



the leading secure software development firm



ThreadFix

Powered by Denim Group

BlackHat Webinar

Dan Cornell
CTO, Denim Group
[@danielcornell](https://twitter.com/danielcornell)

The Problem

- Application security testing typically uses automated static and dynamic test results as well as manual testing results to assess the security of an application
- Each test delivers results in different formats
- Different test platforms also can describe the same flaws differently, creating multiple duplications
- Security teams end up using spreadsheets to keep track manually
- It is extremely difficult to prioritize the severity of flaws as a result
- Software development teams receive unmanageable reports and only a small portion of the flaws get fixed

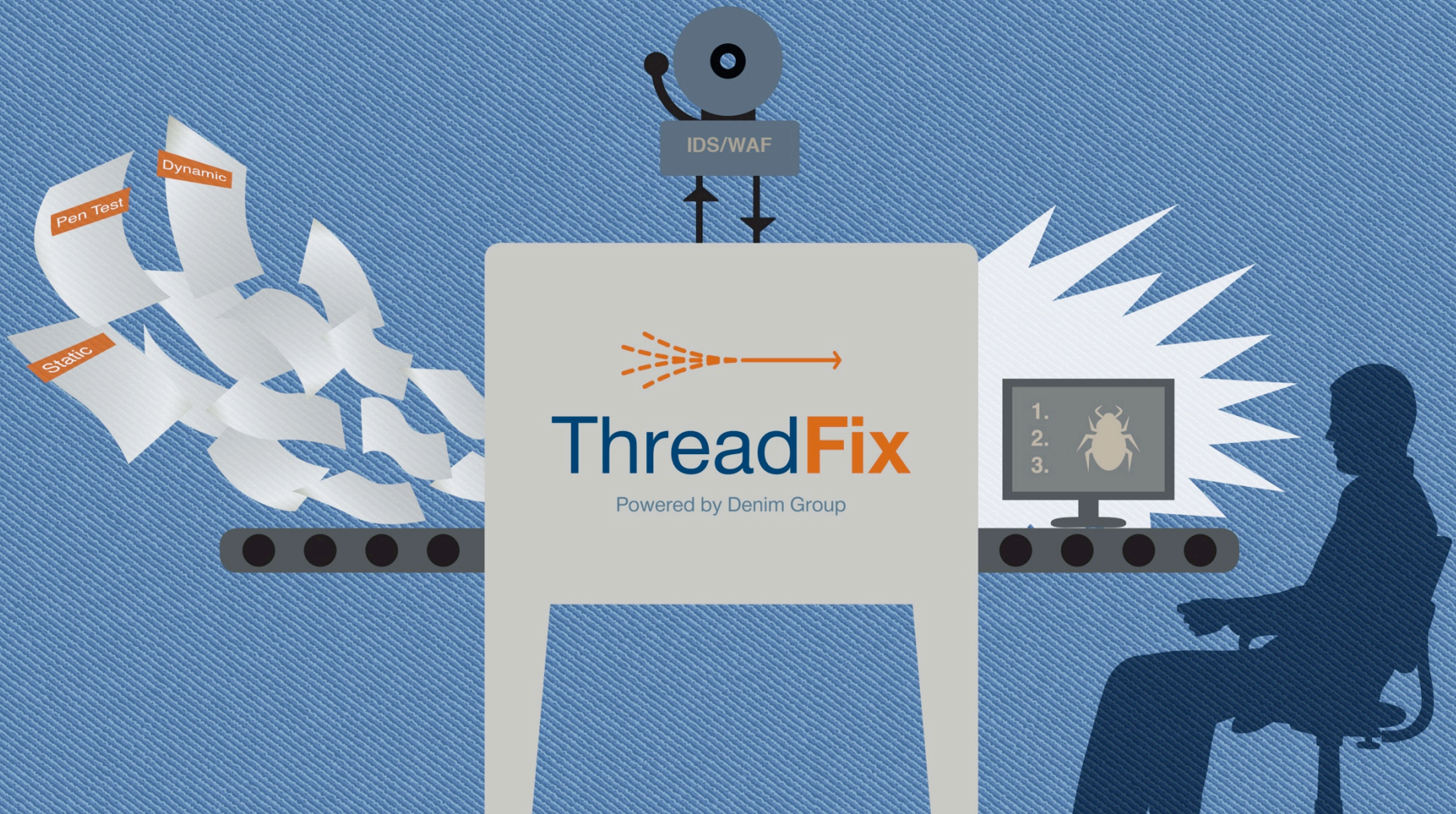
The Result

- Application vulnerabilities persist in applications
 - *The average number of serious vulnerabilities found per website per year is 79*
 - *The average number of days a website is exposed to at least one serious vulnerability is 231 days*
 - *The overall percentage of serious vulnerabilities that are fixed annually is only 63%*
- Part of that problem is there is no easy way for the security team and application development teams to work together on these issues
- Remediation quickly becomes an overwhelming project
- Trending reports that track the number of reduced vulnerabilities are impossible to create

Sources: https://www.whitehatsec.com/assets/WPstats_summer12_12th.pdf , pages 2 & 3
<http://www.veracode.com/reports> (registration required)

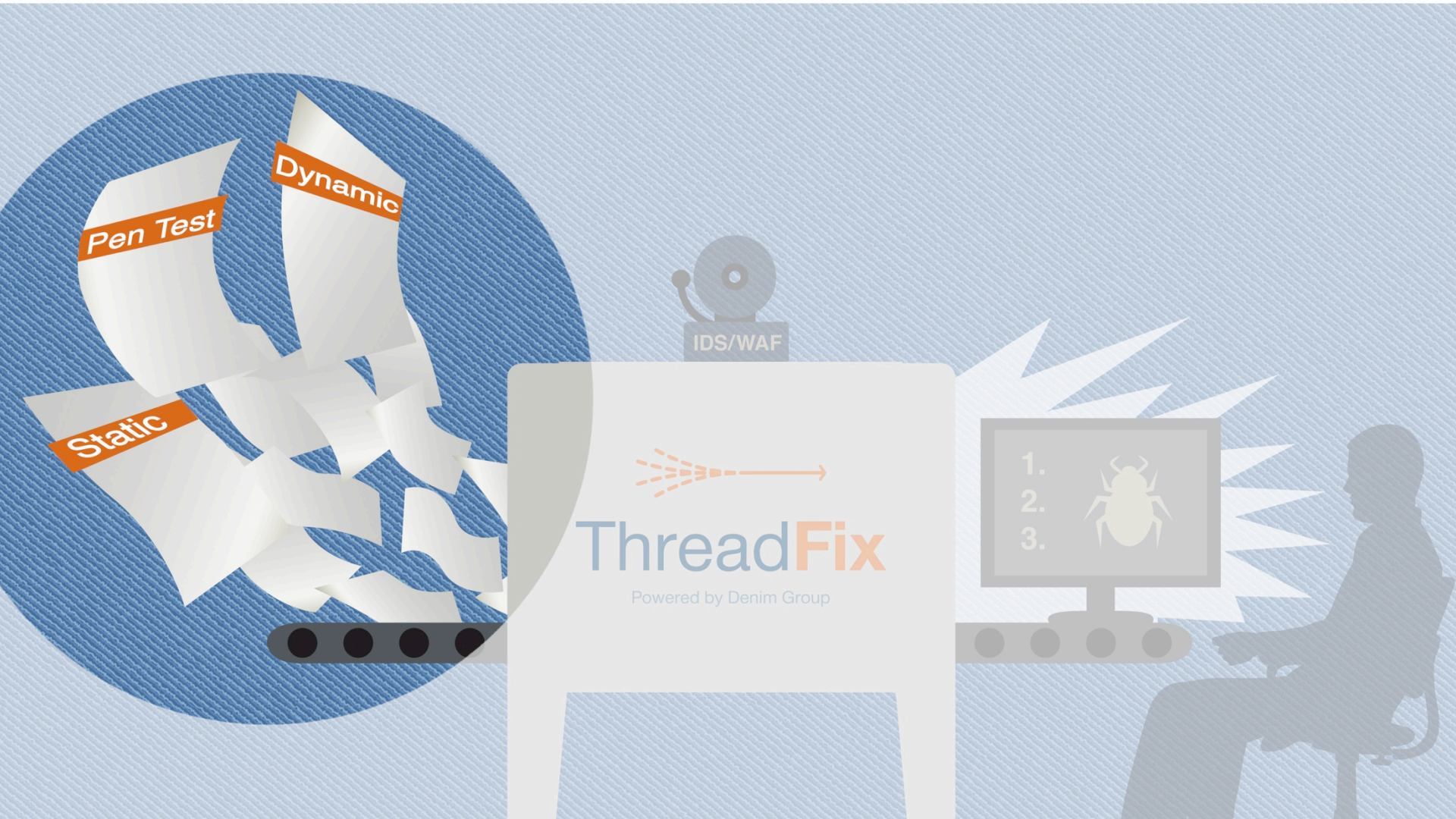
ThreadFix

Consolidates reports so managers can speak intelligently about the status and trends of security within their organization



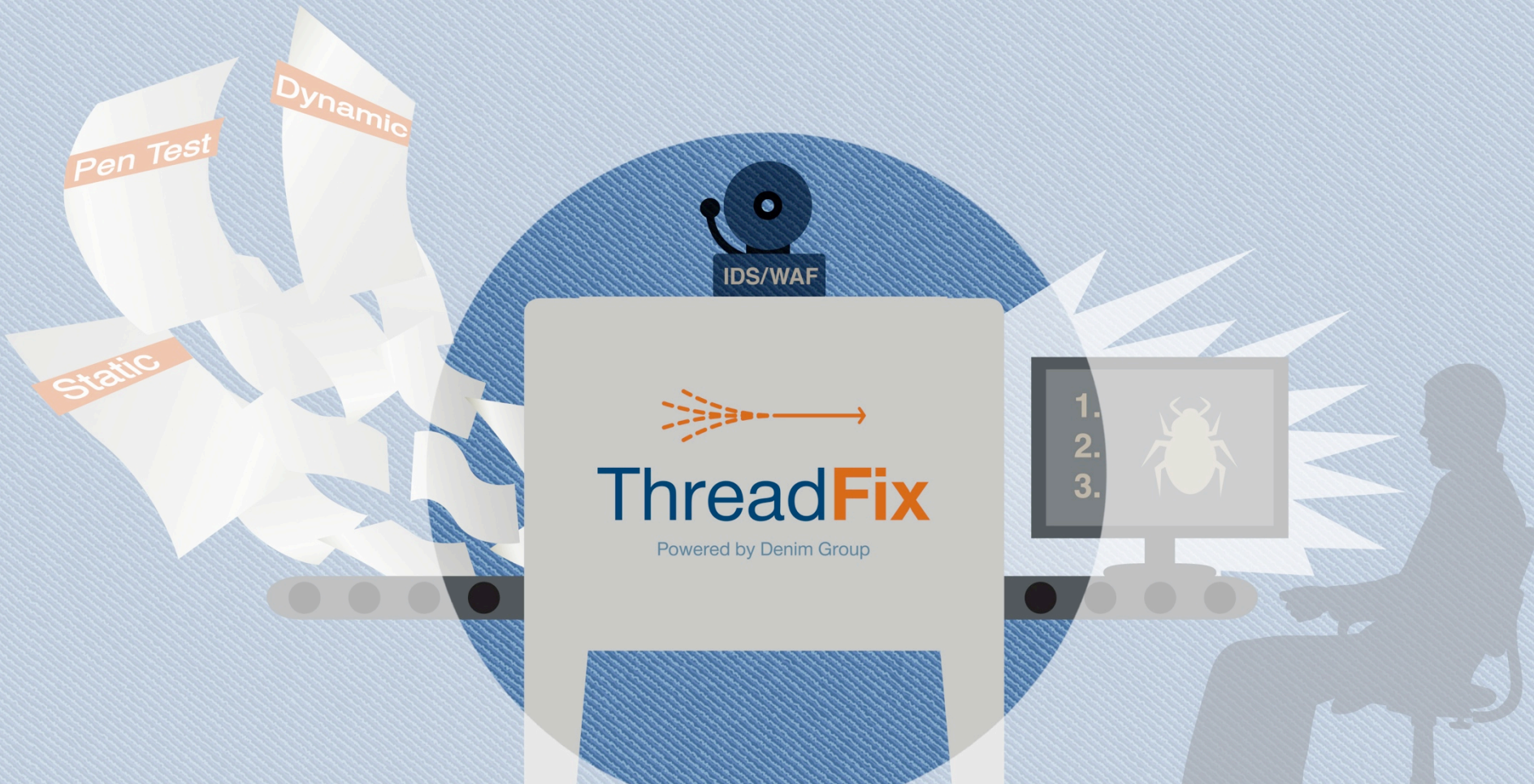
Vulnerability Import

- Pulls in static and dynamic results
- Eliminates duplicate results
- Allows for results to be grouped



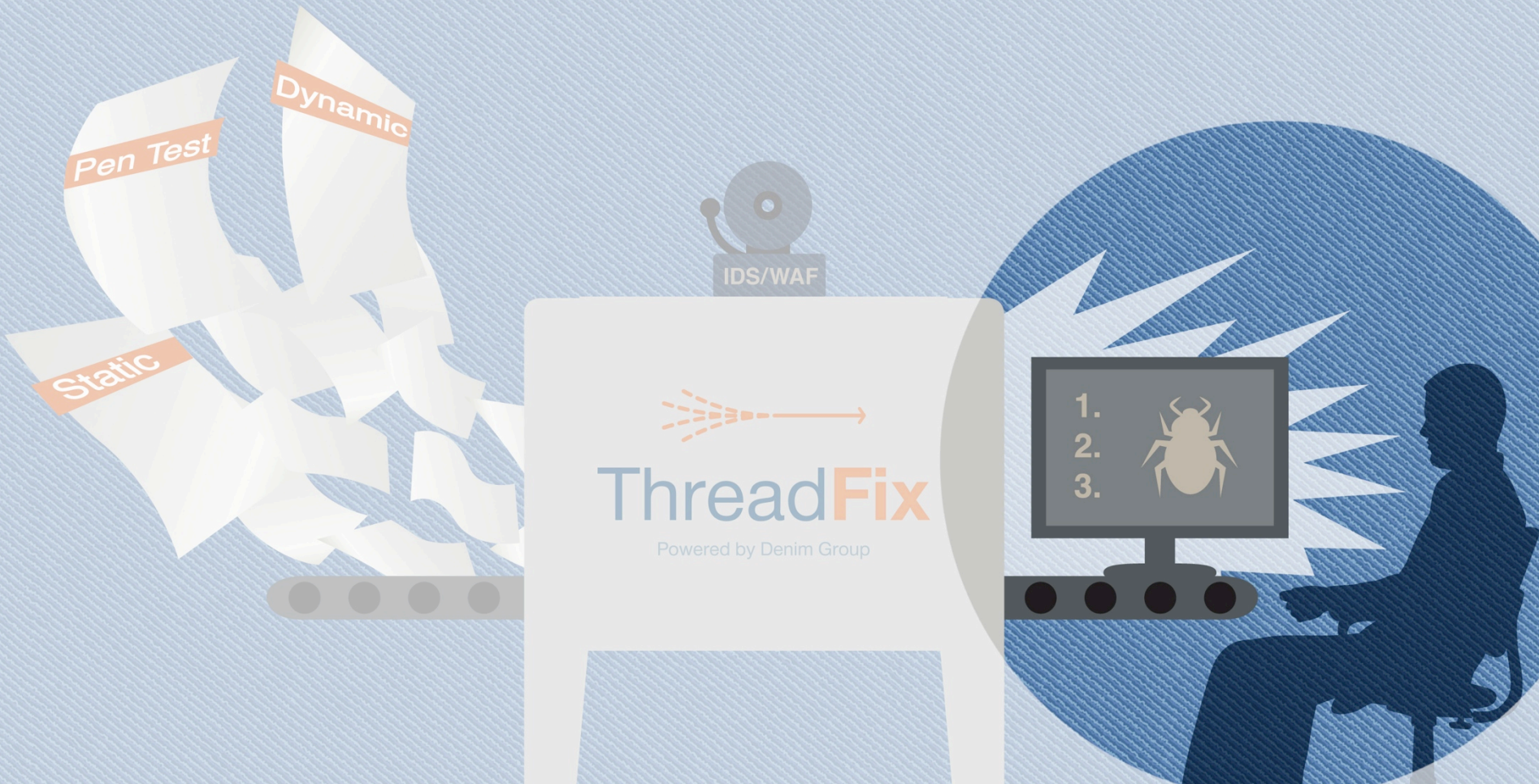
Real-Time Protection

Virtual patching helps protect organizations during remediation



Defect Tracking Integration

- ThreadFix can connect to common defect trackers
- Defects can be created for developers
- Work can continue uninterrupted





the leading secure software development firm



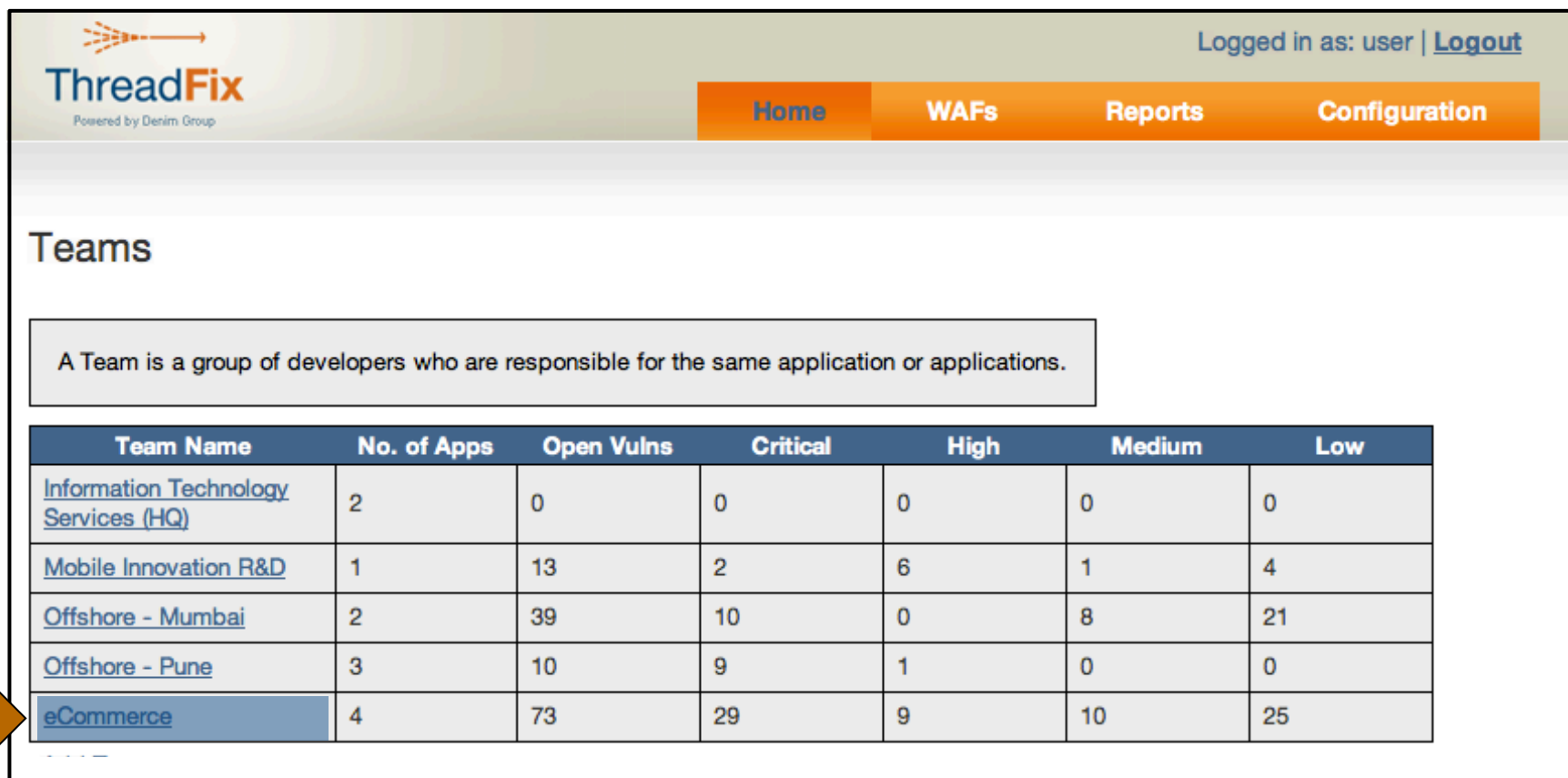
ThreadFix

Powered by Denim Group

Product Demonstration

The Dashboard

- Lists all the development teams in the organization including number of apps for each team and a summary of the security status of those apps.
- Clicking on a team reveals the details on the apps that team is working on.



ThreadFix
Powered by Denim Group

Logged in as: user | [Logout](#)

[Home](#) [WAFs](#) [Reports](#) [Configuration](#)

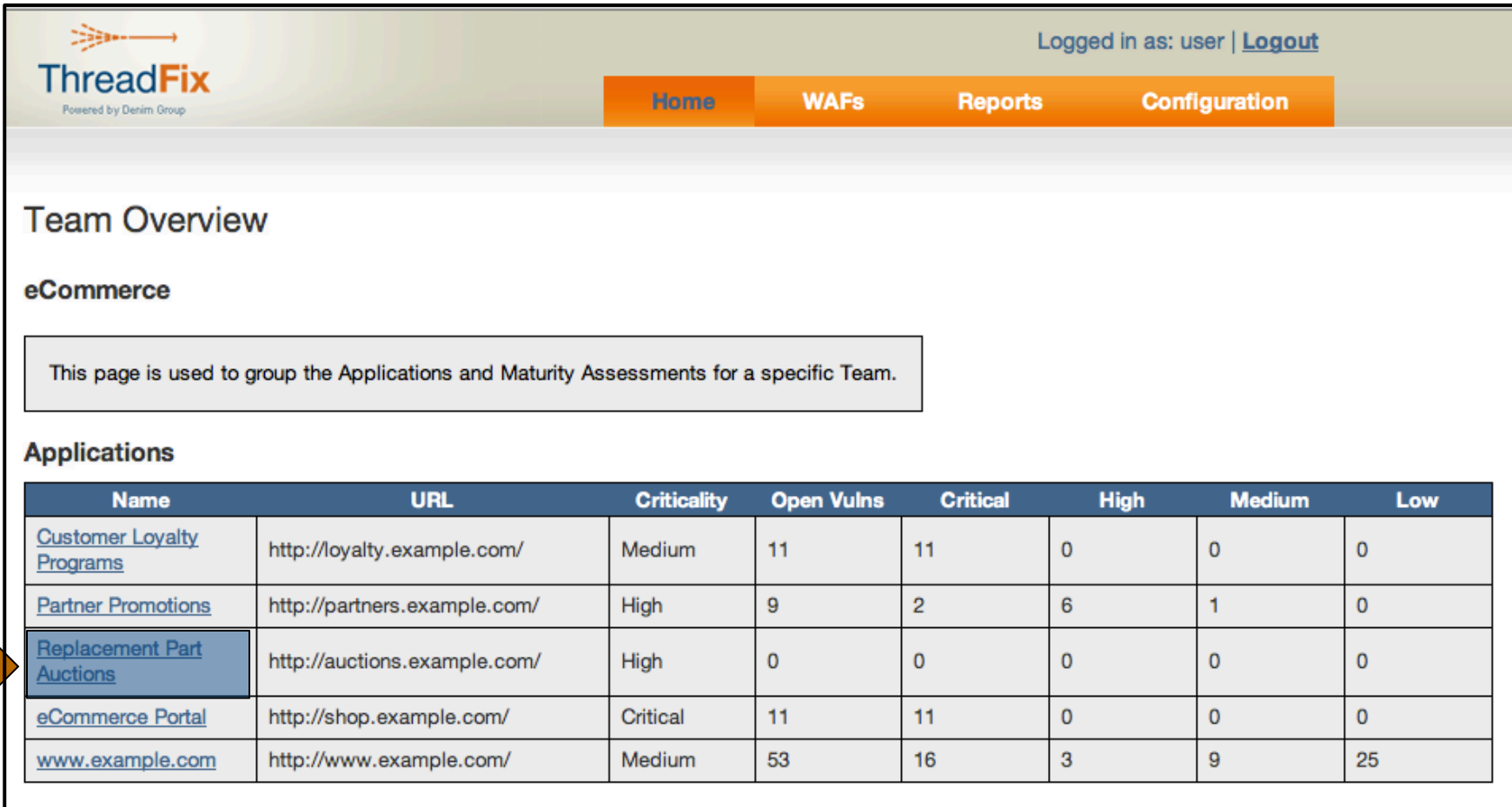
Teams

A Team is a group of developers who are responsible for the same application or applications.

Team Name	No. of Apps	Open Vulns	Critical	High	Medium	Low
Information Technology Services (HQ)	2	0	0	0	0	0
Mobile Innovation R&D	1	13	2	6	1	4
Offshore - Mumbai	2	39	10	0	8	21
Offshore - Pune	3	10	9	1	0	0
eCommerce	4	73	29	9	10	25

Viewing The Applications By Team

- Now all of the applications managed by the eCommerce team are revealed.
- The security analyst now wants to upload new vulnerability scan data for the "Replacement Part Auctions" application and clicks on that link.



ThreadFix
Powered by Denim Group

Logged in as: user | [Logout](#)

[Home](#) [WAFs](#) [Reports](#) [Configuration](#)

Team Overview

eCommerce

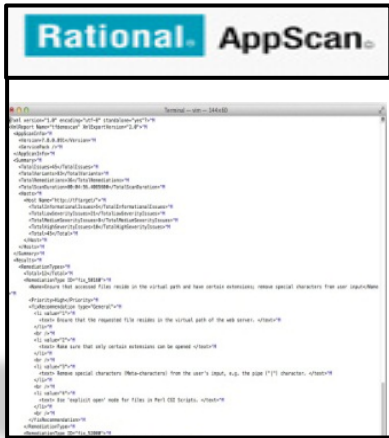
This page is used to group the Applications and Maturity Assessments for a specific Team.

Applications

Name	URL	Criticality	Open Vulns	Critical	High	Medium	Low
Customer Loyalty Programs	http://loyalty.example.com/	Medium	11	11	0	0	0
Partner Promotions	http://partners.example.com/	High	9	2	6	1	0
Replacement Part Auctions	http://auctions.example.com/	High	0	0	0	0	0
eCommerce Portal	http://shop.example.com/	Critical	11	11	0	0	0
www.example.com	http://www.example.com/	Medium	53	16	3	9	25

Fixing an eCommerce Team “Auction” Application –

- Vulnerability data from AppScan, Arachni, Netsparker and W3af scans are uploaded into ThreadFix.



ThreadFix
Powered by Denim Group

Logged in as: user | Logout

Home WAFs Reports Configuration

Application: Replacement Part Auctions [Edit](#) [Delete](#)

Applications are used to store, unify, and manipulate scan results from security scanners.

All Open Vulnerabilities
Listing 23 vulnerabilities from 1 scan. [View Scans](#)

Show Filters

if Merged	Vulnerability Name	Severity	Path	Parameter	Defect	Defect Status	WAF Rule	WAF Events	Select All
2	Improper Sanitization of Special Elements used in an OS Command (OS Command Injection)	Critical	/demo/OSCommandInjection2.php	fileName		No Defect	No	0	<input type="checkbox"/>
	Failure to Control Generation of Code (Code Injection)	Critical	/demo/EvalInjection2.php	command		No Defect	No	0	<input type="checkbox"/>
	Failure to Preserve Web Page Structure (Cross-site Scripting)	High	/demo/XPathInjection2.php	password		No Defect	No	0	<input type="checkbox"/>
	Failure to Preserve Web Page Structure (Cross-site Scripting)	High	/demo/EvalInjection2.php	command		No Defect	No	0	<input type="checkbox"/>
	Failure to Preserve Web Page Structure (Cross-site Scripting)	High	/demo/XSS-reflected2.php	username		No Defect	No	0	<input type="checkbox"/>



Large Range of Tool Compatibility

VERACODE



IBM

PortSwigger
web security



w3af
Web Application Attack and Audit Framework

iMPERVA

ATLASSIAN
JIRA



FindBugs



skipfish

OUNCE LABS



acunetix



hp Enterprise Security

WhiteHat
SECURITY

arachni
web application security scanner framework

netsparker

Compatible Tool Categories

Dynamic Scanners

Burp Suite

HP WebInspect

IBM Rational AppScan

Mavituna Security Netsparker

Tenable Nessus

Acunetix

OWASP Zed Attack Proxy

Arachni

Skipfish

Defect Trackers

Mozilla Bugzilla

Atlassian JIRA

Static Scanners

HP Fortify SCA

Microsoft CAT.NET

FindBugs

Ounce IBM Security AppScan Source

SaaS Testing Platforms

WhiteHat

Veracode

QualysGuard WAS 2.0

IDS/IPS and WAF

F5

Deny All

Snort

mod_security

Imperva

The ThreadFix Consolidation

- All of the vulnerability scans have been aggregated into ThreadFix providing a centralized view of the security status of the Auction application.

ThreadFix
Powered by Denim Group

Logged in as: user | [Logout](#)

[Home](#) [WAFs](#) [Reports](#) [Configuration](#)

All Open Vulnerabilities

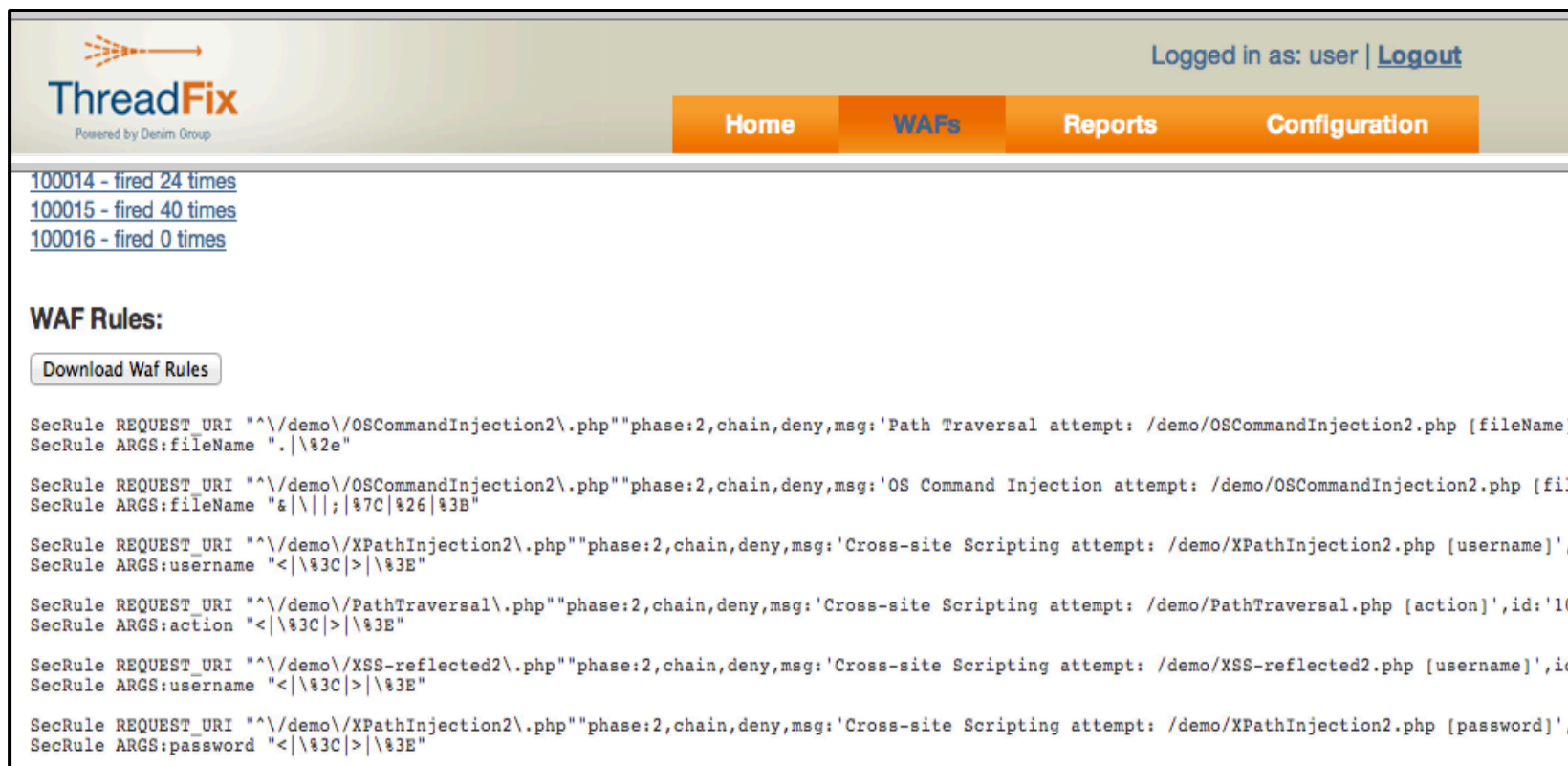
Listing 57 vulnerabilities from 4 scans. [View Scans](#) [View / Unmark 11 False Positives](#)

[Show Filters](#)

If Merged ↓	Vulnerability Name ↓	Severity ↓	Path ↓	Parameter ↓	Defect ↓	Defect Status ↓	WAF Rule ↓	WAF Events	Select All <input type="checkbox"/>
	Data Handling	Critical	/stuff/			No Defect	No	0	<input type="checkbox"/>
	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Critical	/demo/OSCommandInjection2.php	fileName		No Defect	Yes	46	<input type="checkbox"/>
	Improper Sanitization of Special Elements used in a Command ('Command Injection')	Critical	/demo/OSCommandInjection2.php	fileName	292	RESOLVED	No	0	<input type="checkbox"/>
3	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	Critical	/demo/OSCommandInjection2.php	fileName	292	RESOLVED	Yes	35	<input type="checkbox"/>
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/PathTraversal.php	action		No Defect	Yes	136	<input type="checkbox"/>
3	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/XPathInjection2.php	username		No Defect	Yes	35	<input type="checkbox"/>
3	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/XSS-reflected2.php	username		No Defect	Yes	30	<input type="checkbox"/>

Web Application Firewall Rules Are Generated

- ThreadFix now uses the vulnerability data to automatically generate additional Web Application Firewall (WAF) “virtual patch” rules designed to protect those specific applications and their vulnerabilities.
- Since the additional WAF rules are created based on real vulnerabilities, they greatly strengthen the protection offered by the firewall system.



The screenshot shows the ThreadFix web application interface. At the top left is the ThreadFix logo with the tagline "Powered by Denim Group". At the top right, it says "Logged in as: user | Logout". Below the logo is a navigation bar with four buttons: "Home", "WAFs", "Reports", and "Configuration". The "WAFs" button is highlighted. Below the navigation bar, there are three links: "100014 - fired 24 times", "100015 - fired 40 times", and "100016 - fired 0 times". Below these links is a section titled "WAF Rules:" with a "Download Waf Rules" button. The main content area displays a list of WAF rules in a code-like format, each consisting of a "SecRule REQUEST_URI" and a "SecRule ARGS:" line. The rules are designed to detect and deny various types of attacks, including Path Traversal, OS Command Injection, Cross-site Scripting (XSS), and Cross-site Scripting (XSS) attempts.

```
SecRule REQUEST_URI "^\/demo\/OSCommandInjection2\.php"phase:2,chain,deny,msg:'Path Traversal attempt: /demo/OSCommandInjection2.php [fileName]
SecRule ARGS:fileName ".|\%2e"

SecRule REQUEST_URI "^\/demo\/OSCommandInjection2\.php"phase:2,chain,deny,msg:'OS Command Injection attempt: /demo/OSCommandInjection2.php [fil
SecRule ARGS:fileName "%5b|\%7c|\%26|\%3b"

SecRule REQUEST_URI "^\/demo\/XPathInjection2\.php"phase:2,chain,deny,msg:'Cross-site Scripting attempt: /demo/XPathInjection2.php [username]',
SecRule ARGS:username "<|\%3c|\%3e"

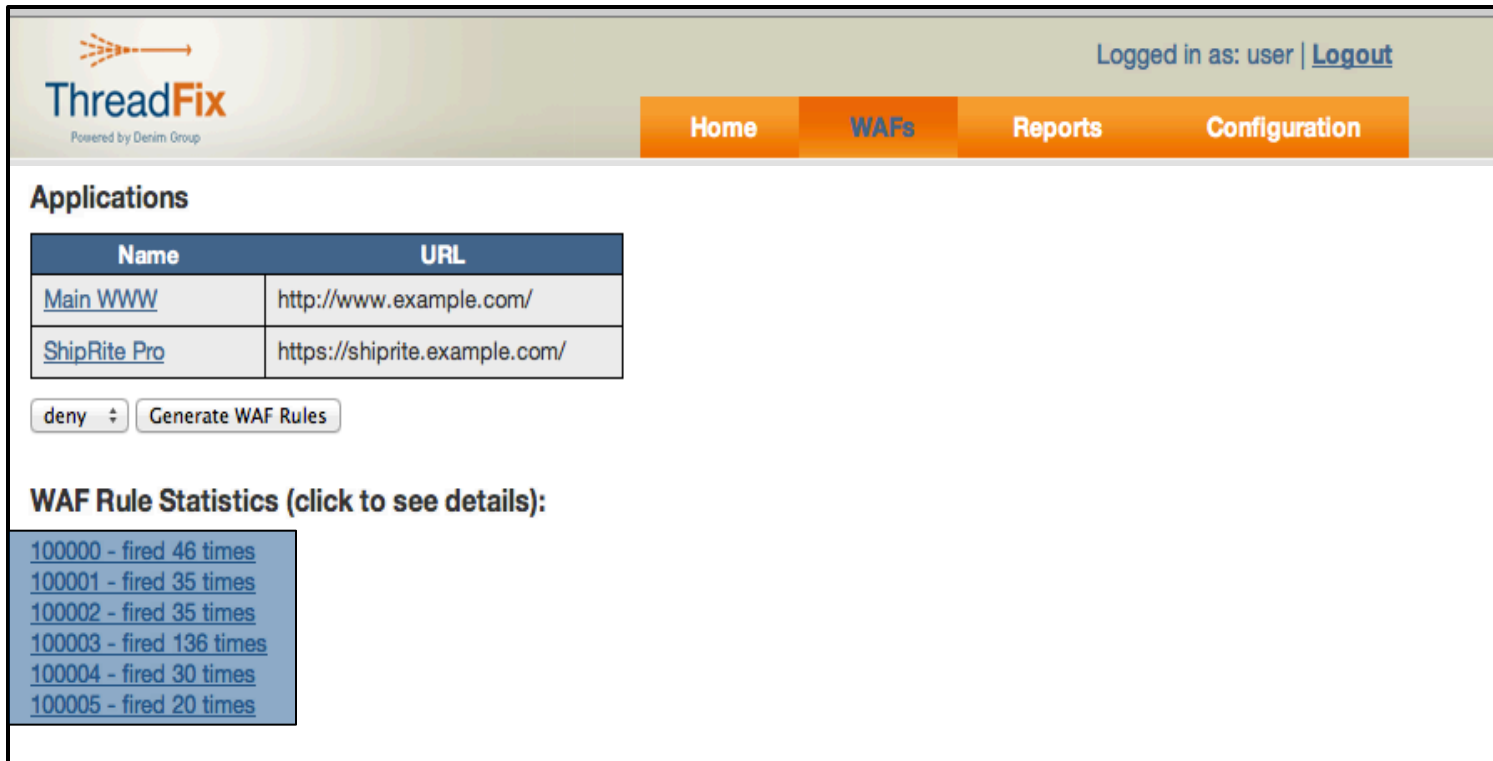
SecRule REQUEST_URI "^\/demo\/PathTraversal\.php"phase:2,chain,deny,msg:'Cross-site Scripting attempt: /demo/PathTraversal.php [action]',id:'10
SecRule ARGS:action "<|\%3c|\%3e"

SecRule REQUEST_URI "^\/demo\/XSS-reflected2\.php"phase:2,chain,deny,msg:'Cross-site Scripting attempt: /demo/XSS-reflected2.php [username]',ic
SecRule ARGS:username "<|\%3c|\%3e"

SecRule REQUEST_URI "^\/demo\/XPathInjection2\.php"phase:2,chain,deny,msg:'Cross-site Scripting attempt: /demo/XPathInjection2.php [password]',
SecRule ARGS:password "<|\%3c|\%3e"
```

Protecting the Application While It Is Vulnerable

- The WAF and Intrusion Detection Systems use the ThreadFix generated “virtual patch” rules to isolate application attacks.
- The ThreadFix user can analyze this attack data to further fine-tune the WAF to actively block application exploit attempts while the application is being fixed.
- Applications are susceptible to fewer risks as a result.



ThreadFix
Powered by Denim Group

Logged in as: user | [Logout](#)

Home WAFs Reports Configuration

Applications

Name	URL
Main WWW	http://www.example.com/
ShipRite Pro	https://shiprite.example.com/

deny ▾ Generate WAF Rules

WAF Rule Statistics (click to see details):

- [100000 - fired 46 times](#)
- [100001 - fired 35 times](#)
- [100002 - fired 35 times](#)
- [100003 - fired 136 times](#)
- [100004 - fired 30 times](#)
- [100005 - fired 20 times](#)

Attack Data Is Also Aggregated in ThreadFix

- The attack data is also imported into ThreadFix to present a more complete picture of the organization's security profile.

ThreadFix
Powered by Denim Group

Logged in as: user | [Logout](#)

Home WAFs Reports Configuration

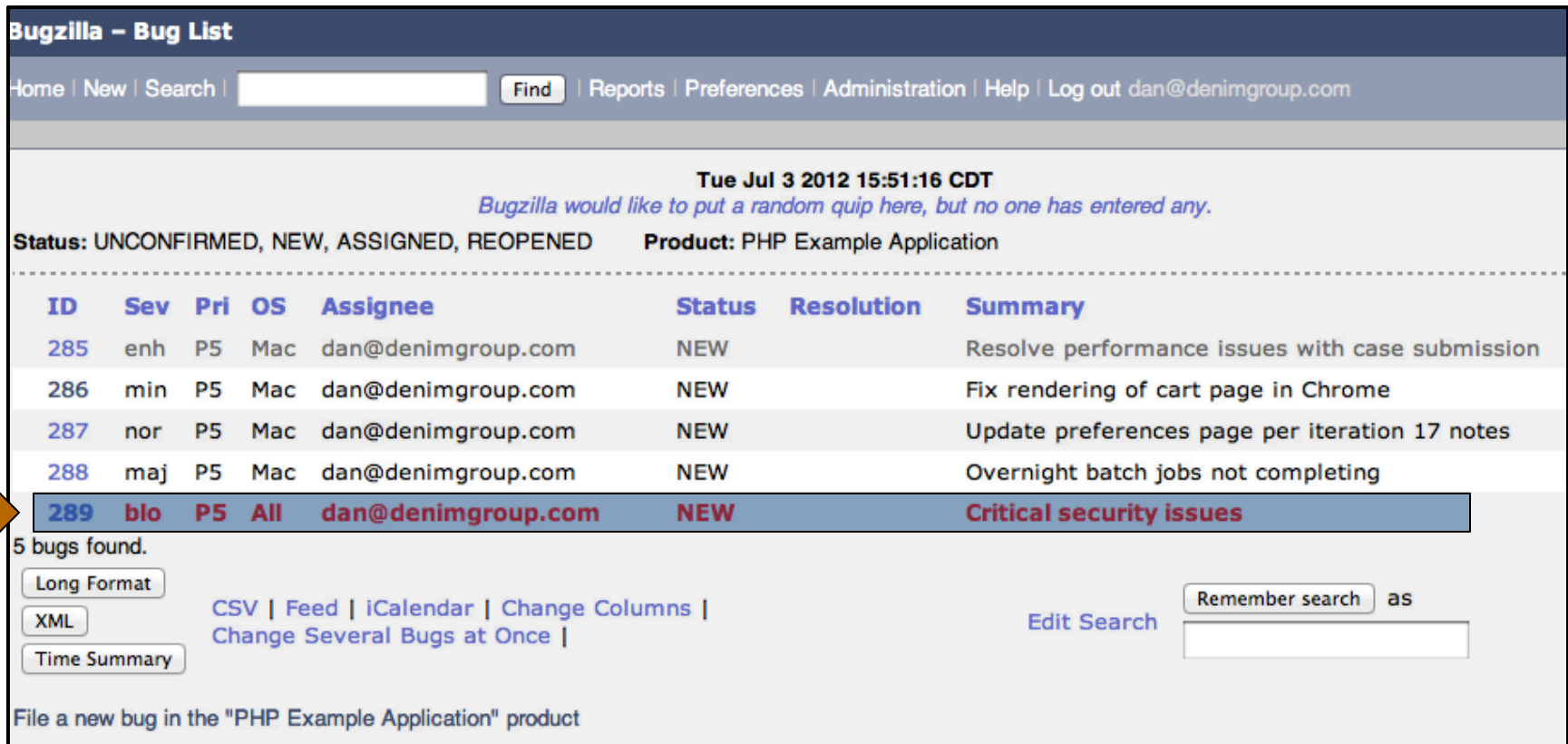
If Merged ↓	Vulnerability Name ↓	Severity ↓	Path ↓	Parameter ↓	Defect ↓	Defect Status ↓	WAF Rule ↓	WAF Events	Select All <input type="checkbox"/>
	Data Handling	Critical	/stuff/			No Defect	No	0	<input type="checkbox"/>
	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	Critical	/demo/OSCommandInjection2.php	fileName		No Defect	Yes	46	<input type="checkbox"/>
	Improper Sanitization of Special Elements used in a Command ('Command Injection')	Critical	/demo/OSCommandInjection2.php	fileName	292	RESOLVED	No	0	<input type="checkbox"/>
3	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	Critical	/demo/OSCommandInjection2.php	fileName	292	RESOLVED	Yes	35	<input type="checkbox"/>
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/PathTraversal.php	action		No Defect	No	136	<input type="checkbox"/>
3	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/XPathInjection2.php	username		No Defect	Yes	35	<input type="checkbox"/>
3	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/XSS-reflected2.php	username		No Defect	Yes	30	<input type="checkbox"/>
3	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/XPathInjection2.php	password		No Defect	Yes	20	<input type="checkbox"/>
3	Failure to Preserve Web Page Structure ('Cross-site Scripting')	Critical	/demo/EvalInjection2.php	command		No Defect	Yes	20	<input type="checkbox"/>

The Negotiations Begin

- The ThreadFix aggregated data report for the Auction application provides the basis needed to decide what is to be fixed and by who
- The security analyst and the eCommerce development team leader use the report which includes both vulnerability and attack data to decide which vulnerabilities will get fixed and which vulnerabilities represent an acceptable risk to the organization
- Next, the two team leaders agree on how to best package the targeted vulnerabilities for the development team
 - *By type (i.e. Cross Site Scripting vulnerabilities because it's more efficient to fix a class of vulnerabilities regardless of where they are located in the application.)*
 - *By developer (i.e. Joe created the user interface and is the only developer that knows how to work in that part of the application)*
 - *By severity (i.e. the critical vulnerabilities that need to be fixed now.)*
 - *Or any combination of the above*

The Defect Tracking System

- The security analyst exports vulnerabilities with Critical Severity to the Defect Tracking System which is Bugzilla in this example.
- The eCommerce development team then uses Bugzilla to keep track of the outstanding bugs and management tasks still to be done.



Bugzilla - Bug List

Home | New | Search | | Reports | Preferences | Administration | Help | Log out dan@denimgroup.com

Tue Jul 3 2012 15:51:16 CDT
Bugzilla would like to put a random quip here, but no one has entered any.

Status: UNCONFIRMED, NEW, ASSIGNED, REOPENED Product: PHP Example Application

ID	Sev	Pri	OS	Assignee	Status	Resolution	Summary
285	enh	P5	Mac	dan@denimgroup.com	NEW		Resolve performance issues with case submission
286	min	P5	Mac	dan@denimgroup.com	NEW		Fix rendering of cart page in Chrome
287	nor	P5	Mac	dan@denimgroup.com	NEW		Update preferences page per iteration 17 notes
288	maj	P5	Mac	dan@denimgroup.com	NEW		Overnight batch jobs not completing
289	blo	P5	All	dan@denimgroup.com	NEW		Critical security issues

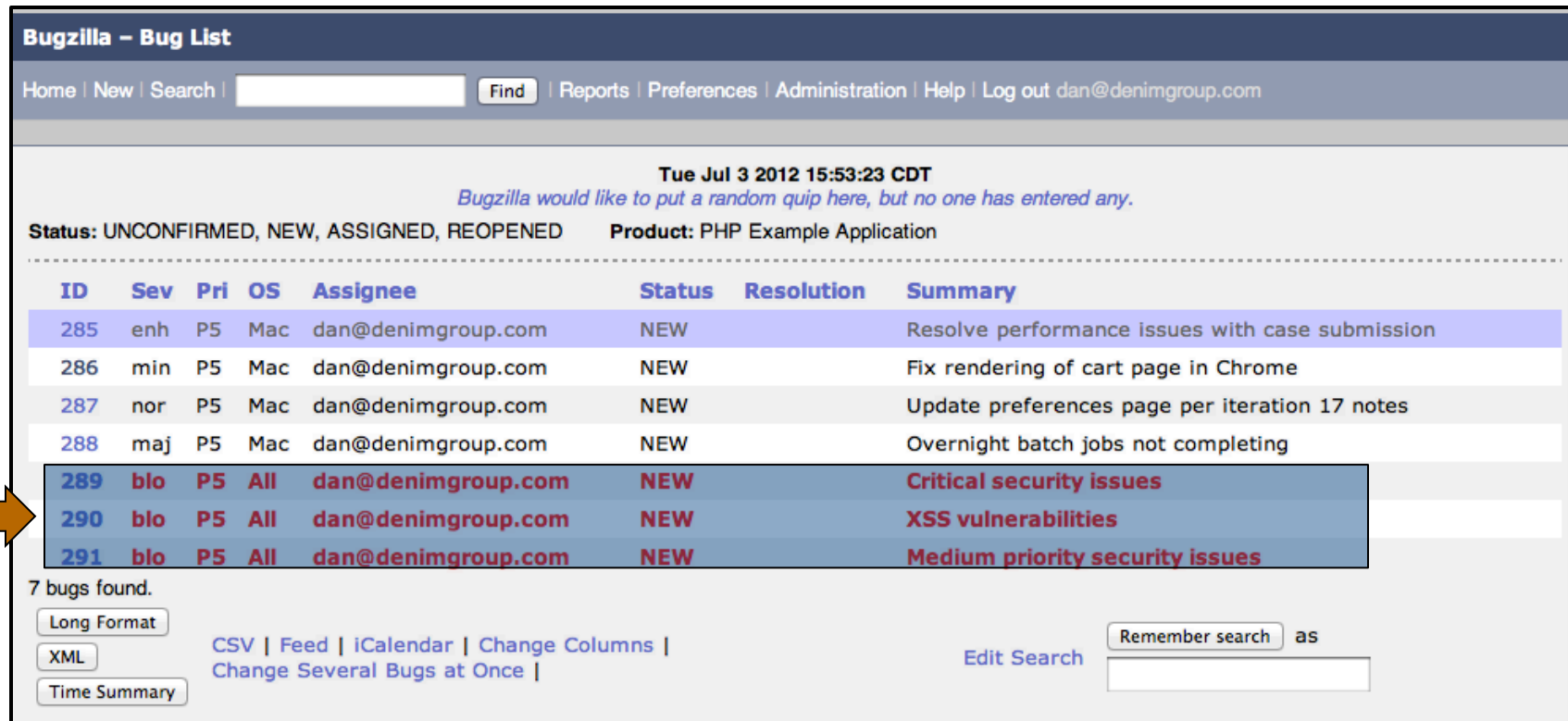
5 bugs found.

 [CSV](#) | [Feed](#) | [iCalendar](#) | [Change Columns](#) | [Change Several Bugs at Once](#) | [Edit Search](#) as

File a new bug in the "PHP Example Application" product

Vulnerabilities Now Become Defects

- All the vulnerabilities to be fixed are packaged in a manner that makes sense to the development team's work process.
- These vulnerabilities, which are now recognized as defects to software developers, are transferred to Bugzilla, the platform the development team is used to using.



Bugzilla - Bug List

Home | New | Search | | Reports | Preferences | Administration | Help | Log out dan@denimgroup.com

Tue Jul 3 2012 15:53:23 CDT
Bugzilla would like to put a random quip here, but no one has entered any.

Status: UNCONFIRMED, NEW, ASSIGNED, REOPENED Product: PHP Example Application

ID	Sev	Pri	OS	Assignee	Status	Resolution	Summary
285	enh	P5	Mac	dan@denimgroup.com	NEW		Resolve performance issues with case submission
286	min	P5	Mac	dan@denimgroup.com	NEW		Fix rendering of cart page in Chrome
287	nor	P5	Mac	dan@denimgroup.com	NEW		Update preferences page per iteration 17 notes
288	maj	P5	Mac	dan@denimgroup.com	NEW		Overnight batch jobs not completing
289	blo	P5	All	dan@denimgroup.com	NEW		Critical security issues
290	blo	P5	All	dan@denimgroup.com	NEW		XSS vulnerabilities
291	blo	P5	All	dan@denimgroup.com	NEW		Medium priority security issues

7 bugs found.

[CSV](#) | [Feed](#) | [iCalendar](#) | [Change Columns](#) | [Change Several Bugs at Once](#)

as


[Edit Search](#)

The Defect Categories & Status Inside of ThreadFix


- At the same time, the security analyst can see all of the open vulnerabilities as well as the defects they are linked to.
- Currently none of the bugs have been resolved by the development team.

ThreadFix <small>Powered by Denim Group</small>									
Logged in as: user Logout									
Home WAFs Reports Configuration									
If Merged ↓	Vulnerability Name ↓	Severity ↓	Path ↓	Parameter ↓	Defect ↓	Defect Status ↓	WAF Rule ↓	WAF Events	
2	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	Critical	/demo/OSCommandInjection2.php	fileName	289	OPEN	No	0	
	Failure to Control Generation of Code ('Code Injection')	Critical	/demo/EvalInjection2.php	command	289	OPEN	No	0	
Second Defect	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/XPathInjection2.php	password	290	OPEN	No	0	
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/EvalInjection2.php	command	290	OPEN	No	0	
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/XSS-reflected2.php	username	290	OPEN	No	0	
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/SQLI2.php	username	290	OPEN	No	0	
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/XPathInjection2.php	username	290	OPEN	No	0	
Third Defect	Improper Control of Resource Identifiers ('Resource Injection')	High	/demo/OSCommandInjection2.php	fileName	291	OPEN	No	0	
	Information Leak Through Include Source Code	Medium	/demo/OSCommandInjection2.php	fileName	291	OPEN	No	0	


First Defect



Second Defect



Third Defect



A Defect (Security Vulnerability) Is Fixed (Or is it?)

- The developers look into the bug containing the Critical vulnerabilities.
- They work with representatives from security to resolve the issue and then mark the bug as fixed in Bugzilla.

Bugzilla - Bug List

Home | New | Search | | Reports | Preferences | Administration | Help | Log out dan@denimgroup.com

Blocks:

Show dependency [tree](#) / [graph](#)

Orig. Est.	Current Est.	Hours Worked	Hours Left	%Complete	Gain	Deadline
<input type="text" value="0.0"/>	0.0	0.0 + <input type="text" value="0"/>	<input type="text" value="0.0"/>	0	0.0	<input type="text"/> (YYYY-MM-DD)

[Summarize time \(including time for bugs blocking this bug\)](#)

Attachments

[Add an attachment](#) (proposed patch, testcase, etc.)

Additional Comments:

Worked with Terry in security and the issues should be resolved. Please re-scan and we will deploy to

Status:

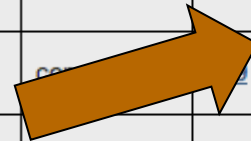
[Mark as Duplicate](#)



Bugzilla Updates Are Synchronized With ThreadFix

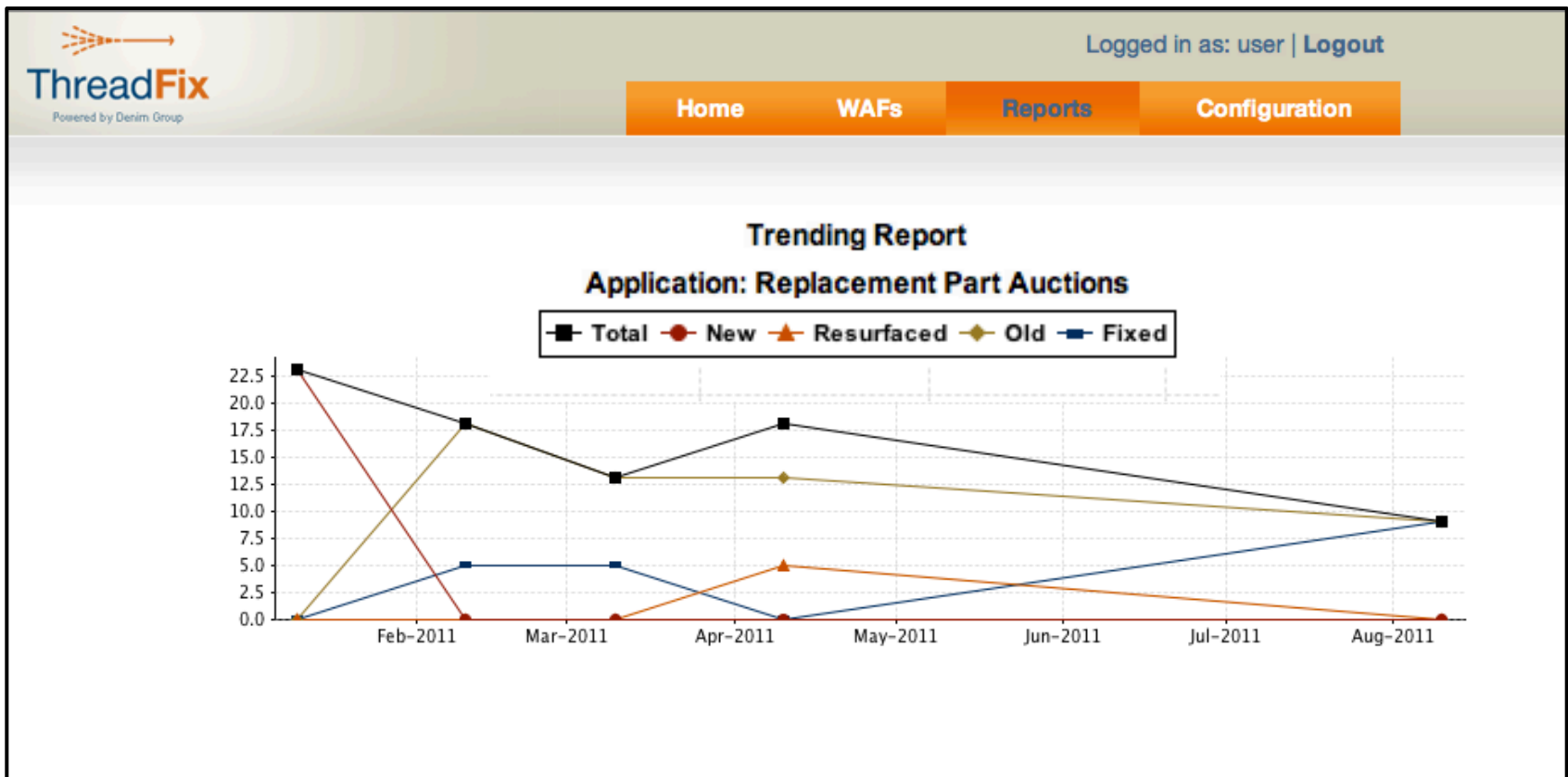
- When a ThreadFix update is performed, Bugzilla’s developer notes regarding bug status are synchronized with ThreadFix
- The security team then performs additional scans to confirm that the bugs have, indeed, been fixed.

ThreadFix <small>Powered by Denim Group</small>		Logged in as: user Logout						
		Home	WAFs	Reports	Configuration			
If Merged ↓	Vulnerability Name ↓	Severity ↓	Path ↓	Parameter ↓	Defect ↓	Defect Status ↓	WAF Rule ↓	WAF Events
2	Improper Sanitization of Special Elements used in an OS Command ('OS Command Injection')	Critical	/demo/OSCommandInjection2.php	fileName	289	RESOLVED	No	0
	Failure to Control Generation of Code ('Code Injection')	Critical	/demo/EvalInjection2.php	command	289	RESOLVED	No	0
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/XPathInjection2.php	password	290	NEW	No	0
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/EvalInjection2.php	command	290	NEW	No	0
	Failure to Preserve Web Page Structure ('Cross-site Scripting')	High	/demo/XSS-reflected2.php	username	290	NEW	No	0



Trending Reports Help Improve Quality

By repeating this process over time, the security teams can start to collect trending data about vulnerabilities as well as statistics of how long it is taking to resolve security issues.



ThreadFix Feature Summary

- **Vulnerability Import**
 - *Imports dynamic, static and manual testing results from a variety of sources (both commercial and freely-available scanning tools as well as SaaS testing providers)*
 - *Correlates and normalizes application vulnerabilities across different sources*
- **Defect Tracking Integration**
 - *Allows application security teams to group vulnerabilities into individual defects*
- **Real-Time Protection Generation**
 - *Virtual patching provides protection while code-level fixes are in development*
 - *Application-specific rules based upon identified vulnerabilities*
- **Application Portfolio Management**
 - *Tracks security status of applications across the enterprise*
 - *Enables critical communication with developers in tools they are already using*
- **Maturity Evaluation**
 - *Store and report on software security program progress*
 - *Benchmarks security improvement against industry standards*

ThreadFix Benefits

- Reduces the time required to fix vulnerable applications.
- Dramatically simplifies the effort required
- Compares the relative performance and test coverage of application vulnerability scanning technologies.
- Provides centralized visibility into current security state of applications as well as trending
- Facilitates communication between security analysts and development teams
- Provides enterprise-wide software security metrics in support of benchmarking and budget justification efforts
- No licensing fees
- Open community support

Where to Get ThreadFix

- Go to <http://code.google.com/p/threadfix/> and download the zip file.
- Click on the Threadfix.bat icon in Windows, or, in Linux, navigate to the folder and execute `bash threadfix.sh`.
- Go on the wiki and open the “Getting Started” file for more step by step directions.
- For more information, go to <http://www.denimgroup.com/threadfix>

Contact Information

Dan Cornell

Principal and CTO

dan@denimgroup.com

Twitter [@danielcornell](https://twitter.com/danielcornell)

(210) 572-4400

www.denimgroup.com

www.threadstrong.com

blog.denimgroup.com