IDOR Checklist

Intro

People make mistakes, and If they have been made once, they will be made again. I have decided to make a checklist of things to look for when searching for IDORs, this list is based of 220* prior reports from hacker one.

This doc is set out in tables representing categories, each table has the number of times times the check was found in reports, the check represents what to look for, and the report ID is the hacker one report ID which can be navigated to using the URL `https://hackerone.com/reports/{report ID}`

*220 as of 10th March 2021, sadly this number is less realistic considering the amount of not fully disclosed reports or reports that are in other languages.

Logins

Password reset feature

Times occoured	check	report ID
1	if an ID is submitted, does it reveal some sort of information? eg, email address	293490
1	if a OTP/ID/user hash is needed, can you submit a one you've just made on a different account?	842625

Times occoured	check	report ID
1	If a OTP is needed, what happens if you just submit new credentials without the OTP parameter?	843160
1	Check weak admin OTPs, 111111, 123456, 999999, 000000 etc	715054
1	Can you supply someone else's ID instead of yours in order to get account takeover	42587
Untitled		

URL

Times occoured	check	report ID
17	Is there an ID in the URL? (get)	1085782, 819807, 681001, 723118, 797685, 398316, 536853, 868590, 390346, 404797, 300179, 285432, 293845, 99600, 333767, 220864, 126861, 126861
1	Can a low priv user access resources via bypass?	681001
1	user's may be given a random directory ID in the url, this can be used to get other's info	906907

POST

Times occoured	check	report ID
14	Is there an ID sent during POST request	661978, 547663, 587687, 302485, 227522, 258260, 172545, 199281, 317332, 313050, 95552, 162147, 85720

Times occoured	check	report ID
2	if you save a settings page, is your ID sent?	974222, 969223
2	Are there IDs in the cookies?	514897, 854290
2	is there an ID in the request headers?	397137, 395246
1	when you buy something, is a payment ID sent? eg, saved credit card id	391092
Untitled		

APIs

Times occoured	check	report ID
21	is there an ID in a rest API?	819807, 681001, 788375, 888729, 783117, 848625, 854290, 741683, 148764, 320173, 181748, 287789, 271393, 308610. 245872, 192388, 56511, 154410, 120115, 120289
6	if sending a request to an API endpoint can you leak any data? emails, payment methods, etc	980511, 723461, 668439, 783708, 439729, 152407
6	If it employs graphQL, are they using any queries which update items? or maybe leak info?	980511, 924914, 835005, 397031, 587687, 291721
3	can you change parameter IDs to leak user IDs? or leak info? or do actions on others behalfs?	1005020, 725569, 258260
1	are other query langs employed? NRQL?	397137
Untitled		

Misc

Aa Times occoured	☰ check	☰ report ID
9	Can a resource be accessed directly, without prior access?	293845, 194790, 258260, 172545, 245872, 230328, 152407, 230870, 126861
5	Can IDs of accounts, images, documents etc be found by visiting them? or navigating the site? in the source code?	404797, 181748, 308610, 217558, 317332
3	Does the site own any similar sites that do the same process but have less protection?	876300, 715054, 271393
3	What happens if the action is done from users with different privileges?	980511, 148764, 308610
3	Can you use different methods than originally intended? eg PUT instead of GET to edit resources	204984, 199321, 297751
2	Just because the user ID seems encrypted, does not mean it is *always* encrypted. Can it be decoded?	1005020, 291721
2	Is the username an ID?	262661, 152407
1	If the request needs authentication, does it work if you remove the authentication parameter?	843160
1	Is a user's info deleted when they delete their account? if you create an account with the same name of a deleted one, can you see their info?	882258
1	An ID may not always be labelled as such, is there a suspicious number or ID somewhere?	302485
4	Can you destroy or damage any assets or information?	156537, 264754, 153905, 120115
Untitled		