Twitter Recap #1 – Bug Bounty Tips by the Intigriti Community

BY INTIGRITI · FEBRUARY 24, 2020 · LAST UPDATED ON MARCH 6, 2025

Bug Bounty Tips

Over the past years we have shared a lot of tips to help our readers in one way or another. Thinking outside the box or trying a different approach could be the defining factor in finding that one juicy bug!

We dove deep into our archives and made a list out of all the Bug Bounty tips we posted up untill this point. Here is a summary.

Index

    - Bypass JWT Signature
    - 403 Forbidden Bypass
    - Bypass Paywalls
    - Bypass Firewalls
    - Send Back Responses
    - From False to True
- Business Logic
    - Focus on Impact
    - The Birthday Trick
    - Skipping Steps
    - The Coupon Trick
- Informative
    - Asking Questions
    - XSS Passwords

Recon

The way you perform your reconnaissance is what differentiates you from other hackers. Here are some tips to step up your recon game!

Copyright Footer

> "Simple but effective recon tip from @_zulln: Google the © to discover more assets! #BugBountyTip #HackWithIntigriti pic.twitter.com/H1CQlwr2pn
>
> — Intigriti (@intigriti) March 20, 2019"

Company Owned Domains

> "Start your weekend & your recon with this #BugBountyTip from @hacker_! But remember... always stay in-scope! #HackWithIntigriti pic.twitter.com/vFhJoqCy4A
>
> — Intigriti (@intigriti) April 19, 2019"

Company Resources

> "Doing recon? Don't forget the company resources! Slides, tutorials and other examples often contain a lot of juicy information! Thanks for the #BugBountyTip, @Alyssa_Herrera_! #HackWithIntigriti pic.twitter.com/CT1UYBZefH
>
> — Intigriti (@intigriti) August 9, 2019"

Webinars

> "Thanks for the #BugBountyTip, @securinti! #HackWithIntigriti
> (P.S.: You are now banned from our live webinars) pic.twitter.com/z8Cz3rAUgS
>
> — Intigriti (@intigriti) August 30, 2019"

OpenSSL for Recon

> “Did you know you can use OpenSSL for recon purposes?
> Thanks for the #BugBountyTip, @michael1026h1! pic.twitter.com/mRraH8cK2z
>
> — Intigriti (@intigriti) December 9, 2019”

Deleted Accounts Recon

> “Did you know you can sometimes retrieve data from 'deleted' accounts, by signing up with the e-mail that was associated to it? Another good example of why e-mail verification matters. Thanks for the tip, @StijnJans! #HackWithIntigriti #BugBounty #BugBountyTip pic.twitter.com/DSMf4qKCnq
>
> — Intigriti (@intigriti) January 3, 2019”

Premium Features

> “Earn a €1000 bounty? Save €100 to purchase premium features in bounty programs. According to @vdeschutter, it often results in more bounties! Now that’s what we call a good investment! #BugBountyTip #HackWithIntigriti pic.twitter.com/wh5Pfx5oxm
>
> — Intigriti (@intigriti) January 24, 2019”

E-mail Template Injection

> “Have you ever checked the text version of a HTML e-mail for template injection? Always make sure to inspect the original e-mail source for hidden treasures . Thanks for the #BugBountyTip, @honoki! #HackWithIntigriti pic.twitter.com/nJG4qDnQFS
>
> — Intigriti (@intigriti) March 7, 2019”

RTFM

> “.@KarimPwnz bug bounty tip for today: RTFM! #BugBountyTip #HackWithIntigriti pic.twitter.com/kkDoIAmknW
>
> — Intigriti (@intigriti) April 18, 2019”

Rails Application Testing

> “Testing a Ruby on Rails app? Add .json to the URL and see what happens!
> Thanks for the #BugBountyTip, @yaworsk! pic.twitter.com/oHlHilQtr7
>
> — Intigriti (@intigriti) September 26, 2019”

API Endpoints Recon

> “Looking for API endpoints? OPTIONS to the rescue! Thanks for the tip, @dewolfrobin! #BugBounty #HackWithIntigriti pic.twitter.com/nF0IWxaH54
>
> — Intigriti (@intigriti) December 6, 2018”

Tools

There are lots and lots of security tools out there, these are the ones we tried throughout the years. The might me worth your time looking into!

Objection

> “Mobile hackers, check out this awesome tool recommended by @skeltavik! #BugBounty #HackWithIntigriti https://t.co/bPMn0ijxcl pic.twitter.com/8I0VC2kobg
>
> — Intigriti (@intigriti) December 20, 2018”

EyeWitness

> “Instead of looking through 100's of screenshots, sort them by file size to get to the juicy stuff right away. Thanks for the tip, @stokfredrik! #BugBountyTip #HackwithIntigriti #bugbounty pic.twitter.com/VuyEKmBIjx
>
> — Intigriti (@intigriti) March 28, 2019”

Apktool

> “This is @lucio_89. Lucio scores a lot of bounties just by looking inside APK's and extracting secrets with apktool. Be like Lucio, and #HackWithIntigriti. pic.twitter.com/Bep22V1Zku
>
> — Intigriti (@intigriti) February 14, 2019”

FileChangeMonitor

> “Did you know you can use FileChangeMonitor by @jackhcable to monitor JavaScript files and discover endpoints when they're added? Check out https://t.co/jN2bFPapDT #HackWithIntigriti pic.twitter.com/ApUFBpmGi8
>
> — Intigriti (@intigriti) May 1, 2019”

Exiftool

> “A PDF file can tell more than you think! Great advice from @QuintenBombeke! #BugBountyTip #HackWithIntigriti #BugBounty pic.twitter.com/73ZTUWlH0O
>
> — Intigriti (@intigriti) May 9, 2019”

Cloud_Enum

> “Open your eyes and see: there is more than S3! @hussein98d recommends cloud_enum to find unprotected Google Cloud buckets and Microsoft Azure storage accounts! #BugBountyTip https://t.co/jdufh0L7fR pic.twitter.com/OqRtTIanb5
>
> — Intigriti (@intigriti) September 23, 2019”

Security_Trails

> “One bug does not mean one bounty! Maximise your using https://t.co/1RdjyFImaB, thanks to this excellent tip from @emgeekboy! #HackWithIntigriti pic.twitter.com/oteW6sGpgZ
>
> — Intigriti (@intigriti) October 19, 2019”

Payloads

Sometimes you feel like you are close to finding something but you are not quite there yet. It could be a matter of executing the right payload in the right place. The next example might help you in the right direction.

XSS in Parameter Names

> “ Looking for XSS? Don't forget the parameter names! Thanks for the #BugBountyTip, @p4fg! #HackWithIntigriti pic.twitter.com/VsFLtVFJRm
>
> — Intigriti (@intigriti) September 20, 2019”

Youtube XSS

> “This also works for other embedded services (vimeo, dailymotion, twitter, facebook...)! Thanks for the #BugBountyTip, @ L i v e O v e r f l o w @EdOverflow! pic.twitter.com/bAE0snqYcZ
>
> — Intigriti (@intigriti) January 9, 2020”

XSS with htmlentities()

> “So you thought htmlentities() always protects against XSS?
> x54x68x69x6ex6bx20x61x67x61x69x6ex21! Thanks for the #BugBountyTip, @karel_origin!
> #HackWithIntigriti pic.twitter.com/0TaQcSZKok
>
> — Intigriti (@intigriti) May 19, 2019”

Hidden GET and POST Parameters

> “Bug bounty tip: Always be on the lookout for hidden GET and POST parameters, especially on pages with HTML forms.
> Thanks for the #BugBountyTip, @Kuromatae666! #HackWithIntigriti pic.twitter.com/eyBkK1uesd
>
> — Intigriti (@intigriti) June 3, 2019”

Payloads in E-mail Address

> “Did you know you can smuggle payloads in a valid e-mail address using round brackets? Thanks for the tip, @securinti! #BugBounty #HackWithIntigriti pic.twitter.com/i1OMbzjBfl
>
> — Intigriti (@intigriti) December 27, 2018”

X-Forwarded-For Headers

> “The X-Forwarded-For header turns out to be a perfect place to hide your blind XSS or SQL injection payloads, according to @_zulln. Thanks for the tip, Linus! #BugBountyTip #HackWithIntigriti pic.twitter.com/qeGYNwlPnj
>
> — Intigriti (@intigriti) February 7, 2019”

Long String Parameters

> “The best way to cause errors exposing sensitive information?
> Long strings in POST parameters (50.000+ characters)
> Using the 'Euler number' (e) in numbers to gain exponentially large values
> Thanks for the #BugBountyTip, @pxmme1337! pic.twitter.com/gPJ37I6o7z
>
> — Intigriti (@intigriti) October 24, 2019”

Hidden Wildcarts

> “Sometimes, one character is all you need! Use % as a wildcard for codes, booking references or even SSN's!
> Awesome #BugBountyTip, @itscachemoney! pic.twitter.com/bDPq2uINaF
>
> — Intigriti (@intigriti) October 25, 2019”

Fuzz Non-Printable Characters

> “Want to find 'cosmic brain' bugs, just like @0xACB and @samwcyo?
> Use the following 'invisible' ranges in your payloads #BugBountyTip
> 0x00 0x2F
> 0x3A 0x40
> 0x5B 0x60
> 0x7B 0xFF pic.twitter.com/B2WlljEJXu
>
> — Intigriti (@intigriti) October 18, 2019”

JSONp Callback

> “When adding one parameter to an endpoint can earn you thousands of . Thanks for the tip, @inhibitor181! #HackWithIntigriti #BugBountyTip pic.twitter.com/jBTrU090sU
>
> — Intigriti (@intigriti) January 10, 2019”

XSS in API

> “Bug bounty tip: if none of your XSS payloads are firing – try to insert them through the API! #BugBountyTip #HackWithIntigriti pic.twitter.com/HpAUhMqFfx
>
> — Intigriti (@intigriti) April 4, 2019”

XSS in MathJax or KaTeX

> “Just testing if Twitter is vulnerable: url{javascript:alert(1)}. Thanks for the #BugBountyTip, @EdOverflow ! #HackWithIntigriti pic.twitter.com/T9gbx9kfSq
>
> — Intigriti (@intigriti) March 1, 2019”

Authentication & Authorization

Many problems reside in the authentication and authorization process. These vulnerabilities cause huge security risks for company’s so your reports wil gladly be received. With these tips you will be sure to find more of them.

UUID IDOR Trick

> “So you believe UUID's are a sufficient protection against IDOR's?
> Think again! Thanks for the #BugBountyTip, @securinti pic.twitter.com/zx5Xn7iDrE
>
> — Intigriti (@intigriti) January 16, 2020”

Username Takeover

> “Time for a fresh #BugBountyTip from @EdOverflow: change your username to cause namespace collisions and see what happens! Read more: https://t.co/iEDKRjrwDq #HackWithIntigriti pic.twitter.com/SKiSnkampQ
>
> — Intigriti (@intigriti) May 16, 2019”

Swapping Tokens

> “Excellent #BugBountyTip from XSS wizard @filedescriptor: got XSS without access to the cookies or CSRF tokens? Try swapping the victim's CSRF token with yours – it often works and results in a higher impact and bounty! #HackWithIntigriti pic.twitter.com/t7Gcw34afG
>
> — Intigriti (@intigriti) June 12, 2019”

Leaked Slack Tokens

> “Tip of the day: check for exposed Slack tokens using @streaak's #BugBountyTip and find out if hackers could have been snooping on your Slack conversations. pic.twitter.com/jh41qZJkgb
>
> — Intigriti (@intigriti) July 31, 2019”

Facebook Account Takeover Vulnerabilities

> “According to @itscachemoney, this sometimes leads to account takeover vulnerabilities. #BugBountyTip #HackWithIntigriti pic.twitter.com/jQ84SF3tdq
>
> — Intigriti (@intigriti) August 5, 2019”

Hidden OAuth Providers

> “This actually worked on the first site we tested!
> P.S.: Legacy or unimplemented OAuth flows often contain vulnerabilities that can lead to account takeover. Thanks for the #BugBountyTip, @ngalongc! pic.twitter.com/vwAi9hhHrm
>
> — Intigriti (@intigriti) September 16, 2019”

Change Request Method

> “Can't get CSRF with POST? Then GET it!
> Use 'change request method' in Burp Suite to check if the server also accepts GET requests. Thanks for the #BugBountyTip, @spaceraccoonsec! #HackWithIntigriti pic.twitter.com/YVRPwZD6L0
>
> — Intigriti (@intigriti) October 3, 2019”

JWT Account Takeover

> “ Open staging environments can lead to production account takeover
> If they use a separate DB, but same JWT secret
> If the username or e-mail address is used as identifier
> This is an excellent #BugBountyTip, thanks @kapytein! pic.twitter.com/yZkBoDBO1d
>
> — Intigriti (@intigriti) December 4, 2019”

Extract AWS S3 Bucket Name

> “Did you know you can extract the AWS S3 bucket name from an object URL by appending these parameters? Thanks for the #BugBountyTip, @neeraj_sonaniya! #HackWithIntigriti pic.twitter.com/cfVpRpOw1s
>
> — Intigriti (@intigriti) September 4, 2019”

Support Subdomain Takeover

> “Cool support desk subdomain takeover trick by @rootxharsh , always check the MX records! #HackWithIntigriti pic.twitter.com/HIYTuQ1MS5
>
> — Intigriti (@intigriti) November 1, 2019”

Bypasses

You find yourself getting stuck against some type of wall while hunting? No worries! The next tips might help you get past them.

Bypass JWT Signature

> “ Are you signing your JWT tokens? Good...unless hackers can change the signing algorithm to . Make sure to check this, or @yassineaboukir will do it for you and claim yet another #BugBounty! #BugBountyTip #HackWithIntigriti pic.twitter.com/1sW1B766Qi
>
> — Intigriti (@intigriti) February 13, 2020”

403 Forbidden Bypass

> “Some #bugbounty hunters made over €50.000 in bug bounties with this simple trick. Thanks for the #BugBountyTip, @rez0__! pic.twitter.com/z9sPFJTNqV
>
> — Intigriti (@intigriti) January 30, 2020”

Bypass Paywalls

> “Testing a service with a paywall? Try bypassing it by including "Googlebot" in your user agent. Excellent #BugBountyTip by @intidc! #HackWithIntigiti #BugBounty pic.twitter.com/8RBG61mM0L
>
> — Intigriti (@intigriti) November 29, 2018”

Bypass Firewalls

> “Want to bypass an annoying firewall? @vincentcox_be is here to help! Use https://t.co/iak3mu2tuu. #HackWithIntigriti #BugBounty pic.twitter.com/UZ1RTWImnF
>
> — Intigriti (@intigriti) December 13, 2018”

Send Back Responses

> “.@YassineAboukir's #BugBountyTip:
> Check JSON responses for additional properties, and send them back! #HackWithIntigriti pic.twitter.com/qIwEXtV9S8
>
> — Intigriti (@intigriti) November 11, 2019”

From False to True

> “Sometimes, TRUE is all you need . Use @Burp_Suite's match and replace to enable new functionalities in the UI and expand your attack surface! Thanks for the #BugBountyTip, @anshuman_bh! pic.twitter.com/D55uMIl6Sx
>
> — Intigriti (@intigriti) November 6, 2019”

Business Logic

Tired of getting only low or medium bounties? Then you need to hit where it really hurts. Try thinking in the company’s perspective and what is important for them. You will get more money for your work!

Focus on Impact

> “Context is key. Find out what your target cares about to score higher bounties. Great advice from @jackds1986! #BugBountyTip #HackWithIntigriti pic.twitter.com/6syeIMjxrQ
>
> — Intigriti (@intigriti) April 25, 2019”

The Birthday Trick

> “BOUNTY TIP: Get yourself a nice bounty present by buying giftcards with birthday discounts ! Repeat & recycle your gift cards to generate infinite money. Thanks, and happy (real) birthday, @securinti! #BugBountyTip #HackWithIntigriti pic.twitter.com/cY1NcM3J4c
>
> — Intigriti (@intigriti) May 14, 2019”

Skipping Steps

> “Looking for business logic flaws ? Flows with multiple steps are a good place to start. Try to skip steps or execute them in a wrong order and see what happens
> Thanks for the #BugBountyTip, @InsiderPhD! pic.twitter.com/bw6Z28K6fE
>
> — Intigriti (@intigriti) November 7, 2019”

The Coupon Trick

> “ It's also #BlackFriday in #BugBounty land ! Harvest all the coupon codes, try this #BugBountyTip by @quintenvi and score some bounties! pic.twitter.com/mZnQGkOnF3
>
> — Intigriti (@intigriti) November 29, 2019”

Informative

Asking Questions

> “Got a question? Follow @codingo_'s advice to get help faster! #BugBountyTip pic.twitter.com/pkmcXReL9P
>
> — Intigriti (@intigriti) August 7, 2019”

XSS Passwords

> “Want to catch someone snooping plaintext passwords? Follow @quintenvi's advice! #HackWithIntigriti #BugBounty pic.twitter.com/obTxFELITr
>
> — Intigriti (@intigriti) December 10, 2018”