Forum:Hack Forums

Thread: IDOR Tutorial

Faucet Failure - *September 22, 2019, 7:18 pm*

So IDOR
(Insecure Direct Object Reference) is a common vulnerability that occurs when a reference to an internal implementation object is exposed without any other access control. The vulnerability is often easy to discover and allows attackers to access unauthorized data.

Basically it's like thinking of common males for files are if its in a numerical sequence, just going back or up a number (enumeration)

If you were sent a link to a file like this

https://hackforums.net/fileview.php?id=newthread.pdf

And you substituted "newthread.pdf" for say "payroll.pdf"
https://hackforums.net/fileview.php?id=payroll.pdf

If there was a file with the name payroll PDF in that folder then it would call it, WITHOUT you knowing that was even a file

Today we will do this common attack on multiple unsuspecting file hosts

Now we can test these by uploading a blank file named 1.txt
On this file host, I got this url back

Quote:http://s000.tinyupload.com/?file_id=06062155144424049776
I can almost guarantee there are not
6,062,155,144,424,049,776 files on there so they are generating a unique file hash. Sure you can make a bot to guess all numbers and hope one of them matches and the file is love and worth something, not prned from the databases, but we are after something better.

Now this next file host gave us this url
Code http://www.yourfilelink.com/get.php?fid=21560822,156,082 files seems more reasonable so lets tick it back by a number

http://www.yourfilelink.com/get.php?fid=2156081

YES, that is a link to someone else's file

you cant always see what file names they are but if you were to make a bot to check all numbers in the sequence and report back with links and file names, you can pick which ones you want

I hope this helped you out with IDOR vulns