Risk I/O

The Search For Intelligent Life
SecTor 2011
Or......

The First 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
Stage 1: 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

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

Lack of Communication
Lack of Data
Lack of Coordination
Silos, Silos, Everywhere
Stage 4: A New Beginning

Or......

Using What You Got!
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

Web App 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
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

Meta Data
- Business Unit
- Geographic Location
- Development Team
- Ops Team
- Compliance Regulation
- Security Policy
- Internal IP Address
- External IP Address
- Network Location
- Site Name
- Asset Group
- VERIS data

Risk I/O
Vulnerability Management: A Case Study

Meta Data
- Business Unit
- Geographic Location
- Development Team
- Ops Team
- Compliance Regulation
- Security Policy
- Internal IP Address
- External IP Address
- Network Location
- Site Name
- Asset Group
- VERIS data
Vulnerability Management: A Case Study

**WebApp Vulnerability**
- **Type**: XSS
- **Severity**
- **Threat**
- **Subtype**: (persistent, reflected, etc)
- **Asset URL**
- **Platform / Code**
- **Web Server Version**
- **Application Server Version**
- **Database Version**
- **Confirmed?**
- **Dates Found/Opened**
- **Dates Closed**
- **Description**
- **Attack Parameters**

**Asset: Host**
- **Host Operating System**
- **Other Applications/Versions**
- **IP Addresses**
- **Mac Address**
- **Open Services/Ports**
Vulnerability Management: A Case Study

Apply Internal Threat Data

WebApp

- **Type:** XSS
- **Severity:**
- **Threat Subtype:** (persistent, reflected, etc)
- **Asset URL/URI**
- **Confirmed?**
- **Dates Found/Opened**
- **Dates Closed**
- **Description**
- **Attack Parameters**
  - **Platform/Code**
  - **Web Server Version**
  - **Application Server Version**
  - **Database Version**
  - **Host Operating System**
  - **Other Applications/Version**
  - **IP Addresses**
  - **Mac Address**
  - **Open Services/Ports**

Asset:URL

Asset:Host
Vulnerability Management: A Case Study

WebApp
Type: XSS
Severity
Threat
Subtype: (persistent, reflected, etc)
Asset URL
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

Apply External Threat Data

**WebApp Vulnerability**
- Type: XSS
- Severity
- Threat
- Subtype:
- 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

Apply External Threat Data

Example Data Sources

- DataLossDB
- Verizon DBIR
- WHID
- Trustwave Global Security Report
- FS-ISAC
- SANS ISC
- Veracode State of S/W Security
- ExploitDB
Vulnerability Management: A Case Study

**WebApp Vulnerability**
- Type: XSS
- Severity
- Threat
- Subtype: (persistent, reflected, etc)
- Asset URL
- 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/Version
- IP Addresses
- Mac Address
- Open Services/Ports
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
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information
Data Lenses: Views into the Warehouse

- Applying Filters To Glean Information
Data Lenses: Views into the Warehouse

- Laundry List of Low Hanging Fruit
Data Lenses: Views into the Warehouse

- Laundry List of Low Hanging Fruit
Data Lenses: Views into the Warehouse

- Laundry List of Low Hanging Fruit
Data Lenses: Views into the Warehouse

- Laundry List of Low Hanging Fruit
Data Lenses: Views into the Warehouse

- HD Moore’s Law
Data Lenses: Views into the Warehouse

- HD Moore’s Law
Data Lenses: Views into the Warehouse

- Most vulnerable apps - apply training
Data Lenses: Views into the Warehouse

- Most vulnerable apps - apply training
Data Lenses: Views into the Warehouse

- How affective was that training?
The Alex Hutton Formula

My(vuln posture * other threat activity) / (other vuln posture * other threat activity)
The Alex Hutton Formula
My(vuln posture * other threat activity) / (other vuln posture * other threat activity)

OR

When Will Our Luck Run Out?
THE NEW SCHOOL

(we need more of this)
using what we have
RT @ebellis: . @securitytwits what non-security tools are you using for security purposes? < I carry this here big stick.

@chrisjager
Chris Jager

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

@dfranke
Daniel Franke

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

@ebebellis telnet; Firefox

@securitytwits showmount, smbclient, snmpwalk, and ldapsearch

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

@ebellis @securitytwits telnet, no joke :)
@ebellis group policy

@ebellis sourceninja, for keeping open source software up to date.

BrianHonan @securitytwits @ebellis Google & LinkedIn - can get a lot of intel from both. Have found passwords for client systems with Google #sectorca

hckhckhck "@securitytwits: RT @ebellis: Hey @securitytwits what's your favorite non-security tool for security? #sectorca <- mine is telnet

Owasp RT @ebellis: Hey @securitytwits what's your favorite non-security tool for security? - has to be grep

lactichaze @ebellis @securitytwits what's your favorite non-security tool for security? #sectorca <- 3M sticky notes (best with ppl's passwords on)
The Twitter Poll

@curphey
Mark Curphey

@ebellis There is only one real king
office.microsoft.com/en-us/excel/
33 minutes ago via TweetDeck ★ Favorite » Retweet ★ Reply

@alexhutton
Alex Hutton

@ebellis @securitytwits excel :)
44 minutes ago via web ★ Favorite » Retweet ★ Reply
My Favorite Non-Sec Tools

- TeaLeaf
- GreenPlum
- Zettaset
- Ruby
- Selenium
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/


ExploitDB http://www.exploit-db.com/


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

WHID http://projects.webappsec.org/w/page/13246995/Web-Hacking-Incident-Database/

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

XForce http://xforce.iss.net/

Q & A

follow us

the blog
http://blog.honeyapps.com/

twitter
@ebellis
@risk_io

And one more thing....

We’re Hiring! https://www.risk.io/jobs