ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-01090

АУТЕНТИФИКАЦИЯ, АВТОРИЗАЦИЯ ҲАМДА OPENID CONNECT ПРОТОКОЛИНИНГ ИШЛАШ ЖАРАЁНЛАРИ ТАҲЛИЛИ

Ботирхўжа Шухрат ўғли Саъдуллаев
Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университенти магистранти
ibiyun@mail.ru

АННОТАЦИЯ

Мазкур мақоллада интернетдаги маълумотлар базаси, маълум платформалар, почта манзилларига ёки дастурларга кириш ва улардан фойдаланиш жараёнида фойдаланувчи махфий логин ва паролини ҳимоялаш ҳамда фойдаланувчидан унинг ҳисоб маълумотларини олиш ва уларни ҳақиқийлигини текшириш жараёнларининг таҳлили ҳақида сўз боради.

Калит сўзлар: Идентификация, аутентификация, авторизация, OpenID, OpenID Connect, Oauth, man-in-the-middle attack.

ANALYSIS OF THE PROCESS OF OPERATION OF THE AUTHENTICATION, AUTHORIZATION AND OPENID CONNECT PROTOCOL

ABSTRACT

This article talks about the protection of the user's secret Login and password in the process of accessing and using the database, certain platforms, mailing addresses or programs on the internet, and also the analysis of the processes of obtaining the user's account information and checking their authenticity.

Keywords: Identification, Authentication, Authorization, OpenID, OpenID Connect, Oauth, man-in-the-middle attack.

КИРИШ

Аутентификация ва авторизация жараёнларига асосланган кириш ҳуқуқларини ажратишсиз хеч кандай дастур химоялана олмайди. Шунинг учун, улар аввал қандай содир бўлган ва ҳозирда қандай содир бўлятганини тушуниш жуда муҳим.

Асосий атамалар:

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-01090

Идентификация – бу қаршимизда қандай шахс турганлигини аниқлаш жараёни.

Аутентификация – бу даво қилаётган шахс айнан ўша эканлигини тасдиқлаш жараёни.

Авторизация – бу аутентификацияланган шахсга нима қилиш мумкинлиги хақидаги қарорни қабул қилиш жараёни.

Бу уч хил, кетма-кет ва ўзаро алмаштириб бўлмайдиган тушунчалардир. Идентификацияни кўпинча аутентификация таркибига киради деб назарда тутилади. Энг муҳими, аутентификация ва авторизацияни аниқ ажратиш керак. Аутентификация жараёнида, биз олдимизда турган инсон ўз шахсини тасдиқловчи далилларга эга эканлигига ишонч ҳосил қиламиз.

АДАБИЁТЛАР ТАҲЛИЛИ ВА МЕТОДОЛОГИЯ

HTTP протоколини ишлатиш жараёнида аутентификациянинг энг содда усули бу – Basic access authentication (асосий кириш аутентификацияси)дир. Аслида бу протокол эскирган бўлиб камдан-кам ҳолларда интернетда қўлланилади, айниқса ҳимояланмаган боғланишларда, шунингдек ички корпоратив тизимларида сақланиб қолган, чунки уларнинг баъзилари анча аввал яратилган.

Биринчи бўлиб, ҳимояланган ресурсга мурожаат қилинганида, кириш хуқуқига эга бўлмаган фойдаланувчига сервер берадиган биринчи нарса бу 401 Unauthorized (авторизацияланмаган) хатосидир. Бунда жавоб шунингдек қабул қилиши ва таъсир этиш мумкин бўлган контекст (Realm) аутентификация тури (бизнинг ҳолатимизда, Basic) ҳақида малумотни ўз ичига олади. Фойдаланувчи логин ва паролни киритади, улар Base64 га жамланади ва серверга текшириш учун юборилади. Бунда турли хил хавф-хатарлар мавжуд. Энг кенг тарқалган хавф-хатар – бу man-in-the-middle attack (ўртада турувчи инсон ҳужуми) ёки воситачиларнинг ҳужуми бўлиб, унинг давомида тажавузкорлар ҳавфсиз бўлмаган уланишдан фойдаланган ҳолда мижоздан серверга ёки аксинча узатиш давомида, хисобга олиш маълумотларини қўлга туширишлари мумкин.

HTTP Digest Authentication

Технологияни ривожлантиришнинг кейинги босқичи бироз мураккаброқ HTTP digest authentication қилиш тизими бўлиб, у ҳисоб маълумотларини очиқ кўринишда узатишни инкор этади. Унда текшириш учун MD5-хеш бази бир киритмалар билан ишлатиладиб бу эса логин ва паролни тасодифий танлашни

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-01090

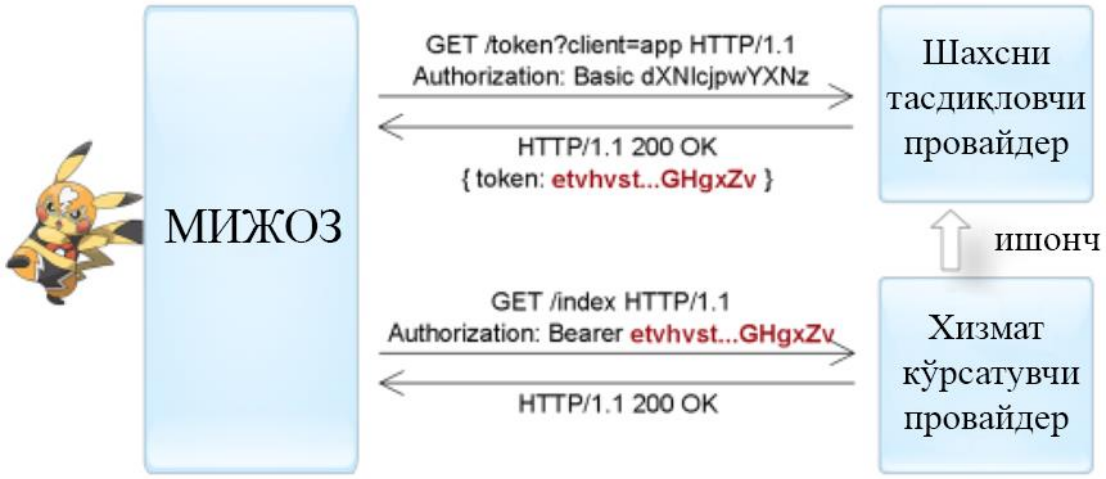
олдини олади. Албатта, бу алгоритм ишончлироқ кўриниши мумкин, бироқ у ҳам бир қанча мукаммал бўлмаган ҳужумларга учраши мумкин.

Forms Authentication



Кейинчалик Forms authentication (формаларни аутентификация қилиш) жараёни пайдо бўлган. Унда аутентификация абстракция моделининг нисбатан юқори даражасида содир бўлади. Бунда HTTP сервер киришга ижозат хатоси ҳақида хабар бермайди, балки аутентификацияланмаган фойдаланувчини бошқа саҳифага йўналтиради. Одатда, ушбу саҳифада логин ва паролни киритиш учун майдончалар чиқади, сўнгра улар тўлдирилгандан сўнг малумотларга эга бўлган POST-сўрови шаклланади ва хавфсиз канал орқали серверга юборилади. Сервер томони, ўз навбатида, фойдаланувчига Cookies да сақланадиган ва кейинчалик ҳимояланган ресурсга киришга ижозат бериш учун фойдаланувчига токен ёки сессия идентификаторини қайтаради.

Token Authentication



Аутентификация қилишнинг кейинги авлоди бу Token Based Authentication (Token асосидаги аутентификация) бўлиб, одатда у Single sign-on (ягона кириш) (SSO) тизимларини яратишда қўлланилади. Ундан

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-01090

фойдаланилаётганда, сўров қилинаётган сервис фойдаланувчи ҳақидаги маълумотларининг ҳаққонийлигини текшириш функциясини бошқа хизматга юборади. Яъни, хизмат кўрсатувчи провайдер токен-провайдерга (Identity provider) киришга рухсат беручи токенларни беришга ишонади. Масалан, ижтимоий тармоқлардаги дастур иловаларига аккаунтлар орқали кириш жараёнини кўришимиз мумкин. IT технологиялардан ташқари ушбу жараёнга энг содда ўхшашлик бу фуқаролик паспортидан фойдаланишдир. Расмий ҳужжат – бу сизга токен (ички ишлар) томонидан берилган хужжат ҳисобланади ва унга барча расмий давлат хизматлари ишонадилар. Паспорт ўз амал қилиш даврида уни бутун сақлаган ҳолда сизнинг аутентификациянгиз учун етарли ҳисобланади.

НАТИЖАЛАР ВА МУҲОКАМА

Ҳимояланган ресурсга кириш ҳуқуқини олиш вақтида токен-аутентификация фойдаланувчининг бевосита қатнашиши талаб қилади, шунинг учун жараённи янада такомиллаштириш талаб қилинади. Identity provider унга бошқариш берилганда фойдаланувчи билан алоқада бўлади, масалан, логин ва паролни сўрайди.

Агар фойдаланувчи номидан маълум вақтлар оралиғида учинчи ресурс суриштирилган сервис ҳолида, – фараз қилайликки ижтимоий тармоқлардаги контактлар рўйхатига рухсат олинса – токен аутентификация ишламай қолади. Гап шундаки, сессия идентификаторлари унча кўп фаолият кўрсатмайди, агар тажавузкорлар уларни қўлга киритсалар сервисга чекланган вақтгагина рухсат олишади. Бироқ хизмат қилиш вақти камлиги ҳисобига токен етишмайди, масалан, кечки жараёнга.

2006 йилда Twitter учун Open ID протоколини табиқ қилиш устида ишлар амалга оширилиши давомида янги очиқ авторизация протоколига эҳтиёж пайдо бўлди. 2007 да Google ва AOL муҳандислари биргаликда уни яратиш устида иш бошладилар, 2009 да Twitter ўз фойдаланувчиларига, ташқи сервисларга аккаунтларга кириш ҳуқуқини берадиган ва OAuth протоколига асосланган ечимни таклиф қилди. Уч йил ўтгач унинг янги версияси – OAuth 2 эълон қилинди. У клиент дастурларини ишлаб чиқаришни соддалаштирди ва бир қатор янги имкониятларга эга бўлди, улар жумласида токенни фойдаланувчисиз янгилаш ҳам бор эди. Кўпгина хизматлар ушбу протоколни расмий тасдиқлангунига қадар ишлата бошладилар.

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-01090

ХУЛОСА

Айни пайтда қуйидаги протоколлар амалда:

OpenID – фойдаланувчининг ҳисоб маълумотларини текшириш учун (identification & authentication).

OAuth – бирор нарсага киришга рухсат олиш.

OpenID Connect – иккаласи ҳақида бир вақтнинг ўзида.

Учала протокол ҳам фойдаланувчига махфий логин ва паролини ишончсиз дастурларга ошкор қилмасликка имкон беради. OpenID & OAuth 2014 йилгача parallel равишда алоҳида ишлаб чиқилган ва охир-оқибат OpenID connect га бирлаштирилган.

OpenID Connect (2014) OpenID 2.0, OpenID Attribute Exchange 1.0 ва OAuth 2.0 имкониятларини битта умумий протоколга бирлаштиради. У иловаларга тасдиқловчи марказни ишлатиш имкониятини қуйидаги ҳоллар учун беради:

Фойдаланувчиларнинг ҳисоб маълумотларини текшириш.

Фойдаланувчи профилини (ёки унинг бир қисмини) олиш.

OpenID Connect ташқи ресурсларга кириш имкониятини бермайди. У профил параметрларини худди улар ресурслар каби тасаввур этиш учун OAuth 2.0 дан фойдаланади.

OpenID Connect фойдаланувчидан унинг ҳисоб маълумотларини олиш ва уларни текшириш учун керак. OAuth 2.0 эса кириш токенларини олиш ва улар ёрдамида ресурсларга кириш учун керак.

Open ID Connect Provider – марказлаштирилган аутентификация хизматининг барча конструкциясининг энг муҳим объекти бўлиб, у яна Security Token Service, Identity Provider authorization server ва бошқача номлар билан ҳам аталиши мумкин. Турли манбалар уни турлича ном билан аташади, аммо моҳиятига кўра у клиентларга токенлар берувчи сервисдир.

OpenID Connect Протоколининг асосий функциялари:

- Фойдаланувчиларнинг ички хотираси ёки ташқи манбадан (масалан, Active Directory) фойдаланиб, аутентификация қилиш.
- Клиентларни бошқариш (сақлаш) ва уларни аутентификация қилиш.
- Сессияни бошқаришга ва Single sing-on ни амалга оширишга рухсат бериш.
- Клиентларга identity-токен ва access-токенни бериш.
- Олдин берилган токенларни текшириш.

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
DOI: 10.24411/2181-1385-2021-01090

Аутентификация жараёни



Агар фойдаланувчи мижозга мурожаат қилса, фойдаланувчини фойдаланувчини номи ва паролини сўрайдиган Open ID Connect Провайдерига йўналтиради. Муваффақиятли бўлса, у идентификатор белгиси ва фойдаланувчи ҳимояланган манбага кириши мумкин бўлган кириш белгисини қайтаради.

REFERENCES

1. OpenID Foundation, “OpenID Authentication 2.0 - Final,” 2007. [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html. [Accessed: 19-May-2017].
2. B. Leiba, “OAuth web authorization protocol,” IEEE Internet Comput., vol. 16, no. 1, pp. 74–77, 2012.
3. OpenID Foundation, “Welcome to OpenID Connect,” 2016. [Online]. Available: http://openid.net/connect/. [Accessed: 19-May-2017].