XSS, CROSS SITE SCRIPTING VA UNDAN HIMOYALANISH

Qurbonmurodov Diyorbek Ulug'bek o'g'li
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti talabasi

Annotatsiya: Ushbu maqolada veb-saytlararo XSS, cross site scripting holatlari haqida ma'lumot berish, aniqlash va oldini olish choralarini ko'rib chiqildi.

Kalit so'zlar: XSS, cross site scripting, zaiflikni skanerlash vositlari, reflected scripting, persistent scripting, XSStrike, XSS hunter, WAF, kiritishni tasdiqlash, chiqishni kodlash.

Hozirgi kunda veb-saytlar insonlarning kundalik yumushlarida muhim ahamiyat kasb etadi. Biz veb-saytlar orqali o'zimizga kerakli ma'lumotlarni olishimiz, biron-bir faoliyat haqida yoritib borishimiz, o'zimiz ijod mahsullarimizni ulashishimiz, ma'lum bir sohani online o'rganishimiz mumkin.

Texnologiyalar rivojlangani sari insonlarning ham o'z ehtiyojlarini uydan chiqmasdan turib, masofaviy amalga oshirishga harakat qilishlari ham kuchaymoqda. Bunda albatta veb-saytlarga murojaat qilishga to'g'ri keladi. Bu ixtiyoriy ko'rinishda bo'lishi mumkin. Masalan internet orqali online xarid qilishimiz yoki biror sayohat qilmoqchi bo'lgan hududlaringiz haqida ma'lumot olishingiz, urf-odatlari bilan yaqindan tanishishingiz mumkin. Shu sababli ham veb-saytlarning hayotimzidagi o'rni shiddat bilan o'sib bormoqda va katta ahamiyat kasb etmoqda. Bu sohaning rivojlangani sari biz uchun qulayliklar yaratilyapti, kundan kunga ijtimoiy hayotni yengillashtirishga qaratilgan ximatlar yaratilmoqda va tatbiq etilmoqda. Shu bilan bir qatorda biz yangidan yangi ko'rinishdagi firibgarlik faoliyatlariga duch kelmoqdamiz va bu ba'zi jamoa, tashkilot yoki inson uchun katta talofatlar olib kelishi ham mumkin.

Biror bir soha rivojlanishi bilan birga buzg'unchilarning ham shu soha doirasidagi faoliyati keygayishi birgalikda kechadi. Chunki buzg'unchilar iloji boricha ko'proq foyda olishga intiladi. Veb-saytlardan foydalanishga bo'lgan talabni ortishi bilan veb-saytlarning faoliyatini tashkil etayotgan shaxs yoki shaxslar jamoasi turli xil yangidan yangi noqulayliklarga duch kelyapti. Shulardan biri bu cross-siting hujumlaridir. Bu hozirda aktual voqealardan hisoblanib, omma oldida turgan va e'tibor qaratilishi muhim bo'lgan muammolardan biri hisoblanadi. Shu sababli biz hozirda bu muammoli holatdan ogoh bo'lishimiz, yetarlicha nazariy va amaliy ko'nikmalarga ega bo'lishimizva bu

holatlarga duch kelmaslik yokida duch kelgan taqdirda qay tarzda harakatlarni amalga oshirishimiz kerakligi haqida ma’lumotlarga ega bo’lishimiz kerak.

*Veb-say*t ko'plab veb-sahifalar to'plamidir va veb-sahifalar HTML (HyperText Markup Language) yordamida yozilgan raqamli fayllardir.

Veb-saytning veb-sahifalari giperhavolalar va gipermatnlar bilan bog'langan va umumiy interfeys va dizaynga ega. Veb-sayt shuningdek, rasmlar, videolar yoki boshqa raqamli aktivlar kabi qo'shimcha hujjatlar va fayllarni o'z ichiga olishi mumkin[1].

Veb-saytlarning ommalashuvi buzg’unchilarning ham e’tiborini tortmasdan qolmayapti. Veb-saytlar orqali amalga oshiriladigan firibgarliklar ham kun sayin oshib bormoqda. Kiber jinoyatchilar veb-saytlarda kiber jinoyatlarni amalga oshirish uchun keng ko'lamli usullardan foydalanadilar. Veb xavfsizligiga tahdidlarning eng keng tarqalgan turlaridan ba'zilari[2]:

Fishing;

DDOS;

XSS;

Ransomware;

SQL injection;

Saytlararo skriptlash hujumlarining ikkita asosiy ko’rinishi mavjud[3]:

-reflected cross site scripting;

-persistent cross site scripting;

Reflected cross site scripting - Bu eng ko'p uchraydigan saytlararo skript hujumidir. Ko'rsatilgan hujum bilan zararli kod veb-sayt url oxiriga qo'shiladi; ko'pincha bu qonuniy, ishonchli veb-sayt bo'ladi. Jabrlanuvchi ushbu havolani veb-brauzeriga yuklaganida, brauzer url-ga kiritilgan kodni bajaradi. Tajovuzkor odatda jabrlanuvchini havolani bosish uchun aldash uchun ijtimoiy muhandislikning qandaydir shakllaridan foydalanadi.

Misol uchun, foydalanuvchi o'z bankidan kelganligini da'vo qiladigan qonuniy ko'rinishdagi elektron pochta xabarini olishi mumkin. Elektron pochtadan bank veb-saytida ba'zi choralar ko'rish va havolani taqdim etish so'raladi. Havola quyidagicha ko'rinishi mumkin:

http://aloqabank.uz/index.php?user=<script>zararli kod!</script>

Garchi urlning birinchi qismi xavfsiz ko‘rinsa va ishonchli veb-sayt domenini o‘z ichiga olgan bo‘lsa-da, url oxiriga kiritilgan kod zararli bo‘lishi mumkin.

Persistent(doimiy) saytlararo skript (XSS) hujumining bir turidir. XSS hujumlari inyeksiyaning bir turi bo'lib, unda zararli skriptlar xavfsiz va ishonchli veb-saytlarga kiritiladi. XSS hujumlari tajovuzkor veb-ilovadan zararli kodni, odatda, brauzer tomoni

skripti shaklida boshqa oxirgi foydalanuvchiga yuborish uchun foydalanganda sodir bo'ladi.

Doimiy XSS hujumlari - bu kiritilgan skript doimiy ravishda maqsadli serverlarda, masalan, ma'lumotlar bazasida, xabarlar forumida, tashrif buyuruvchilar jurnalida, sharhlar maydonida saqlanadigan hujumlardir. Zararli kiritilgan skript keyinchalik veb-sahifalarda va doimiy ravishda saqlanadi. skriptni o'z ichiga olgan veb-sahifaga kirgan har qanday foydalanuvchiga qaytariladi[6].

Saytlararo skript hujumlari xakerlar zararli skriptlarni jabrlanuvchining brauzeriga kiritish uchun xavfli veb-ilovalarni tekshirish va kodlash amaliyotidan foydalanganda ro'y beradi, bu esa hisobni egallab olish, zararli veb-saytga yo'naltirish yoki boshqa zararli faoliyatga olib kelishi mumkin.

Saytlararo skript (XSS) zaifliklari juda keng tarqalgan va o'z veb-saytlari va veb-ilovalariga bog'liq bo'lgan tashkilotlar o'z aktivlarini va brend obro'sini xavfsiz saqlash uchun kiberxavfsizlik va xavfsiz kodlash amaliyotiga ustuvor ahamiyat berishlari kerak. XSS hujumlari zararli skriptlar bilan to'la zararsiz ko'rinadigan veb-sahifalarni qoldirishi mumkin, bu esa halokatli oqibatlarga va mijozlarga zarar etkazishi mumkin.

Veb-ilovalaringizni himoya qilish uchun muntazam zaifliklarni skanerlash, HTTP-faqat cookie-fayllar, chiqishdan chiqish va foydalanuvchi kiritishini tekshirish kabi proaktiv choralarni ko'ring. XSS hujumlari bir necha usulda sodir bo'ladi va o'zgaruvchilarni tekshirish, chiqish kodlash va HTMLni tozalash xavfsizlikni kuchaytirishga yordam beradi.

Xavfsiz va foydalanuvchilar uchun qulay veb-saytni saqlash uchun DOMPurify kabi ishonchli kutubxonalarga tayanish uchun kodingizni qayta tahrirlang. XSS hujumining oldini olish va veb-ilovalar xavfsizligini birinchi o'ringa qo'yish foydalanuvchilar xavfsiz tajribaga ishonishlari mumkinligini bilib, ularga ishonch uyg'otadi.

Saytlararo skript keng tarqalgan, ammo murakkab hujum vektori bo'lib, uni tuzatish qiyin. Biroq, ba'zi eng yaxshi kiberxavfsizlik amaliyotlariga rioya qilish orqali siz ilovangizni himoya qilishingiz va saytlararo skript hujumining oldini olishingiz mumkin . Bu shunchalik keng tarqalgan muammoki, DevSecOps rollari har qachongidan ham mashhur bo'lib bormoqda.

Bu yerda biz saytlararo skript hujumining oldini olishning ba'zi usullarini muhokama qilamiz.

Tasdiqlash. Muvaffaqiyatli XSS hujumi tajovuzkor veb-sahifaga zararli kodni kiritganda sodir bo'lganligi sababli, XSS hujumlaridan himoyalanishning eng yaxshi usullaridan biri har bir kirishni qabul qilingan nuqtada tekshirishdir .

Bunga misol, agar foydalanuvchi nomi elektron pochta manzili formatida bo'lishi kerak bo'lsa, kiritish qiymati elektron pochta manzili uchun kutilgan belgilarni o'z ichiga olishi kerak.

Manbada kiritilgan ma'lumotlarni tekshirish orqali siz ilovangizni buzishga bo'lgan istalmagan urinishlarni bloklashingiz va faqat to'g'ri tuzilgan ma'lumotlar orqali o'tishini ta'minlashingiz mumkin.

Chiqish kodlash - bu o'zaro skript hujumidan himoya qilishning yana bir usuli. Bu brauzer ma'lum belgilarni kod sifatida talqin qilmasligini ta'minlash uchun HTML-da ko'rsatishdan oldin kirishlarni kodlashni o'z ichiga oladi.

Kodlash foydalanuvchi hissalari skriptlar sifatida bajarilmasdan, oddiy matn sifatida talqin qilinishini ta'minlaydi[4].

Zaifliklarni skanerlash vositalari , kirishni tekshirish vositalari va veb-ilovalar xavfsizlik devorlari ham XSS hujumlarining oldini olishga yordam beradi va veb-saytingizni buzib tashlashdan saqlaydi.

Zaifliklarni skanerlash vositalari veb-ilovalar, tarmoqlar va tizimlardagi xavfsizlik zaif tomonlarini aniqlaydi va baholaydi. Ular kod va kirishlarni skanerlaydi, potentsial zaifliklarni aniqlaydi va ularni tuzatish uchun ishlab chiquvchilar, IT va xavfsizlik guruhlariga xabar qiladi.

XSStrike
XSS hunter
XSSER
Acunetix
Intruder
Dalfox

Veb-ilovaning xavfsizlik devori (WAF) - bu veb-ilovaga yetib borgunga qadar zararli trafikni kuzatuvchi, filtrlaydigan va bloklaydigan xavfsizlik moslamasi. U XSS va SQL in'ektsiyasi kabi hujumlarni aniqlab, blokirovka qiluvchi darvozabon vazifasini bajaradi. WAFs, shuningdek, trafikni faol tahlil qilish va zararli so'rovlarni bloklash orqali real vaqt rejimida himoya qilishni ta'minlaydi.

Akamai App va API Protector
AppTrana
AWS WAF
Cloudflare WAF
Imperva WAF

Xulosa

Saytlararo skript (XSS) zaifliklari juda keng tarqalgan va o'z veb-saytlari va veb-ilovalariga bog'liq bo'lgan tashkilotlar o'z aktivlarini va brend obro'sini xavfsiz saqlash uchun kiberxavfsizlik va xavfsiz kodlash amaliyotiga ustuvor ahamiyat berishlari kerak. XSS hujumlari zararli skriptlar bilan to'la zararsiz ko'rinadigan veb-sahifalarni qoldirishi mumkin, bu esa halokatli oqibatlarga va mijozlarga zarar etkazishi mumkin.

Veb-ilovalaringizni himoya qilish uchun muntazam zaifliklarni skanerlash, HTTP-faqat cookie-fayllar, chiqishdan chiqish va foydalanuvchi kiritishini tekshirish kabi proaktiv choralarni ko'ring. XSS hujumlari bir necha usulda sodir bo'ladi va o'zgaruvchilarni tekshirish, chiqish kodlash va HTMLni tozalash xavfsizlikni kuchaytirishga yordam beradi.

Xavfsiz va foydalanuvchilar uchun qulay veb-saytni saqlash uchun DOMPurify kabi ishonchli kutubxonalarga tayanish uchun kodingizni qayta tahrirlang. XSS hujumining oldini olish va veb-ilovalar xavfsizligini birinchi o'ringa qo'yish foydalanuvchilar xavfsiz tajribaga ishonishlari mumkinligini bilib, ularga ishonch uyg'otadi.

Foydalanilgan adabiyotlar.

1. https://www.geeksforgeeks.org/what-is-a-website/
2. https://www.fortinet.com/resources/cyberglossary/web-security-threats
3. https://www.cloudflare.com/learning/security/threats/cross-site-scripting/
4. https://www.codemotion.com/magazine/cybersecurity/cross-site-scripting-attack/