МАХКАМОВ Анваржон Абдужабборович
Ўзбекистон халқаро ислом академияси Замонавий ахборот-коммуникация технологиялари кафедраси доценти, PhD

РАХИМОВА Сайёра Яшин қизи
Ўзбекистон халқаро ислом академияси Замонавий ахборот-коммуникация технологиялари кафедраси магистранти

ВЕБ-САЙТЛАР ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ МУАММОЛАРИ ВА УЛАРНИ БАРТАРАФ ЭТИШ МАСАЛАЛАРИ

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ВЕБ-САЙТОВ И ИХ УСТРАНЕНИЯ

WEB-SITE SECURITY ISSUES AND THE PROBLEMS OF ELIMINATING

Аннотация: *Ушбу мақолада веб-сайтлар хавфсизлигини таъминлаш муаммолари ва уларни бартараф этиш масалалари кўриб чиқилган.*

Тизим хавфсизлиги соҳасидаги юқори ютуқларга қарамай, веб сайтларга ҳамон бузғунчилар томонидан ҳужумларнинг уюштирилиши жуда катта муаммоларни келтириб чиқармоқда. Шуни хисобга олган холда мақолада веб сайтлар хавфсизлигига бўладиган хужумларнинг турлари, веб сайтлар заифликлари, хумумларга бардошлилик даражаси, веб сайтларнинг хавфсизлик ва ишончлилик коеффициентини белгилаб берувчи махсус веб тестлаш дастурлари, маълумотлар махфийлигини сақлаш учун бир қанча ҳимоя технологиялари хақида маълумот келтириб ўтилган.

Калит сўзлар: *заифлик, ҳимоя, ахборотни ҳимоя қилиш, ddos-ҳужум, сервер, ахборот хавфсизлиги, вирус, антивирус, компютер тармоқлари, сўровлар, қимматли маълумотлар.*

Аннотация: *В этой статье рассматриваются проблемы безопасности веб-сайтов и способы их преодоления.*

Несмотря на высокий прогресс в области системной безопасности, хакерские атаки на веб-сайты по-прежнему представляют собой большую проблему. С учетом этого в статье приведены сведения о видах атак на безопасность веб-сайтов, уязвимостях веб-сайтов, уровне устойчивости к угрозам, специальных программах веб-тестирования, определяющих коэффициент безопасности и надежности веб-сайтов, и ряде технологий защиты для сохранения конфиденциальности данных.

Ключевые слова: *уязвимость, защита, защита информации, ddos-атака, сервер, защита информации, вирус, антивирус, компьютерные сети, запросы, ценные данные.*

Annotation: *This article discusses website security issues and how to overcome them.*

Despite the high progress in the field of system security, hacker attacks on websites are still a big problem. With this in mind, the article provides information about the types of attacks on website security, website vulnerabilities, the level of resistance to threats, special web testing programs that determine the safety and reliability of websites, and a number of protection technologies. to maintain data confidentiality.

Keywords: *vulnerability, protection, information security, ddos attack, server, information protection, virus, antivirus, computer networks, requests, valuable data.*

КИРИШ

Бугунги кунда аксарият замонавий ахборот тизимлари веб-сайтлар шаклида яратилмоқда. Хозирги кунга келиб шу сабабли веб-сайтлар хавфсизлиги таъминланишига алоҳида эътибор қаратилиши керак. Операцион тизим ва дастурий таъминотга эга қурилма пайдо бўлиши биланоқ у дарҳол хакерларнинг қизиқишини тортмоқда.

Айни вақтда ишлаб чиқарувчилар ҳар доим ҳам яратилган сайтларнинг тўлиқ ҳимояси ва хавфсизлигига алоҳида эътибор бермасликлари мумкин. Ҳар бир сайт у ёки бу тарзда ҳакерлар ҳужумига учраши ва ахборот хавфсизлигига зарар келтириши мумкин. Шуни ҳисобга олган ҳолда яратилаётган веб-сайтлар ҳавфсизлик ҳимоясини таъминлаш жуда муҳим аҳамиятга касб этмоқда.

АСОСИЙ ҚИСМ

Ушбу мақоланинг асосий мақсади, веб-сайтлар хавфсизлигини таъминлаш муаммолари ва уларни бартараф этишдан иборат. Веб-сайтлар жуда ҳилма-ҳил бўлиши мумкин: рақамли кутубхоналар, ижтимоий тармоқлар, турли таълим муассасаларининг веб-порталлари, онлайн-дўконлар, турли

ташкилотларнинг расмий веб-сайтлари, банклар ва бошқалар.

Буларда аввало, веб-сервер хавфсизлигига эътибор берилиши зарур. Чунки, у мижозлардан веб-сайтга http сўровларини қабул қилиши ва қайта ишлаши учун жавобгар ҳисобланади. Айнан у бутун дунё бўйлаб кўплаб веб-сайтларнинг ишлашини таъминлайди, шунингдек, асосий хизматлар учун жавобгар ва фойдаланувчиларнинг шахсий маълумотларини сақлайди. Серверларни ҳимоя қилиш зарурати ҳар қандай ташкилотнинг энг муҳим вазифаларидан бири хисобланади. Биринчи веб-сайтлар пайдо бўлиши пайтида ҳам хакерлар Американинг SitiBank (1994) каби муҳим ташкилотларнинг сайтларига ҳужумлар уюштиришган бўлиб, бунинг натижасида 12 миллион доллар маблағ ўғирланган. Ўшанда NATO, АҚШ марказий разведка бошқармаси ва Адлия вазирлиги ҳам қурбон бўлган. Ҳозирги вақтда бундай таҳдидлар камайиши ёки умуман бўлмаслиги керакдек туюлади, аммо бу хақиқатдан йироқ. Бунинг иложи йўқ аммо қисман бўлсада таҳдидларни камайтиришга эришиш мумкин[1, 3, 7].

Хозирда ҳам жуда кўп сонли киберҳужумлар амалга оширилмоқда. Бунинг сабаби шундаки, бундай контент катта миқдордаги пулни “ишлаб олиши” ёки давлат учун муҳим воқеаларга қандайдир тарзда таъсир қилиши мумкин бўлган маълумотларни олиши ва ўзгартириши мумкин. Эътиборга молик жиҳати шундан иборатки, сервернинг географик жойлашуви унинг ҳимоясига ҳеч қандай таъсир кўрсатмайди. Сиз унга исталган кириш нуқтасидан ҳужум қилишингиз мумкин. Бунинг сабаби, веб-серверлар ўзларининг очиқлиги туфайли фойдаланувчилар ўртасида маълумот узатиш учун мўлжалланган ва шунинг учун улар жуда кўп заифликларга эга. Мисол учун, тажаввузкор http сервери ёки маълумотлар базаси сервери кодига ёки веб-сайт саҳифаларининг ўзига баъзи ўзгаришлар (модификациялар) киритиб, унинг асл функциясини ўзгартириши мумкин.

Бугунги кунда кўп кузатилаётган, киберҳужумларда ҳуқуқбузарларнинг энг кўп учрайдиган ҳаракатлари:

• сайтга нотўғри маълумот жойлаштириш;

• қимматли маълумотлар тўпланган серверга рухсатсиз кириш;

• банк пластик карталари эгалари маълумотлар базасига ҳужум қилиш. асосий банк карталари эгаларининг ҳисоб рақамлари, уларнинг исм-шарифлари, фамилиялари, алоқа маълумотлари ҳақидаги маълумотларни ўғирлаш, кейин эса катта миқдордаги пул маблағларига эга бўлишга ҳаракат қилиш;

• паролларни осонликча бузадиган вируслар яратиш ва уларни юбориш ёки ўғирланган маълумотларни сақлаш ва фойдаланиш;

• турли мамлакатлардаги давлат муассасаларнинг веб-сайтларига ҳужумлар уюштириш;

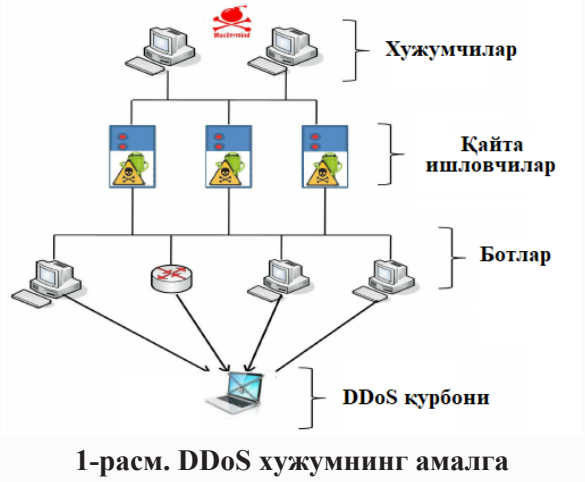
• интернет тезлигини сезиларли даражада секинлашишига олиб келган вирусларнинг тарқалиши (бундай вируслар натижасида айрим ҳудудлар тармоқдан бутунлай узилиб қолган ҳолатлар ҳам бўлган);

• тармоқни қўшимча сўровлар билан тўлдириш мақсадида тармоқдаги ddos-ҳужумлар;

• корпоратив компютер тармоқлари хавфсизлигини таъминлаш учун фойдаланиладиган SecurID технологияси билан боғлиқ маълумотларга кириш ҳуқуқини олиш.

Веб-сайтларнинг хавфсизлик ва ишончлилик коэффицентини белгилаб берувчи махсус веб-тестлаш дастурлари мавжуд.

Ҳисоб-китобларга кўра, ҳар учинчи сайт бошқа шахслар томонидан назорат қилинади. Бу веб-ишлаб чиқувчилар учун жуда ёқимсиз ва безовта қилувчи фактлар хисобланади. Қуйидаги расмда DDoS хужумнинг амалга оширилиши босқичлари схемаси келтириб ўтилган.



1-расм. DDoS хужумнинг амалга оширилиши босқичлари

Статистик маълумотларга кўра катта компаниялар бошқаларга нисбатан энг кўп зарар кўради [2, 4].

2-расм. DDoS хужумга учровчи қурбонлар улуши

Олиб борилган тадқиқотларга кўра касперский антивирус лабораторияси томонидан аниқланган зарарли дастурларнинг тахминан 90% банк карталари ҳақидаги маълумотларни ўғирлайдиган банк вирусларига тўғри келади.

Янги веб-сайт яратишда ишлаб чиқувчилар мавжуд платформалардан, аниқроғи CMS (контентни бошқариш тизими) дан фойдаланишлари ёки ҳамма нарсани нолдан ёзишлари мумкин, лекин кўпинча кичик компаниялар тайёр воситалардан фойдаланишни афзал кўришади. CMS нинг асосий функциялари қуйидагилардан иборат[6, 7]:

• контент яратиш воситаларини тақдим этиш, контент билан ҳамкорликни ташкил этиш;

• контентни бошқариш: сақлаш, версияни бошқариш, киришни тизимини бошқариш, ҳужжатлар оқимини бошқариш ва бошқалар;

• контентни нашр этиш;

• ахборотни қидириш ва навигация учун қулай шаклда тақдим этиш.

CMS нинг асосий камчилиги шундан иборатки, улар одатда интернетда топилиши мумкин бўлган ўзларининг заиф томонларига эга. Ҳар йили тобора кўпроқ янги CMS янгиланади ва шу билан бирга янги заифликлар пайдо бўлади. Бу веб-сайт маъмурлари, дастурчилар ва дизайнерларнинг биргаликдаги ҳаракатларини талаб қилади, шунингдек, антивирус дастурлари, операцион тизимлар ва кириш ҳуқуқлари доимо алоҳида эътибор талаб қилади.

CMS ларни турли хил ҳужумлардан ҳимоя қилишнинг энг машҳур усуллари қуйидагилардан иборат:

1. XSS-инъекциялардан ҳимоя қилиш;
2. ортиқча маълумотларни яшириш;
3. SSL дан мажбурий фойдаланиш;
4. илдиз файлни ҳимоя қилиш;
5. спамерлар ва ботларни олдини олиш усуллари;
6. зарарли URL сўровлардан химоялашда турли плагинлардан фойдаланиш;
7. сервердаги директорияни кўришдан ҳимоя қилиш.

Маълумотлар махфийлигини сақлаш учун бир қанча ҳимоя технологиялари мавжуд бўлиб, улар қуйидагилардан иборат:

1. WEP. WEP протоколи узатилаётган маълумотларни RC 4 алгоритми асосида шифрлаш имконини беради. Аммо протоколнинг кўплаб заиф томонлари мавжудлиги сабабли, хакерлар томонидан у осонгина бузилишини инобатга олиб, 2003 йили хавфсизликнинг WPA (инг. Wi-Fi Protected Access - Wi-Fi га ҳимояланган кириш) стандарти фойдаланиш учун таклиф этилди.

2. WPA2 2004 йилнинг июнь ойида қабул қилиниб, 2006 йилнинг 13 март кунидан бошлаб барча сертификатлаштирилган Wi-Fi қурилмаларида ўрнатилиши шартдир. WPA2 протоколлари аутенфикациянинг икки режимида ишлайди: персонал (Personal) ва корпоратив (Enterprise). Мазкур протокол калитларни қайта қўллашга имкон бермайди.

3. MAC-манзилларни фильтрлаш - ушбу функция барча замонавий кириш нуқталарини қўллаб-қувватлайди ва тармоқ хавфсизлигини самарали таъминлайди. Фильтрлаш уч хил усулда амалга оширилади:

• Кириш нуқтаси ҳар қандай MAC-манзилли станцияга киришга рухсат беради;

• Кириш нуқтаси махсус ишончли рўйхатда турган MAC-манзиллар станциясига киришга имкон беради;

• Кириш нуқтаси “қора рўйхатда” турган MAC-манзиллари мавжуд станцияга кириш имконини бермайди.

4. SSID тармоқни яширин идентификация қилиш режими. Фойдаланувчи тармоққа

кирмоқчи бўлганида, симсиз адаптер драйвери, аввало ундаги мавжуд симсиз тармоқларни сканерлайди. Ҳар бир кадр таркибида уланиш учун хизмат ахбороти ва SSID мавжуддир [1, 7, 8].

Юқорида кўрсатилган ҳимояланиш усулларининг жузъий камчиликлари мавжуд бўлсада, бугунги кунда улар симсиз тармоқларни 85-90 фоизгача хакерлар ҳужумидан асраб, ҳимояланишнинг асосий усулларидан бири бўлиб қолмоқда.

Замонавий ҳимоя воситаларини жорий этиш ахборот хавфсизлигини таъминлаш чора-тадбирларининг ажралмас бир бўлаги ҳисобланади.

Веб-сайтларни ҳимоя қилиш веб-ишлаб чиқувчилар учун энг муҳим вазифалардан бири хисобланади. Агар бунга аълоҳида эътибор берилмаса, моддий ва сиёсий жиҳатдан жуда катта йўқотишларга олиб келиши мумкин.

ХУЛОСА

Хулоса қилиб айтадиган бўлсак, хозирги кунга келиб веб-сайтларга ҳужумларнинг тўхтамаслиги сабабли (барча зарарли ҳаракатлар қонун билан жазоланишини ҳисобга олсак), дастурчилар биринчи навбатда унинг яратилиш жараёнида хавфсизлиги ҳақида ўйлашлари зарур. Веб-сайтларни ҳимоя қилишнинг кўплаб усуллари мавжуд, аммо улар қанчалик самарали бўлишмасин, заифликларни вақти-вақти билан текшириб бориш зарур. Шундай экан, веб-сайтларни ишлаб чиқарувчилар ва маъмурлари учун асосий бериладиган маслаҳат унинг ишончлилиги ва хавфсизлиги даражасини қайта-қайта текширишдан иборат.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. Крис Митчелл. Артем Конев. Обеспечение безопасности веб-сайтов. Australia: SophosLabs.
2. URL: http://help.yandex.ru/webmaster/protecting-sites/ contents.xml
3. Смирнов С.Н. Безопасность систем баз данных М.: Гелиос АРВ, 2007.-352с.
4. «Лаборатория Касперского» Сложные кибератаки пришли на смену массовым эпидемиям
5. URL: http://pda.cnews.ru/reviews/index.shtml?2014/12/24/591211
6. DDoS атаки и малый бизнес.
7. URL: http://bezshablona.ospfmon.com/2014/02/ddos_4866.html?m=0
8. Хасанов П.Ф., Хасанов Х.П., Ахмедова О.П., Давлатов А.Б. “Криптотаҳлил ва унинг маҳсус усуллари” электрон ўқув қўлланма. 2010 й.
9. С.К.Ганиев, А.А.Ганиев, З.Т.Худойқулов. Киберхавфсизлик асослари: ўқув қўлланма. – Т.: «Алоқачи», 2020, 303 бет.
10. Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonized Criteria (1991) Luxembourg: Office for Official Publications of the European Communities, 1991 ISBN 92-826-3004-8, Catalogue Number: CD-71- 91-502-EN-C © ECSC-EEC-EAEC, Brussels. Luxembourg.
11. Stamp M. Information security: principles and practice. John Wiley & Sons, 2011, -P. – 606.