EYIB
EDUCATIONAL YIELD
INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.5 №2
https://eyib.uz

WEB ILOVALARGA BO‘LADIGAN HUJUMLAR TASNIFI

Ibroximov A.R	*“Kiberxavfsizlik markazi” DUK Axborot tizimlari kiberxavfsizligi bo‘limi boshlig‘i, PhD*
Haydarov E.D.	*Muhammad al-Xorazmiy nomidagi TATU Axborot xavfsizligi kafedrasi mudiri, PhD*

Annotatsiya

Ushbu maqolada veb ilovalarga qaratilgan autentifikatsiya hujumlari, maxfiylikni, foydalanuvchanlikni, yaxlitlik buzishga qaratilgan hujumlar, parolni qidirish hujumlari, fishing hujumlari tahlil etilgan, ularni amalga oshirish usullari tadqiq etilgan hamda ularni oldini olish usullari taklif etilgan.

Kalit so‘zlar: Maxfiylik hujumlari, foydalanuvchanlik hujumlari, yaxlitlik hujumlari, parolni qidirish hujumlari, fishing hujumlari, koddagi zaifliklar.

Web-ilovalarga qilingan hujumlar turli mezonlarga ko‘ra tasniflanishi mumkin. Web-ilovalarga hujumlarning asosiy turlarini ko‘rib chiqamiz:

Autentifikatsiya hujumlari. ushbu toifaga foydalanuvchi nomi va paroliga hujumlar, shuningdek elektron pochta yoki SMS orqali tasdiqlash kabi boshqa autentifikatsiya usullari kiradi. Hujumlarga misollar: fishing hujumlari, parolni himoya qilish hujumlari, sessiyaga hujumlar.

Maxfiylik hujumlari. bunday hujumlarda tajovuzkor maxfiy ma’lumotlarga, masalan, foydalanuvchilarning shaxsiy ma’lumotlariga (ism, manzil, ijtimoiy ta'minot raqami va boshqalar) kirishga harakat qiladi. Hujumlarga misollar: SQL in'ektsiyalari, yashirin kirish maydonlari, sessiyalarni o‘g‘irlash.

Foydalanuvchanlik hujumlari. bunday hujumlar tizimni haddan tashqari yuklashga yoki ko‘plab so‘rovlar yordamida uni yo‘q qilishga qaratilgan. Hujumlarga misollar: DoS hujumlari, DDoS hujumlari.

Yaxlitlik hujumlari. bunday hujumlar Web-ilovadagi ma’lumotlarni o‘zgartirishga qaratilgan, masalan, ma’lumotlar bazasidan yozuvlarni qo‘shish yoki o‘chirish. Hujumlarga misollar: SQL inyeksiyalari, saytlararo so‘rovlarni almashtirish (CSRF), saytlararo skriptlar (XSS).

Infratuzilmadagi zaifliklarga qarshi hujumlar. tizim dasturiy ta'minotidagi kamchiliklar kabi Web-ilovalar infratuzilmasidagi zaifliklarga qarshi hujumlar Web-

ilovalar xavfsizligiga jiddiy ta'sir ko‘rsatishi mumkin. Hujumlarga misollar: protokollar va tarmoq xizmatlariga hujumlar, SSL va TLS hujumlari.

Web-ilovalarni hujumlardan himoya qilish uchun foydalanuvchi kiritishni filtrlash, ma’lumotlarni shifrlash, autentifikatsiya xavfsizligini ta'minlash, ko‘p darajali himoya qilish, ilovalarni muntazam yangilash va sinovdan o‘tkazish kabi ko‘plab texnologiyalar va usullardan foydalanish kerak. Web-ilovalarni xavfsiz saqlashning keng qamrovli yondashuvi ilovani har xil hujumlardan himoya qilishga yordam beradi.

Internet texnologiyalarining yaratilishi turli manbalardan tez va oson yo‘l bilan axborot olish imkoniyatlarini hamma uchun-oddiy fuqarodan tortib yirik tashkilotlargacha misli ko‘rilmagan darajada oshirib yubordi. Davlat muassasalari, fan-ta‘lim muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib-saqlay boshladilar. Bu muhit avvalgi fizikaviy saqlashga nisbatan katta qulayliklar tug‘diradi: saqlash juda ixcham, uzatish esa bir onda yuz beradi va tarmoq orqali boy ma‘lumotlar bazalariga murojaat qilish imkoniyatlari juda keng. Axborotdan samarali foydalanish imkoniyatlari axborot miqdorining tez ko‘payishiga olib keldi. Biznes qator tijorat sohalarida bugun axborotni o‘zining eng qimmatli mulki deb biladi. Bu albatta ommaviy axborot va hamma bilishi mumkin bo‘lgan axborot haqida gap borganda o‘ta ijobiy hodisa. Lekin pinhona(konfidentsial) va maxfiy axborot oqimlari uchun Internet texnologiyalari qulayliklar bilan bir qatorda yangi muammolar keltirib chiqardi. Internet muhitida axborot xavfsizligiga tahdid keskin oshdi:

- axborot o‘g‘irlash;
- axborot mazmunini buzib qo‘yish, egasidan iznsiz o‘zgartirib qo‘yish;
- tarmoqqa va serverlarga o‘g‘rincha suqulib kirish.

Tarmoqqa tajovuz qilish. Avval qo‘lga kiritilgan transaktsiya(amallarning yaxlit ketma-ketligi)larni qayta yuborish, "xizmatdan yo axborotga daxldorlikdan bo‘yin tovlash" , jo‘natmalarni ruxsat berilmagan yo‘l orqali yo‘naltirish.

Web-ilovalarga qaratilgan hujum. Yuqorida ta'kidlab o‘tilganidek, ishlab chiquvchilar Web-ilovalarni ishlab chiqish uchun server tomonidagi skript (ASP, PHP, va hokazo) va mijoz tomoni skripti (HTML, JavaScript va boshqalar) kombinatsiyasidan foydalanadilar - Web-ilovalarga hujum - bu zaifliklardan foydalanishga qaratilgan har qanday urinishdir. maxfiy ma’lumotlarga kirish, ruxsatsiz harakatlarni amalga oshirish yoki dasturning normal ishlashini buzish uchun ushbu jarayonning istalgan tomoni, mijoz yoki server.

Hujumlar tajovuzkorning Web-sahifaning URL manzilidagi ma’lumotlarni o‘zgartirishi kabi oddiy bo‘lishi mumkin, bu esa ilovadagi nosozlikni yuzaga keltirishi mumkin. Masalan, ikkita eng keng tarqalgan Web-ilova hujumlari SQL in'ektsiyasi va saytlar aroscriptdir . SQL injection ekspluatatsiyasini amalga oshirish faqat URL manzilini o‘zgartirishni o‘z ichiga olishi mumkin - bu muvaffaqiyatli ekspluatatsiyani ishga tushirish uchun bitta qo‘shimcha belgi kerak bo‘ladi. Bu xakerga ilova ustidan nazorat va server, ma’lumotlar bazasi va boshqa IT resurslariga kirish imkonini berishi mumkin.

Web ilovalarda foydalanuvchi autentifikatsiyasi har qanday tizimning muhim qismidir, chunki u cheklangan resurslar va ma’lumotlarga kirishni ta'minlaydi. Biroq, Web-ilovalarda foydalanuvchilarning autentifikatsiya xavfsizligini buzishi mumkin

bo‘lgan turli xil hujumlar mavjud. Quyida Web-ilovalarda foydalanuvchi autentifikatsiyasiga qarshi eng keng tarqalgan hujumlar keltirilgan:

Parolni qidirish hujumlari. Bu Web-ilovalarda foydalanuvchi autentifikatsiyasiga qarshi hujumning eng keng tarqalgan turi. Tajovuzkor turli xil kombinatsiyalar yordamida foydalanuvchi nomi va parolni taxmin qilishga harakat qiladi.

Fishing hujumlari. bunday hujumlarda tajovuzkorlar haqiqiy Web-ilovalarning autentifikatsiya sahifalariga o‘xshash soxta Web-sahifalarni yaratadilar. Ushbu sahifalar Foydalanuvchining Login va parolini so‘raydi va tajovuzkor ushbu ma’lumotlarga kirish huquqiga ega bo‘ladi.

Transfer hujumlari. Ushbu hujumlar foydalanuvchi ma’lumotlari himoyalanmagan aloqa kanallari orqali yuborilganda sodir bo‘lishi mumkin. Buzg‘unchi ularni ushlab qolishi va ma’lumotlarni ushlab turish vositalari yordamida foydalanuvchi hisobiga kirishi mumkin.

Koddagi zaifliklar. Kodni yaratishda ishlab chiquvchining xatolari tizimni buzish uchun tajovuzkorlar tomonidan ishlatilishi mumkin bo‘lgan zaifliklarga olib kelishi mumkin. Bunday zaifliklar, masalan, ma’lumotlar bazasiga ruxsatsiz kirish yoki parollarni etarli darajada saqlamaslik bo‘lishi mumkin.

Ushbu hujumlarning oldini olish uchun ma’lumotlarni shifrlash, ma'lum miqdordagi muvaffaqiyatsiz kirish urinishlaridan so‘ng hisoblarni avtomatik ravishda blokirovka qilish, ko‘p faktorli autentifikatsiya va boshqa xavfsizlik choralarini o‘z ichiga olgan qatlamli himoya tizimidan foydalanish kerak. Bundan tashqari, dasturni zaifliklar uchun muntazam ravishda tekshirish va tajovuzkorlar ularni ishlatishdan oldin ularni tuzatish kerak.

Saytlararo skriptlash (XSS) hujumi keng tarqalgan Web ilova hujumi bo‘lib, unda tajovuzkor mavjud vakolatli dasturga zararli kod qo‘shadi yoki kiritadi. Ular to‘g‘ridan-to‘g‘ri alohida saytni buzishi yoki u ishlaydigan barcha saytlarga birdaniga kirish uchun uchinchi tomon skriptini buzishi mumkin. Hujumlar zararli kodning boshqa Web-sayt foydalanuvchilariga yuborilishini va mijozlarga ularning maxfiy ma’lumotlarini oshkor qiluvchi zararli dasturlarni yuqtirganini ko‘rishi mumkin. DOM-ga asoslangan XSS hujumlarini aniqlash eng qiyin, chunki zaiflik server kodida emas, balki mijoz kodida, shuning uchun server hech qachon hujum sodir bo‘layotganini ko‘rish imkoniyatiga ega bo‘lmaydi.

XSS hujumlari odatda web-ilova foydalanuvchi kiritgan ma’lumotlarni Web-sahifada ko‘rsatishdan oldin uni to‘g‘ri tasdiqlamasa sodir bo‘ladi. Misol uchun, agar mahsulot sahifasidagi sharhlar yoki sharhlar bo‘limi sharhlarni ko‘rsatishdan oldin ularni to‘g‘ri sanitarizatsiya qilmasa, tajovuzkor sharhlar maydoniga zararli kodni kiritishi mumkin, bu keyinchalik sahifaga qo‘shiladi va qurbonning Web-brauzeri tomonidan amalga oshiriladi. . Bu "saqlangan" yoki "doimiy" XSS hujumi sifatida tanilgan, chunki zararli foydali yuk doimiy ravishda server tomonida saqlanadi, bu esa dasturning barcha kelajakdagi foydalanuvchilariga zararli yukni xizmat qilishiga olib keladi.

Misol uchun, tajovuzkor mahsulot sahifasining sharhlar bo‘limidagi yozuvlarni tozalamaydigan web-ilovani topishi va keyin to‘g‘ridan-to‘g‘ri Web-saytga qo‘shiladigan yozuvlarni kiritishi mumkin. Bunday holda, tajovuzkor zararli

JavaScript qatorini qo‘shishi mumkin. U yerdan zararli skript manba kodi sifatida paydo bo‘ladi va keyingi tashrif buyuruvchilarning brauzerlarida ishlaydi:

<script src="http://192.160.0.106:4444/hook.js"></script>

```
<br>
<strong>Comment:</strong>
<br>
<script src="http://192.160.0.106:4444/hook.js"></script>
<br>
<hr>
</span>
<h2 class="title-regular-2">Leave a Comment</h2>
```

1-rasm. Skripting hujumi

Endi tajovuzkor mahalliy xotirani o‘qish, cookie-fayllarga kirish, jumladan, shaxsni aniqlash ma’lumotlarini (PII) o‘g‘irlash, fishing yoki zararli dasturlarni tarqatish kabi turli hujumlarni amalga oshirish uchun skriptdan foydalanishi mumkin.

XSS hujumlarining oldini olish uchun Web-ilovalar foydalanuvchi kiritgan ma’lumotlarni Web-sahifada ko‘rsatishdan oldin uni to‘g‘ri tekshirishi va tozalashi muhimdir. Buni Web-brauzer tomonidan HTML sifatida talqin qilinmasligi uchun foydalanuvchi kiritgan <va kabi maxsus belgilarni kodlaydigan funksiyalar yordamida amalga oshirilishi mumkin .>

Content-Security-Policy Web-ilovalar uchun Web-sahifaga qaysi manbalar kontentni yuklashga ruxsat berilganligini ko‘rsatadigan sarlavhani o‘rnatish ham muhimdir . Bu tajovuzkorlarning Web-sahifaga tashqi manbalardan zararli kod kiritishining oldini olishga yordam beradi.

SQL injection hujumlari

SQL injection (SQLI) hujumi XSS hujumiga o‘xshaydi, chunki tajovuzkor Web-ilovaga zararli kodni kiritadi, lekin ushbu kodning mijoz tomonidan bajarilishini maqsad qilib qo‘yish o‘rniga, tajovuzkor o‘z kiritish maydonlari orqali backend ma’lumotlar bazasini nishonga oladi. Ushbu hujumning maqsadi kirish ma’lumotlari yoki moliyaviy ma’lumotlar kabi maxfiy ma’lumotlarga kirish yoki yozuvlarni qo‘shish yoki o‘chirish kabi ruxsatsiz harakatlarni amalga oshirish uchun ma’lumotlar bazasini manipulyatsiya qilishdir.

XSS hujumlari singari, SQL in'ektsion hujumlari Web-ilova foydalanuvchi kiritgan ma’lumotlarini to‘g‘ri tasdiqlamaganda sodir bo‘ladi. Misol uchun, foydalanuvchilarga qidiruv so‘zini kiritish maydoniga kiritish orqali ma’lumotlar bazasidagi mahsulotlarni qidirishga imkon beruvchi Web-ilovani ko‘rib chiqing. Qidiruv funksiyasi quyidagi SQL so‘rovi yordamida amalga oshirilishi mumkin:

SELECT * FROM products WHERE name LIKE '%SEARCH_TERM%';

Agar Web-ilova qidiruv so‘zini to‘g‘ri tasdiqlamasa, tajovuzkor ma’lumotlar bazasini manipulyatsiya qilish uchun kirish maydoniga zararli kodni kiritishi mumkin. Masalan, tajovuzkor quyidagi qidiruv so‘zini kiritishi mumkin:

YOKI 1=1; --

Ushbu kiritish SQL so‘rovini quyidagilarga o‘zgartiradi:

'%' YOKI 1=1 bo‘lgan mahsulotlardan * TANLANING; --%';

Olingan so‘rov jadvaldagi barcha qatorlarni qaytaradi products, chunki WHERE bandi har doim TRUE ga baholanadi . Kirish oxiridagi so‘rov asl so‘rovning qolgan qismini sharhlash uchun ishlatiladi, bu tajovuzkorning zararli kodiga xalaqit bermasligi uchun.

SQL inyeksiya hujumlarining oldini olish uchun Web-ilovalar foydalanuvchi kiritgan ma’lumotlarni to‘g‘ri tekshirishi va tozalashi muhimdir. Buni tayyorlangan bayonotlar va parametrlangan so‘rovlar yordamida amalga oshirish mumkin, bu esa ishlab chiquvchilarga SQL so‘roviga to‘g‘ridan-to‘g‘ri kiritishdan ko‘ra, foydalanuvchi kiritish uchun to‘ldiruvchini belgilash imkonini beradi.

Yo‘lni bosib o‘tish hujumlari. “Katalogdan o‘tish” hujumi sifatida ham tanilgan yo‘lni bosib o‘tish hujumi konfiguratsiya fayllari yoki jurnal fayllariga kirish uchun Web-serverdagi fayllar va kataloglarga kirishni o‘z ichiga olgan turli Web-ilova hujumidir. serverda ixtiyoriy kodni bajarish.

Yo‘lni bosib o‘tish hujumlari Web-ilova fayl yoki katalog yo‘lini belgilash uchun ishlatiladigan foydalanuvchi kiritishini to‘g‘ri tasdiqlamaganida yuzaga keladi. Misol uchun, foydalanuvchilarga fayl nomini kiritish maydoniga kiritish orqali cheklangan katalogdan fayllarni yuklab olish imkonini beruvchi Web-ilovani ko‘rib chiqing. Agar Web-ilova fayl nomini to‘g‘ri tasdiqlamasa, tajovuzkor cheklangan katalogdan tashqaridagi fayllarga kirish uchun kabi kataloglarni o‘tish belgilarini o‘z ichiga olgan fayl nomini kiritishi mumkin.

Mahalliy fayllarni qo‘shish (LFI) hujumi yo‘lni bosib o‘tish hujumining bir variantidir, bunda tajovuzkor Web-ilovani Web-serverdagi fayllarni ochish yoki ishga tushirish uchun aldaydi. Yo‘lni bosib o‘tish hujumida bo‘lgani kabi, orqa aktyor serverdagi fayllarni topish uchun kataloglar bo‘ylab harakatlanishdan foydalanadi va keyin Web-serverdan faylni ishga tushirishni taklif qiladi va keyingi hujumlar va kirishlar uchun eshikni ochadi.

Saytlararo so‘rovni qalbakilashtirish. Saytlararo so‘rovlarni soxtalashtirish (CSRF) hujumi foydalanuvchini avval autentifikatsiya qilingan Web-ilovada ko‘zda tutilmagan harakatlar qilish uchun aldashni o‘z ichiga oladi. Buzg‘unchining maqsadi qonuniy ko‘rinadigan Web-ilovaga zararli so‘rov yuborish orqali pul o‘tkazish yoki parolni o‘zgartirish kabi ruxsatsiz harakatlarni amalga oshirishdir.

Misol uchun, agar foydalanuvchi bank Web ilovasiga kirgan bo‘lsa, u foydalanuvchilarga shaklni to‘ldirish va yuborish orqali pul o‘tkazish imkonini beradi, lekin bu dastur serverda tekshirilgan shaklda noyob tokenni o‘z ichiga olmasa, tajovuzkor potentsial ravishda qonuniy shakl bilan bir xil maydonlarga ega shaklni o‘z ichiga olgan zararli Web-sayt yaratish va ijtimoiy muhandislik orqali foydalanuvchini ushbu saytga yo‘naltiradi. Agar jabrlanuvchi Web ilovaga kirsa va zararli web saytga kirsa, tajovuzkorning shakli yuborilishi mumkin, bu esa jabrlanuvchini bilmagan holda pul o‘tkazmasini amalga oshirishiga sabab bo‘lishi mumkin.

CSRF hujumlarining oldini olish uchun Web-ilovalar formalarga noyob tokenni qo‘shishi va serverdagi so‘rovlarning haqiqiyligini tekshirishi muhimdir. Buni "sinxronizator tokeni" yordamida amalga oshirish mumkin, bu server tomonidan

yaratilgan va shaklga kiritilgan noyob qiymatdir. Shakl topshirilganda, server so‘rovni qayta ishlashdan oldin tokenning haqiqiyligini tekshiradi. Bundan tashqari, sinxronizator tokenini bekor qiladigan Web-sahifalarga "chiqish" tugmachasini qo‘shish yaxshi fikr bo‘lib, uni kelajakdagi hujumlar uchun ishlatib bo‘lmaydi.

```
{% extends 'base.html' %}

{% block title %}
{{ title }}
{% endblock title %}

{% block main %}
<form action="" enctype="multipart/form-data" method="post">
    {% csrf_token %}
    {{ form.as_p }}
    <button class=" btn btn-warning" type="submit">
        Register
    </button>
</form>

{% endblock main %}
```

2-rasm. csrf_token

Ushbu rasmda *csrf_token* amaliy tarzda ko‘rsatilgan:

```
# Password validation
# https://docs.djangoproject.com/en/4.1/ref/settings/#auth-password-validators

AUTH_PASSWORD_VALIDATORS = [
    {
        'NAME': 'django.contrib.auth.password_validation.UserAttributeSimilarityValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.MinimumLengthValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.CommonPasswordValidator',
    },
    {
        'NAME': 'django.contrib.auth.password_validation.NumericPasswordValidator',
    },
]
```

3-rasm. password_validators

Parollarni soda yoki murakkablikka tekshiruvchi *password_validators.*

Foydalanilgan adabiyotlar ro‘yxati

1. Askar T. Rakhmanov, Rustam Kh. Khamdamov, Komil F. Kerimov, Shukhrat K. Kamalov, Automatic Vulnerability Detection Algorithm for the SQLInjection// Journal of Automation and Information Sciences DOI: 10.1615/JAutomatInfScien. v51.i6.60 New York, USA 7,2019. –pp.47-54. Scopus (https://www.scopus.com/sourceid/25497).

2. Ibrohimov A.R. “Веб серверлардаги заифликларни гуруҳлаш усули ва алгоритми”, “Муҳаммад ал-Хоразмий авлодлари” журнали. N 2(20)/2022. –Б. 15-22.

3. A. Büyükçakir, H. Bonab, F. Can A novel online stacked ensemble for multi-label stream classification International Conference on Information and

Knowledge Management, Proceedings, Association for Computing Machinery (2018), pp. 1063-1072.

4. R. Devi, M. Abualkibash Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets - a review paper International Journal of Computer Science and Information Technology, 11 (2019), pp. 65-80.

5. Ibrohimov A.R . Tarmoq hujumlarini aniqlash usul va algoritmlari, International conference Recent advances in intelligent information and communication technologies “ISPC-2022” Tashkent -2022, pp. 352-356.

6. Хамдамов Р.Х., Керимов К.Ф., Методы блокирования уязвимостей вида XSS на основе сервис ориентированной архитектуры // Международный научно-технический журнал ―Проблемы управления и информатики‖. – Украина, Киев 2019. – №6. – С.86-91.