

What is IDOR?

- Insecure Direct Object Reference (IDOR) is a type of vulnerability that occurs when a user is able to access or modify resources that they are not authorised to access. vulnerabilities can be exploited to gain unauthorised access to sensitive information, such as user accounts, financial records.

How to detect IDOR?

- If an application has a URL structure like this:
 - https://www.example.com/view_orders?id=12345
- An attacker could try changing the 'id' parameter to a different value, such as "id = 12346" and see if the application does not properly check the user's authorization to view the order information, this could indicate an IDOR vulnerability.

SOC169 - Possible IDOR Attack Detected:

Medium Feb, 28, 2022, 10:48 PM SOC169 - Possible IDOR Attack Detected

EventID :	119
Event Time :	Feb, 28, 2022, 10:48 PM
Rule :	SOC169 - Possible IDOR Attack Detected
Level :	Security Analyst
Hostname :	WebServer1005
Destination IP Address :	172.16.17.15
Source IP Address :	134.209.118.137
HTTP Request Method :	POST
Requested URL :	https://172.16.17.15/get_user_info/
User-Agent :	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)
Alert Trigger Reason :	consecutive requests to the same page
Device Action :	Allowed
Show Hint	

- Source IP address: 134.209.118.137
- Destination IP Address: 172.16.17.15
- Requested URL: https://172.16.17.15/get_user_info/

I have done an investigation on 134.209.118.137 using VirusTotal, Cisco Talos and IBM xForce. There is a high rate of suspicious activities given by VirusTotal compared to others. This can be malicious traffic.

6
/ 87

?

Community Score

6 security vendors flagged this IP address as malicious

134.209.118.137 (134.209.0.0/16)
AS 14061 (DIGITALOCEAN-ASN)

US

DETECTION

DETAILS

RELATIONS

COMMUNITY 3

Security vendors' analysis

CMC Threat Intelligence	Malware	Comodo Valkyrie Verdict	Malicious
CRDF	Malicious	Cyble	Malicious
CyRadar	Malicious	Fortinet	Malware

I looked into Log management for what are the activities made by this IP address (134.209.118.137).

DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Feb, 28, 2022, 10:45 PM	Firewall	134.209.118.137	49211	172.16.17.15	443	🔍
Feb, 28, 2022, 10:45 PM	Firewall	134.209.118.137	48523	172.16.17.15	443	🔍
Feb, 28, 2022, 10:46 PM	Firewall	134.209.118.137	47274	172.16.17.15	443	🔍
Feb, 28, 2022, 10:47 PM	Firewall	134.209.118.137	43261	172.16.17.15	443	🔍
Feb, 28, 2022, 10:48 PM	Firewall	134.209.118.137	49271	172.16.17.15	443	🔍

Here we can clearly see there are several requests asked by the attacker to the webserver1005. Attacker perform IDOR attacks by changing the “id” value from 1 to 5. To get the information about the user.

Request URL: `https://172.16.17.15/get_user_info/`

User-Agent: `Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)`

Request Method: `POST`

Device Action: `Permitted`

HTTP Response Size:: `253`

HTTP Response Status: `200`

POST Parameters: `?user_id=2`

Request URL: `https://172.16.17.15/get_user_info/`

User-Agent: `Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322)`

Request Method: `POST`

Device Action: `Permitted`

HTTP Response Size:: `188`

HTTP Response Status: `200`

POST Parameters: `?user_id=1`

The attacker successfully got the information of another User by using the IDOR attack. We can say that by changes in HTTP Response size and also each request has HTTP Status 200 (OK).

Playbook answers:

EventID :	119
Event Time :	Feb, 28, 2022, 10:48 PM
Rule :	SOC169 - Possible IDOR Attack Detected
Answer :	True Positive (+5 Point)
Playbook Answers :	Do You Need Tier 2 Escalation? (+5 Point) Was the Attack Successful? (+5 Point) What Is the Direction of Traffic? (+5 Point) Check If It Is a Planned Test (+5 Point) What Is The Attack Type? (+5 Point) Is Traffic Malicious? (+5 Point)

- Yes, we need Tier 2 Escalation.
- The attack was successful
- The Direction of Traffic : internet to company network
- There is no information about Test. so, it was not a Planned Test
- Insecure Directory Object Reference (IDOR)
- Malicious Traffic