КИБЕРБЕЗОПАСНОСТЬ: РЕАЛЬНЫЙ ПРИМЕР УЯЗВИМОСТИ “IDOR” И СТРАТЕГИИ ЕЕ ПРЕДОТВРАЩЕНИЯ

Абдуллаев Азизбек Сухробов угли, *Бухарский государственный педагогический институт, Теория и методика обучения и воспитания (Допризывное военное образование) Направление магистрантб 1 курс, Узбекистан, Бухара*
abdullayev20040321@gmail.com

Аннотация: *В этой статье рассматривается уязвимость “Insecure Direct Object references” (IDOR), которая является одним из наиболее важных аспектов кибербезопасности, и эффективные стратегии ее предотвращения. Уязвимость “IDOR” обеспечивает несанкционированный доступ к важной информации через идентификаторы, которыми пользователь может манипулировать в веб-приложениях. В статье показано, как работает эта уязвимость и связанные с ней риски на реальном примере.*

Ключевые слова: *Кибербезопасность, “IDOR” (Insecure Direct Object references), уязвимости, стратегические решения, защита данных, технологические решения.*

CYBERSECURITY: THE “IDOR” VULNERABILITY IN THE REAL EXAMPLE AND ITS PREVENTION STRATEGY

Abdullaev Azizbek Sukhrob ugli, *Bukhara State Pedagogical Institute,Theory and methodology of Education and training (Military Pre-Conscription Training)1st-year Master's Student,Uzbekistan, Bukhara*
abdullayev20040321@gmail.com

Annotation: *This article discusses the Insecure Direct Object References (IDOR) vulnerability, an important aspect of cybersecurity, and effective strategies for its prevention. The “IDOR” vulnerability enables unauthorized access to critical information through identifiers that can be manipulated by the user in web applications. The article shows how this vulnerability works and the associated risks through a realistic example.*

Keywords: *Cybersecurity, “IDOR” (Insecure Direct Object References), vulnerabilities, strategic solutions, data protection, technological solutions.*

KIBERXAVFSIZLIK: REAL MISOLDAGI “IDOR” ZAIFLIGI VA UNING OLDINI OLISH STRATEGIYASI

Abdullayev Azizbek Suxrob o‘g‘li, *Buxoro davlat pedagogika instituti, Ta’lim va tarbiya nazariyasi va metodikasi (Chaqiriqqacha harbiy ta’lim) yo‘nalishi 1 – bosqich magistranti, O‘zbekiston, Buxoro*
abdullayev20040321@gmail.com

Annotatsiya: *Ushbu maqolada kiberxavfsizlikning muhim jihatlaridan biri bo‘lgan “Insecure Direct Object References” (IDOR) zaifligi va uning oldini olishning samarali strategiyalari haqida so‘z boradi. “IDOR” zaifligi veb-ilovalarda foydalanuvchi tomonidan manipulyatsiya qilinishi mumkin bo‘lgan identifikatorlar orqali muhim ma’lumotlarga ruxsatsiz kirishni amalga oshiradi. Maqolada real misol orqali bu zaiflikning qanday ishlashi va u bilan bog‘liq xavf-xatarlar ko‘rsatilgan.*

Kalit so‘zlar: *Kiberxavfsizlik, “IDOR” (Insecure Direct Object References), zaifliklar, strategik yechimlar, ma’lumotlarni himoya qilish, texnologik yechimlar.*

Kirish: Kiberxavfsizlik sohasidagi muammolar, texnologiyalar rivojlanishi va internet tarmog‘ining kengayishi bilan birga yanada murakkablashmoqda. Bugungi kunda kompaniyalar va tashkilotlar o‘zlarining ma’lumotlarini himoya qilishga alohida e’tibor qaratmoqda. Internetda ma’lumotlar almashinuvi va onlayn xizmatlarning ko‘payishi bilan birga, kiberxavfsizlikka bo‘lgan talab ham ortmoqda. Shu bilan birga, kiberxavfsizlik

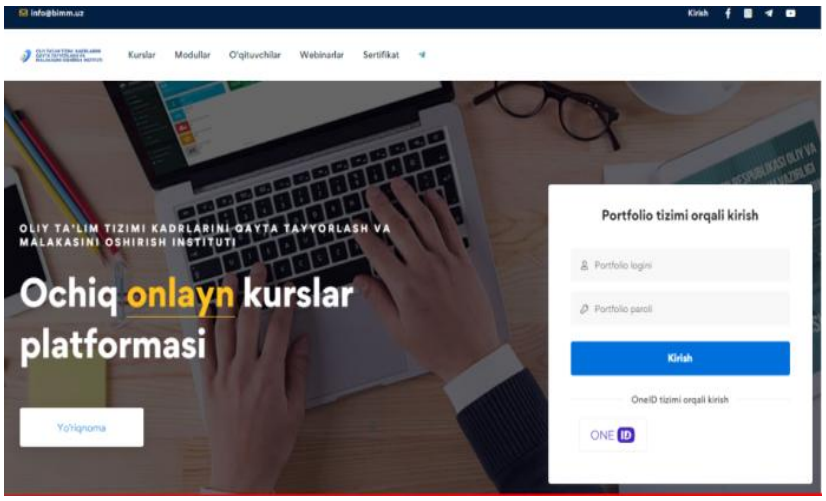
sohasida eng keng tarqalgan xavf-xatarlar va zaifliklar orasida “IDOR” (Insecure Direct Object References) katta o‘rinni egallaydi.

“IDOR” bu veb - ilovalar yoki tizimlar orqali foydalanuvchilar tomonidan manipulyatsiya qilinadigan identifikatorlar yordamida ma’lumotlarga ruxsatsiz kirish imkonini beruvchi xavfli zaiflikdir. Bu turdagi zaiflik, foydalanuvchi tizimga qandaydir obyektga murojaat qilayotganda, obyektning identifikatori (masalan, “URL” yoki boshqa parametrlar orqali) oson o‘zgartirilishi mumkinligidan kelib chiqadi. “IDOR” zaifligi veb-ilovalarning autentifikatsiya va avtorizatsiya tizimlarining zaif joylaridan foydalanish imkoniyatini beradi, bu esa tizimga kirgan foydalanuvchiga noma’lum yoki nomaqbul ma’lumotlarga kirish imkonini yaratadi. Bu holat ko‘pincha tizimdagi muhim ma’lumotlar, masalan, foydalanuvchi ma’lumotlari, to‘lovlar yoki maxfiy hujjatlar kabi resurslarga ruxsatsiz kirishga olib kelishi mumkin. [1]

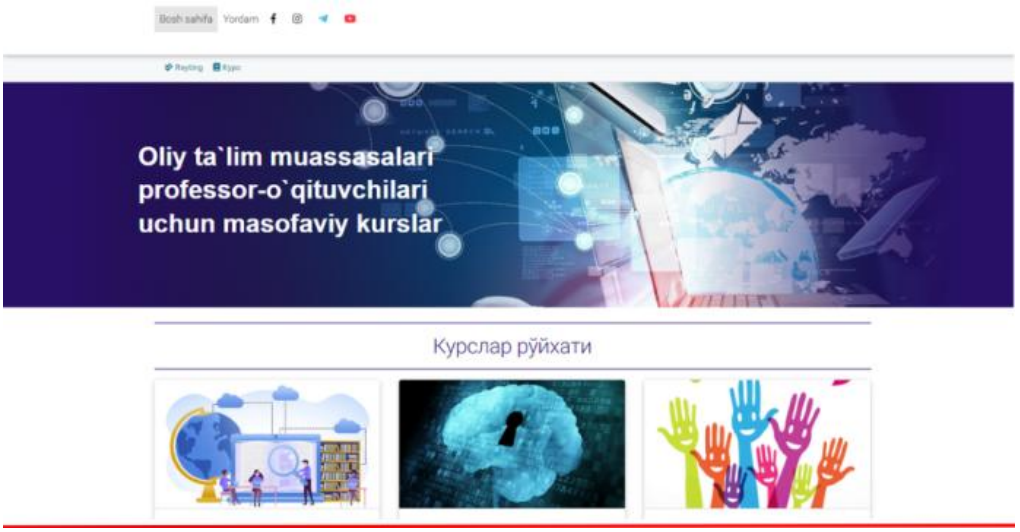
Kiberxavfsizlik sohasidagi strategik va texnologik yechimlar muhim ahamiyatga ega. “IDOR” kabi zaifliklarni aniqlash va ularga qarshi samarali strategiyalarni ishlab chiqish kiberxavfsizlikni yaxshilash uchun zarurdir. Buning uchun ilovalarda tizimli tekshiruvlar, autentifikatsiya va avtorizatsiya jarayonlarini to‘g‘ri tashkil etish, hamda foydalanuvchi ma’lumotlarini himoya qilishda ilg‘or texnologiyalarni qo‘llash zarur. “IDOR” zaifligini bartaraf etish uchun maxsus mexanizmlar va himoya tizimlari, masalan, parametrlar tekshiruvi, so‘rovlar filteringi va foydalanilayotgan identifikatorlar nomlarining xavfsizligi haqida chuqur bilimlarga ega bo‘lish talab qilinadi.

Tadqiqot obyekti: Bu maqolada “IDOR” zaifligining kiberxavfsizlikka ta’siri va unga qarshi kurashishda qo‘llaniladigan zamonaviy strategik va texnologik yechimlar muhokama qilinadi. Shuningdek, “IDOR” va unga o‘xshash xavflarga qarshi kurashishda ko‘rsatiladigan texnologik yondashuvlar va ularni muvaffaqiyatli tatbiq etish usullari taqdim etiladi. Maqola davomida “IDOR” ning real misolda qanday ishlashini ko‘rib chiqamiz. [2]

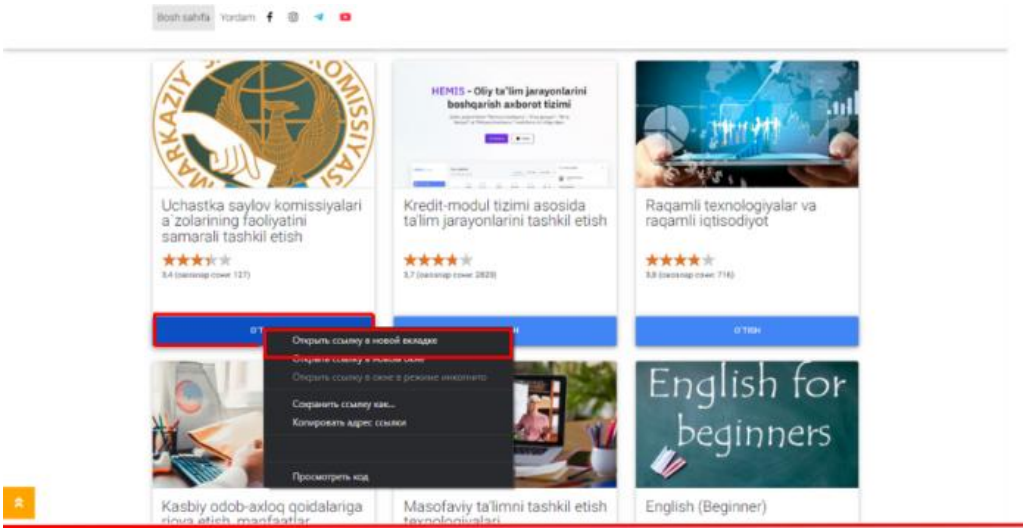
Misol (Ushbu misol, faqatgina o‘quv maqsadlarida bajarildi!):



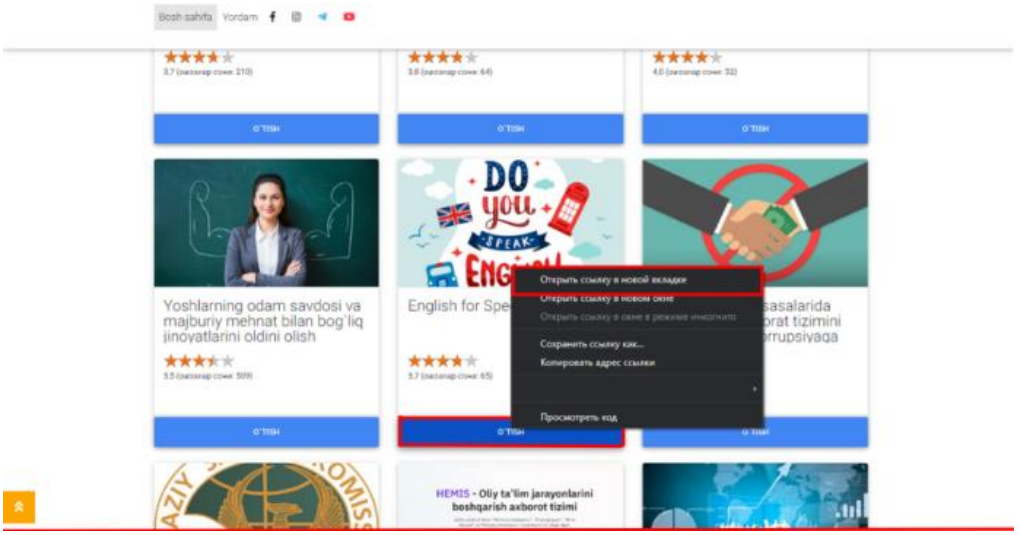
1-qadam (Avtorizatsiya sahifasi, sayt: https://mk.bimm.uz/)



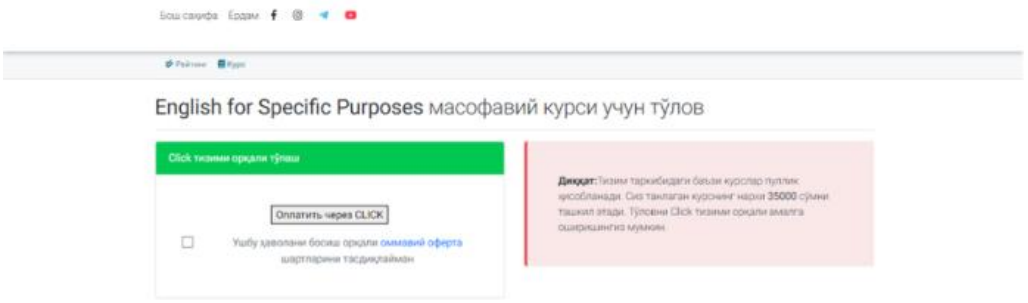
2-qadam (Avtorizatsiya sahifasidan so‘ng, bosh sahifaga avtomatik o‘tiladi. Ushbu saytda har xil pullik va bepul kurslar mavjud)



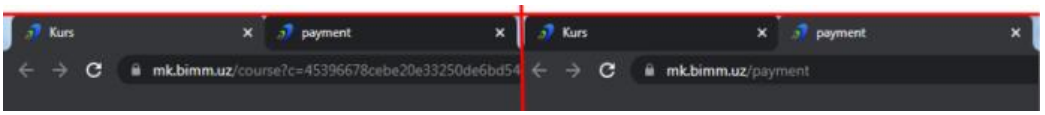
3-qadam (Mana shunday nomli kursni topamiz: “Uchastka saylov komissiyalari a’zolarining faoliyatini samarali tashkil etish” va sichqonchani o‘ng tugmasini bosib, “Открыть ссылку в новой вкладке” degan variantni tanlaymiz)



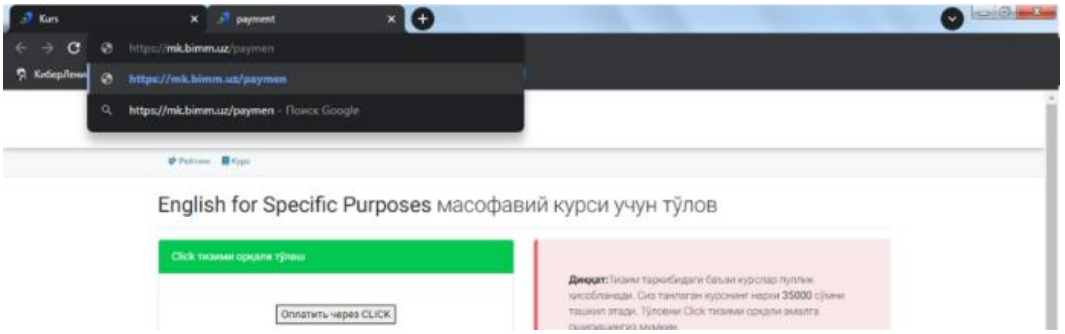
4-qadam (Mana shunday nomli kursni topamiz: “English for Specific Purposes” va sichqonchani o‘ng tugmasini bosib, “Открыть ссылку в новой вкладке” degan variantni tanlaymiz)



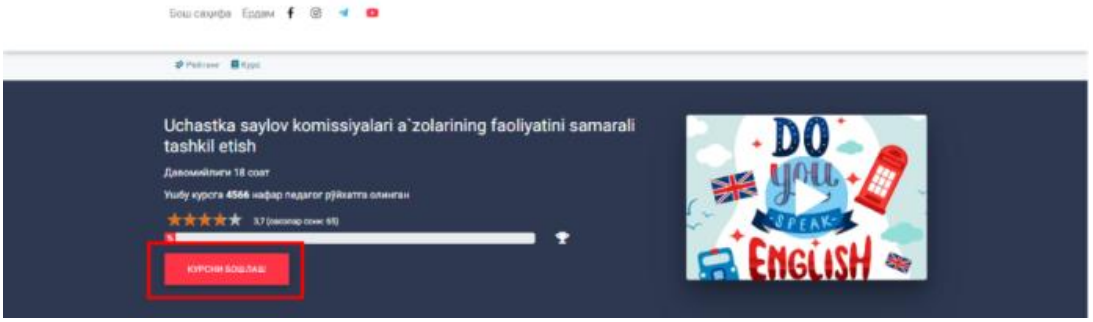
5-qadam (Ushbu rasmga e’tibor bersak, ushbu kurs ushun 35.000 so‘m pul talab qilinyabti)



6-qadam (Shunday qilib, biz ikkita yorliq yaratdik. Birinchi yorliq bu, bizning bepul kursimizniki: “Uchastka saylov komissiyalari a’zolarining faoliyatini samarali tashkil etish” va ikkinchi yorliq bu pullik kursniki: “English for Specific Purposes” – payment deb yozilishining sababi, 5-qadamda ko‘rsatilgan. To‘lov qilinmaguncha, pullik kursni boshlab bo‘lmaydi)



7-qadam (Brauzer qidiruv joyidan, havolaning bitta harfini o‘chiramiz
Avval: https://mk.bimm.uz/payment
O‘zgatirilgandan so‘ng: https://mk.bimm.uz/paymen va “Enter” tugmasini bosamiz)



8-qadam (“Kursni boshlash” tugmasi bosiladi. Ochilgan yorliqlar yopilmasin. Avvalambor yangi yorliqda “Uchastka saylov komissiyalari a’zolarining faoliyatini samarali tashkil etish” kursi ochiladi, so‘ngra esa pullik kurslar “Открыть ссылку в новой вкладке” orqali ochiladi. Shu orqali biz, pullik to‘lov jarayonini “IDOR” zaifligi orqali aylanib o‘tdik)

“IDOR” zaifligini oldini olish strategiyasi. “IDOR” (Insecure Direct Object

References) zaifligini bartaraf etish uchun bir nechta samarali strategiyalar mavjud. Ushbu zaiflikni yo‘q qilish uchun autentifikatsiya va avtorizatsiya tizimlarini mustahkamlash, foydalanuvchi kirish huquqlarini nazorat qilish, so‘rovlarni tekshirish, identifikatorlarni xavfsiz boshqarish, kuchli xavfsizlik devorlarini joriy etish, va vaziyatga mos ravishda sinovlarni o‘tkazish talab etiladi.

Quyida ushbu strategiyalar batafsil bayon etiladi:

1. Foydalanuvchi autentifikatsiyasini mustahkamlash
2. Avtorizatsiya tizimini to‘g‘ri tashkil etish
3. So‘rovlarni tekshirish va filtrlash
4. Identifikatorlarni xavfsiz boshqarish
5. “Pentesting” va xavfsizlik sinovlarini muntazam o‘tkazish

Xulosa: “IDOR” zaifligi kiberxavfsizlik sohasidagi eng keng tarqalgan va xavfli muammolardan biridir. Ushbu zaiflikdan himoyalanish uchun autentifikatsiya va avtorizatsiya tizimlarini kuchaytirish, foydalanuvchi so‘rovlarini tekshirish, obyekt identifikatorlarini xavfsiz boshqarish hamda muntazam xavfsizlik testlarini o‘tkazish juda muhimdir. Zamonaviy himoya strategiyalarini qo‘llash orqali “IDOR” zaifligi va unga o‘xshash kiberxavfsizlik tahdidlarini minimallashtirish mumkin.

Shunday qilib, har qanday veb-ilova va axborot tizimida kuchli xavfsizlik strategiyasini joriy etish va muntazam ravishda tekshiruvlar olib borish “IDOR” xurujlarini oldini olishning eng samarali usuli hisoblanadi.

FOYDALANILGAN ADABIYOTLAR:

[1]. Yoshlar Forumi. (2024). Milliy raqamli xavfsizlikni kuchaytirish va yosh “IT” mutaxassislarini tayyorlash uchun kiberxavfsizlik, axborot xavfsizligi bo‘yicha volontyorlar guruhlarini tashkil etish. *Abdullayev Azizbek. Retrieved from https://yoshlarforumi.uz/uz/idea/item/0421664. (2928 votes).*

[2]. SecurityLab. (n.d.). IDOR (Insecure Direct Object References). *Retrieved from https://www.securitylab.ru/glossary/idor/*