Author: Jack Fitzgerald

LetsDefend

Official Incident Report

Date: Feb, 28, 2022, 10:48 PM

Event ID: 119

Rule Name: SOC169 - Possible IDOR Attack Detected

Table of Contents

Alert Details

Severity: Medium

Type: Web Attack

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

Based on the information provided in the alert, it appears that an attacker has performed consecutive requests to the same page, running on **WebServer1005** to host **172.16.17.15**. The alert is triggered by rule SOC169 - Possible IDOR Attack Detected.

It is important to review all logs from the source IP address. The device action is marked **allowed**, indicating that the request attempts to the webpage were passed.

Overall, it appears that the **alert** may be suspicious, and further investigation is needed to identify the extent of the alert and determine if any necessary actions are required to remediate the situation.

Detection

Verify

As a security analyst, one of the first steps we take to verify the alert and determine whether it is a **false positive** or a **true positive** incident is to analyse the logs collected from the host by our security products.

At Feb, 28, 2022, 10:48 PM, **Webserver1005** with the IP address **172.16.17.15** received an HTTP POST request from **134.209.118.137** containing **https://172.16.17.15/get_user_info/** request URL.

It is important to understand why the alert was triggered:

- **Rulename:** Possible IDOR Attack Detected
- **Alert Reason:** consecutive requests to the same page
- **Source Address:** 134.209.118.137
- **Destination Address:** 172.16.17.15
- **Protocol:** TCP

It is also important to understand where the traffic is coming from and what the target of the web attack is:

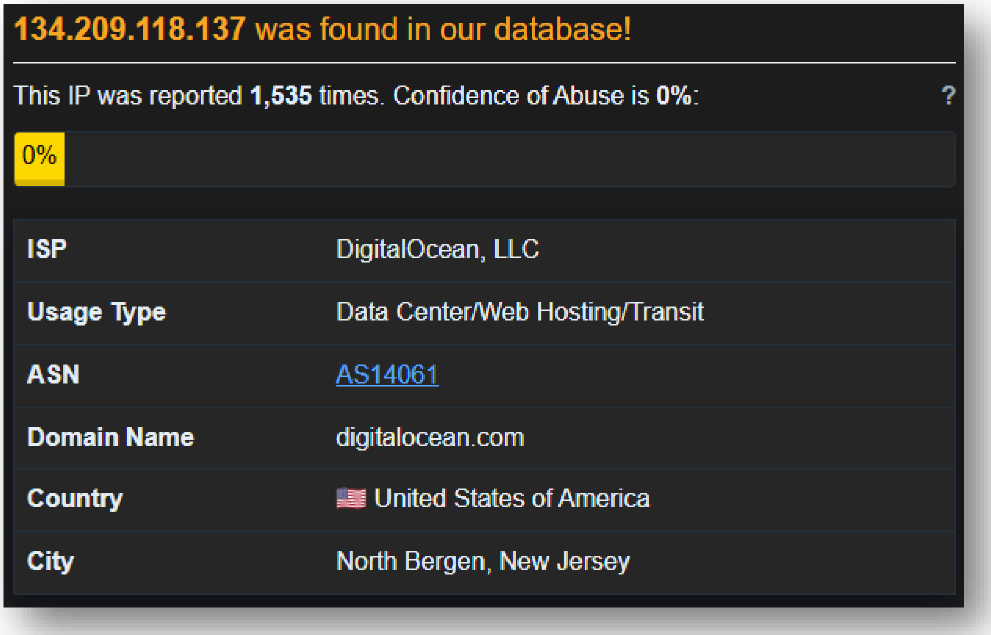
- **Primary User** of WebServer1005 (172.16.16.15): webadmin35
- **Last user logon**: Feb, 15, 2022, 01:43 PM
- Traffic is coming from **outside** (Internet)
- **Location** of 134.209.118.137: USA
- **Reputation** of 134.209.118.137: Poor

To gather this information, we analyse the source address **134.209.118.137** using online analysis tools such as **VirusTotal** and **AbuseIPDB**.

https://www.virustotal.com/gui/ip-address/134.209.118.137

No security vendor flagged this IP address as malicious

https://www.abuseipdb.com/check/134.209.118.137



134.209.118.137 was found in our database!

This IP was reported **1,535** times. Confidence of Abuse is **0%**: ?

0%

ISP	DigitalOcean, LLC
Usage Type	Data Center/Web Hosting/Transit
ASN	AS14061
Domain Name	digitalocean.com
Country	🇺🇸 United States of America
City	North Bergen, New Jersey

We should examine the HTTP traffic to understand what sort of web attack is occurring.

This sort of web attack shows patterns of an IDOR (Insecure Direct Object References) attack. IDOR is a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly.

According to PortSwigger, IDOR vulnerabilities often arise when sensitive resources are in static files on the server-side filesystem. For example, a website might save chat message transcripts to disk using an incrementing filename, and allow users to retrieve these by visiting a URL like the following:

- https://insecure-website.com/static/12144.txt

In this situation, an attacker can simply modify the filename to retrieve a transcript created by another user and potentially obtain user credentials and other sensitive data.

Attackers will first identify an IDOR vulnerability in a web application, then systematically test a series of reference values in the URL to gain access to sensitive information, sending repeated requests in a brute force to identify direct object reference values, for example:

- https://insecure-website.com/get_user_info?userid=1
- https://insecure-website.com/get_user_info?userid=2
- https://insecure-website.com/get_user_info?userid=3
- https://insecure-website.com/get_user_info?userid=4
- https://insecure-website.com/get_user_info?userid=5

Ways to spot IDOR attacks include:

- Consecutive requests to the same page from the same source
- Patterns in URL parameters

Analysis

The next step of our investigation into this IDOR web attack is to analyse the logs of the incident. We found that 5 events occurred originating from this alert, coming from a source address of **134.209.118.137** to the **WebServer1005** destination address of **172.16.17.15**.

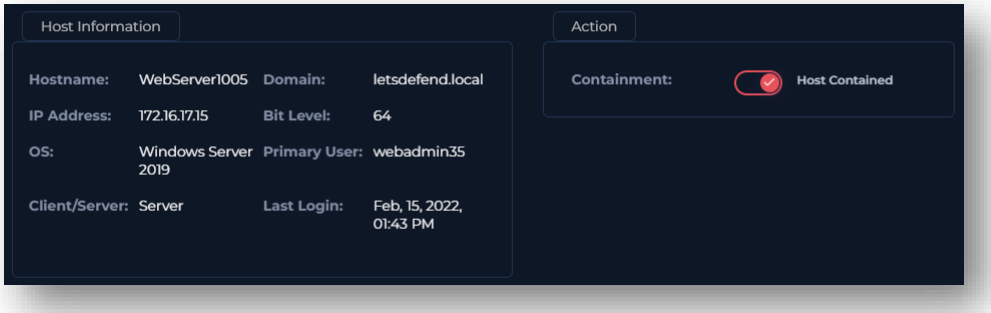
All 5 logs contain the same Request URL **https://172.16.17.15/get_user_info/** via POST method. The server sends back user ID's {1, 2, 3, 4, 5} with HTTP Response 200 (OK) indicating all 5 POST Requests were successful.

The User-Agent of all 5 requests was Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET CLR 1.1.4322), indicating a Microsoft XP machine using a Mozilla Firefox search engine.

From these analyses, we can conclude that the attacker's **IDOR** attack on **WebServer1005** was **successful**, due to HTTP Response Status: 200 (OK).

Containment

Based on the information gathered during the investigation, it is highly likely that the system has been compromised. Immediate isolation of the system from the network is required. Tier 2 escalation must be performed due to a successful attack.



Host Information

Hostname:	WebServer1005	Domain:	letsdefend.local
IP Address:	172.16.17.15	Bit Level:	64
OS:	Windows Server 2019	Primary User:	webadmin35
Client/Server:	Server	Last Login:	Feb, 15, 2022, 01:43 PM

Action

Containment: Host Contained

Summary

The incident involves a compromised system named **WebServer1005** with an IP address of **172.16.17.15**. The alert was triggered by the detection of consecutive requests to the same page, based on the rule SOC169 - Possible IDOR Attack Detected.

Upon further analysis, it was discovered that the source address **134.209.118.137** used to communicate with the server 5 different times, performing multiple **IDOR** attempts. This is evidenced by the log analysis seen on Feb, 28, 2022.

Based on the findings of the incident, on the Log Management page, we filter by source IP address and detect all requests. When the requests were examined, it was determined that the attacker wanted to change the ID value and **access information belonging to different users**. When the request sizes are examined, there is a different response size for each user, and the status code is 200. For this reason, the attack is considered to have been **successful**. Since the attack may have been successful, the device should be contained and **escalated to Tier 2**.

Immediate action needs to be taken to isolate the compromised system, and the event was identified as a **True Positive**.

Lessons Learned

- The primary failure was that the application trusted user-supplied identifiers without validating whether the requesting user owned the resource; this allowed an attacker to change the ID value and access another user's records

- The application design assumed attackers would not guess or tamper with identifiers, predictable IDs made enumeration easy

- Authentication was present, but authorization was missing or incomplete, controllers or API endpoints failed to implement ownership checks before serving the requested object

Remediation Actions

- Every object access must verify ownership or permission, regardless of the request source

- Use UUIDs, hashed IDs, or internal mapping tokens instead of sequential IDs, this doesn't replace authorization, but reduces predictability and makes enumeration more difficult

- Enforce least-privilege access policies

Appendix

MITRE ATT&CK

MITRE Tactics	MITRE Techniques
Initial Access	T1190 - Exploit Public-Facing Application
Privilege Escalation	T1134 - Access Token Manipulation
Discovery	T1087 - Account Discovery
Exfiltration	T1567 - Exfiltration Over Web Service

Artifacts

Value	Comment	Type
https://172.16.17.15/get_user_info/	Requested URL (IDOR)	URL Address
134.209.118.137	Attacker source address	IP Address

LetsDefend Playbook

LetsDefend Event ID: 119