OWASP
Open Web Application
Security Project

Heroes vs Villains:

Building an Application Security Program that Scales

Kevin Delaney, B.IT Hons. NetSec
Director of Solutions Architecture
Security Compass

NASDAQ

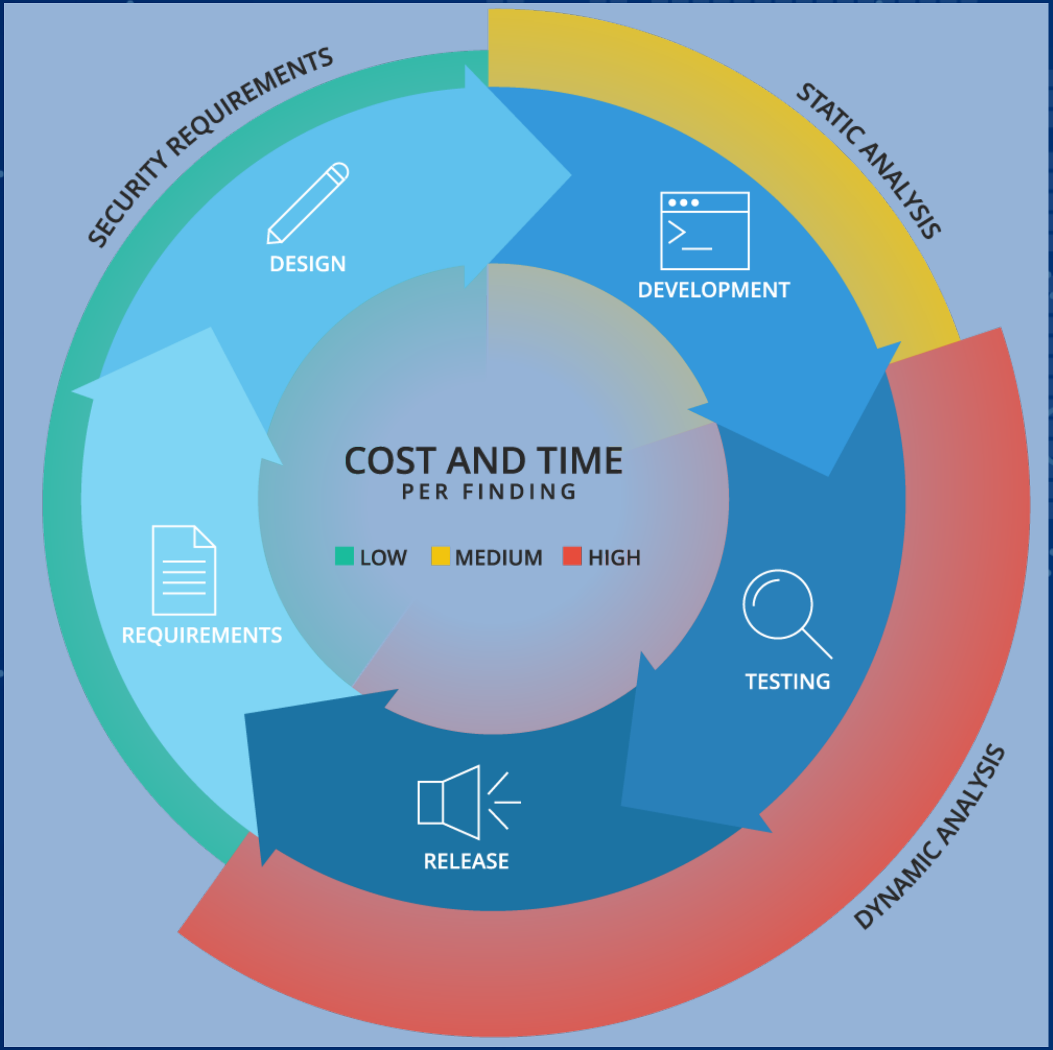
JCPenney

jetBlue

Over 160 Million Credit Cards lifted over 7 years

Villains are **PROACTIVE**

Heroes are REACTIVE



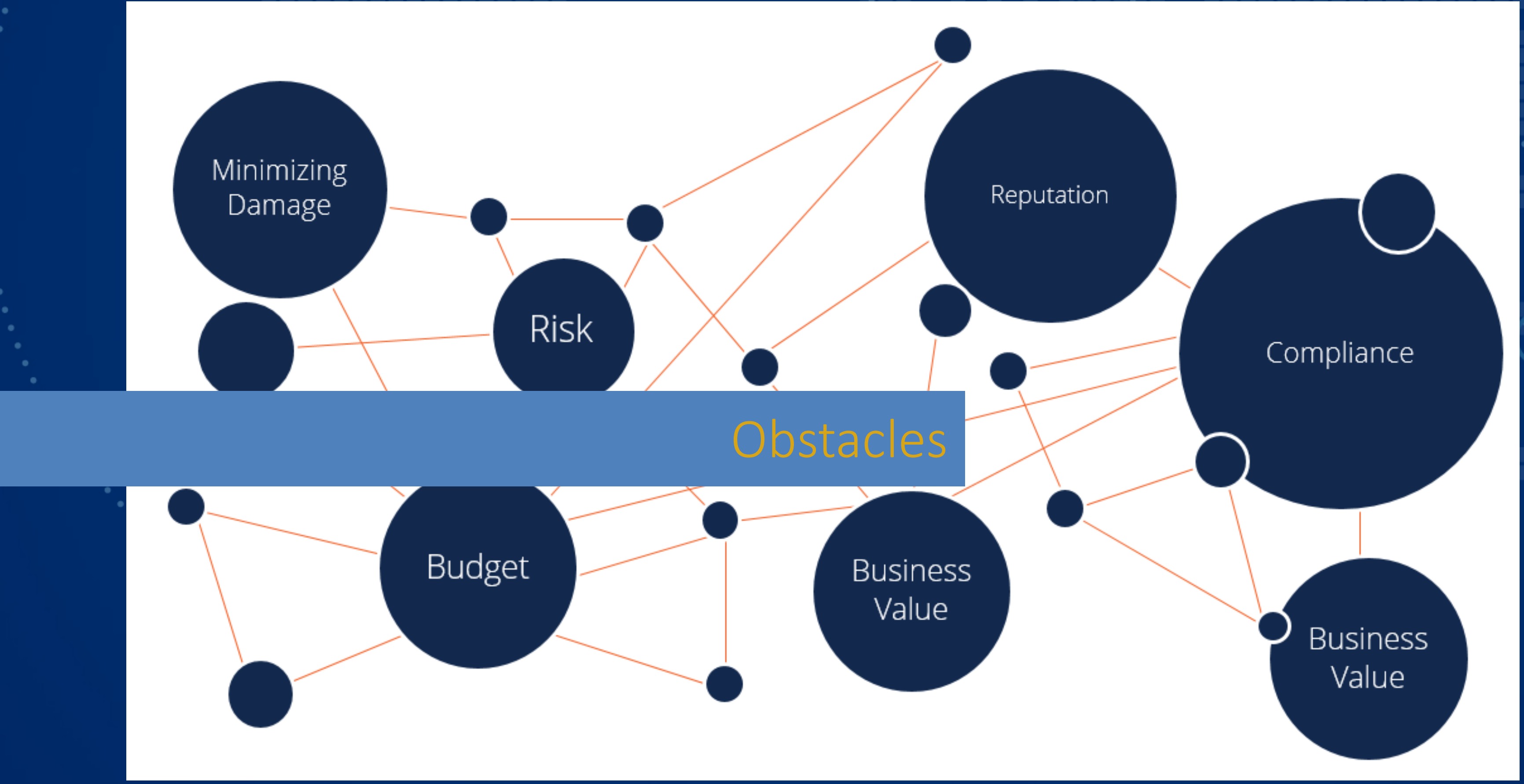
OWASP
Open Web Application
Security Project

5 Step Process

Why does this happen?

- Inexperienced developers
- Apathy towards secure development
- Overwhelming requirements documents
- Too much reliance on static and dynamic analysis tools

OWASP
Open Web Application
Security Project



Obstacles

OWASP
Open Web Application
Security Project

Time, Skills, Security Talent

Pin-pointing vulnerabilities before cyber criminals do

Customer requirements and ever changing compliance standards

The Struggle is Real.

Good help is hard to find

OWASP
Open Web Application
Security Project

Your company is not the only one that struggles to find the experienced IT professionals and security architects necessary to perform risk assessments

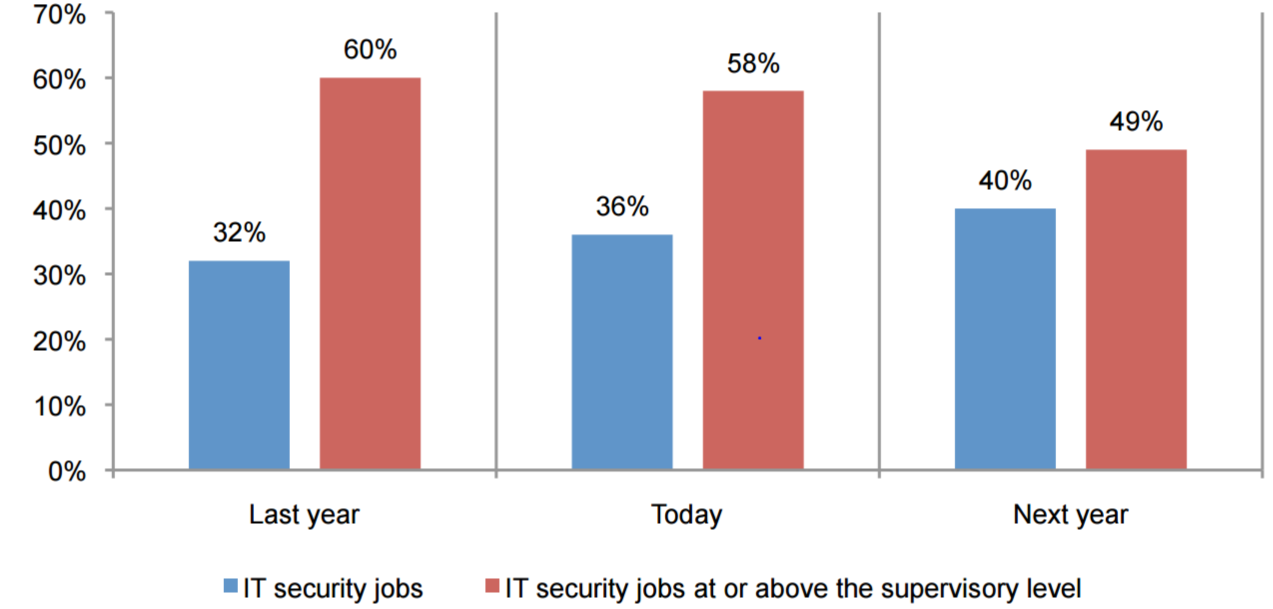
- **70%** of respondents believe their organization does not have enough IT Security Staff
- **36%** of security positions were unfilled.
- **58%** of senior security positions were unfilled.

.

Shallow Talent Pool

Open Web Application Security Project

Figure 4. Average percentage of IT security positions not filled



Understaffed and at Risk:
Today's IT Security Department - Ponemon Institute

The Numbers

OWASP
Open Web Application
Security Project

- Demand for InfoSec jobs growing 3.5x faster than other IT jobs, 12x faster than all jobs.
- 12,000 InfoSec professionals surveyed believe that talent shortage weakened their defenses [ISC2]
- 70% of companies surveyed in the US believe their IT Security department is understaffed.
- 50,000 CISSP postings in the US alone, but only 60,000 CISSP’s worldwide.

burningglass
CAREERS IN FOCUS

An Expensive Endeavor

Average Security Architect salary in the United Kingdom is £75,000

Employers want certified domain experts with multiple years of experience in:

- Network security governance
- Policies
- Procedures
- Application Security

General Security Knowledge is not Enough

Do more with less

- Stop relying on just your security team for security
- Identify security champions in your development team and empower them.
- Incentivize with training and certifications - transferrable skills.
- Teach your heroes to think like VILLAINS!

CSSLP®

Certified Secure
Software Lifecycle Professional

OWASP
Open Web Application
Security Project

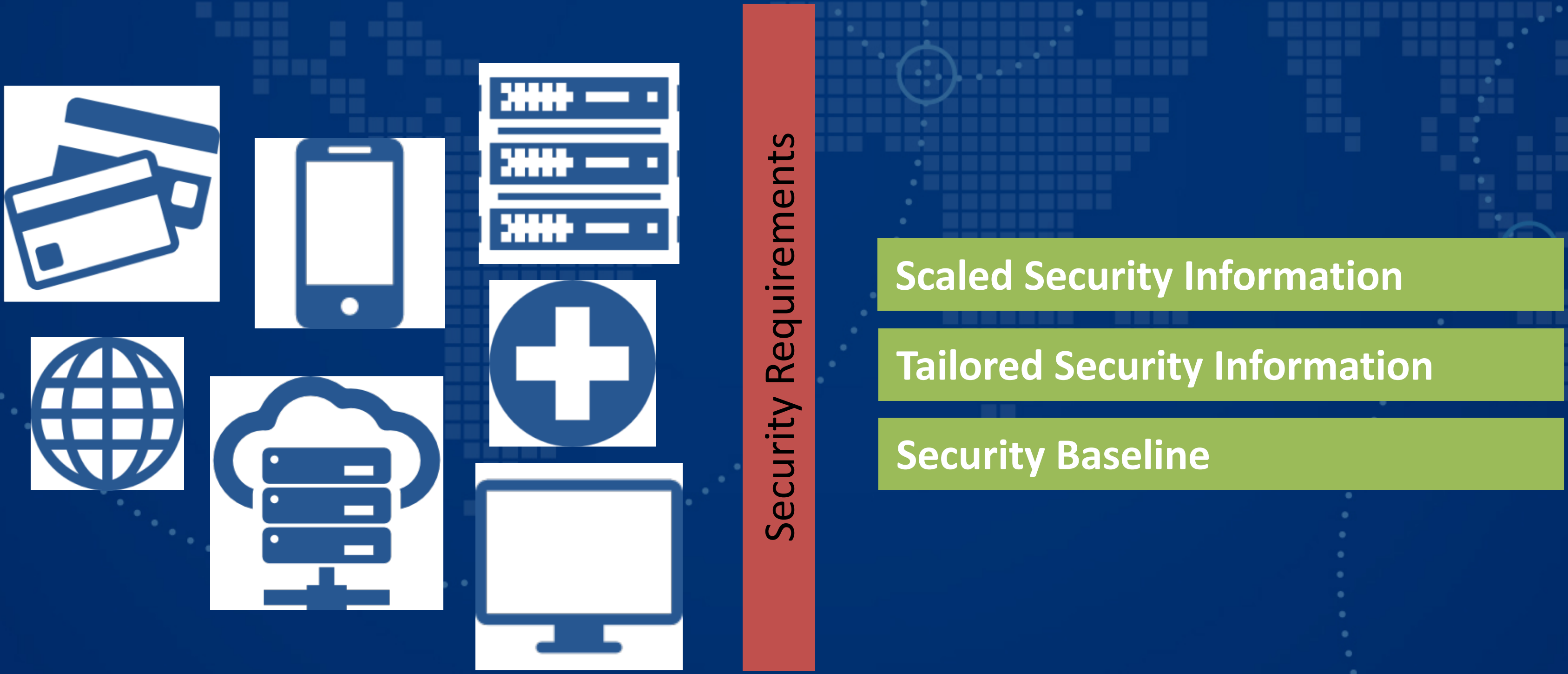
- How to develop an application security program
- How to reduce production costs, application vulnerabilities, and delivery delays
- How to ensure that secure software is accepted and delivered effectively.

OWASP

Open Web Application
Security Project

What makes a GREAT AppSec Program?

Adaptable



Security Requirements

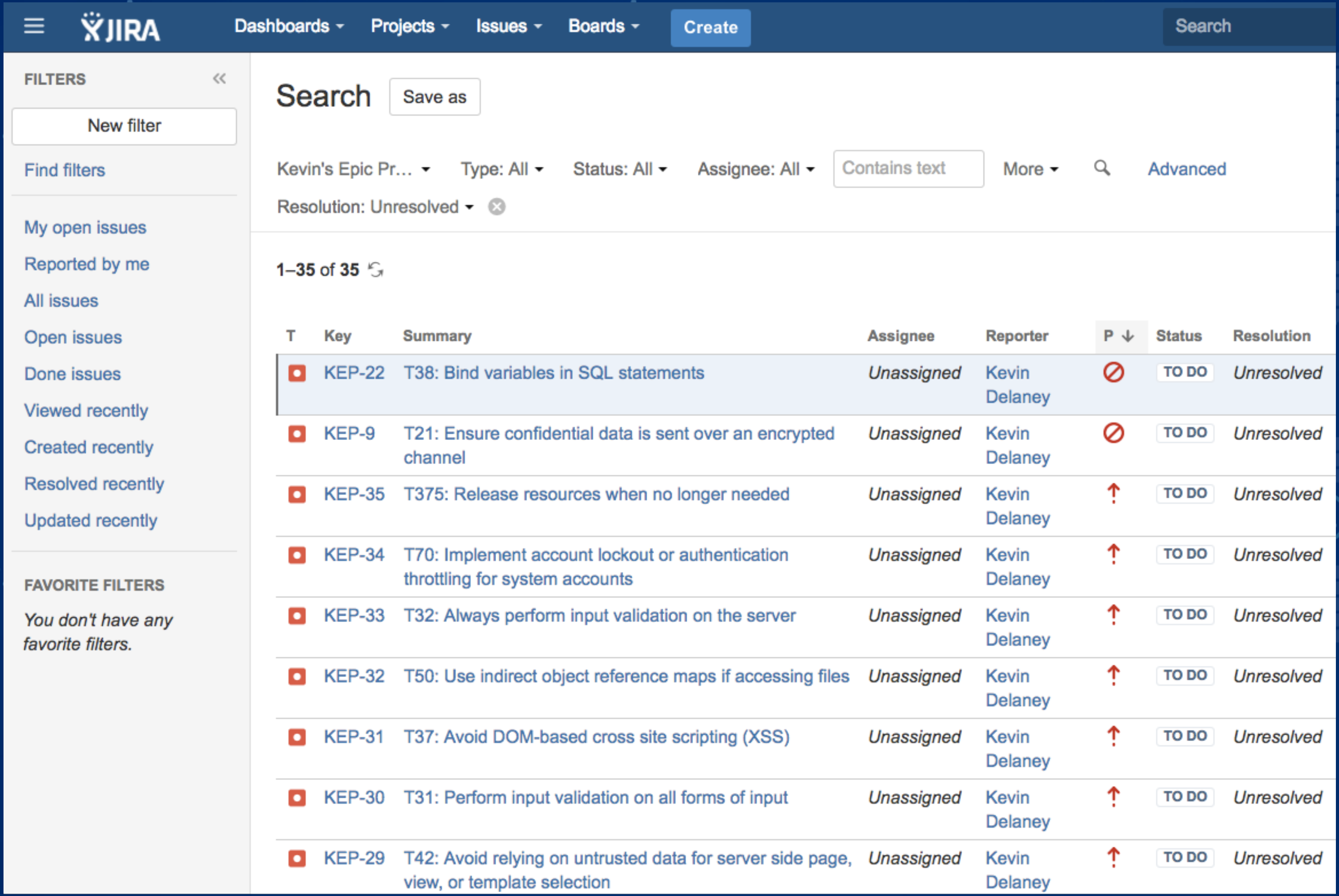
Scaled Security Information

Tailored Security Information

Security Baseline

Focused

- A great appsec program is focused on the strengths of the people participating.
- Ideally, security tasks should be generated on-the-fly based on the profile of the application and its associated risks and delivered directly into your developers' ALM tools like JIRA or TFS.
- Ensures nothing is missed and reduces time spent searching for what's applicable to a project by multitudes.



You don't have any favorite filters.

Search

Kevin's Epic Pr… Type: All Status: All Assignee: All

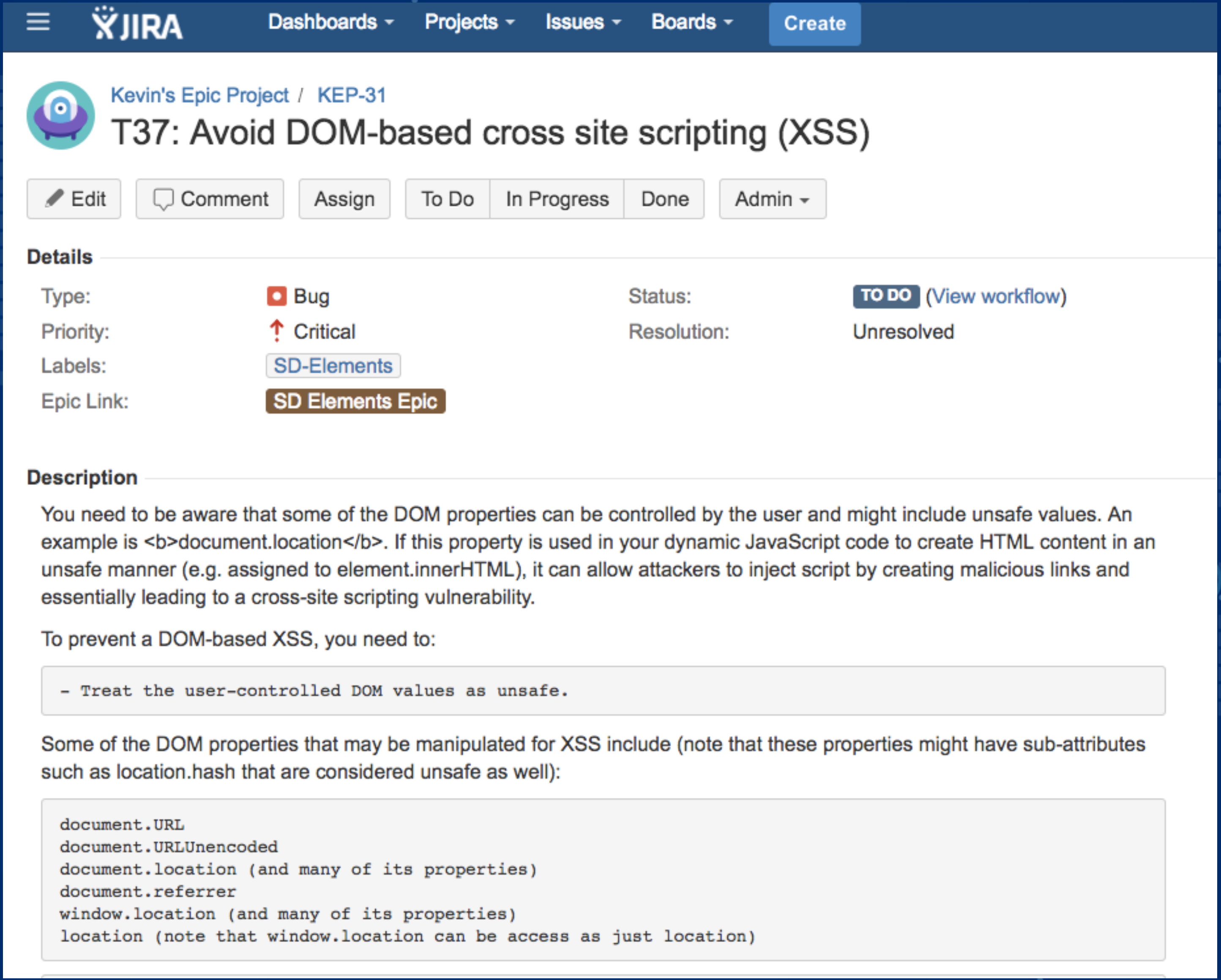
Resolution: Unresolved

1–35 of 35

T	Key	Summary	Assignee	Reporter	P ↓	Status	Resolution
■	KEP-22	T38: Bind variables in SQL statements	*Unassigned*	Kevin Delaney	⊘	TO DO	*Unresolved*
■	KEP-9	T21: Ensure confidential data is sent over an encrypted channel	*Unassigned*	Kevin Delaney	⊘	TO DO	*Unresolved*
■	KEP-35	T375: Release resources when no longer needed	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*
■	KEP-34	T70: Implement account lockout or authentication throttling for system accounts	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*
■	KEP-33	T32: Always perform input validation on the server	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*
■	KEP-32	T50: Use indirect object reference maps if accessing files	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*
■	KEP-31	T37: Avoid DOM-based cross site scripting (XSS)	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*
■	KEP-30	T31: Perform input validation on all forms of input	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*
■	KEP-29	T42: Avoid relying on untrusted data for server side page, view, or template selection	*Unassigned*	Kevin Delaney	↑	TO DO	*Unresolved*

Task

Code



Kevin's Epic Project / KEP-31

T37: Avoid DOM-based cross site scripting (XSS)

Details

Type:	Bug	Status:	TO DO (View workflow)
Priority:	Critical	Resolution:	Unresolved
Labels:	SD-Elements		
Epic Link:	SD Elements Epic		

Description

You need to be aware that some of the DOM properties can be controlled by the user and might include unsafe values. An example is <b>document.location</b>. If this property is used in your dynamic JavaScript code to create HTML content in an unsafe manner (e.g. assigned to element.innerHTML), it can allow attackers to inject script by creating malicious links and essentially leading to a cross-site scripting vulnerability.

To prevent a DOM-based XSS, you need to:

```
- Treat the user-controlled DOM values as unsafe.
```

Some of the DOM properties that may be manipulated for XSS include (note that these properties might have sub-attributes such as location.hash that are considered unsafe as well):

```
document.URL
document.URLUnencoded
document.location (and many of its properties)
document.referrer
window.location (and many of its properties)
location (note that window.location can be access as just location)
```

Collaborative

- No more “us vs. them” mentality between developers and security.
- Developers must take responsibility for security tasks.
- You cannot create a security culture – it is created from within the development org.

Recap

Open Web Application Security Project

- Proper management of security requirements early in the SLDC prevents problems before they happen and turns down the noise from static/dynamic analysis tools.
- Delivering these requirements directly to developers in the tools they use every day is critical for acceptance.
- Leverage and empower your existing resources, because finding new ones is no easy task.
- Make sure your AppSec program is adaptable, focused, and collaborative.

OWASP
Open Web Application
Security Project

Thank You, Villains!

Kevin Delaney
Director, Solutions Architecture
kdelaney@securitycompass.com

http://securitycompass.com/