BUGCROWD'S

VULNERABILITY RATING TAXONOMY

Bugcrowd is proud to release our VRT, a valuable resource for both researchers and customers to better understand the technical rating we use to classify vulnerabilities. This report details how and why we created the VRT, and a usage guide to accompany the taxonomy itself.

v0.4.0 - November 18, 2016

THE METHODOLOGY

At the beginning 2016, we released the Bugcrowd Vulnerability Rating Taxonomy (VRT) in an effort to further bolster transparency and communication, as well as to contribute valuable and actionable content to the bug bounty community.

Bugcrowd's VRT is a resource outlining Bugcrowd's baseline priority rating, including certain edge cases, for vulnerabilities that we see often. To arrive at this baseline priority, Bugcrowd's security engineers started with generally accepted industry impact and further considered the average acceptance rate, average priority, and commonly requested program-specific exclusions (based on business use cases) across all of Bugcrowd's programs.

Implications For Bug Hunters

Bugcrowd's VRT is an invaluable resource for bug hunters as it outlines the types of issues that are normally seen and accepted by bug bounty programs. We hope that being transparent about the typical priority level for various bug types will help bug bounty participants save valuable time and effort in their quest to make bounty targets more secure. The VRT can also help researchers identify which types of high-value bugs they have overlooked, and when to provide exploitation information (POC info) in a report where it might impact priority.

Interested in becoming a Bugcrowd researcher? **Join the crowd.**

Implications For Customers

The VRT helps customers gain a more comprehensive understanding of bug bounties. Not only will our customers be better able to understand priorities and their impact better, but this also helps them write better bounty briefs, adjust bounty scope, and communicate more clearly about bugs. In the fixing stage, the VRT will help business units across the board in communicating about and remediating the identified security issues. For more information on our priority rating and worth of a bug, **read our recently launched guide "What's A Bug Worth."**

USAGE GUIDE:

The VRT is intended to provide valuable information for bug bounty stakeholders. It is important that we identify the ways in which we use it successfully, and what considerations should be kept in mind.

Priority is a Baseline

The **recommended priority, from Priority 1 (P1) to Priority 5 (P5)**, is a baseline. That having been said, while this baseline priority might apply without context, it's possible that application complexity, bounty brief restrictions, or unusual impact could result in a different rating. As a customer, it's important to weigh the VRT alongside your internal application security ratings.

For bug hunters, if you think a bug's impact warrants reporting despite the VRT's guidelines, or that the customer has misunderstood the threat scenario, we encourage you to submit the issue regardless and use the **Bugcrowd Crowdcontrol** commenting system to clearly communicate your reasoning.

Low Priority Does not Imply Insignificance

For customers, it's important to recognize that base priority does not equate to "industry accepted impact." Base priority is defined by our Technical Operations Team and our VRT is a living document - see the following point about a "Vulnerability Roundtable." Your internal teams or engineers might assess certain bugs – especially those designated P4 or P5 within the VRT – differently. **Read more about our vulnerability prioritization.** As a bug hunter, it's important to not discount lower priority bugs, as many bug hunters have used such bugs within "exploit chains" consisting of two or three bugs resulting in creative, valid, and high-impact submissions.

Importance of a Vulnerability Roundtable

Bugcrowd reviews proposed changes to the VRT every week at an operations meeting called the "Vulnerability Roundtable." We use this one-hour meeting to discuss new vulnerabilities, edge cases for existing vulnerabilities, priority level adjustments, and to share general bug validation knowledge. When the team comes to a consensus regarding each proposed change, it is committed to the master version. Members of the Technical Operations team look forward to this meeting each week, as examining some of the most difficult to validate bugs serves as a unique learning exercise.

This specific document will be updated externally on a quarterly basis.

Communication is King

Having cut-and-dry baseline ratings as defined by our VRT, makes rating bugs a faster and less difficult process. We have to remember, however, that strong communication is the most powerful tool for anyone running or participating in a bug bounty.

Both sides of the bug bounty equation must exist in balance. When in doubt, ask dumb questions, be verbose, and more generally, behave in a way that allows you and your bounty opposite to foster a respectful relationship.
As a customer, keep in mind that every bug takes time and effort to find.
As a bounty hunter, try to remember that every bug's impact is ultimately determined by the customer's environment and use cases.

One Size Doesn't Fit All

As the version of the VRT we have released only covers some web and mobile application vulnerabilities, it should be viewed as a foundation. Any vulnerability taxonomy would look much more robust with the addition of IoT, reverse engineering, network level, and other vulnerability categories – most of which have been validated and triaged by Bugcrowd in the past.

In addition, while this taxonomy maps bugs to the OWASP Top Ten and the OWASP Mobile Top Ten to add more contextual information, additional meta-data could include CWE or WASC, among others. As always, the program owner retains all rights to choose final bug prioritization levels.

Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P1	A1 - Injection	File Inclusion	Local
	A1 - Injection	Remote Code Execution (RCE)	
	A1 - Injection	SQL Injection	Error-Based
	A1 - Injection	SQL Injection	Blind
	A1 - Injection	XML External Entity Injection (XXE)	
	A2 - Broken Authentication and Session Management	Authentication Bypass	Vertical
	A4 - Insecure Direct Object References (IDOR)	Insecure Direct Object Reference (IDOR)	Critical Function
	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	Critical Impact
	A5 - Security Misconfiguration	Using Default Credentials	Production Server
	A6 - Sensitive Data Exposure	Critically Sensitive Data	Password Disclosure
	A6 - Sensitive Data Exposure	Critically Sensitive Data	Private API Keys
	I2 - Insufficient Authentication/Authorization	Cryptographic Flaw	Incorrect Usage
	I6 - Insecure Cloud Interface	Insecure Direct Object Reference (IDOR)	Critical API Function
	I9 - Insecure Software/Firmware	Command Injection	
	I9 - Insecure Software/Firmware	Hardcoded Password	Privileged User
P2	A2 - Broken Authentication and Session Management	Authentication Bypass	Horizontal
	A3 - Cross-Site Scripting (XSS)	Stored	Non-Admin to Anyone
	A4 - Insecure Direct Object References (IDOR)	Insecure Direct Object Reference (IDOR)	Important Function
	A4 - Insecure Direct Object References (IDOR)	Server-Side Request Forgery (SSRF)	Internal
	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	High Impact
	A5 - Security Misconfiguration	Misconfigured DNS	Subdomain Takeover
	A5 - Security Misconfiguration	Using Default Credentials	Staging/Development Server
	A8 - Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Critical Function
	B1 - Application-Level Denial-of-Service (DoS)	Critical Impact and/or Easy Difficulty	
	I1 - Insecure Web Interface	Insecure Data Storage	Password
	I6 - Insecure Cloud Interface	Insecure Direct Object Reference (IDOR)	Important API Function
	I9 - Insecure Software/Firmware	Hardcoded Password	Non-Privileged User
P3	A1 - Injection	HTTP Response Manipulation	Response Splitting (CRLF)
	A1 - Injection	Content Spoofing	iframe Injection
	A10 - Unvalidated Redirects and Forwards	Open Redirect	GET-Based (Unauthenticated)

BUGCROWD'S VRT

v0.4.0 - November 18, 2016

Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P3 CONTINUED	A2 - Broken Authentication and Session Management	Weak Login Function	Over HTTP
	A2 - Broken Authentication and Session Management	Session Fixation	With POC (of Account Takeover)
	A3 - Cross-Site Scripting (XSS)	Stored	Admin to Anyone
	A3 - Cross-Site Scripting (XSS)	Reflected	Non-Admin to Anyone
	A4 - Insecure Direct Object References (IDOR)	Insecure Direct Object Reference (IDOR)	Unimportant Function
	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	Medium Impact
	A5 - Security Misconfiguration	Mail Server Misconfiguration	Missing SPF on Email Domain
	A5 - Security Misconfiguration	Mail Server Misconfiguration	Email Spoofable Via Third-Party API Misconfiguration
	A5 - Security Misconfiguration	Weak Password Policy	Complexity, Both Length and Char Type Not Enforced
	A5 - Security Misconfiguration	No Rate Limiting on Form	Login
	A6 - Sensitive Data Exposure	EXIF Geolocation Data Not Stripped From Uploaded Images	Automatic User Enumeration
	A6 - Sensitive Data Exposure	Visible Detailed Error Page	Critical Information
	A8 - Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Important Function
	B1 - Application-Level Denial-of-Service (DoS)	High Impact and/or Medium Difficulty	
	I6 - Insecure Cloud Interface	Insecure Direct Object Reference (IDOR)	Unimportant API Function
P4			
	A1 - Injection	Reflected File Download	On Domain
	A1 - Injection	Content Spoofing	External Authentication Injection
	A1 - Injection	Content Spoofing	Email HTML Injection
	A10 - Unvalidated Redirects and Forwards	Open Redirect	GET-Based (Authenticated)
	A10 - Unvalidated Redirects and Forwards	Open Redirect	POST-Based (Unauthenticated)
	A2 - Broken Authentication and Session Management	Failure to Invalidate Session	On Logout
	A2 - Broken Authentication and Session Management	Failure to Invalidate Session	On Password Reset
	A2 - Broken Authentication and Session Management	Failure to Invalidate Session	On Password Change
	A2 - Broken Authentication and Session Management	Session Token in URL	Over HTTP
	A2 - Broken Authentication and Session Management	Weak Registration Implementation	Over HTTP
	A3 - Cross-Site Scripting (XSS)	Reflected	Admin to Anyone
	A3 - Cross-Site Scripting (XSS)	Cookie-Based	
	A3 - Cross-Site Scripting (XSS)	IE-Only	Older Version (IE 10/11)
	A3 - Cross-Site Scripting (XSS)	Referer	With POC
	A3 - Cross-Site Scripting (XSS)	Universal (UXSS)	With POC
	A3 - Cross-Site Scripting (XSS)	Off-Domain	Data URI
	A4 - Insecure Direct Object References (IDOR)	Server-Side Request Forgery (SSRF)	External

BUGCROWD'S VRT

v0.4.0 - November 18, 2016

Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P4 CONTINUED	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	Low Impact
	A5 - Security Misconfiguration	Same-Site Scripting	With POC
	A5 - Security Misconfiguration	Lack of Password Confirmation	Change Email Address
	A5 - Security Misconfiguration	Lack of Password Confirmation	Change Password
	A5 - Security Misconfiguration	Lack of Password Confirmation	Delete Account
	A5 - Security Misconfiguration	No Rate Limiting on Form	Registration
	A5 - Security Misconfiguration	No Rate Limiting on Form	Email-Triggering
	A5 - Security Misconfiguration	Unsafe File Upload	No Antivirus
	A5 - Security Misconfiguration	Unsafe File Upload	No Size Limit
	A5 - Security Misconfiguration	Weak Password Policy	Complexity, Length Not Enforced
	A5 - Security Misconfiguration	Weak Password Policy	Complexity, Char Type Not Enforced
	A5 - Security Misconfiguration	Weak Password Reset Implementation	Token is Not Invalidated After Use
	A5 - Security Misconfiguration	Lack of Security Header	Cache-Control for a Sensitive Page
	A5 - Security Misconfiguration	Missing Secure or HTTPOnly Cookie Flag	With POC (that Token is Session Token)
	A5 - Security Misconfiguration	Clickjacking for Sensitive Action	With POC
	A5 - Security Misconfiguration	OAuth Misconfiguration	Missing State Parameter
	A5 - Security Misconfiguration	Captcha Bypass	Implementation Vulnerability
	A6 - Sensitive Data Exposure	Visible Detailed Error Page	Important Information
	A6 - Sensitive Data Exposure	Sensitive Token in URL	
	A6 - Sensitive Data Exposure	EXIF Geolocation Data Not Stripped From Uploaded Images	Manual User Enumeration
	A6 - Sensitive Data Exposure	Weak Password Reset Implementation	Password Reset Token Sent Over HTTP
	A6 - Sensitive Data Exposure	Token Leakage via Referer	Over HTTP
	A6 - Sensitive Data Exposure	Mixed Content	Sensitive Data Disclosure
	A7 - Missing Function Level Access Control	Username Enumeration	Data Leak
	A8 - Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Unimportant Function
	A9 - Using Components with Known Vulnerabilities	Rosetta Flash	With POC
	I3 - Insecure Network Services	Telnet Enabled	Credentials Required
	I5 - Privacy Concerns	Unnecessary Data Collection	WiFi SSID+Password
	M2 - Insecure Data Storage	Credentials Stored Unencrypted	On External Storage
	M2 - Insecure Data Storage	Sensitive Application Data Stored Unencrypted	On External Storage
	M4 - Unintended Data Leakage	Improper Export of Android Application Components	With POC
v0.4.0 - November 18, 2016	M5 - Poor Authorization and Authentication	Change Account Data Without Password	

BUGCROWD'S VRT

Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P5	A1 - Injection	CSV Injection	
	A1 - Injection	Reflected File Download	Off Domain
	A1 - Injection	Content Spoofing	Text Injection
	A1 - Injection	Content Spoofing	Homograph/IDN-Based
	A10 - Unvalidated Redirects and Forwards	Open Redirect	POST-Based (Authenticated)
	A10 - Unvalidated Redirects and Forwards	Open Redirect	Tabnabbing
	A10 - Unvalidated Redirects and Forwards	Open Redirect	Header-Based
	A2 - Broken Authentication and Session Management	Concurrent Logins	
	A2 - Broken Authentication and Session Management	Failure to Invalidate Session	All Sessions
	A2 - Broken Authentication and Session Management	Failure to Invalidate Session	On Email Change
	A2 - Broken Authentication and Session Management	Session Token in URL	Over HTTPS
	A2 - Broken Authentication and Session Management	Session Fixation	Without POC (of Account Takeover)
	A2 - Broken Authentication and Session Management	Failure to Invalidate Session	Long Timeout
	A3 - Cross-Site Scripting (XSS)	Stored	Self
	A3 - Cross-Site Scripting (XSS)	Reflected	Self
	A3 - Cross-Site Scripting (XSS)	TRACE Method	
	A3 - Cross-Site Scripting (XSS)	Universal (UXSS)	Without POC
	A3 - Cross-Site Scripting (XSS)	IE-Only	XSS Filter Disabled
	A3 - Cross-Site Scripting (XSS)	IE-Only	Older Version (< IE10)
	A3 - Cross-Site Scripting (XSS)	Referer	Without POC
	A5 - Security Misconfiguration	Unsafe Cross-Origin Resource Sharing	No Impact
	A5 - Security Misconfiguration	Same-Site Scripting	Without POC
	A5 - Security Misconfiguration	SSL Attack (BREACH, POODLE etc.)	Without POC
	A5 - Security Misconfiguration	Browser Feature	Plaintext Password Field
	A5 - Security Misconfiguration	Browser Feature	Save Password
	A5 - Security Misconfiguration	Browser Feature	Autocomplete Enabled
	A5 - Security Misconfiguration	Browser Feature	Autocorrect Enabled
	A5 - Security Misconfiguration	Browser Feature	Aggressive Offline Caching
	A5 - Security Misconfiguration	Mail Server Misconfiguration	Missing SPF on Non-Email Domain
	A5 - Security Misconfiguration	Mail Server Misconfiguration	SPF Uses a Soft Fail
	A5 - Security Misconfiguration	Mail Server Misconfiguration	SPF Includes > 10 Lookups
	A5 - Security Misconfiguration	Mail Server Misconfiguration	Missing DMARC

BUGCROWD'S VRT

Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P5 CONTINUED	A5 - Security Misconfiguration	Exposed Admin Portal	To Internet
	A5 - Security Misconfiguration	Unsafe File Upload	File Extension Filter Bypass
	A5 - Security Misconfiguration	Weak Password Reset Implementation	Token is Not Invalidated After Email Change
	A5 - Security Misconfiguration	Weak Password Reset Implementation	Token is Not Invalidated After Password Change
	A5 - Security Misconfiguration	Missing Secure or HTTPOnly Cookie Flag	Non-Session Cookie
	A5 - Security Misconfiguration	Clickjacking for Sensitive Action	Without POC
	A5 - Security Misconfiguration	Clickjacking for Non-Sensitive Action	
	A5 - Security Misconfiguration	Lack of Verification Email	
	A5 - Security Misconfiguration	Lack of Notification Email	
	A5 - Security Misconfiguration	Missing DNSSEC	
	A5 - Security Misconfiguration	Weak Password Policy	Allows Reuse of Old Passwords
	A5 - Security Misconfiguration	Weak Password Policy	Allows Password to be Same as Email/Username
	A5 - Security Misconfiguration	Weak Password Reset Implementation	Token Has Long Timed Expiry
	A5 - Security Misconfiguration	Weak Password Reset Implementation	Token is Not Invalidated After New Token is Requested
	A5 - Security Misconfiguration	Lack of Security Speed Bump Page	
	A5 - Security Misconfiguration	Captcha Bypass	Brute Force
	A5 - Security Misconfiguration	Captcha Bypass	OCR (Optical Character Recognition)
	A5 - Security Misconfiguration	Captcha Bypass	Crowdsourcing
	A5 - Security Misconfiguration	Username Enumeration	Brute Force
	A5 - Security Misconfiguration	Potentially Unsafe HTTP Method Enabled	OPTIONS
	A5 - Security Misconfiguration	Potentially Unsafe HTTP Method Enabled	TRACE
	A5 - Security Misconfiguration	Insecure SSL	Lack of Forward Secrecy
	A5 - Security Misconfiguration	Insecure SSL	Insecure Cipher Suite
	A5 - Security Misconfiguration	Lack of Security Headers	X-Frame-Options
	A5 - Security Misconfiguration	Lack of Security Headers	Cache-Control for a Non-Sensitive Page
	A5 - Security Misconfiguration	Lack of Security Headers	X-XSS-Protection
	A5 - Security Misconfiguration	Lack of Security Headers	Strict-Transport-Security
	A5 - Security Misconfiguration	Lack of Security Headers	X-Content-Type-Options
	A5 - Security Misconfiguration	Lack of Security Headers	Content-Security-Policy
	A5 - Security Misconfiguration	Lack of Security Headers	Public-Key-Pins
	A5 - Security Misconfiguration	Lack of Security Headers	X-Content-Security-Policy
	A5 - Security Misconfiguration	Lack of Security Headers	X-Webkit-CSP
	A5 - Security Misconfiguration	Lack of Security Headers	Content-Security-Policy-Report-Only
	A5 - Security Misconfiguration	Weak Registration Implementation	Allows Disposable Email Addresses

BUGCROWD'S VRT

Priority	OWASP Top Ten + Bugcrowd Extras	Specific Vulnerability Name	Variant or Affected Function
P5 CONTINUED	A5 - Security Misconfiguration	Weak 2FA Implementation	Missing Failsafe
	A6 - Sensitive Data Exposure	Visible Detailed Error Page	Unimportant Information
	A6 - Sensitive Data Exposure	Disclosure of Known Public Information	
	A6 - Sensitive Data Exposure	Token Leakage via Referer	Over HTTPS
	A6 - Sensitive Data Exposure	Non-Sensitive Token in URL	
	A6 - Sensitive Data Exposure	Mixed Content	Requires Being a Man-in-the-Middle
	A8 - Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)	Irrelevant Function (or Public Form)
	A9 - Using Components with Known Vulnerabilities	Outdated Software Version	Without POC
	B2 - Design Decision	Parameter Pollution	Social Media Sharing Buttons
	M10 - Lack of Binary Protections	Lack of Exploit Mitigations	
	M10 - Lack of Binary Protections	Lack of Jailbreak Detection	
	M10 - Lack of Binary Protections	Lack of Obfuscation	
	M10 - Lack of Binary Protections	Runtime Instrumentation-Based	
	M2 - Insecure Data Storage	Credentials Stored Unencrypted	On Internal Storage
	M2 - Insecure Data Storage	Sensitive Application Data Stored Unencrypted	On Internal Storage
	M2 - Insecure Data Storage	Non-Sensitive Application Data Stored Unencrypted	
	M3 - Insufficient Transport Layer Protection	SSL Certificate Pinning	Absent
	M3 - Insufficient Transport Layer Protection	SSL Certificate Pinning	Defeatable
	M4 - Unintended Data Leakage	Sensitive Data Hardcoded	OAuth Secret
	M4 - Unintended Data Leakage	Sensitive Data Hardcoded	File Paths
	M4 - Unintended Data Leakage	System Clipboard Leak	Shared Links
	M4 - Unintended Data Leakage	Improper Export of Android Application Components	Without POC
	M4 - Unintended Data Leakage	Screen Caching Enabled	
	M4 - Unintended Data Leakage	User Password Persisted in Memory	
	M8 - Security Decisions Via Untrusted Inputs	App Crash	Malformed Android Intents
	M8 - Security Decisions Via Untrusted Inputs	App Crash	Malformed iOS URL Schemes

BUGCROWD'S VRT

A NOTE FROM OUR TECHNICAL OPERATIONS TEAM

We believe in growth and transparency for security and bug bounty communities and see the release of our VRT as a tool that may help align expectations between researchers and program owners across ALL programs. Much of our employees' expertise in validating and rating thousands of submissions across hundreds of managed bounties is distilled into this document, making it a key component of Bugcrowd's managed services. Our internal VRT is a living document that changes constantly in response to discussions at our Vulnerability Roundtable, so specific priority ratings and notes are frequently updated.

As our first and foremost goal is usability, the VRT is not exhaustive. We believe that foregoing extreme technical depth for usability in creating such a community resource is a worthwhile tradeoff. We're confident that a security engineer using our VRT as a guide can triage and run a successful bug bounty program.

Happy Hunting,

Bugcrowd Technical Operations Team

Follow us at **@BugcrowdOps** and continue the discussion on **our forum.**

UPDATES

0.1.0 - February 5, 2016 (PDF)
Original

0.2.0 - March 23, 2016 (PDF)
Divided the Cross-Site Scripting (XSS) entries to provide additional granularity that captures priority variations for XSS within applications with multiple user privilege levels. Documentation **here**.

0.4.0 - November 18, 2016 (current)
Minor priority changes, minor additions and subtractions, and typo fixes. Switched to a formal versioning system now.