VEB SAYTLARNI HIMOYALASHDA HUJUM TURLARI TADBIQI

Po'latov Doston Normurod o'g'li
Roziqov Abdug'ani Ilhomjon o'g'li
Jumaboyev Javlonbek Sherqul o'g'li
Shonazarov Sarvarbek Maqsud o'g'li

Annotatsiya

Ushbu maqola veb saytlarni himoyalashda hujum turlari shaxsiy kompyuter, yoki korporativ tizmlarga bo'ladigan hurujlarni aniqlash va ularga qarshi chora tadbirlarining samarasini oshirish.

Kalit so'zlar: tarmoq, korporativ tarmoq, virtual tarmoq,ma'lumotlar bazasi, xavfsizlik,himoya,kompaniya,reklama,hujum

Abstract

This article protects websites from types of attacks on personal computers or corporate systems identification of future outbreaks and the effectiveness of measures against them increase

Keywords: network, corporate network, virtual network, database, security, protection, company, advertising, attack

Zamonaviy texnologiyalar keskin rivojlanish cho'qqisiga chiqmoqda. Internet saytlar hayotimizning ajralmas bir qismi bo'lib kelgan, bu istisno emas, buni rad ham etolmaymiz. Aslida, dunyodagi deyarli har bir tashkilotning Internetda veb-sayti bor, tarmoq orqali esa bu saytlarni osonlik bilan himoyasini buzish va tajovuz qilish mumkin.

Bugungi kunning eng dolzarb muammolari ham veb saytlarni turli hujumlardan himoya qilish maslasidir. Tarmoqning rivojlanishi davlatlarning rivojlanishiga ham katta turtki bo'ldi, chunki bu davlatlardagi barcha sohalarida zamonaviy texnologiyalar turli kompaniyalar va firmalarni boshqaruvida va rivojlanishida maxsulot sifati va reklamasiga bog'liq. Bunday ommabob reklamalar aynan veb saytlar orqali amalga oshiriladi.Agar bunday tarmoq reklamalari bo'lmasa kompaniya, firma yoki oliy ta'lim muassasida rivojlanish bo'lmaydi. Veb saytlar orqali reklama bu eng ko'p foyda beradigan usuldir, ammo bu saytlarga kuchli himoya tizimlari o'rnatilmasa yoki kuchliroq himoya qilinmasa buzg'unchilar tomonidan reklamamiz buzilishi yoki o'zgartirilishi mumkin. Buning uchun bu saytlarni kiber jinoyatchilaridan himoya qilish va uning yangi algaritmlarini, usullarini va dasturlarini ishlab chiqish lozim va hozirgacha ham ba'zi ishlab chiqilganlari mavjud. Internet olamidagi Veb saytlar uch holatda bo'ladi. Bular quyidagilar:

1. Allaqachon hujum ta'sirida ishdan chiqqan Veb saytlar.

2. Yaxshi ishlaydigan ammo himoyaga muhtoj Veb saytlar.
3. Juda zo'r ishlaydigan hujmlarga qarshi himoyalangan Veb saytlar.

▪Birinchi holatdagi veb saytlar turli xil hujumlar asosida o'z holatini yo'qogan va kichik korxonalarga tegishli bo'lgan veb saytlar.

▪Ikkinchi holatda o'rtacha himoyalangan ammo himoyani yana kuchaytirishi lozim bo'lgan va yaxshi rivojlanib borayotgan katta va o'rta korxonalarning veb saytlar

▪Uchinchi holatda kuchli himoyalangan va himoyaga bardoshli bolgan yirik va kuchli korxonalarning veb saytlari.

Aslida hujumlarga ayniqsa berilgan parametrlarini va paroldan foydalanishdagi kamchiliklar, dasturiy ta'minotning kamchiliklari yoki tizim rahbarlarining oddiy xatolari, ma'lumotlar bazasini o'rnatishdagi qisman xatolar va shu kabi ko'plab zaifliklar sabab bo'ladi. Bunday zaifliklarni aniqlash va ularni yaxshilash Ochiq Veb sayt xavfsizligi loyihasi ishlab chiqilgan. Veb saytlarda xavfsizlik, dasturiy ta'minotning tahlilini va veb saytlarni yaxshilashga qaratilgan xalqaro nodavlat notijorat tashkilot hisoblanadi. Bu maqolada biz oliy ta'lim muassalaridagi Vebga asoslangan saytlar, va ularni himoya qilish usullarini, hujum vektorlarining har bir bilan yaqindan tanishib chiqamiz. Bizning qator doiradagi amaliy ishlarimiz, real ish misoli ustida xavf darajasi usullarini, shuningdek amaliy usullarni, Vebga asoslangan dasturlar va vebga asoslangan xizmatlarni himoya qilish uchun ilmiy ish olib boryapmiz.

Vebga asoslangan saytlar uchun 5 ta eng xavfli hujum turini ajaratib chiqdik. Endi o'sha beshta xavfli hujum turlari bilan tanishsak.

1.Ma'lumotlar bazasiga qilinadigan hujumlar. Hammamizga ma'lum barcha ma'lumotlar odatda maxsus ma'lumotlar bazasida saqlanadi. Ma'lumotlar ko'pincha maxsus so'rovlar tili SQL tilida yozilgan so'rovlar shaklida qurilgan bo'ladi. Agar siz shaxsiy foydalanuvchi ma'lumotlarini tahrirlash, ma'lumotni olish va kiritish, o'zgartirish yoki ma'lumotlarni o'chirish uchun SQL-so'rovlar tilidan foydalanib Veb saytimiz shaklni to'ldirib hiqamiz. Buning uchun esa SQL-so'rovlar tilini maxsus kodlaridan foydalanish mumkin. Misol uchun shunga o'xshash kod:

$sql = "SELECT * FROM users WHERE username=\'$username\' AND password=\'$password\';";

SELECT * FROM users WHERE username='' OR '1'='1' AND password='' OR '1'='1'; Undan tashqari PHP kodlarini ham misol qilishimiz mumkin.

```
$yourName = $_GET['name'];
exec("echo $yourName");
```

SQL-Injection - Ushbu hujum turi eng keng tarqalgan bo'lib ma'lumotlar

bazasiga qilinadigan hujumdir. SQL-Injection bu xavfli hujum bo'lib ma'lumotlar bazasi va undagi ma'lumotlarni o'chirish uchun tajovvuzkorlar tomonidan amalga oshiriladi.Misol uchun ismi familiyangiz bilan birga sizning hisob balansingizni o'zgartirish va nozik shaxsiy ma'lumotlarni o'g'irlash, hisobda boshqa muvozanatini joylashtirib qo'yishi mumkin. Bularga qarshi esa yangi algaritmlar ishlab chiqilmoqda.

2.Aniqlikni yo'qotish va boshqaruvni qo'lga olish. Boshqa bir foydalanuvchi ajratish maqsadida veb saytimizda qo'shimcha foydalanuvchi qo'shishimiz mumkin. Boshqa qo'shgan foydalanuvchimiz ham saytimizga ma'lumot yoki qo'shimchalar qo'shishi yoki o'zhartirishi mumkin. Bu foydalanuvchi ham o'z login va paroli orqali saytimizga kiradi. Bu login va parolni kiritgan paytda ular aniq serverdagi ma'lumot orqali tekshiriladi. Buzg'unchilar xuddi shu server orqali login parollarni bilib foydalanuvchi kabi saytimizga kirishi mumkin.Saytimizga xuddi shunday bir necha ulanishlar bir paytning o'zida hosil qilinadi shuning uchun IP-manzilni brauzerda saqlab so'ngra ma'lumotlarni o'zgartirib ma'lumotlar aniqligini buzishlari mumkin. Bunda onlayn bank, hisob yoki to'lov tizimi bo'lsa, bunday ruxsatsiz foydalanish oqibatlari juda ayanchli bo'ladi.

3. JavaScript yoki HTML kodlari orqali hujum qilish. Cross Site Scripting – JavaScript kodi orqali foydalanuvchi brauzeriga hujum qilinishi imkonini beradi. Foydalanuvchi ma'lumotlarni tekshirishi davomida xatoliklarni vujudga keltiradi. Ushbu turdagi hujumlar ko'pincha ularni amalga oshirish mexanizmi SQL-Injectionga juda o'xshash, chunki HTML-kodlarida ham shu kabi o'xshashliklar mavjud.Ammo farqli o'laroq foydalanuvchi brauzerida ijro kodni aynan ikkinchisi amalga oshiradi.

- Birinchidan,tajovvuz qilish oson, ma'lumotlar osonlikcha o'g'irlanishi mumkin. Bu barcha dasturlar orqali serverlarga hujum qilganda zaif ekanini ta'kidlash lozim.
- Ikkinchidan, u zararlangan sahifa shaklida kirgan ma'lumotlarni o'g'irlagan bo'lishi mumkin. Va yomon va nozik tomoni shundaki shaxsiy ma'lumotlarni yoki CVC-kodi bilan kredit karta ma'lumotlar o'g'irlanishi mumkin.
- Uchinchidan, JavaScript orqali, siz sahifada joylashgan ma'lumotlarni o'zgartirishingiz mumkin, masalan ba'zi kodlar va modellarining o'rniga bir tajovuzkor yoki bankdan pul o'tkazish uchun ma'lumotlarni o'g'irlashi mumkin.

4. Xatarli ob'ektlarni kiritish. Xavf xatarning bu turi ham foydalanuvchi ma'lumotlarining etarli aniqlash natijasidir. Uning mohiyati shundaki brauzeringizga tahdid matn ichida uzatiladi va ob'ektlar uchun tasdiq erkin foydalanish huquqlarini amalga oshiradi. Bunday ob'ekt identifikatori kirish uchun maxsus xabarlar, yoki indeks kartalari mijozlarga sifatida har qanday nozik ma'lumotlarni qaytarishda ishlatiladi.

5. Xavfli konfiguratsiya. Veb server, ma'lumotlar bazasi serveri va platforma o'z dastur komponentlarini ya'ni Vebga asoslangan saytlar infratuzilma komponentlarini xavfsiz konfiguratsiyani talab qiladi. Har xil sozlamalar server qismlariga ko'pincha xavfli va hujum imkoniyatlarini ochib beradi. Misol uchun, JavaScript orqali hujum ya'ni XSS-hujum tufayli faqat http sozlamalari yo'qotilishi mumkin. Server to'g'ri tuzilgan bo'lsa va imkoniyat http yoki faqat JavaScript kodlari orqali hujum qilinishi mumkin, lekin tez-tez bu oddiy va muhim sozlama to'lov tizimlari xususiy ofislaridagi kabi tanqidiy muhim hujumlardan biri bo'lib qoladi. Serverda IP-manzil mavjud va ishlab chiqaruvchi oldindan o'rnatgan paroldan foydalanishingiz mumkin. Bu bir hujumni oson turi bo'lib, osonlik bilan ma'lumotlarni o'zgartirish imkonini beradi.

Ayrim hollarda Web-sayt bilan birgalikda taqdim etiladigan bazaviy ma'muriy interfeys ishlab chiqaruvchilar nazarda tutmagan maqsadlarda qo'llanilishi mumkin. Masalan, Macromedia'sColdFusion kelishuvga binoan ssenariylarning boshlang ich kodini ko rib chiqishga imkon beradi. Bu funksiyani suiste'mol qilish Web-sayt tomonidan kritik axborotning olinishiga olib keoali. Bu funksiyani o chirish yoki o chirish muammo tug diradi, chunki saytning muhim tashkil etuvchilari unga bog liq bo ladi. Smartwin Cyber Office da narxni o zgartirish Ayrim hollarda sayt tomonidan qayta ishlanuvchi ma'lumotlarni o'zgartirish dastuming hatti-harakatini o zgartirish imkonini beradi. Masalan, CyberOffice saytda xarid qilish funksiyasidagi kamchilik foyalanuvchiga HTML-formaning yashiringan maydonida uzatiladigan narx qiymatini o zgartirishga imkon bergan edi. Buyurtmani tasdiqlash sahifasi g araz niyatli kishi tomonidan yuklatildi, mijozda o'zgartirildi va serverga o zgartirilgan narx qiymati bilan uzatilar edi.

Zaifliklarning yillar davomida keskin ravishda ortib borishi xususan so nggi yillarda web saytlarning zaifligi turli tipidagi tahdidlarni ko'payishiga olib kelmoqda. Ularni himoyalashda himoya tizimlarini o'rnatishni taklif qilamiz. Biz aynan shu tahdidlarga qarshi chora tadbirlarni va dasturlarni yaratyapmiz.

FOYDALANILAGAN ADABIYOTLAR:

1. Петренко С.А. "Управление информационными рисками компании" Экспресс-электроника-2002.
2. Karen S., Peter M. "Guide to Intrusion Detection and Prevention systems(IDPS)" - 2007.