Public HackerOne (https://hackerone.com) bug reports.

2,696 Bug Reports - **$1,137,264** Paid Out - Last Updated: **12th November, 2016**
★ **1st Place:** Uber (https://hackerone.com/uber) ($174,700 Paid Out)
★ **2nd Place:** Shopify (https://hackerone.com/shopify) ($92,000 Paid Out)
★ **3rd Place:** The Internet (https://hackerone.com/internet) ($87,000 Paid Out)

Highest Bounty Paid: $20,000 by **Pornhub** for [phpobject in cookie] Remote shell/command execution (https://hackerone.com/reports/141956)

Show Bounties Only (bounties.html)

Team	Bounty	Title
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	DMARC Not found for paragonie.com URGENT (https://hackerone.com/reports/179828)
Blockchain (https://hackerone.com/blockchain)	$100	Information disclosure at https://blockchain.atlassian.net (https://hackerone.com/reports/179599)
Brave Software (https://hackerone.com/brave)	-	Denial of service(POP UP Recursion) on Brave browser (https://hackerone.com/reports/179248)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	[Airship CMS] Local File Inclusion - RST Parser (https://hackerone.com/reports/179034)
GitLab (https://hackerone.com/gitlab)	-	Read files on application server, leads to RCE (https://hackerone.com/reports/178152) **CVE-2016-9086** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9086)
HackerOne (https://hackerone.com/security)	-	Information disclosure via policy update notifications after removal from program (https://hackerone.com/reports/177484)
Nextcloud (https://hackerone.com/nextcloud)	-	Content spoofing due to the improper behavior of the 403 page in Private Server (https://hackerone.com/reports/177335)
OLX (https://hackerone.com/olx)	-	Reflective XSS at m.olx.ph (https://hackerone.com/reports/177230)
Mindoktor (https://hackerone.com/mindoktor)	$2,000	XSS at endpoint clinic.mindoktor.se in flash cookie (https://hackerone.com/reports/177041)

Team	Bounty	Title
Mindoktor (https://hackerone.com/mindoktor)	$300	Storing sensitive information on cookie post-registration (https://hackerone.com/reports/177018)
Brave Software (https://hackerone.com/brave)	$50	[ios] Address bar spoofing in Brave for iOS (https://hackerone.com/reports/176929)
Brave Software (https://hackerone.com/brave)	-	DOS in browser using window.print() function (https://hackerone.com/reports/176364)
Brave Software (https://hackerone.com/brave)	$100	Denial of service attack(window object) on brave browser (https://hackerone.com/reports/176197)
Brave Software (https://hackerone.com/brave)	-	[iOS] URI Obfuscation in iOS application (https://hackerone.com/reports/176159)
Shopify (https://hackerone.com/shopify) ★	$500	race condition in adding team members (https://hackerone.com/reports/176127)
Brave Software (https://hackerone.com/brave)	-	JavaScript URL Issues in the latest version of Brave Browser (https://hackerone.com/reports/176083)
Brave Software (https://hackerone.com/brave)	-	Javascript confirm() crashes Brave on PC (https://hackerone.com/reports/176076)
OLX (https://hackerone.com/olx)	-	Reflected XSS in OLX.in (https://hackerone.com/reports/175801)
Brave Software (https://hackerone.com/brave)	$100	Address Bar Spoofing - Already resolved - Retroactive report (https://hackerone.com/reports/175779)
Brave Software (https://hackerone.com/brave)	-	Status Bar Obfuscation (https://hackerone.com/reports/175701)
Brave Software (https://hackerone.com/brave)	$150	URI Obfuscation (https://hackerone.com/reports/175529)
Twitter (https://hackerone.com/twitter)	$140	Full Path Disclosure at 27.prd.vine.co (https://hackerone.com/reports/175451)
OLX (https://hackerone.com/olx)	-	Reflected XSS at m.olx.ph (https://hackerone.com/reports/175410)
Brave Software (https://hackerone.com/brave)	$50	[website] Script injection in newsletter signup https://brave.com/brave_youth_program_signup.html (https://hackerone.com/reports/175403)
Brave Software (https://hackerone.com/brave)	-	Subdomain Takeover of Brave.com (https://hackerone.com/reports/175397)

Team	Bounty	Title
Brave Software (https://hackerone.com/brave)	$100	Homograph attack (https://hackerone.com/reports/175286)
Yelp (https://hackerone.com/yelp)	$500	Requesting Show CheckIn Alert for Non Friend User (https://hackerone.com/reports/174882)
Trello (https://hackerone.com/trello)	$128	XSS on blog.trello.com (https://hackerone.com/reports/174729)
Badoo (https://hackerone.com/badoo)	$140	No rate-limit in SERVER_SECURITY_CHECK (https://hackerone.com/reports/174668)
HackerOne (https://hackerone.com/security)	-	Possible CSRF during external programs (https://hackerone.com/reports/174470)
Zopim (https://hackerone.com/zopim)	$150	Full Sub Domain Takeover at wx.zopim.net (https://hackerone.com/reports/174395)
Romit (https://hackerone.com/romit)	$513	[CRITICAL]-Taking over entire subdomain of romit.io (https://hackerone.com/reports/173681)
Algolia (https://hackerone.com/algolia)	-	Possilbe Sub Domain takever at prestashop.algolia.com (https://hackerone.com/reports/173417)
RubyGems (https://hackerone.com/rubygems)	-	Login credentials transmitted in cleartext on index.rubygems.org (https://hackerone.com/reports/173268)
RubyGems (https://hackerone.com/rubygems)	-	Password Reset emails missing TLS leads account takeover (https://hackerone.com/reports/173251)
Legal Robot (https://hackerone.com/legalrobot)	$40	Bypass 8 chars password complexity with 6 chars only due to insecure password reset functionaliy (https://hackerone.com/reports/173195)
HackerOne (https://hackerone.com/security)	-	Obtain the username & the uid of the one doing the S3 sync on Hackerone (https://hackerone.com/reports/173175)
Shopify (https://hackerone.com/shopify) ★	$500	password less login token expiration issue (https://hackerone.com/reports/172837)
WebSummit (https://hackerone.com/websummit)	-	WebSummit - Open Redirect (https://hackerone.com/reports/172746)
Shopify (https://hackerone.com/shopify) ★	$500	Add signature to transactions without any permission (https://hackerone.com/reports/172733)
itBit Exchange (https://hackerone.com/itbit)	-	Open Redirect in https://exchange.itbit.com - False Positive (https://hackerone.com/reports/172696)

Team	Bounty	Title
Ian Dunn (https://hackerone.com/iandunn-projects)	-	All Plugins - Direct file access to plugin files Vulnerability (https://hackerone.com/reports/172618)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	Google Authenticator0.6 - PHP Version Dosclosure (https://hackerone.com/reports/172609)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	Google Authenticator - Cross Site Scripting (https://hackerone.com/reports/172606)
LocalTapiola (https://hackerone.com/localtapiola)	$50	Reflected XSS in LTContactFormReceiver (/cs/Satellite) (https://hackerone.com/reports/172595)
Automattic (https://hackerone.com/automattic)	$100	Follow Button XSS (https://hackerone.com/reports/172574)
Trello (https://hackerone.com/trello)	-	Unvalidated/Open Redirect allowing attackers to implement phishing attack (https://hackerone.com/reports/172363)
Legal Robot (https://hackerone.com/legalrobot)	$20	Information Disclosure on rate limit defense mechanism (https://hackerone.com/reports/172296)
Trello (https://hackerone.com/trello)	-	Subdomain Take over & username enemuration (https://hackerone.com/reports/172024)
Snapchat (https://hackerone.com/snapchat)	-	Subdomain takeover of blog.snapchat.com (https://hackerone.com/reports/171942)
OLX (https://hackerone.com/olx)	-	Name, email, phone and more disclosure on user ID (API) (https://hackerone.com/reports/171917)
CodeIgniter (https://hackerone.com/codeigniter)	-	Link sanitation bypass in xss_clean() (https://hackerone.com/reports/171670)
Nextcloud (https://hackerone.com/nextcloud)	-	Content spoofing in lookup.nextcloud.com (https://hackerone.com/reports/171497)
HackerOne (https://hackerone.com/security)	-	(HackerOne SSO-SAML) Login CSRF, Open Redirect, and Self-XSS Possible Exploitation (https://hackerone.com/reports/171398)
ownCloud (https://hackerone.com/owncloud)	-	Accessable Htaccess (https://hackerone.com/reports/171272)
OLX (https://hackerone.com/olx)	-	Full path disclosure vulnerability at http://corporate.olx.ph (https://hackerone.com/reports/171048)

Team	Bounty	Title
RubyGems (https://hackerone.com/rubygems)	-	Invalid username updating (https://hackerone.com/reports/170301)
Trello (https://hackerone.com/trello)	$128	SSRF in account webhook (through API) (https://hackerone.com/reports/170151)
Slack (https://hackerone.com/slack)	$400	Email information leakage for certain addresses (https://hackerone.com/reports/169992)
Skyliner (https://hackerone.com/skyliner)	-	DNSSEC misconfiguration (https://hackerone.com/reports/169704)
IRCCloud (https://hackerone.com/irccloud)	$50	Exposed, outdated nginx server (v1.4.6) potentially vulnerable to heap-based buffer overflow & RCE (https://hackerone.com/reports/168485)
Snapchat (https://hackerone.com/snapchat)	$250	Incoming email hijacking on sc-cdn.net (https://hackerone.com/reports/168476)
Uber (https://hackerone.com/uber) ★	$500	Users can falsely declare their own Uber account info on the monthly billing application (https://hackerone.com/reports/168453)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Not clearing hex-decoded variable after usage in Authentication (https://hackerone.com/reports/168293)
Coinbase (https://hackerone.com/coinbase)	-	coinbase Email leak while sending and requesting (https://hackerone.com/reports/168289)
Boozt Fashion AB (https://hackerone.com/boozt)	-	Http header injection (https://hackerone.com/reports/168254)
Nextcloud (https://hackerone.com/nextcloud)	-	Unauthenticated Stored xss (https://hackerone.com/reports/168054)
Zomato (https://hackerone.com/zomato)	-	[CRITICAL] Complete source code disclosure via exposed Jenkins Dashboard (https://hackerone.com/reports/167859)
Shopify (https://hackerone.com/shopify) ★	$500	Deleted Post and Administrative Function Access in eCommerce Forum (https://hackerone.com/reports/167846)
HackerOne (https://hackerone.com/security)	-	Ability to enumerate private programs using SAML (https://hackerone.com/reports/167828)
New Relic (https://hackerone.com/newrelic)	-	HOST HEADER INJECTION in rpm.newrelic.com (https://hackerone.com/reports/167809)
Boozt Fashion AB (https://hackerone.com/boozt)	$80	Make victim buy in attacker's account without any idea - http://www.booztlet.com/ (https://hackerone.com/reports/167731)

Team	Bounty	Title
Python (https://hackerone.com/ibb-python)	$1,000	msilib.OpenDatabase Type Confusion (https://hackerone.com/reports/167688)
Boozt Fashion AB (https://hackerone.com/boozt)	-	Host header poisoning leads to account password reset links hijacking (https://hackerone.com/reports/167631)
Pornhub (https://hackerone.com/pornhub)	$750	Unsecured Grafana instance (https://hackerone.com/reports/167585)
Pornhub (https://hackerone.com/pornhub)	$750	Disclosure of private photos/albums - http://www.pornhub.com/album/show_image_box (https://hackerone.com/reports/167582)
Yelp (https://hackerone.com/yelp)	$200	Bybass The Closing of the account and logged again to your account (https://hackerone.com/reports/167489)
Eobot (https://hackerone.com/eobotcom)	$12	No password length restriction (https://hackerone.com/reports/167351)
Boozt Fashion AB (https://hackerone.com/boozt)	$120	XSS (https://hackerone.com/reports/167321)
OLX (https://hackerone.com/olx)	-	XSS and Open Redirect on https://jobs.dubizzle.com/ (https://hackerone.com/reports/167107)
Shopify (https://hackerone.com/shopify) ★	$500	XSS in SHOPIFY: Unsanitized Supplier Name can lead to XSS in Transfers Timeline (https://hackerone.com/reports/167075)
Shopify (https://hackerone.com/shopify) ★	$500	Unsanitized Location Name in POS Channel can lead to XSS in Orders Timeline (https://hackerone.com/reports/166887)
Boozt Fashion AB (https://hackerone.com/boozt)	$80	Instance of Apache Vulnerable to Several Issues (https://hackerone.com/reports/166871)
Boozt Fashion AB (https://hackerone.com/boozt)	$120	Potential Subdomain Takeover Possible (https://hackerone.com/reports/166826)
WebSummit (https://hackerone.com/websummit)	-	Reflected xss on websummit.net (https://hackerone.com/reports/166699)
Keybase (https://hackerone.com/keybase)	$100	Denial of Service through set_preference.json (https://hackerone.com/reports/166682)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	SSLv2 doesn't block disabled ciphers (CVE-2015-3197) (https://hackerone.com/reports/166634)

Team	Bounty	Title
OpenSSL (https://hackerone.com/ibb-openssl)	$2,500	Cross-protocol attack on TLS using SSLv2 (DROWN) (CVE-2016-0800) (https://hackerone.com/reports/166629)
Yelp (https://hackerone.com/yelp)	$500	Verification of E-Mail address possible on https://biz.yelp.com/login and https://biz.yelp.com/forgot (https://hackerone.com/reports/166265)
Boozt Fashion AB (https://hackerone.com/boozt)	-	No csrf protection on logout (https://hackerone.com/reports/165923)
Boozt Fashion AB (https://hackerone.com/boozt)	-	User Enumeration. (https://hackerone.com/reports/165894)
Harvest (https://hackerone.com/harvest)	$500	Invoices can be added to any retainers - even closs-platform (https://hackerone.com/reports/165862)
OLX (https://hackerone.com/olx)	-	Bypassing Phone Verification For Posting AD On OLX (https://hackerone.com/reports/165854)
Mindoktor (https://hackerone.com/mindoktor)	$500	Vulnerable Mobile Phone configuration (https://hackerone.com/reports/165712)
Shopify (https://hackerone.com/shopify) ★	-	Subdomain Takeover in http://genghis-cdn.shopify.io/ pointing to Fastly (https://hackerone.com/reports/165309)
Mapbox (https://hackerone.com/mapbox)	-	target="_blank" Vulnerability Resulting in Critical Phishing Vector (https://hackerone.com/reports/165136)
Python (https://hackerone.com/ibb-python)	$1,000	urllib HTTP header injection CVE-2016-5699 (https://hackerone.com/reports/165102)
Shopify (https://hackerone.com/shopify) ★	$500	Access to Splunk via shard3-db2.ec2.shopify.com endpoint (https://hackerone.com/reports/165048)
Shopify (https://hackerone.com/shopify) ★	$500	Open redirect allows changing iframe content in *.myshopify.com/admin/themes/<id>/editor (https://hackerone.com/reports/165046)
Algolia (https://hackerone.com/algolia)	$100	Hyperlink Injection in Friend Invitation Emails (https://hackerone.com/reports/164833)
LocalTapiola (https://hackerone.com/localtapiola)	$400	SQL Injection on `/cs/Satellite` path (https://hackerone.com/reports/164739)
Ian Dunn (https://hackerone.com/iandunn-projects)	$50	CSV Injection in Camptix (https://hackerone.com/reports/164674)

Team	Bounty	Title
Nextcloud (https://hackerone.com/nextcloud)	-	Reflected Self-XSS Vulnerability in the Comment section of Files (Different-payloads) (https://hackerone.com/reports/164520)
Phabricator (https://hackerone.com/phabricator)	-	link reset problem (https://hackerone.com/reports/164483)
Udemy (https://hackerone.com/udemy)	-	NON VALIDATION OF SESSIONS AFTER PASSWORD CHANGE (https://hackerone.com/reports/164239)
Legal Robot (https://hackerone.com/legalrobot)	$20	Possible content spoofing due to missing error page (https://hackerone.com/reports/164137)
Mail.Ru (https://hackerone.com/mailru)	-	Reflected XSS @ games.mail.ru (https://hackerone.com/reports/164039)
Nextcloud (https://hackerone.com/nextcloud)	$100	Reflected Self-XSS Vulnerability in the Comment section of Files Information (https://hackerone.com/reports/164027)
Slack (https://hackerone.com/slack)	$2,500	Snooping into messages via email service (https://hackerone.com/reports/163938)
Legal Robot (https://hackerone.com/legalrobot)	-	Click Jacking (https://hackerone.com/reports/163888)
Legal Robot (https://hackerone.com/legalrobot)	$20	unsecured legalrobot.co.uk assets (https://hackerone.com/reports/163885)
Nextcloud (https://hackerone.com/nextcloud)	-	Slow Http attack on nextcloud(DOS) (https://hackerone.com/reports/163823)
Instacart (https://hackerone.com/instacart)	-	[Critical] Subdomain Takeover (https://hackerone.com/reports/163790)
Legal Robot (https://hackerone.com/legalrobot)	-	UI Redressing (ClickJacking) Issue on Information submit form (https://hackerone.com/reports/163753)
Dropbox (https://hackerone.com/dropbox)	-	XSS in OAuth Redirect Url (https://hackerone.com/reports/163707)
Legal Robot (https://hackerone.com/legalrobot)	-	2 vulns (https://hackerone.com/reports/163677)
Legal Robot (https://hackerone.com/legalrobot)	$20	Legal | Application is Missing CSP(Content Security Policy) Header (https://hackerone.com/reports/163676)

Team	Bounty	Title
Legal Robot (https://hackerone.com/legalrobot)	-	Clickjacking: X-Frame-Options header missing (https://hackerone.com/reports/163646)
Legal Robot (https://hackerone.com/legalrobot)	-	Amazon Bucket Accessible (http://legalrobot.s3.amazonaws.com/) (https://hackerone.com/reports/163599)
New Relic (https://hackerone.com/newrelic)	-	Java RMI (Remote Code Execution) (https://hackerone.com/reports/163547)
Legal Robot (https://hackerone.com/legalrobot)	-	Email spoofing-fake mail from your mail domain server (https://hackerone.com/reports/163501)
Legal Robot (https://hackerone.com/legalrobot)	$20	CORS (Cross-Origin Resource Sharing) (https://hackerone.com/reports/163491)
Legal Robot (https://hackerone.com/legalrobot)	$20	Information Disclosure in AWS S3 Bucket (https://hackerone.com/reports/163476)
Legal Robot (https://hackerone.com/legalrobot)	$120	User Information leak allows user to bypass email verification. (https://hackerone.com/reports/163467)
Legal Robot (https://hackerone.com/legalrobot)	$120	User Information sent to client through websockets (https://hackerone.com/reports/163464)
Nextcloud (https://hackerone.com/nextcloud)	-	Wordpress: Directory Traversal / Denial of Serivce (https://hackerone.com/reports/163421)
Nextcloud (https://hackerone.com/nextcloud)	-	Expired SSL certificate (https://hackerone.com/reports/163342)
New Relic (https://hackerone.com/newrelic)	-	Cookie Misconfiguration (https://hackerone.com/reports/163227)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Email Spoofing With Your Website's Email (https://hackerone.com/reports/163156)
HackerOne (https://hackerone.com/security)	-	Users contents on AWS is cacheable (https://hackerone.com/reports/163131)
Skyliner (https://hackerone.com/skyliner)	-	[skyliner.io / qa.skyliner.io] Open Redirect (https://hackerone.com/reports/163124)
Nextcloud (https://hackerone.com/nextcloud)	-	Information Disclosure of .htaccess file in Private Server/Subdomain (https://hackerone.com/reports/163106)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	$100	Stealing users password (Limited Scenario) (https://hackerone.com/reports/163067)
Instacart (https://hackerone.com/instacart)	$150	Fetch private list metadata and any user's personal name (https://hackerone.com/reports/162822)
Uber (https://hackerone.com/uber) ★	$5,000	Changing paymentProfileUuid when booking a trip allows free rides (https://hackerone.com/reports/162809)
OLX (https://hackerone.com/olx)	-	XSS and HTML Injection https://sharjah.dubizzle.com/ (https://hackerone.com/reports/162296)
GitLab (https://hackerone.com/gitlab)	-	Boards leak private label names and desciptions (https://hackerone.com/reports/162147)
Gratipay (https://hackerone.com/gratipay)	-	Cross Site Scripting In Profile Statement (https://hackerone.com/reports/162120)
Shopify (https://hackerone.com/shopify) ★	$500	Open Redirect possible in https://www.shopify.com/admin/ (https://hackerone.com/reports/161991)
Certly (https://hackerone.com/certly)	-	Non secure requests at guard.certly.io not upgrading to https (https://hackerone.com/reports/161932)
Nextcloud (https://hackerone.com/nextcloud)	-	Password Reset Link issue (https://hackerone.com/reports/161924)
Gratipay (https://hackerone.com/gratipay)	-	Reset Link Issue (https://hackerone.com/reports/161918)
Airbnb (https://hackerone.com/airbnb)	-	[redacted] discloses valid Airbnb SSO login names via Google Search Results (https://hackerone.com/reports/161659)
Gratipay (https://hackerone.com/gratipay)	-	XSS Via Method injection (https://hackerone.com/reports/161621)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	Potentially vulnerable version of Apache software in and default files on https://iandunn.name/ (https://hackerone.com/reports/161459)
Bime (https://hackerone.com/bime)	$150	Subdomain takeover at ws.bimedb.com due to unclaimed Amazon S3 bucket (https://hackerone.com/reports/161428)
Mail.Ru (https://hackerone.com/mailru)	-	[cfire.mail.ru] CSRF Bypassed - Changing anyone's 'User Info' (https://hackerone.com/reports/161408)
Nextcloud (https://hackerone.com/nextcloud)	-	Content Injection - demo.nextcloud.com (https://hackerone.com/reports/161323)

Team	Bounty	Title
Nextcloud (https://hackerone.com/nextcloud)	-	Content Injection - apps.nextcloud.com (https://hackerone.com/reports/161299)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	bypass to csv injection (https://hackerone.com/reports/161290)
Ian Dunn (https://hackerone.com/iandunn-projects)	$100	Bypass fix in https://hackerone.com/reports/151516 report. (https://hackerone.com/reports/160520)
Ian Dunn (https://hackerone.com/iandunn-projects)	$50	Bypassing CSV injection using new line charcter (https://hackerone.com/reports/160500)
Coinbase (https://hackerone.com/coinbase)	$300	window.opener is leaking to external domains upon redirect on Safari (https://hackerone.com/reports/160498)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	stored SELF xss on Basic Google Maps Placemarks Settings plugin (https://hackerone.com/reports/160488)
Instacart (https://hackerone.com/instacart)	-	API OAuth Public Key disclosure in mobile app (https://hackerone.com/reports/160120)
Instacart (https://hackerone.com/instacart)	$150	Brute force login and bypass locked account restrictions via iOS app (https://hackerone.com/reports/160109)
Shopify (https://hackerone.com/shopify) ★	$500	[apps.shopify.com] Open Redirect (https://hackerone.com/reports/160047)
Mail.Ru (https://hackerone.com/mailru)	-	[realty.mail.ru] XSS, SSI Injection (https://hackerone.com/reports/159985)
GitLab (https://hackerone.com/gitlab)	-	XSS On meta tags in profile page (https://hackerone.com/reports/159984)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	Send emails to all users using Camptix (https://hackerone.com/reports/159925)
HackerOne (https://hackerone.com/security)	-	Ability to monitor reports' submission in real time (https://hackerone.com/reports/159890)
Instacart (https://hackerone.com/instacart)	$150	Issues with uploading list images (https://hackerone.com/reports/159820)
Shopify (https://hackerone.com/shopify) ★	$500	Open CouchDB on experiments.ec2.shopify.com:5984 (https://hackerone.com/reports/159536)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	$500	Information leakage of private program (https://hackerone.com/reports/159526)
Shopify (https://hackerone.com/shopify) ★	$500	Open redirect using checkout_url (https://hackerone.com/reports/159522)
HackerOne (https://hackerone.com/security)	$500	Requesting Mediation possible on reports that are too old for mediation (https://hackerone.com/reports/159512)
OLX (https://hackerone.com/olx)	-	full path disclosure vulnerability at https://security.olx.com/* (https://hackerone.com/reports/159481)
Harvest (https://hackerone.com/harvest)	$150	Unauthorized read access to Invoices by PM (Access control Issues) (https://hackerone.com/reports/159399)
Harvest (https://hackerone.com/harvest)	$150	Unauthorized access to all the actions of invoices by PM (Access control Issues) (https://hackerone.com/reports/159395)
Harvest (https://hackerone.com/harvest)	$100	PM can delete payment of any invoice in company (Access control Issue) (https://hackerone.com/reports/159393)
Harvest (https://hackerone.com/harvest)	$100	Record payment for any invoice by PM (Access control Issue) (https://hackerone.com/reports/159391)
Harvest (https://hackerone.com/harvest)	$100	PM can delete the company logo image (Vertical Privilege Escalation) (https://hackerone.com/reports/159387)
OLX (https://hackerone.com/olx)	-	Full Account Takeover (https://hackerone.com/reports/159202)
HackerOne (https://hackerone.com/security)	$1,000	Hacker.One Subdomain Takeover (https://hackerone.com/reports/159156)
Harvest (https://hackerone.com/harvest)	$250	PM with can Set up email for invoices and estimates (Access control Issue) (https://hackerone.com/reports/158979)
OLX (https://hackerone.com/olx)	-	[Critical] Delete any account (https://hackerone.com/reports/158872)
Binary.com (https://hackerone.com/binary)	$75	Cross site scripting (https://hackerone.com/reports/158757)
Instacart (https://hackerone.com/instacart)	$100	Hyperlink Injection in Friend Invitation Emails (https://hackerone.com/reports/158554)
Instacart (https://hackerone.com/instacart)	-	Reflected File Download on recipe list search (https://hackerone.com/reports/158505)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	-	Attacker could setup reminder remotely using brute force (https://hackerone.com/reports/158393)
GitLab (https://hackerone.com/gitlab)	-	Ability to access all user authentication tokens, leads to RCE (https://hackerone.com/reports/158330)
Certly (https://hackerone.com/certly)	-	Business logic Failure - Browser cache management and logout vulnerability in Certly (https://hackerone.com/reports/158270)
Trello (https://hackerone.com/trello)	$1,024	File access using image tragick (https://hackerone.com/reports/158192)
HackerOne (https://hackerone.com/security)	$500	Non-secure requests are not automatically upgraded to HTTPS (https://hackerone.com/reports/158186)
Instacart (https://hackerone.com/instacart)	$250	shopper login_code's can be brute forced (https://hackerone.com/reports/158157)
Twitter (https://hackerone.com/twitter)	$560	reverb.twitter.com redirects to vulnerable reverb.guru (https://hackerone.com/reports/158148)
Shopify (https://hackerone.com/shopify) ★	$500	Access to Splunk at https://apt.ec2.shopify.com:8089 (https://hackerone.com/reports/158118)
Trello (https://hackerone.com/trello)	-	XSS and Open-Redirect via SVG (https://hackerone.com/reports/158034)
Instacart (https://hackerone.com/instacart)	$100	Image Upload Path Disclosure (https://hackerone.com/reports/158021)
Instacart (https://hackerone.com/instacart)	$150	Host Header Injection/Redirection in: https://www.instacart.com/ (https://hackerone.com/reports/158019)
Instacart (https://hackerone.com/instacart)	$50	Server side request forgery on image upload for lists (https://hackerone.com/reports/158016)
Instacart (https://hackerone.com/instacart)	$75	Missing rel=noreferrer tag allows link in list to change url of currently open tab (https://hackerone.com/reports/158002)
Instacart (https://hackerone.com/instacart)	$200	Race Condition in Redeeming Coupons (https://hackerone.com/reports/157996)
Instacart (https://hackerone.com/instacart)	$100	Cross-Site Request Forgery (CSRF) (https://hackerone.com/reports/157993)
Veris (https://hackerone.com/veris)	-	Internal server error 500 at log.veris.in (https://hackerone.com/reports/157986)

Team	Bounty	Title
Instacart (https://hackerone.com/instacart)	$150	Stored XSS (https://hackerone.com/reports/157958)
Instacart (https://hackerone.com/instacart)	$50	CSRF To change Email Notification Settings (https://hackerone.com/reports/157956)
OLX (https://hackerone.com/olx)	-	these are my old reports and still i have not receive any good replys, these all are Cross Site Scripting(XSS) issues: POC1: https://www.youtube.com/w (https://hackerone.com/reports/157889)
Shopify (https://hackerone.com/shopify) ★	$500	(FULL PATH DISCLOSURE) Unknown MySQL server host 'shardm-reader.chi2.shopify.io' (https://hackerone.com/reports/157876)
HackerOne (https://hackerone.com/security)	$500	Disclosure of external users invited to a specific report (https://hackerone.com/reports/157699)
Gratipay (https://hackerone.com/gratipay)	-	Cookie:HttpOnly Flag not set (https://hackerone.com/reports/157563)
Gratipay (https://hackerone.com/gratipay)	-	Host Header Injection/Redirection Attack (https://hackerone.com/reports/157465)
New Relic (https://hackerone.com/newrelic)	-	All Active user sessions should be destroyed when user change his password! (https://hackerone.com/reports/157450)
SecNews (https://hackerone.com/secnews)	$300	Querying private posts and changing post meta (https://hackerone.com/reports/157412)
New Relic (https://hackerone.com/newrelic)	-	Login CSRF vulnerability (https://hackerone.com/reports/156992)
Veris (https://hackerone.com/veris)	-	bug (https://hackerone.com/reports/156941)
Uber (https://hackerone.com/uber) ★	$10,000	Reading Emails in Uber Subdomains (https://hackerone.com/reports/156536)
Nextcloud (https://hackerone.com/nextcloud)	-	Directory listening enabled in: 88.198.160.130 (https://hackerone.com/reports/156510)
Nextcloud (https://hackerone.com/nextcloud)	-	demo.nextcloud.com: Content spoofing due to default Apache Error Page (https://hackerone.com/reports/156425)
Algolia (https://hackerone.com/algolia)	$100	Stored XSS from Display Settings triggered on Save and viewing realtime search demo (https://hackerone.com/reports/156387)
Algolia (https://hackerone.com/algolia)	$100	Stored xss (https://hackerone.com/reports/156373)

Team	Bounty	Title
Algolia (https://hackerone.com/algolia)	$100	Stored XSS triggered by json key during UI generation (https://hackerone.com/reports/156347)
Open-Xchange (https://hackerone.com/open-xchange)	$1,000	OX (Guard): Stored Cross-Site Scripting via Incoming Email (https://hackerone.com/reports/156258)
Phabricator (https://hackerone.com/phabricator)	-	Error page Text Injection. (https://hackerone.com/reports/156196)
Uber (https://hackerone.com/uber) ★	-	XSS At "pages.et.uber.com" (https://hackerone.com/reports/156098)
Trello (https://hackerone.com/trello)	-	Verification Code Reused For activating 2FA (https://hackerone.com/reports/155862)
Slack (https://hackerone.com/slack)	$500	CSRF - Add optional two factor mobile number (https://hackerone.com/reports/155774)
Coinbase (https://hackerone.com/coinbase)	-	Create Multiple Account Using Similar X-CSRF token (https://hackerone.com/reports/155726)
Shopify (https://hackerone.com/shopify) ★	$500	Staff member can delete Private Apps (https://hackerone.com/reports/155704)
Nextcloud (https://hackerone.com/nextcloud)	-	Arbitrary File Upload in Logo & Log in image Theming setting. (https://hackerone.com/reports/155690)
Uber (https://hackerone.com/uber) ★	-	Content injection on 404 error page at faspex.uber.com (https://hackerone.com/reports/155685)
Uber (https://hackerone.com/uber) ★	-	User Enumeration and Information Disclosure (https://hackerone.com/reports/155578)
Algolia (https://hackerone.com/algolia)	-	[github.algolia.com] XSS (https://hackerone.com/reports/155576)
Shopify (https://hackerone.com/shopify) ★	$500	(BYPASS) Open Redirect after login at http://ecommerce.shopify.com (https://hackerone.com/reports/155222)
Nextcloud (https://hackerone.com/nextcloud)	-	demo.nextcloud.com: Content spoofing due to default Apache Error Page (https://hackerone.com/reports/155189)
OLX (https://hackerone.com/olx)	-	Unauthorised access to olx.in user accounts. (https://hackerone.com/reports/155130)
Gratipay (https://hackerone.com/gratipay)	$1	Content Spoofing/Text Injection (https://hackerone.com/reports/154921)

Team	Bounty	Title
Nextcloud (https://hackerone.com/nextcloud)	$50	More content spoofing through dir param in the files app (https://hackerone.com/reports/154827)
Uber (https://hackerone.com/uber) ★	$3,000	Missing authorization checks leading to the exposure of ubernihao.com administrator accounts (https://hackerone.com/reports/154762)
Nextcloud (https://hackerone.com/nextcloud)	-	Bookmarks: Delete all existing bookmarks of a user (https://hackerone.com/reports/154529)
Snapchat (https://hackerone.com/snapchat)	$3,000	Subdomain takeover on http://fastly.sc-cdn.net/ (https://hackerone.com/reports/154425)
Shopify (https://hackerone.com/shopify) ★	$500	Delete/modify your own comment after limited access(IDOR) (https://hackerone.com/reports/154410)
Moneybird (https://hackerone.com/moneybird)	$50	[Stored Cross-Site-Scripting] When search about Incoming (Manual Jurnal) (https://hackerone.com/reports/154397)
Shopify (https://hackerone.com/shopify) ★	$1,000	Unauthorized access to Zookeeper on http://locutus-zk3.ec2.shopify.com:2181 (https://hackerone.com/reports/154369)
ownCloud (https://hackerone.com/owncloud)	-	[forum.owncloud.org] IE, Edge XSS via Request-URI (https://hackerone.com/reports/154319)
ownCloud (https://hackerone.com/owncloud)	-	[api.owncloud.org] CRLF Injection (https://hackerone.com/reports/154306)
ownCloud (https://hackerone.com/owncloud)	-	[doc.owncloud.org] CRLF Injection (https://hackerone.com/reports/154275)
Uber (https://hackerone.com/uber) ★	$500	Blind OOB XXE At "http://ubermovement.com/" (https://hackerone.com/reports/154096)
Shopify (https://hackerone.com/shopify) ★	-	Redirect url after login is not validated (https://hackerone.com/reports/153652)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	[Not just a server configuration issue] Full Path Disclosure (https://hackerone.com/reports/153628)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	CSRF in changing settings of Basic Google Maps Placemarks (https://hackerone.com/reports/153580)
Mail.Ru (https://hackerone.com/mailru)	-	[opensource.mail.ru] system accounts enumeration (https://hackerone.com/reports/153178)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	-	Can add employee in business.uber.com without add payment method (https://hackerone.com/reports/153175)
Uber (https://hackerone.com/uber) ★	-	Text Only Content Spoofing on ubermovement.com Community Page (https://hackerone.com/reports/153095)
Ian Dunn (https://hackerone.com/iandunn-projects)	$50	Multiple XSS in Camptix Event Ticketing Plugin (https://hackerone.com/reports/152958)
New Relic (https://hackerone.com/newrelic)	-	Session Management Flaw (https://hackerone.com/reports/152944)
Harvest (https://hackerone.com/harvest)	$500	Project Disclosure of all Harvest Instances (https://hackerone.com/reports/152929)
Nextcloud (https://hackerone.com/nextcloud)	-	Content spoofing in cloud.nextcloud.com (https://hackerone.com/reports/152925)
Harvest (https://hackerone.com/harvest)	$1,000	Leak of all project names and all user names , even across applications (https://hackerone.com/reports/152696)
Harvest (https://hackerone.com/harvest)	$350	Users enumeration is possible through cycling through recurring[client_id] argument value. (https://hackerone.com/reports/152669)
Harvest (https://hackerone.com/harvest)	$350	Stored XSS on invoice, executing on any subdomain (https://hackerone.com/reports/152591)
Harvest (https://hackerone.com/harvest)	$250	CSRF token fixation in Sign in with Google (https://hackerone.com/reports/152586)
Harvest (https://hackerone.com/harvest)	$1,000	S3 bucket takeover due to proxy.harvestfiles.com (https://hackerone.com/reports/152584)
Harvest (https://hackerone.com/harvest)	$100	Cross-Site Request Forgery (CSRF) (https://hackerone.com/reports/152569)
Gratipay (https://hackerone.com/gratipay)	-	Username .. (double dot) should be restricted or handled carefully (https://hackerone.com/reports/152477)
PHP (https://hackerone.com/ibb-php)	$500	NULL Pointer Dereference in exif_process_user_comment (https://hackerone.com/reports/152232)
PHP (https://hackerone.com/ibb-php)	$1,000	Out of bound read in exif_process_IFD_in_MAKERNOTE (https://hackerone.com/reports/152231)

Team	Bounty	Title
Coursera (https://hackerone.com/coursera)	-	Broken authentication and session management flaw (https://hackerone.com/reports/152080)
OLX (https://hackerone.com/olx)	-	Stored XSS on contact name (https://hackerone.com/reports/152069)
Uber (https://hackerone.com/uber) ★	$5,000	Stored XSS on developer.uber.com via admin account compromise (https://hackerone.com/reports/152067)
concrete5 (https://hackerone.com/concrete5)	-	CSRF Full Account Takeover (https://hackerone.com/reports/152052)
Algolia (https://hackerone.com/algolia)	$100	No Rate Limit In Inviting Similar Contact Multiple Times (https://hackerone.com/reports/151868)
Nextcloud (https://hackerone.com/nextcloud)	-	The application uses basic authentication. (https://hackerone.com/reports/151847)
Gratipay (https://hackerone.com/gratipay)	-	User Supplied links on profile page is not validated and redirected via gratipay. (https://hackerone.com/reports/151831)
Gratipay (https://hackerone.com/gratipay)	-	The contribution save option seem to be vulnerable to CSRF (https://hackerone.com/reports/151827)
GoCD (https://hackerone.com/gocd)	-	X-Content-Type-Options header missing at Auth Login (https://hackerone.com/reports/151786)
GoCD (https://hackerone.com/gocd)	-	Directory Listening (https://hackerone.com/reports/151772)
OLX (https://hackerone.com/olx)	-	XSS on Home page olx.com.ar via auto save search text (https://hackerone.com/reports/151691)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	User enumeration in wp-admin (https://hackerone.com/reports/151583)
Ian Dunn (https://hackerone.com/iandunn-projects)	$375	CSV Injection at Camptix Event Ticketing (https://hackerone.com/reports/151516)
ownCloud (https://hackerone.com/owncloud)	$50	ownCloud 2.2.2.6192 DLL Hijacking Vulnerability (https://hackerone.com/reports/151475)
Uber (https://hackerone.com/uber) ★	$2,000	[IODR] Get business trip via organization id (https://hackerone.com/reports/151470)
Uber (https://hackerone.com/uber) ★	$3,000	Get organization info base on uuid (https://hackerone.com/reports/151465)

Team	Bounty	Title
Slack (https://hackerone.com/slack)	$500	Creating Post on a restricted channel (https://hackerone.com/reports/151459)
OLX (https://hackerone.com/olx)	-	xss yaman.olx.ph (https://hackerone.com/reports/151310)
Gratipay (https://hackerone.com/gratipay)	-	don't allow directory browsing on grtp.co (https://hackerone.com/reports/151295)
OLX (https://hackerone.com/olx)	-	Reflected XSS at yaman.olx.ph (https://hackerone.com/reports/151258)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Content-type sniffing leads to stored XSS in CMS Airship on Internet Explorer (https://hackerone.com/reports/151231)
OLX (https://hackerone.com/olx)	-	Manipulating joinolx.com Job Vacancy alert subscription emails (HTML Injection / Script Injection) (https://hackerone.com/reports/151149)
OLX (https://hackerone.com/olx)	-	XSS yaman.olx.ph (https://hackerone.com/reports/151147)
Automattic (https://hackerone.com/automattic)	$300	[bbPress] Stored XSS in any forum post. (https://hackerone.com/reports/151117)
Dropbox (https://hackerone.com/dropbox)	$729	SSRF allows access to internal services like Ganglia (https://hackerone.com/reports/151086)
Shopify (https://hackerone.com/shopify) ★	$1,500	Stealing livechat token and using it to chat as the user - user information disclosure (https://hackerone.com/reports/151058)
Gratipay (https://hackerone.com/gratipay)	-	prevent null bytes in email field (https://hackerone.com/reports/150917)
OLX (https://hackerone.com/olx)	-	Reflected Cross Site scripting Attack (XSS) (https://hackerone.com/reports/150837)
OLX (https://hackerone.com/olx)	-	Arbitrary File Reading (https://hackerone.com/reports/150783)
OLX (https://hackerone.com/olx)	-	Reflected XSS in www.olx.ph (https://hackerone.com/reports/150746)
OLX (https://hackerone.com/olx)	-	SQLi in Payment Request (https://hackerone.com/reports/150633)
OLX (https://hackerone.com/olx)	-	Updating and Deleting any Ads on OLX Philippines (https://hackerone.com/reports/150631)
OLX (https://hackerone.com/olx)	-	CSRF in account configuration leads to complete account compromise (https://hackerone.com/reports/150586)
OLX (https://hackerone.com/olx)	-	XSS @ yaman.olx.ph (https://hackerone.com/reports/150565)

Team	Bounty	Title
OLX (https://hackerone.com/olx)	-	XSS @ *.olx.com.ar (https://hackerone.com/reports/150560)
Uber (https://hackerone.com/uber) ★	$1,000	newsroom.uber.com is vulnerable to 'SOME' XSS attack via plupload.flash.swf (https://hackerone.com/reports/150375)
Shopify (https://hackerone.com/shopify) ★	$500	https://windsor.shopify.com/ takeover (https://hackerone.com/reports/150374)
Twitter (https://hackerone.com/twitter)	$420	Html Injection and Possible XSS in sms-be-vip.twitter.com (https://hackerone.com/reports/150179)
Uber (https://hackerone.com/uber) ★	$4,000	SQL Injection on sctrack.email.uber.com.cn (https://hackerone.com/reports/150156)
IRCCloud (https://hackerone.com/irccloud)	$500	Cross Site Scripting(XSS) on IRCCloud Badges Page (using Parameter Pollution) (https://hackerone.com/reports/150083)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	Brute force on wp-login (https://hackerone.com/reports/150079)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	SSL certificate public key less than 2048 bit (https://hackerone.com/reports/150078)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Full Path Disclosure by removing CSRF token (https://hackerone.com/reports/150018)
Bime (https://hackerone.com/bime)	$1,000	Attacker can access graphic representation of every query (https://hackerone.com/reports/149914)
Bime (https://hackerone.com/bime)	$1,000	Urgent: attacker can access every data source on Bime (https://hackerone.com/reports/149907)
Gratipay (https://hackerone.com/gratipay)	-	don't leak Server version for assets.gratipay.com (https://hackerone.com/reports/149710)
Uber (https://hackerone.com/uber) ★	$2,250	Subdomain takeover of translate.uber.com, de.uber.com and fr.uber.com (https://hackerone.com/reports/149679)
GitLab (https://hackerone.com/gitlab)	-	Insecure 2FA/authentication implementation creates a brute force vulnerability (https://hackerone.com/reports/149598)
Legal Robot (https://hackerone.com/legalrobot)	$40	AWS S3 website can't serve security headers, may allow clickjacking (https://hackerone.com/reports/149572)
Whisper (https://hackerone.com/whisper)	$100	Stored XSS in wis.pr (https://hackerone.com/reports/149571)
Uber (https://hackerone.com/uber) ★	-	Server version disclosure (https://hackerone.com/reports/149483)

Team	Bounty	Title
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Site support SNI But Browser can't (https://hackerone.com/reports/149442)
HackerOne (https://hackerone.com/security)	-	Reward Money Leakage (https://hackerone.com/reports/149435)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	ssl info shown (https://hackerone.com/reports/149369)
CodeIgniter (https://hackerone.com/codeigniter)	-	Web Server Disclosure (https://hackerone.com/reports/149327)
ExpressionEngine (https://hackerone.com/expressionengine)	-	Arbitrary SQL query execution and reflected XSS in the "SQL Query Form" (https://hackerone.com/reports/149279)
ExpressionEngine (https://hackerone.com/expressionengine)	-	Filename and directory enumeration (https://hackerone.com/reports/149273)
ExpressionEngine (https://hackerone.com/expressionengine)	-	Full path + some back-end code disclosure (https://hackerone.com/reports/149212)
Algolia (https://hackerone.com/algolia)	$100	Stored xss (https://hackerone.com/reports/149154)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	[URGENT] Password reset emails are sent in clear-text (without encryption) (https://hackerone.com/reports/149028)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Issue with password reset functionality [Minor] (https://hackerone.com/reports/149027)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Session Management Issue CMS Airship (https://hackerone.com/reports/148914)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	User enumeration via Password reset page [Minor] (https://hackerone.com/reports/148911)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Airship doesn't reject weak passwords (https://hackerone.com/reports/148903)
Nextcloud (https://hackerone.com/nextcloud)	-	[Thirdparty] Stored XSS in chat module - nextcloud server 9.0.51 installed in ubuntu 14.0.4 LTS (https://hackerone.com/reports/148897)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Full path disclosure when CSRF validation failed (https://hackerone.com/reports/148890)
Phabricator (https://hackerone.com/phabricator)	$600	HTML in Diffusion not escaped in certain circumstances (https://hackerone.com/reports/148865)

Team	Bounty	Title
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	$50	Stored XSS using SVG (https://hackerone.com/reports/148853)
Legal Robot (https://hackerone.com/legalrobot)	$100	Subdomain takeover at api.legalrobot.com due to non-used domain in Modulus.io. (https://hackerone.com/reports/148770)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Nginx Version Disclosure On Forbidden Page (https://hackerone.com/reports/148768)
Pornhub (https://hackerone.com/pornhub)	$1,500	[idor] Unauthorized Read access to all the private posts(Including Photos,Videos,Gifs) (https://hackerone.com/reports/148764)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Email spoofing in security@paragonie.com (https://hackerone.com/reports/148763)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	$25	Stored XSS in comments (https://hackerone.com/reports/148751)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	$50	Stored Cross-Site-Scripting in CMS Airship's authors profiles (https://hackerone.com/reports/148741)
Dropbox (https://hackerone.com/dropbox)	-	XSS, Unvalidated redirects & phishing website hosting on dropbox servers (https://hackerone.com/reports/148640)
Keybase (https://hackerone.com/keybase)	$350	Register multiple users using one invitation (race condition) (https://hackerone.com/reports/148609)
Coinbase (https://hackerone.com/coinbase)	-	No authorization required in iOS device web-application (https://hackerone.com/reports/148538)
Coinbase (https://hackerone.com/coinbase)	-	No authorization required in Windows phone web-application (https://hackerone.com/reports/148537)
HackerOne (https://hackerone.com/security)	-	Possible CSRF during joining report as participant (https://hackerone.com/reports/148517)
Instacart (https://hackerone.com/instacart)	-	CSRF with redeem coupon request (https://hackerone.com/reports/148417)
Uber (https://hackerone.com/uber) ★	$1,000	Wordpress Vulnerabilities in transparencyreport.uber.com and eng.uber.com domains (https://hackerone.com/reports/148163)
Mail.Ru (https://hackerone.com/mailru)	-	Cross Site Request Forgery (CSRF) (https://hackerone.com/reports/148156)

Team	Bounty	Title
Trello (https://hackerone.com/trello)	-	Sending Unlimited Mails To Anybody With Easy Social Share Buttons Plugin (https://hackerone.com/reports/148112)
Slack (https://hackerone.com/slack)	$1,500	Source code leakage through GIT web access at host '52.91.137.42' (https://hackerone.com/reports/148068)
HackerOne (https://hackerone.com/security)	$500	Know undisclosed Bounty Amount when Bounty Statistics are enabled. (https://hackerone.com/reports/148050)
Veris (https://hackerone.com/veris)	-	Email spoofing in support@veris.in (https://hackerone.com/reports/147919)
Badoo (https://hackerone.com/badoo)	$140	Change contents of the careers iframe in https://corp.badoo.com/jobs (https://hackerone.com/reports/147776)
Mail.Ru (https://hackerone.com/mailru)	-	Back Refresh Attack after registration and successful logout (https://hackerone.com/reports/147744)
Moneybird (https://hackerone.com/moneybird)	$25	Logging out any user (https://hackerone.com/reports/147656)
leetfiles (https://hackerone.com/leetfiles)	-	[leetfil.es] MSIE, Edge XSS via Request-URI (https://hackerone.com/reports/147646)
concrete5 (https://hackerone.com/concrete5)	-	Local File Inclusion path bypass (https://hackerone.com/reports/147570)
Slack (https://hackerone.com/slack)	$100	Generate new Test token (https://hackerone.com/reports/147544)
FantasyTote (https://hackerone.com/fantasytote)	-	Session doesn't expired after login (https://hackerone.com/reports/147388)
Slack (https://hackerone.com/slack)	$100	User can start call in a channel of an unpaid account (https://hackerone.com/reports/147369)
FantasyTote (https://hackerone.com/fantasytote)	-	Weak HSTS age (https://hackerone.com/reports/147260)
FantasyTote (https://hackerone.com/fantasytote)	-	Betting more than max amount (https://hackerone.com/reports/147237)
FantasyTote (https://hackerone.com/fantasytote)	-	Urgent Fix Balance Limit bypass (https://hackerone.com/reports/147220)
FantasyTote (https://hackerone.com/fantasytote)	-	Bypass logout (https://hackerone.com/reports/147204)

Team	Bounty	Title
FantasyTote (https://hackerone.com/fantasytote)	-	Insecure password change mechanism may lead to full account takeover (https://hackerone.com/reports/147203)
FantasyTote (https://hackerone.com/fantasytote)	-	Stored number of clicks in the Deposits button (https://hackerone.com/reports/147188)
FantasyTote (https://hackerone.com/fantasytote)	-	No email verification required when we change email from settings (https://hackerone.com/reports/147182)
Informatica (https://hackerone.com/informatica)	-	[oneclickdrsfdc-test.informatica.com] Tomcat Example Scripts Exposed Unauthenticated (https://hackerone.com/reports/147161)
Dropbox (https://hackerone.com/dropbox)	-	Can make any number of dropbox accounts with one email (https://hackerone.com/reports/147155)
VK.com (https://hackerone.com/vkcom)	-	DOM XSS в /activation.php?act=activate_mobile (https://hackerone.com/reports/146939)
New Relic (https://hackerone.com/newrelic)	-	http://newrelic.com SSRF/XSPA (https://hackerone.com/reports/146875)
Uber (https://hackerone.com/uber) ★	-	faspex.uber.com uses an invalid SSL certificate (https://hackerone.com/reports/146847)
HackerOne (https://hackerone.com/security)	$500	Race Conditions in Popular reports feature. (https://hackerone.com/reports/146845)
Uber (https://hackerone.com/uber) ★	-	Authentication Issue for easter egg on bonjour.uber.com (https://hackerone.com/reports/146838)
Uber (https://hackerone.com/uber) ★	-	Command Injection, Information (https://hackerone.com/reports/146735)
Pornhub (https://hackerone.com/pornhub)	$500	RCE Possible Via Video Manager Export using @ character in Video Title (https://hackerone.com/reports/146593)
Nextcloud (https://hackerone.com/nextcloud)	-	No Rate Limiting on stats.nextcloud.com login (https://hackerone.com/reports/146424)
Mail.Ru (https://hackerone.com/mailru)	-	BRUTE FORCE ATTACK (https://hackerone.com/reports/146368)
Uber (https://hackerone.com/uber) ★	-	Server version disclosure: team.uberinternal.com (https://hackerone.com/reports/146327)
Nextcloud (https://hackerone.com/nextcloud)	-	Deny access to download.nextcloud.com + folders (https://hackerone.com/reports/146314)

Team	Bounty	Title
Nextcloud (https://hackerone.com/nextcloud)	-	Log pollution can lead to HTML Injection. (https://hackerone.com/reports/146278)
PHP (https://hackerone.com/ibb-php)	$1,000	ZipArchive class Use After Free Vulnerability in PHP's GC algorithm and unserialize (https://hackerone.com/reports/146235)
PHP (https://hackerone.com/ibb-php)	$1,000	Use After Free Vulnerability in PHP's GC algorithm and unserialize (https://hackerone.com/reports/146233)
Trello (https://hackerone.com/trello)	-	Report bug on jetpack plugin (https://hackerone.com/reports/146196)
Nextcloud (https://hackerone.com/nextcloud)	-	REG: Content provider information leakage (https://hackerone.com/reports/146179)
Nextcloud (https://hackerone.com/nextcloud)	-	Email ID Disclosure. (https://hackerone.com/reports/146106)
Nextcloud (https://hackerone.com/nextcloud)	-	WordPress Vulnerabilities: User Enumeration, Vulnerable Akismet Plugin, XML-RPC Interface available (https://hackerone.com/reports/146093)
Nextcloud (https://hackerone.com/nextcloud)	$100	Read-only share recipient can restore old versions of file (https://hackerone.com/reports/146067)
Nextcloud (https://hackerone.com/nextcloud)	$250	Uploading files to a folder where invited user don't have any EDIT privilege (https://hackerone.com/reports/145950)
Uber (https://hackerone.com/uber) ★	-	Error Message on 404 page (https://hackerone.com/reports/145893)
Nextcloud (https://hackerone.com/nextcloud)	-	Content Injection in subdomain (https://hackerone.com/reports/145854)
Nextcloud (https://hackerone.com/nextcloud)	-	Content injection in subdomain (https://hackerone.com/reports/145853)
Nextcloud (https://hackerone.com/nextcloud)	-	Content Spoofing/Text Injection - docs.nextcloud.org (https://hackerone.com/reports/145850)
Nextcloud (https://hackerone.com/nextcloud)	-	Content Injection 404 page (https://hackerone.com/reports/145849)
Nextcloud (https://hackerone.com/nextcloud)	-	Business/Functional logic bypass: Remove admins from admin group. (https://hackerone.com/reports/145745)
Nextcloud (https://hackerone.com/nextcloud)	-	help.nextcloud Email Address/Username enumeration (https://hackerone.com/reports/145734)

Team	Bounty	Title
Nextcloud (https://hackerone.com/nextcloud)	-	newsletter.nextcloud.com: Bypass firewall protection (https://hackerone.com/reports/145730)
Nextcloud (https://hackerone.com/nextcloud)	-	Bruteforcing help.nextcloud.com (https://hackerone.com/reports/145727)
Nextcloud (https://hackerone.com/nextcloud)	-	Bruteforce attack is possible on newsletter.nextcloud.com (https://hackerone.com/reports/145722)
Slack (https://hackerone.com/slack)	-	Unauthenticated Access to some old file thumbnails (https://hackerone.com/reports/145621)
Nextcloud (https://hackerone.com/nextcloud)	-	No captcha on newsletter.nextcloudcom leaves vulnerable to email spammers (https://hackerone.com/reports/145612)
Nextcloud (https://hackerone.com/nextcloud)	-	https://newsletter.nextcloud.com Directory listening and Information Disclosure (https://hackerone.com/reports/145603)
Nextcloud (https://hackerone.com/nextcloud)	-	Lost Password CSRF (https://hackerone.com/reports/145583)
Nextcloud (https://hackerone.com/nextcloud)	-	Directory Listing On download.nextcloud.com & Practical Attacks on PGP (Pretty Good Privacy) (https://hackerone.com/reports/145552)
Nextcloud (https://hackerone.com/nextcloud)	-	Server side request forgery (SSRF) on nextcloud implementation. (https://hackerone.com/reports/145524)
Nextcloud (https://hackerone.com/nextcloud)	-	Vulnerable Javascript library (https://hackerone.com/reports/145517)
Nextcloud (https://hackerone.com/nextcloud)	-	nextcloud.com: Directory listening for 'wp-includes' forders (https://hackerone.com/reports/145495)
Vimeo (https://hackerone.com/vimeo)	$600	Downloading password protected / restricted videos (https://hackerone.com/reports/145467)
Nextcloud (https://hackerone.com/nextcloud)	$50	Nextcloud server software: Content Spoofing (https://hackerone.com/reports/145463)
Nextcloud (https://hackerone.com/nextcloud)	-	No rate limiting on password protected shared file link (https://hackerone.com/reports/145462)
Nextcloud (https://hackerone.com/nextcloud)	-	nextcloud.com: Mail Bombing (No Rate Limiting On Sending Emails On Contact us Page) (https://hackerone.com/reports/145458)

Team	Bounty	Title
Nextcloud (https://hackerone.com/nextcloud)	-	help.nextcloud.com: Session Management Issue (https://hackerone.com/reports/145430)
Nextcloud (https://hackerone.com/nextcloud)	-	help.nextcloud.com: Known DoS condition (null pointer deref) in Nginx running (https://hackerone.com/reports/145409)
Nextcloud (https://hackerone.com/nextcloud)	-	No permission set on Activities [Android App] (https://hackerone.com/reports/145402)
Nextcloud (https://hackerone.com/nextcloud)	-	Enumeration of subscribed users and unauthenticated email unsubscriptions on https://newsletter.nextcloud.com/?p=unsubscribe (https://hackerone.com/reports/145396)
Nextcloud (https://hackerone.com/nextcloud)	-	Response Header injection using redirect_uri together with PHP that utilizes Header Folding according to RFC1945 and Internet Explorer 11 (https://hackerone.com/reports/145392)
Nextcloud (https://hackerone.com/nextcloud)	-	stats.nextcloud.com: Content Injection (https://hackerone.com/reports/145375)
Nextcloud (https://hackerone.com/nextcloud)	-	Content Spoofing (https://hackerone.com/reports/145374)
Nextcloud (https://hackerone.com/nextcloud)	$750	Stored XSS on Share-popup of a directory's Gallery-view (https://hackerone.com/reports/145355)
Nextcloud (https://hackerone.com/nextcloud)	-	nextcloud.com: Content Injection Custom 404 Error (https://hackerone.com/reports/145344)
Veris (https://hackerone.com/veris)	-	Registeration Link "Jacking&Redirecting" (https://hackerone.com/reports/145306)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Session Management (https://hackerone.com/reports/145300)
Uber (https://hackerone.com/uber) ★	-	Self-XSS in Partners Profile (https://hackerone.com/reports/145289)
Uber (https://hackerone.com/uber) ★	$7,000	xss in https://www.uber.com (https://hackerone.com/reports/145278)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Full path disclosure vulnerability on paragonie.com (https://hackerone.com/reports/145260)
Zomato (https://hackerone.com/zomato)	-	Stored Cross site scripting (https://hackerone.com/reports/145246)
Uber (https://hackerone.com/uber) ★	$1,500	Bulk UUID enumeration via invite codes (https://hackerone.com/reports/145150)

Team	Bounty	Title
Ian Dunn (https://hackerone.com/iandunn-projects)	$50	Stored XSS from ticket messages in admin table in SupportFlow (https://hackerone.com/reports/145091)
Ian Dunn (https://hackerone.com/iandunn-projects)	$50	Stored XSS in SupportFlow Ticket Subject (https://hackerone.com/reports/145086)
Uber (https://hackerone.com/uber) ★	-	Bruteforce INVITE codes easy way (https://hackerone.com/reports/144877)
Uber (https://hackerone.com/uber) ★	-	Email Address Enumeration (https://hackerone.com/reports/144803)
Python (https://hackerone.com/ibb-python)	$1,000	CVE-2016-0772 - python: smtplib StartTLS stripping attack (https://hackerone.com/reports/144782)
Sucuri (https://hackerone.com/sucuri)	$250	[support.sucuri.net] CRLF Injection (https://hackerone.com/reports/144769)
Sucuri (https://hackerone.com/sucuri)	$250	SSRF in sitecheck.sucuri.net (https://hackerone.com/reports/144724)
Mail.Ru (https://hackerone.com/mailru)	$150	[townwars.mail.ru] Time-Based SQL Injection (https://hackerone.com/reports/144674)
Uber (https://hackerone.com/uber) ★	$750	Brute-Forcing invite codes in partners.uber.com (https://hackerone.com/reports/144616)
bitaccess (https://hackerone.com/bitaccess)	$200	EXTREMELY URGENT: Missing control of bitcoin amount when selling bitcoin allows a user to withdraw any amount of money, unrestricted. (https://hackerone.com/reports/144526)
Ruby (https://hackerone.com/ruby)	-	Heap corruption in string.c tr_trans() due to undersized buffer (https://hackerone.com/reports/144485)
Ruby (https://hackerone.com/ruby)	-	Heap corruption in DateTime.strftime() on 32 bit for certain format strings (https://hackerone.com/reports/144484)
Ruby (https://hackerone.com/ruby)	$500	StringIO strio_getline() can divulge arbitrary memory (https://hackerone.com/reports/144482)
WebSummit (https://hackerone.com/websummit)	-	Time Based SQL injection in url parameter (https://hackerone.com/reports/144359)
Uber (https://hackerone.com/uber) ★	-	Newsroom.uber HTML form without CSRF protection (https://hackerone.com/reports/144147)
HackerOne (https://hackerone.com/security)	$500	All information is not removed from published reports (https://hackerone.com/reports/144129)

Team	Bounty	Title
SecNews (https://hackerone.com/secnews)	-	Text injection on error page. (https://hackerone.com/reports/144104)
SecNews (https://hackerone.com/secnews)	-	Content spoofing due to the improper behavior of the not-found message (https://hackerone.com/reports/144084)
Instacart (https://hackerone.com/instacart)	$100	Authorization Bypass in Delivery Chat Logs (https://hackerone.com/reports/144000)
The Internet (https://hackerone.com/internet) ★	$7,500	Insufficient shell characters filtering leads to (potentially remote) code execution (CVE-2016-3714) (https://hackerone.com/reports/143966)
Slack (https://hackerone.com/slack)	$500	File upload over private IM channel (https://hackerone.com/reports/143903)
Uber (https://hackerone.com/uber) ★	$10,000	Change any Uber user's password through /rt/users/passwordless-signup - Account Takeover (critical) (https://hackerone.com/reports/143717)
Uber (https://hackerone.com/uber) ★	-	Email Enumeration Vulnerability (https://hackerone.com/reports/143672)
Badoo (https://hackerone.com/badoo)	$280	Получение оригинала скрытого изображения (https://hackerone.com/reports/143669)
Phabricator (https://hackerone.com/phabricator)	-	Full path disclosure (https://hackerone.com/reports/143575)
Coinbase (https://hackerone.com/coinbase)	-	Transaction Pending Via Ip Change (https://hackerone.com/reports/143541)
Shopify (https://hackerone.com/shopify) ★	$3,000	Authentication Bypass on Icinga monitoring server (https://hackerone.com/reports/143482)
Shopify (https://hackerone.com/shopify) ★	$1,500	Potentially Sensitive Information on GitHub (https://hackerone.com/reports/143438)
Veris (https://hackerone.com/veris)	-	Unauthenticated CSRF(User can input any value for CSRF Token) (https://hackerone.com/reports/143321)
Zomato (https://hackerone.com/zomato)	-	XSS on zomato.com (https://hackerone.com/reports/143294)
Uber (https://hackerone.com/uber) ★	-	Password Reset Does Not Confirm the Existence of an Email Address (https://hackerone.com/reports/143291)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	$250	Mail.ru for Android Content Provider Vulnerability (https://hackerone.com/reports/143280)
Uber (https://hackerone.com/uber) ★	-	Header Injection (https://hackerone.com/reports/143076)
drchrono (https://hackerone.com/drchrono)	$50	Information Disclosure (https://hackerone.com/reports/143064)
Python (https://hackerone.com/ibb-python)	$500	Heap corruption via Python 2.7.11 IOBase readline() (https://hackerone.com/reports/143022)
Uber (https://hackerone.com/uber) ★	$750	xss vulnerability in http://ubermovement.com/community/daniel (https://hackerone.com/reports/142946)
drchrono (https://hackerone.com/drchrono)	$50	Bug Report (https://hackerone.com/reports/142940)
Moneybird (https://hackerone.com/moneybird)	$50	[STORED XSS] in debtor reports of ,,invoices'' (https://hackerone.com/reports/142893)
WePay (https://hackerone.com/wepay)	$250	Invited users can modify and/or remove account owner (https://hackerone.com/reports/142842)
Shopify (https://hackerone.com/shopify) ★	$500	Fetching external resources through svg images (https://hackerone.com/reports/142709)
LocalTapiola (https://hackerone.com/localtapiola)	$100	DOM XSS bypassing in Regional Office -selector (https://hackerone.com/reports/142609)
Urban Dictionary (https://hackerone.com/urbandictionary)	-	Infinite Upvoting/Downvoting: Lockout Bypass, Plus: Exposed API Documentation (https://hackerone.com/reports/142569)
Pornhub (https://hackerone.com/pornhub)	$10,000	[RCE] Unserialize to XXE - file disclosure on ams.upload.pornhub.com (https://hackerone.com/reports/142562)
Mail.Ru (https://hackerone.com/mailru)	$150	[tidaltrek.mail.ru] SQL Injection (https://hackerone.com/reports/142479)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	CVE-2016-2177 Undefined pointer arithmetic in SSL code (https://hackerone.com/reports/142472)
Pornhub (https://hackerone.com/pornhub)	$1,500	(Pornhub & Youporn & Brazzers ANDROID APP) : Upload Malicious APK / Overrite Existing APK / Android BackOffice Access (https://hackerone.com/reports/142352)

Team	Bounty	Title
Zomato (https://hackerone.com/zomato)	-	Bypass OTP verification when placing Order (https://hackerone.com/reports/142221)
Trello (https://hackerone.com/trello)	-	XSS in Jetpack plugin (https://hackerone.com/reports/142174)
Pornhub (https://hackerone.com/pornhub)	$20,000	[phpobject in cookie] Remote shell/command execution (https://hackerone.com/reports/141956)
Pornhub (https://hackerone.com/pornhub)	$1,000	Private Photo Disclosure - /user/stream_photo_attach?load=album&id= endpoint (https://hackerone.com/reports/141868)
drchrono (https://hackerone.com/drchrono)	$50	Bypassing Password Reset (https://hackerone.com/reports/141734)
drchrono (https://hackerone.com/drchrono)	-	XSS in Blog (https://hackerone.com/reports/141728)
GlassWire (https://hackerone.com/glasswire)	$25	Bypass GlassWire's monitoring of Hosts file (https://hackerone.com/reports/141700)
New Relic (https://hackerone.com/newrelic)	-	SSRF on synthetics.newrelic.com permitting access to sensitive data (https://hackerone.com/reports/141682)
Bime (https://hackerone.com/bime)	-	Bime Unable to load Data Sources (https://hackerone.com/reports/141676)
HackerOne (https://hackerone.com/security)	$500	Able to remove the admin access of my program (https://hackerone.com/reports/141629)
Pornhub (https://hackerone.com/pornhub)	-	Reflected XSS by way of jQuery function (https://hackerone.com/reports/141493)
drchrono (https://hackerone.com/drchrono)	$50	Stored XSS via AngularJS Injection (https://hackerone.com/reports/141463)
Ubiquiti Networks (https://hackerone.com/ubnt)	$260	Open Redirect in unifi.ubnt.com [Controller Finder] (https://hackerone.com/reports/141355)
drchrono (https://hackerone.com/drchrono)	$50	[CRITICAL] CSRF leading to account take over (https://hackerone.com/reports/141344)
Uber (https://hackerone.com/uber) ★	-	Uber is Flooding my Mobile with SMS Daily like a cron JOB (https://hackerone.com/reports/141339)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	$150	Code source discloure & ability to get database information "SQL injection" in [townwars.mail.ru] (https://hackerone.com/reports/141329)
New Relic (https://hackerone.com/newrelic)	-	Blind SSRF on synthetics.newrelic.com (https://hackerone.com/reports/141304)
Nginx (https://hackerone.com/ibb-nginx)	-	Module ngx_http_auth_basic_module is broken and allowing all password after specific length (https://hackerone.com/reports/141239)
drchrono (https://hackerone.com/drchrono)	$50	Template stored XSS (https://hackerone.com/reports/141198)
drchrono (https://hackerone.com/drchrono)	$50	node.drchrono.com - Information Disclosure and Windows Host Exposed (https://hackerone.com/reports/141174)
drchrono (https://hackerone.com/drchrono)	$50	Ngnix Server version disclosure (https://hackerone.com/reports/141125)
drchrono (https://hackerone.com/drchrono)	$50	Bypass password complexity requirements on passsword reset page (https://hackerone.com/reports/141086)
drchrono (https://hackerone.com/drchrono)	$100	Security Issue : CSRF Token Design Flaw (https://hackerone.com/reports/141065)
Mail.Ru (https://hackerone.com/mailru)	$150	[tidaltrek.mail.ru] SQL Injection (https://hackerone.com/reports/140899)
Mail.Ru (https://hackerone.com/mailru)	-	[sales.mail.ru] CRLF Injection (https://hackerone.com/reports/140851)
Uber (https://hackerone.com/uber) ★	-	XSS in people.uber.com (https://hackerone.com/reports/140791)
Mail.Ru (https://hackerone.com/mailru)	-	Insecure cookies without httpOnly flag set (https://hackerone.com/reports/140760)
Coinbase (https://hackerone.com/coinbase)	-	Cookie not secure (https://hackerone.com/reports/140742)
HackerOne (https://hackerone.com/security)	-	Denial of service in report view. (https://hackerone.com/reports/140720)
Mail.Ru (https://hackerone.com/mailru)	$100	[my.mail.ru] HTML injection в письмах от myadmin@corp.mail.ru (https://hackerone.com/reports/140705)
Mail.Ru (https://hackerone.com/mailru)	$160	[upload-X.my.mail.ru] /uploadphoto Insecure Direct Object References (https://hackerone.com/reports/140548)

Team	Bounty	Title
Slack (https://hackerone.com/slack)	$500	Open Redirect on slack.com (https://hackerone.com/reports/140447)
Gratipay (https://hackerone.com/gratipay)	$10	configure a redirect URI for Facebook OAuth (https://hackerone.com/reports/140432)
Binary.com (https://hackerone.com/binary)	$50	CJ vulnerability in subdomain (https://hackerone.com/reports/140392)
Gratipay (https://hackerone.com/gratipay)	-	don't store CSRF tokens in cookies (https://hackerone.com/reports/140377)
New Relic (https://hackerone.com/newrelic)	-	Session takeover (https://hackerone.com/reports/140333)
New Relic (https://hackerone.com/newrelic)	-	No CSRF validation on Account Monitors in Synthetics Block (https://hackerone.com/reports/140275)
Trello (https://hackerone.com/trello)	$128	XSS in Jetpack Plugin (https://hackerone.com/reports/140264)
Zomato (https://hackerone.com/zomato)	-	XSS onmouseover (https://hackerone.com/reports/139981)
Phabricator (https://hackerone.com/phabricator)	-	No authentication required to add an email address. (https://hackerone.com/reports/139965)
LocalTapiola (https://hackerone.com/localtapiola)	$100	Exploiting Secure Shell (SSH) on mobilelt.lahitapiola.fi (https://hackerone.com/reports/139940)
Uber (https://hackerone.com/uber) ★	-	DOM based XSS on (https://hackerone.com/reports/139875)
Phabricator (https://hackerone.com/phabricator)	$300	Passphrase credential lock bypass (https://hackerone.com/reports/139626)
Dovecot (https://hackerone.com/dovecot)	-	Outdated Apache Server in www.dovecot.fi is vulnerable to various attack. (https://hackerone.com/reports/139591)
Dovecot (https://hackerone.com/dovecot)	-	Apache version disclosure (https://hackerone.com/reports/139547)
Ubiquiti Networks (https://hackerone.com/ubnt)	$2,750	Read-Only user can execute arbitraty shell commands on AirOS (https://hackerone.com/reports/139398)
ok.ru (https://hackerone.com/ok)	-	Missing proper error message. (https://hackerone.com/reports/139319)
Automattic (https://hackerone.com/automattic)	$500	WordPress core stored XSS via attachment file name (https://hackerone.com/reports/139245)

Team	Bounty	Title
Badoo (https://hackerone.com/badoo)	$280	Ability to collect users' ids that have visited a specific web page with malicious code (https://hackerone.com/reports/139192)
Dropbox (https://hackerone.com/dropbox)	-	Lack of account link warning enables dropbox hijacking (https://hackerone.com/reports/139099)
LocalTapiola (https://hackerone.com/localtapiola)	$300	Persistent XSS at verkkopalvelu.tapiola.fi using spoofed React element and React v.0.13.3 (https://hackerone.com/reports/139004)
Uber (https://hackerone.com/uber) ★	-	Phone Number Enumeration (https://hackerone.com/reports/138881)
Uber (https://hackerone.com/uber) ★	$7,000	OneLogin authentication bypass on WordPress sites via XMLRPC (https://hackerone.com/reports/138869)
New Relic (https://hackerone.com/newrelic)	-	Missing rate limit on password (https://hackerone.com/reports/138863)
LocalTapiola (https://hackerone.com/localtapiola)	$100	Remote Code Execution in NovaStor NovaBACKUP DataCenter backup software (Hiback) (https://hackerone.com/reports/138824)
Veris (https://hackerone.com/veris)	-	Text injection can be used in phishing 404 page and should not include attacker text (https://hackerone.com/reports/138786)
Pornhub (https://hackerone.com/pornhub)	$1,000	SSRF & XSS (W3 Total Cache) (https://hackerone.com/reports/138721)
Gratipay (https://hackerone.com/gratipay)	-	don't expose path of Python (https://hackerone.com/reports/138659)
Uber (https://hackerone.com/uber) ★	-	Self-XSS on partners.uber.com (https://hackerone.com/reports/138622)
Dovecot (https://hackerone.com/dovecot)	-	DIrectory Listing Found (https://hackerone.com/reports/138558)
LocalTapiola (https://hackerone.com/localtapiola)	$300	Abusing and Hacking the SMTP Server secure.lahitapiola.fi (https://hackerone.com/reports/138315)
Zomato (https://hackerone.com/zomato)	-	Instagram OAuth2 Implementation Leaks Access Token; Allows for Cross-Site Script Inclusion (XSSI) (https://hackerone.com/reports/138270)
Zomato (https://hackerone.com/zomato)	-	Reflected Cross-Site Scripting in www.zomato.com/php/instagram_tag_relay (https://hackerone.com/reports/138262)
WP API (https://hackerone.com/wp-api)	$100	Missing access control exposing detailed information on all users (https://hackerone.com/reports/138244)

Team	Bounty	Title
Pornhub (https://hackerone.com/pornhub)	$150	Same-Origin Method Execution bug in plupload.flash.swf on /insights (https://hackerone.com/reports/138226)
OpenSSL (https://hackerone.com/ibb-openssl)	$1,000	Bleichenbacher oracle in SSLv2 (CVE-2016-0704) (https://hackerone.com/reports/138181)
OpenSSL (https://hackerone.com/ibb-openssl)	$2,500	Divide-and-conquer session key recovery in SSLv2 (CVE-2016-0703) (https://hackerone.com/reports/138179)
Pornhub (https://hackerone.com/pornhub)	$5,000	Weak user aunthentication on mobile application - I just broken userKey secret password (https://hackerone.com/reports/138101)
Pornhub (https://hackerone.com/pornhub)	$1,500	[stored xss, pornhub.com] stream post function (https://hackerone.com/reports/138075)
Pornhub (https://hackerone.com/pornhub)	$250	XSS Reflected incategories*p (https://hackerone.com/reports/138046)
Pornhub (https://hackerone.com/pornhub)	$250	XSS ReflectedGET /*embed_player*? (https://hackerone.com/reports/138045)
Mail.Ru (https://hackerone.com/mailru)	$150	SQL Injection (https://hackerone.com/reports/137956)
Pornhub (https://hackerone.com/pornhub)	$1,500	[IDOR] post to anyone even if their stream is restricted to friends only (https://hackerone.com/reports/137954)
Veris (https://hackerone.com/veris)	-	Reflected XSS in domain www.veris.in (https://hackerone.com/reports/137938)
Pornhub (https://hackerone.com/pornhub)	$100	CSV Macro injection in Video Manager (CEMI) (https://hackerone.com/reports/137850)
Veris (https://hackerone.com/veris)	-	Stored XSS on 'Badges' page (https://hackerone.com/reports/137845)
Square Open Source (https://hackerone.com/square-open-source)	-	Cache poisoning for okhttp (https://hackerone.com/reports/137756)
Ruby (https://hackerone.com/ruby)	-	SMTP command injection (https://hackerone.com/reports/137631)
HackerOne (https://hackerone.com/security)	-	Inadequate access controls in "Vote" functionality??? (https://hackerone.com/reports/137503)
Vimeo (https://hackerone.com/vimeo)	$600	All Vimeo Private videos disclosure via Authorization Bypass (https://hackerone.com/reports/137502)

Team	Bounty	Title
LocalTapiola (https://hackerone.com/localtapiola)	$100	Amazon Bucket Accessible (http://inpref.s3.amazonaws.com/) (https://hackerone.com/reports/137487)
New Relic (https://hackerone.com/newrelic)	-	New Relic - Session Hijacking (https://hackerone.com/reports/137480)
Twitter (https://hackerone.com/twitter)	-	List of a ton of internal twitter servers available on GitHub (https://hackerone.com/reports/137404)
Sucuri (https://hackerone.com/sucuri)	$500	CRLF/HTTP header injection www.sucuri.net (https://hackerone.com/reports/137288)
Dovecot (https://hackerone.com/dovecot)	-	nginx server vulnerable (https://hackerone.com/reports/137230)
Dropbox (https://hackerone.com/dropbox)	-	Dropbox apps Server side request forgery (https://hackerone.com/reports/137229)
ThisData (https://hackerone.com/thisdata)	-	Host Header Poisoning in thisdata.com (https://hackerone.com/reports/137181)
Uber (https://hackerone.com/uber) ★	-	Clickjacking in love.uber.com (https://hackerone.com/reports/137152)
Veris (https://hackerone.com/veris)	-	[Stored XSS] sandbox.veris.in (https://hackerone.com/reports/137127)
ok.ru (https://hackerone.com/ok)	$500	Xss in m.ok.ru (https://hackerone.com/reports/137126)
Veris (https://hackerone.com/veris)	-	[XSS] sandbox.veris.in (https://hackerone.com/reports/137119)
Mail.Ru (https://hackerone.com/mailru)	-	AXFR на plexus.m.smailru.net работает (https://hackerone.com/reports/137093)
Vimeo (https://hackerone.com/vimeo)	-	XSS in Subtitles of Vimeo Flash Player and Hubnut (https://hackerone.com/reports/137023)
OpenSSL (https://hackerone.com/ibb-openssl)	$2,500	Padding oracle in AES-NI CBC MAC check (CVE-2016-2107) (https://hackerone.com/reports/136986)
Ubiquiti Networks (https://hackerone.com/ubnt)	$1,000	Source code disclosure on https://107.23.69.180 (https://hackerone.com/reports/136891)
Uber (https://hackerone.com/uber) ★	$8,000	[CRITICAL] -- Complete Account Takeover (https://hackerone.com/reports/136885)
Gratipay (https://hackerone.com/gratipay)	$1	don't leak server version of grtp.co in error pages (https://hackerone.com/reports/136720)

Team	Bounty	Title
Moneybird (https://hackerone.com/moneybird)	$50	Reflected XSS in Backend search (https://hackerone.com/reports/136600)
Uber (https://hackerone.com/uber) ★	-	Compromising Atlassian Confluence (team.uberinternal.com) via WordPress (newsroom.uber.com) (https://hackerone.com/reports/136531)
Vimeo (https://hackerone.com/vimeo)	$750	CSRF on Vimeo via cross site flashing leading to info disclosure and private videos go public (https://hackerone.com/reports/136481)
ThisData (https://hackerone.com/thisdata)	-	STORED XSS FOUND (https://hackerone.com/reports/136396)
GitLab (https://hackerone.com/gitlab)	-	Persistent XSS on public wiki pages (https://hackerone.com/reports/136333)
Mapbox (https://hackerone.com/mapbox)	$400	Denial of service in account statistics endpoint (https://hackerone.com/reports/136221)
Uber (https://hackerone.com/uber) ★	$10,000	OneLogin authentication bypass on WordPress sites (https://hackerone.com/reports/136169)
Moneybird (https://hackerone.com/moneybird)	$100	Employees with Any Permissions Can Create App with Full Permissions and Perform any API Action (https://hackerone.com/reports/135989)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	EBCDIC overread (CVE-2016-2176) (https://hackerone.com/reports/135946)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	EVP_EncryptUpdate overflow (CVE-2016-2106) (https://hackerone.com/reports/135945)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	EVP_EncodeUpdate overflow (CVE-2016-2105) (https://hackerone.com/reports/135944)
Uber (https://hackerone.com/uber) ★	-	Missing authentication on Notification setting . (https://hackerone.com/reports/135891)
Romit (https://hackerone.com/romit)	$50	Session Fixation (https://hackerone.com/reports/135797)
Moneybird (https://hackerone.com/moneybird)	$25	information disclose (https://hackerone.com/reports/135782)
Shopify (https://hackerone.com/shopify) ★	$500	View all deleted comments and rating of any app . (https://hackerone.com/reports/135756)

Team	Bounty	Title
Dropbox Acquisitions (https://hackerone.com/dropbox-acquisitions)	-	Session hacking (https://hackerone.com/reports/135631)
Dovecot (https://hackerone.com/dovecot)	-	Cross-Site Scripting Vulnerability in dovecot.fi (https://hackerone.com/reports/135316)
Uber (https://hackerone.com/uber) ★	$5,000	Multiple vulnerabilities in a WordPress plugin at drive.uber.com (https://hackerone.com/reports/135288)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Email Authentication Bypass (https://hackerone.com/reports/135283)
LocalTapiola (https://hackerone.com/localtapiola)	$400	Possibly big authorization problem in Lähitapiola´s varainhoito (https://hackerone.com/reports/135252)
Mapbox (https://hackerone.com/mapbox)	$1,000	Reflected cross-site scripting (XSS) on api.tiles.mapbox.com (https://hackerone.com/reports/135217)
LocalTapiola (https://hackerone.com/localtapiola)	$5,000	Blind Stored XSS Against Lahitapiola Employees - Session and Information leakage (https://hackerone.com/reports/135154)
PHP (https://hackerone.com/ibb-php)	$1,500	Integer overflow in ZipArchive::getFrom* (https://hackerone.com/reports/135152)
HackerOne (https://hackerone.com/security)	$2,500	RCE in profile picture upload (https://hackerone.com/reports/135072)
OpenSSL (https://hackerone.com/ibb-openssl)	-	Potential double free in EVP_DigestInit_ex (https://hackerone.com/reports/135027)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	The Anti-CSRF Library fails to restrict token to a particular IP address when being behind a reverse-proxy/WAF (https://hackerone.com/reports/134894)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	ASN.1 BIO excessive memory allocation (CVE-2016-2109) (https://hackerone.com/reports/134880)
Shopify (https://hackerone.com/shopify) ★	$500	staff memeber can install apps even if have limitied access (https://hackerone.com/reports/134757)
Automattic (https://hackerone.com/automattic)	$1,337	WordPress SOME bug in plupload.flash.swf leading to RCE (https://hackerone.com/reports/134738)
Automattic (https://hackerone.com/automattic)	$1,337	WordPress Flash XSS in *flashmediaelement.swf* (https://hackerone.com/reports/134546)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	-	Uber for Business Allows Administrators to Change Uber Driver Ratings Due to Failure to Authenticate `fast-rating` Endpoint (https://hackerone.com/reports/134521)
Zendesk (https://hackerone.com/zendesk)	$250	XSS In /zuora/ functionality (https://hackerone.com/reports/134434)
LocalTapiola (https://hackerone.com/localtapiola)	-	Source Code Disclosure on out of scope domain viestinta.lahitapiola.fi (https://hackerone.com/reports/134406)
LocalTapiola (https://hackerone.com/localtapiola)	$100	Content Spoofing or Text Injection (404 error page injection) (https://hackerone.com/reports/134388)
Algolia (https://hackerone.com/algolia)	$500	RCE on facebooksearch.algolia.com (https://hackerone.com/reports/134321)
GitLab (https://hackerone.com/gitlab)	-	Private snippets in public / internal projects leaked though GitLab API (https://hackerone.com/reports/134305)
GitLab (https://hackerone.com/gitlab)	-	Confidential issues leaked in public projects when attached to milestone (https://hackerone.com/reports/134300)
GitLab (https://hackerone.com/gitlab)	-	Attacker can post notes on private MR, snippets, and issues (https://hackerone.com/reports/134299)
GitLab (https://hackerone.com/gitlab)	-	Attacker can delete (and read) private project webhooks (https://hackerone.com/reports/134292)
ownCloud (https://hackerone.com/owncloud)	-	doc.owncloud.com: PHP info page disclosure (https://hackerone.com/reports/134216)
Uber (https://hackerone.com/uber) ★	-	Defect-Security | Driver-Broken Authentication | Able to update the Subscription Setting anonymously (https://hackerone.com/reports/134206)
QIWI (https://hackerone.com/qiwi)	-	SSL Certificate on qiwi.com will expire soon. (https://hackerone.com/reports/134145)
Uber (https://hackerone.com/uber) ★	-	Stored self-XSS at m.uber.com (https://hackerone.com/reports/134124)
Uber (https://hackerone.com/uber) ★	$2,000	Reflected XSS via Livefyre Media Wall in newsroom.uber.com (https://hackerone.com/reports/134061)
New Relic (https://hackerone.com/newrelic)	-	newrelic.com rails directory traversal vuln (https://hackerone.com/reports/134032)

Team	Bounty	Title
Automattic (https://hackerone.com/automattic)	$75	XSS on www.wordpress.com (https://hackerone.com/reports/133963)
concrete5 (https://hackerone.com/concrete5)	-	ProBlog 2.6.6 CSRF Exploit (https://hackerone.com/reports/133847)
Moneybird (https://hackerone.com/moneybird)	$25	Content Spoofing In Moneybird (https://hackerone.com/reports/133753)
Veris (https://hackerone.com/veris)	-	XSS in Asset name (https://hackerone.com/reports/133744)
Badoo (https://hackerone.com/badoo)	-	AWS S3 Bucket hotornot-images permissions allow for listing and removing files (https://hackerone.com/reports/133680)
Uber (https://hackerone.com/uber) ★	-	Information Disclosure on lite.uber.com (https://hackerone.com/reports/133375)
HackerOne (https://hackerone.com/security)	-	Manipulate report timeline activity by using null byte. (https://hackerone.com/reports/133322)
GitLab (https://hackerone.com/gitlab)	-	Labels created in private projects are leaked (https://hackerone.com/reports/132777)
New Relic (https://hackerone.com/newrelic)	-	Stored Cross-Site Scripting via Angular Template Injection (https://hackerone.com/reports/132658)
Udemy (https://hackerone.com/udemy)	$50	Stored XSS at Udemy (https://hackerone.com/reports/132602)
New Relic (https://hackerone.com/newrelic)	-	Open redirection (https://hackerone.com/reports/132251)
Slack (https://hackerone.com/slack)	$1,000	Stored XSS on team.slack.com using new Markdown editor of posts inside the Editing mode and using javascript-URIs (https://hackerone.com/reports/132104)
HackerOne (https://hackerone.com/security)	-	Reputation Manipulation (Theoretical) (https://hackerone.com/reports/132057)
Zendesk (https://hackerone.com/zendesk)	$500	[HIGH RISK] CSRF could potentially delete a zendesk subdomain. (https://hackerone.com/reports/132049)
Moneybird (https://hackerone.com/moneybird)	$50	Open Redirect vulnerability in moneybird.com (https://hackerone.com/reports/131728)
bitaccess (https://hackerone.com/bitaccess)	-	Missing SPF for hackerone.com (https://hackerone.com/reports/131722)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	-	CrashPlan Backup is Vulnerable Allowing to a DoS Attack Against Uber's Backups to ```backup.uber.com``` (https://hackerone.com/reports/131560)
New Relic (https://hackerone.com/newrelic)	-	Login Open Redirect (https://hackerone.com/reports/131552)
Uber (https://hackerone.com/uber) ★	$7,500	Stored XSS in developer.uber.com (https://hackerone.com/reports/131450)
CloudFlare (https://hackerone.com/cloudflare)	-	Reflected XSS on partners.cloudflare.com (https://hackerone.com/reports/131397)
GitLab (https://hackerone.com/gitlab)	-	Privilege escalation to access all private groups and repositories (https://hackerone.com/reports/131210)
Twitter (https://hackerone.com/twitter)	$840	[Critical] - Steal OAuth Tokens (https://hackerone.com/reports/131202)
Coinbase (https://hackerone.com/coinbase)	$100	User's legal name could be changed despite front end controls being disabled (https://hackerone.com/reports/131192)
Uber (https://hackerone.com/uber) ★	-	XSS via password recovering (https://hackerone.com/reports/131123)
Automattic (https://hackerone.com/automattic)	$75	Akismet Several CSRF vulnerabilities (https://hackerone.com/reports/131108)
ownCloud (https://hackerone.com/owncloud)	$150	Open Redirector via (apps/files_pdfviewer) for un-authenticated users. (https://hackerone.com/reports/131082)
Gratipay (https://hackerone.com/gratipay)	$1	bring grtp.co up to A grade on SSLLabs (https://hackerone.com/reports/131065)
Uber (https://hackerone.com/uber) ★	-	XSS in uber oauth (https://hackerone.com/reports/131052)
Moneybird (https://hackerone.com/moneybird)	$50	Stored XSS in Financial Account executing in Bank tab (https://hackerone.com/reports/131038)
Moneybird (https://hackerone.com/moneybird)	$100	Malicious File Upload (https://hackerone.com/reports/131028)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Vunerability : spf (https://hackerone.com/reports/130990)
ownCloud (https://hackerone.com/owncloud)	-	doc.owncloud.org: XSS via Referrer (https://hackerone.com/reports/130951)

Team	Bounty	Title
Vimeo (https://hackerone.com/vimeo)	-	Error page Text Injection. (https://hackerone.com/reports/130914)
Ubiquiti Networks (https://hackerone.com/ubnt)	$275	Reflected XSS in scores.ubnt.com (https://hackerone.com/reports/130889)
Trello (https://hackerone.com/trello)	-	Error Page Text Injection. (https://hackerone.com/reports/130850)
New Relic (https://hackerone.com/newrelic)	-	Sensitive information contained with New Relic APM iOS application (https://hackerone.com/reports/130739)
Uber (https://hackerone.com/uber) ★	-	Unsubscribe any user from receiving email (https://hackerone.com/reports/130521)
bitaccess (https://hackerone.com/bitaccess)	$50	BYASSING OTP Verification (https://hackerone.com/reports/130460)
Badoo (https://hackerone.com/badoo)	-	Badoo and Hotornot User Disclosure (https://hackerone.com/reports/130453)
Uber (https://hackerone.com/uber) ★	-	Requested and received edit access to Google form (https://hackerone.com/reports/130440)
Moneybird (https://hackerone.com/moneybird)	$50	CSV Injection with the CSV export feature (https://hackerone.com/reports/130338)
Trello (https://hackerone.com/trello)	$128	Cross site scripting in blog.trello.com (https://hackerone.com/reports/130265)
Uber (https://hackerone.com/uber) ★	-	developer.uber.com/404 and developer.uber.com/docs/404 are susceptible to iframes (https://hackerone.com/reports/130136)
Xero (https://hackerone.com/xero)	-	Insecure Payment System Integration (https://hackerone.com/reports/129942)
Slack (https://hackerone.com/slack)	$2,000	Authentication bypass leads to sensitive data exposure (token+secret) (https://hackerone.com/reports/129918)
APITest.IO (https://hackerone.com/apitest)	-	beta version reveals paths, environment variables and partially files contents (https://hackerone.com/reports/129869)
Zendesk (https://hackerone.com/zendesk)	$50	Stored XSS on [your_zendesk].zendesk.com in Facebook Channel (https://hackerone.com/reports/129862)
APITest.IO (https://hackerone.com/apitest)	-	Login Via FB Leads To Create A New Account Instead Of Loging In (https://hackerone.com/reports/129830)

Team	Bounty	Title
Dropbox (https://hackerone.com/dropbox)	-	No Rate Limiting while sending the feedback under Dropbox Help Centre (https://hackerone.com/reports/129808)
Python (https://hackerone.com/ibb-python)	$500	Python 2.7 strop.replace Integer Overflow (https://hackerone.com/reports/129771)
GitLab (https://hackerone.com/gitlab)	-	Persistent XSS on public project page (https://hackerone.com/reports/129736)
Uber (https://hackerone.com/uber) ★	-	reopen #128853 (Information disclosure at lite.uber.com) (https://hackerone.com/reports/129712)
APITest.IO (https://hackerone.com/apitest)	-	Clickjacking: X-Frame-Options header missing (https://hackerone.com/reports/129650)
ownCloud (https://hackerone.com/owncloud)	-	Cross site scripting in apps.owncloud.com (https://hackerone.com/reports/129551)
Twitter (https://hackerone.com/twitter)	$700	xss in DM group name in twitter (https://hackerone.com/reports/129436)
Veris (https://hackerone.com/veris)	-	Stored XSS in member book (https://hackerone.com/reports/129342)
Uber (https://hackerone.com/uber) ★	-	Disclosure of ways to the site root (https://hackerone.com/reports/129027)
LocalTapiola (https://hackerone.com/localtapiola)	$300	The PdfServlet-functionality used by the "Tee vakuutustodistus" allows injection of custom PDF-content via CSRF-attack (https://hackerone.com/reports/129002)
LocalTapiola (https://hackerone.com/localtapiola)	$400	Cookie-based client-side denial-of-service to all of the Lähitapiola domains (https://hackerone.com/reports/129001)
Uber (https://hackerone.com/uber) ★	-	User credentials are not strong on vault.uber.com (https://hackerone.com/reports/128895)
Uber (https://hackerone.com/uber) ★	-	Information disclosure at lite.uber.com (https://hackerone.com/reports/128853)
Algolia (https://hackerone.com/algolia)	$100	No rate-limit in Two factor Authentication leads to bypass using bruteforce attack (https://hackerone.com/reports/128777)
Gratipay (https://hackerone.com/gratipay)	-	text injection in website title (https://hackerone.com/reports/128764)
Ubiquiti Networks (https://hackerone.com/ubnt)	$1,500	Read-Only user can execute arbitraty shell commands on AirOS (https://hackerone.com/reports/128750)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	-	Enumerating userIDs with phone numbers (https://hackerone.com/reports/128723)
APITest.IO (https://hackerone.com/apitest)	-	SSRF on testing endpoint (https://hackerone.com/reports/128685)
New Relic (https://hackerone.com/newrelic)	-	Clickjacking on authenticated pages which is inscope for New Relic (https://hackerone.com/reports/128645)
ownCloud (https://hackerone.com/owncloud)	-	doc.owncloud.org: X-XSS-Protection not enabled (https://hackerone.com/reports/128493)
Trello (https://hackerone.com/trello)	$1,536	Payments informations are sent to the webhook when a team changes its visibility (https://hackerone.com/reports/128388)
OpenSSL (https://hackerone.com/ibb-openssl)	$1,000	BN_mod_exp may produce incorrect results on x86_64 (CVE-2015-3193) (https://hackerone.com/reports/128169)
Gratipay (https://hackerone.com/gratipay)	$10	fix bug in username restriction (https://hackerone.com/reports/128121)
Snapchat (https://hackerone.com/snapchat)	$1,000	Administrator access to a Django Administration Panel on *.sc-corp.net via bruteforced credentials (https://hackerone.com/reports/128114)
InVision (https://hackerone.com/invision)	$400	CRITICAL : Delete Boards Admin's (or any other user) comment. (IDOR) (https://hackerone.com/reports/128112)
HackerOne (https://hackerone.com/security)	$2,500	AWS S3 bucket writeable for authenticated aws users (https://hackerone.com/reports/128088)
GitLab (https://hackerone.com/gitlab)	-	Bypassing password authentication of users that have 2FA enabled (https://hackerone.com/reports/128085)
GitLab (https://hackerone.com/gitlab)	-	Attacker can extract list of private project's project members (https://hackerone.com/reports/128051)
Gratipay (https://hackerone.com/gratipay)	-	Getting Error Message and in use python version 2.7 is exposed. (https://hackerone.com/reports/128041)
Gratipay (https://hackerone.com/gratipay)	-	An adversary can harvest email address for spamming. (https://hackerone.com/reports/128035)
Uber (https://hackerone.com/uber) ★	$5,000	Stored XSS on newsroom.uber.com admin panel / Stream WordPress plugin (https://hackerone.com/reports/127948)
Uber (https://hackerone.com/uber) ★	$250	Easy spam with USE My PHONE Feature (https://hackerone.com/reports/127918)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	-	Deleted name still present via mouseover functionality for user accounts (https://hackerone.com/reports/127914)
HackerOne (https://hackerone.com/security)	$1,500	Web Authentication Endpoint Credentials Brute-Force Vulnerability (https://hackerone.com/reports/127844)
HackerOne (https://hackerone.com/security)	-	DOS Report FILE html inside <code> in markdown (https://hackerone.com/reports/127827)
New Relic (https://hackerone.com/newrelic)	-	Password disclosure during signup process (https://hackerone.com/reports/127766)
New Relic (https://hackerone.com/newrelic)	-	Open redirection bypass (https://hackerone.com/reports/127741)
Badoo (https://hackerone.com/badoo)	$852	[CRITICAL] Full account takeover using CSRF (https://hackerone.com/reports/127703)
Uber (https://hackerone.com/uber) ★	-	Session Impersonation in riders.uber.com (https://hackerone.com/reports/127645)
HackerOne (https://hackerone.com/security)	$500	New hacktivity view discloses report IDs of non-public reports (https://hackerone.com/reports/127620)
ownCloud (https://hackerone.com/owncloud)	-	Reflected XSS in owncloud.com (https://hackerone.com/reports/127259)
HackerOne (https://hackerone.com/security)	$500	New hacktivity view discloses report IDs of non-public reports (https://hackerone.com/reports/127235)
PHP (https://hackerone.com/ibb-php)	$1,000	php_snmp_error() Format String Vulnerability (https://hackerone.com/reports/127212)
New Relic (https://hackerone.com/newrelic)	-	rpm.newrelic.com - monitor creation to other accounts (https://hackerone.com/reports/127203)
HackerOne (https://hackerone.com/security)	-	HackerOne Important Emails Notification are sent in clear-text (https://hackerone.com/reports/127175)
Coursera (https://hackerone.com/coursera)	-	XSS in https://www.coursera.org/courses/ (https://hackerone.com/reports/127163)
Uber (https://hackerone.com/uber) ★	$5,000	Information regarding trips from other users (https://hackerone.com/reports/127161)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	$5,000	Possibility to get private email using UUID (https://hackerone.com/reports/127158)
Uber (https://hackerone.com/uber) ★	$3,000	Possible to View Driver Waybill via Driver UUID (https://hackerone.com/reports/127087)
Uber (https://hackerone.com/uber) ★	-	Use Partner/Driver App Without Being Activated (https://hackerone.com/reports/127085)
LocalTapiola (https://hackerone.com/localtapiola)	$100	www.lahitapiola.fi DOM XSS by choosing regional company (https://hackerone.com/reports/127077)
New Relic (https://hackerone.com/newrelic)	-	CSV Injection in sub_accounts.csv (https://hackerone.com/reports/127032)
New Relic (https://hackerone.com/newrelic)	-	Old CAPTCHA offers no protection (https://hackerone.com/reports/127028)
New Relic (https://hackerone.com/newrelic)	-	User enumeration possible from log-in timing difference (https://hackerone.com/reports/127026)
Uber (https://hackerone.com/uber) ★	-	Brute Forcing rider-view Endpoint Allows for Counting Number of Active Uber Drivers (https://hackerone.com/reports/127025)
Uber (https://hackerone.com/uber) ★	$3,000	Stored XSS in archive.uber.com Due to Injection of Javascript:alert(0) (https://hackerone.com/reports/126906)
Badoo (https://hackerone.com/badoo)	-	Insecure Direct Object Reference on badoo.com (https://hackerone.com/reports/126861)
Uber (https://hackerone.com/uber) ★	-	It is possible to re-rate a driver after a very long time (https://hackerone.com/reports/126835)
Uber (https://hackerone.com/uber) ★	-	Pixel flood attack in https://riders.uber.com/profile (https://hackerone.com/reports/126826)
Coinbase (https://hackerone.com/coinbase)	$1,000	Sending payments via QR code does not require confirmation (https://hackerone.com/reports/126784)
Uber (https://hackerone.com/uber) ★	-	Disclosure of ip addresses in local network of uber (https://hackerone.com/reports/126569)
Shopify (https://hackerone.com/shopify) ★	$500	XSS on https://app.shopify.com/ (https://hackerone.com/reports/126539)
Uber (https://hackerone.com/uber) ★	-	SMS Flood with Update Profile (https://hackerone.com/reports/126536)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	-	Changing Driver Passwords With Only an Authenticated Session (no password, no email) (https://hackerone.com/reports/126377)
Coinbase (https://hackerone.com/coinbase)	$500	Email leak in transcations in Android app (https://hackerone.com/reports/126376)
Uber (https://hackerone.com/uber) ★	-	Uploading Plain Text to uber-documents.s3.amazonaws.com Through the Driver Document Upload Page (https://hackerone.com/reports/126374)
Uber (https://hackerone.com/uber) ★	-	Uber password reset link EMAIL FLOOD (https://hackerone.com/reports/126364)
Uber (https://hackerone.com/uber) ★	-	Privilege escalation to allow non activated users to login and use uber partner ios app (https://hackerone.com/reports/126260)
Trello (https://hackerone.com/trello)	$1,024	If a team is public, the web socket receives data about the Team visible boards (https://hackerone.com/reports/126242)
Uber (https://hackerone.com/uber) ★	-	text injection in get.uber.com/check-otp (https://hackerone.com/reports/126235)
LocalTapiola (https://hackerone.com/localtapiola)	$1,000	Posting modified information in 'Investment section' will cause unintended information change in verkkopalvelu.tapiola.fi (https://hackerone.com/reports/126209)
Uber (https://hackerone.com/uber) ★	$500	CBC "cut and paste" attack may cause Open Redirect(even XSS) (https://hackerone.com/reports/126203)
Uber (https://hackerone.com/uber) ★	$750	XSS In archive.uber.com Due to Mime Sniffing in IE (https://hackerone.com/reports/126197)
Uber (https://hackerone.com/uber) ★	$1,000	CSV Injection in business.uber.com (https://hackerone.com/reports/126109)
Uber (https://hackerone.com/uber) ★	$2,000	Stored XSS in drive.uber.com WordPress admin panel (https://hackerone.com/reports/126099)
Uber (https://hackerone.com/uber) ★	-	Cross-site Scripting (XSS) (https://hackerone.com/reports/126049)
Uber (https://hackerone.com/uber) ★	-	CRLF Injection in developer.uber.com (https://hackerone.com/reports/125984)
Uber (https://hackerone.com/uber) ★	$10,000	uber.com may RCE by Flask Jinja2 Template Injection (https://hackerone.com/reports/125980)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	$3,000	SQL injection in Wordpress Plugin Huge IT Video Gallery at https://drive.uber.com/frmarketplace/ (https://hackerone.com/reports/125932)
Veris (https://hackerone.com/veris)	-	XSS on multiple fields (https://hackerone.com/reports/125858)
Uber (https://hackerone.com/uber) ★	$3,000	Reflected XSS via Unvalidated / Open Redirect in uber.com (https://hackerone.com/reports/125791)
Zomato (https://hackerone.com/zomato)	-	Reflected XSS on Zomato API (https://hackerone.com/reports/125762)
Uber (https://hackerone.com/uber) ★	-	Session retention is present which reveals the customer info (https://hackerone.com/reports/125634)
Uber (https://hackerone.com/uber) ★	-	Brute Force Amplification Attack (https://hackerone.com/reports/125624)
Uber (https://hackerone.com/uber) ★	-	CSRF on eng.uber.com may lead to server-side compromise (https://hackerone.com/reports/125594)
Uber (https://hackerone.com/uber) ★	$5,000	Possibility to brute force invite codes in riders.uber.com (https://hackerone.com/reports/125505)
Uber (https://hackerone.com/uber) ★	-	Stored Cross Site Scripting [SELF] in partners.uber.com (https://hackerone.com/reports/125503)
Uber (https://hackerone.com/uber) ★	$3,000	Dom Based Xss (https://hackerone.com/reports/125498)
Uber (https://hackerone.com/uber) ★	$500	Estimation of a Lower Bound on Number of Uber Drivers via Enumeration (https://hackerone.com/reports/125488)
New Relic (https://hackerone.com/newrelic)	-	Too many included lookups (https://hackerone.com/reports/125400)
PHP (https://hackerone.com/ibb-php)	-	Null pointer deref (segfault) in stream_context_get_default (https://hackerone.com/reports/125397)
Mapbox (https://hackerone.com/mapbox)	$1,000	XSS (cross-site scripting) on www.mapbox.com/maki (https://hackerone.com/reports/125386)
Uber (https://hackerone.com/uber) ★	$3,000	Avoiding Surge Pricing (https://hackerone.com/reports/125250)
Uber (https://hackerone.com/uber) ★	-	Create account in uber without signup form (https://hackerone.com/reports/125242)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	$2,000	Bypassing Uber Partner's 3 Cancel Limit (https://hackerone.com/reports/125218)
Uber (https://hackerone.com/uber) ★	$3,000	Lack of rate limiting on get.uber.com leads to enumeration of promotion codes and estimation of a lower bound on the number of Uber drivers (https://hackerone.com/reports/125200)
Uber (https://hackerone.com/uber) ★	$3,000	SQLi in love.uber.com (https://hackerone.com/reports/125181)
Uber (https://hackerone.com/uber) ★	-	XSS on love.uber.com (https://hackerone.com/reports/125179)
Uber (https://hackerone.com/uber) ★	-	HTML Escaping Error in the 404 Page on developer.uber.com/docs/ (https://hackerone.com/reports/125130)
Uber (https://hackerone.com/uber) ★	$1,500	Lack of CNAME/A Record Trimming Pointing Uber Domains to Insecure Non-Uber AWS Instances/Sites (https://hackerone.com/reports/125118)
Uber (https://hackerone.com/uber) ★	$3,000	XSS in getrush.uber.com (https://hackerone.com/reports/125112)
Uber (https://hackerone.com/uber) ★	-	LIsting of http://archive.uber.com/pypi/simple/ (https://hackerone.com/reports/125068)
Uber (https://hackerone.com/uber) ★	-	Self-XSS Vulnerability on Password Reset Form (https://hackerone.com/reports/125059)
Uber (https://hackerone.com/uber) ★	$3,000	Reflected XSS on developer.uber.com via Angular template injection (https://hackerone.com/reports/125027)
Uber (https://hackerone.com/uber) ★	$500	Open Redirect in m.uber.com (https://hackerone.com/reports/125000)
Gratipay (https://hackerone.com/gratipay)	$1	Hijacking user session by forcing the use of invalid HTTPs Certificate on images.gratipay.com (https://hackerone.com/reports/124976)
Uber (https://hackerone.com/uber) ★	-	Cross-site Scripting (XSS) autocomplete generation in https://www.uber.com/ (https://hackerone.com/reports/124975)
HackerOne (https://hackerone.com/security)	$1,500	External programs revealing info (https://hackerone.com/reports/124929)
HackerOne (https://hackerone.com/security)	$500	Websites opened from reports can change url of report page (https://hackerone.com/reports/124889)
Shopify (https://hackerone.com/shopify) ★	$500	Bypassed password authentication before enabling OTP verification (https://hackerone.com/reports/124845)

Team	Bounty	Title
New Relic (https://hackerone.com/newrelic)	-	Stored XSS through Angular Expression Sandbox Escape (https://hackerone.com/reports/124724)
HackerOne (https://hackerone.com/security)	-	External links should use rel="noopener" or use the redirect service (https://hackerone.com/reports/124620)
HackerOne (https://hackerone.com/security)	$500	Disclosure of private programs that have an "external" page on HackerOne (https://hackerone.com/reports/124611)
Vimeo (https://hackerone.com/vimeo)	-	Missing rate limit on private videos password (https://hackerone.com/reports/124564)
Shopify (https://hackerone.com/shopify) ★	$500	Stored XSS via "Free Shipping" option (Discounts) (https://hackerone.com/reports/124429)
Imgur (https://hackerone.com/imgur)	$100	XSS via React element spoofing (https://hackerone.com/reports/124277)
HackerOne (https://hackerone.com/security)	$500	CSV Injection via the CSV export feature (https://hackerone.com/reports/124223)
Veris (https://hackerone.com/veris)	-	Captcha Bypass enable login bruteforce (https://hackerone.com/reports/124173)
Zomato (https://hackerone.com/zomato)	-	Authentication Bypassing and Sensitive Information Disclosure on Verify Email Address in Registration Flow (https://hackerone.com/reports/124151)
Veris (https://hackerone.com/veris)	-	Wordpress Pingback DDoS Attacks in domain: veris.in (https://hackerone.com/reports/124097)
Trello (https://hackerone.com/trello)	$768	Using WebSocket I can always access organization data even if I am removed (https://hackerone.com/reports/123984)
Veris (https://hackerone.com/veris)	-	Stored XSS in Access Rules (https://hackerone.com/reports/123905)
Veris (https://hackerone.com/veris)	-	Complete Profile URL is not Random and not expiring (https://hackerone.com/reports/123902)
Gratipay (https://hackerone.com/gratipay)	-	csrf_token cookie don't have the flag "HttpOnly" (https://hackerone.com/reports/123900)
Gratipay (https://hackerone.com/gratipay)	$1	auto-logout after 20 minutes (https://hackerone.com/reports/123897)
Gratipay (https://hackerone.com/gratipay)	$1	Cookie Does Not Contain The "secure" Attribute (https://hackerone.com/reports/123849)

Team	Bounty	Title
Gratipay (https://hackerone.com/gratipay)	-	Vulnerable to clickjacking (https://hackerone.com/reports/123782)
Veris (https://hackerone.com/veris)	-	Not Using Secure Flag Option on Cookies Could Lead to a Man in the Middle Session Highjacking (https://hackerone.com/reports/123748)
HackerOne (https://hackerone.com/security)	-	Sending emails (via HackerOne) impersonating other users (https://hackerone.com/reports/123743)
Gratipay (https://hackerone.com/gratipay)	$1	suppress version in Server header on gratipay.com or grtp.co (https://hackerone.com/reports/123742)
Veris (https://hackerone.com/veris)	-	Complete or Edit Another User's Profile (https://hackerone.com/reports/123731)
Veris (https://hackerone.com/veris)	-	Insecure Direct 'org-visitor-log' References (https://hackerone.com/reports/123713)
Veris (https://hackerone.com/veris)	-	Insecure Direct 'org-invite-log' References (https://hackerone.com/reports/123712)
Dropbox (https://hackerone.com/dropbox)	-	Possible SQL injection can cause denial of service attack (https://hackerone.com/reports/123660)
New Relic (https://hackerone.com/newrelic)	-	Synthetics Xss (https://hackerone.com/reports/123649)
Informatica (https://hackerone.com/informatica)	-	[marketplace.informatica.com] Open Redirect (https://hackerone.com/reports/123625)
HackerOne (https://hackerone.com/security)	$500	SECURITY: Referencing previous Reports attachment_IDs on new Reports via Draft_Sync DELETES Attachments (https://hackerone.com/reports/123615)
HackerOne (https://hackerone.com/security)	-	Unauthorized Team members viewing (https://hackerone.com/reports/123572)
Veris (https://hackerone.com/veris)	-	Security Vulnerability - SMTP protection not used (https://hackerone.com/reports/123518)
New Relic (https://hackerone.com/newrelic)	-	Host Header Injection / Cache Poisoning (https://hackerone.com/reports/123513)
Veris (https://hackerone.com/veris)	-	Insecure Direct Member Disclosure (https://hackerone.com/reports/123501)

Team	Bounty	Title
Veris (https://hackerone.com/veris)	-	User enumeration via error message (https://hackerone.com/reports/123496)
New Relic (https://hackerone.com/newrelic)	-	Normal user can set "Job title" of other users by Direct Object Reference (https://hackerone.com/reports/123435)
HackerOne (https://hackerone.com/security)	$500	Mediation link can be accepted by other users (https://hackerone.com/reports/123420)
Veris (https://hackerone.com/veris)	-	Creating multiple user with the same link which is sent to email after registeration (https://hackerone.com/reports/123380)
HackerOne (https://hackerone.com/security)	-	Possible XSS (https://hackerone.com/reports/123278)
Veris (https://hackerone.com/veris)	-	Server and PHP version Disclosed in Response Header (https://hackerone.com/reports/123194)
New Relic (https://hackerone.com/newrelic)	-	All the active session should destroy when user change his password (https://hackerone.com/reports/123183)
New Relic (https://hackerone.com/newrelic)	-	Open redirection on login (https://hackerone.com/reports/123172)
HackerOne (https://hackerone.com/security)	-	Email Address Leak (https://hackerone.com/reports/123170)
New Relic (https://hackerone.com/newrelic)	-	no email confirmation on signup (https://hackerone.com/reports/123127)
New Relic (https://hackerone.com/newrelic)	-	newrelic.com vulnerable to clickjacking ! (https://hackerone.com/reports/123126)
Shopify (https://hackerone.com/shopify) ★	$500	XSS on hardware.shopify.com (https://hackerone.com/reports/123125)
New Relic (https://hackerone.com/newrelic)	-	Emails and alert policies can be altered by malicious users. (https://hackerone.com/reports/123120)
Mail.Ru (https://hackerone.com/mailru)	-	Reflected XSS на games.mail.ru (https://hackerone.com/reports/123093)
New Relic (https://hackerone.com/newrelic)	-	Vulnerable Link Leaks the User Names (https://hackerone.com/reports/123089)

Team	Bounty	Title
New Relic (https://hackerone.com/newrelic)	-	https://rpm.newrelic.com/.htaccess file is world readable (https://hackerone.com/reports/123074)
HackerOne (https://hackerone.com/security)	$1,000	Edit Auto Response Messages (https://hackerone.com/reports/123027)
Zomato (https://hackerone.com/zomato)	-	Persistent XSS on Reservation / Booking Page (https://hackerone.com/reports/123005)
Mail.Ru (https://hackerone.com/mailru)	$200	bgplay.mail.ru (https://hackerone.com/reports/122932)
Xero (https://hackerone.com/xero)	-	Default.aspx exposing full path and other info on wip.origin-community.xero.com (https://hackerone.com/reports/122898)
Shopify (https://hackerone.com/shopify) ★	$500	Stored XSS in https://checkout.shopify.com/ (https://hackerone.com/reports/122849)
Uber (https://hackerone.com/uber) ★	-	Active Email Hyperlink Sent on riders.uber.com (https://hackerone.com/reports/122791)
New Relic (https://hackerone.com/newrelic)	-	Server Side Browsing - localhost open port enumeration (https://hackerone.com/reports/122697)
Imgur (https://hackerone.com/imgur)	$5,000	Local file read in image editor (https://hackerone.com/reports/122475)
Mapbox (https://hackerone.com/mapbox)	$200	Mapbox API Access Token with No Scope Can Read Styles (https://hackerone.com/reports/122050)
Ubiquiti Networks (https://hackerone.com/ubnt)	$1,300	Shell Injection via Web Management Console (dl-fw.cgi) (https://hackerone.com/reports/121940)
Vimeo (https://hackerone.com/vimeo)	$100	Private, embeddable videos leaks data through Facebook & Open Graph (https://hackerone.com/reports/121919)
Xero (https://hackerone.com/xero)	-	Additonal stored XSS in Add note/Expected payment Date (https://hackerone.com/reports/121903)
PHP (https://hackerone.com/ibb-php)	$1,000	Buffer overflow in HTTP url parsing functions (https://hackerone.com/reports/121863)
Badoo (https://hackerone.com/badoo)	$850	Account Takeover (https://hackerone.com/reports/121827)
Xero (https://hackerone.com/xero)	-	Vulnerability : XSS Vulnerability (https://hackerone.com/reports/121705)

Team	Bounty	Title
LocalTapiola (https://hackerone.com/localtapiola)	$400	CRLF injection in https://verkkopalvelu.lahitapiola.fi/ (https://hackerone.com/reports/121489)
Badoo (https://hackerone.com/badoo)	$427	Broken Authentication on Badoo (https://hackerone.com/reports/121469)
Bime (https://hackerone.com/bime)	$150	Subdomain takeover due to unclaimed Amazon S3 bucket on a2.bime.io (https://hackerone.com/reports/121461)
ownCloud (https://hackerone.com/owncloud)	-	doc.owncloud.org has missing PHP handler (https://hackerone.com/reports/121382)
Veris (https://hackerone.com/veris)	-	Multiple Stored XSS on Sanbox.veris.in through Veris Frontdesk Android App (https://hackerone.com/reports/121275)
General Motors (https://hackerone.com/gm)	-	Reflected Cross Site Script in m.chevrolet.com.wpsegment5.gm.com (https://hackerone.com/reports/120656)
Veris (https://hackerone.com/veris)	-	Multiple Stored XSS (https://hackerone.com/reports/120324)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Make Rule for Any Group & Any Venue remotely (https://hackerone.com/reports/120318)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Get Rules of any organization remotely (https://hackerone.com/reports/120314)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Can select any Parent while creating new Venue (https://hackerone.com/reports/120312)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Get venue data of any organization remotely (https://hackerone.com/reports/120305)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Get Authentication Details of any Terminal/Gatekeeper (https://hackerone.com/reports/120293)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Set anyone's Terminal Data remotely (https://hackerone.com/reports/120291)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Get anyone's Terminal Data remotely (https://hackerone.com/reports/120289)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Delete any terminal/gatekeeper of any organization remotely (https://hackerone.com/reports/120288)
Veris (https://hackerone.com/veris)	-	Missing Server Side Validation of CSRF Middleware Token in Change Password Request (https://hackerone.com/reports/120143)

Team	Bounty	Title
Veris (https://hackerone.com/veris)	-	Critical IDOR - Delete any rule of any organization remotely (https://hackerone.com/reports/120126)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Delete any venue of any organization remotely (https://hackerone.com/reports/120123)
Veris (https://hackerone.com/veris)	-	Critical IDOR - Delete any group of any organization remotely (https://hackerone.com/reports/120121)
Veris (https://hackerone.com/veris)	-	Critical - Insecure Direct Object Reference - Deleting any member of any organization remotely (https://hackerone.com/reports/120115)
Gratipay (https://hackerone.com/gratipay)	$1	don't serve hidden files from Nginx (https://hackerone.com/reports/120026)
OpenSSL (https://hackerone.com/ibb-openssl)	-	b2i_PVK_bio heap corruption (https://hackerone.com/reports/119989)
Pornhub (https://hackerone.com/pornhub)	$250	Public Facing Barracuda Login (https://hackerone.com/reports/119918)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	BN_hex2bn/BN_dec2bn NULL pointer deref/heap corruption (CVE-2016-0797) (https://hackerone.com/reports/119873)
Pornhub (https://hackerone.com/pornhub)	$2,500	Unprotected Memcache Installation running (https://hackerone.com/reports/119871)
Pornhub (https://hackerone.com/pornhub)	$50	HTTP Track/Trace Method Enabled (https://hackerone.com/reports/119860)
LeaseWeb (https://hackerone.com/leaseweb)	-	Found clickjacking vulnerability (https://hackerone.com/reports/119828)
ownCloud (https://hackerone.com/owncloud)	-	DROWN Attack (https://hackerone.com/reports/119808)
Badoo (https://hackerone.com/badoo)	-	Password modification without knowing actual password & httpOnly bypass (https://hackerone.com/reports/119794)
LeaseWeb (https://hackerone.com/leaseweb)	-	Server version is disclosure in http://leasewebnoc.com/ (https://hackerone.com/reports/119666)
Coinbase (https://hackerone.com/coinbase)	-	An adversary can overwhelm the resources by automating Forgot password/Sign Up requests (https://hackerone.com/reports/119605)

Team	Bounty	Title
Veris (https://hackerone.com/veris)	-	Password(s) can be found via login process. (https://hackerone.com/reports/119454)
Veris (https://hackerone.com/veris)	-	www.veris.in DOM based XSS (https://hackerone.com/reports/119453)
HackerOne (https://hackerone.com/security)	-	Race Conditions Exist When Accepting Invitations (https://hackerone.com/reports/119354)
Ubiquiti Networks (https://hackerone.com/ubnt)	$1,500	Read-Only user can execute arbitraty shell commands on AirOS (https://hackerone.com/reports/119317)
Udemy (https://hackerone.com/udemy)	$150	Session Takeover vulnerability (https://hackerone.com/reports/119262)
Shopify (https://hackerone.com/shopify) ★	$500	xss in the all widgets of shopifyapps.com (https://hackerone.com/reports/119250)
Uber (https://hackerone.com/uber) ★	$500	Open Redirection on Uber.com (https://hackerone.com/reports/119236)
HackerOne (https://hackerone.com/security)	$500	User with Read-Only permissions can edit the Internal comment Activities on Bug Reports After Revoke the team access permissions (https://hackerone.com/reports/119221)
Twitter (https://hackerone.com/twitter)	$280	Sub-Domain Takeover (https://hackerone.com/reports/119220)
InVision (https://hackerone.com/invision)	$500	CRITICAL Stored XSS in https://projects.invisionapp.com (https://hackerone.com/reports/119203)
New Relic (https://hackerone.com/newrelic)	-	CSRF - Regenerate all admin api keys (https://hackerone.com/reports/119148)
Coinbase (https://hackerone.com/coinbase)	$500	Misconfiguration in 2 factor allows sensitive data expose (https://hackerone.com/reports/119129)
Cakebet (https://hackerone.com/cakebet)	-	Sender policy framework (SPF) records evaluation return (Too many DNS lookups) error (https://hackerone.com/reports/119033)
Twitter (https://hackerone.com/twitter)	$2,520	Tweet Deck XSS- Persistent- Group DM name (https://hackerone.com/reports/119022)
HackerOne (https://hackerone.com/security)	$500	Distinguish EP+Private vs Private programs in HackerOne (https://hackerone.com/reports/118965)
Veris (https://hackerone.com/veris)	-	Stored XSS (https://hackerone.com/reports/118950)

Team	Bounty	Title
Veris (https://hackerone.com/veris)	-	Password reset link is not Expiring (https://hackerone.com/reports/118948)
Algolia (https://hackerone.com/algolia)	$1,000	API Key added for one Indices works for all other indices too. (https://hackerone.com/reports/118925)
OpenSSL (https://hackerone.com/ibb-openssl)	$500	CVE-2016-0799 memory issues in BIO_*printf functions (https://hackerone.com/reports/118855)
ThisData (https://hackerone.com/thisdata)	-	Login CSRF using Google OAuth (https://hackerone.com/reports/118737)
HackerOne (https://hackerone.com/security)	-	User with Read-Only permissions can edit the SwagAwarded Activities on Bug Reports (https://hackerone.com/reports/118731)
HackerOne (https://hackerone.com/security)	$500	User with Read-Only permissions can manually public disclosure the report (https://hackerone.com/reports/118718)
Shopify (https://hackerone.com/shopify) ★	$500	File name and folder enumeration. (https://hackerone.com/reports/118688)
HackerOne (https://hackerone.com/security)	-	Abusing HOF rankings in limited circumstances (https://hackerone.com/reports/118684)
HackerOne (https://hackerone.com/security)	-	Denial of Service any Report (https://hackerone.com/reports/118663)
HackerOne (https://hackerone.com/security)	$500	CSV Injection at the CSV export feature (https://hackerone.com/reports/118582)
KIWI.KI GmbH (https://hackerone.com/kiwi-ki)	-	Subdomain takeover : URGENT (https://hackerone.com/reports/118514)
Mail.Ru (https://hackerone.com/mailru)	-	Утечка информации через JSONP (XXSI) (https://hackerone.com/reports/118418)
Shopify (https://hackerone.com/shopify) ★	-	Injection via CSV Export feature in Admin Orders (https://hackerone.com/reports/118103)
LeaseWeb (https://hackerone.com/leaseweb)	-	MISSING SPF RECORDS & MISSING DKIM POLICY (https://hackerone.com/reports/117818)
LeaseWeb (https://hackerone.com/leaseweb)	-	Apache version disclosed on developer.leaseweb.com (https://hackerone.com/reports/117593)

Team	Bounty	Title
LeaseWeb (https://hackerone.com/leaseweb)	-	Directory Listening (https://hackerone.com/reports/117573)
Zendesk (https://hackerone.com/zendesk)	$50	Stored XSS via Angular Expression injection on developer.zendesk.com (https://hackerone.com/reports/117480)
Gratipay (https://hackerone.com/gratipay)	$1	strengthen Diffie-Hellman (DH) key exchange parameters in grtp.co (https://hackerone.com/reports/117458)
Shopify (https://hackerone.com/shopify) ★	$500	XSS in Draft Orders in Timeline i SHOPIFY Admin Site! (https://hackerone.com/reports/117449)
LeaseWeb (https://hackerone.com/leaseweb)	-	PHP and Web Server version disclosed on leasewebnoc.com (https://hackerone.com/reports/117385)
Gratipay (https://hackerone.com/gratipay)	$1	stop serving grtp.co over HTTP (https://hackerone.com/reports/117330)
Gratipay (https://hackerone.com/gratipay)	$10	DMARC is misconfigured for grtp.co (https://hackerone.com/reports/117325)
Uber (https://hackerone.com/uber) ★	$3,000	Reflected XSS on Uber.com careers (https://hackerone.com/reports/117190)
Gratipay (https://hackerone.com/gratipay)	$2	SPF/DKIM/DMARC for aspen.io (https://hackerone.com/reports/117159)
Mail.Ru (https://hackerone.com/mailru)	$250	SSRF на element.mail.ru (https://hackerone.com/reports/117158)
Gratipay (https://hackerone.com/gratipay)	$2	SPF/DKIM/DMARC for grtp.co (https://hackerone.com/reports/117149)
Gratipay (https://hackerone.com/gratipay)	$1	limit HTTP methods on other domains (https://hackerone.com/reports/117142)
Gratipay (https://hackerone.com/gratipay)	$10	Email Forgery through Mandrillapp SPF (https://hackerone.com/reports/117097)
Uber (https://hackerone.com/uber) ★	$250	Multiple Vulnerabilities (Including SQLi) in love.uber.com (https://hackerone.com/reports/117080)
Informatica (https://hackerone.com/informatica)	-	[informatica.com] Blind SQL Injection (https://hackerone.com/reports/117073)
Uber (https://hackerone.com/uber) ★	$3,000	XSS @ love.uber.com (https://hackerone.com/reports/117068)
Gratipay (https://hackerone.com/gratipay)	$10	No Valid SPF Records. (https://hackerone.com/reports/116973)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	$500	Increase number of bugs by sending duplicate of your own valid report (https://hackerone.com/reports/116951)
Zopim (https://hackerone.com/zopim)	$100	Chat History CSV Export Excel Injection Vulnerability (https://hackerone.com/reports/116937)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Spf (https://hackerone.com/reports/116927)
Legal Robot (https://hackerone.com/legalrobot)	$20	SSL Issue on legalrobot.com (https://hackerone.com/reports/116805)
HackerOne (https://hackerone.com/security)	$500	Private Program Disclosure in /:handle/settings/allow_report_submission.json endpoint (https://hackerone.com/reports/116798)
Gratipay (https://hackerone.com/gratipay)	-	UDP port 5060 (SIP) Open (https://hackerone.com/reports/116774)
Algolia (https://hackerone.com/algolia)	-	PHP version disclosed on blog.algolia.com (https://hackerone.com/reports/116692)
Gratipay (https://hackerone.com/gratipay)	-	server calendar and server status available to public (https://hackerone.com/reports/116621)
Gratipay (https://hackerone.com/gratipay)	-	proxy port 7000 and shell port 514 not filtered (https://hackerone.com/reports/116618)
Legal Robot (https://hackerone.com/legalrobot)	$20	SPF Issue (https://hackerone.com/reports/116609)
Legal Robot (https://hackerone.com/legalrobot)	$120	Remote Code Execution (upload) (https://hackerone.com/reports/116575)
Mail.Ru (https://hackerone.com/mailru)	$600	VERY DANGEROUS XSS STORED inside emails (https://hackerone.com/reports/116570)
Mail.Ru (https://hackerone.com/mailru)	$150	[3k.mail.ru] SQL Injection (https://hackerone.com/reports/116508)
Ubiquiti Networks (https://hackerone.com/ubnt)	$1,000	Auth bypass on directory.corp.ubnt.com (https://hackerone.com/reports/116504)
General Motors (https://hackerone.com/gm)	-	E-mail Spoof in media.gm.com (https://hackerone.com/reports/116432)
Slack (https://hackerone.com/slack)	$100	an xss issue in https://hunter22.slack.com/help/requests/793043 (https://hackerone.com/reports/116419)

Team	Bounty	Title
General Motors (https://hackerone.com/gm)	-	Content Spoof in webcaps.ecomm.gm.com (https://hackerone.com/reports/116382)
Gratipay (https://hackerone.com/gratipay)	$1	The POODLE attack (SSLv3 supported) for https://grtp.co/ (https://hackerone.com/reports/116360)
Gratipay (https://hackerone.com/gratipay)	-	nginx SPDY heap buffer overflow for https://grtp.co/ (https://hackerone.com/reports/116352)
WePay (https://hackerone.com/wepay)	$150	2-step Verification bypass (https://hackerone.com/reports/116302)
Python (https://hackerone.com/ibb-python)	$1,000	Type confusion in partial.setstate, partial_repr, partial_call leads to memory corruption, reliable control flow hijack (https://hackerone.com/reports/116286)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Persistent XSS In Account Profile (https://hackerone.com/reports/116254)
New Relic (https://hackerone.com/newrelic)	-	Potential Subdomain Takeover - http://storefront.newrelic.com/ (https://hackerone.com/reports/116243)
Sucuri (https://hackerone.com/sucuri)	$500	Manipulating of Sucuri.net (List Subscription) Emails (HTML/Script Injection) (https://hackerone.com/reports/116214)
HackerOne (https://hackerone.com/security)	-	Null byte injection (https://hackerone.com/reports/116189)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	file full path discloser. (https://hackerone.com/reports/116057)
HackerOne (https://hackerone.com/security)	$500	Private Program Disclosure in /:handle/reports/draft.json endpoint (https://hackerone.com/reports/116032)
HackerOne (https://hackerone.com/security)	$5,000	Private program activity timeline information disclosure (https://hackerone.com/reports/116029)
Shopify (https://hackerone.com/shopify) ★	$500	XSS on hardware.shopify.com (https://hackerone.com/reports/116006)
Imgur (https://hackerone.com/imgur)	$1,000	SSRF / Local file enumeration / DoS due to improper handling of certain file formats by ffmpeg (https://hackerone.com/reports/115978)
New Relic (https://hackerone.com/newrelic)	-	[login.newrelic.com] XSS via return_to (https://hackerone.com/reports/115860)

Team	Bounty	Title
Imgur (https://hackerone.com/imgur)	$800	SSRF and local file read in video to gif converter (https://hackerone.com/reports/115857)
Legal Robot (https://hackerone.com/legalrobot)	$20	Rate limiting on Email confirmation link (https://hackerone.com/reports/115845)
Legal Robot (https://hackerone.com/legalrobot)	-	Rate limiting on password reset links (https://hackerone.com/reports/115844)
Imgur (https://hackerone.com/imgur)	$2,000	SSRF in https://imgur.com/vidgif/url (https://hackerone.com/reports/115748)
New Relic (https://hackerone.com/newrelic)	-	SUBDOMAIN TAKEOVER(FIXED) (https://hackerone.com/reports/115628)
Zomato (https://hackerone.com/zomato)	-	Two XSS vulns in widget parameters (all_collections.php and o2.php) (https://hackerone.com/reports/115560)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Email Spoof (https://hackerone.com/reports/115452)
Urban Dictionary (https://hackerone.com/urbandictionary)	-	Cross-Site Scripting Vulnerability in urbandictionary.com (https://hackerone.com/reports/115438)
Zomato (https://hackerone.com/zomato)	-	XSS via modified Zomato widget (res_search_widget.php) (https://hackerone.com/reports/115402)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Missing SPF for paragonie.com (https://hackerone.com/reports/115390)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	$50	Full Path Disclosure (https://hackerone.com/reports/115337)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	CSRF AT SUBSCRIBE TO LIST (https://hackerone.com/reports/115323)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Missing SPF for paragonie.com (https://hackerone.com/reports/115315)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Blind SQL INJ (https://hackerone.com/reports/115304)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Missing SPF (https://hackerone.com/reports/115294)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	$300	[orsotenslimselfie.lady.mail.ru] SQL Injection (https://hackerone.com/reports/115291)
Gratipay (https://hackerone.com/gratipay)	$10	prevent content spoofing on /search (https://hackerone.com/reports/115284)
Gratipay (https://hackerone.com/gratipay)	$5	SPF DNS Record (https://hackerone.com/reports/115275)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	SSL certificate public key less than 2048 bit (https://hackerone.com/reports/115271)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Missing SPF records for paragonie.com (https://hackerone.com/reports/115250)
Zomato (https://hackerone.com/zomato)	-	XSS and CSRF in Zomato Contact form (https://hackerone.com/reports/115248)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	DNSsec not configured (https://hackerone.com/reports/115246)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Email Authentication bypass Vulnerability (https://hackerone.com/reports/115245)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Email spoofing (https://hackerone.com/reports/115232)
Keybase (https://hackerone.com/keybase)	$50	Content spoofing due to the improper behavior of the not-found meesage (https://hackerone.com/reports/115230)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Information Disclosure in Error Page (https://hackerone.com/reports/115219)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Missing SPF for https://paragonie.com/ (https://hackerone.com/reports/115214)
Uber (https://hackerone.com/uber) ★	-	Unauthorized file (invoice) download (https://hackerone.com/reports/115209)
HackerOne (https://hackerone.com/security)	$500	Putting link inside link in markdown (https://hackerone.com/reports/115205)
Zomato (https://hackerone.com/zomato)	-	Weak Password Policy (https://hackerone.com/reports/115036)
Keybase (https://hackerone.com/keybase)	$350	Race conditions can be used to bypass invitation limit (https://hackerone.com/reports/115007)

Team	Bounty	Title
Zomato (https://hackerone.com/zomato)	-	Persistent input validation mail encoding vulnerability in the "just followed you" email notification. (https://hackerone.com/reports/114879)
New Relic (https://hackerone.com/newrelic)	-	Basic Authorization over HTTP (https://hackerone.com/reports/114870)
New Relic (https://hackerone.com/newrelic)	-	Html injection in monitor name textbox (https://hackerone.com/reports/114852)
New Relic (https://hackerone.com/newrelic)	-	Unsafe HTML in reset password email and Account verification in email is missing in Sign up (https://hackerone.com/reports/114807)
New Relic (https://hackerone.com/newrelic)	-	No validation on account names (https://hackerone.com/reports/114796)
Keybase (https://hackerone.com/keybase)	$250	Remote Server Restart Lead to Denial of Service by only one Request. (https://hackerone.com/reports/114698)
Zomato (https://hackerone.com/zomato)	-	Several XSS affecting Zomato.com and developers.zomato.com (https://hackerone.com/reports/114631)
Mapbox (https://hackerone.com/mapbox)	$200	Content Spoofing and Local Redirect in Mapbox Studio (https://hackerone.com/reports/114529)
VK.com (https://hackerone.com/vkcom)	$2,500	Внедрение внешних сущностей в функционале импорта пользователей YouTrack (https://hackerone.com/reports/114476)
Shopify (https://hackerone.com/shopify) ★	$500	CSRF on https://shopify.com/plus (https://hackerone.com/reports/114430)
Zomato (https://hackerone.com/zomato)	-	Remote File Upload Vulnerability in business-blog.zomato.com (https://hackerone.com/reports/114389)
Mail.Ru (https://hackerone.com/mailru)	-	[touch.lady.mail.ru] CRLF Injection (https://hackerone.com/reports/114198)
Twitter (https://hackerone.com/twitter)	$2,520	Bypassing Digits web authentication's host validation with HPP (https://hackerone.com/reports/114169)
Zomato (https://hackerone.com/zomato)	-	Cross Site Scripting - type Patameter (https://hackerone.com/reports/114151)
Snapchat (https://hackerone.com/snapchat)	$1,000	Subdomain takeover in http://support.scan.me pointing to Zendesk (a Snapchat acquisition) (https://hackerone.com/reports/114134)

Team	Bounty	Title
Zomato (https://hackerone.com/zomato)	-	Twitter Disconnect CSRF (https://hackerone.com/reports/114127)
Keybase (https://hackerone.com/keybase)	$250	Remote Server Restart Lead to Denial of Server by only one Request. (https://hackerone.com/reports/114125)
Ruby on Rails (https://hackerone.com/rails)	-	Remote code execution using render :inline (https://hackerone.com/reports/113928)
Zomato (https://hackerone.com/zomato)	-	Subdomain Takeover (https://hackerone.com/reports/113869)
Zomato (https://hackerone.com/zomato)	-	CSRF AT INVITING PEOPLE THOUGH PHONE NUMBER (https://hackerone.com/reports/113865)
Zomato (https://hackerone.com/zomato)	-	CSRF AT SELECTING ZAMATO HANDLE (https://hackerone.com/reports/113857)
Ruby on Rails (https://hackerone.com/rails)	-	Regarding [CVE-2016-0752] Possible Information Leak Vulnerability in Action View (https://hackerone.com/reports/113831)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	-	Cross-domain AJAX request (https://hackerone.com/reports/113339)
OpenSSL (https://hackerone.com/ibb-openssl)	$2,500	OpenSSL Key Recovery Attack on DH small subgroups (CVE-2016-0701) (https://hackerone.com/reports/113288)
ownCloud (https://hackerone.com/owncloud)	-	No Any Kind of Protection on Delete account (https://hackerone.com/reports/113211)
Paragon Initiative Enterprises (https://hackerone.com/paragonie)	$50	Open-redirect on paragonie.com (https://hackerone.com/reports/113112)
HackerOne (https://hackerone.com/security)	$500	Multiple issues with Markdown and URL parsing (https://hackerone.com/reports/113070)
withinsecurity (https://hackerone.com/withinsecurity)	$250	WordPress Failure Notice page will generate arbitrary hyperlinks (https://hackerone.com/reports/112955)
HackerOne (https://hackerone.com/security)	$500	Unintended HTML inclusion as a result of https://hackerone.com/reports/110578 (https://hackerone.com/reports/112935)
Gratipay (https://hackerone.com/gratipay)	-	grtp.co is vulnerable to http-vuln-cve2011-3192 (https://hackerone.com/reports/112687)
Mail.Ru (https://hackerone.com/mailru)	$300	[afisha.mail.ru] SQL Injection (https://hackerone.com/reports/112555)

Team	Bounty	Title
Coinbase (https://hackerone.com/coinbase)	$1,000	Session Issue Maybe Can lead to huge loss [CRITICAL] (https://hackerone.com/reports/112496)
Binary.com (https://hackerone.com/binary)	$250	Full takeover of some binary.com sub domains (https://hackerone.com/reports/112306)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.help: Text Injection (https://hackerone.com/reports/112304)
Bime (https://hackerone.com/bime)	$100	The JDBC driver used by the Vertica connector allows to create files on the backends (https://hackerone.com/reports/112166)
Bime (https://hackerone.com/bime)	$1,000	SSRF in the Connector Designer (REST and Elastic Search) (https://hackerone.com/reports/112156)
Bime (https://hackerone.com/bime)	$750	XXE in the Connector Designer (https://hackerone.com/reports/112116)
Udemy (https://hackerone.com/udemy)	-	Stored XSS (https://hackerone.com/reports/112025)
General Motors (https://hackerone.com/gm)	-	XSS on gmchat.gm.com (https://hackerone.com/reports/112001)
General Motors (https://hackerone.com/gm)	-	Full Path Disclosure on gmchat.gm.com (https://hackerone.com/reports/111999)
HackerOne (https://hackerone.com/security)	$500	Interstitial redirect bypass / open redirect in https://hackerone.com/zendesk_session (https://hackerone.com/reports/111968)
Mail.Ru (https://hackerone.com/mailru)	$150	[allods.my.com] SSRF / XSPA (https://hackerone.com/reports/111950)
Zendesk (https://hackerone.com/zendesk)	$100	[CRITICAL] HTML injection issue leading to account take over (https://hackerone.com/reports/111915)
HackerOne (https://hackerone.com/security)	-	Report title and issue information prepopulated (https://hackerone.com/reports/111868)
withinsecurity (https://hackerone.com/withinsecurity)	$250	Error Page Text Injection #106350 (https://hackerone.com/reports/111860)
Khan Academy (https://hackerone.com/khanacademy)	-	XSS vulnerability in "/coach/roster/" (create your first class) (https://hackerone.com/reports/111763)
Imgur (https://hackerone.com/imgur)	$50	Big Bug in SSL : breach compression attack (CVE-2013-3587) affect imgur.com (https://hackerone.com/reports/111752)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	-	attack in not an authorized user (https://hackerone.com/reports/111676)
Shopify (https://hackerone.com/shopify) ★	$500	Full access to Amazon S3 bucket containing AWS CloudTrail logs (https://hackerone.com/reports/111643)
Automattic (https://hackerone.com/automattic)	$75	XSS at wordpress.com (https://hackerone.com/reports/111500)
Shopify (https://hackerone.com/shopify) ★	$500	www.shopify.com XSS via third-party script (https://hackerone.com/reports/111475)
Trello (https://hackerone.com/trello)	$1,152	DOM based XSS via Wistia embedding (https://hackerone.com/reports/111440)
VK.com (https://hackerone.com/vkcom)	$100	Checking whether user liked the media or not even when you are blocked (https://hackerone.com/reports/111417)
Vimeo (https://hackerone.com/vimeo)	$100	Legacy API exposes private video titles (https://hackerone.com/reports/111386)
Automattic (https://hackerone.com/automattic)	$75	XSS at www.woothemes.com (https://hackerone.com/reports/111365)
Pornhub (https://hackerone.com/pornhub)	$1,500	[ssrf] libav vulnerable during conversion of uploaded videos (https://hackerone.com/reports/111269)
ownCloud (https://hackerone.com/owncloud)	-	The csrf token remains same after user logs in (https://hackerone.com/reports/111262)
Shopify (https://hackerone.com/shopify) ★	$500	Attach Pinterest account - no State/CSRF parameter in Oauth Call back (https://hackerone.com/reports/111218)
Shopify (https://hackerone.com/shopify) ★	$500	Twitter Disconnect CSRF (https://hackerone.com/reports/111216)
HackerOne (https://hackerone.com/security)	$500	CSV Injection via the CSV export feature (https://hackerone.com/reports/111192)
Binary.com (https://hackerone.com/binary)	-	XSS (https://hackerone.com/reports/111131)
withinsecurity (https://hackerone.com/withinsecurity)	$250	Content Spoofing OR Text Injection in https://withinsecurity.com (https://hackerone.com/reports/111094)
Gratipay (https://hackerone.com/gratipay)	$15	Sub Domian Take over (https://hackerone.com/reports/111078)

Team	Bounty	Title
Automattic (https://hackerone.com/automattic)	$250	Internal GET SSRF via CSRF with Press This scan feature (https://hackerone.com/reports/110801)
ownCloud (https://hackerone.com/owncloud)	$250	Information Exposure Through Directory Listing (https://hackerone.com/reports/110655) **CVE-2016-1499** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1499)
HackerOne (https://hackerone.com/security)	$500	HTML injection can lead to data theft (https://hackerone.com/reports/110578)
Perl (https://hackerone.com/ibb-perl)	$1,000	Perl 5.22 VDir::MapPathA/W Out-of-bounds Reads and Buffer Over-reads (https://hackerone.com/reports/110352)
Phabricator (https://hackerone.com/phabricator)	$300	Extended policy checks are buggy (https://hackerone.com/reports/109959)
Binary.com (https://hackerone.com/binary)	-	HTML injection via 'underlying' parameter (https://hackerone.com/reports/109832)
Coinbase (https://hackerone.com/coinbase)	$200	Direct URL access to completed reports (https://hackerone.com/reports/109815)
Coinbase (https://hackerone.com/coinbase)	-	The 'Create a New Account' action is vulnerable to CSRF (https://hackerone.com/reports/109810)
Ubiquiti Networks (https://hackerone.com/ubnt)	$500	Subdomain Takeover in http://assets.goubiquiti.com/ (https://hackerone.com/reports/109699)
HackerOne (https://hackerone.com/security)	$500	User with Read-Only permissions can request/approve public disclosure (https://hackerone.com/reports/109483)
General Motors (https://hackerone.com/gm)	-	refelected Xss on https://gmid.gm.com/gmid/jsp/GMIDInitialLogin.jsp (https://hackerone.com/reports/109461)
HackerOne (https://hackerone.com/security)	-	Requesting unknown file type returns Ruby object w/ address (https://hackerone.com/reports/109420)
General Motors (https://hackerone.com/gm)	-	gmmovinparts.com SQLi via forgot_password.jsp (https://hackerone.com/reports/109395)
Mail.Ru (https://hackerone.com/mailru)	-	Multiple vulnerabilities in mail.ru subdomains (https://hackerone.com/reports/109373)
General Motors (https://hackerone.com/gm)	-	XSS in GM (https://hackerone.com/reports/109352)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	$150	[parapa.mail.ru] SQL Injection (https://hackerone.com/reports/109212)
PHP (https://hackerone.com/ibb-php)	$1,000	Use After Free in sortWithSortKeys() (https://hackerone.com/reports/109175)
Gratipay (https://hackerone.com/gratipay)	$5	HTTP trace method is enabled (https://hackerone.com/reports/109054)
HackerOne (https://hackerone.com/security)	-	Signals get affected once reports closed as self (https://hackerone.com/reports/108928)
Ruby on Rails (https://hackerone.com/rails)	-	Validation bypass for Active Record and Active Model (https://hackerone.com/reports/108723)
ownCloud (https://hackerone.com/owncloud)	-	Mixed Active Scripting Issue on stats.owncloud.org (https://hackerone.com/reports/108692)
ownCloud (https://hackerone.com/owncloud)	-	otrs.owncloud.com: Reflected Cross-Site Scripting (https://hackerone.com/reports/108288)
Twitter (https://hackerone.com/twitter)	$2,520	Bypassing callback_url validation on Digits (https://hackerone.com/reports/108113)
ownCloud (https://hackerone.com/owncloud)	$350	Exploiting unauthenticated encryption mode (https://hackerone.com/reports/108082)
ownCloud (https://hackerone.com/owncloud)	-	[https://test1.owncloud.com/owncloud6/] Guessable password used for admin user (https://hackerone.com/reports/107849)
Mail.Ru (https://hackerone.com/mailru)	$150	[cfire.mail.ru] Time Based SQL Injection (https://hackerone.com/reports/107780)
Mail.Ru (https://hackerone.com/mailru)	-	XSS at forum : (https://hackerone.com/reports/107718)
Mail.Ru (https://hackerone.com/mailru)	$500	reflected in xss (https://hackerone.com/reports/107358)
HackerOne (https://hackerone.com/security)	$500	Team Member(s) associated with a Group have Read-only permission (Post internal comments) can post comment to all the participants (https://hackerone.com/reports/107336)
WePay (https://hackerone.com/wepay)	$100	Unauthenticated Stored XSS in API Panel (https://hackerone.com/reports/107321)
Automattic (https://hackerone.com/automattic)	$50	Possible Timing Side-Channel in XMLRPC Verification (https://hackerone.com/reports/107296)

Team	Bounty	Title
GlassWire (https://hackerone.com/glasswire)	$100	GlassWireSetup.exe subject to EXE planting attack (https://hackerone.com/reports/107213)
Imgur (https://hackerone.com/imgur)	$150	XSS in imgur mobile 3 (https://hackerone.com/reports/107036)
Imgur (https://hackerone.com/imgur)	$150	XSS in imgur mobile (https://hackerone.com/reports/106982)
Shopify (https://hackerone.com/shopify) ★	$500	Stored XSS in /admin/orders (https://hackerone.com/reports/106897)
Zendesk (https://hackerone.com/zendesk)	$500	Stored XSS in comments (https://hackerone.com/reports/106779)
Shopify (https://hackerone.com/shopify) ★	$500	Strored Cross Site Scripting (https://hackerone.com/reports/106636)
PHP (https://hackerone.com/ibb-php)	$1,000	Format string vulnerability in zend_throw_or_error() (https://hackerone.com/reports/106548)
Shopify (https://hackerone.com/shopify) ★	$500	HTTP-Response-Splitting on v.shopify.com (https://hackerone.com/reports/106427)
CloudFlare (https://hackerone.com/cloudflare)	-	Clickjacking : https://partners.cloudflare.com/ (https://hackerone.com/reports/106362)
Coinbase (https://hackerone.com/coinbase)	$100	Race condition allowing user to review app multiple times (https://hackerone.com/reports/106360)
withinsecurity (https://hackerone.com/withinsecurity)	$250	text injection can be used in phishing 404 page should not include attacker text (https://hackerone.com/reports/106350)
Algolia (https://hackerone.com/algolia)	$100	text injection can be used in phishing 404 page should not include attacker text (https://hackerone.com/reports/106348)
Coinbase (https://hackerone.com/coinbase)	-	Potential for Double Spend via Sign Message Utility (https://hackerone.com/reports/106315)
HackerOne (https://hackerone.com/security)	$500	Improve signals in reputation (https://hackerone.com/reports/106305)
Shopify (https://hackerone.com/shopify) ★	$500	Reflective XSS on wholesale.shopify.com (https://hackerone.com/reports/106293)
HackerOne (https://hackerone.com/security)	$500	Team Member(s) associated with a Custom Group Created with 'Program Managment' only permissions can Comments on Bug Reports (https://hackerone.com/reports/106084)

Team	Bounty	Title
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Parameter pollution in social sharing buttons (https://hackerone.com/reports/106024)
Shopify (https://hackerone.com/shopify) ★	$500	"Remember me" token generated when "Remember me" box unchecked (https://hackerone.com/reports/105991)
ownCloud (https://hackerone.com/owncloud)	-	XXE at host vpn.owncloud.com (https://hackerone.com/reports/105980)
GlassWire (https://hackerone.com/glasswire)	$100	DLL Hijacking Vulnerability in GlassWireSetup.exe (https://hackerone.com/reports/105977)
HackerOne (https://hackerone.com/security)	$500	Parameter pollution in social sharing buttons (https://hackerone.com/reports/105953)
HackerOne (https://hackerone.com/security)	$500	Know whether private program for company exist or not (https://hackerone.com/reports/105887)
LeaseWeb (https://hackerone.com/leaseweb)	$100	DOM Based XSS in Checkout (https://hackerone.com/reports/105688)
Shopify (https://hackerone.com/shopify) ★	$500	many xss in widgets.shopifyapps.com (https://hackerone.com/reports/105659)
Phabricator (https://hackerone.com/phabricator)	-	libphutil: removing bytes from a PhutilRope does not work as intended (https://hackerone.com/reports/105657)
Pornhub (https://hackerone.com/pornhub)	$50	[crossdomain.xml] Dangerous Flash Cross-Domain Policy (https://hackerone.com/reports/105655)
Pornhub (https://hackerone.com/pornhub)	$250	PornIQ Reflected Cross-Site Scripting (https://hackerone.com/reports/105486)
Imgur (https://hackerone.com/imgur)	$150	risk of having secure=false in a crossdomain.xml (https://hackerone.com/reports/105463)
Informatica (https://hackerone.com/informatica)	-	[rev-app.informatica.com] - XXE (https://hackerone.com/reports/105434)
Instacart (https://hackerone.com/instacart)	$100	Cookie-Based Injection (https://hackerone.com/reports/105419)
Shopify (https://hackerone.com/shopify) ★	-	[livechat.shopify.com] Cookie bomb at customer chats (https://hackerone.com/reports/105363)

Team	Bounty	Title
Square Open Source (https://hackerone.com/square-open-source)	$2,000	Unsafe usage of Ruby string interpolation enabling command injection in git-fastclone (https://hackerone.com/reports/105190)
ownCloud (https://hackerone.com/owncloud)	-	directory listing in https://demo.owncloud.org/doc/ (https://hackerone.com/reports/105149)
Shopify (https://hackerone.com/shopify) ★	$500	CSRF in Connecting Pinterest Account (https://hackerone.com/reports/104931)
Instacart (https://hackerone.com/instacart)	$100	Cross-Site Scripting Reflected On Main Domain (https://hackerone.com/reports/104917)
Zopim (https://hackerone.com/zopim)	$100	[status.zopim.com] Open Redirect (https://hackerone.com/reports/104896)
Coinbase (https://hackerone.com/coinbase)	-	XXE in OAuth2 Applications gallery profile App logo (https://hackerone.com/reports/104620)
Automattic (https://hackerone.com/automattic)	$75	XSS on codex.wordpress.org (https://hackerone.com/reports/104559)
Coinbase (https://hackerone.com/coinbase)	$200	HTML injection in apps user review (https://hackerone.com/reports/104543)
Square Open Source (https://hackerone.com/square-open-source)	$2,000	git-fastclone allows arbitrary command execution through usage of ext remote URLs in submodules (https://hackerone.com/reports/104465)
Shopify (https://hackerone.com/shopify) ★	$1,000	shopifyapps.com XSS on sales channels via currency formatting (https://hackerone.com/reports/104359)
Slack (https://hackerone.com/slack)	$1,000	Trick make all fixed open redirect links vulnerable again (https://hackerone.com/reports/104087)
Python (https://hackerone.com/ibb-python)	$500	tokenizer crash when processing undecodable source code (https://hackerone.com/reports/104033)
Python (https://hackerone.com/ibb-python)	$1,000	PyFloat_FromString & PyNumber_Long Buffer Over-reads (https://hackerone.com/reports/104032)
PHP (https://hackerone.com/ibb-php)	-	Improved fix for bug #69545 (Integer overflow in ftp_genlist() resulting in heap overflow) (https://hackerone.com/reports/104028) **CVE-2015-4643** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4643)

Team	Bounty	Title
PHP (https://hackerone.com/ibb-php)	$500	Memory Corruption in phar_parse_tarfile when entry filename starts with null (https://hackerone.com/reports/104027) **CVE-2015-4021** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4021)
PHP (https://hackerone.com/ibb-php)	$500	invalid pointer free() in phar_tar_process_metadata() (https://hackerone.com/reports/104026) **CVE-2015-3307** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3307)
Python (https://hackerone.com/ibb-python)	$500	use after free in load_newobj_ex (https://hackerone.com/reports/104025)
Python (https://hackerone.com/ibb-python)	$500	array.fromstring Use After Free (https://hackerone.com/reports/104024)
Python (https://hackerone.com/ibb-python)	$1,000	bytearray.find Buffer Over-read (https://hackerone.com/reports/104023)
Python (https://hackerone.com/ibb-python)	$500	hotshot pack_string Heap Buffer Overflow (https://hackerone.com/reports/104022)
Python (https://hackerone.com/ibb-python)	$500	audioop.adpcm2lin Buffer Over-read (https://hackerone.com/reports/104021)
Python (https://hackerone.com/ibb-python)	$500	audioop.lin2adpcm Buffer Over-read (https://hackerone.com/reports/104020)
PHP (https://hackerone.com/ibb-php)	$500	Files extracted from archive may be placed outside of destination directory (https://hackerone.com/reports/104019) **CVE-2015-6833** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6833)
PHP (https://hackerone.com/ibb-php)	$1,500	Multiple Use After Free Vulnerabilites in unserialize() (https://hackerone.com/reports/104018) **CVE-2015-6831** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6831)
PHP (https://hackerone.com/ibb-php)	$1,000	Arbitrary code execution in str_ireplace function (https://hackerone.com/reports/104017) **CVE-2015-6527** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6527)

Team	Bounty	Title
PHP (https://hackerone.com/ibb-php)	$1,000	Dangling pointer in the unserialization of ArrayObject items (https://hackerone.com/reports/104016) **CVE-2015-6832** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6832)
PHP (https://hackerone.com/ibb-php)	$500	curl_setopt_array() type confusion (https://hackerone.com/reports/104015)
The Internet (https://hackerone.com/internet) ★	$1,000	libcurl duphandle read out of bounds (https://hackerone.com/reports/104014) **CVE-2014-3707** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3707)
PHP (https://hackerone.com/ibb-php)	$500	heap buffer overflow in enchant_broker_request_dict() (https://hackerone.com/reports/104013) **CVE-2014-9705** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9705)
PHP (https://hackerone.com/ibb-php)	$500	Integer overflow in unserialize() (32-bits only) (https://hackerone.com/reports/104012) **CVE-2014-3669** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3669)
PHP (https://hackerone.com/ibb-php)	$500	AddressSanitizer reports a global buffer overflow in mkgmtime() function (https://hackerone.com/reports/104011) **CVE-2014-3668** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3668)
PHP (https://hackerone.com/ibb-php)	$1,500	SOAP serialize_function_call() type confusion / RCE (https://hackerone.com/reports/104010) **CVE-2015-6836** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6836)
PHP (https://hackerone.com/ibb-php)	$500	zend_throw_or_error() format string vulnerability (https://hackerone.com/reports/104009)
PHP (https://hackerone.com/ibb-php)	$1,000	Uninitialized pointer in phar_make_dirstream (https://hackerone.com/reports/104008) **CVE-2015-7804** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7804)
PHP (https://hackerone.com/ibb-php)	$1,000	Buffer over-read in exif_read_data with TIFF IFD tag (https://hackerone.com/reports/104007)

Team	Bounty	Title
PHP (https://hackerone.com/ibb-php)	$500	Null pointer deref (segfault) in spl_autoload via ob_start (https://hackerone.com/reports/104006)
PHP (https://hackerone.com/ibb-php)	$500	null pointer deref (segfault) in zend_eval_const_expr (https://hackerone.com/reports/104005)
PHP (https://hackerone.com/ibb-php)	$500	Mem out-of-bounds write (segfault) in ZEND_ASSIGN_DIV_SPEC_CV_UNUSED_HANDLER (https://hackerone.com/reports/104004)
Python (https://hackerone.com/ibb-python)	$1,000	Python deque.index() uninitialized memory (https://hackerone.com/reports/104003)
Python (https://hackerone.com/ibb-python)	$500	Python scan_eol() Buffer Over-read (https://hackerone.com/reports/104002)
Python (https://hackerone.com/ibb-python)	$500	time_strftime() Buffer Over-read (https://hackerone.com/reports/104001)
Python (https://hackerone.com/ibb-python)	$500	Python xmlparse_setattro() Type Confusion (https://hackerone.com/reports/104000)
PHP (https://hackerone.com/ibb-php)	$500	Use after free vulnerability in unserialize() with GMP (https://hackerone.com/reports/103999)
PHP (https://hackerone.com/ibb-php)	$500	Use After Free Vulnerability in session deserializer (https://hackerone.com/reports/103998) **CVE-2015-6835** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6835)
PHP (https://hackerone.com/ibb-php)	$1,000	Use After Free Vulnerability in unserialize() (https://hackerone.com/reports/103997) **CVE-2015-6834** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6834)
PHP (https://hackerone.com/ibb-php)	$1,000	Use After Free Vulnerability in unserialize() with SplObjectStorage (https://hackerone.com/reports/103996) **CVE-2015-6834** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6834)
PHP (https://hackerone.com/ibb-php)	$1,000	Use After Free Vulnerability in unserialize() with SplDoublyLinkedList (https://hackerone.com/reports/103995) **CVE-2015-6834** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6834)

Team	Bounty	Title
Python (https://hackerone.com/ibb-python)	$500	Python 3.3 - 3.5 product_setstate() Out-of-bounds Read (https://hackerone.com/reports/103994)
Ruby (https://hackerone.com/ibb-ruby)	$1,500	Request Hijacking Vulnerability In RubyGems 2.4.6 And Earlier (https://hackerone.com/reports/103993) **CVE-2015-3900** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3900)
Python (https://hackerone.com/ibb-python)	$500	Integer overflow in _Unpickler_Read (https://hackerone.com/reports/103992)
Apache httpd (https://hackerone.com/ibb-apache)	$500	mod_lua: Crash in websockets PING handling (https://hackerone.com/reports/103991) **CVE-2015-0228** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0228)
PHP (https://hackerone.com/ibb-php)	$500	Null pointer dereference in phar_get_fp_offset() (https://hackerone.com/reports/103990) **CVE-2015-7803** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-7803)
Khan Academy (https://hackerone.com/khanacademy)	-	Escaping the iframe via exceptions (https://hackerone.com/reports/103989)
HackerOne (https://hackerone.com/security)	$2,500	CSRF possible when SOP Bypass/UXSS is available (https://hackerone.com/reports/103787)
Shopify (https://hackerone.com/shopify) ★	$500	Open Redirect at *.myshopify.com/account/login?checkout_url= (https://hackerone.com/reports/103772)
Urban Dictionary (https://hackerone.com/urbandictionary)	-	URGENT - Subdomain Takeover in support.urbandictionary.com pointing to Zendesk (https://hackerone.com/reports/103432)
Shopify (https://hackerone.com/shopify) ★	$500	[CSRF] Install premium themes (https://hackerone.com/reports/103351)
Imgur (https://hackerone.com/imgur)	-	Attack User Privacy Settings - X-Frame-Options missing on m.imgur.com/user/username/settings (https://hackerone.com/reports/103178)
Algolia (https://hackerone.com/algolia)	$100	Stored XSS in name selection (https://hackerone.com/reports/102755)
ok.ru (https://hackerone.com/ok)	$500	Обход защиты от csrf-ок в m.ok.ru (https://hackerone.com/reports/102376)

Team	Bounty	Title
withinsecurity (https://hackerone.com/withinsecurity)	$250	content injection (https://hackerone.com/reports/102327)
ok.ru (https://hackerone.com/ok)	$500	Same-Origin Policy Bypass #2 (https://hackerone.com/reports/102236)
ok.ru (https://hackerone.com/ok)	$500	Same-Origin Policy bypass on main domain - ok.ru (https://hackerone.com/reports/102234)
Zendesk (https://hackerone.com/zendesk)	$500	[CRITICAL] CSRF leading to account take over (https://hackerone.com/reports/102194)
Sucuri (https://hackerone.com/sucuri)	$250	XSS Vuln in Sucuri Security - Auditing, Malware Scanner (https://hackerone.com/reports/102019)
Binary.com (https://hackerone.com/binary)	$75	Cookie bug (https://hackerone.com/reports/101983)
Shopify (https://hackerone.com/shopify) ★	$500	Open redirect using theme install (https://hackerone.com/reports/101962)
Shopify (https://hackerone.com/shopify) ★	$500	XSS in creating tweets (https://hackerone.com/reports/101450)
Automattic (https://hackerone.com/automattic)	$75	Remove anyone's pic gravtar (https://hackerone.com/reports/101145)
Pornhub (https://hackerone.com/pornhub)	$250	Reflected Cross-Site Scripting on French subdomain (https://hackerone.com/reports/101108)
Twitter (https://hackerone.com/twitter)	$140	Subdomain Expired (https://hackerone.com/reports/101104)
Uber (https://hackerone.com/uber) ★	$500	Drivers can change profile picture (https://hackerone.com/reports/101063)
Shopify (https://hackerone.com/shopify) ★	-	Cookie securing your "Opening soon" store is not secured against XSS (https://hackerone.com/reports/100956)
Shopify (https://hackerone.com/shopify) ★	$500	An administrator without any permission is able to get order notifications using his APNS Token. (https://hackerone.com/reports/100938)
Twitter (https://hackerone.com/twitter)	$560	xss in link items (mopub.com) (https://hackerone.com/reports/100931)
Yelp (https://hackerone.com/yelp)	$1,500	Access to internal CMS containing private Data (https://hackerone.com/reports/100926)

Team	Bounty	Title
Imgur (https://hackerone.com/imgur)	$5,500	Imgur dev environments facing the Internet (https://hackerone.com/reports/100916)
Twitter (https://hackerone.com/twitter)	$560	URGENT : NICHE.co Account Take Over Vulnerability (https://hackerone.com/reports/100849)
Coinbase (https://hackerone.com/coinbase)	$5,000	Stored-XSS in https://www.coinbase.com/ (https://hackerone.com/reports/100829)
Twitter (https://hackerone.com/twitter)	$560	Add tweet to collection CSRF (https://hackerone.com/reports/100820)
Shopify (https://hackerone.com/shopify) ★	-	CSV Excel Macro Injection Vulnerability in export list of current users - app.shopify.com (https://hackerone.com/reports/100667)
Slack (https://hackerone.com/slack)	-	Executing scripts on slack-files.com using SVG (https://hackerone.com/reports/100565)
Pornhub (https://hackerone.com/pornhub)	$250	Cross Site Scripting - On Mouse Over, Blog page (https://hackerone.com/reports/100552)
Pornhub (https://hackerone.com/pornhub)	$250	[xss, pornhub.com] /user/[username], multiple parameters (https://hackerone.com/reports/100550)
HackerOne (https://hackerone.com/security)	$1,000	Pre-generation of 2FA secret/backup codes seems like an unnecessary risk (https://hackerone.com/reports/100509)
Mail.Ru (https://hackerone.com/mailru)	-	[tz.mail.ru] XSS в функционале авторизации (https://hackerone.com/reports/100500)
Coinbase (https://hackerone.com/coinbase)	$500	Transactions visible on Unconfirmed devices (https://hackerone.com/reports/100186)
Algolia (https://hackerone.com/algolia)	$200	User with limited access to Index configuration can rename the Index (https://hackerone.com/reports/99969)
drchrono (https://hackerone.com/drchrono)	$100	Request Accepts without X-CSRFToken [Header - Cookie] (https://hackerone.com/reports/99857)
HackerOne (https://hackerone.com/security)	$500	Limited CSRF bypass. (https://hackerone.com/reports/99708)
HackerOne (https://hackerone.com/security)	-	profile cover can also load external URL's (https://hackerone.com/reports/99687)
drchrono (https://hackerone.com/drchrono)	$100	CSRF Add Album On onpatient.com (https://hackerone.com/reports/99647)

Team	Bounty	Title
Uber (https://hackerone.com/uber) ★	$1,000	Mass Assignment Vulnerability in partners.uber.com (https://hackerone.com/reports/99424)
Shopify (https://hackerone.com/shopify) ★	$500	deleted staff member can add his amazon marketplace web services account to the store. (https://hackerone.com/reports/99374)
Algolia (https://hackerone.com/algolia)	$100	an xss issue (https://hackerone.com/reports/99368)
Shopify (https://hackerone.com/shopify) ★	$500	[CSRF] Activate PayPal Express Checkout (https://hackerone.com/reports/99321)
QIWI (https://hackerone.com/qiwi)	$3,137	XML External Entity (XXE) in qiwi.com + waf bypass (https://hackerone.com/reports/99279)
Mapbox (https://hackerone.com/mapbox)	$1,000	XSS in L.mapbox.shareControl in mapbox.js (https://hackerone.com/reports/99245)
Shopify (https://hackerone.com/shopify) ★	$1,000	S3 Buckets open to the world thanks to 'Authenticated Users' ACL (https://hackerone.com/reports/98819)
ownCloud (https://hackerone.com/owncloud)	-	RCE in ci.owncloud.com / ci.owncloud.org (https://hackerone.com/reports/98559)
Shopify (https://hackerone.com/shopify) ★	$500	Apps can access 'channels' beta api (https://hackerone.com/reports/98499)
Binary.com (https://hackerone.com/binary)	$50	Email Verification Link can be Used as Password Reset Link! (https://hackerone.com/reports/98469)
Twitter (https://hackerone.com/twitter)	$280	Urgent : Disclosure of all the apps with hash ID in mopub through API request (Authentication bypass) (https://hackerone.com/reports/98432)
QIWI (https://hackerone.com/qiwi)	$200	XSS Reflected in test.qiwi.ru (https://hackerone.com/reports/98281)
Shopify (https://hackerone.com/shopify) ★	$1,500	'Limited' RCE in certain places where Liquid is accepted (https://hackerone.com/reports/98259)
Binary.com (https://hackerone.com/binary)	$300	login to any user's cashier account and full account information disclosure (https://hackerone.com/reports/98247)
Shopify (https://hackerone.com/shopify) ★	-	Non-owner user can remove online store channel and re-add it. (https://hackerone.com/reports/98151)
itBit Exchange (https://hackerone.com/itbit)	$100	No password length restriction denial of service (https://hackerone.com/reports/98083)

Team	Bounty	Title
Algolia (https://hackerone.com/algolia)	$100	Stored XSS on https://www.algolia.com/realtime-search-demo/* (https://hackerone.com/reports/98012)
HackerOne (https://hackerone.com/security)	$2,500	Cross-domain AJAX request (https://hackerone.com/reports/97948)
Imgur (https://hackerone.com/imgur)	$150	XSS m.imgur.com (https://hackerone.com/reports/97938)
Slack (https://hackerone.com/slack)	$100	Reflected Self-XSS in Slack (https://hackerone.com/reports/97683)
Twitter (https://hackerone.com/twitter)	$1,120	File Upload XSS in image uploading of App in mopub (https://hackerone.com/reports/97672)
Slack (https://hackerone.com/slack)	$200	File upload XSS (Java applet) on http://slackatwork.com/ (https://hackerone.com/reports/97657)
Binary.com (https://hackerone.com/binary)	-	User Enumeration : Due to rate limiting on registration (https://hackerone.com/reports/97609)
Shopify (https://hackerone.com/shopify) ★	$500	List of devices is accessible regardless of the account limitations (https://hackerone.com/reports/97535)
Twitter (https://hackerone.com/twitter)	$280	Following a User After Favoriting Actually Follows Another User (related to #95243) (https://hackerone.com/reports/97510)
Shopify (https://hackerone.com/shopify) ★	$500	SVG parser loads external resources on image upload (https://hackerone.com/reports/97501)
Shopify (https://hackerone.com/shopify) ★	$500	Staff members with no permission can access to the files, uploaded by the administrator (https://hackerone.com/reports/97452)
HackerOne (https://hackerone.com/security)	-	Hackerone impersonation (https://hackerone.com/reports/97377)
ok.ru (https://hackerone.com/ok)	$250	Multiple critical vulnerabilities in Odnoklassniki Android application (https://hackerone.com/reports/97295)
HackerOne (https://hackerone.com/security)	$1,000	HTTP header injection in info.hackerone.com allows setting cookies for hackerone.com (https://hackerone.com/reports/97292)
HackerOne (https://hackerone.com/security)	$2,500	Send AJAX request to external domain (https://hackerone.com/reports/97191)
Twitter (https://hackerone.com/twitter)	$1,120	Can see private tweets via keyword searches on tweetdeck (https://hackerone.com/reports/97161)

Team	Bounty	Title
Shopify (https://hackerone.com/shopify) ★	$500	An administrator without the 'Settings' permission is able to see payment gateways (https://hackerone.com/reports/96908)
Shopify (https://hackerone.com/shopify) ★	$500	A 'Full access' administrator is able to see the shop owners user details (https://hackerone.com/reports/96890)
Shopify (https://hackerone.com/shopify) ★	$500	Staff members with no permission to access domains can access them. (https://hackerone.com/reports/96855)
Keybase (https://hackerone.com/keybase)	$50	Un-handled exception leads to Information Disclosure (https://hackerone.com/reports/96847)
itBit Exchange (https://hackerone.com/itbit)	-	email not required to be unique (https://hackerone.com/reports/96826)
Snapchat (https://hackerone.com/snapchat)	$1,500	Password Reset - query param overrides postdata (https://hackerone.com/reports/96636)
Shopify (https://hackerone.com/shopify) ★	$500	Missing of csrf protection (https://hackerone.com/reports/96470)
Imgur (https://hackerone.com/imgur)	$50	Persistent XSS in https://p.imgur.com/albumview.gif and http://p.imgur.com/imageview.gif / post statistics (https://hackerone.com/reports/96467)
Slack (https://hackerone.com/slack)	$500	Stored XSS in Slack (weird, trial and error) (https://hackerone.com/reports/96337)
withinsecurity (https://hackerone.com/withinsecurity)	-	DDOS using xmlrpc.php (https://hackerone.com/reports/96294)
withinsecurity (https://hackerone.com/withinsecurity)	-	Uses unsafe-inline without nonce (https://hackerone.com/reports/96218)
Shopify (https://hackerone.com/shopify) ★	-	Domain takoever - https://sellocdn.com (https://hackerone.com/reports/96007)
Binary.com (https://hackerone.com/binary)	$75	Http Response Splitting - Validate link (https://hackerone.com/reports/95981)
itBit Exchange (https://hackerone.com/itbit)	$50	user-agent Content spoofing (https://hackerone.com/reports/95932)
Mail.Ru (https://hackerone.com/mailru)	$300	[api.allodsteam.com] Authentication Data (https://hackerone.com/reports/95804)

Team	Bounty	Title
Udemy (https://hackerone.com/udemy)	-	Reflected XSS and/or malicious redirection via JWPlayer 6 configuration modification (https://hackerone.com/reports/95640)
Binary.com (https://hackerone.com/binary)	$50	Cross Site Scripting (https://hackerone.com/reports/95599)
Shopify (https://hackerone.com/shopify) ★	$500	Privilege escalation and circumvention of permission to limited access user (https://hackerone.com/reports/95589)
Imgur (https://hackerone.com/imgur)	$250	Persistent XSS in image title (https://hackerone.com/reports/95564)
Twitter (https://hackerone.com/twitter)	$5,040	IDOR- Activate Mopub on different organizations- steal api token-Fabric.io (https://hackerone.com/reports/95552)
Shopify (https://hackerone.com/shopify) ★	$500	Unauthorized access to any Store Admin's First & Last name (https://hackerone.com/reports/95441)
Twitter (https://hackerone.com/twitter)	$280	Following a User Actually Follows Another User (https://hackerone.com/reports/95243)
Twitter (https://hackerone.com/twitter)	$280	XSS in the "Poll" Feature on Twitter.com (https://hackerone.com/reports/95231)
InVision (https://hackerone.com/invision)	-	X-Frame-Options Header Not Set (https://hackerone.com/reports/95125)
Shopify (https://hackerone.com/shopify) ★	$500	Reflected XSS in cart at hardware.shopify.com (https://hackerone.com/reports/95089)
Coinbase (https://hackerone.com/coinbase)	-	Balance Manipulation - BUG (https://hackerone.com/reports/94925)
Shopify (https://hackerone.com/shopify) ★	$4,000	Paid account can review\download any invoice of any other shop (https://hackerone.com/reports/94899)
Whisper (https://hackerone.com/whisper)	$30	Host Header Injection/Redirection (https://hackerone.com/reports/94637)
Ruby on Rails (https://hackerone.com/rails)	-	http_basic_authenticate_with is suseptible to timing attacks. (https://hackerone.com/reports/94568)
Mail.Ru (https://hackerone.com/mailru)	-	Reflective Xss on news.mail.ru and admin.news.mail.ru (https://hackerone.com/reports/94517)
Shopify (https://hackerone.com/shopify) ★	$500	Some S3 Buckets are world readable (and one is world writeable) (https://hackerone.com/reports/94502)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	-	Minimum bounty of a private program is visible for users that were removed from the program (https://hackerone.com/reports/94336)
Zopim (https://hackerone.com/zopim)	$1,000	Cross-site Scripting in all Zopim (https://hackerone.com/reports/94230)
Shopify (https://hackerone.com/shopify) ★	$1,500	Arbitrary read on s3://shopify-delivery-app-storage/files (https://hackerone.com/reports/94087)
Shopify (https://hackerone.com/shopify) ★	$2,500	Unauthorized access to all collections, products, pages from other stores (https://hackerone.com/reports/93921)
Shopify (https://hackerone.com/shopify) ★	$500	Bypassing password requirement during deletion of accout (https://hackerone.com/reports/93901)
FanFootage (https://hackerone.com/fanfootage)	-	XSS by image file name (https://hackerone.com/reports/93807)
Shopify (https://hackerone.com/shopify) ★	$2,000	Arbitrary write on s3://shopify-delivery-app-storage/files (https://hackerone.com/reports/93691)
Shopify (https://hackerone.com/shopify) ★	$500	Missing authorization check on dashboard overviews (https://hackerone.com/reports/93680)
Shopify (https://hackerone.com/shopify) ★	$500	get users information without full access (https://hackerone.com/reports/93616)
Adobe (https://hackerone.com/adobe)	-	Reflected XSS via. search (https://hackerone.com/reports/93550)
Shopify (https://hackerone.com/shopify) ★	$1,000	Unauthenticated access to details of hidden products in any shop via title emuneration (https://hackerone.com/reports/93394)
Shopify (https://hackerone.com/shopify) ★	$500	First & Last Name Disclosure of any Shopify Store Admin (https://hackerone.com/reports/93294)
Imgur (https://hackerone.com/imgur)	-	Csrf near report abuse meme (https://hackerone.com/reports/93154)
WePay (https://hackerone.com/wepay)	$100	Subdomain Takeover in http://staging.wepay.com/ pointing to Fastly (https://hackerone.com/reports/93106)
VK.com (https://hackerone.com/vkcom)	$100	Способ узнать имя человека и ВУЗ удаленной страницы (https://hackerone.com/reports/93020)
Shopify (https://hackerone.com/shopify) ★	$2,000	unauthorized access to all collections name (https://hackerone.com/reports/93004)
Keybase (https://hackerone.com/keybase)	-	xss (https://hackerone.com/reports/92915)

Team	Bounty	Title
Coinbase (https://hackerone.com/coinbase)	$100	SPF records not found (https://hackerone.com/reports/92740)
HackerOne (https://hackerone.com/security)	-	HackerOne Private Programs users disclosure and de-anonymous-ize (https://hackerone.com/reports/92716)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Referer protection Bypassed (https://hackerone.com/reports/92644)
Shopify (https://hackerone.com/shopify) ★	-	The POS Firmware is leaking the root Password which can be used for unauthorized access to the device. (https://hackerone.com/reports/92633)
HackerOne (https://hackerone.com/security)	-	Content spoofing on invitations page (https://hackerone.com/reports/92607)
Shopify (https://hackerone.com/shopify) ★	$500	Accessing Payments page and adding payment methods with limited access accounts (https://hackerone.com/reports/92481)
Badoo (https://hackerone.com/badoo)	$456	Tokens from services like Facebook can be stolen (https://hackerone.com/reports/92472)
Shopify (https://hackerone.com/shopify) ★	$2,500	unauthorized access to all customers first and last name (https://hackerone.com/reports/92453)
Automattic (https://hackerone.com/automattic)	$75	CSV Injection in polldaddy.com (https://hackerone.com/reports/92353)
Trello (https://hackerone.com/trello)	$128	CSV Injection (https://hackerone.com/reports/92350)
Shopify (https://hackerone.com/shopify) ★	$500	customers password hash leak!!!! (https://hackerone.com/reports/92344)
Uber (https://hackerone.com/uber) ★	$100	Issue with Password reset functionality (https://hackerone.com/reports/92251)
ownCloud (https://hackerone.com/owncloud)	-	Self-XSS in mails sent by hello@owncloud.com (https://hackerone.com/reports/92111)
Trello (https://hackerone.com/trello)	$256	Normal User can add new users to group (https://hackerone.com/reports/92050)
Imgur (https://hackerone.com/imgur)	$1,600	Server Side Request Forgery In Video to GIF Functionality (https://hackerone.com/reports/91816)

Team	Bounty	Title
Imgur (https://hackerone.com/imgur)	$50	Crossdomain.xml settings on api.imgur.com too open (https://hackerone.com/reports/91604)
Automattic (https://hackerone.com/automattic)	$50	WooCommerce: Support Ticket indirect object reference (https://hackerone.com/reports/91599)
Imgur (https://hackerone.com/imgur)	$50	Reflected Flash XSS using swfupload.swf with an epileptic reloading to bypass the button-event (https://hackerone.com/reports/91421)
Imgur (https://hackerone.com/imgur)	-	Content Sniffing not enabled (https://hackerone.com/reports/91366)
Imgur (https://hackerone.com/imgur)	$50	"Sign me out everywhere" does not work for desktop sessions (https://hackerone.com/reports/91350)
Imgur (https://hackerone.com/imgur)	-	Open Url redirection on login with facebook (https://hackerone.com/reports/91332)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: WP Super Cache plugin is outdated (https://hackerone.com/reports/90980)
IRCCloud (https://hackerone.com/irccloud)	$500	Inadequate input validation on API endpoint leading to self denial of service and increased system load. (https://hackerone.com/reports/90912)
Shopify (https://hackerone.com/shopify) ★	-	Passwords Returned in Later Responses. (https://hackerone.com/reports/90862)
Gratipay (https://hackerone.com/gratipay)	-	implement a cross-domain policy for Adobe products (https://hackerone.com/reports/90778)
Zendesk (https://hackerone.com/zendesk)	$50	Content Spoofing (https://hackerone.com/reports/90753)
Mail.Ru (https://hackerone.com/mailru)	-	[ling.go.mail.ru] Server-Status opened for all users (https://hackerone.com/reports/90691)
Shopify (https://hackerone.com/shopify) ★	$1,000	change Login Services settings without owner access (https://hackerone.com/reports/90690)
Shopify (https://hackerone.com/shopify) ★	$1,000	create staff member without owner access (https://hackerone.com/reports/90688)
Shopify (https://hackerone.com/shopify) ★	$500	Privilege escalation vulnerability (https://hackerone.com/reports/90671)
ownCloud (https://hackerone.com/owncloud)	-	No email verification during registration (https://hackerone.com/reports/90643)

Team	Bounty	Title
ownCloud (https://hackerone.com/owncloud)	-	[s3.owncloud.com] Web Server HTTP Trace/Track Method Support (https://hackerone.com/reports/90601)
Ruby on Rails (https://hackerone.com/rails)	-	Nested attributes reject_if proc can be circumvented by providing "_destroy" parameter (https://hackerone.com/reports/90457)
Zaption (https://hackerone.com/zaption)	-	CSV Excel Macro Injection in Export Response (https://hackerone.com/reports/90415)
HackerOne (https://hackerone.com/security)	-	Minor Bug: Public un-compiled CSS with original sass, versioning, source map, comments, etc. (https://hackerone.com/reports/90367)
ownCloud (https://hackerone.com/owncloud)	-	Apache documentation (https://hackerone.com/reports/90321)
Coinbase (https://hackerone.com/coinbase)	$100	User email enumuration using Gmail (https://hackerone.com/reports/90308)
Zopim (https://hackerone.com/zopim)	$100	CSV Excel Macro Injection Vulnerability in export chat logs (https://hackerone.com/reports/90274)
Twitter (https://hackerone.com/twitter)	$280	Tweetdeck (twitter owned app) not revoked (https://hackerone.com/reports/90172)
Zendesk (https://hackerone.com/zendesk)	$100	CSV Excel Macro Injection Vulnerability in export customer tickets (https://hackerone.com/reports/90131)
Zendesk (https://hackerone.com/zendesk)	$100	Cross-site Scripting https://www.zendesk.com/product/pricing/ (https://hackerone.com/reports/89624)
Slack (https://hackerone.com/slack)	$100	Self-XSS in posts by formatting text as code (https://hackerone.com/reports/89505)
BitHunt (https://hackerone.com/bithunt)	-	No rate limit or captcha to identify humans (https://hackerone.com/reports/89178)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: CVE-2015-5477 BIND9 TKEY Vulnerability + Exploit (Denial of Service) (https://hackerone.com/reports/89097)
Mail.Ru (https://hackerone.com/mailru)	-	Vulnerability :- "XSS vulnerability" (https://hackerone.com/reports/89081)
ownCloud (https://hackerone.com/owncloud)	-	Apache Range Header Denial of Service Attack (Confirmed PoC) (https://hackerone.com/reports/88904)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	$500	XSS: https://light.mail.ru/compose, https://m.mail.ru/compose/[id]/reply при ответе на специальным образом сформированное письмо (https://hackerone.com/reports/88881)
Phabricator (https://hackerone.com/phabricator)	$300	Information leakage through Graphviz blocks (https://hackerone.com/reports/88395)
ownCloud (https://hackerone.com/owncloud)	-	Webview Vulnerablity [OwnCloudAndroid Application] (https://hackerone.com/reports/87835)
Mail.Ru (https://hackerone.com/mailru)	-	[support.my.com] Internet Explorer XSS (https://hackerone.com/reports/87806)
Mail.Ru (https://hackerone.com/mailru)	-	[rabota.mail.ru] Open Redirect (https://hackerone.com/reports/87804)
ownCloud (https://hackerone.com/owncloud)	-	gallery_plus: Content Spoofing (https://hackerone.com/reports/87752)
Udemy (https://hackerone.com/udemy)	$100	XSS Vulnerability (https://hackerone.com/reports/87588)
Vimeo (https://hackerone.com/vimeo)	$200	Stored XSS on vimeo.com and player.vimeo.com (https://hackerone.com/reports/87577)
Coinbase (https://hackerone.com/coinbase)	$100	OAUTH pemission set as true= lead to authorize malicious application (https://hackerone.com/reports/87561)
Gratipay (https://hackerone.com/gratipay)	-	Mail spaming (https://hackerone.com/reports/87531)
ownCloud (https://hackerone.com/owncloud)	$25	Full Path Disclosure (https://hackerone.com/reports/87505) **CVE-2016-1501** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1501)
Shopify (https://hackerone.com/shopify) ★	$500	www.shopify.com XSS on blog pages via sharing buttons (https://hackerone.com/reports/87168)
Twitter (https://hackerone.com/twitter)	$2,520	XSS on OAuth authorize/authenticate endpoint (https://hackerone.com/reports/87040)
Keybase (https://hackerone.com/keybase)	$500	[keybase.io] Open Redirect (https://hackerone.com/reports/87027)
Anghami (https://hackerone.com/anghami)	$100	[CRITICAL] Login To Any Account Linked With Google+ With Email Only (https://hackerone.com/reports/86504)
Anghami (https://hackerone.com/anghami)	$300	[https://www.anghami.com/updatemailinfo/] Sql Injection (https://hackerone.com/reports/86468)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	-	Weak HSTS age in support hackerone site (https://hackerone.com/reports/86067)
Phabricator (https://hackerone.com/phabricator)	$450	Multiple so called 'type juggling' attacks. Most notably PhabricatorUser::validateCSRFToken() is 'bypassable' in certain cases. (https://hackerone.com/reports/86022)
Romit (https://hackerone.com/romit)	$250	IDOR on remoing Share (https://hackerone.com/reports/85720)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Potential XSS (https://hackerone.com/reports/85577)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: CSRF change privacy settings (https://hackerone.com/reports/85565)
ownCloud (https://hackerone.com/owncloud)	-	Password appears in user name field (https://hackerone.com/reports/85559)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Mixed Active Scripting Issue (https://hackerone.com/reports/85541)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Edit Question didn't check ACLs (https://hackerone.com/reports/85532)
Mail.Ru (https://hackerone.com/mailru)	$150	XSS at af.attachmail.ru (https://hackerone.com/reports/85421)
InVision (https://hackerone.com/invision)	$400	Deleting a Project for which the user is not owner but a normal member (https://hackerone.com/reports/85401)
Shopify (https://hackerone.com/shopify) ★	$500	XSS https://www.shopify.com/signup (https://hackerone.com/reports/85291)
ownCloud (https://hackerone.com/owncloud)	$25	Full Path Disclosure (https://hackerone.com/reports/85201) **CVE-2016-1501** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-1501)
Phabricator (https://hackerone.com/phabricator)	-	Dashboard panel embedded onto itself causes a denial of service (https://hackerone.com/reports/85011)
ownCloud (https://hackerone.com/owncloud)	-	Config (https://hackerone.com/reports/84797)
Gratipay (https://hackerone.com/gratipay)	-	Stored XSS On Statement (https://hackerone.com/reports/84740)
Zopim (https://hackerone.com/zopim)	$100	[API ISSUE] agents can Create agents even after they are disabled ! (https://hackerone.com/reports/84709)

Team	Bounty	Title
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Outdated plugins contains public exploits (https://hackerone.com/reports/84581)
ownCloud (https://hackerone.com/owncloud)	-	Lack of HSTS on https://apps.owncloud.com (https://hackerone.com/reports/84453)
ownCloud (https://hackerone.com/owncloud)	-	CSRF in apps.owncloud.com (https://hackerone.com/reports/84395)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Malicious file upload leads to remote code execution (https://hackerone.com/reports/84374)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Account Compromise Through CSRF (https://hackerone.com/reports/84372)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Stored XSS in profile page (https://hackerone.com/reports/84371)
Gratipay (https://hackerone.com/gratipay)	-	DKIM records not present, Email Hijacking is possible (https://hackerone.com/reports/84287)
ownCloud (https://hackerone.com/owncloud)	-	demo.owncloud.org: HTTP compression is enabled potentially leading to BREACH attack (https://hackerone.com/reports/84105)
ownCloud (https://hackerone.com/owncloud)	-	daily.owncloud.com: Information disclosure (https://hackerone.com/reports/84085)
ownCloud (https://hackerone.com/owncloud)	-	*.owncloud.com / *.owncloud.org: Using not strong enough SSL ciphers (https://hackerone.com/reports/84078)
ownCloud (https://hackerone.com/owncloud)	-	test1.owncloud.com: Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability (https://hackerone.com/reports/83971)
Ruby on Rails (https://hackerone.com/rails)	-	DoS Attack in Controller Lookup Code (https://hackerone.com/reports/83962)
ownCloud (https://hackerone.com/owncloud)	-	s2.owncloud.com: SSL Session cookie without secure flag set (https://hackerone.com/reports/83856)
ownCloud (https://hackerone.com/owncloud)	-	s2.owncloud.com: Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability (https://hackerone.com/reports/83855)
ownCloud (https://hackerone.com/owncloud)	-	demo.owncloud.org: Web Server HTTP Trace/Track Method Support Cross-Site Tracing Vulnerability (https://hackerone.com/reports/83837)

Team	Bounty	Title
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: SSL Server Allows Anonymous Authentication Vulnerability (SMTP) (https://hackerone.com/reports/83803)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Path Disclosure (https://hackerone.com/reports/83801)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: SSL Session cookie without secure flag set (https://hackerone.com/reports/83710)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Session Cookie in URL can be captured by hackers (https://hackerone.com/reports/83667)
Khan Academy (https://hackerone.com/khanacademy)	-	Html injection on khanacademy (https://hackerone.com/reports/83604)
Mail.Ru (https://hackerone.com/mailru)	-	[riot.mail.ru] Reflected XSS in debug-mode (https://hackerone.com/reports/83585)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: PermError SPF Permanent Error: Too many DNS lookups (https://hackerone.com/reports/83578)
Mail.Ru (https://hackerone.com/mailru)	-	[start.icq.com] Reflected XSS via Cookies (https://hackerone.com/reports/83576)
Pornhub (https://hackerone.com/pornhub)	$100	[reflected xss, pornhub.com] /blog, any (https://hackerone.com/reports/83566)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: Multiple reflected XSS by insecure URL generation (IE only) (https://hackerone.com/reports/83381)
ownCloud (https://hackerone.com/owncloud)	-	apps.owncloud.com: XSS via referrer (https://hackerone.com/reports/83374)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Cross Site Tracing (https://hackerone.com/reports/83373)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Content Sniffing not disabled (https://hackerone.com/reports/83251)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: Allowed an attacker to force a user to change profile details. (XCSRF) (https://hackerone.com/reports/83239)
ownCloud (https://hackerone.com/owncloud)	-	owncloud.com: DOM Based XSS (https://hackerone.com/reports/83178)

Team	Bounty	Title
Pornhub (https://hackerone.com/pornhub)	$50	Cross Site Scripting – Album Page (https://hackerone.com/reports/82929)
Zendesk (https://hackerone.com/zendesk)	$500	Stored XSS in comments (https://hackerone.com/reports/82725)
Hired (https://hackerone.com/hired)	$420	Stored XSS in Company Name (https://hackerone.com/reports/82608)
Shopify (https://hackerone.com/shopify) ★	$500	Self XSS in chat. (https://hackerone.com/reports/81757)
Automattic (https://hackerone.com/automattic)	$100	XSS in WordPress (https://hackerone.com/reports/81736)
Gratipay (https://hackerone.com/gratipay)	$1	Possible SQL injection on "Jump to twitter" (https://hackerone.com/reports/81701)
Shopify (https://hackerone.com/shopify) ★	$500	XSS https://delivery.shopifyapps.com/ (Digital Downloads App in myshopify.com) (https://hackerone.com/reports/81441)
Ruby on Rails (https://hackerone.com/rails)	-	[Rails42] We can inject HTML tags when server is using strip_tags method (https://hackerone.com/reports/81396)
Ruby on Rails (https://hackerone.com/rails)	$2,000	Potential XSS on sanitize/Rails::Html::WhiteListSanitizer (https://hackerone.com/reports/81212)
InVision (https://hackerone.com/invision)	$100	Reflective XSS in projects.invisionapp.com (https://hackerone.com/reports/81201)
Informatica (https://hackerone.com/informatica)	-	[now.informatica.com] Reflective Xss (https://hackerone.com/reports/81191)
HackerOne (https://hackerone.com/security)	$500	Internal bounty and swag details disclosed as part of JSON response (https://hackerone.com/reports/81083)
HackerOne (https://hackerone.com/security)	$500	Private Program and bounty details disclosed as part of JSON search response (https://hackerone.com/reports/80936)
Gratipay (https://hackerone.com/gratipay)	-	Authentication errors in server side validaton of E-MAIL (https://hackerone.com/reports/80883)
Urban Dictionary (https://hackerone.com/urbandictionary)	-	Reflective Xss Vulnerability (https://hackerone.com/reports/80694)
HackerOne (https://hackerone.com/security)	$500	Number of invited researchers disclosed as part of JSON search response (https://hackerone.com/reports/80597)

Team	Bounty	Title
VK.com (https://hackerone.com/vkcom)	$500	Внедрение произвольного javascript-сценария в функционале просмотра изображений мобильной версии сайта (https://hackerone.com/reports/80298)
Gratipay (https://hackerone.com/gratipay)	-	[gratipay.com] CRLF Injection (https://hackerone.com/reports/79552)
QIWI (https://hackerone.com/qiwi)	$500	Открытый доступ к корпоративным данным. (https://hackerone.com/reports/79393)
Slack (https://hackerone.com/slack)	$1,000	OSX slack:// protocol handler javascript injection (https://hackerone.com/reports/79348)
Flox (https://hackerone.com/flox)	$25	Content spoofing through Referel header (https://hackerone.com/reports/79185)
ok.ru (https://hackerone.com/ok)	$300	Доступ к чужим групповым беседам. (https://hackerone.com/reports/79046)
ok.ru (https://hackerone.com/ok)	$150	Critical : Access to group videos where videos are restricted for all users(Broken authentication) (https://hackerone.com/reports/78781)
Udemy (https://hackerone.com/udemy)	$50	information disclosure (https://hackerone.com/reports/78765)
Flox (https://hackerone.com/flox)	-	Email spoofing configuration missing (https://hackerone.com/reports/78685)
ok.ru (https://hackerone.com/ok)	$200	Доступ к чужим приватным фотографиям (3) через обложку видео (https://hackerone.com/reports/78516)
Mail.Ru (https://hackerone.com/mailru)	$150	Time-Based Blind SQL Injection Attacks (https://hackerone.com/reports/78443)
ok.ru (https://hackerone.com/ok)	$500	(URGENT!) Покупка ОК дешевле, чем он стоит (https://hackerone.com/reports/78436)
Mail.Ru (https://hackerone.com/mailru)	$150	Cross site scripting (https://hackerone.com/reports/78412)
ok.ru (https://hackerone.com/ok)	$150	Покупка песни дешевле, чем она стоит. (https://hackerone.com/reports/78219)
ok.ru (https://hackerone.com/ok)	$150	xss in group (https://hackerone.com/reports/78052)
Keybase (https://hackerone.com/keybase)	-	Sensitive server-side/application information disclosure (https://hackerone.com/reports/78012)

Team	Bounty	Title
ok.ru (https://hackerone.com/ok)	-	Cross site scripting On api Calculator API requests (https://hackerone.com/reports/78003)
ok.ru (https://hackerone.com/ok)	$500	SSRF/XSPA в форме загрузки видео по URL (https://hackerone.com/reports/77817)
Shopify (https://hackerone.com/shopify) ★	$1,000	TCP Source Port Pass Firewall (https://hackerone.com/reports/77802)
ok.ru (https://hackerone.com/ok)	$100	http://217.20.144.201 privilege escalation in apache tomcat SessionEample-script (https://hackerone.com/reports/77679)
MapLogin (https://hackerone.com/maplogin)	-	Account creation code bypass (https://hackerone.com/reports/77330)
Keybase (https://hackerone.com/keybase)	$100	Full path disclosure at https://keybase.io/_/api/1.0/invitation_request.json (https://hackerone.com/reports/77319)
WordPoints (https://hackerone.com/wordpoints)	$25	Weak Cryptographic Hash (https://hackerone.com/reports/77231)
Mavenlink (https://hackerone.com/mavenlink)	$25	Open/Unvalidated Redirect Issue (https://hackerone.com/reports/77221)
Keybase (https://hackerone.com/keybase)	$250	Content Sniffing not disabled (https://hackerone.com/reports/77081)
Romit (https://hackerone.com/romit)	$250	GA code not verified on the server side allows sending Verification Documents on behalf of another user (https://hackerone.com/reports/77076)
Keybase (https://hackerone.com/keybase)	$250	No rate limiting for sensitive actions (like "forgot password") enables user enumeration (https://hackerone.com/reports/77067)
Keybase (https://hackerone.com/keybase)	$500	Stealing CSRF Tokens (https://hackerone.com/reports/77065)
Keybase (https://hackerone.com/keybase)	$500	SMTP protection not used (https://hackerone.com/reports/77060)
Keybase (https://hackerone.com/keybase)	-	NO SPF RECORDS (https://hackerone.com/reports/77058)
Zaption (https://hackerone.com/zaption)	-	Cheating at gallery rating (https://hackerone.com/reports/76784)
Zaption (https://hackerone.com/zaption)	$25	Open redirect filter bypass (https://hackerone.com/reports/76738)
Zaption (https://hackerone.com/zaption)	$25	Using GET method for account login with CSRF token leaking to external sites Via Referer. (https://hackerone.com/reports/76733)

Team	Bounty	Title
Zaption (https://hackerone.com/zaption)	$50	XSS - Gallery Search Listing (https://hackerone.com/reports/76713)
Gratipay (https://hackerone.com/gratipay)	-	Self XSS Protection not used , I can trick users to insert JavaScript (https://hackerone.com/reports/76307)
Gratipay (https://hackerone.com/gratipay)	-	weak ssl cipher suites (https://hackerone.com/reports/76303)
Zopim (https://hackerone.com/zopim)	-	Security Missconfiguration in Autologin (https://hackerone.com/reports/75936)
Zendesk (https://hackerone.com/zendesk)	$200	Stored Cross site scripting In developer.zendesk.com (https://hackerone.com/reports/75727)
Romit (https://hackerone.com/romit)	$250	No rate limit which leads to "Users information Disclosure" including verfification documents etc. (https://hackerone.com/reports/75702)
Envoy (https://hackerone.com/envoy)	-	Stored XSS (https://hackerone.com/reports/75684)
Envoy (https://hackerone.com/envoy)	-	XSS in "Guest Pre-Registration" page after registration (https://hackerone.com/reports/75676)
HackerOne (https://hackerone.com/security)	$500	Accessing title of the report of which you are marked as duplicate (https://hackerone.com/reports/75556)
QIWI (https://hackerone.com/qiwi)	$100	Session Cookie without HttpOnly and secure flag set (https://hackerone.com/reports/75357)
Envoy (https://hackerone.com/envoy)	-	Stored XSS in /settings/ipad Page (https://hackerone.com/reports/75096)
Mapbox (https://hackerone.com/mapbox)	$500	Disclosure of map information (https://hackerone.com/reports/74933)
DigitalSellz (https://hackerone.com/digitalsellz)	-	The product/status method CSRF (https://hackerone.com/reports/74595)
DigitalSellz (https://hackerone.com/digitalsellz)	-	The email updates issues (https://hackerone.com/reports/74518)
DigitalSellz (https://hackerone.com/digitalsellz)	-	Own downloading link isn't properly checked in the email template (https://hackerone.com/reports/74514)
Romit (https://hackerone.com/romit)	$250	Potential for financial loss, negative Values for "Buy fee" and "Sell Fee" (https://hackerone.com/reports/74147)
Ubiquiti Networks (https://hackerone.com/ubnt)	$500	Yet another Buffer Overflow in PHP of the AirMax Products (https://hackerone.com/reports/74025)

Team	Bounty	Title
Ubiquiti Networks (https://hackerone.com/ubnt)	$500	Other Buffer Overflow in PHP of the AirMax Products (https://hackerone.com/reports/74004)
Udemy (https://hackerone.com/udemy)	$150	Extremely high Course rating values could be set in order to make really high Average rating of the course. Negative values could be set to. (https://hackerone.com/reports/73808)
Shopify (https://hackerone.com/shopify) ★	$3,000	Attention! Remote Code Execution at http://wpt.ec2.shopify.com/ (https://hackerone.com/reports/73567)
Shopify (https://hackerone.com/shopify) ★	$500	Reflected XSS in chat (https://hackerone.com/reports/73566)
Ubiquiti Networks (https://hackerone.com/ubnt)	$250	Buffer Overflow in PHP of the AirMax Products (https://hackerone.com/reports/73491)
Ubiquiti Networks (https://hackerone.com/ubnt)	$18,000	Arbritrary file Upload on AirMax (https://hackerone.com/reports/73480)
Python (https://hackerone.com/python)	$1,000	Integer overflow in _json_encode_unicode leads to crash (https://hackerone.com/reports/73260)
Python (https://hackerone.com/python)	$500	Integer overflow in _pickle.c (https://hackerone.com/reports/73259)
Python (https://hackerone.com/python)	$1,000	Python: imageop Unsafe Arithmetic (https://hackerone.com/reports/73258)
PHP (https://hackerone.com/php)	$500	PHP yaml_parse/yaml_parse_file/yaml_parse_url Unsafe Deserialization (https://hackerone.com/reports/73257)
PHP (https://hackerone.com/php)	$1,500	PHP yaml_parse/yaml_parse_file/yaml_parse_url Double Free (https://hackerone.com/reports/73256)
PHP (https://hackerone.com/php)	$500	str_repeat() sign mismatch based memory corruption (https://hackerone.com/reports/73255)
Python (https://hackerone.com/python)	$500	Multiple type confusions in unicode error handlers (https://hackerone.com/reports/73253)
Python (https://hackerone.com/python)	$500	Use after free in get_filter (https://hackerone.com/reports/73252)
Python (https://hackerone.com/python)	$1,500	Multiple use after free bugs in json encoding (https://hackerone.com/reports/73251)
Python (https://hackerone.com/python)	$1,500	Multiple use after free bugs in heapq module (https://hackerone.com/reports/73250)

Team	Bounty	Title
Python (https://hackerone.com/python)	$1,500	Multiple use after free bugs in element module (https://hackerone.com/reports/73249)
Python (https://hackerone.com/python)	$500	Tokenizer crash when processing undecodable source code (https://hackerone.com/reports/73248)
PHP (https://hackerone.com/php)	$500	php_stream_url_wrap_http_ex() type-confusion vulnerability (https://hackerone.com/reports/73247)
PHP (https://hackerone.com/php)	$500	Use-after-free in php_curl related to CURLOPT_FILE/_INFILE/_WRITEHEADER (https://hackerone.com/reports/73246)
PHP (https://hackerone.com/php)	$500	Type Confusion Vulnerability in SoapClient (https://hackerone.com/reports/73245)
PHP (https://hackerone.com/php)	$1,500	Use after free vulnerability in unserialize() with DateInterval (https://hackerone.com/reports/73244)
The Internet (https://hackerone.com/internet) ★	$3,000	libcurl: URL request injection (https://hackerone.com/reports/73242) **CVE-2014-8150** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8150)
OpenSSL (https://hackerone.com/openssl)	$2,500	Malformed ECParameters causes infinite loop (https://hackerone.com/reports/73241) **CVE-2015-1788** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1788)
PHP (https://hackerone.com/php)	$1,500	Integer overflow in ftp_genlist() resulting in heap overflow (https://hackerone.com/reports/73240) **CVE-2015-4022** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4022)
PHP (https://hackerone.com/php)	$1,500	ZIP Integer Overflow leads to writing past heap boundary (https://hackerone.com/reports/73239) **CVE-2015-2331** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2331)
PHP (https://hackerone.com/php)	$1,000	Buffer Over-read in unserialize when parsing Phar (https://hackerone.com/reports/73238) **CVE-2015-2783** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2783)

Team	Bounty	Title
PHP (https://hackerone.com/php)	$1,000	Buffer Over flow when parsing tar/zip/phar in phar_set_inode (https://hackerone.com/reports/73237) **CVE-2015-3329** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-3329)
OpenSSL (https://hackerone.com/openssl)	$500	X509_to_X509_REQ NULL pointer deref (https://hackerone.com/reports/73236) **CVE-2015-0288** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0288)
PHP (https://hackerone.com/php)	$1,500	Use After Free Vulnerability in unserialize() (https://hackerone.com/reports/73235) **CVE-2015-2787** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-2787)
PHP (https://hackerone.com/php)	$500	out of bounds read crashes php-cgi (https://hackerone.com/reports/73234) **CVE-2014-9427** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-9427)
Shopify (https://hackerone.com/shopify) ★	-	Body injection in mailto link while commenting shop blog (https://hackerone.com/reports/72976)
Shopify (https://hackerone.com/shopify) ★	-	Prevent Shop Admin From Seeing his Installed Apps / Install Persistent Unremovable App (https://hackerone.com/reports/72793)
HackerOne (https://hackerone.com/security)	$500	CSV Injection with the CVS export feature (https://hackerone.com/reports/72785)
Pornhub (https://hackerone.com/pornhub)	$5,000	Unauthenticated access to Content Management System - www1.pornhubpremium.com (https://hackerone.com/reports/72735)
ThisData (https://hackerone.com/thisdata)	-	Xss via Dropbox (https://hackerone.com/reports/72526)
Shopify (https://hackerone.com/shopify) ★	$500	XSS at Bulk editing ProductVariants (https://hackerone.com/reports/72331)
Pornhub (https://hackerone.com/pornhub)	$2,500	Multiple endpoints are vulnerable to XML External Entity injection (XXE) (https://hackerone.com/reports/72272)
Pornhub (https://hackerone.com/pornhub)	$10,000	Publicly exposed SVN repository, ht.pornhub.com (https://hackerone.com/reports/72243)

Team	Bounty	Title
Hired (https://hackerone.com/hired)	$250	URGENT - Subdomain Takeover on be.hired.com. due to unclaimed domain pointing to Heroku.com (https://hackerone.com/reports/71718)
Shopify (https://hackerone.com/shopify) ★	$500	XSS in Myshopify Admin Site in DISCOUNTS (https://hackerone.com/reports/71614)
VK.com (https://hackerone.com/vkcom)	$250	Отвязываем Twitter от любого профиля вк ! + несколько багов по дизайну (https://hackerone.com/reports/71337)
Airbnb (https://hackerone.com/airbnb)	-	authenticity_token is not random across page loads (https://hackerone.com/reports/71006)
HackerOne (https://hackerone.com/security)	-	Redirection Page throwing error instead of redirecting to site (https://hackerone.com/reports/67929)
Automattic (https://hackerone.com/automattic)	$100	Verification code issues for Two-Step Authentication (https://hackerone.com/reports/67660)
VK.com (https://hackerone.com/vkcom)	$100	Issue in the implementation of captcha and race condition (https://hackerone.com/reports/67562)
Shopify (https://hackerone.com/shopify) ★	$1,000	Bypass access restrictions from API (https://hackerone.com/reports/67557)
InVision (https://hackerone.com/invision)	$150	Enumeration and Guessable Email (OWASP-AT-002)T hrough Login Form (https://hackerone.com/reports/67393)
Shopify (https://hackerone.com/shopify) ★	$500	SSRF via 'Insert Image' feature of Products/Collections/Frontpage (https://hackerone.com/reports/67389)
Mail.Ru (https://hackerone.com/mailru)	$160	[my.mail.ru] CRLF Injection (https://hackerone.com/reports/67386)
Shopify (https://hackerone.com/shopify) ★	$500	SSRF via 'Add Image from URL' feature (https://hackerone.com/reports/67377)
Shopify (https://hackerone.com/shopify) ★	$500	Expire User Sessions in Admin Site does not expire user session in Shopify Application in IOS (https://hackerone.com/reports/67220)
Mail.Ru (https://hackerone.com/mailru)	$200	Possible xWork classLoader RCE: shared.mail.ru (https://hackerone.com/reports/67161)
Shopify (https://hackerone.com/shopify) ★	$500	XSS at Bulk editing products (https://hackerone.com/reports/67132)

Team	Bounty	Title
Shopify (https://hackerone.com/shopify) ★	$500	XSS at importing Product List (https://hackerone.com/reports/67125)
Slack (https://hackerone.com/slack)	-	Link vulnerability leads to phishing attacks (https://hackerone.com/reports/66994)
Sandbox Escape (https://hackerone.com/sandbox)	$3,000	Microsoft Internet Explorer ActiveX Broker Allows EPM Bypass (https://hackerone.com/reports/66958)
Marktplaats (https://hackerone.com/marktplaats)	-	Multiple Apache 2.2.22 Vulnerabilities (XSS/ Code Exec/ DoS) (https://hackerone.com/reports/66929)
Marktplaats (https://hackerone.com/marktplaats)	-	Content Spoofing - http://aanbieding.marktplaats.nl/wp-admin/admin-ajax.php (https://hackerone.com/reports/66914)
Legal Robot (https://hackerone.com/legalrobot)	$20	- Guessing registered users in legalrobot.com (https://hackerone.com/reports/66845)
LibSass (https://hackerone.com/libsass)	-	type confusion in Sass::ParserState::ParserState(Sass::ParserState const&) (https://hackerone.com/reports/66724) **CVE-2015-4459** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-4459)
Marktplaats (https://hackerone.com/marktplaats)	-	Secret Password reset key disclosed to third party site via referer in header (https://hackerone.com/reports/66626)
Mail.Ru (https://hackerone.com/mailru)	-	[tanks.mail.ru] Internet Explorer XSS via Request-URI (https://hackerone.com/reports/66423)
Mail.Ru (https://hackerone.com/mailru)	-	[mrgs.mail.ru] Internet Explorer XSS via Request-URI (https://hackerone.com/reports/66422)
Shopify (https://hackerone.com/shopify) ★	$500	[www.*.myshopify.com] CRLF Injection (https://hackerone.com/reports/66386)
Legal Robot (https://hackerone.com/legalrobot)	$20	No valid SPF record (https://hackerone.com/reports/66385)
Envoy (https://hackerone.com/envoy)	-	[dashboard.signwithenvoy.com] Open Redirect (https://hackerone.com/reports/66384)
HackerOne (https://hackerone.com/security)	$500	mailto: link injection on https://hackerone.com/directory (https://hackerone.com/reports/66262)
Mail.Ru (https://hackerone.com/mailru)	$250	[s.mail.ru] CRLF Injection (https://hackerone.com/reports/66257)

Team	Bounty	Title
VK.com (https://hackerone.com/vkcom)	$200	Уязвимость в Указание мест на фото + фича + хакинг (https://hackerone.com/reports/66235)
Coinbase (https://hackerone.com/coinbase)	-	Two-factor authentication (via SMS) (https://hackerone.com/reports/66223)
HackerOne (https://hackerone.com/security)	$500	Invitation is not properly cancelled while inviting to bug reports. (https://hackerone.com/reports/66151)
VK.com (https://hackerone.com/vkcom)	$500	XSS at http://vk.com on IE using flash files (https://hackerone.com/reports/66121)
Mail.Ru (https://hackerone.com/mailru)	-	help2.m.smailru.net: XSS (https://hackerone.com/reports/65921)
Coinbase (https://hackerone.com/coinbase)	$5,000	OAuth authorization page vulnerable to clickjacking (https://hackerone.com/reports/65825)
concrete5 (https://hackerone.com/concrete5)	-	No CSRF protection when creating new community points actions, and related stored XSS (https://hackerone.com/reports/65808)
VK.com (https://hackerone.com/vkcom)	$100	Не достаточная проверка логина скайп (https://hackerone.com/reports/65330)
VK.com (https://hackerone.com/vkcom)	-	XSS on added name album on videos. (https://hackerone.com/reports/65324)
Mapbox (https://hackerone.com/mapbox)	$1,000	Stored Cross-Site Scripting in Map Share Page (https://hackerone.com/reports/65284)
Legal Robot (https://hackerone.com/legalrobot)	$20	CSRF (https://hackerone.com/reports/65167)
Coinbase (https://hackerone.com/coinbase)	$5,000	Big Bug with Vault which i have already reported: Case #606962 (https://hackerone.com/reports/65084)
Mail.Ru (https://hackerone.com/mailru)	$250	HTML Injection на e.mail.ru (https://hackerone.com/reports/65013)
VK.com (https://hackerone.com/vkcom)	$500	API: Bug in method auth.validatePhone (https://hackerone.com/reports/64963)
Legal Robot (https://hackerone.com/legalrobot)	$40	Registration bypass using OAuth logical bug (https://hackerone.com/reports/64946)
Shopify (https://hackerone.com/shopify) ★	-	Header Misconfiguration - PHP API (https://hackerone.com/reports/64941)

Team	Bounty	Title
MapLogin (https://hackerone.com/maplogin)	-	Bypass verification of email while creating account(No rate limiting enable for verification code) (https://hackerone.com/reports/64666)
Legal Robot (https://hackerone.com/legalrobot)	$20	Missing security headers, possible clickjacking (https://hackerone.com/reports/64645)
MapLogin (https://hackerone.com/maplogin)	-	Not Completed Accounts Take Over (Urgent bug) (https://hackerone.com/reports/64626)
Legal Robot (https://hackerone.com/legalrobot)	$20	missing SPF for legalrobot.com (https://hackerone.com/reports/64561)
concrete5 (https://hackerone.com/concrete5)	-	No csrf protection on index.php/ccm/system/user/add_group, index.php/ccm/system/user/remove_group (https://hackerone.com/reports/64184)
Shopify (https://hackerone.com/shopify) ★	$1,000	Privilege Escalation - A `MEMBER` with no ACCESS to `ORDERS` can still access the orders by using `Order Printer APP` (https://hackerone.com/reports/64164)
Romit (https://hackerone.com/romit)	$50	Cross site scripting (https://hackerone.com/reports/63888)
HackerOne (https://hackerone.com/security)	$100	Potential denial of service in hackerone.com/<program>/reward_settings (https://hackerone.com/reports/63865)
HackerOne (https://hackerone.com/security)	$500	Logic error with notifications: user that has left team continues to receive notifications and can not 'clean' this area on account (https://hackerone.com/reports/63729)
Mavenlink (https://hackerone.com/mavenlink)	$100	XSS in https://app.mavenlink.com/workspaces/ (https://hackerone.com/reports/63537)
HackerOne (https://hackerone.com/security)	$500	External URL page bypass (https://hackerone.com/reports/63158)
Ruby on Rails (https://hackerone.com/rails)	-	Changeable model ids on vanilla update can lead to severely bad side-effects (https://hackerone.com/reports/63131)
Mail.Ru (https://hackerone.com/mailru)	-	https://voip.agent.mail.ru/phpinfo.php (https://hackerone.com/reports/63075)
Shopify (https://hackerone.com/shopify) ★	$500	Bulk Discount App in myshopify.com exposes http://bulkdiscounts.shopifyapps.com vulnerable to XSS (https://hackerone.com/reports/62861)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	-	Email Notification should be get while changing Paypal Email (https://hackerone.com/reports/62827)
Udemy (https://hackerone.com/udemy)	$150	Multiple sub domain are vulnerable because of leaking full path (https://hackerone.com/reports/62778)
Mail.Ru (https://hackerone.com/mailru)	$150	http://tp-dev1.tp.smailru.net/ (https://hackerone.com/reports/62544)
Mail.Ru (https://hackerone.com/mailru)	$200	tt-mac.i.mail.ru: Quagga 0.99.23.1 (Router) : Default password and default enable password (https://hackerone.com/reports/62531)
Shopify (https://hackerone.com/shopify) ★	$500	XSS in myshopify.com Admin site in TAX Overrides (https://hackerone.com/reports/62427)
Udemy (https://hackerone.com/udemy)	$100	XSS on https://www.udemy.com/asset/export.html (https://hackerone.com/reports/62400)
jsDelivr (https://hackerone.com/jsdelivr)	-	Pretty Photo Dom XSS (https://hackerone.com/reports/62385)
Udemy (https://hackerone.com/udemy)	$100	Ability to add pishing links in discusion ," Bypassing uneductional Links add " (https://hackerone.com/reports/62301)
concrete5 (https://hackerone.com/concrete5)	-	Multiple XSS Vulnerabilities in Concrete5 5.7.3.1 (https://hackerone.com/reports/62294)
Sandbox Escape (https://hackerone.com/sandbox)	$3,000	Internet Explorer Enhanced Protected Mode sandbox escape via a broker vulnerability (https://hackerone.com/reports/62174)
Udemy (https://hackerone.com/udemy)	$150	leak receipt of another user (https://hackerone.com/reports/61371)
Udemy (https://hackerone.com/udemy)	$100	xss on autoserch (https://hackerone.com/reports/61367)
Slack (https://hackerone.com/slack)	$100	Bypass of the SSRF protection (Slack commands, Phabricator integration) (https://hackerone.com/reports/61312)
Mail.Ru (https://hackerone.com/mailru)	$400	http://fitter1.i.mail.ru/browser/ торчит Graphite в мир (https://hackerone.com/reports/60573)
HackerOne (https://hackerone.com/security)	-	Logical Issue (Boosting Reputation points) (https://hackerone.com/reports/60429)
Mail.Ru (https://hackerone.com/mailru)	$400	store-agent.mail.ru: stacked blind injection (https://hackerone.com/reports/60420)
HackerOne (https://hackerone.com/security)	$500	Content Spoofing - External Link Warning Page (https://hackerone.com/reports/60402)

Team	Bounty	Title
Udemy (https://hackerone.com/udemy)	-	Misconfigured SPF Record Flag (https://hackerone.com/reports/60260)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	XSS Vulnerability on all pages (https://hackerone.com/reports/60201)
Udemy (https://hackerone.com/udemy)	$150	teach.udemy.com log poison vulnerability through wordpress debug.log being publically available (https://hackerone.com/reports/60058)
Udemy (https://hackerone.com/udemy)	$150	xss profile (https://hackerone.com/reports/60016)
concrete5 (https://hackerone.com/concrete5)	-	Local File Inclusion Vulnerability in Concrete5 version 5.7.3.1 (https://hackerone.com/reports/59665)
concrete5 (https://hackerone.com/concrete5)	-	SQL Injection Vulnerability in Concrete5 version 5.7.3.1 (https://hackerone.com/reports/59664)
concrete5 (https://hackerone.com/concrete5)	-	Sendmail Remote Code Execution Vulnerability in Concrete5 version 5.7.3.1 (https://hackerone.com/reports/59663)
concrete5 (https://hackerone.com/concrete5)	-	Multiple Stored Cross Site Scripting Vulnerabilities in Concrete5 version 5.7.3.1 (https://hackerone.com/reports/59662)
concrete5 (https://hackerone.com/concrete5)	-	Multiple Reflected Cross Site Scripting Vulnerabilities in Concrete5 version 5.7.3.1 (https://hackerone.com/reports/59661)
concrete5 (https://hackerone.com/concrete5)	-	Multiple Cross Site Request Forgery Vulnerabilities in Concrete5 version 5.7.3.1 (https://hackerone.com/reports/59660)
HackerOne (https://hackerone.com/security)	$500	Reopen Disable Accounts/ Hidden Access After Disable (https://hackerone.com/reports/59659)
drchrono (https://hackerone.com/drchrono)	$100	Accessing all appointments vulnerability (https://hackerone.com/reports/59508)
HackerOne (https://hackerone.com/security)	$500	Fake URL + Additional vectors for homograph attack (https://hackerone.com/reports/59469)
HackerOne (https://hackerone.com/security)	$500	Homograph attack (https://hackerone.com/reports/59375)
HackerOne (https://hackerone.com/security)	-	Homograph Attack (https://hackerone.com/reports/59372)
HackerOne (https://hackerone.com/security)	$500	Making any Report Failed to load (https://hackerone.com/reports/59369)

Team	Bounty	Title
Dropbox (https://hackerone.com/dropbox)	$512	XSS in dropbox main domain (https://hackerone.com/reports/59356)
Dropbox (https://hackerone.com/dropbox)	$216	Race condition when redeeming coupon codes (https://hackerone.com/reports/59179)
Shopify (https://hackerone.com/shopify) ★	$500	Stored XSS in the Shopify Discussion Forums (https://hackerone.com/reports/59015)
Mail.Ru (https://hackerone.com/mailru)	-	Flash XSS on img.mail.ru (https://hackerone.com/reports/58831)
OkCupid (https://hackerone.com/okcupid)	-	An XSS bug was fixed due to my report, but I didn't submit it through the h1 (https://hackerone.com/reports/58782)
Shopify (https://hackerone.com/shopify) ★	$500	SSL cookie without secure flag set (https://hackerone.com/reports/58679)
Shopify (https://hackerone.com/shopify) ★	$500	Content Spoofing (https://hackerone.com/reports/58630)
HackerOne (https://hackerone.com/security)	$500	Homograph attack (https://hackerone.com/reports/58612)
Romit (https://hackerone.com/romit)	$50	HTML injection in email sent by romit.io (https://hackerone.com/reports/57914)
HackerOne (https://hackerone.com/security)	-	Missing spf flags for hackerone.com (https://hackerone.com/reports/57736)
Romit (https://hackerone.com/romit)	$50	Server responds with the server error logs on account creation (https://hackerone.com/reports/57692)
Vimeo (https://hackerone.com/vimeo)	$500	API: missing invalidation of OAuth2 Authorization Code during access revocation causes authorization bypass (https://hackerone.com/reports/57603)
Shopify (https://hackerone.com/shopify) ★	$500	amazon aws s3 bucket content is public :- http://shopify.com.s3.amazonaws.com/ (https://hackerone.com/reports/57505)
Shopify (https://hackerone.com/shopify) ★	$500	XSS in experts.shopify.com (https://hackerone.com/reports/57459)
WordPoints (https://hackerone.com/wordpoints)	-	Rank Creation function not validating user inputs. (https://hackerone.com/reports/57263)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	$500	Open-redirect on hackerone.com (https://hackerone.com/reports/57163)
Shopify (https://hackerone.com/shopify) ★	-	comment out causes information disclosure (https://hackerone.com/reports/57125)
Shopify (https://hackerone.com/shopify) ★	$4,000	Notification request disclose private information about other myshopify accounts (https://hackerone.com/reports/56936)
Dropbox (https://hackerone.com/dropbox)	$512	SSRF vulnerablity in app webhooks (https://hackerone.com/reports/56828)
Dropbox (https://hackerone.com/dropbox)	-	XSS in version history of an HTML file in a shared folder (https://hackerone.com/reports/56803)
Shopify (https://hackerone.com/shopify) ★	-	Multiple issues on Checkout Process (https://hackerone.com/reports/56800)
Whisper (https://hackerone.com/whisper)	$30	Missing DMARC record (https://hackerone.com/reports/56793)
Shopify (https://hackerone.com/shopify) ★	$500	XSS on ecommerce.shopify.com (https://hackerone.com/reports/56779)
Shopify (https://hackerone.com/shopify) ★	-	XSS on support.shopify.com (https://hackerone.com/reports/56760)
HackerOne (https://hackerone.com/security)	$1,000	SPF whitelist of mandrill leads to email forgery (https://hackerone.com/reports/56742)
Shopify (https://hackerone.com/shopify) ★	$500	Invitation issue (https://hackerone.com/reports/56726)
Shopify (https://hackerone.com/shopify) ★	-	XSS - URL Redirects (https://hackerone.com/reports/56662)
Shopify (https://hackerone.com/shopify) ★	$500	Payment gateway status transferred to Shopify without authentication (https://hackerone.com/reports/56628)
Shopify (https://hackerone.com/shopify) ★	$1,000	Shop admin can change external login services (https://hackerone.com/reports/56626)
Shopify (https://hackerone.com/shopify) ★	$1,000	IDOR expire other user sessions (https://hackerone.com/reports/56511)

Team	Bounty	Title
Dropbox Acquisitions (https://hackerone.com/dropbox-acquisitions)	$216	Get email ID of any user on hackpad.com (https://hackerone.com/reports/56494)
Vimeo (https://hackerone.com/vimeo)	-	May cause account take over (Via invitation page) (https://hackerone.com/reports/56182)
Coin.Space (https://hackerone.com/coinspace)	-	SMTP protection not used (https://hackerone.com/reports/56177)
Twitter (https://hackerone.com/twitter)	-	Privecy Issue : view "Protected users" followers and following (https://hackerone.com/reports/56119)
Shopify (https://hackerone.com/shopify) ★	$2,000	Shopify android client all API request's response leakage, including access_token, cookie, response header, response body content (https://hackerone.com/reports/56002)
Shopify (https://hackerone.com/shopify) ★	$500	CSRF token fixation in facebook store app that can lead to adding attacker to victim acc (https://hackerone.com/reports/55911)
Shopify (https://hackerone.com/shopify) ★	$1,000	[persistent cross-site scripting] customers can target admins (https://hackerone.com/reports/55842)
Coinbase (https://hackerone.com/coinbase)	-	iframes considered harmful (https://hackerone.com/reports/55827)
Shopify (https://hackerone.com/shopify) ★	$500	Force 500 Internal Server Error on any shop (for one user) (https://hackerone.com/reports/55716)
Twitter (https://hackerone.com/twitter)	$280	Fabric.io: Ex-admin of an organization can delete team members (https://hackerone.com/reports/55670)
Shopify (https://hackerone.com/shopify) ★	-	Lack of SSL Pinning on POS Application (iOS) (https://hackerone.com/reports/55644)
Shopify (https://hackerone.com/shopify) ★	$500	Open Redirect after login at http://ecommerce.shopify.com (https://hackerone.com/reports/55546)
Shopify (https://hackerone.com/shopify) ★	$500	Authentication Failed Mobile version (https://hackerone.com/reports/55530)
Shopify (https://hackerone.com/shopify) ★	$500	Open redirection in OAuth (https://hackerone.com/reports/55525)
Twitter (https://hackerone.com/twitter)	-	Privacy Issue on protected tweets (https://hackerone.com/reports/55506)

Team	Bounty	Title
drchrono (https://hackerone.com/drchrono)	$700	XML Parser Bug: XXE over which leads to RCE (https://hackerone.com/reports/55431)
Faceless (https://hackerone.com/faceless)	-	Bypass Setup by External Activity Invoke (https://hackerone.com/reports/55064)
PHP (https://hackerone.com/php)	$3,000	Use after free vulnerability in unserialize() (https://hackerone.com/reports/55033)
PHP (https://hackerone.com/php)	$2,500	SoapClient's __call() type confusion through unserialize() (https://hackerone.com/reports/55030)
PHP (https://hackerone.com/php)	$2,500	Use after free vulnerability in unserialize() with DateTimeZone (https://hackerone.com/reports/55029)
PHP (https://hackerone.com/php)	$2,500	Free called on unitialized pointer in exif.c (https://hackerone.com/reports/55028)
OpenSSL (https://hackerone.com/openssl)	$3,000	Segmentation fault for invalid PSS parameters (https://hackerone.com/reports/55018)
Python (https://hackerone.com/python)	$9,000	Multiple Python integer overflows (https://hackerone.com/reports/55017)
Factlink (https://hackerone.com/factlink)	-	Frameset Proxy Problem (https://hackerone.com/reports/55009)
Shopify (https://hackerone.com/shopify) ★	$500	Missing spf flags for myshopify.com (https://hackerone.com/reports/54779)
Coinbase (https://hackerone.com/coinbase)	$1,000	Sandboxed iframes don't show confirmation screen (https://hackerone.com/reports/54733)
Mail.Ru (https://hackerone.com/mailru)	$500	e.mail.ru stored XSS in agent via sticker (smile) (https://hackerone.com/reports/54719)
Snapchat (https://hackerone.com/snapchat)	$100	Captcha Bypass in Snapchat's Geofilter Submission Process (https://hackerone.com/reports/54641)
Snapchat (https://hackerone.com/snapchat)	$100	Vulnerable to JavaScript injection. (WXS) (Javascript injection)! (https://hackerone.com/reports/54631)
Slack (https://hackerone.com/slack)	$100	Logout any user of same team (https://hackerone.com/reports/54610)
Mapbox (https://hackerone.com/mapbox)	$1,000	Persistent cross-site scripting (XSS) in map attribution (https://hackerone.com/reports/54327)

Team	Bounty	Title
Shopify (https://hackerone.com/shopify) ★	$500	Xss in website's link (https://hackerone.com/reports/54321)
HackerOne (https://hackerone.com/security)	-	Reflected Filename Download (https://hackerone.com/reports/54034)
Twitter (https://hackerone.com/twitter)	$420	Insecure Direct Object Reference - access to other user/group DM's (https://hackerone.com/reports/53858)
Twitter (https://hackerone.com/twitter)	$2,800	HTTP Response Splitting (CRLF injection) due to headers overflow (https://hackerone.com/reports/53843)
Dropbox Acquisitions (https://hackerone.com/dropbox-acquisitions)	$216	XSS in https://hackpad.com/ (https://hackerone.com/reports/53628)
Twitter (https://hackerone.com/twitter)	$1,400	XSS in twitter.com/safety/unsafe_link_warning (https://hackerone.com/reports/53098)
Phabricator (https://hackerone.com/phabricator)	$300	SSRF vulnerability (access to metadata server on EC2 and OpenStack) (https://hackerone.com/reports/53088)
Coinbase (https://hackerone.com/coinbase)	$100	Blacklist bypass on Callback URLs (https://hackerone.com/reports/53004)
Vimeo (https://hackerone.com/vimeo)	$250	[URGENT ISSUE] Add or Delete the videos in watch later list of any user . (https://hackerone.com/reports/52982)
OkCupid (https://hackerone.com/okcupid)	-	XSS on Send A Message Option (https://hackerone.com/reports/52831)
Phabricator (https://hackerone.com/phabricator)	$300	XSS with Time-of-Day Format (https://hackerone.com/reports/52822)
Vimeo (https://hackerone.com/vimeo)	$250	Share your channel to any user on vimeo without following him (https://hackerone.com/reports/52708)
Vimeo (https://hackerone.com/vimeo)	$250	Invite any user to your group without even following him (https://hackerone.com/reports/52707)
Twitter (https://hackerone.com/twitter)	$420	Insecure direct object reference - have access to deleted DM's (https://hackerone.com/reports/52646)
itBit Exchange (https://hackerone.com/itbit)	$200	secretKey for OTP , is getting leaked in response of a delete request ! (https://hackerone.com/reports/52645)

Team	Bounty	Title
itBit Exchange (https://hackerone.com/itbit)	$200	confirmation bypass of 2FA devices while they are deleting (https://hackerone.com/reports/52644)
Ubiquiti Networks (https://hackerone.com/ubnt)	$500	UniFi v3.2.10 Cross-Site Request Forgeries / Referer-Check Bypass (https://hackerone.com/reports/52635)
HackerOne (https://hackerone.com/security)	-	"learn more here", reward email - domain expired. (https://hackerone.com/reports/52532)
Dropbox Acquisitions (https://hackerone.com/dropbox-acquisitions)	-	unknow files Upload in profile photo (https://hackerone.com/reports/52383)
Vimeo (https://hackerone.com/vimeo)	$150	Insecure Direct Object References that allows to read any comment (even if it should be private) (https://hackerone.com/reports/52181)
Vimeo (https://hackerone.com/vimeo)	$500	Insecure Direct Object References in https://vimeo.com/forums (https://hackerone.com/reports/52176)
Twitter (https://hackerone.com/twitter)	$3,500	HTTP Response Splitting (CRLF injection) in report_story (https://hackerone.com/reports/52042)
HackerOne (https://hackerone.com/security)	$500	Open redirect in "Language change". (https://hackerone.com/reports/52035)
Caviar (https://hackerone.com/caviar)	$500	Remotely modifying courier Account Details (https://hackerone.com/reports/51846)
Vimeo (https://hackerone.com/vimeo)	$250	Post in private groups after getting removed (https://hackerone.com/reports/51817)
Flash (https://hackerone.com/flash)	$2,000	Flash Cross Domain Policy Bypass by Using File Upload and Redirection - only in Chrome (https://hackerone.com/reports/51265)
IRCCloud (https://hackerone.com/irccloud)	-	Email verification links still valid after changing it 2x (https://hackerone.com/reports/51166)
itBit Exchange (https://hackerone.com/itbit)	-	ITBit Vulnerable to SSLSTrip (https://hackerone.com/reports/51154)
Mail.Ru (https://hackerone.com/mailru)	-	XSS in touch.sports.mail.ru (https://hackerone.com/reports/51140)
Mail.Ru (https://hackerone.com/mailru)	-	XSS in ad.mail.ru (https://hackerone.com/reports/51061)
Mail.Ru (https://hackerone.com/mailru)	-	XSS in realty.mail.ru (https://hackerone.com/reports/51060)

Team	Bounty	Title
Vimeo (https://hackerone.com/vimeo)	$250	A user can enhance their videos with paid tracks without buying the track (https://hackerone.com/reports/50941)
Whisper (https://hackerone.com/whisper)	$10	CVE-2014-0224 openssl ccs vulnerability (https://hackerone.com/reports/50885)
Whisper (https://hackerone.com/whisper)	$100	Bypass pin(4 digit passcode on your android app) (https://hackerone.com/reports/50884)
Vimeo (https://hackerone.com/vimeo)	$500	A user can post comments on other user's private videos (https://hackerone.com/reports/50829)
Vimeo (https://hackerone.com/vimeo)	$250	A user can add videos to other user's private groups (https://hackerone.com/reports/50786)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Image Alt. Text (https://hackerone.com/reports/50782)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Message to Display When No Pages Listed. (https://hackerone.com/reports/50780)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Bio/Quote (https://hackerone.com/reports/50779)
Vimeo (https://hackerone.com/vimeo)	$250	A user can edit comments even after video comments are disabled (https://hackerone.com/reports/50776)
Twitter (https://hackerone.com/twitter)	$560	open redirect sends authenticity_token to any website or (ip address) (https://hackerone.com/reports/50752)
Ubiquiti Networks (https://hackerone.com/ubnt)	$500	CSRF in login form would led to account takeover (https://hackerone.com/reports/50703)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS In Company URL (https://hackerone.com/reports/50662)
HackerOne (https://hackerone.com/security)	-	Reflected File Download attack allows attacker to 'upload' executables to hackerone.com domain (https://hackerone.com/reports/50658)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in testimonial Company (https://hackerone.com/reports/50656)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Testimonial Position (https://hackerone.com/reports/50645)

Team	Bounty	Title
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Testimonial name (https://hackerone.com/reports/50644)
concrete5 (https://hackerone.com/concrete5)	-	Stored Xss in Feature Paragraph (https://hackerone.com/reports/50642)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Feature tile (https://hackerone.com/reports/50639)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in title of date navigation (https://hackerone.com/reports/50627)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Title of the topic List (https://hackerone.com/reports/50626)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in Contact Form (https://hackerone.com/reports/50564)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS on Search Title (https://hackerone.com/reports/50556)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS on Title of Page List in edit page list (https://hackerone.com/reports/50554)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS on Blog's page Tile (https://hackerone.com/reports/50552)
Phabricator (https://hackerone.com/phabricator)	-	Server Side Request Forgery in macro creation (https://hackerone.com/reports/50537)
concrete5 (https://hackerone.com/concrete5)	-	Self Xss on File Replace (https://hackerone.com/reports/50481)
Adobe (https://hackerone.com/adobe)	-	Adobe XSS (https://hackerone.com/reports/50389)
Adobe (https://hackerone.com/adobe)	-	Open redirect and reflected xss in http://youthvoices.adobe.com/community?return_url=[payload her] (https://hackerone.com/reports/50379)
Adobe (https://hackerone.com/adobe)	-	files.acrobat.com stored XSS via send file (https://hackerone.com/reports/50358)
The Internet (https://hackerone.com/internet) ★	$7,500	FREAK: Factoring RSA_EXPORT Keys to Impersonate TLS Servers (https://hackerone.com/reports/50170)

Team	Bounty	Title
Adobe (https://hackerone.com/adobe)	-	Reflected Cross Site Scripting - 'puser' Parameter in login page (https://hackerone.com/reports/50157)
Twitter (https://hackerone.com/twitter)	$1,400	XSS in original referrer after follow (https://hackerone.com/reports/50134)
Square (https://hackerone.com/square)	-	Invitation threshold (https://hackerone.com/reports/50120)
Romit (https://hackerone.com/romit)	$50	The csrf token remains same after user logs in (https://hackerone.com/reports/49974)
Ruby on Rails (https://hackerone.com/rails)	$1,000	rails-ujs will send CSRF tokens to other origins (https://hackerone.com/reports/49935)
Twitter (https://hackerone.com/twitter)	$560	Twitter Ads Campaign information disclosure through admin without any authentication. (https://hackerone.com/reports/49806)
Twitter (https://hackerone.com/twitter)	$1,400	Open Redirect leak of authenticity_token lead to full account take over. (https://hackerone.com/reports/49759)
Vimeo (https://hackerone.com/vimeo)	-	URGENT - Subdomain Takeover on status.vimeo.com due to unclaimed domain pointing to statuspage.io (https://hackerone.com/reports/49663)
HackerOne (https://hackerone.com/security)	$5,000	Improperly validated fields allows injection of arbitrary HTML via spoofed React objects (https://hackerone.com/reports/49652)
HackerOne (https://hackerone.com/security)	-	Auto Approval of Invitation to join Team as a Team member (https://hackerone.com/reports/49566)
Vimeo (https://hackerone.com/vimeo)	$250	Vimeo + & Vimeo PRO Unautorised Tax bypass (https://hackerone.com/reports/49561)
Airbnb (https://hackerone.com/airbnb)	-	SSL Issues (https://hackerone.com/reports/49537)
Airbnb (https://hackerone.com/airbnb)	-	Vulnerability type xss uncovered in airbnb.es (https://hackerone.com/reports/49513)
Airbnb (https://hackerone.com/airbnb)	-	Generating Unlimited Free Travel Gift Invites | IDOR (https://hackerone.com/reports/49499)
Twitter (https://hackerone.com/twitter)	-	Cross site Port Scanning bug in twitter developers console (https://hackerone.com/reports/49474)
Mail.Ru (https://hackerone.com/mailru)	$300	RCE через JDWP (https://hackerone.com/reports/49408)

Team	Bounty	Title
Dropbox (https://hackerone.com/dropbox)	-	Create N Accounts In Dropbox Irrespective Of Domain (https://hackerone.com/reports/49378)
HackerOne (https://hackerone.com/security)	-	Substantially weakened authenticity verification when using 'Remember me for a week' (https://hackerone.com/reports/49357)
Airbnb (https://hackerone.com/airbnb)	-	I Can Delete Any Airbnb Users Symbol! (https://hackerone.com/reports/49356)
Vimeo (https://hackerone.com/vimeo)	-	Bypassing Email verification (https://hackerone.com/reports/49304)
Mail.Ru (https://hackerone.com/mailru)	$150	scfbp.tng.mail.ru: Heartbleed (https://hackerone.com/reports/49139)
Mail.Ru (https://hackerone.com/mailru)	$150	HDFS NameNode Public disclosure: http://185.5.139.33:50070/dfshealth.jsp (https://hackerone.com/reports/49035)
Todoist (https://hackerone.com/todoist)	$25	Remotely removing credit cards from business accounts! (https://hackerone.com/reports/48690)
Todoist (https://hackerone.com/todoist)	$25	Taking over a Business Account Admin (https://hackerone.com/reports/48682)
Twitter (https://hackerone.com/twitter)	$1,400	Redirect URL in /intent/ functionality is not properly escaped (https://hackerone.com/reports/48516)
HackerOne (https://hackerone.com/security)	$500	Team member invitations to sandboxed teams are not invalidated consistently (v2) (https://hackerone.com/reports/48422)
HackerOne (https://hackerone.com/security)	-	Restrict any user from logging into his account. (https://hackerone.com/reports/48416)
The Internet (https://hackerone.com/internet) ★	$5,000	Bad Write in TTF font parsing (win32k.sys) (https://hackerone.com/reports/48100)
Coinbase (https://hackerone.com/coinbase)	$100	open authentication bug (https://hackerone.com/reports/48065)
Slack (https://hackerone.com/slack)	$200	Team admin can add billing contacts (https://hackerone.com/reports/47940)
Dropbox Acquisitions (https://hackerone.com/dropbox-acquisitions)	$729	Privilege Escalation at invite feature @hackpad.com (https://hackerone.com/reports/47932)

Team	Bounty	Title
Twitter (https://hackerone.com/twitter)	$140	Reporting user's profile by using another people's ID (https://hackerone.com/reports/47888)
Mail.Ru (https://hackerone.com/mailru)	-	Full Path Disclosure (https://hackerone.com/reports/47876)
The Internet (https://hackerone.com/internet) ★	$3,000	Heap overflow in H. Spencer's regex library on 32 bit systems (https://hackerone.com/reports/47779)
Romit (https://hackerone.com/romit)	$50	Email Enumeration (POC) (https://hackerone.com/reports/47627)
QIWI (https://hackerone.com/qiwi)	$200	[ishop.qiwi.com] XSS + Misconfiguration (https://hackerone.com/reports/47536)
Mail.Ru (https://hackerone.com/mailru)	$600	Same Origin Policy bypass (https://hackerone.com/reports/47495)
HackerOne (https://hackerone.com/security)	$2,000	CSP Bypass: Click handler for links with data-method="post" can cause authenticity_token to be sent off domain (https://hackerone.com/reports/47472)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Approve topup method by sender of this method (https://hackerone.com/reports/47384)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Enum phone numbers thru /en/sims/topup/add/ (https://hackerone.com/reports/47362)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Username and sim id enum (https://hackerone.com/reports/47358)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	CSRF token from another valid user session accepted (https://hackerone.com/reports/47357)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Stored xss in user name (2) affected another user. (https://hackerone.com/reports/47349)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Stored xss in user name (https://hackerone.com/reports/47343)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Reflected xss in user name thru cookie (https://hackerone.com/reports/47341)
Mail.Ru (https://hackerone.com/mailru)	-	XSS Vulnerability in cfire.mail.ru/screen/1/ (https://hackerone.com/reports/47322)
Ruby on Rails (https://hackerone.com/rails)	-	JSON keys are not properly escaped (https://hackerone.com/reports/47280)

Team	Bounty	Title
Informatica (https://hackerone.com/informatica)	-	XSS in Search Communities Function (https://hackerone.com/reports/47235)
Flash (https://hackerone.com/flash)	$7,500	Use After Free in Flash MessageChannel.send can cause arbitrary code execution (https://hackerone.com/reports/47234)
Flash (https://hackerone.com/flash)	$10,000	Use after free during the StageVideoAvailabilityEvent can result in arbitrary code execution (https://hackerone.com/reports/47232)
Flash (https://hackerone.com/flash)	$10,000	Race condition in workers may cause an exploitable double free by abusing bytearray.compress() (https://hackerone.com/reports/47227)
InVision (https://hackerone.com/invision)	$200	Javascript Injection (https://hackerone.com/reports/47223)
itBit Exchange (https://hackerone.com/itbit)	$50	Leakage of sensitive wallet tokens to third party sites (https://hackerone.com/reports/47140)
Flash (https://hackerone.com/flash)	$2,000	Adobe Flash Player Out-of-Bound Access Vulnerability (https://hackerone.com/reports/47012)
Vimeo (https://hackerone.com/vimeo)	$250	Red October 1511493148.cloud.vimeo.com (https://hackerone.com/reports/46954)
HackerOne (https://hackerone.com/security)	-	Markdown code block sequence makes report unreadable (https://hackerone.com/reports/46952)
HackerOne (https://hackerone.com/security)	$5,000	Markdown parsing issue enables insertion of malicious tags and event handlers (https://hackerone.com/reports/46916)
Twitter (https://hackerone.com/twitter)	$560	Twitter Card - Parent Window Redirection (https://hackerone.com/reports/46818)
Slack (https://hackerone.com/slack)	$100	Team admin can change unauthorized team setting (allow_message_deletion) (https://hackerone.com/reports/46750)
Slack (https://hackerone.com/slack)	$200	Team admin can change unauthorized team setting (require_at_for_mention) (https://hackerone.com/reports/46747)
Romit (https://hackerone.com/romit)	-	CSRF token leakage (https://hackerone.com/reports/46736)
Romit (https://hackerone.com/romit)	$50	Frictionless Transferring of Wallet Ownership (https://hackerone.com/reports/46618)
Square (https://hackerone.com/square)	-	Redirecting a victim elsewhere through shopseen 0auth (https://hackerone.com/reports/46497)

Team	Bounty	Title
Twitter (https://hackerone.com/twitter)	$1,260	Problem with OAuth (https://hackerone.com/reports/46485)
HackerOne (https://hackerone.com/security)	$500	Team member invitations to sandboxed teams are not invalidated consistently (https://hackerone.com/reports/46429)
HackerOne (https://hackerone.com/security)	$500	Insecure Direct Object Reference vulnerability (https://hackerone.com/reports/46397)
Nearby Live (https://hackerone.com/nearby)	-	Group Invite not properly authenticated (https://hackerone.com/reports/46379)
HackerOne (https://hackerone.com/security)	-	In markdown, parsing things like @danlec and #46072 after links is unsafe (https://hackerone.com/reports/46312)
Vimeo (https://hackerone.com/vimeo)	-	Can message users without the proper authorization (https://hackerone.com/reports/46113)
Vimeo (https://hackerone.com/vimeo)	-	Brute force on "vimeo" cookie (https://hackerone.com/reports/46109)
HackerOne (https://hackerone.com/security)	$5,000	Vulnerability with the way \ escaped characters in <http://danlec.com> style links are rendered (https://hackerone.com/reports/46072)
Ruby on Rails (https://hackerone.com/rails)	-	Explicit, dynamic render path: Dir. Trav + RCE (https://hackerone.com/reports/46019)
Vimeo (https://hackerone.com/vimeo)	$250	CRITICAL vulnerability - Insecure Direct Object Reference - Unauthorized access to `Videos` of Channel whose privacy is set to `Private`. (https://hackerone.com/reports/45960)
Zaption (https://hackerone.com/zaption)	-	[zaption.com] Open Redirect (https://hackerone.com/reports/45516)
Trello (https://hackerone.com/trello)	$128	[blog.trello.com] CRLF Injection (https://hackerone.com/reports/45514)
Trello (https://hackerone.com/trello)	$64	[trello.com] Open Redirect (https://hackerone.com/reports/45513)
Vimeo (https://hackerone.com/vimeo)	$100	XSS on Vimeo (https://hackerone.com/reports/45484)
Vimeo (https://hackerone.com/vimeo)	-	CSRF bypass (https://hackerone.com/reports/45428)
Vimeo (https://hackerone.com/vimeo)	$100	ftp upload of video allows naming that is not sanitized as the manual naming (https://hackerone.com/reports/45368)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Number, username and name disclosure (https://hackerone.com/reports/45243)

Team	Bounty	Title
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Stored XSS in Direct debit name (https://hackerone.com/reports/45233)
Vimeo (https://hackerone.com/vimeo)	-	Full account takeover via Add a New Email to account without email verified and without password confirmation. (https://hackerone.com/reports/45084)
Informatica (https://hackerone.com/informatica)	-	[community.informatica.com] - CSRF in Private Messages allows to move user's messages to Trash (https://hackerone.com/reports/45050)
Square (https://hackerone.com/square)	-	HTTP Header revealing server information. (https://hackerone.com/reports/45033)
itBit Exchange (https://hackerone.com/itbit)	$50	weird bug ! (missing validation on new email verfication) (https://hackerone.com/reports/44909)
HackerOne (https://hackerone.com/security)	$500	Improper way of validating a program (https://hackerone.com/reports/44888)
itBit Exchange (https://hackerone.com/itbit)	$200	Unsecure data in "device" response - OTP (https://hackerone.com/reports/44864)
Vimeo (https://hackerone.com/vimeo)	$100	Vimeo Search - XSS Vulnerability [http://vimeo.com/search] (https://hackerone.com/reports/44798)
Dropbox (https://hackerone.com/dropbox)	-	Unvalidated Redirects and Stored XSS (https://hackerone.com/reports/44739)
Twitter (https://hackerone.com/twitter)	$140	Insecure Data Storage in Vine Android App (https://hackerone.com/reports/44727)
Mobile Vikings (https://hackerone.com/mobilevikings)	-	Insecure crossdomain.xml (https://hackerone.com/reports/44652)
itBit Exchange (https://hackerone.com/itbit)	$50	Email Length Verification (https://hackerone.com/reports/44588)
Twitter (https://hackerone.com/twitter)	-	URGENT - SUBDOMAIN TAKEOVER ON TWITTER ACQ. (https://hackerone.com/reports/44578)
itBit Exchange (https://hackerone.com/itbit)	$500	Notification Emails: IP + Content-Spoofing (https://hackerone.com/reports/44555)
Ruby on Rails (https://hackerone.com/rails)	$500	RCE due to Web Console IP Whitelist bypass in Rails 4.0 and 4.1 (https://hackerone.com/reports/44513)

Team	Bounty	Title
Vimeo (https://hackerone.com/vimeo)	$1,000	XSS on any site that includes the moogaloop flash player | deprecated embed code (https://hackerone.com/reports/44512)
Twitter (https://hackerone.com/twitter)	$140	Flaw in login with twitter to steal Oauth tokens (https://hackerone.com/reports/44492)
Vimeo (https://hackerone.com/vimeo)	-	unvalid open authentication with facebook (https://hackerone.com/reports/44425)
Twitter (https://hackerone.com/twitter)	-	Path disclosure in platform0.twitter.com (https://hackerone.com/reports/44371)
HackerOne (https://hackerone.com/security)	-	Add text to the title of the page "Thanks" (https://hackerone.com/reports/44359)
Mail.Ru (https://hackerone.com/mailru)	-	http://217.69.136.200/?p=2&c=Fetcher%20cluster&h=fetcher1.mail.ru (https://hackerone.com/reports/44295)
Mail.Ru (https://hackerone.com/mailru)	$150	Heartbleed: my.com (185.30.178.33) port 1433 (https://hackerone.com/reports/44294)
Vimeo (https://hackerone.com/vimeo)	-	Application XSS filter function Bypass may allow Multiple stored XSS (https://hackerone.com/reports/44217)
Vimeo (https://hackerone.com/vimeo)	-	Poodle bleed vulnerability in cloud sub domain (https://hackerone.com/reports/44202)
Vimeo (https://hackerone.com/vimeo)	-	Open Redirection Security Filter bypassed (https://hackerone.com/reports/44157)
Vimeo (https://hackerone.com/vimeo)	$1,000	Make API calls on behalf of another user (CSRF protection bypass) (https://hackerone.com/reports/44146)
Vimeo (https://hackerone.com/vimeo)	-	USER PRIVACY VIOLATED (PRIVATE DATA GETTING TRANSFER OVER INSECURE CHANNEL) (https://hackerone.com/reports/44056)
Mail.Ru (https://hackerone.com/mailru)	$150	Hadoop Node available to public (https://hackerone.com/reports/44052)
Vimeo (https://hackerone.com/vimeo)	$100	CRITICAL full source code/config disclosure for Cameo (https://hackerone.com/reports/43998)
Vimeo (https://hackerone.com/vimeo)	-	Serious Vulnerability Found (https://hackerone.com/reports/43997)
Twitter (https://hackerone.com/twitter)	$420	twitter android app Fragment Injection (https://hackerone.com/reports/43988)

Team	Bounty	Title
Vimeo (https://hackerone.com/vimeo)	$1,000	abusing Thumbnails(https://vimeo.com/upload/select_thumb) to see a private video (https://hackerone.com/reports/43850)
Vimeo (https://hackerone.com/vimeo)	-	No Limitation on Following allows user to follow people automatically! (https://hackerone.com/reports/43846)
Vimeo (https://hackerone.com/vimeo)	$250	Ability to Download Music Tracks Without Paying (Missing permission check on `/musicstore/download`) (https://hackerone.com/reports/43770)
Vimeo (https://hackerone.com/vimeo)	-	profile photo update bypass (https://hackerone.com/reports/43758)
Mail.Ru (https://hackerone.com/mailru)	$100	Раскрытие номера мобильного телефона при двухфакторной аутентификации (https://hackerone.com/reports/43752)
Mail.Ru (https://hackerone.com/mailru)	-	3k.mail.ru: XSS (https://hackerone.com/reports/43723)
Vimeo (https://hackerone.com/vimeo)	$100	player.vimeo.com - Reflected XSS Vulnerability (https://hackerone.com/reports/43672)
Vimeo (https://hackerone.com/vimeo)	$1,000	Adding profile picture to anyone on Vimeo (https://hackerone.com/reports/43617)
Vimeo (https://hackerone.com/vimeo)	$260	Buying ondemand videos that 0.1 and sometimes for free (https://hackerone.com/reports/43602)
Python (https://hackerone.com/python)	$1,000	PyUnicode_FromFormatV crasher (https://hackerone.com/reports/43443)
Ruby on Rails (https://hackerone.com/rails)	$1,000	Arbitrary file existence disclosure in Action Pack (https://hackerone.com/reports/43440) **CVE-2014-7829** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7829)
OkCupid (https://hackerone.com/okcupid)	-	Stored XSS in popup messages window (https://hackerone.com/reports/43324)
HackerOne (https://hackerone.com/security)	-	HTTPS is not enforced for objects stored by HackerOne on Amazon S3 (https://hackerone.com/reports/43280)
Dropbox (https://hackerone.com/dropbox)	-	WP User Enumeration is possible at https://blog.dropbox.com (https://hackerone.com/reports/43269)
Vimeo (https://hackerone.com/vimeo)	-	Misconfigured crossdomain.xml - vimeo.com (https://hackerone.com/reports/43070)

Team	Bounty	Title
Twitter (https://hackerone.com/twitter)	$1,120	Fabric.io - an app admin can delete team members from other user apps (https://hackerone.com/reports/43065)
Twitter (https://hackerone.com/twitter)	$1,400	fabric.io - app member can make himself an admin (https://hackerone.com/reports/42961)
Ruby on Rails (https://hackerone.com/rails)	-	Denial of Service in Action Pack Exception Handling (https://hackerone.com/reports/42797)
Nearby Live (https://hackerone.com/nearby)	-	Web Server information disclosure. (https://hackerone.com/reports/42780)
Ruby on Rails (https://hackerone.com/rails)	-	Data-Tags and the New HTML Sanitizer Subverts CSRF protection (https://hackerone.com/reports/42728)
Vimeo (https://hackerone.com/vimeo)	$100	APIs for channels allow HTML entities that may cause XSS issue (https://hackerone.com/reports/42702)
Vimeo (https://hackerone.com/vimeo)	$5,000	Vimeo.com Insecure Direct Object References Reset Password (https://hackerone.com/reports/42587)
Vimeo (https://hackerone.com/vimeo)	$100	Vimeo.com - reflected xss vulnerability (https://hackerone.com/reports/42584)
Vimeo (https://hackerone.com/vimeo)	$100	Vimeo.com - Reflected XSS Vulnerability (https://hackerone.com/reports/42582)
Twitter (https://hackerone.com/twitter)	-	Account Deleted without any confirmation (https://hackerone.com/reports/42403)
Uber (https://hackerone.com/uber) ★	$500	XSS on partners.uber.com (https://hackerone.com/reports/42393)
Twitter (https://hackerone.com/twitter)	-	No rate limiting on creating lists (https://hackerone.com/reports/42250)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in adding fileset (https://hackerone.com/reports/42248)
Flash (https://hackerone.com/flash)	$1,000	chrome allows POST requests with custom headers using flash + 307 redirect (https://hackerone.com/reports/42240)
Twitter (https://hackerone.com/twitter)	$420	URGENT - Subdomain Takeover on users.tweetdeck.com , the same issue of report #32825 (https://hackerone.com/reports/42236)
Romit (https://hackerone.com/romit)	$250	stored xss in transaction (https://hackerone.com/reports/42161)

Team	Bounty	Title
Nearby Live (https://hackerone.com/nearby)	-	Gain access to any user's email address (https://hackerone.com/reports/42154)
Mail.Ru (https://hackerone.com/mailru)	-	/surveys/2auth: DOM-based XSS (https://hackerone.com/reports/41940)
Mail.Ru (https://hackerone.com/mailru)	-	GET /surveys/2auth: XSS (https://hackerone.com/reports/41939)
Twitter (https://hackerone.com/twitter)	$1,400	HTML/XSS rendered in Android App of Crashlytics through fabric.io (https://hackerone.com/reports/41856)
Romit (https://hackerone.com/romit)	$250	Stored XSS in api key of operator wallet (https://hackerone.com/reports/41758)
Romit (https://hackerone.com/romit)	$100	Error stack trace (https://hackerone.com/reports/41469)
Twitter (https://hackerone.com/twitter)	$140	POODLE Bug: 199.16.156.44, 199.16.156.108, mx4.twitter.com (https://hackerone.com/reports/41240)
HackerOne (https://hackerone.com/security)	-	Reflected File Download (https://hackerone.com/reports/39658)
Twitter (https://hackerone.com/twitter)	$280	Open redirection in fabric.io (https://hackerone.com/reports/39631)
Mail.Ru (https://hackerone.com/mailru)	$100	No bruteforce protection leads to enumeration of emails in http://e.mail.ru/ (https://hackerone.com/reports/39486)
Phabricator (https://hackerone.com/phabricator)	$500	Phabricator Phame Blog Skins Local File Inclusion (https://hackerone.com/reports/39428)
Mail.Ru (https://hackerone.com/mailru)	-	[odnoklassniki.ru] XSS via Host (https://hackerone.com/reports/39316)
Dropbox (https://hackerone.com/dropbox)	-	[monitor.sjc.dropbox.com] CRLF Injection (https://hackerone.com/reports/39261)
Informatica (https://hackerone.com/informatica)	-	Missing SPF for informatica.com (https://hackerone.com/reports/39250)
WePay (https://hackerone.com/wepay)	-	Broken Authentication – Session Token bug (https://hackerone.com/reports/39203)
C2FO (https://hackerone.com/c2fo)	-	[admin.c2fo.com] Open Redirect (https://hackerone.com/reports/39198)
Vimeo (https://hackerone.com/vimeo)	$500	[vimeopro.com] CRLF Injection (https://hackerone.com/reports/39181)

Team	Bounty	Title
HackerOne (https://hackerone.com/security)	-	URL Crashing browser. {Tested on firefox, Chrome and Safari} (https://hackerone.com/reports/39139)
Phabricator (https://hackerone.com/phabricator)	$300	Phabricator Diffusion application allows unauthorized users to delete mirrors (https://hackerone.com/reports/38965)
concrete5 (https://hackerone.com/concrete5)	-	stored XSS in concrete5 5.7.2.1 (https://hackerone.com/reports/38890)
concrete5 (https://hackerone.com/concrete5)	-	SQL injection in conc/index.php/ccm/system/search/users/submit (https://hackerone.com/reports/38778)
Square (https://hackerone.com/square)	$500	Delayed, fraudulent transactions possible with encrypted Square Reader devices due to lack of server-side verification of device transaction counter (https://hackerone.com/reports/38682)
Mail.Ru (https://hackerone.com/mailru)	$250	[connect.mail.ru] Memory Disclosure / IE XSS (https://hackerone.com/reports/38615)
HackerOne (https://hackerone.com/security)	$500	Issue with password change (https://hackerone.com/reports/38343)
HackerOne (https://hackerone.com/security)	$500	Breaking Bugs as team member (https://hackerone.com/reports/38232)
Openfolio (https://hackerone.com/openfolio)	$100	xss in /browse/contacts/ (https://hackerone.com/reports/38189)
Python (https://hackerone.com/python)	$6,500	Misc Python bugs (Memory Corruption & Use After Free) (https://hackerone.com/reports/38170)
QIWI (https://hackerone.com/qiwi)	$150	[qiwi.com] Open Redirect (https://hackerone.com/reports/38157)
Greenhouse.io (https://hackerone.com/greenhouse)	$1,000	Subdomain Takeover using blog.greenhouse.io pointing to Hubspot (https://hackerone.com/reports/38007)
Eobot (https://hackerone.com/eobotcom)	-	Multiple information disclosure (https://hackerone.com/reports/37862)
Twitter (https://hackerone.com/twitter)	-	Abuse of "Remember Me" functionality. (https://hackerone.com/reports/37822)
OkCupid (https://hackerone.com/okcupid)	-	Rosetta flash vulnerability in clientstats AJAX script (https://hackerone.com/reports/37786)
Sucuri (https://hackerone.com/sucuri)	-	Form contained inside page loaded over SSL submits its contents to another page over HTTP (https://hackerone.com/reports/37652)

Team	Bounty	Title
Eobot (https://hackerone.com/eobotcom)	$10	XSS in www.eobot.com(IE9 only) (https://hackerone.com/reports/37622)
Sucuri (https://hackerone.com/sucuri)	$250	Open Redirect in unmask.sucuri.net (https://hackerone.com/reports/37593)
InVision (https://hackerone.com/invision)	$150	CSRF Token in cookies! (https://hackerone.com/reports/37301)
Twitter (https://hackerone.com/twitter)	-	Homograph attack. (https://hackerone.com/reports/37108)
Eobot (https://hackerone.com/eobotcom)	-	OPTIONS METHOD ENABLED (https://hackerone.com/reports/37102)
Twitter (https://hackerone.com/twitter)	$1,400	[Stored XSS] vine.co - profile page (https://hackerone.com/reports/36986)
Twitter (https://hackerone.com/twitter)	-	Notifications can mark as read by CSRF (https://hackerone.com/reports/36980)
Coinbase (https://hackerone.com/coinbase)	$100	New Device Confirmation, token is valid until not used. (https://hackerone.com/reports/36594)
QIWI (https://hackerone.com/qiwi)	-	Metadata in hosted files is disclosing Usernames, Printers, paths, admin guides. emails (https://hackerone.com/reports/36586)
ThisData (https://hackerone.com/thisdata)	-	Missing SPF header on revert.io (https://hackerone.com/reports/36459)
QIWI (https://hackerone.com/qiwi)	$1,000	[send.qiwi.ru] Soap-based XXE vulnerability /soapserver/ (https://hackerone.com/reports/36450)
Openfolio (https://hackerone.com/openfolio)	-	Options Method Enabled (https://hackerone.com/reports/36409)
QIWI (https://hackerone.com/qiwi)	$100	[qiwi.com] /oauth/confirm.action XSS (https://hackerone.com/reports/36319)
Flash (https://hackerone.com/flash)	$2,000	Adobe Flash Player MP4 Use-After-Free Vulnerability (https://hackerone.com/reports/36279)
Apache httpd (https://hackerone.com/apache)	$500	mod_proxy_fcgi buffer overflow (https://hackerone.com/reports/36264) **CVE-2014-3583** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3583)
HackerOne (https://hackerone.com/security)	$500	Logic Issue with Reputation: Boost Reputation Points (https://hackerone.com/reports/36211)

Team	Bounty	Title
Phabricator (https://hackerone.com/phabricator)	-	Content injection (https://hackerone.com/reports/36112)
QIWI (https://hackerone.com/qiwi)	$250	CRLF Injection [ishop.qiwi.com] (https://hackerone.com/reports/36105)
Twitter (https://hackerone.com/twitter)	-	Headers Missing (https://hackerone.com/reports/36053)
Factlink (https://hackerone.com/factlink)	-	File name/folder enumeration. (https://hackerone.com/reports/35823)
QIWI (https://hackerone.com/qiwi)	-	Code for registration of qiwi account is not coming even after a long interval of time for Indian mobile number (https://hackerone.com/reports/35532)
QIWI (https://hackerone.com/qiwi)	$200	[send.qiwi.ru] XSS at auth?login= (https://hackerone.com/reports/35413)
QIWI (https://hackerone.com/qiwi)	$200	[static.qiwi.com] XSS proxy.html (https://hackerone.com/reports/35363)
Twitter (https://hackerone.com/twitter)	$140	getting emails of users/removing them from victims account [using typical attack] (https://hackerone.com/reports/35287)
HackerOne (https://hackerone.com/security)	$500	Gain reputation by creating a duplicate of an existing report (https://hackerone.com/reports/35237)
PHP (https://hackerone.com/php)	$2,500	Locale::parseLocale Double Free (https://hackerone.com/reports/35102)
Ian Dunn (https://hackerone.com/iandunn-projects)	-	XSS in Tagregator plugin (https://hackerone.com/reports/35036)
Block.io (https://hackerone.com/blockio)	-	Bypassed or command injection (https://hackerone.com/reports/34917)
Mail.Ru (https://hackerone.com/mailru)	-	Нежелательная информация (https://hackerone.com/reports/34799)
Eobot (https://hackerone.com/eobotcom)	-	IDOR on https://www.eobot.com/paypal (https://hackerone.com/reports/34728)
Twitter (https://hackerone.com/twitter)	$280	XSS via Fabrico Account Name (https://hackerone.com/reports/34725)
Mail.Ru (https://hackerone.com/mailru)	$500	Ошибка фильтрации (https://hackerone.com/reports/34686)
Block.io (https://hackerone.com/blockio)	-	Various Low level Vulnerabilities (https://hackerone.com/reports/34188)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	-	Flash XSS на old.corp.mail.ru (https://hackerone.com/reports/34130)
Block.io (https://hackerone.com/blockio)	$150	SMPT Protection not used, I can hijack your email server. (https://hackerone.com/reports/34112)
Twitter (https://hackerone.com/twitter)	$420	Bad extended ascii handling in HTTP 301 redirects of t.co (https://hackerone.com/reports/34084)
Twitter (https://hackerone.com/twitter)	-	Options Method Enabled (https://hackerone.com/reports/33987)
Twitter (https://hackerone.com/twitter)	-	Option Method Enabled on web server (https://hackerone.com/reports/33986)
HackerOne (https://hackerone.com/security)	$500	File Name Enumeration (https://hackerone.com/reports/33935)
Twitter (https://hackerone.com/twitter)	-	BROKEN AUTHENTICATION IN MOBILE VERIFICATION (https://hackerone.com/reports/33432)
InVision (https://hackerone.com/invision)	-	Password reset tokens is valid after changing the password by logging in the account (https://hackerone.com/reports/33385)
Uzbey (https://hackerone.com/uzbey)	-	test (https://hackerone.com/reports/33358)
Twitter (https://hackerone.com/twitter)	-	Flaw in valid password policy. (https://hackerone.com/reports/33331)
Uzbey (https://hackerone.com/uzbey)	-	Test (https://hackerone.com/reports/33154)
Uzbey (https://hackerone.com/uzbey)	-	Test (https://hackerone.com/reports/33153)
Twitter (https://hackerone.com/twitter)	$1,400	DOM Cross-Site Scripting (XSS) (https://hackerone.com/reports/33091)
InVision (https://hackerone.com/invision)	$300	Backup of wordpress configuration file found. Leaking database users/passwords (https://hackerone.com/reports/33083)
Slack (https://hackerone.com/slack)	$500	a stored xss in slack integration https://onerror.slack.com/services/import (https://hackerone.com/reports/33018)
HackerOne (https://hackerone.com/security)	-	Enumeration/Guess of Private (Invited) Programs (https://hackerone.com/reports/32990)
WP API (https://hackerone.com/wp-api)	-	MD5 used for Key-Auth signatures (https://hackerone.com/reports/32944)

Team	Bounty	Title
Twitter (https://hackerone.com/twitter)	$1,680	URGENT - Subdomain Takeover on media.vine.co due to unclaimed domain pointing to AWS (https://hackerone.com/reports/32825)
99designs (https://hackerone.com/99designs)	-	Source Code Disclosure (PHP) (https://hackerone.com/reports/32632)
Mail.Ru (https://hackerone.com/mailru)	$200	OpenSSL HeartBleed (CVE-2014-0160) (https://hackerone.com/reports/32570)
Twitter (https://hackerone.com/twitter)	$280	XSS in fabric.io (https://hackerone.com/reports/32519)
HackerOne (https://hackerone.com/security)	-	Content Spoofing via reports (https://hackerone.com/reports/32137)
The Internet (https://hackerone.com/internet) ★	$3,000	Drupal 7 pre auth sql injection and remote code execution (https://hackerone.com/reports/31756)
Twitter (https://hackerone.com/twitter)	$140	Singup Page HTML Injection Vulnerability (https://hackerone.com/reports/31554)
Mail.Ru (https://hackerone.com/mailru)	-	Авторизуюсь от имени любого пользователя parapa.mail.ru (https://hackerone.com/reports/31418)
RelateIQ (https://hackerone.com/relateiq)	$500	PoodleBleed (https://hackerone.com/reports/31415)
Flash (https://hackerone.com/flash)	$5,000	Adobe Flash Player Out-of-Bound Read/Write Vulnerability (https://hackerone.com/reports/31408)
HackerOne (https://hackerone.com/security)	$1,000	Ability to see common response titles of other teams (limited) (https://hackerone.com/reports/31383)
Localize (https://hackerone.com/localize)	-	files likes of README.md is public (https://hackerone.com/reports/31255)
Twitter (https://hackerone.com/twitter)	-	Creating Unauthorized Audience Lists (https://hackerone.com/reports/31188)
concrete5 (https://hackerone.com/concrete5)	-	Weak random number generator used in concrete/authentication/concrete/controller.php (https://hackerone.com/reports/31171)
WP API (https://hackerone.com/wp-api)	$50	Cryptographic Side Channel in OAuth Library (https://hackerone.com/reports/31168)
joola.io (https://hackerone.com/joola-io)	-	Timing Attack Side-Channel on API Token Verification (https://hackerone.com/reports/31167)

Team	Bounty	Title
joola.io (https://hackerone.com/joola-io)	-	Weak Random Number Generator for Auth Tokens (https://hackerone.com/reports/31166)
Twitter (https://hackerone.com/twitter)	$420	Unauthorized Tweeting on behalf of Account Owners (https://hackerone.com/reports/31082)
Khan Academy (https://hackerone.com/khanacademy)	-	Sql injection And XSS (https://hackerone.com/reports/31023)
Twitter (https://hackerone.com/twitter)	$560	Improper Verification of email address while saving Account Settings (https://hackerone.com/reports/30975)
RelateIQ (https://hackerone.com/relateiq)	$250	Relateiq SSLv3 deprecated protocol vulnerability. (https://hackerone.com/reports/30852)
Localize (https://hackerone.com/localize)	-	PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings. (https://hackerone.com/reports/30787)
Bookfresh (https://hackerone.com/bookfresh)	-	Missing Function Level Access Control in /cindex.php/widget/customize/ (https://hackerone.com/reports/30575)
Flash (https://hackerone.com/flash)	$2,000	Adobe Flash Player MP4 Use-After-Free Vulnerability (https://hackerone.com/reports/30567)
Coinbase (https://hackerone.com/coinbase)	$100	New Device confirmation tokens are not properly validated. (https://hackerone.com/reports/30238)
99designs (https://hackerone.com/99designs)	-	CSRF to connect attacker's twitter account to logged in victims account (https://hackerone.com/reports/30142)
concrete5 (https://hackerone.com/concrete5)	-	Stored XSS in concrete5 5.7.0.4. (https://hackerone.com/reports/30019)
Square (https://hackerone.com/square)	$250	CSRF on adding a calendar event (https://hackerone.com/reports/30015)
Square (https://hackerone.com/square)	$500	square google calendar integration CSRF,https://squareup.com/appointments/business/settings(state parameter not checking properly) (https://hackerone.com/reports/30011)
Mail.Ru (https://hackerone.com/mailru)	-	Выполнение кода PHP через FastCGI (https://hackerone.com/reports/30008)
Square (https://hackerone.com/square)	$500	CSRF on adding clients (https://hackerone.com/reports/30004)

Team	Bounty	Title
The Internet (https://hackerone.com/internet) ★	$20,000	GNU Bourne-Again Shell (Bash) 'Shellshock' Vulnerability (https://hackerone.com/reports/29839)
Twitter (https://hackerone.com/twitter)	$280	Profile Pic padding (Length-hiding) fails due to use of GZIP (https://hackerone.com/reports/29835)
HackerOne (https://hackerone.com/security)	$500	homograph attack. IDNs displayed in unicode in bug reports and on external link warning page (https://hackerone.com/reports/29491)
IRCCloud (https://hackerone.com/irccloud)	$300	Unvalidated Channel names causes IRC Command Injection (https://hackerone.com/reports/29480)
Square (https://hackerone.com/square)	$250	Privilege Escalation (https://hackerone.com/reports/29471)
WePay (https://hackerone.com/wepay)	$350	Horizontal Privilege Escalation (https://hackerone.com/reports/29420)
Twitter (https://hackerone.com/twitter)	$1,120	XSS platform.twitter.com | video-js metadata (https://hackerone.com/reports/29360)
HackerOne (https://hackerone.com/security)	$500	No email verification on username change (https://hackerone.com/reports/29331)
Twitter (https://hackerone.com/twitter)	$1,120	XSS platform.twitter.com (https://hackerone.com/reports/29328)
Sucuri (https://hackerone.com/sucuri)	$250	Usage of HTTP for exporting graph data as images (https://hackerone.com/reports/29288)
Square (https://hackerone.com/square)	$250	Redirect while opening link in new tabs (https://hackerone.com/reports/29263)
Coinbase (https://hackerone.com/coinbase)	$100	Credit Card Validation Issue (https://hackerone.com/reports/29234)
Twitter (https://hackerone.com/twitter)	-	Twitter Flight SSL 2.0 deprecated protocol vulnerability. (https://hackerone.com/reports/29206)
HackerOne (https://hackerone.com/security)	-	"early preview" programs disclosure (https://hackerone.com/reports/29185)
HackerOne (https://hackerone.com/security)	$500	Redirect FILTER bypass in report/comment (https://hackerone.com/reports/28865)
Mail.Ru (https://hackerone.com/mailru)	$500	touch.mail.ru XSS via message id (https://hackerone.com/reports/28832)

Team	Bounty	Title
Phabricator (https://hackerone.com/phabricator)	-	Content Spoofing through URL (https://hackerone.com/reports/28792)
IRCCloud (https://hackerone.com/irccloud)	-	Weak password policy (https://hackerone.com/reports/28703)
Mavenlink (https://hackerone.com/mavenlink)	-	Email field filtering problem. (https://hackerone.com/reports/28632)
Twitter (https://hackerone.com/twitter)	$420	iOS App can establish Facetime calls without user's permission (https://hackerone.com/reports/28500)
Ruby on Rails (https://hackerone.com/rails)	$1,500	Active Record SQL Injection Vulnerability Affecting PostgreSQL (https://hackerone.com/reports/28450) **CVE-2014-3483** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3483)
Ruby on Rails (https://hackerone.com/rails)	$1,500	Active Record SQL Injection Vulnerability Affecting PostgreSQL (https://hackerone.com/reports/28449) **CVE-2014-3482** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3482)
PHP (https://hackerone.com/php)	$2,500	SPL ArrayObject/SPLObjectStorage Unserialization Type Confusion Vulnerabilities (https://hackerone.com/reports/28445) **CVE-2014-3515** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3515)
Twitter (https://hackerone.com/twitter)	$1,400	Cross site scripting on ads.twitter.com (https://hackerone.com/reports/28150)
HackerOne (https://hackerone.com/security)	$500	Window Opener Property Bug (https://hackerone.com/reports/27987)
Twitter (https://hackerone.com/twitter)	$1,400	Stored xss (https://hackerone.com/reports/27846)
Square (https://hackerone.com/square)	$2,000	malicious file upload (https://hackerone.com/reports/27704)
Flash (https://hackerone.com/flash)	$1,000	Flash Local Sandbox Bypass (https://hackerone.com/reports/27651) **CVE-2014-0554** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0554)
GlassWire (https://hackerone.com/glasswire)	-	Clickjacking: X-Frame-Options header missing (https://hackerone.com/reports/27594)
Phabricator (https://hackerone.com/phabricator)	-	Content spoofing (https://hackerone.com/reports/27564)

Team	Bounty	Title
Twitter (https://hackerone.com/twitter)	$1,400	ads.twitter.com xss (https://hackerone.com/reports/27511)
Square (https://hackerone.com/square)	$400	Reflected XSS in widget script thru cookie (https://hackerone.com/reports/27468)
Twitter (https://hackerone.com/twitter)	$2,800	Delete Credit Cards from any Twitter Account in ads.twitter.com [New Vulnerability] (https://hackerone.com/reports/27404)
Square (https://hackerone.com/square)	$1,000	Reflected XSS in connect.square.com (https://hackerone.com/reports/27389)
Square (https://hackerone.com/square)	$750	Editing Client Details of other People (https://hackerone.com/reports/27357)
Twitter (https://hackerone.com/twitter)	$140	Missing Rate Limiting on https://twitter.com/account/complete (https://hackerone.com/reports/27166)
The Internet (https://hackerone.com/internet) ★	$3,000	open redirect in rfc6749 (https://hackerone.com/reports/26962)
Mail.Ru (https://hackerone.com/mailru)	$1,337	XSS via .eml file (https://hackerone.com/reports/26935)
WePay (https://hackerone.com/wepay)	$350	Critical : Account removing using CSRF attack (https://hackerone.com/reports/26866)
Square (https://hackerone.com/square)	-	XSS on bookfresh (https://hackerone.com/reports/26857)
Twitter (https://hackerone.com/twitter)	$140	Full path disclosure at ads.twitter.com (https://hackerone.com/reports/26825)
Slack (https://hackerone.com/slack)	-	HTTP Strict Transport Policy not enabled on newly made accounts (https://hackerone.com/reports/26763)
Phabricator (https://hackerone.com/phabricator)	-	Password Policy issue (https://hackerone.com/reports/26758)
Square (https://hackerone.com/square)	$2,000	CRITICAL Account takeover via AngularJS template injection in connect.squareup.com (https://hackerone.com/reports/26700)
Django (https://hackerone.com/django)	$1,000	CSRF protection bypass on any Django powered site via Google Analytics (https://hackerone.com/reports/26647)
Square (https://hackerone.com/square)	$500	XSS in Client Past Activity (https://hackerone.com/reports/26527)

Team	Bounty	Title
ExpressionEngine (https://hackerone.com/expressionengine)	-	Stored Cross-Site Scripting Vulnerability in /admin.php?/cp/admin_system/general_configuration (https://hackerone.com/reports/26482)
HackerOne (https://hackerone.com/security)	-	Notification of previous signed out user leakage. (https://hackerone.com/reports/26395)
Mavenlink (https://hackerone.com/mavenlink)	-	DNS load balancing not enabled (https://hackerone.com/reports/26181)
WePay (https://hackerone.com/wepay)	-	CSRF (Make email primary) may lead to account compromise (https://hackerone.com/reports/25405)
CloudFlare (https://hackerone.com/cloudflare)	-	Apache mod_negotiation filename bruteforcing (https://hackerone.com/reports/25382)
Square (https://hackerone.com/square)	$250	Open Redirect [FreshBook] (https://hackerone.com/reports/25334)
Square (https://hackerone.com/square)	$500	XSS [BookFresh] (https://hackerone.com/reports/25332)
HackerOne (https://hackerone.com/security)	$100	Change Any username and profile link in hackerone (https://hackerone.com/reports/25281)
Greenhouse.io (https://hackerone.com/greenhouse)	-	[greenhouse.io] CRLF Injection / Insecure nginx configuration (https://hackerone.com/reports/25275)
CloudFlare (https://hackerone.com/cloudflare)	-	User can request for password reset link without giving his website, eventhough he have it (https://hackerone.com/reports/25270)
Greenhouse.io (https://hackerone.com/greenhouse)	-	SMTP protection not used (please read carefully) (https://hackerone.com/reports/25191)
Phabricator (https://hackerone.com/phabricator)	$400	Open redirection on secure.phabricator.com (https://hackerone.com/reports/25160)
Twitter (https://hackerone.com/twitter)	-	HTML form without CSRF protection at http://try.crashlytics.com/enterprise/ (https://hackerone.com/reports/25128)
Greenhouse.io (https://hackerone.com/greenhouse)	-	openssh-server Forced Command Handling Information Disclosure Vulnerability on blog.greenhouse.io (https://hackerone.com/reports/24984)
Factor.io (https://hackerone.com/factor)	-	Reflected XSS - factor.io (https://hackerone.com/reports/24579)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	-	Не уверен, что этому место на периметре: 94.100.180.95, 94.100.180.96, 94.100.180.97, 94.100.180.98 (https://hackerone.com/reports/24183)
concrete5 (https://hackerone.com/concrete5)	-	broken authentication (https://hackerone.com/reports/23921)
Twitter (https://hackerone.com/twitter)	-	User's DM won't deleted after logout from Twitter for iOS (com.atebits.xxx.application-state) (https://hackerone.com/reports/23913)
Mail.Ru (https://hackerone.com/mailru)	$150	money.mail.ru: Странное поведение SMS (https://hackerone.com/reports/23852)
Secret (https://hackerone.com/secret)	-	Broken Authentication and Session Management (https://hackerone.com/reports/23579)
Mail.Ru (https://hackerone.com/mailru)	-	Version Disclosure (NginX) (https://hackerone.com/reports/23447)
HackerOne (https://hackerone.com/security)	$500	Redirect while opening links in new tabs (https://hackerone.com/reports/23386)
Phabricator (https://hackerone.com/phabricator)	$300	Forgot Password Issue (https://hackerone.com/reports/23363)
Square (https://hackerone.com/square)	-	CSRF login (https://hackerone.com/reports/23150)
Square (https://hackerone.com/square)	$1,500	Blind SQL injection in www.bookfresh.com (https://hackerone.com/reports/23098)
Uzbey (https://hackerone.com/uzbey)	-	SQL Injection (https://hackerone.com/reports/23014)
Uzbey (https://hackerone.com/uzbey)	-	XSS in 3rd party plugin (not affecting Uzbey's users) (https://hackerone.com/reports/23010)
Phabricator (https://hackerone.com/phabricator)	-	Password Reset Links Not Expiring (https://hackerone.com/reports/22858)
Twitter (https://hackerone.com/twitter)	-	Broken authentication and invalidated email address leads to account takeover (https://hackerone.com/reports/22203)
Automattic (https://hackerone.com/automattic)	-	Open Redirect in WordPress Feed Statistics {Affected All Versions} (https://hackerone.com/reports/22142)

Team	Bounty	Title
Slack (https://hackerone.com/slack)	$200	Content Spoofing all Integrations in https://team.slack.com/services/new/ (https://hackerone.com/reports/22093)
Twitter (https://hackerone.com/twitter)	-	Password reset link not validated. (https://hackerone.com/reports/22012)
Yahoo! (https://hackerone.com/yahoo)	-	caesary.yahoo.net Blind Sql Injection (https://hackerone.com/reports/21899)
IRCCloud (https://hackerone.com/irccloud)	-	Bruteforce protection not enabled on the login page https://www.irccloud.com/ (https://hackerone.com/reports/21603)
Slack (https://hackerone.com/slack)	$100	Content spoofing at Stripe Integrations (https://hackerone.com/reports/21248)
Mavenlink (https://hackerone.com/mavenlink)	$50	privilege escalation (https://hackerone.com/reports/21210)
Mavenlink (https://hackerone.com/mavenlink)	$200	Flash XSS on swfupload.swf showing at app.mavenlink.com (https://hackerone.com/reports/21150)
Mavenlink (https://hackerone.com/mavenlink)	$50	Clickjacking (https://hackerone.com/reports/21110)
HackerOne (https://hackerone.com/security)	-	Account Hijacking (Only rare case scenario) (https://hackerone.com/reports/21083)
Mavenlink (https://hackerone.com/mavenlink)	$100	Login CSRF (https://hackerone.com/reports/21069)
Phabricator (https://hackerone.com/phabricator)	-	Back - Refresh - Attack To Obtain User Credentials (https://hackerone.com/reports/21064)
Coinbase (https://hackerone.com/coinbase)	$1,000	Invoice Details activate JS that filled in (https://hackerone.com/reports/21034)
The Internet (https://hackerone.com/internet) ★	$3,000	rsync hash collisions may allow an attacker to corrupt or modify files (https://hackerone.com/reports/20873)
Apache httpd (https://hackerone.com/apache)	$500	moderate: mod_deflate denial of service (https://hackerone.com/reports/20861) **CVE-2014-0118** (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0118)

Team	Bounty	Title
Mail.Ru (https://hackerone.com/mailru)	$150	cloud.mail.ru: File upload XSS using Content-Type header (https://hackerone.com/reports/20720)
Python (https://hackerone.com/python)	$1,500	integer overflow in 'buffer' type allows reading memory (https://hackerone.com/reports/20671)
WePay (https://hackerone.com/wepay)	-	oauth redirect uri validation bug leads to open redirect and account compromise (https://hackerone.com/reports/20661)
Mail.Ru (https://hackerone.com/mailru)	$1,000	e.mail.ru: File upload "Chapito" circus (https://hackerone.com/reports/20616)
Mail.Ru (https://hackerone.com/mailru)	-	files.mail.ru: HTTP Header Injection (https://hackerone.com/reports/20400)
Mail.Ru (https://hackerone.com/mailru)	$100	m.agent.mail.ru: Подделываем j2me app-descriptor (https://hackerone.com/reports/20391)
DigitalSellz (https://hackerone.com/digitalsellz)	-	USER Account is not being deleted after user "Delete Account" from DASHBOARD (https://hackerone.com/reports/20305)
DigitalSellz (https://hackerone.com/digitalsellz)	-	Verbose SQL error messages (https://hackerone.com/reports/20279)
ExpressionEngine (https://hackerone.com/expressionengine)	-	Cross Site Scripting (Stored) (https://hackerone.com/reports/20221)
HackerOne (https://hackerone.com/security)	-	No option to logout concurrent sessions (https://hackerone.com/reports/20122)
Twitter (https://hackerone.com/twitter)	-	password sent over HTTP (https://hackerone.com/reports/20081)
Automattic (https://hackerone.com/automattic)	-	Missing HSTS header in https://app.simplenote.com (https://hackerone.com/reports/20072)
Automattic (https://hackerone.com/automattic)	-	Missing HSTS header in https://public-api.wordpress.com (https://hackerone.com/reports/20071)
RelateIQ (https://hackerone.com/relateiq)	$100	Cross-site Scripting in mailing (username) (https://hackerone.com/reports/20049)
Envoy (https://hackerone.com/envoy)	-	Authentication Bypass (https://hackerone.com/reports/20044)
Coin.co (https://hackerone.com/coinco)	-	Host header is not Validated resulting in Redirect (https://hackerone.com/reports/19948)