



Czy masz pewność, że Twoja strona jest bezpieczna

Czy chcesz szybko i tanio znaleźć podatności i luki w zabezpieczeniach

Czy chcesz mieć łatwy i zdalny dostęp do skanowanych danych

Acunetix w chmurze (Vulnerability Scanner)

Od grudnia 2019 roku Acunetix wzbogacił swoją ofertę o rozwiązanie dedykowane w chmurze pod nazwą Acunetix 360.

Czym jest Acunetix 360?

Acunetix 360 to **zautomatyzowany, w pełni konfigurowalny, skaner bezpieczeństwa aplikacji internetowych**, który umożliwia skanowanie stron internetowych, aplikacji internetowych i serwisów w celu zidentyfikowania wad w bezpieczeństwie. Acunetix 360 skanuje wszystkie rodzaje aplikacji niezależnie od platformy lub języka, w którym są napisane.

Acunetix 360 to najszybszy skaner bezpieczeństwa aplikacji internetowych, który automatycznie skanuje aplikację internetową, identyfikuje i zgłasza wszelkie luki w zabezpieczeniu z minimalną liczbą fałszywych trafień.

Technologia skanowania Acunetix 360 została stworzona, by pomóc w prostym zabezpieczeniu aplikacji bez zbędnego zamieszania, dzięki czemu można skupić się na naprawie zgłoszonych luk.

Zalety Acunetix 360

Dostęp do danych z każdego dowolnego miejsca, korzystając z sieci internetowej

Brak konieczności wykonywania kopii zapasowych

Wysoka dostępność rozwiązania

Oszczędności finansowe – brak konieczności posiadania zasobów sprzętowych

Łatwiejsza konfiguracja z rozwiązaniami chmurowymi – np. AWS

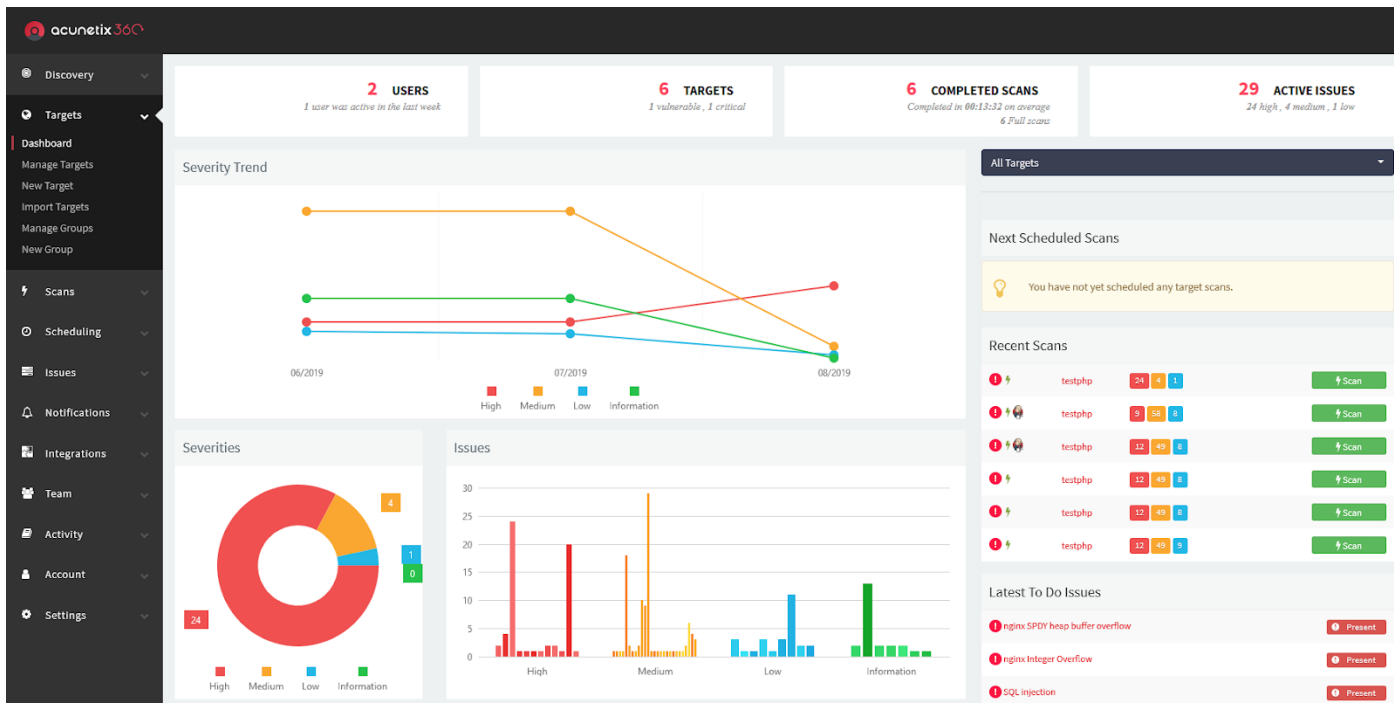
O Acunetix 360

Technologia Indeksowania i Skanowania

Acunetix 360 wykorzystuje wiodącą w branży technologię skanowania w zakresie wykrywania podatności i luk w zabezpieczeniach.

Web Security Scanner

Acunetix 360 to platforma dla wielu użytkowników, która ma pomóc przedsiębiorstwom w zarządzaniu długoterminowym bezpieczeństwem tysięcy stron internetowych. Wbudowane narzędzia pomagają również zautomatyzować większość zadań już po skanowaniu, takich jak zarządzanie podatnościami, co pozwala zespołom współpracować z większą wydajnością i precyzją.



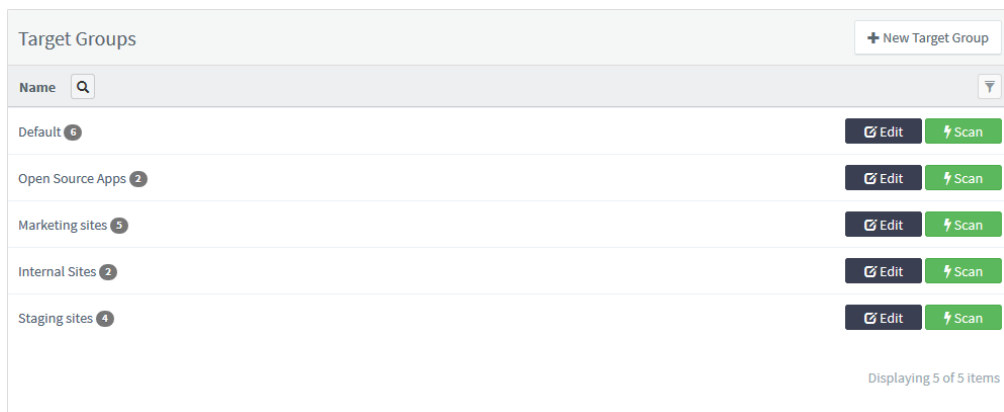
Skalowalność usługi

Acunetix 360 jest hostowany na infrastrukturze chmury Amazon (AWS), dzięki czemu pozwala w nieograniczony sposób wykorzystywać zasoby chmury.

Podobną skalowalność można uzyskać dzięki Acunetix 360 On Premise, który daje możliwość dodania wielu mechanizmów skanowania. Dzięki temu można wybrać interesujące klienta opcje skanowania.

Wyróżnienie funkcji: Grupy witryn

Acunetix 360 umożliwia grupowanie stron internetowych, konfigurowanie ogólnych ustawień skanowania oraz uruchamianie lub planowanie skanowania bezpieczeństwa sieci za pomocą jednego kliknięcia.



Praca zespołowa

Acunetix 360 to środowisko dla wielu użytkowników. Każdy członek zespołu ma własną nazwę użytkownika na koncie Acunetix 360 i może uruchamiać skanowanie bezpieczeństwa aplikacji internetowych, przeglądać raporty i podatności. Administrator może skonfigurować różne uprawnienia dla każdego użytkownika.

Manage Team				+ New Team Member	My Account
Name	Email	User State			
Admin	admin@domain.local	Enabled		Edit	
Joe Doe	joedoe@domain.local	Enabled		Edit	
Mark Moe	markmoe@domain.local	Enabled		Edit	
Larry Loe	larrylow@domain.local	Enabled		Edit	

Displaying 4 of 4 items

Issue		Report	Send To
Issue	Blind SQL Injection		
Issue URL	/sendcommand.php		
Target Name	testphp (http://testphp.vulnweb.com/)		
Severity	High		
State	Present		
First Seen	14/08/2019 12:39 PM		
Last Seen	14/08/2019 12:39 PM		
Assignee	Joe Doe		
Update			
State			
<input checked="" type="radio"/> Accepted Risk <input type="radio"/> False Positive <input type="radio"/> Fixed (Unconfirmed)			
Assignee			
Joe Doe			
Note			
<div style="border: 1px solid #ccc; height: 40px;"></div>			
Save			

Najważniejsze funkcje: Zarządzanie lukami i zadaniami

Podobnie jak dedykowane systemy śledzenia błędów, Acunetix 360 pozwala przypisać zidentyfikowane luki w zabezpieczeniach jako zadania do naprawy dla członków zespołu. Jest to niezbędna funkcja podczas śledzenia bezpieczeństwa wielu aplikacji internetowych.

Zadania oznaczone jako naprawione są automatycznie skanowane ponownie. W zależności od wyniku są one albo zamknięte, albo ponownie otwarte i ponownie przypisane.

System zarządzania podatnością na zagrożenia został zaprojektowany tak, aby każdy użytkownik wiedział, co powinien zrobić, a wyniki i poprawki były sprawdzane automatycznie. Można także zintegrować istniejące rozwiązanie do śledzenia błędów.

Issues									
Title	Severity	Target Group	Target	URL	First Seen	Last Seen	Assignee	Status	
AngularJS client-side template injection	High	Default Marketing sites Staging sites	testhtml5	http://testhtml5.vulnweb.com/contact	13/05/2019 10:47 AM	13/05/2019 10:47 AM	Admin	Present	
AngularJS client-side template injection	High	Default Marketing sites Staging sites	testhtml5	http://testhtml5.vulnweb.com/contact	13/05/2019 10:47 AM	13/05/2019 10:47 AM	Admin	Present	
Blind SQL Injection	High	Default Internal Sites Staging sites	testphp	http://testphp.vulnweb.com/sendcomman...	14/08/2019 12:39 PM	14/08/2019 12:39 PM	Joe Doe	Present	
Blind SQL Injection	High	Default Internal Sites Staging sites	testphp	http://testphp.vulnweb.com/userinfo.php	14/08/2019 12:38 PM	14/08/2019 12:38 PM	Admin	Present	
Blind SQL Injection	High	Default Internal Sites Staging sites	testphp	http://testphp.vulnweb.com/userinfo.php	14/08/2019 12:38 PM	14/08/2019 12:38 PM	Admin	Present	

Skanowanie zabezpieczeń aplikacji sieci Web na karcie SDLC

Acunetix 360 można łatwo zintegrować z procesami SDLC i Continuous Integration. Ma rozbudowany i dobrze udokumentowany interfejs API, którego można użyć do uruchomienia dowolnego rodzaju akcji dostępnych na pulpicie nawigacyjnym.

Dbanie o bezpieczeństwo aplikacji internetowych

Uruchomienie pojedynczego skanu zabezpieczeń aplikacji sieci Web i usunięcie zidentyfikowanych luk może być dość trudne. Jeszcze bardziej wymagające jest częste skanowanie wszystkich aplikacji internetowych i upewnienie się, że wykryte luki zostały usunięte, a zastosowane poprawki nie otwierają nowych luk w zabezpieczeniach. Acunetix 360 jest rozwiązaniem dla tych problemów.

Raporty dotyczące trendów i skorelowane są automatycznie aktualizowane przy każdym skanowaniu strony internetowej lub aplikacji internetowej. To eliminuje potrzebę ręcznego porównywania wyników.

Trend Matrix Report - testphp									
HTTP://TESTPHPVULNWEB.COM/	PARAMETER	METHOD	ISSUE	24/07/2019 01:06 PM	24/07/2019 03:02 PM	14/08/2019 05:23 PM			
			nginx SPDY heap buffer overflow	Not Fixed	Not Fixed	Not Fixed			
			nginx Integer Overflow	Not Fixed	Not Fixed	Not Fixed			
		GET	Macromedia Dreamweaver remote database scripts	Not Fixed	Not Fixed	Not Fixed			
		GET	Insecure crossdomain.xml file	Not Fixed	Not Fixed	Not Fixed			
		GET	HTML form without CSRF protection	Not Fixed	Not Fixed	Not Fixed			
		GET	JetBrains .idea project directory	Not Fixed	Not Fixed	Not Fixed			
/		GET	User credentials are sent in clear text	Not Fixed	Not Fixed	Not Fixed			
		GET	Clickjacking: X-Frame-Options header missing	Not Fixed	Not Fixed	Not Fixed			
			Possible virtual host found	Not Fixed	Not Fixed	Not Fixed			
		GET	Content Security Policy (CSP) not implemented	Not Fixed	Not Fixed	Not Fixed			
			Email address found	Not Fixed	Not Fixed	Not Fixed			
		GET	Password type input with auto-complete enabled	Not Fixed	Not Fixed	Not Fixed			
		POST	SQL injection	Not Fixed	Not Fixed	Not Fixed			
		POST	Cross site scripting (Verified)	Not Fixed	Not Fixed	Not Fixed			



Przemysław Błatkiewicz – tel. +48 22 100 10 60, +48 507 005 496, przemyslaw.blatkiewicz@biztech.pl
 Leszek Ryciuk – tel. +48 507 005 481, leszek.ryciuk@biztech.pl
 Andrzej Snopek – tel. +48 507 005 478, andrzej.snopek@biztech.pl