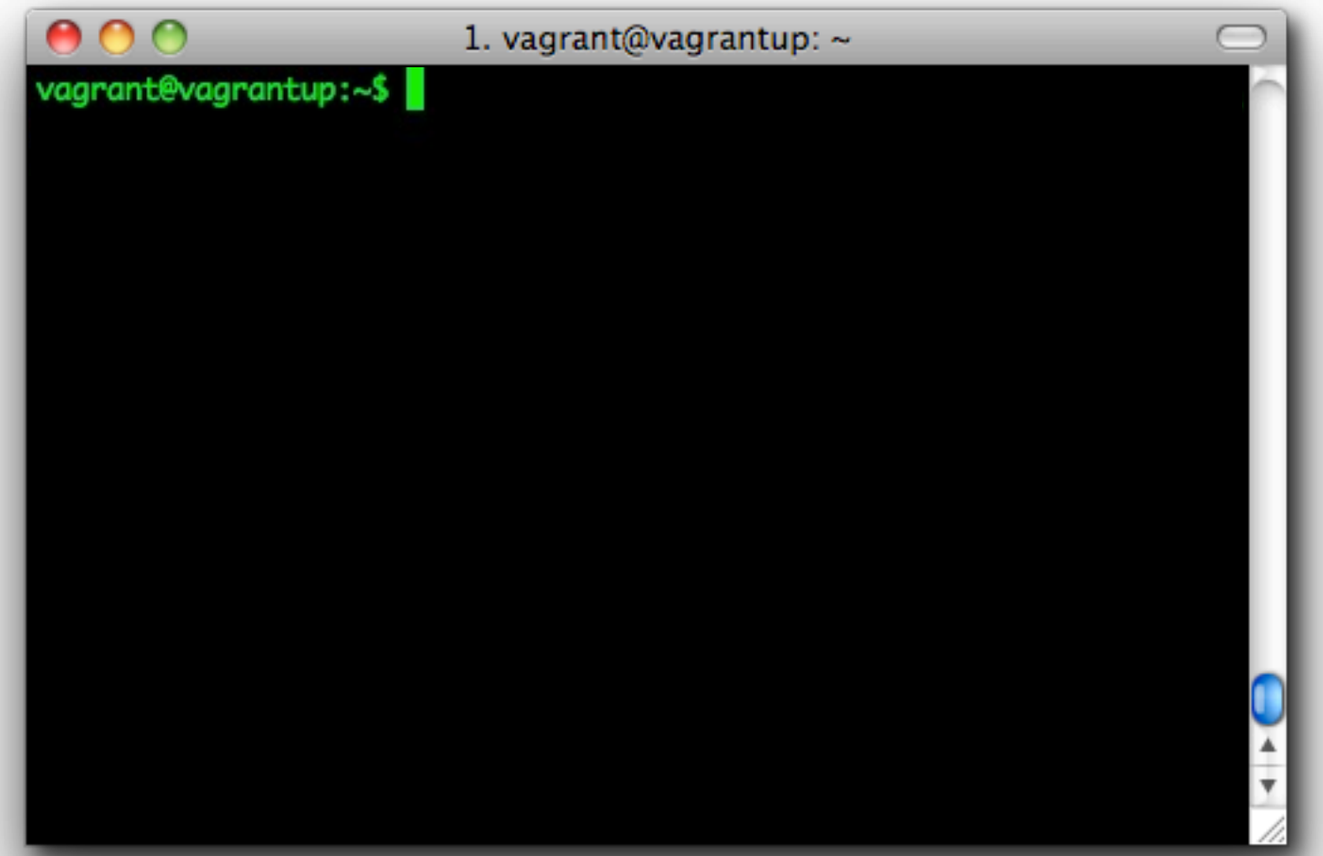
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

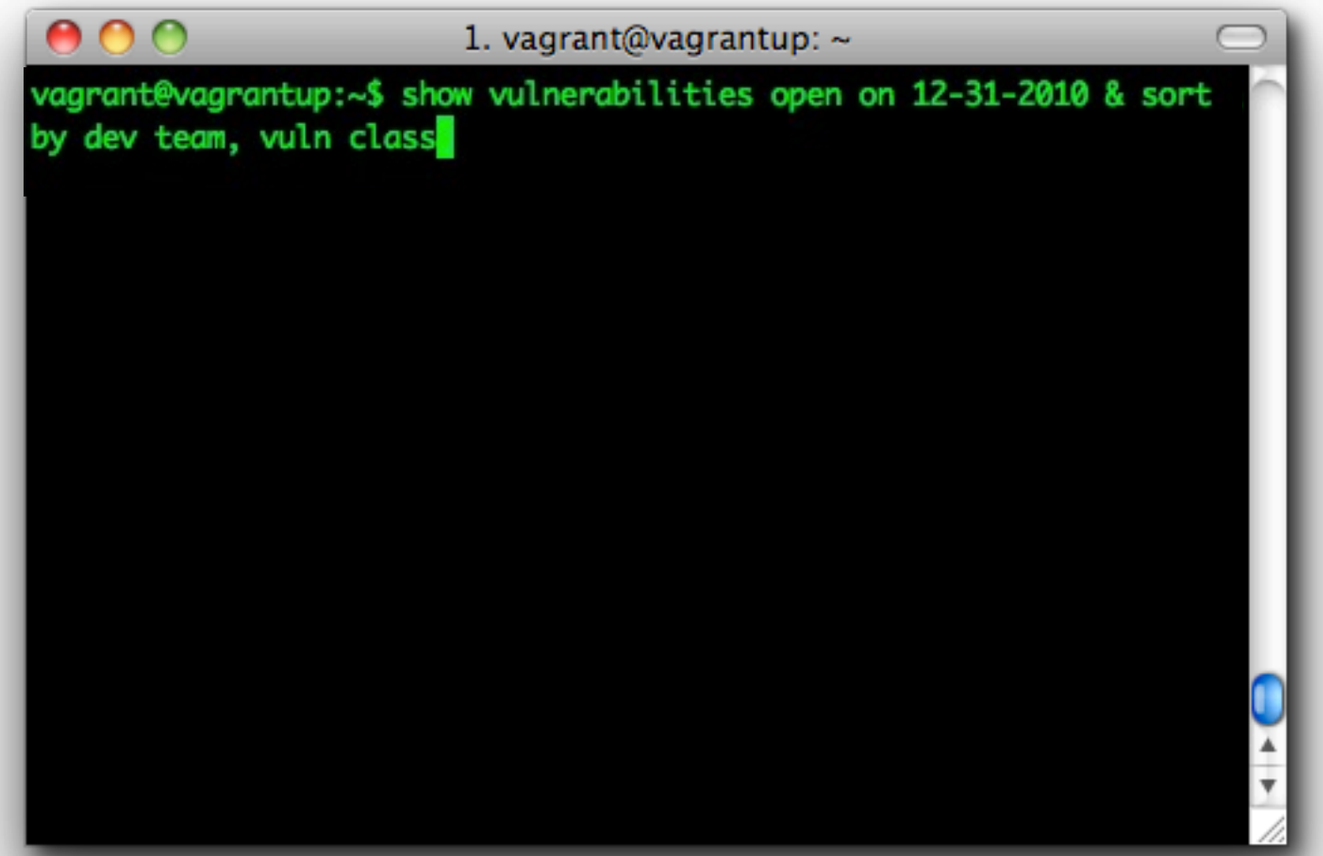
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

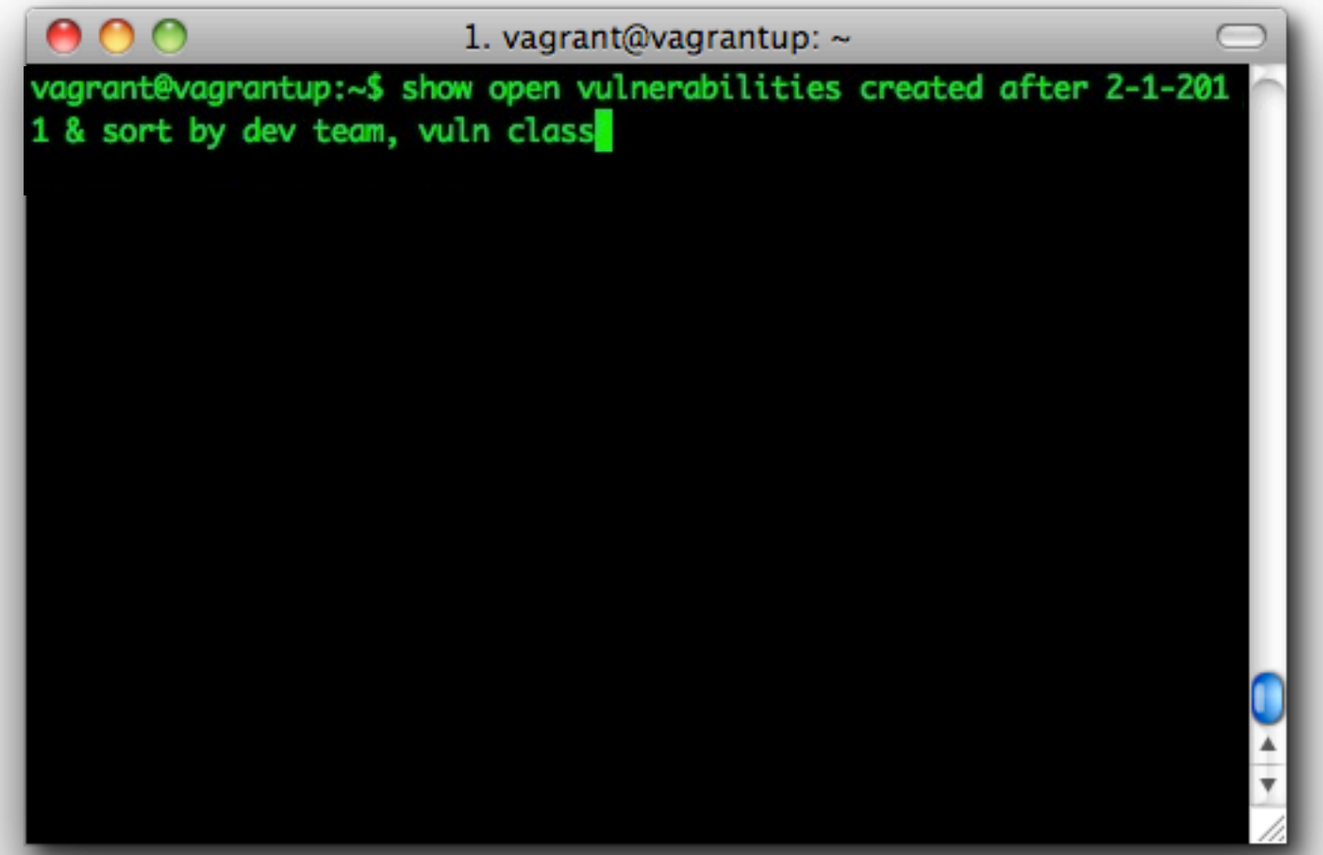
- Applying Filters To Glean Information



honeyapps Inc

Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information



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 twhirl ☆ 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

@robdew
Rob Dewhirst

@ebellis grep, awk, sed, gnuplot

10 May via web ☆ Favorite ↻ Retweet ↩ Reply

@innismir
Ben Jackson

@ebellis perl :)

@Clint326
Clint Laskowski

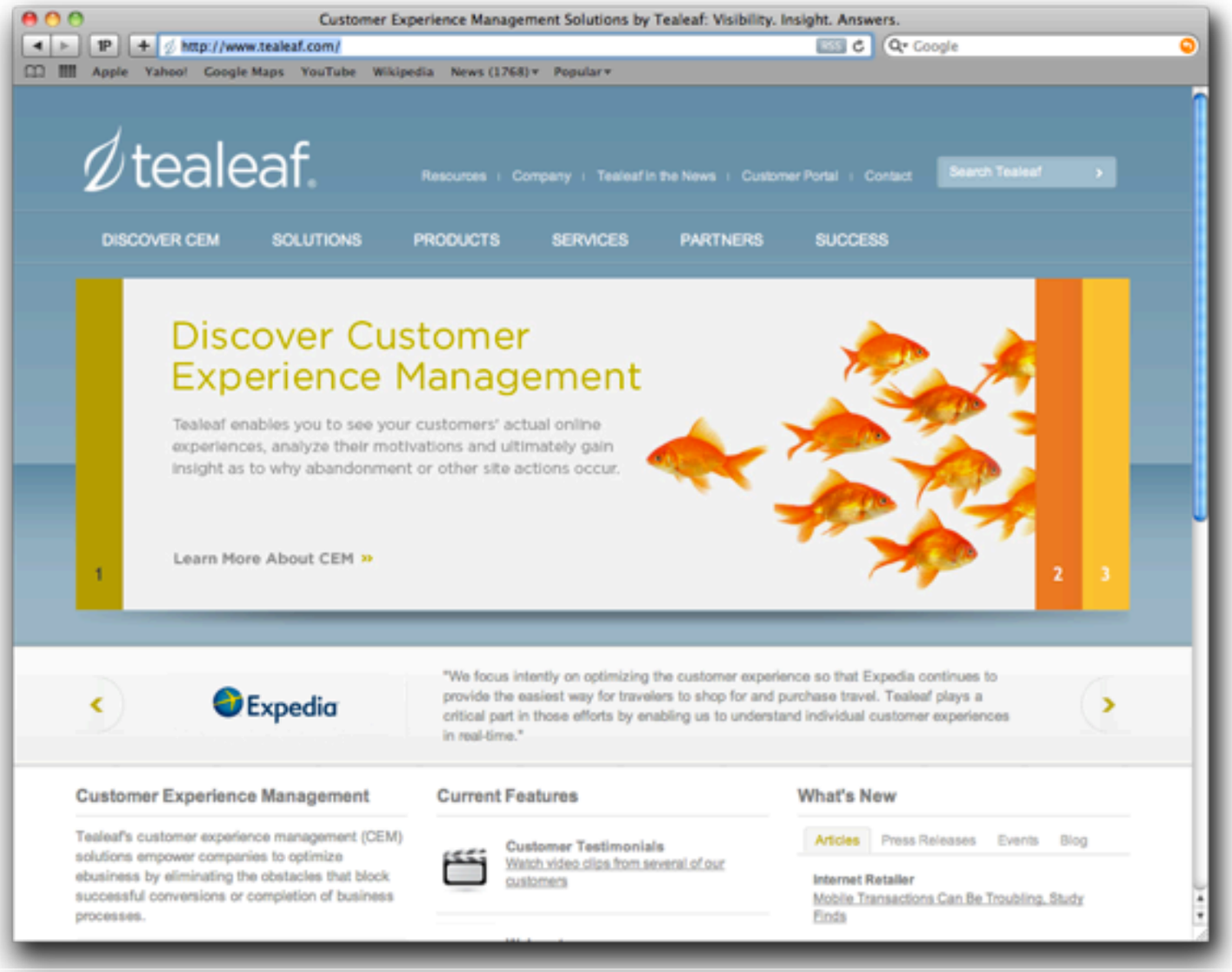
@ebellis @securitytwits I use Text Filter (http://www.musetips.com/text-filter.html) all the time for search logs, lists, etc. Very fast.

10 May via web ☆ Favorite ↻ Retweet ↩ Reply

honeyapps Inc

My Favorite Non-Sec Tools

- TeaLeaf
- 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/

honeyapps Inc

Q & A

follow us

the blog

http://blog.honeyapps.com/

twitter

@honeyapps

@ebellis