

Blog

[Home](#) > 2020 > February > 24 > bugbountytips > Twitter Recap #1 – Bug Bounty Tips by the Intigriti Community

BUG BOUNTY TIPS

Twitter recap by the intigriti community

Powered by



1

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

BUG BOUNTY TIPS

Twitter recap by the intigriti community

Powered by



1

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

- **Recon**
 - Copyright Footer
 - Company Owned Domains
 - Company Resources
 - Webinars
 - OpenSSL Recon
 - Deleted Accouts Recon
 - Premium Features
 - E-mail Template Injection
 - RTFM
 - Rails Application Testing
 - API Endpoints Recon
- **Tools**
 - Objection
 - EyeWitness
 - Apktool
 - FileChangeMonitor
 - Exiftool
 - Cloud_Enum
 - SecurityTrails
- **Payloads**
 - XSS in Parameter Names
 - Youtube XSS

- XSS with htmlentities()
- Hidden GET and POST Parameters
- Payloads in E-mail Address
- X-Forwarded-For Headers
- Long String POST Parameters
- Hidden Wildcards
- Fuzz Non-Printable Characters
- JSONP Callback
- XSS in API
- XSS in Mathjax or KaTex
- **Authentication & Authorization**
 - UUID IDOR Trick
 - Username Takeover
 - Swapping Tokens
 - Leaked Slack Tokens
 - Facebook Account Takeover Vulnerabilities
 - Hidden OAuth Providers
 - Change Request Method
 - JWT Account Takeover
 - Extract AWS S3 Bucket Name
 - Support Subdomain Takeover
- **Bypasses**
 - 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



INTIGRITI
@intigriti



Simple but effective recon tip from [@_zulln](#): Google the © to discover more assets! [#BugBountyTip](#) [#HackWithIntigriti](#)

BUG BOUNTY TIP

“Google the copyright footer

151 1:52 PM - Mar 20, 2019



57 people are talking about this



Company Owned Domains



INTIGRITI
@intigriti



Start your weekend & your recon with this #BugBountyTip from @hacker_! But remember... always stay in-scope! 😊
#HackWithIntigriti

BUG BOUNTY TIP

“Want to find more company owned domains? Use [whoxy.com](#) to perform reverse whois lookups with the email used to register the main domain”

Twitter icon @hacker_

 161 10:36 AM - Apr 19, 2019

(i)

 60 people are talking about this

>

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](#)

BUG BOUNTY RECON TIP

Search for **slides**, **docs**,
demos and **video tutorials** by
your target! You'd be surprised
how many innocent examples
contain **juicy endpoints or creds!**

[@Alyssa_Herrera_](#)

 121 12:08 PM - Aug 9, 2019

(i)

 38 people are talking about this

>

Webinars



INTIGRITI
@intigriti



Thanks for the #BugBountyTip, @securinti! #HackWithIntigriti
(P.S.: You are now banned from our live webinars) 🕶🚫

INTI'S BUG BOUNTY TIP

Join webinars!

Instead of ignoring webinar invites from your bug bounty target... [join them](#) and be on the lookout for the sales person's [bookmarks](#), [autofill data](#) and [API keys](#)!



Inbox [Free Webinar] Testing in Continuous Delivery with Lisa Cr...

26 Aug

Inbox Live Webinar | How far is it? About 15 minutes away - in th...

22 Aug

136 2:19 PM - Aug 30, 2019



34 people are talking about this



OpenSSL for Recon



INTIGRITI
@intigriti



Did you know you can use OpenSSL for recon purposes? 🔒 😊

Thanks for the #BugBountyTip, @michael1026h1!

BUG BOUNTY TIP

OpenSSL recon

Use OpenSSL to get certificates of servers.
They contain **valuable info** and **common names** for finding more subdomains!

```
openssl s_client -connect example.com:443  
2>/dev/null | openssl x509 -noout -text
```



@michael1026h1



@michael1026

www.intigriti.com

♡ 222 1:08 PM - Dec 9, 2019



Q 104 people are talking about this



Deleted Accounts Recon



INTIGRITI
@intigriti



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](#)

BUG BOUNTY TIP

Try to recover data from deleted accounts by signing up with the old e-mail address.

@StijnJans

110 2:37 PM - Jan 3, 2019



37 people are talking about this



Premium Features



INTIGRITI
@intigriti



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](#)

BUG BOUNTY TIP

"If a bounty target offers premium features, **buy them** and **test the new endpoints**. Most of the times.



60 4:18 PM - Jan 24, 2019



See INTIGRITI's other Tweets



E-mail Template Injection



INTIGRITI
@intigriti



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

BUG BOUNTY TIP

106 5:15 PM - Mar 7, 2019



46 people are talking about this



RTFM



INTIGRITI
@intigriti



@KarimPwnz bug bounty tip for today: RTFM! 😎📖
#BugBountyTip #HackWithIntigriti

BUG BOUNTY TIP

"RTFM!"

If you're stuck on a bug, read the specs!
Edgecases and obscure features are
often described in the docs.
Read them to score!"

Twitter icon @KarimPwnz



86 11:04 AM - Apr 18, 2019



17 people are talking about this



Rails Application Testing



INTIGRITI
@intigriti



Testing a Ruby on Rails app? Add .json to the URL and see what happens! 😊

Thanks for the #BugBountyTip, @yaworsk! 🙌

@YAWORSK'S BUG BOUNTY TIP

The .json trick

Testing a Rails application?
Append .json to URL endpoints.
This sometimes returns way more sensitive data than it should!



330 11:11 AM - Sep 26, 2019



102 people are talking about this



API Endpoints Recon



INTIGRITI
@intigriti



Looking for API endpoints? OPTIONS to the rescue! Thanks for the tip, [@dewolfrobin!](#) #BugBounty #HackWithIntigriti

BUG BOUNTY TIP



"Try an OPTIONS request on the api root path to see what endpoints exist."

@haywire

55 12:55 PM - Dec 6, 2018 [i](#)

28 people are talking about this >

Tools

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

Objection

 **INTIGRITI**
@intigriti 

Mobile hackers, check out this awesome tool recommended by
[@skeltavik!](#) #BugBounty #HackWithIntigriti

go.intigriti.com/objection

BUG BOUNTY TIP



"Struggling with SSL Pinning or root detection on Android or iOS? Use Objection to easily bypass them."

@skeltavik

65 1:48 PM - Dec 20, 2018 i

19 people are talking about this >

EyeWitness

 **INTIGRITI**
@intigriti Twitter icon

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

BUG BOUNTY TIP

"Got a big scope?
Take screenshots with EyeWitness
and sort them by file size to get
the most out of it."

107 4:13 PM - Mar 28, 2019



44 people are talking about this >



Apktool



INTIGRITI
@intigriti



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 [#HackWithIntigrity](#).

BUG BOUNTY TIP

♡ 86 2:28 PM - Feb 14, 2019



21 people are talking about this



FileChangeMonitor



INTIGRITI
@intigriti



Did you know you can use FileChangeMonitor by [@jackhcable](#) to monitor JavaScript files and discover endpoints when they're added? 🐶 Check out github.com/cablej/FileCh...
[#HackWithIntigriti](#)

BUG BOUNTY TIP

“Use FileChangeMonitor to detect changes in JavaScript files, and get notified when new API endpoints are added.”

[FileChangeMonitor] Update for <https://filechangemonitor.herokuapp.com/testingFile.js> [Inbox]

to me ↗
no-reply@filechangemonitor.io ↗ sendgrid.net

3:09 PM (4 hours ago)

An update has been detected for <https://filechangemonitor.herokuapp.com/testingFile.js>.

Changes to relative urls:

/createAutomationView
/getIssue
/getIssueDetails
/createIssue
/updateIssue

♡ 233 8:20 PM - May 1, 2019



 88 people are talking about this >

Exiftool



A PDF file can tell more than you think! Great advice from
[@QuintenBombeke!](#) #BugBountyTip #HackWithIntigriti #BugBounty

BUG BOUNTY TIP

“Use exiftool to extract
metadata from documents.
It might reveal vulnerable
htmltopdf generators”

[@QuintenBombeke](#)



 130 9:25 PM - May 9, 2019



 48 people are talking about this >

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

👉 go.intigriti.com/cloud_enum

HUSSEIN98D'S BUG BOUNTY TIP

There's more than S3!

While everyone is looking for open S3 buckets, use [cloud_enum](#) to find open [Google Cloud buckets](#) & [Microsoft Azure storage accounts](#)!

https://go.intigriti.com/cloud_enum

263 1:45 PM - Sep 23, 2019



93 people are talking about this >

Security_Trails



One bug does not mean one bounty! Maximise your 💰 using securitytrails.com, thanks to this excellent tip from [@emgeekboy](#)!
🇮🇳 #HackWithIntigriti

GEEKBOY'S BUG BOUNTY TIP

One bug, multiple bounties

Found one vulnerability
in an on-premises app or library?
Use securitytrails.com to find other
hosts with the same bug!

[http://securitytrails.com/list/ip/\\$IP](http://securitytrails.com/list/ip/$IP)
[http://securitytrails.com/list/cname/\\$CNAME](http://securitytrails.com/list/cname/$CNAME)

240 11:46 AM - Oct 19, 2019

77 people are talking about this >

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

P4FG'S BUG BOUNTY TIP

Looking for XSS?

Also inject payloads in the parameter names!

?filter[<script>alert(0)</script>]=true



♡ 269 3:39 PM - Sep 20, 2019



🗨 99 people are talking about this



Youtube XSS



INTIGRITI
@intigriti



This also works for other embedded services (vimeo, dailymotion, twitter, facebook...)! Thanks for the #BugBountyTip, @LiveOverflow @EdOverflow!

BUG BOUNTY TIP

YouTube XSS

Found an app that embeds YouTube videos?
Try to embed YouTube videos with XSS payloads in their title and description.

<https://www.youtube.com/watch?v=2HoM-2UtbfA>
<https://www.youtube.com/watch?v=sNvC5A9ad0I>

♡ 280 1:05 PM - Jan 9, 2020



🗨 78 people are talking about this



XSS with htmlentities()



INTIGRITI
@intigriti



So you thought htmlentities() always protects against XSS?
\x54\x68\x69\x6e\x6b\x20\x61\x67\x61\x69\x6e\x21! Thanks for the
#BugBountyTip, @karel_origin! #HackWithIntigriti

BUG BOUNTY TIP

Use [unicode or hexadecimal](#)

♥ 608 11:21 AM - May 19, 2019 (i)

253 people are talking about this >

Hidden GET and POST Parameters

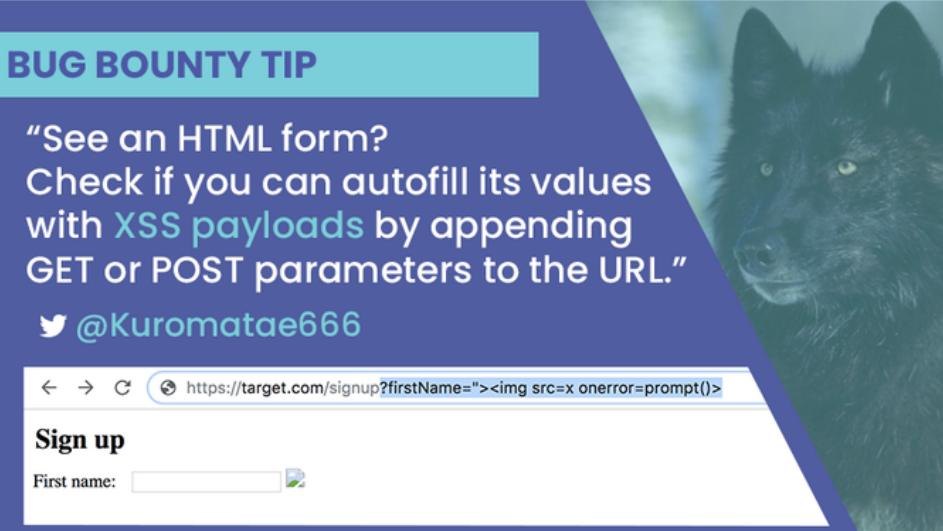
 **INTIGRITI**
@intigriti [!\[\]\(bd2a32f947c5766cd49562c6434da5d4_img.jpg\)](#)

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](#)

BUG BOUNTY TIP

“See an HTML form?
Check if you can autofill its values
with [XSS payloads](#) by appending
GET or POST parameters to the URL.”

 [@Kuromatae666](#)



♥ 179 2:26 PM - Jun 3, 2019 (i)

 61 people are talking about this >

Payloads in E-mail Address



INTIGRITI
@intigriti



Did you know you can smuggle payloads in a valid e-mail address using round brackets? Thanks for the tip, [@securinti!](#) #BugBounty #HackWithIntigriti

BUG BOUNTY TIP

Use round brackets to inject XSS / SQLi / RCE payloads in a **valid** e-mail address.

- ✗ `yourname${}<>'/*-@domain.com`
- ✓ `yourname(${}<>'/*-}@domain.com`
- ✓ `yourname@(${}<>'/*-)domain.com`

@securinti



 663 3:54 PM - Dec 27, 2018 >



 295 people are talking about this >

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

BUG BOUNTY TIP



"Put bXSS and SQLi payloads in x-forwarded-for headers. Almost nobody escapes IP's!"

- Linus Särud, @_zulln

♡ 303 11:17 AM - Feb 7, 2019



› 129 people are talking about this



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!

PXMME1337'S BUG BOUNTY TIP

Go big or go home.

"Large values in POST params may cause verbose (SQL) errors leaking sensitive data, code and even creds!"

String: `AAAAAAAAAA...`

Number: `9e999`

♡ 339 12:44 PM - Oct 24, 2019



130 people are talking about this >

Hidden Wildcards



INTIGRITI
@intigriti



Sometimes, one character is all you need! Use % as a wildcard for codes, booking references or even SSN's! 🎉

Awesome #BugBountyTip, @itscachemoney! 🎉

BUG BOUNTY TIP

Hidden wildcards

Need a last name, SSN or code to lookup data? Use '%'!

% is a wildcard for the SQL LIKE operator and will match all records.

@itscachemoney



199 11:48 AM - Oct 25, 2019



67 people are talking about this



Fuzz Non-Printable Characters



INTIGRITI
@intigriti



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

0xACB'S BUG BOUNTY TIP

From %00 to %FF

Fuzz non-printable characters in any user input! This may result in:

- Regex bypasses (blacklists)
- Account takeover (e-mail, username)

343 11:47 AM - Oct 18, 2019



128 people are talking about this



JSONp Callback



INTIGRITI
@intigriti



When adding one parameter to an endpoint can earn you thousands of 💰. Thanks for the tip, [@inhibitor181!](#)

#HackWithIntigriti #BugBountyTip

BUG BOUNTY TIP

"See an API endpoint displaying sensitive data?



♡ 262 12:58 PM - Jan 10, 2019



🗨 112 people are talking about this



XSS in API



INTIGRITI
@intigriti



Bug bounty tip: if none of your XSS payloads are firing - try to insert them through the API! 😊 #BugBountyTip #HackWithIntigriti

BUG BOUNTY TIP

"Try inserting your payloads through the API instead of the UI. Very often, filters are not present!"

```
{  
  "new_members": [  
    {  
      "member_email": "hunter2@intigriti.me",  
      "member_name": "<script>alert(document.domain)</script>"  
    }  
  ]  
}
```



♡ 212 12:34 PM - Apr 4, 2019



78 people are talking about this >

XSS in MathJax or KaTeX



INTIGRITI
@intigriti



Just testing if Twitter is vulnerable: \url{javascript:alert(1)}. Thanks for the #BugBountyTip, @EdOverflow 🐸! #HackWithIntigriti

BUG BOUNTY TIP

If an application uses MathJax or KaTeX and does not have protocol whitelisting enabled, try using the \href or \url macros to craft XSS payloads.

@EdOverflow

165 3:49 PM - Mar 1, 2019



62 people are talking about this >

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

INTIGRITI
@intigriti

So you believe UUID's are a sufficient protection against IDOR's?
Think again! 🙌 Thanks for the #BugBountyTip, @securinti

BUG BOUNTY TIP

UUID IDOR Trick

Need to find the UUID for a specific user?
Try registering the target username or e-mail!
The response will often include their UUID.

```
{"statusCode": "409",  
 "error": "This user already exists.",  
 "ref": "f2837aea-2d51-11ea-978f-2e728ce88125"}
```

[@securinti](#) [@IntiDC](#) www.intigriti.com

600 1:02 PM - Jan 16, 2020

187 people are talking about this >

Username Takeover



Time for a fresh #BugBountyTip from @EdOverflow: change your username to cause namespace collisions and see what happens!
Read more: go.intigriti.com/usernamespace-... #HackWithIntigriti

BUG BOUNTY TIP

Username takeovers

"When signing up, try to claim a username that collides with existing page namespaces, such as `/login`. This can have unpredictable outcomes.

 @EdOverflow



 212 12:48 PM - May 16, 2019



 71 people are talking about this



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

BUG BOUNTY TIP

Swapping tokens

Got XSS, but no access to cookies or CSRF tokens? Swap the unknown token with yours: just set a cookie with the same name, but a different path.

THIS
IS
AVATAR

Twitter @FileDescriptor

Heart 175 11:01 AM - Jun 12, 2019



Comment 52 people are talking about this



Leaked Slack Tokens



INTIGRITI
@intigriti



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. 🥺

@STREAAK'S BUG BOUNTY TIP

Leaked Slack tokens

Looking for leaked Slack tokens?
Use the [team_id](#) from the [login page](#) in a [GitHub](#) or [BitBucket](#) code search!

[view-source:https://bugbountyforum.slack.com](#)

234 11:55 AM - Jul 31, 2019

84 people are talking about this >



Facebook Account Takeover Vulnerabilities

 INTIGRITI
@intigriti 

According to [@itscachemoney](#), this sometimes leads to account takeover vulnerabilities. 😱#BugBountyTip #HackWithIntigriti

BUG BOUNTY TIP

183 2:26 PM - Aug 5, 2019



68 people are talking about this



Hidden OAuth Providers



INTIGRITI
@intigriti



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!

@NGALONGC'S BUG BOUNTY TIP

Hidden OAuth providers

Try endpoint bruteforcing on the login page to discover hidden or legacy OAuth providers.

/login/facebook
/login/oauth/twitter
/login/oauth/v2/yahoo



♡ 373 11:56 AM - Sep 16, 2019



122 people are talking about this



Change Request Method



INTIGRITI
@intigriti



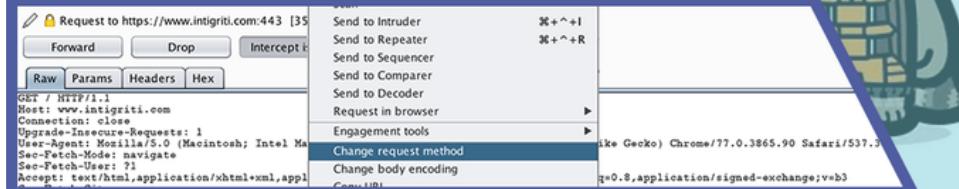
Can't get CSRF with POST? Then GET it!

Use 'change request method' in Burp Suite to check if the server also accepts GET requests. Thanks for the [#BugBountyTip](#),
[@spaceraccoonsec!](#) [#HackWithIntigriti](#)

BUG BOUNTY TIP

Use '[change request method](#)' in Burp Suite to check if the server accepts [GET](#) instead of [POST](#) requests. This is usually vulnerable to [CSRF](#).

[@spaceraccoonsec](#)



♡ 246 2:18 PM - Oct 3, 2019



78 people are talking about this



JWT Account Takeover

 **INTIGRITI**
@intigriti 

⚠ 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!](#)

BUG BOUNTY TIP

JWT Account Takeover

See a staging environment using JWT tokens?

- Create an account for your victim
- Try the victim JWT token on prod

This could result in account takeover!



 @kapytein  @kapytein www.intigriti.com

Heart icon 259 3:47 PM - Dec 4, 2019 

Comment icon 87 people are talking about this 

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

@NEERAJ_SONANIYA'S BUG BOUNTY TIP

You can get an AWS S3 bucket name from an object URL by appending:

?AWSAccessKeyId=[valid-access-key-id]&Expires=2123456789&Signature=

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<?xml version="1.0"?>
<Error>
<Code>SignatureDoesNotMatch</Code>
<Message>
The request signature we calculated does not match the signature you provided. Check your key and
signature.
</Message>
<AWSAccessKeyId>AKIAJ5CJTYWPR5JXNVQQ</AWSAccessKeyId>
<StringToSign>
GET 2123456789/target-img/a.png
</StringToSign>
```

237 12:27 PM - Sep 4, 2019



70 people are talking about this



Support Subdomain Takeover



Cool support desk subdomain takeover trick by @rootxharsh 🇮🇳, always check the MX records! #HackWithIntigriti

ROOTXHARSH BUG BOUNTY TIP

Got support subdomain takeover?
Check if you can receive mails
to support@ to join services like
Slack, Yammer and Quip!

Help Center / My tickets

My tickets

139 1:26 PM - Nov 1, 2019

26 people are talking about this >



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

 **INTIGRITI**
@intigriti 

⚠ Are you signing your JWT tokens? Good...unless hackers can change the signing algorithm to *none*. Make sure to check this, or [@yassineaboukir](#) will do it for you and claim yet another #BugBounty! 😂 #BugBountyTip #HackWithIntigriti

BUG BOUNTY TIP

Bypass JWT signature

Change JWT tokens to bypass privileges!

Decode the token, set the header `alg` to `none`.

Re-encode and leave out the signature (keep the `"."`)

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}  
{  
  "username": "admin"  
}  
<header>.<payload>.<signature>  
  
{  
  "alg": "none",  
  "typ": "JWT"  
}  
{  
  "username": "admin"  
}  
<header>.<payload>.<signature>
```



♡ 431 2:05 PM - Feb 13, 2020



🗨 151 people are talking about this



403 Forbidden Bypass



INTIGRITI
@intigriti



Some [#bugbounty](#) hunters made over €50.000 in bug bounties with this simple trick. 💰 Thanks for the [#BugBountyTip](#), [@rez0__](#)!

BUG BOUNTY TIP

403 Forbidden bypass



1,301 1:06 PM - Jan 30, 2020



506 people are talking about this



INTIGRITI
@intigriti



Testing a service with a paywall? Try bypassing it by including "Googlebot" in your user agent. Excellent #BugBountyTip by @intidc! #HackWithIntigriti #BugBounty

BUG BOUNTY TIP

"You can bypass most paywalls by using a Google Bot user agent"

@intidc



135 11:09 AM - Nov 29, 2018



57 people are talking about this



Bypass Firewalls



INTIGRITI
@intigriti



Want to bypass an annoying firewall? [@vincentcox_be](#) is here to help! Use go.intigriti.com/bypass-firewall.... #HackWithIntigriti
#BugBounty

BUG BOUNTY TIP

"Need to bypass a firewall?
Use [securitytrails.com](#)
to find the originating server IP."

[@vincentcox_be](#)



59 11:53 AM - Dec 13, 2018



30 people are talking about this



Send Back Responses



INTIGRITI
@intigriti



.@YassineAboukir's #BugBountyTip:

Check JSON responses for additional properties, and send them back! 🎉#HackWithIntigriti

BUG BOUNTY TIP

Send back responses!

See object properties in the response but not in the request?

Add them to the request! You may be able to gain control over these properties!

Request:

```
{"id": "7"}  
{"id": "7", "admin": true}
```

Response:

```
{"id": "7", "admin": false}  
{"id": "7", "admin": true}
```

🐦 YassineAboukir



♡ 265 12:46 PM - Nov 11, 2019



🗨 90 people are talking about this



From False to True



INTIGRITI
@intigriti



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!

BUG BOUNTY TIP

From False to True

Use Burp Suite's "match & replace" to replace **false** with **true** in the response. This may uncover hidden functionalities!





Twitter icon: anshuman_bh

Heart icon: 210 3:34 PM - Nov 6, 2019

Info icon: ⓘ

Comment icon: 83 people are talking about this >

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



INTIGRITI
@intigriti



Context is key. Find out what your target cares about to score higher bounties. Great advice from [@jackds1986](#)! #BugBountyTip

#HackWithIntigriti

BUG BOUNTY TIP



“Don't focus too much on vulnerability types. Focus on issues that really impact the company's business”

Twitter icon @jackds1986

Heart icon 64 11:25 AM - Apr 25, 2019 Information icon

Comment icon 21 people are talking about this View icon

The Birthday Trick



INTIGRITI
@intigriti Twitter icon

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

BUG BOUNTY TIP

The Birthday Trick

"If you sign up for a target, set your birthday to today or tomorrow! Then use birthday discount vouchers in your inbox to buy gift cards. Repeat!"



♡ 243 8:35 AM - May 14, 2019



61 people are talking about this



Skiping Steps



INTIGRITI
@intigriti



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!

BUG BOUNTY TIP

Skip some steps!

See a process with several steps?



♡ 221 1:04 PM - Nov 7, 2019

ⓘ

🗨 80 people are talking about this

>

The Coupon Trick



INTIGRITI
@intigriti



🛍 It's also #BlackFriday in #BugBounty land 🛒! Harvest all the coupon codes, try this #BugBountyTip by @quintenvi and score some bounties! 💰

QUINTENVI'S BUG BOUNTY TIP

Harvest #BlackFriday coupon codes in webshops. Try to:



- Check if they expire after friday
- Check if the discounts apply on gift cards. Repeat to generate infinite money!

♡ 63 12:38 PM - Nov 29, 2019



17 people are talking about this



Informative

Asking Questions



INTIGRITI
@intigriti



Got a question? Follow [@codingo_](#)'s advice to get help faster!
[#BugBountyTip](#)

BUG BOUNTY TIP

"Asking a question?

**Say what you tried & think.
You'll earn more respect and it
will help you understand the issue!"**

@codingo_

♡ 44 4:51 PM - Aug 7, 2019



See INTIGRITI's other Tweets



XSS Passwords



INTIGRITI
@intigriti



Want to catch someone snooping plaintext passwords? Follow
@quintenvi's advice! #HackWithIntigriti #BugBounty

BUG BOUNTY TIP

**"Use a blind XSS as password.
If it fires, someone is
in deep trouble!"**

@quintenvi



♡ 49 5:29 PM - Dec 10, 2018



› 18 people are talking about this



Share this:



Like this:

Loading...

Search

RECENT POSTS

Bug Bounty Q&A #3: What effort does it take to set up a bug bounty program?

Bug Bytes #67 – Hacking Containers, Auth0 Bypass & @Hussein98d's Methodologies

Bug Bytes #66 – Abusing Slack's TURN, Breaking AWS & Azure & @spaceraccoonsec SQLi secrets

Bug Bounty Q&A #1: What is ethical hacking and bug bounty?

Bug Bytes #65 – Hacking webcams, internal servicedesks & parsers

CATEGORIES

bugbountytips

bugbusiness

bugbytes

challenge

changelog

events

general

Q&A

testimonial

Uncategorised

ARCHIVES

Select Month

