MAXKAMOV Anvarjon Abdujabborovich
O‘zbekiston xalqaro islomshunoslik akademiyasi Zamonaviy axborot-kommunikatsiya texnologiyalari kafedrasi dotsenti, PhD
mahkamovanvar2020@gmail.com

WEB SAYTLARDAGI TAHDIDLARNING DARAJALAR BO‘YICHA TASNIFLANISHI

КЛАССИФИКАЦИЯ УГРОЗ ВЕБ-САЙТОВ ПО УРОВНЮ

CLASSIFICATION OF WEBSITE THREATS BY SEVERITY LEVELS

Annotatsiya. *Ushbu maqolada axborot xavfsizligini ta’minlashda web saytlardagi tahdidlarning darajalar bo‘yicha tasniflanishi keltirib o‘tilgan. Ayni vaqtga kelib web saytlardagi tahdidlarning darajalar bo‘yicha tasniflanishini aniqlashdan nima maqsad va tahdidlarning oldini olish bo‘yicha qanday ishlarni amalga oshirish zarurligi haqida qisqacha ma’lumotlar keltirib o‘tilgan. Bundan tashqari web saytlarga bo‘ladigan tahdidlar turlari va subyektlari, axborot xavfsizligi konsepsiyasining tuzilishi haqida ma’lumotlar keltirib o‘tilgan.*

Kalit so‘zlar: *tarmoq, filtr, axborot xavfsizligi, trafik, server, tarmoqni boshqaradigan qoidalar, tarmoq siyosati.*

Аннотация. *В данной статье представлена классификация угроз на веб-сайтах по уровням в контексте обеспечения информационной безопасности. Кратко изложены цели определения данной классификации, а также описаны необходимые меры, которые следует предпринять для предотвращения угроз. Кроме того, приведена информация о типах и субъектах угроз для веб-сайтов и о структуре концепции информационной безопасности.*

Ключевые слова: *сеть, фильтр, информационная безопасность, трафик, сервер, правила управления сетью, сетевая политика.*

Abstract. *This article presents a classification of threats on websites according to their levels in the context of ensuring information security. The purpose of determining this classification of threats and the necessary measures that must be taken for threat prevention are briefly described. Furthermore, information is provided on the types and subjects of threats to websites, as well as the structure of the information security concept.*

Keywords: *network, filter, information security, traffic, server, network management rules, network policy.*

KIRISH

Web saytlarning axborot xavfsizligiga tahdid manbalari tasodifiy yoki oldindan ko‘zlangan bo‘lishi mumkin. Dastur ta’minotidagi kamchiliklar, texnik vositalarning nosozligi, malakaning yetishmasligi yoki foydalanuvchining xatolari tasodifiy tahdidlar hisoblanadi. Oldindan ko‘zlangan tahdidlar esa axborot zaxiralariga zarar yetkazish maqsadida atayin amalga oshiriladi. Ular faol (aktiv) va nofaol (passiv) bo‘ladi. Nofaol tahdidlarga axborot zaxiralaridan ularning vazifalariga ta’sir ko‘rsatmagan holda ruxsat berilmagan foydalanishga bo‘lgan intilishlar kiradi. Texnik va dastur vositalariga, axborot zaxiralariga ta’sir qilish yo‘li bilan tizimning mo‘tadil faoliyatini buzishga qaratilgan tahdidlar faol tahdidlar hisoblanadi.

Tajribadan ma’lumki, xavfni bartaraf etishning eng oson yo‘li, shu xavfni oldindan aniqlab, unga qarshi ehtiyot choralarini qo‘llash hisoblanadi. Shu nuqtai nazardan, axborot xavfsizligini ta’minlash borasida ham sohaga nisbatan potensial tahdid manbalarini aniqlash va himoya choralarini qo‘llash birlamchi vazifalardan hisoblanadi.

ASOSIY QISM

Web saytlar axborot xavfsizligiga tahdid manbalari ichki va tashqi manbalarga bo‘linadi. Mutaxassislarning e’tirof etishicha, axborot xavfsizligining dolzarb muammoga aylanishiga asosan tashqi manbalar sabab bo‘lgan. Chunki, bugun zamonaviy dunyoga egalik qilish uchun kurashning asosiy vositasi sifatida axborot tilga olinmoqda. Bunday vaziyatda axborot texnologiyalari va axborot boshqaruvi yuksak darajada taraqqiy etgan davlatlar o‘zidagi bu ustunlikdan ijtimoiy ongga ta’sir ko‘rsatish yo‘lida foydalanishdan tom ma’noda manfaatdor hisoblanadi.

Axborot xavfsizligiga tahdidning tashqi manbalari:

– Chet el josuslik va maxsus xizmatlarining faoliyati;

ISSN 2181-9572

– Chet el ommaviy axborot va global kommunikasiya vositalari;

– Xalqaro guruhlar, tuzilmalar va alohida shaxslarning noqonuniy harakatlari;

– Axborot tarqatish va foydalanish bo‘yicha xorijiy davlatlar siyosatining amalga oshirilish;

– Tabiiy ofatlar va fojealar.

Axborot xavfsizligiga tahdidning ichki manbalari:

– Siyosiy, iqtisodiy va jamoat tashkilotlarining, alohida shaxslar va guruhlarning axborot to‘plash, tarqatish va foydalanish sohasidagi noqonuniy faoliyatlari;

– Axborot sohasida fuqarolar va tashkilotlar huquqlarining buzilishiga olib keluvchi davlat tizimlarining qonuniy harakatlari va ko‘zda tutilmagan xatolari;

– Axborot tizimlarining dasturiy-texnik vositalarining bazaviy texnologiyalarini yaratish, sinash va ishlab chiqarish bo‘yicha mahalliy sanoatning talab darajasida emasligi kabi hususiyatlar shular jumlasidandir.

Axborot makonining vujudga kelishi nafaqat uni bo‘lib olish, balki unda kechayotgan jarayonlarni nazorat qilish va boshqarishni hoxlovchi tomonlarning paydo bo‘lishiga olib keldi. Bu guruhlarning kurash vositasi ham aynan axborot qurolidir. Tahlilchilar axborot quroli deganda odamlarga ruhiy ta’sir ko‘rsatadigan va ularning ustidan nazorat qilish imkonini beruvchi vositalarni, kompyuter viruslarini, mantiqiy bomba, telekommunikasiya tarmoqlarida axborot almashinuvini bostiruvchi moslamalarni, davlat va harbiy sohalarni boshqarishda axborotlarni soxtalashtirish kabi harakatlarni nazarda tutishadi.

Axborot xavfsizligiga nisbatan tahdidlarning asosiy ta’sir vositasi bir martalik tashviqot aksiyalari, uzoq muddatli targ‘ibot kampaniyalari, mafkuraviy tazyiq, madaniy ekspansiya, axborot blokadasi kabi ruhiy-informatsion ta’sir vositalari hisoblanadi[1].

Axborot xavfsizligini ta’minlashda qandaydir zaiflik vujudga kelsa, foydalanuvchilar tomonidan tahdidlar amalga oshirilishi mumkin. Ushbu tahdidlar natijasida, xalq xo‘jaligi tarmog‘iga kattagina zarar yetkazish mumkin. Quyidagi jadvalda (1-jadval) amalga oshirilishi mumkin bo‘lgan ayrim tahdidlar ifoda etilgan .

1-jadval

Tahdid turlari va subyektlari[2]

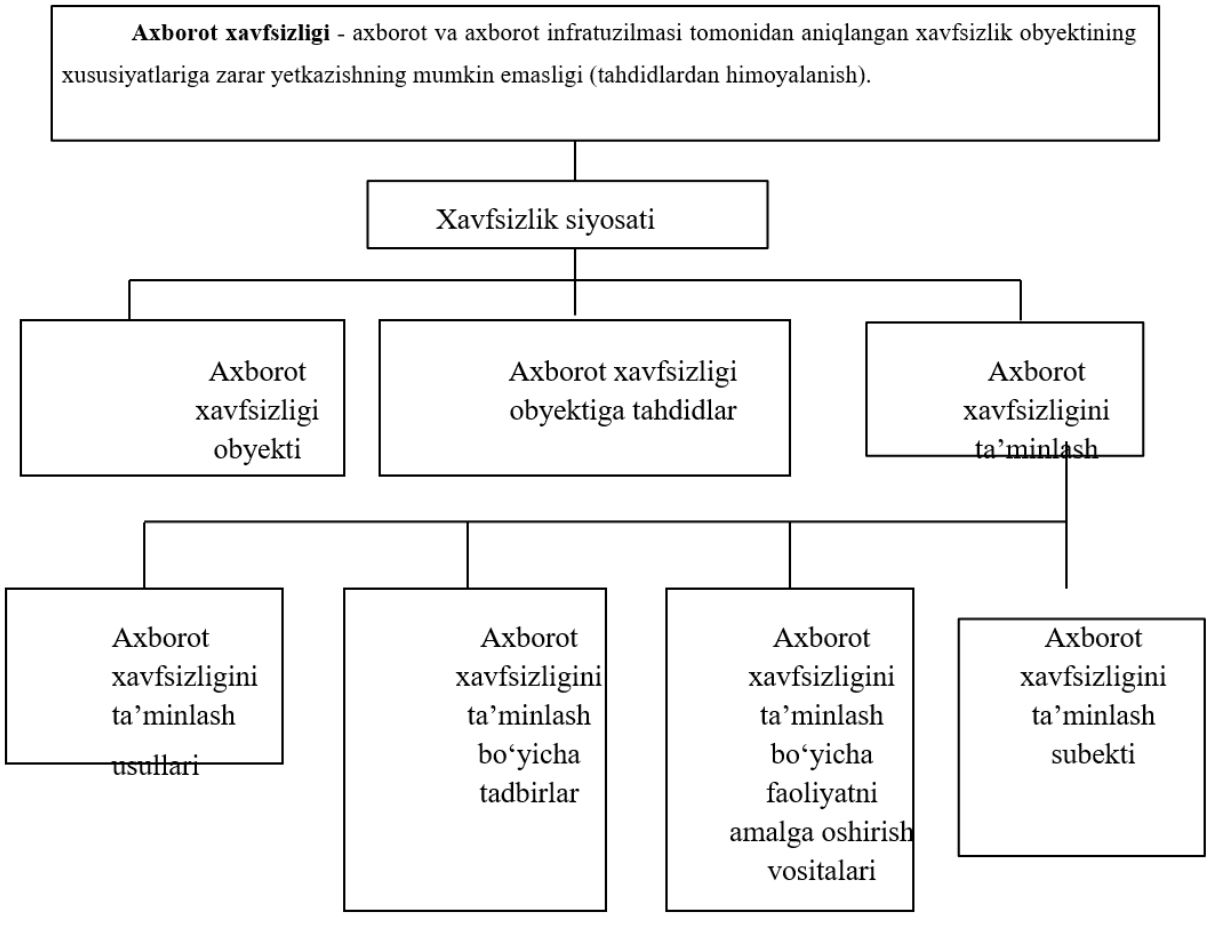
	Tahdidlar turlari	Operator	Boshliq	Dasturchi	Injiner (texnik)	Foydalanuvchi	Raqo-batchi
1	Kodlarni o‘zgartirish	+		+			
2	Fayllarni ko‘chirish	+		+			
3	Fayllarni yo‘q qilish	+	+	+		+	+
4	Dasturlarni o‘zlashtirib olish			+	+		+
5	Shpionaj	+	+	+			+
6	Yashirincha kuzatish			+	+		+
7	Sabotaj	+		+	+		+
8	Ma’lumot-larni sotish	+	+	+		+	+
9	O‘g‘irlik		+	+		+	+

Nafaqat web saytlarda, balki umuman olganda barcha axborot tizimlarida axborot xavfsizligi konsepsiyasining tuzilishi muhim ahamiyatga egadir. Quyidagi rasmda (1-rasm) axborot xavfsizligi konsepsiyasining sxematik tuzilishi ifodalangan.

Ushbu sxemadan xulosa qilish mumkun-ki, web saytlar axborot xavfsizligini ta’minlash, uning xavfsizlik siyosati amalga oshirish bosqichma bosqich amalga oshiriladi.

[1] https://nargis.uz/?p=197

[2] Jadval muallif tomonidan ishlab chiqilgan.



1- rasm. Axborot xavfsizligi konsepsiyasining tuzilishi[1]

[1] Muallif tomonidan ishlab chiqilgan.

Web saytlar xavfsizligi jamoatchilikka qarashli mavjud shaxsiy va tashkilot web saytlarini kiber hujumlardan himoya qilishni ifodalaydi.

Ommaviy web saytlarga kiberhujumlar hajmi, kelib chiqishi va tasnifidan qat'iy nazar bugungi kunda juda keng tarqalgan bo'lib, bunday hujumlar aksariyat hollarda quyidagi muammolarni keltirib chiqaradi:

– web saytni buzish;

– web sayt mavjudligini yashirish va xizmat ko'rsatishni rad etish (DoS) holatini yuzaga keltirish;

– maxfiy mijozlar va tashkilot nomlarini buzish yoki soxtalashtirish;

– hujumchi butun sayt faoliyatini o'z nazorati ostiga olishi yoki web saytdan hujumlarni amalga oshirish uchun asosiy qurol sifatida foydalanishi;

Ushbu hujumlarning bari axborot xavfsizligi tamoyillariga sezilarli ta'sir qilib, axborot xavfsizligining asosiy xususiyatlaridan hisoblangan yaxlitlik, konfedensiallik va foydalanuvchanlik tushunchalarini izdan chiqaradi. Natijada, web sayt va uning egasi obro'siga sezilarli ta'sir ko'rsatishi mumkin.

Umuman olganda nafaqat web sayt balki, istalgan axborot xavfsizligi sohasidagi obyektni himoyalash mukammal konseptual bosqichli yondashuvni talab etadi. Web sayt turiga qarab xavfsizlik choralarini qo'llash jihatlari turlicha bo'lishi mumkin, lekin umumiy hisobda har qanday web sayt xavfsizligi uchun biz quyidagi jarayonlarga alohida e'tibor bilan yondashishimiz zarur.

Xavfsiz domen ekotizimi – biz bilgan internet bevosita DNS (Domain Name System) ga bog'liqdir. Bu xuddi Internetning telefon kitobiga o'xshaydi, domen nomlari IP manzilga tarjima qilinadi, shuning uchun sayt foydalanuvchisi web saytlarni izlashda raqamlar qatori o'rniga uning nomini yozgan holda osongina topib olishi mumkin.

DNS yagona obyekt emas, balki u protokol, nom maydoni va xizmatni o‘z ichiga oladi oladi. DNS xavfsizligi bu DNS infratuzilmasini tez va ishonchli ishlashini ta’minlash uchun uni kiberhujumlardan himoya qilish amaliyotidir [2:75]. Samarali DNS xavfsizlik strategiyasi bir-biriga o‘xshash bir qator himoya vositalarini o‘z ichiga oladi, jumladan, ortiqcha DNS serverlarini o‘rnatish, DNSSEC kabi xavfsizlik protokollarini qo‘llash va qat’iy DNS jurnalini talab qilish.

Xavfsiz foydalanuvchi hisoblari - foydalanuvchi hisoblaridan ehtiyotkorlik bilan foydalanish tarmog‘ingiz uchun xavfsizlikning eng muhim turi hisoblanadi. To‘g‘ri sozlangan foydalanuvchi hisoblari ruxsatsiz foydalanuvchilarning tarmoqqa jismoniy kirish huquqiga ega bo‘lsa ham, tarmoqqa kirishini oldini oladi.

Muhim va yuqori darajadagi zaifliklarni oldini olish uchun doimiy ravishda skanerlashni amalga oshirish – internet orqali kirish mumkin bo‘lgan tizimlardagi barcha muhim va yuqori darajadagi zaifliklarni uchraydigan bo‘shliqlarni har 15-30 kunda yangilab to‘ldirishga harakat qiling. Iloji boricha doimo avtomatik yangilash tizimini yoqib qo‘yish lozim.

Tranzitda xavfsiz ma’lumotlar – ma’lumotlarni gipermatnli uzatish protokoli (HTTP) o‘rniga, xavfsiz gipermatnli uzatish protokoli (HTTPS) va HTTP qat’iy transport xavfsizligi (HSTS) dan foydalanish lozim bo‘ladi. Istalgan web sayt foydalanuvchisi o‘zining shaxsiy ma’lumotlari va sayt o‘rtasidagi almashinuv xavfsiz bo‘lishini xohlaydi. HTTPS esa aynan ma’lumotlarning tarmoq protokoli orqali shifrlangan holatda uzatilishini va ruxsat etilmagan shaxslar tomonidan o‘qilmasligini ta’minlaydi.

Ma’lumotlarni zaxiralash – web saytdagi muhim ma’lumotlarni va web sayt sozlamalarini avtomatik ravishda zaxiralash orqali siz ma’lumotlarni uzoq va xavfsiz saqlash imkoniyatiga ega bo‘lasiz.

Xavfsiz web-serverlar – server SSL kabi xavfsizlik protokolini qo‘llab-quvvatloydi. Kredit karta raqamlari va web-serverdan uzatiladigan va boshqa maxfiy ma’lumotlarga ega buyurtma shakllari foydalanuvchi himoyasi uchun shifrlangan bo‘lishi kerak. Uchinchi tomon uzatishni qo‘lga kirita olgan taqdirda ham, ma’lumotlarni shifrlash juda qiyin bo‘ladi.

Zamonaviy texnologiyalar rivojlanish natijasida bugungi kunga kelib web-dasturlash sohasida ma’lum bir web sayt xavfsizligini ta’minlash uchun dasturchidan mutloq yangi algoritm yoki tizim ishlab chiqishni talab qilmaydi. Bugungi kunga kelib, web sayt xavfsizligini ta’minlash uchun ko‘plab texnologiyalardan foydalangan holda mukammal yechimga ega bo‘lish mumkin.

OpenID mavjud qaydnomadan foydalangan holda yangi parol generatsiya qilmasdan bir nechta web saytga kirish imkoniyatini taklif etadigan texnologiya hisoblanadi.

Odamlar kundalik hayotida turli web saytlarda ro‘yxatdan o‘tadi va ko‘plab qaydnomalarga ega bo‘ladi, lekin hammasining ham parolini eslab qolish yoki saqlash foydalanuvchilarga ko‘plab noqulayliklarni keltirib chiqarishi mumkin. Shunday vaziyatlarda OpenID bu muammoga o‘z yechimini taklif etadi. OpenID bilan faqat bitta foydalanuvchi nomi va parol kerak bo‘ladi. Identifikatsiya provayderida identifikator va parol bilan bitta hisob yaratish mumkin va bu provayder tashrif buyurgan web saytlarga foydalanuvchi shaxsini tasdiqlaydi. Provayderdan boshqa hech bir web sayt parolni ko‘rmaydi.

OpenID rasman 2005-yilda taqdim etilgan. Google, Facebook, Yahoo!, Microsoft, AOL, MySpace, Sears, Universal Music Group, France Telecom, Novell, Sun, Telecom Italia kabi ko‘plab yirik korxonalar OpenIDdan foydalanadi.

Foydalanuvchi OpenID providerida o‘z qaydnomasiga ega va tizimga o‘z shaxsini shaxsiy identifikatori bilan tanishtirishi lozim. OpenID identifikator yoki URL bo‘lishi mumkin.

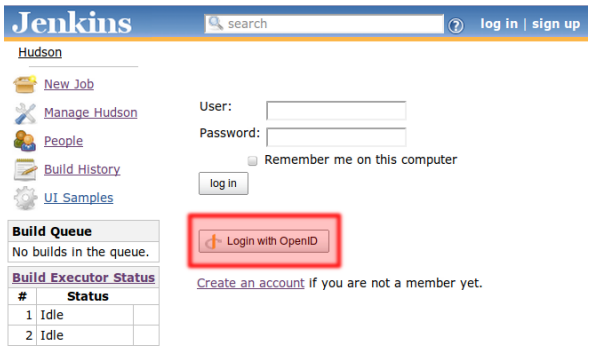
1. OpenID olish uchun, foydalanuvchi avvalo OpenID providerida ro‘yxatdan o‘tishi lozim. Foydalanuvchi ishonchli tomonga (relying party) o‘z shaxsini isbotlashi kerak. Shunday qilib, ishonchli tomon kirishni so‘raganda, foydalanuvchi OpenIDni kiritishi kerak. Har qanday web saytlar o‘z web saytlariga kirish uchun OpenIDni qabul qilishi mumkin.

Ushbu OpenIDdan foydalangan holda foydalanuvchi istalgan web saytga kirishi mumkin.

OpenID yordamida autentifikatsiya jarayonini amalga oshirish mumkin, chunki har bir foydalanuvchi OpenID yordamida aniqlash mumkin.

OpenID provayderida ro‘yxatdan o‘tib o‘z qaydnomasiga ega foydalanuvchi har qanday web saytga kirganda o‘z ma’lumotlarini taqdim etishi kerak bo‘ladi.

Quyidagi rasmda Jenkins foydalanuvchidan OpenIDni kiritishni so‘rayotganini ko‘rsatilgan. (2-rasm)



2-rasm. Jenkins tizimida OpenID yordamida tizimga kirish[3]

2. Foydalanuvchi tizimga o‘z OpenIDsini kiritgach, tizim ushbu unikal parol logini OpenID provideriga yo‘naltiradi.

3. Keyin foydalanuvchi OpenID providerida o‘zini shaxsini autentifikatsiyadan o‘tkazishi kerak bo‘ladi.

4. Foydalanuvchi muvaffaqiyatli autentifikatsiyadan o‘tgach, OpenID provayderi foydalanuvchi shaxsini tizimga yo‘naltiradi.

5. Keyin tizim foydalanuvchiga o‘z web saytiga kirishga ruxsat beradi.

– foydalanuvchi kirmoqchi bo‘lgan, OpenID provayderi o‘rtasida xavfsizlik tizimi Diffie-Hellman almashinuvi yordamida almashiladi.

OAuth 2.0 web-ilovalar, kompyuter dasturlari, mobil telefonlar va uyda foydalaniladigan texnologiyalari uchun maxsus avtorizatsiya jarayonini tashkillashtirib, mijoz qism dasturiy ta’minotini ancha yengillashtiradi. OAuth 2.0 foydalnuvchi nomlari, parollari va boshqa ma’lumotlarni saqlagan holda maxfiy saqlagan holda ilova bilan xavfsiz ma’lumot almashinish imkoniyatini beradi. Masalan, web sayt yoki ilova foydalanuvchilardan fayllarni Google Disklarda saqlashga ruxsat olish uchun OAuth 2.0 dan foydalanishi mumkin.

OAuth (Ochiq avtorizatsiya) internetda tokenga asoslangan avtorizatsiya uchun ochiq standart avtorizatsiya tizimidir. “Oh-auth” deb talaffuz qilinadigan OAuth oxirgi foydalanuvchining hisob ma’lumotlaridan Facebook va Google kabi uchinchi tomon xizmatlari tomonidan foydalanuvchining hisob ma’lumotlarini uchinchi tomonga oshkor qilmasdan foydalanish imkonini beradi. U oxirgi foydalanuvchi nomidan vositachi bo‘lib, uchinchi tomon xizmatiga hisob ma’lumotlarini baham ko‘rishga ruxsat beruvchi kirish tokenini taqdim etadi. Tokenni olish jarayoni avtorizatsiya oqimi deb ataladi [1”10-25].

Oddiy OAuth 2.0 ilovasida avtorizatsiya oqimi olti bosqichli jarayondir. Quyidagi misolda, onlayn taqvim yaratish ilovasi foydalanuvchining Google Drive-da saqlangan fotosuratlariga kirish imkoniyatiga ega bo‘lish misoli keltirilgan:

1. Taqvim yaratish ilovasi (mijoz) himoyalangan resurslarga, bu holda foydalanuvchiga (resurs egasiga) tegishli bo‘lgan tasvir fayllari foydalanuvchini avtorizatsiya so‘nggi nuqtasiga yo‘naltirish orqali ruxsat so‘raydi.

2. Resurs egasi ilovadan manbaga kirish so‘rovini autentifikatsiya qiladi va avtorizatsiya qiladi va avtorizatsiya so‘nggi nuqtasi mijozga avtorizatsiya grantini qaytaradi. OAuth 2.0 protokoli grantlarning to‘rt turini belgilaydi: avtorizatsiya kodi, mijoz hisob ma’lumotlari, qurilma kodi va tokenni yangilash.

3. Keyin mijoz avtorizatsiya serveridan kirish tokenini so‘raydi, so‘ngra avtorizatsiya so‘nggi nuqtasidan qaytarilgan avtorizatsiya grantini hamda o‘z identifikatorini token so‘nggi nuqtasiga autentifikatsiya qilish orqali taqdim etadi.

4. Agar mijoz identifikatori autentifikatsiya qilingan bo‘lsa va avtorizatsiya huquqi haqiqiy bo‘lsa, avtorizatsiya serveri yoki autentifikatsiya provayderi -- bu holatda Google avtorizatsiya serveri mijozga kirish tokenini beradi.

5. Mijoz endi resurs serveridan himoyalangan resurslarni so‘rashi mumkin -ushbu misolda Google Drive - autentifikatsiya uchun kirish tokenini taqdim etish orqali.

6. Agar kirish tokeni haqiqiy bo‘lsa, resurs serveri so‘ralgan resurslarni kalendar yaratish ilovasiga (mijoz) qaytaradi.

Endi kalendar yaratish ilovasi taqvim yaratish uchun foydalanuvchi suratlariga kirishi va Google Diskdan rasmlarni import qilishi mumkin.

JSON web tokeni (JWT) - bu ochiq standart (RFC 7519) bo‘lib, JSON obyekti sifatida tomonlar o‘rtasida ma’lumotni xavfsiz uzatishning ixcham va mustaqil usulini ta’minlaydi [3:45-52].

[3] https://cdn.jsdelivr.net/gh/jenkinsci/openid-plugin@master/docs/images/login-with-openid.png

ISSN 2181-9572

Nisbatan kichik hajmi tufayli JWT URL orqali, POST parametri orqali yoki HTTP sarlavhasi ichida yuborilishi mumkin va u tezda uzatiladi. JWT ma'lumotlar bazasini bir necha marta so'ramaslik uchun obyekt haqida barcha kerakli ma'lumotlarni o'z ichiga oladi. JWT oluvchisi tokenni tasdiqlash uchun serverga murojaat qilishi shart emas.

Agar foydalanuvchi o'z hisob ma'lumotlari yordamida tizimga muvaffaqiyatli kirsa, ID tokeni qaytariladi. OpenID Connect (OIDC) xususiyatlariga ko'ra, ID tokeni har doim JWT hisoblanadi.

Foydalanuvchi tizimga muvaffaqiyatli kirgandan so'ng, dastur ushbu foydalanuvchi nomidan marshrutlarga, xizmatlarga yoki resurslarga (masalan, API) kirishni so'rashi mumkin. Buning uchun har bir so'rovda u JWT shaklida bo'lishi mumkin bo'lgan Access tokenini o'tkazishi kerak. Yagona tizimga kirish (SSO) formatning kichik yuki va turli domenlarda osongina foydalanish qobiliyati tufayli JWTdan keng foydalanadi.

Axborot almashinuvi: JWTlar tomonlar o'rtasida ma'lumotni xavfsiz uzatishning yaxshi usuli hisoblanadi, chunki ular imzolanishi mumkin, ya'ni jo'natuvchilar ular aytganidek ekanligiga ishonch hosil qilishingiz mumkin. Bundan tashqari, JWT tuzilmasi kontent buzilmaganligini tekshirish imkonini beradi.

JSON obyektidagi ma'lumotlar raqamli imzolanganligi sababli tekshirilishi va ishonchli bo'lishi mumkin. JWTlar tomonlar o'rtasida maxfiylikni ta'minlash uchun shifrlanishi ham mumkin bo'lsa-da, Auth0 tomonidan chiqarilgan JWTlar JSON Web Imzolari (JWS), ya'ni ular shifrlangan emas, balki imzolangan. Shunday qilib, biz imzolangan tokenlarga e'tibor qaratamiz, ular tarkibidagi da'volarning yaxlitligini tekshirishi mumkin, shifrlangan tokenlar esa bu da'volarni boshqa tomonlardan yashiradi.

Umuman olganda, JWTlar RSA yoki ECDSAdan foydalangan holda maxfiy (HMAC algoritmi bilan) yoki umumiy/maxfiy kalitlar juftligi yordamida imzolanishi mumkin. Tokenlar ochiq/maxfiy kalit juftliklari yordamida imzolanganda, imzo faqat shaxsiy kalitga ega bo'lgan tomon uni imzolagan shaxs ekanligini tasdiqlaydi [4:105].

Qabul qilingan JWT dan foydalanishdan oldin uning imzosi yordamida to'g'ri tekshirilishi kerak. E'tibor bering, muvaffaqiyatli tasdiqlangan token faqat token tarkibidagi ma'lumotlar boshqa hech kim tomonidan o'zgartirilmaganligini anglatadi. Bu oddiy matnda saqlangan tarkibni boshqalar ko'ra olmaganligini anglatmaydi. Shu sababli, siz hech qachon JWT ichida maxfiy ma'lumotlarni saqlamasligingiz kerak va JWTlarning tutib olinmasligini ta'minlash uchun boshqa choralarni ko'rishingiz kerak, masalan, JWTlarni faqat HTTPS orqali yuborish, eng yaxshi amaliyotlarga rioya qilish va faqat xavfsiz va yangilangan kutubxonalardan foydalanish.

XULOSA

Xulosa o'rnida shuni ta'kidlab o'ish joizki, bugungi kunda web saytlardagi tahdidlarning darajalar bo'yicha tasniflari juda ham dolzarb vazifaga aylanmoqda hamda ularni darajalar bo'yicha davolash dolzarb bo'lib bormoqda.

FOYDALANILGAN ADABIYOTLAR

1. Mengliyev Sh. Kompyuter tarmoqlarida axborotlarni himoyalash, zamonaviy informatikaning dolzarb muammolari:o'tmish tajribasi, istiqbollari Respublika miqyosida ilmiy-amaliy anjuman materiallari, Toshkent-2018.
2. G'aniev S.K., Karimov M.M., Tashev K.A. Axborot xavfsizligi: o'quv qo'llanma – T.: Aloqachi, 2008.
3. Kamilov Sh.M., Masharipov A.K., Zakirova T.A., Ermatov Sh.T., Musayeva M.A. "Kompyuter tizimlarida axborotni himoyalash": ma'ruzalar matnlari. – Toshkent, TDIU, 2003.
4. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. – М.: Инфра, 2002.