TEXNİKA ELMLƏRİ

TECHNICAL SCIENCES

DOI: https://doi.org/10.36719/2789-6919/32/192-196

Vüsal Rəhimli
Azərbaycan Texniki Universiteti
rahimlivusal2001@gmail.com

IDOR (INSECURE DIRECT OBJECT REFERENCES) ÜMUMİ NÖVLƏRİ, TƏSİRLƏRİ VƏ HÜCUMLARI

Xülasə

IDOR Təhlükəsiz Birbaşa Obyekt Referansları deməkdir ki, bu da proqram müvafiq təsdiq və ya icazə olmadan obyektlərə birbaşa daxil olmaq üçün istifadəçi girişindən istifadə etdikdə baş verən təhlükəsizlik zəifliyinin bir növüdür. Bu, təcavüzkarlara giriş nəzarətlərini yan keçməyə və həssas məlumat və ya funksionallığa icazəsiz giriş əldə etməyə imkan verə bilər. IDOR, istifadəçi tərəfindən təmin edilən daxiletmə ilə məşğul olan REST proqramlarında ümumi zəifliklərdən biridir.

Təhlükəsiz Birbaşa Obyekt Referansları (IDOR) veb proqramlardakı həssas resurslara icazəsiz girişə səbəb ola biləcək kritik təhlükəsizlik zəifliyidir. Bu bloq yazısında Java proqramlarında real həyat kimi IDOR ssenarilərini müzakirə ediləcək, bəzi zəiflikləri tapmaq nisbətən asan, digərləri isə daha çətin olur. Burada həssas ssenariləri təmsil edən kod parçaları təqdim ediləcək və onları təhlükəsiz şəkildə necə düzəlir nümayiş olunacaq. Bundan əlavə, PRD təhlükəsizlik baxışları kimi erkən mərhələlərdə IDOR zəifliklərini azaltmaq üçün Təhlükəsiz Proqram Təminatının İnkişafı Həyat Dövründə (SSDLC) müxtəlif yanaşmalar araşdırılacaq.

Açar sözlər: *IDOR, verilənlər bazası, JavaScript Obyekt Notasiyası, IDOR hücumları, kod baxışları, sorğu parametrləri*

Vusal Rahimli
Azerbaijan Technical University
rahimlivusal2001@gmail.com

IDOR (Insecure Direct Object References) common types, constructions and attacks

Abstract

IDOR defines Safe Direct Object References, which use user access to access objects without requiring software or input. This may allow investigators to gain access to data or functionality obtained after access control. IDOR is a common vulnerability in REST applications that deal with input provided by

Insecure Direct Object References (IDOR) is a critical security vulnerability that can lead to unauthorized access to sensitive resources in web applications. This blog post will discuss real-life IDOR scenarios in Java applications, where some vulnerabilities are relatively easy to find, while others are more difficult. Here, code snippets representing vulnerable scenarios will be presented and how to fix them safely. Additionally, various approaches in the Secure Software Development Lifecycle (SSDLC) will be explored to mitigate IDOR vulnerabilities at early stages such as PRD security reviews.

Keywords: *IDOR, database, JavaScript Object Notation, IDOR attacks, code reviews, query parameters*

Giriş

Təhlükəsiz Birbaşa Obyekt İstinadları tətbiqin daxili resurslara (məsələn, fayllar, verilənlər bazası qeydləri) lazımi giriş nəzarəti olmadan birbaşa çıxışına icazə verdiyi zaman baş verir. Təcavüzkarlar məxfi məlumatlara daxil olmaq və ya müəyyən istifadəçilərlə məhdudlaşdırılmalı olan hərəkətləri yerinə yetirmək üçün IDOR-dan istifadə edə bilər ki, bu da məlumat sızmasına, icazəsiz açıqlamaya və ya hətta sistemin tam kompromisinə gətirib çıxarır.

✓ *IDOR Zəifliklərini Azaltmaq üçün SSDLC yanaşması*

Təhlükəsiz Proqram Təminatının İnkişafı Həyat Dövründə (SSDLC) müxtəlif mərhələlər IDOR zəifliklərini kritik problemlərə çevrilməzdən əvvəl müəyyən etməyə və azaltmağa kömək edə bilər. Bu mərhələlərdən bəzilərini araşdıraq:

❖ ***PRD Təhlükəsizlik Baxışı***

Məhsul Tələbləri Sənədinin (PRD) nəzərdən keçirilməsi zamanı təhlükəsizlik ekspertləri və maraqlı tərəflər potensial IDOR risklərini müəyyən etmək üçün tətbiqin dizaynını və arxitekturasını qiymətləndirə bilərlər. Girişə nəzarət mexanizmlərinə və məlumat axını diaqramlarına diqqət yetirilməlidir (El Bachir, El Moussaid, 2020; 3-6).

❖ ***Təhdidlərin Modelləşdirilməsi***

İnkişaf prosesinin əvvəlində potensial IDOR təhlükələrini müəyyən etmək üçün təhlükə modelləşdirmə sessiyaları keçirmək lazımdır. Tətbiq komponentlərinin və məlumat axınlarının xəritəsini tərtib etməklə tərtibatçılar təhlükəsizlik nəzarətlərini və giriş məhdudiyyətlərini fəal şəkildə həyata keçirə bilərlər.

❖ ***Kod Baxışları və Statik Təhlil***

IDOR zəifliklərinə həssas olan kod nümunələrini müəyyən etmək üçün kodu nəzərdən keçirmək və statik analiz alətlərindən istifadə etmək lazımdır. Rəyçilər müvafiq icazə yoxlamaları olmadan birbaşa obyekt istinadlarını yoxlaya bilərlər (Eran, Yuval, Tom, 2020; 34-38).

❖ ***Təhlükəsizlik Testi***

Real hücum ssenarilərini simulyasiya etmək və tətbiqdə IDOR zəifliklərini müəyyən etmək üçün nüfuzetmə testi və zəifliyin skan edilməsi daxil olmaqla dinamik təhlükəsizlik testini həyata keçirmək lazımdır.

❖ ***İstifadəçi İcazələri və Rol Əsaslı Giriş Nəzarəti (RBAC)***

Hər bir istifadəçinin yalnız istifadə etməyə icazə verdiyi resurslara daxil ola bilməsini təmin etmək üçün güclü istifadəçi icazələri və RBAC mexanizmlərini tətbiq etmək lazımdır (Əliquliyev, İmamverdiyev, 2020; 62).

❖ **Təhlükəsiz API Dizaynı**

Tətbiq API təmin edirsə, həssas məlumatlara icazəsiz girişin qarşısını almaq üçün onlara giriş nəzarətləri və istifadəçi autentifikasiyası mexanizmlərini daxil etdiyinə əmin olmaq lazımdır.

❖ **Ən az imtiyaz prinsipi**

Resurslara və funksiyalara girişi yalnız hər bir istifadəçi rolu üçün zəruri olanlarla məhdudlaşdırmaq üçün ən az imtiyaz prinsipini tətbiq etmək lazımdır.

Təhlükəsiz birbaşa obyekt istinadları veb proqramlarda giriş nəzarətinin pozulması nəticəsində yaranan ümumi, potensial dağıdıcı zəifliklərdir. IDOR səhvləri təcavüzkarın verilənlər bazası açarı, sorğu parametri və ya fayl adı kimi "birbaşa obyekt arayışı" ilə manipulyasiya edərək veb tətbiqi ilə zərərli şəkildə qarşılıqlı əlaqədə olmağa imkan verir (4).

✓ ***Dörd ümumi IDOR növü***

Bu günlərdə identifikatorlar istifadəçinin ünvan çubuğunda olduğundan daha çox başlıqlarda və ya API-lərdə tapılır. Bununla belə, əksər veb-saytların dinamik təbiəti o deməkdir ki, identifikatorlar və parametrlər hələ də bu və ya digər formada çox istifadə olunur. İdentifikatorlara aşağıdakılar daxil ola bilər:

- *Verilənlər bazası açarları*
- *Sorğu parametrləri*
- *İstifadəçi və ya sessiya identifikatorları*
- *Fayl adları*

IDOR zəifliklərini necə müəyyən etmək olar?

IDOR zəifliklərindən istifadə etmək çox vaxt sadədir, lakin tərtibatçılar üçün müəyyən etmək çətin ola bilər. Kod təhlili və avtomatlaşdırılmış skanlama kimi alətlər və üsullar IDOR səhvlərini aşkar etməkdə bir çox digər ümumi təhlükəsizlik problemləri kimi yaxşı deyil, bu o deməkdir ki, bu zəifliklərin müəyyən edilməsi əl ilə təhlükəsizlik testi tələb edə bilər (5).

Zəifliklər müəyyən etməyin bəzi yollarına aşağıdakılar daxildir:

- Veb brauzerində quraşdırılmış developer alətlərindən istifadə edərək əsas testlərin həyata keçirilməsi;
- Manual testin effektivliyini artırmaq üçün Burp Suite və ya Open Web Application Security Project Zed Attack Proxy (OWASP ZAP) kimi bir vasitədən istifadə etmək;
- Zəifliyin aşkarlanması proqramında iştirak etmək;
- Kritik veb tətbiqlərini nəzərdən keçirmək üçün xarici nüfuz testi firmasının işə götürülməsi (6).

✓ *Dörd növ IDOR hücumu*

Konseptual olaraq, IDOR-dan istifadə edən hücumların əksəriyyəti oxşar tərzdə işləyir, lakin identifikatorun hakerlər tərəfindən ifşa edildiyi və ya manipulyasiya edildiyi kiçik nüanslar var:

1. URL-in dəyişdirilməsi

URL-nin dəyişdirilməsi IDOR zəifliyindən istifadə etmək üçün ən sadə üsuldur və çox vaxt az və ya heç bir texniki təcrübə tələb etmir. Bu cür hücumda sadəcə olaraq veb brauzerin ünvan çubuğundakı parametrin dəyərini dəyişmək olar (7).

2. Bədən manipulyasiyası

Bədən manipulyasiyası URL-nin dəyişdirilməsinə çox bənzəyir, istisna olmaqla, təcavüzkar URL-də deyil, sənədin mətnində bir və ya bir neçə dəyəri dəyişdirir. Bu, radio düymələrinin, onay qutularının və ya digər forma elementlərinin dəyərlərinin dəyişdirilməsi demək ola bilər. Gizli forma dəyərlərini dəyişdirmək də mümkün ola bilər.

Ola bilsin ki, kontaktın hazırda daxil olmuş hesab üçün istifadəçi identifikatoruna ötürülən gizli forma dəyəri var. Formanı təqdim etməzdən əvvəl həmin gizli dəyəri dəyişdirə bilsək, sorğumuzu başqa istifadəçidən gələn kimi göstərə bilərik (8).

3. Kuki və ya JSON ID manipulyasiyası

Kukilər və JavaScript Obyekt Notasiyası (JSON) hər ikisi müştəri və server arasında məlumatların saxlanması və mübadiləsi üçün pərdə arxasında geniş şəkildə istifadə edilir və veb səhifələri daha dinamik etməyə kömək edir. Biz vebsayta daxil olduğumuz zaman, məsələn, server kuki və ya JSON obyektində istifadəçi və ya sessiya ID dəyərini saxlaya bilər. Tətbiqdə IDOR zəifliyi varsa, təcavüzkar bu dəyərləri dəyişə bilər.

4. Yol keçidi

Yol keçidi, həmçinin qovluq keçidi adlanır, təcavüzkarın veb tətbiqini idarə edən serverdə fayl və ya qovluqlara daxil olmaq və ya manipulyasiya etmək üçün istifadə etdiyi unikal IDOR zəifliyi növüdür. Bu, IDOR hücumlarının digər növləri ilə müqayisədə daha dərin səviyyədir, çünki verilənlər bazası qeydləri əvəzinə fayl sistemi resurslarına birbaşa giriş imkanı verir (İnformasiya Təhlükəsizliyi, 2020; 101-105). Yol keçidi təcavüzkarın konfiqurasiya fayllarına daxil olmasına, istifadəçi etimadnaməsini kəşf etməyə və hətta hədəfdə tam funksional qabıq əldə etməyə imkan verə bilər.

✓ *IDOR dataya necə təsir edir?*

IDOR zəifliklərindən istifadə etmək sadə ola bilər, lakin bu tip hücumun təsirləri potensial olaraq fəlakətlidir. Aşağıda IDOR-un təşkilatınızın məlumatlarının məxfiliyinə, bütövlüyünə və əlçatanlığına təsir göstərə biləcəyi bir neçə üsul var (Qasımov, 2018; 56-59):

- ***Məxfilik*** - Uğurlu IDOR hücumu təcavüzkarın görə bilməməsi lazım olan bir şeyə giriş imkanı verir. Bu, rəqəmsal vitrində tez-tez alıcılar üçün endirim kodundan tutmuş şəxsi sağlamlıq məlumatlarına və ya ticarət sirlərinə qədər hər şey ola bilər.
- ***Dürüstlük*** - Bəzi hallarda təcavüzkar məlumatları dəyişdirmək üçün IDOR-dan istifadə edə bilər. Adətən, bu cür hücumlar HTTP POST sorğusunda parametrləri manipulyasiya edir. 2020-ci

ildə bir təhlükəsizlik tədqiqatçısı təcavüzkarın ABŞ Müdafiə Nazirliyinin veb serverlərində istifadəçi hesablarının parolunu dəyişməsinə imkan verən IDOR zəifliyini aşkar etdi. Təcavüzkarlar şübhəli olmayan istifadəçiyə saxta maliyyə məlumatları və ya ittihamedici sənədlər kimi icazəsiz məlumatlar əlavə etmək üçün oxşar zəifliklərdən istifadə edə bilər (Shar, Briand, 2018: 1-5).

- ***Əlçatımlılıq*** - IDOR həmçinin resursların mövcudluğuna təsir etmək üçün sui-istifadə edilə bilər. PHP proqramında sənədləri fayl adına görə silən bir funksiyanı təsəvvür edin. Müvafiq icazə yoxlamaları olmadan təcavüzkar fayl adını dəyişə və hətta girişi olmayan sənədləri silə bilər!
- *IDOR zəifliklərinin qarşısını almaq üçün dörd məsləhət*

IDOR zəifliklərinin qarşısı birbaşa obyekt istinadlarından qaçınmaqla, istifadəçi daxiletməsinin təsdiqini həyata keçirməklə və qlobal miqyasda unikal identifikatorlar (GUID kimi tanınan) və ya təsadüfi identifikatorlar tətbiq etməklə alına bilər. IDOR zəifliklərinin qarşısının alınmasına dair heç bir qüsursuz həll yolu olmasa da, bu addımlardan bəziləri kömək edə bilər.

1. Müvafiq giriş nəzarəti və sessiyanın idarə edilməsini həyata keçirmək;

"Təhlükəsiz birbaşa obyekt arayışı" terminini işlədən OWASP, IDOR-u hər şeydən əvvəl girişə nəzarət məsələsi hesab edir. Düzgün girişə nəzarət yoxlamaları və sessiyanın idarə edilməsi xüsusiyyətləri, hətta asanlıqla sadalanan identifikatorlardan istifadə edildikdə belə, zərərli istifadəçinin məlumatlara daxil olmaq və ya manipulyasiya etmək imkanının qarşısını almalıdır.

Avtorizasiya və autentifikasiya üzrə OWASP fırıldaqçı vərəqləri nəzərdən keçirmək üçün faydalı ola bilər.

2. Birbaşa obyekt istinadlarından çəkinmək;

Giriş nəzarəti məsələləri bir yana qalsın, tətbiqinizdə birbaşa obyekt istinadlarından istifadə çox vaxt səliqəsiz kodlaşdırma təcrübəsi hesab olunur. Bu xüsusilə tələbə/işçi şəxsiyyət vəsiqələri, hesab nömrələri və s. kimi həssas dataya gəldikdə doğrudur. Dolayı obyekt istinadları – çox vaxt ya istinad xəritələri və ya heşinq formasında – gizlədilmiş həqiqi identifikatoru gizlətməklə və ya çaşdırmaqla IDOR zəifliklərini ünvanlayır.

3. GUID və ya təsadüfi identifikatorlardan istifadə etmək;

İterativ və ya ardıcıl identifikatorlardan və ya parametr dəyərlərindən istifadə edən tətbiqlərdə etibarlı olmayan birbaşa obyekt istinad açığını sadalamaq işin öhdəsindən gəlmək olar. Nə GUID-lər, nə də universal unikal identifikatorlar əsas zəifliyi aradan qaldırmır, lakin onlar sadalamağı və istismar etməyi xeyli çətinləşdirir (Yang, Shen, 2021: 56).

4. İstifadəçi daxiletməsini təsdiq etmək;

İstifadəçi daxiletməsinin yoxlanılması IDOR daxil olmaqla, çoxlu sayda təhlükəsizlik problemlərini azaltmağa kömək edə bilər. Müvafiq uzunluq və format üçün istifadəçi tərəfindən təmin edilən parametrləri ciddi şəkildə yoxlasaq, identifikatorların sadalanması daha çətinləşir. Doğrulama ən uyğun olandan asılı olaraq ya müştəri, ya da server tərəfində baş verə bilər.

Nəticə

IDOR zəifliklərı təhlükəli ola bilər və onları aşkar etmək çətin ola bilər, çünki onlar tez-tez tətbiqin giriş nəzarətində incə qüsurları ehtiva edir. Düzgün doğrulama yoxlamaları və giriş nəzarətlərini həyata keçirməklə və tətbiqin təhlükəsizlik testini həyata keçirməklə siz IDOR zəifliklərinin qarşısını almaqda və tətbiqinizi icazəsiz girişdən qorumaqda kömək edə bilərsiniz.

Təhlükəsiz Birbaşa Obyekt Referansları (IDOR) həssas resurslara icazəsiz girişə səbəb ola biləcək təhlükəli zəifliklərdir. Bu bloq yazısında biz Java proqramlarında real həyat kimi IDOR ssenarilərini araşdırdıq və onları təhlükəsiz şəkildə necə düzəltməyi nümayiş etdirdik. Müvafiq giriş nəzarətlərini, avtorizasiya yoxlamalarını həyata keçirməklə və Təhlükəsiz Proqram Təminatının İnkişafı Həyat Cycle (SSDLC) ən yaxşı təcrübələrinə riayət etməklə tərtibatçılar IDOR zəifliklərini effektiv şəkildə azalda və veb tətbiqlərinin təhlükəsizliyini təmin edə bilərlər. Daimi təhlükəsizlik testi və proaktiv təhlükəsizlik tədbirləri möhkəm və təhlükəsiz Java proqramlarının yaradılmasında mühüm rol oynayır (8).

Ədəbiyyat

1. El Bachir, N., El Moussaid, A. (2020). Web Application Attacks Detection: A Survey and Classification, International Journal of Computer Applications, pp.3-6.
2. Eran, El., Yuval, R., Tom, T. (2020). System for determining web application vulnerabilities", pp.34-38.
3. Əliquliyev, R.M., İmamverdiyev, Y.N. (2020). İnformasiya təhlükəsizliyi insidentləri. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 62 s.
4. https://crashtest-security.com/insecure-direct-objectreference-idor/
5. https://portswigger.net/web-security/access-control/idor
6. https://www.geeksforgeeks.org/insecure-direct-objectreference-idor vulnerability/
7. https://www.loginradius.com/blog/engineering/httpsecurity-headers
8. https://www.thesslstore.com/blog/http-securityheaders/
9. İnformasiya Təhlükəsizliyi. (2020). Təhlükəsizlik metodları. İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri. Bakı, s.101-105.
10. Qasımov, V. (2018). İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı, s.56-59.
11. Shar, L., Briand, H. (2018). Web Application Vulnerability Prediction using Hybrid Program Analysis and Machine Learning, IEEE Trans. Dependable and Secure Comput., pp.1-5.
12. Yang, C., Shen, C. (2021). Implement Web Attack Detection Engine with Snort by Using Modsecurity Core Rules. 56 p.

Göndərildi: 08.02.2024 Qəbul edildi: 12.04.2024