**SOC169 - Possible IDOR Attack Detected**

**Overview**

EventID 119 corresponds to an alert triggered by Rule **SOC169 - Possible IDOR Attack Detected** on **February 28, 2022, at 10:48 PM**. The rule flagged potential activity consistent with an Insecure Direct Object Reference (IDOR) attack. The activity originated from **source IP 134.209.118.137** targeting **destination IP 172.16.17.15** on hostname **WebServer1005**. The **POST** requests were made to the endpoint https://172.16.17.15/get\_user\_info/, and the **device action allowed** the requests. Consecutive requests with varying user IDs in the parameters triggered the alert.

A screenshot of a computer

Description automatically generated

**Key Details**

* **Source IP:** 134.209.118.137
* **Destination IP:** 172.16.17.15
* **Hostname:** WebServer1005
* **Alert Trigger Reason:** Consecutive requests to the same page with changing parameters (user\_id).
* **Device Action:** Allowed (No blocking of traffic).

**Investigation Findings**

* **Behavior Analysis:**  
  The source made multiple sequential POST requests to get\_user\_info/ with different user IDs (user\_id=1, user\_id=2, user\_id=3, user\_id=4, user\_id=5). This behavior suggests a manual attempt to exploit an IDOR vulnerability to access sensitive data associated with different user accounts.

A blue and white striped background

Description automatically generated

* **Timeline:**  
  The requests were not automated, as indicated by the slight time gaps between them. This indicates manual probing rather than automated exploitation tools.
* **Response Details:**  
  Each request returned HTTP status code **200**, confirming successful access to the requested user information. The varying response sizes further suggest different data sets were retrieved for each user ID, potentially exposing unauthorized information.

A screenshot of a computer

Description automatically generated

**Assessment**

The activity strongly indicates an attempted IDOR attack. While the behavior appears manual and exploratory, the lack of blocking actions allowed sensitive information to be accessed across multiple user accounts. This highlights a security gap in the application, where authorization checks for user data access are either weak or nonexistent.

A screenshot of a computer

Description automatically generated

**Recommendations**

1. **Implement Proper Authorization Controls:** Ensure that access to user-specific data is restricted based on user roles and authentication tokens.
2. **Monitor for Similar Activity:** Set stricter alerting and blocking mechanisms for repeated sequential requests with varying parameters.
3. **Conduct Vulnerability Testing:** Test endpoints for IDOR vulnerabilities and remediate any identified issues.
4. **Log Review:** Continuously review logs for similar patterns to detect and mitigate any further unauthorized attempts.

**Conclusion**

The identified activity confirms a possible IDOR attack where sensitive user data may have been exposed due to inadequate authorization mechanisms. Immediate remediation of this vulnerability is critical to prevent future exploitation and unauthorized data access.

**N/B: Important Considerations for IDOR Monitoring and Investigation**

When investigating and monitoring for **Insecure Direct Object Reference (IDOR)** attacks, it is crucial to keep the following points in mind:

**1. Understanding the Attack Vector**

* **What is IDOR?**  
  IDOR vulnerabilities occur when a web application does not properly verify whether a user has permission to access a specific resource or object (e.g., user profiles, documents, or records). Attackers exploit this by directly modifying parameters (e.g., user\_id=1 to user\_id=2) to access unauthorized data.
* **Where to Check:**
  + Endpoints handling sensitive user or object data (e.g., get\_user\_info, order\_details, etc.).
  + APIs, URL query parameters, POST body fields, or cookies that reference identifiable objects (e.g., IDs, filenames).

**2. Key Indicators of IDOR Attacks**

* **Consecutive Requests with Altered Identifiers:**
  + Look for patterns in logs where an attacker modifies parameters like user\_id, account\_id, file\_id, etc.
  + Example: Requests such as user\_id=1, user\_id=2, user\_id=3 in a short timeframe.
* **Unusual Response Sizes:**
  + Varying HTTP response sizes suggest successful access to different resources.
* **Repeated Status Codes of 200 or 403:**
  + Successful (200) or restricted (403) responses to modified parameters indicate potential probing activity.
* **Unfamiliar IPs or User Agents:**
  + Attackers may use unknown IPs or outdated user agents (e.g., legacy browsers) to bypass filters.

**3. Steps to Monitor and Investigate**

* **Log Analysis:**
  + Focus on URL paths and parameters. For instance, in this case, get\_user\_info/ with user\_id variations triggered the alert.
* **Timeframes Between Requests:**
  + Identify whether the activity is manual (time gaps between requests) or automated (rapid requests).
* **Authorization Checks:**
  + Determine whether the endpoint validates the requester's permissions for each requested object.
* **Source Information:**
  + Check the originating IP address and user agent for potential anomalies or known malicious sources.

**4. Common Mistakes During Investigation**

* **Assuming All Alerts are Automated:**
  + Manual attacks often have small time gaps between requests and may appear subtle.
* **Ignoring Unsuccessful Requests:**
  + Failed attempts (e.g., 403 responses) still indicate probing activity and intent.
* **Overlooking Authorization Configurations:**
  + Investigate server-side logic to ensure access control mechanisms are robust and enforced consistently.

**5. Best Practices for Monitoring IDOR**

* **Implement Behavioral Anomaly Detection:**
  + Use tools to detect unusual patterns, such as parameter tampering or access requests for unrelated resources.
* **Rate Limiting and IP Blocking:**
  + Limit the number of consecutive requests from a single IP or session within a specific timeframe.
* **Enable Detailed Logging:**
  + Record user actions, including request parameters, timestamps, and associated responses.

**References**

1. OWASP Foundation. *Insecure Direct Object References (IDOR)*. Available at: https://owasp.org/www-community/attacks/Insecure\_Direct\_Object\_Reference
2. MITRE ATT&CK Framework. *Valid Accounts (T1078)*. Available at: https://attack.mitre.org/
3. Rapid7 Blog. *Access Control Vulnerabilities*. Available at: https://www.rapid7.com/blog/
4. Let's Defend. *SOC169 - Possible IDOR Attack Detected Lab*. Available at: <https://letsdefend.io/>