ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

Ризуан Рауан Ержанұлы

«Веб-қосымшалардың қауіпсіздік жүйесіне талдау жасау»

Дипломдық жоба

ТҮСІНІКТЕМЕЛІК ЖАЗБА

5В100200 – «Ақпараттық қаупсіздік жүйелері» мамандығы

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі,
т.ғ.к., ассистент-профессор
_____Н.А.Сейлова
«__14__» ____05_____2019 ж.

Дипломдық жобаға
ТҮСІНІКТЕМЕЛІК ЖАЗБА

Тақырыбы: «Веб-қосымшалардың қауіпсіздік жүйесіне талдау жасау»

Мамандығы 5В100200-Ақпараттық қаупсіздік жүйелері

Орындаған Ризуан Р. Е.

Пікір беруші
Техника ғылымдарының кандидаты,
МАИН Академигі, “Ақпараттық қауіпсіздік жүйелері” кафедрасының профессоры
_____ Тынымбаев С. Т.
«__14__» ____05_____ 2019 ж.

Ғылыми жетекші
Техника ғылымдарының магистрі
_____Иманбаев А. Ж.
«__14__» ____05_____2019 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Ақпараттық және телекоммуникациялық технологиялар институты

«Киберқауіпсіздік, Ақпаратты Өңдеу және Сақтау» кафедрасы

5В100200- Ақпараттық қаупсіздік жүйелері

БЕКІТЕМІН
Кафедра меңгерушісі,
т.ғ.к., ассистент-профессор
_____Н.А.Сейлова
«__14__» ____05_____2019 ж.

Дипломдық жобаны орындауға
ТАПСЫРМА

Білім алушы *Ризуан Рауан Ержанұлы*
Тақырыбы: «Веб-қосымшалардың қауіпсіздік жүйесіне талдау жасау».
Университет Ректорының *201_ жылғы «__» _____ №_____* бұйрығымен бекітілген
Аяқталған жұмысты тапсыру мерзімі *20__жылғы «__»___*
Дипломдық жобаның бастапқы берілістері: *Веб-қосымшалардың осалдықтары мен негізгі қауіп көздерін зерттеу. Веб-қосымшалардың қауіпсіздігін тексеруге арналған бағдарламалық жасақтамалары мен қосымшаларын пайдаланып, оларға салыстырмалы талдау жүргізу. Веб-қосымшалардың қауіпсіздігін талдау әдістемесін әзірлеу.*
Дипломдық жобада қарастырылатын мәселелер тізімі
1. Теориялық бөлім
2. Практикалық бөлім
3. *Қосымша*
Сызба материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс)
Сызба материалдары ___слайдта көрсетілген
Ұсынылған негізгі әдебиет *13 атаудан тұрады*

Дипломдық жобаны дайындау

КЕСТЕСІ

Бөлім атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекші мен кеңесшілерге көрсету мерзімі	Ескерту
Теориялық бөлім	19.02.2019-26.03.2019	
Практикалық бөлім	29.03.2019-28.04.2019	

Дипломдық жоба бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жобаға қойған

қолтаңбалары

Бөлімдератауы	**Кеңесшілер аты, әкесінің аты, тегі (ғылымидәрежесі, атағы)**	**Қол қойылған күні**	**Қолы**
Норма бақылау	Зиро А.А.	13.05.2019	

Ғылыми жетекшісі Иманбаев А. Ж.

Тапсырманы орындауға алған білім алушы Ризуан Р. Е.

Күні «14» 05 2019 ж.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ және ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ университеті

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

Дипломдық жобаға
(жұмыс түрлерінің атауы)
Ризуан Рауан Ержанұлы
(студенттің аты жөні)
5В100200-Ақпараттық қауіпсіздік жүйелері
(мамандық атауы мен шифрі)

Тақырыбы: «Веб-қосымшалардың қауіпсіздік жүйесіне талдау жасау»

Ризуан Рауан Ержанұлы дипломдық веб-қосымшалардың қауіпсіздігін арттыру мақсатында талдау жүргізу әдістемесін жасаған.

Студент осы дипломдық жобада веб-қосымшаның ақпараттық қауіпсіздігі қатерлерінің негізгі түрлері, сондай-ақ веб-қосымшаның қауіпсіздігіне тікелей немесе жанама залал келтіруі мүмкін қауіп көздеріне зерттеу жүргізген. Веб-бағдарламалардың осалдықтары мен қауіпсіздігіне төнетін қауіп-қатерлердің негізгі түрлеріне зерттеу жүргізген, сәйкестендіру жасаған және әрқайсысына сипаттама берген.

Сонымен қатар, веб-қосымшаның қауіпсіздік деңгейін зерттеу мақсатында түрлі сканерлеуші бағдарламаларды әртүрлі баптауларда пайдаланып, олардың өзара артықшылықтары мен кемшіліктеріне қарай салыстырулар жүргізген. Зерттеу негізінде веб-қосымшалардың осалдығын автоматты түрде анықтау әдістерінің жіктелуін қалыптастырған. Веб-қосымшаның қауіпсіздігін талдау қорытындысы есебінде веб-қосымшалардың қауіпсіздігін талдау әдістемесі әзірленген.

Дипломдық жобаны орындау барысында студент университеттен алған білімін толықтай пайдаланып, өзінің ғылыми және тәжірибелік білімінің жақсы деңгейде екенін көрсетті. Дипломдық жобаны өз бетінше орындады.

Ризуан Рауан Ержанұлының дипломдық жобасы қойылған талаптарға сай келеді, қорғауға ұсыныс жасаймын.

Ғылыми жетекші

Техникалық ғылымдарының магистрі.
(қызметі, ғыл. дәрежесі, атағы)
_____ Иманбаев А. Ж.

«14» 05 2019 ж

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

Дипломдық жұмыс
(жұмыс түрінің атауы)

Ризуан Рауан Ержанұлы
(білім алушының Т.А.Ә.)

5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

(мамандық атауы мен шифрі)

Тақырыбы: Веб-қосымшалардың қауіпсіздік жүйесіне талдау жасау

Орындалды:
а) графикалық бөлім ___11____ парақ
б) түсініктеме _____28____ бет

ЖҰМЫСҚА ЕСКЕРТУ

Веб-қосымшалардың қауіпсіздігі ақпараттық қауіпсіздікті қамтамасыз етудегі ең өзекті мәселелердің бірі болып табылады. Желіде Интернет-дүкендердің, нарықтардағы, түрлі бизнес-бағдарламалардың және қашықтан басқаратын банктік қызметтердің веб-порталдары кең таралған. Қазіргі заманғы ұйымды (ол ірі корпорация немесе шағын жеке компания болсын) Интернет желісінде өзінің ресми сайты болмауын елестету қиын. Осындай жалпыға қолжетімді веб-бағдарламалар зиянкестер үшін тартымды болып табылады. Веб-бағдарламаларға жасалған шабуылдар зиянкестерге келесі мүмкіндіктерді береді: компанияның ішкі ресурстарына қолжетімділік, құпия ақпарат, бағдарламаның функционалдық жүйесін немесе бизнес-логиканы бұзу - кез-келген шабуыл қаскөйлер үшін қаржылық пайда әкелуі мүмкін, сондай-ақ веб-бағдарламаның иесіне қаржылық және беделді шығындарға алып келеді. Осы жағдайларға байланысты веб-бағдарламаның қауіпсіздік жүйесіне талдау жүргізу оның қауіпсіздігін арттыру мақсатындағы негізгі қадам болып табылады. Бұл жұмыста веб-бағдарламалардың осалдықтары мен қауіптілік көздеріне терең талдау жасалынып, сол талдау негізінде 6 кезеңге бөлінген талдау әдістемесі әзірленді.

Студент Ризуан Р. дипломдық жұмысты орындау кезінде өзінің жұмысқа деген ынтасын, оқу кезінде алған теориялық білімін практикада дұрыс қолдана білетіндігін айқын түрде көрсеткен.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
СӘТБАЕВ УНИВЕРСИТЕТІ

ЖҰМЫСТЫҢ БАҒАСЫ

Дипломдық жұмысты «__90__» бағалаймын және Ризуан Р. 5В100200 мамандығы бойынша әскери іс және қауіпсіздік бакалавры деген біліктілікке лайық деп санаймын.

Пікір беруші
Техника ғылымдарының кандидаты,
МАИН Академигі, "Ақпараттық қауіпсіздік жүйелері" кафедрасының профессоры
_____ Тынымбаев С. Т.
«___» _____ 2019 ж.

Отчет подобия

Университет:	Satbayev University
Название:	Веб-бағдарламалардың қауіпсіздік жүйесіне анализ жасау
Автор:	Рауан Ризуан
Координатор:	Азамат Иманбаев
Дата отчета:	2019-05-06 05:42:15
Коэффициент подобия № 1: ?	**0,2%**
Коэффициент подобия № 2: ?	**0,0%**
Длина фразы для коэффициента подобия № 2: ?	25
Количество слов:	6 169
Число знаков:	52 271
Адреса пропущенные при проверке:	
Количество завершенных проверок: ?	45

>> **Самые длинные фрагменты, определеные, как подобные**

>> **Документы, в которых найдено подобные фрагменты: из RefBooks** i

>> **Документы,содержащие подобные фрагменты: Из домашней базы данных**

>> **Документы,содержащие подобные фрагменты: Из внешних баз данных**

>> **Документы,содержащие подобные фрагменты: Из интернета**

Детали отчета подобия

Фрагменты, найденные в документах базы данных отмечены красным цветом.
Фрагменты, найденные в интернете отмечены в зеленый .
Фрагменты, найденные в базе данных Юридических актов отмечены синим фоном .

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Рауан Ризуан

Название: Веб-бағдарламалардың қауіпсіздік жүйесіне анализ жасау

Координатор: Азамат Иманбаев

Коэффициент подобия 1:0,2

Коэффициент подобия 2:0

Тревога:0

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

V обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
 обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
 обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

……
……
……
……
……

…… ……

Дата 13.05.19 *Подпись заведующего кафедрой /*

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

……
……
……Допущен к защите……
……
……

……

Дата 13.05.19 *Подпись заведующего кафедрой /*

начальника структурного подразделения

Протокол анализа Отчета подобия Научным руководителем

Заявляю, что я ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Рауан Ризуан

Название: Веб-бағдарламалардың қауіпсіздік жүйесіне анализ жасау

Координатор: Азамат Иманбаев

Коэффициент подобия 1:0,2

Коэффициент подобия 2:0

Тревога:0

После анализа Отчета подобия констатирую следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, признаю работу самостоятельной и допускаю ее к защите;

☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;

☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, не допускаю работу к защите.

Обоснование:

……
……
……
……
……
……

…… ……

Дата 13.05.19 *Подпись Научного руководителя*

АҢДАТПА

Дипломдық жұмыстың мақсаты: веб-қосымшалардың қауіпсіздік жүйесіне талдау жүргізу және талдау әдістемесін құру.

Міндеттері:

- веб-қосымшалардың осалдықтары мен статистикалық мәліметтерге сәйкес негізгі қауіп көздеріне зерттеу жасау;
- веб-қосымшалардың осалдықтары мен қауіп көздерін анықтауға арналған қосымшалар мен бағдарламалық жасақтамаларын түрлі баптауларда пайдаланып, оларға салыстырмалы талдау жүргізу;
- веб-қосымшалардың қауіпсіздігін талдау әдістемесін әзірлеу.

Веб-қосымшалардың қауіптеріне және осалдықтарына талдау жүргізілді, сондай-ақ, 6 кезеңнен тұратын веб-қосымшаны қауіпсіздікке талдау әдістемесі әзірленді.

АННОТАЦИЯ

Цель дипломной работы: разработка методики анализа и анализа системы безопасности веб-приложении.

Задачи:

- исследование уязвимости веб-приложении и основных источников риска в соответствии со статистическими данными;
- проведение сравнительного анализа приложений и программного обеспечения для выявления уязвимостей и источников угроз веб-приложении с использованием различных настроек;
- разработка методики анализа безопасности веб-приложении.

Был разработан анализ угроз и уязвимостей веб-приложений, а также метод анализа безопасности веб-приложения, состоящий из 6 этапов.

ANNOTATION

The purpose of the diploma project: development of methods of analysis and analysis of the security system web application.

Tasks:

- research of vulnerability of web application and main sources of risk according to statistical data;
- conducting comparative analysis of applications and software to identify vulnerabilities and sources of threats to the web application using various settings;
- development of methods of analysis of the security of the web application.

An analysis of threats and vulnerabilities of web applications was developed, as well as a method for analyzing the security of a web application, consisting of 6 stages.

МАЗМҰНЫ

КІРІСПЕ

Жұмыстың өзектілігі. Бүгінгі таңда, сарапшылардың айтуынша веб-бағдарламалар ақпараттық қауіпсіздік жағынан ең қауіпті жүйелердің бірі болып табылады, сондықтан веб-бағдарламалардың қауіпсіздігі ең өзекті тақырыптардың біріне жатады. Интернеттің жылдам дамуы кезеңінде көптеген шабуылдар осы веб-бағдарламаларда орын алады.

Веб-бағдарламалардың қауіпсіздігі ақпараттық қауіпсіздікті қамтамасыз етудегі ең өзекті мәселелердің бірі болып табылады. Бұл мәселенің өзектілігі ресми статистика арқылы расталады, оның негізінде веб-қосымшалардың 70% -ында сыни осалдық анықталды және барлық қосымшаларда осалдықтар орташа болып табылады. Соңғы үш жылда жоғары қауіпті кемшіліктерге ұшыраған жүйелердің үлесі 60-70% ішінде бірте-бірте артып келеді, бұл бағдарламалаушылардың кодты сапаға қатысты проблемаларға және әкімшілердің қосымшаларды конфигурациялау қауіпсіздігіне назар аудармайтындығын көрсетті.

Кез келген ұйымның қызметі қандай да бір түрде веб-технологиялармен байланысты. Интернет-дүкендердің, нарықтардағы, түрлі бизнес-қосымшалардың және қашықтан басқаратын банктік қызметтердің веб-порталдары кең таралған. Қазіргі заманғы ұйымды (ол ірі корпорация немесе шағын жеке компания болсын) Интернет желісінде өзінің ресми сайты болмауын елестету қиын. Клиенттік бағдарламалық жасақтаманы орнату және оны үнемі жаңартып отыру қажет корпоративтік қосымшалар бұрында қалып қойды. Веб-технологиялар бір платформада барлық іс-әрекеттерді атқару үшін бизнес-процестерді едәуір жеңілдетуге септігін тигізді.

Веб технологияларының артықшылықтарын барынша арттыру үшін мақсатты аудиторияға арналған ресурстардың қолжетімділігін қамтамасыз ету қажет, мысалы, Интернет желісі арқылы. Жалпыға қолжетімді веб-бағдарламалар зиянкестер үшін тартымды болып табылады. Веб-қосымшаларға жасалған шабуылдар оларға келесі мүмкіндіктерді береді: компанияның ішкі ресурстарына қолжетімділік, құпия ақпарат, бағдарламаның функционалдық жүйесін немесе бизнес-логиканы бұзу - кез-келген шабуыл шабуылдаушы үшін қаржылық пайда әкелуі мүмкін, сондай-ақ веб-бағдарламаның иесіне қаржылық және беделді шығындарға алып келеді. Сонымен қатар, веб-қосымшаларды пайдаланушылар тәуекелге ұшырайды, өйткені табысты шабуылдар тіркелу деректерін ұрлайды, пайдаланушылардың атынан сайттарда әрекеттерді орындайды және зиянды бағдарламалармен жұмыс жасауға қажетті ресурстарды жұқтырады. Веб-ресурстардың иелерінің басым көпшілігі веб-қосымшаның өмірлік циклінің барлық сатыларында қауіпсіздіктің қағидаларын сақтамайды, соның салдарынан осалдықтар дамудың ерте кезеңдерінде анықталмайды, ал ол бір

уақытта тауып оны эксплуатация жасағаннын өзінде ол веб-бағдарламада басқа уақытта қайта шығып қалады, сол себепті зиянкестерге оны бұзу едәуір оңайға түседі. Сондықтан веб-қосымшалардың қауіпсіздігін қамтамасыз ету қазіргі заманғы компаниялардың ақпараттық қауіпсіздік қызметтерінің басымдықтарының бірі болып табылады.

Зерттеудің объектілері - веб-бағдарламалардың қауіпсіздігіне қауіп-қатерлер болып табылады.

Зерттеудің құралдары - осалдықтарды іздеу әдісі және веб-қосымшалардың қауіпсіздігін бағалау.

Зерттеудің мақсаты - веб-қосымшалардың қауіпсіздігін талдау және талдау әдіснамасын әзірлеу.

Тапсырмалар.

- веб-қосымшалардың қауіпсіздігіне қойылатын осалдықтар мен қауіптердің негізгі түрлерін зерттеу және талдау. Зерттеудің негізінде веб-қосымшаның қауіпсіздігіне осалдықтар мен қауіптерді жіктеуді жасау;

- ағымдағы шабуылдардың және осалдықтардың талдауын жүргізу және әлеуетті осалдықтар мен типтік шабуылдардың синтезін жасау, тәуекел дәрежесі мен шабуылдың әлеуетін бағалауды жүргізу;

- веб-қосымшалардың осалдықтарын анықтау және талдау әдістерін зерттеу және сипаттауды жүргізу, олардың мүмкіндіктерін талдау және әр әдіс бойынша артықшылықтар мен кемшіліктерін анықтау;

- веб-қосымшалардың қауіпсіздік сканерлерін салыстырмалы тестілеуін өткізу;

- веб-бағдарламалардың қауіпсіздігін талдау әдістемесі әзірленді.

Зерттеудің теориялық маңыздылығы бар осалдықтарды, веб-қосымшалардың қауіпсіздігіне қауіп-қатерді зерттеуге және талдауға интеграцияланған тәсілді қолдану және мұндай осалдықтарды талдау және анықтау әдістері.

Жұмыстың практикалық маңыздылығы әзірленген әдістеме, жіктеу және тізімдер тәжірибеде қолданылуы мүмкін, осал тұстарын анықтау және зерттеу әдістерінің көмегімен жалпы қауіпсіздікті бағалау үшін веб-қосымшалардың қауіпсіздігі бойынша тестілеуді жүргізу кезінде қолданылуы абзал.

1 Веб-қосымшалардың ақпараттық қауіпсіздігіне қауіп-қатерлер

Ақпараттық қауіпсіздік термині әдетте табиғи немесе жасанды сипатта болатын рұқсат етілмеген әрекеттердің (кездейсоқ немесе қасақана) әр түрлі түрлерінен ақпарат пен оның инфрақұрылымын қорғау деңгейіне қатысты болып келеді. Бұл әрекеттер ақпарат иелеріне немесе пайдаланушыларына, сондай-ақ қолдайтын инфрақұрылымға зиянын тигізуі мүмкін.

Ақпараттық жүйелердің қауіпсіздік деңгейін жақсырақ түсіну үшін ақпараттық қауіпсіздіктің қауіп-қатерлерінің пайда болу көздеріне назар аудару керек.

Веб-бағдарламаның қауіпсіздігіне тікелей немесе жанама зиян келтіруі мүмкін ықтимал процесс, оқиға немесе құбылыс қауіп деп аталады. Қауіп ақпараттың өзіне де, осы ақпарат сақталатын әзірлеу процестеріне де және тасымалдаушыларға да әсер етуі мүмкін.

Ақпарат қауіпсіздігіне қауіп төндіруді жүзеге асыру әрекеті шабуыл деп аталады, ал осындай әрекет жасауға бастамашы тұлға – қаскүнем немесе шабуылдаушы болады.

Қауіпсіздік қатерінің көздері болуы мүмкін:

- жабдықтың (техникалық құралдардың) істен шығуы және бұзылуы;
- қаскүнемдердің қасақана әрекеттері;
- веб-бағдарлама компоненттерін жобалау және әзірлеу қателіктері;
- веб-бағдарламаны пайдалану қателіктері (пайдаланушылар, әкімшілер және басқа субъектілер).

Жиі қауіп - қатер веб-қосымшадағы осал жерлердің болуының салдары болып табылады, бірақ олардың кейбіреулері қандай да бір қателіктердің немесе қателіктердің нәтижесі ретінде қарауға болмайды. Олар әдетте қазіргі заманғы веб-қосымшалардың табиғатына байланысты болады.

Мүмкін қауіптерді екі ішкі сыныпқа бөлуге болады: субъективті (жасанды) және объективті (табиғи) [А.1.1-сурет]

Субъективті - бұл адам қызметі арқылы туындаған қатерлер. Іс-әрекеттің себептеріне қарай, бұл қосалқы екі классқа бөлінуі мүмкін: қасақана емес және қасақана.

Қасақана емес - жұмыс барысында қателіктер мен ақпараттық және бағдарламалық қамтамасыз ету әрекеттерімен, веб-қосымшаның құрылымын, оның элементтерін және т.б. жобалаумен айналысатын кезде кететін қауіптер болып саналады.

Қасақана - бұл қауіптер идеологиялық көзқарастармен, кек алудан, зиянкестердің жалған мақсаттарымен және тағы басқалармен байланысты жасалынатын қауіп-қатерлер.

Объективті - бұл ақпараттық жүйеге және оның құрамдас бөліктеріне объективті физикалық құбылыстар мен табиғи стихиялық процестер арқылы

ықпал ететін қауіп-қатерлер.

Қауіп-қатерді іске асыру үшін қолданылатын негізгі құралдардың түріне сәйкес, жүйеге енудің барлық ықтимал арналары мен ақпараттың ағып кетуін үш топқа бөлуге болады [А.1.2-сурет], мұндай қолданылу тәсілі: субъект (адам), бағдарлама, жабдықтар.

Веб-бағдарлама қауіпсіздігінің қауіп-қатерлерінің негізгі түрлері:

- конфиденциалдыққа қаупі – деректерге рұқсатсыз қатынас алу;
- тұтастылыққа қаупі – рұқсатыз деректерді өзгерту немесе оларды жою;
- қол жетімділік қаупі - деректерге кіруді шектеу немесе бұғаттау;
- қорғалған компьютерлік жүйенің параметрлерін жариялау қаупі.

Ақпараттық қауіпсіздік аспектісі бойынша веб-бағдарламаларға қауіптерді жіктеу [А.1.1 - кесте] келтірілген.

Веб-жүйенің орындалуының бұзылу түрлері мен қауіпсіздікке және әсер ету объектілеріне зақым келтіру әдістеріне сәйкес деректерге рұқсатсыз кірудің жіктелуі [А.1.2-кесте] келтірілген.

Веб-қосымшаларға арналған ақпараттық қауіпсіздік қатерлерінің негізгі көзі *хакерлер* болып табылады (сыртқы құқық бұзушылар). Бұл адамдар шабуылдардың көмегімен веб-қосымшаға, ұйымның беделіне немесе оның коммерциялық мүдделеріне зиян келтіретін дәлелді тұлғалар болып табылады. Сыртқы зиянкестер, әдетте, шабуылға ұшыраған жүйені білмейді, желінің қауіпсіздігін қамтамасыз ету мәселелерінде жоғары біліктілігі бар және ақпараттық жүйелердің әртүрлі түрлеріне түрлі желілік шабуылдарды жүзеге асыруда үлкен тәжірибеге ие.

1.1 Веб-қосымшаларға шабуылдар

Шабуылдардың сипаты

Веб-қосымшаға шабуылдар екі негізгі себептерге байланысты таралады: әлеуетті зиянкестердің кіру шегінің төмендігі және веб-қосымшаның қауіпсіздігіне немқұрайлы қарау, әр түрлі сатыларда: жобалаудан бастап, қолдауға дейін.

Негізгі массада веб-ресурстарда арнайы қорғау, мониторинг және анықтау құралдары пайдаланылмайды, бұдан басқа веб-қосымшаның қауіпсіздігіне жауап беретін персонал жоқ. Сондай-ақ веб-ресурстың қауіпсіздігіне төнетін қауіп-қатерлер туралы тиісті хабардарлықтың деңгейі жоқ. Веб-серверді қауіпсіз күйге келтіру үшін (және веб-қолданбалар) аз көңіл бөлінеді.

Сканерлерді танымал ету және тарату және қауіпсіздік утилитасы әлеуетті зиянкестердің кіру шегінің төмендігін алдын ала анықтайды. Ал көптеген қауымдастықтар мен "хакер аралық" форумдар шабуыл техникаларының таралуына ықпал етеді. Сонымен қатар, бұған жаңа

осалдықтар мен шабуылдардың техникалық аспектілері туралы жедел және кең жариялану ықпал етеді.

Веб-қосымшаларға шабуыл түрлері

Хакерлер веб-қосымшалар қауіпсіздігінің негізгі қатері болып табылады, олардың шабуылдары жүйелі (түпкі мақсаты болуы), сондай-ақ жүйесіз сипатта болуы мүмкін. Бірінші жағдайда қылмыскер бұзудың ықтимал сәтті сценарийлерін қалыптастыру және жүзеге асыру мақсатында шабуыл векторларының шекті ықтимал санын анықтауға мүмкіндігі бар, ал екінші жағдайда веб-қосымшаларда, әдетте, беттік осалдықтардың қатарын пайдалана отырып, жаппай шабуыл жасайды.

Мақсатты шабуылдар - бұл жалғыз веб-сайтқа немесе жалпы белгімен біріктірілген веб-сайттар тобына әдейі бағытталған шабуылдар (мысалы. бір компанияның сайттары). Мұндай шабуылдардың негізгі қаупі көбінесе "тапсырысты шабуылдар" болып табылады, сондықтан мұндай шабуылдардың орындаушылары әдетте веб-қосымшалардың қауіпсіздігі саласында жоғары білікті зиянкестер болып табылады. Осы шабуылдардың мақсаты теріс пиғылды бәсекелестер немесе қылмыскерлер пайда табу үшін пайдалануы мүмкін құпия деректерді алу болып табылады.

Мақсатсыз шабуылдар - бұл іс жүзінде "сәттілікке" жүргізілетін шабуылдар, ал олардың құрбандары қызмет аясына, танымалдығына, географиясына немесе мөлшеріне қарамастан кездейсоқ веб-ресурстар болып табылады. Веб-қосымшаға мақсатсыз шабуыл - бұл интернет - ресурсқа рұқсатсыз қол жеткізу әрекеті, бұл ретте қылмыскер нақты сайтты бұзуды мақсат етпейді,ал қандай да бір критерий бойынша бөлінген жүздеген немесе мыңдаған ресурстарды бірден шабуылдайды. Мысалы, сайтты басқару жүйесінің белгілі бір нұсқасында жұмыс істейтін веб-сайттар. Мұндай шабуылдар ең аз шығынмен веб - қосымшалардың ең көп санын қамтуға тырысады.

Егер шабуыл сәтті болса, қаскүнем осы пайданы алуға ұмтылады: веб-ресурста тіркелу, зиянды кодты енгізу, деректер базасынан қажетті ақпаратты алу, әкімшіні қосу немесе "хакерлік" скриптті (бэкдор, веб-шелл) жүктеу.

Мақсатты шабуылдар-құпия жүргізіледі, әдетте өз мақсатына жетеді. Мақсатсыз шабуылдар жеткілікті "шулы" және жиі қойылған міндеттерге қол жеткізе алмайды, алайда интернет-ресурстың иесіне көптеген проблемаларды жеткізе алады.

1.2 Веб-қосымшалар қауіпсіздігінің осалдықтары мен қауіптерін жіктеу және сипаттау

Веб-қосымшаның қауіпсіздігіне қандай әдіспен талдау жүргізу керек екенін анықтамас бұрын, алдымен ықтимал қауіп-қатерлер мен осалдықтарды зерттеу қажет. Web Application Security Consortium Threat Classification жүйесі бойынша тиісті қауіптерге сәйкес 6 сыныптарды біріктіре отырып, осалдықтардың өзекті түрлерін және оларды пайдаланатын шабуылдарды жіктейміз және сипаттаймыз:

- ақпаратты жария ету;
- аутентификация;
- авторизация;
- клиенттерге шабуылдар;
- кодты орындау;
- логикалық шабуылдар.

Trustwave мәліметтері бойынша, көптеген компаниялар веб-бағдарламаларға шабуыл жасау қаупін дұрыс бағалай алмайды, олардың 66%-ы осалдықтарға өздерінің веб-бағдарламаларының тек 25% - ын ғана сынақтан өткізді. Бұл ретте фирмалардың 20% бұл процестің еңбек сыйымдылығы мен ұзақтығына байланысты тестілеу өткізбейді, ал40% өзінің веб-бағдарламаларының тек 5% ғана тестілейді.

Бұл жіктеу веб-қосымшаның қауіпсіздігін талдауды барынша жеделдету және жеңілдету және өзекті осалдықтар мен танымал шабуылдарға назар аудару үшін ұсынылады.

Осындай жіктеуді енгізудің орындылығы қазіргі кезде мұндай жіктеу жоқ болғандықтан, веб-қосымшалардың инфрақұрылымын дамыту есебінен осалдықтар мен шабуылдардың негізі ғана бар, олардың кейбіреулері қазір қолданылмайды немесе осалдықтар өздерінің өзектілігін жоғалтты.

Ақпаратты ашу

Бұл бөлім веб-бағдарлама туралы қосымша ақпарат алуға бағытталған шабуылдарды ұсынады. Осы осалдықтарды пайдаланған кезде құқық бұзушы қандай бағдарламалық жасақтаманың таратылуын, жаңартуларды, серверді және клиенттік нұсқасын орнатуды анықтау мүмкіндігіне ие болады. Кейбір жағдайларда, ұрланған ақпаратта уақытша файлдар мен сақтық көшірмелер болуы мүмкін. Көптеген веб-серверлер деректердің үлкен көлеміне рұқсат береді, сондықтан қызметтік ақпараттың көлемін азайту қажет. Шабуылдаушы, егер ол үлкен білім көлеміне ие болса, веб - бағдарламаны бұзып алуы оңай болады.

Директорияларды индекстеу.

Клиент веб-бағдарламаның басты бетін сұрағанда, ол, әдетте, домен атауын файл атаусыз көрсетеді, яғни сервер автоматты түрде директорияда

әдепкі файлдарды табады және жауапты жасайды, бірақ мұндай файлдар жоқ болса, пайдаланушы жауап ретінде веб-сервердегі директориядан файлдар тізімін ала алады.

Мұндай жағдайда құқық бұзушы еркін қол жеткізуге арналмаған мамандандырылған деректерге қол жеткізуге мүмкіндігі бар.

Жиі веб-бағдарламалардың әкімшілері гиперсілтеме жоқ болса, ол пайдалануышыларға көрінбейді деп пайымдай отырып, "жасыру арқылы қауіпсіздікті" есептейді.

Қазіргі заманғы осалдық сканерлері сұраныстардың нәтижелері негізінде сканерленетін тізімге файлдар мен директорияларды динамикалық түрде қосуға мүмкіндігі бар. Каталогтар тізіміне немесе «robots.txt» мазмұнына сүйене отырып, сканер жасырын файлдар мен каталогтарды таба алады. Сыртқы, анықтамалықтарды қауіпсіз индекстеу, веб-қосымшаға шабуылдауға қолданылатын құпия ақпараттың ағып кетуіне әкелуі мүмкін.

Бағдарламаны идентификациялау.

Сервер мен клиенттің операциялық жүйелері, браузерлері мен веб-серверлері туралы ақпарат алу үшін шабуылдаушы бағдарламалардың нұсқаларын идентификациялауды пайдаланады. Бұл шабуыл деректер қорының сервері немесе каталог қызметі сияқты басқа веб-қолданбаның құрамдас бөліктеріне де бағытталуы мүмкін.

Әдетте мұндай шабуылдар веб-қосымшаның серверімен ұсынылатын әр түрлі деректерді талдау арқылы орындалады:

- cookie мәні;
- HTTP жауап тақырыптары;
- каталог құрылымы;
- веб-қосымшаларды әзірлеуді қолдау интерфейстері;
- серверді басқару интерфейстері;
- HTTP протоколын іске асыру ерекшеліктері;
- сервер пайдаланатын файл кеңейтілімдері.

Аутентификация

Бұл қауіптер класында веб-серверлерді аутентификациялауды іске асыруда осалдықтарды айналып өтуге және пайдалануға бағытталған шабуылдар сипатталады.

Brute force - автоматты іріктеу процесі, құпия сөзді, пайдаланушының атын, шифрлау кілтін және т.б. табу мақсатында қолданылады.

Көптеген жүйелер кішкене парольдерді немесе шифрлау кілттерін қолдануға мүмкіндік береді, және жиі қолданушылар парольдік сөздердің сөздіктерінде оңай табылатын сөз тіркестерін қолданады.

Осы фактіні назарға ала отырып, қаскүнем сөздіктерді пайдалана алады және ондағы комбинациялардың көптеген санын құпия сөз орнына қолдануға тырысады.

Таңдаудың екі түрі болады: тура және кері. Тура таңдау кезінде бір пайдаланушы аты үшін әр түрлі құпия сөздерді тестілейді. Тура таңдауға қарағанда, кері таңдау пайдаланушылардың әр түрлі аттары іріктеледі, ал пароль тұрақты болып қалады. Танымалдығына және жоғары тиімділігіне қарамастан, таңдау бірнеше сағаттан бірнеше айға дейін өте көп уақыт алады.

Жеткіліксіз аутентификация

Бұл осалдылық, егер веб-сервер шабуылшыға маңызды ақпаратқа немесе сервердің функцияларына тиісті аутентификация болмаған жағдайда қол жеткізуге мүмкіндік берсе пайда болады. Веб бағдарламаны әкімшілеу интерфейстері осы осалдықтың бірден-бір мысалы болады.

Мұндай компоненттер тиісті аутентификациясыз қол жетімді болмауы керек. Аутентификацияны пайдаланбау үшін кейбір ресурстар сервердің негізгі беттерінде немесе басқа қол жетімді ресурстарда көрсетілмейтін мекенжайда «жасырын» болады. Бірақ мұндай тәсіл "жасыру арқылы қауіпсіздік" қана, сондықтан бұл да осалдыққа жатқызылады. Қаскүнем беттің мекенжайын білмейтініне қарамастан, мұндай бет Интернет арқылы да қол жетімді екенін түсіну маңызды.

Қажетті URL стандартты файлдар мен директораларды (/admin/ ұқсас) таңдау арқылы, айқас сілтемелер журналын, қате туралы хабарларды немесе қарапайым құжаттаманы оқу арқылы анықтауға болады.

Авторизация

Бұл класс қолданба, қызмет немесе пайдаланушы әрекеттерді жасау үшін қажетті рұқсаттарға ие болуын анықтау мақсатында веб-сервер пайдаланатын әдістерге негізделген шабуылдарға арналған. Кейбір веб-бағдарламалар тек арнайы рұқсаты бар қолданушыларға ғана бағдарламаның кейбір мүмкіндіктеріне қол жетімділікті ашады. Ал, басқа қолданушыларға ол мүмкіндіктер жабық болу керек. Қаскүнем әртүрлі техникаларды қолдану арқылы өздерінің қол жетімділіктерін арттыра отырып, қорғалған ресурстарға қол жеткізуі мүмкін.

Жеткіліксіз авторизация

Егер веб-сервер зиянкестерге басқалардан бұғатталған маңызды функционалға және деректерге қол жетімділік берсе, осы жағдайда жеткіліксіз авторизация пайда болады. Пайдаланушы аутентификациядан сәтті өткен болса да, сервердің барлық функционалы мен мазмұнына қол жеткізбеуі тиіс. Қолжетімділікті шектеу механизмі іске асырылуы тиіс.

Авторизациялау үрдісі пайдаланушы, бағдарлама немесе қызмет жасай алатын әрекеттерді анықтайды. Маңызды веб-қолданбалар тек әкімшіге қол жетімді болуы керек. Бұл қауіпсіздік саясатына сәйкес пайдаланушының іс-әрекетін шектеуі тиіс және қол жеткізу ережелерін дұрыс құру арқылы ұйымдастырылған болуы керек.

Сессия таймаутының болмауы

Қаскүнем егер сессия таймауты қарастырылмаса, идентификатор және есептік деректер үшін ескі мәліметтерді авторизациялау үшін пайдалануға мүмкіндігі пайды болады. Осыған байланысты идентификациялық деректерді ұрлаумен байланысты шабуылдар үшін сервердің қорғалмауы артады. Веб-серверлер пайдаланушылардың сұраныстарын анықтау мақсатында сессия идентификаторларын қолданады, өйткені HTTP протоколы сессияны ешқандай бақыламайды. Пайдаланушылардың бір тіркеу жазбасымен қатар кіруін болдырмау үшін әрбір идентификатордың құпиялылығы қамтамасыз етілуі тиіс. Ұрланған идентификатор пайдаланушының деректеріне қол жеткізу немесе алаяқтық транзакцияларды жүзеге асыру мақсатында қолданылуы мүмкін. Егер веб-серверде сессия таймауты болмаса,онда бұл барлық шабуылдардың мүмкіндігін арттырады. Қаскүнем желілік анализатордың көмегімен немесе сайтаралық скриптинг түрінің осалдығын пайдалану арқылы сессия идентификаторына қол жеткізе алады.

Қолданушыларға шабуыл

Бұл шабуылдар классы веб-сервердің пайдаланушыларына жасалған шабуылдар түрін білдіреді. Веб-бағдарламаны қолдану кезінде веб-сервер мен пайдаланушы арасында сенімді қарым-қатынас орнатылады. Пайдаланушы веб-сервердің қауіпсіз екеніне сеніп, оның тарапынан ешқандай шабуылдарды күтпейді. Қаскүнем осы мүмкіндікті пайдаланып шабуылды ұйымдастырады.

Сайтаралық сценарийді орындау

Cross-Site Scripting (XSS) - веб-бағдарламаға шабуылдың бұл түрі веб-жүйе арқылы шығарылған бетке зиянды кодты кірістіруден тұрады. Пайдаланушы бұл бетті ашқанда, кірістірілген код дереу орындалады және шабуылдаушының веб-серверімен өзара әрекеттеседі.

Кірістірілген зиянды код қаскүнемге кіру үшін пайдаланушының авторизациясын қолдана алады немесе пайдаланушы авторизациялау деректерін ала алады.

Зиянды кодты сайт бетіне веб-сервердегі осалдық немесе пайдаланушы компьютеріндегі осалдық арқылы кірістіруге болады.

XSS шабуылдарының 3 нұсқасы бар:

- тұрақты (сақталатын) XSS. Java script серверде немесе сайтта сақталады;

- тұрақты емес (көрсетілетін) XSS. Пайдаланушы арнайы сілтемеге басқан кезде орындалады;

- DOM моделіндегі XSS. Ол зиянкестердің серверге деректерді жіберуіне негізделген.

Positive Technologies зерттеуіне сәйкес, XSS веб-сайттарға шабуылдар жалпы шабуылдардың 3% -ын құрайды.

Тұрақты XSS - кросс-сайтты сценарийлік шабуылдың ең жойғыш түрі. Шабуылдаушы сайтқа немесе серверге зиянды кодты енгізуді басқарған кезде

орындалады. Зиянды код ендірілген сайт бетіне кіру кезінде әр уақытта орындалатын болады. Хабарларды сүзгілеусіз пікір қалдыра алатын форумдар бұл шабуылға классикалық мысал болып табылады.

Тұрақты емес (көрсетілетін) XSS шабуылы ең көп таралған шабуыл есебіндегі XSS болып табылады. Шабуылдың бұл түрі URL немесе HTML түріндегі пайдаланушы ұсынған ақпаратты дұрыс деректерді өңдемей жауапты жасағанда мүмкін болады.

XSS шабуылдарынан қорғану үшін келесі әдістерді пайдалануға болады:

- кіріс / шығыс деректерін экрандау. Біртаңбалы емес таңбаларды біртаңбалыға алмастыру. «<Және>» таңбалары адам ретінде де, компьютермен де қабылданады. Мысалы, "<" символын жазатын болсақ ол "<" осы символға тең болады, ал егер ">" символын жазатын болсақ ол ">" осы символға тең болады;

- «ақ тізімдерді» қолдану. Символдарды тек арнайы жолдарда ғана қолданылатын жолдарға теруге рұқсат беру. Сандарды теретін жолға тек сандарды, ал әріптерді теретін жолға тек әріптерді теруге рұқсат беру.

Сайтаралық жалған сұраныс жасау

Кросс-сайтты сұраныстарды жалған ету (CSRF) - HTTP хаттамасының кемшіліктерін пайдаланатын веб-торапқа кірушілерге жасалған шабуыл түрі. Егер қолданушы шабуыл жасаған сайтқа кірсе, онда сұраныс басқа серверге (мысалы, төлем жүйесінің серверіне) жасырын түрде басқа зиянды әрекетті орындауға жіберіледі (мысалы, шабуылдаушының шотына ақша аудару). Бұл шабуылды жүзеге асыру үшін қолданушы сұраныс жіберілген серверде аутентификациядан өткен болуы керек және бұл сұраныс пайдаланушыдан ешқандай растауды талап етпеуі керек (шабуыл жасайтын скриптті жасыруға болмайды, яғни, шабуылдайтын скрипт оған қарсы әрекет жасай алмайды сол себепті шабуыл іске аспай қалады.

SQL операторларын орындау

SQL операторларын орындау - дерекқорлармен жұмыс істейтін веб-сайттарды және бағдарламаларды бұзудың танымал әдістерінің бірі. Бұл шабуыл сұранысқа SQL-кодтың ендірілуімен жүзеге асады.

SQL инъекциясы, пайдаланылатын ДҚБЖ түріне және орналастыру шарттарына байланысты, зиянкестерге дерекқордың сұранымдарын жасауға мүмкіндік береді (мысалы, кез келген кестелердің мазмұнын оқу, деректерді жою, өзгерту немесе қосу), жергілікті файлдарды оқу және / немесе жазу мүмкіндігін алу шабуылдаған серверде ерікті командаларды орындайды.

Бұл шабуыл SQL сұраныстарында пайдаланылатын кіріс деректерін дұрыс өңдемеу кезінде мүмкін болады. Мысалы, келесі түрдегі тестілік сайт бар делік [А1.7 - сурет].

http://осал_сайт/movies/php?id=1

Егер сұранысты «?id=1'» немесе «?id=1"» түрінде өзгертсек, онда суреттегідей [А1.6-сурет] қателік шығарады. Демек, бұл сайт SQL injection шабуылына қарсы қорғалмаған.

SQL шабуылдарынан қорғау үшін, SQL сұраныстарды құру үшін пайдаланылатын кіріс параметрлерін сүзгілеуді пайдаланады:

- сандық параметрлердің дұрыстығын тексеру. PHP-де сандық параметрлердің дұрыстығын тексеру үшін is_numeric (n) функциясын пайдалана аласыз;

- қатарлардың параметрлерінің дұрыстығын тексеру

- символдарды экрандау. PHP серверлі тілінде addslashes ($string); және mysql_real_escape_string($str) функцияларын пайдалануға болады.

Логикалық шабуылдар

Бұл шабуыл түрлері веб-бағдарламаның логикалық функционалдығына немесе қолдану функциясына бағытталған. Веб-бағдарламаның кейбір міндеттерді орындау үшін пайдаланушыдан кезекпен дұрыс орындауды талап етуге мүмкіндігі бар. Шабуылдаушы осы механизмдерді өз мақсаттарында айналып өтуге және қолдануға қабілетті.

Қызмет көрсетуден бас тарту

Қызмет көрсетуден бас тарту (DoS) шабуылы - есептеу жүйесіне қарсы шабуыл. Барлық желілік құрылғыларда бір уақытта өңделетін сұраныстар саны бойынша шектеулер бар. Бұдан басқа, сервер Интернетпен байланысатын арнада өткізу қабілеті шектеулі. Сұраныстар саны шектік мәндерден асса, төмендегі сияқты мәселелер орын алады:

- сұраныстарға жауап әдеттегіден әлдеқайда баяу қалыптасады;

- кейбір пайдаланушылар, мүмкін, барлығы кері жауапсыз қалады.

Қалаған ресурсқа тым көп сұраныстар жіберу үшін, шабуылдаушылар ботнетті (трояндық вирустармен зарарланған компьютерлердің зомби желісі) пайдаланады. Бұл шабуыл *Distributed Denial of Service (DDoS)* атпен белгілі. Оның айырмашылығы мынадай: DoS-шабуыл бір компьютерден шықса, онда DDoS-шабуыл бірнеше компьютерден келеді. Компьютер иелері көбінесе олардың компьютері осы шабуылға қатысы бар деп күдіктенбейді. [Б1.3-суретте] DDOS шабуылының орындалу сұлбасы көрсетілген.

1.3 Енгізілген жіктемені талдау негізінде веб-қосымшалардың осалдықтары мен оларға жасалатын шабуылдардың синтезделген тізбесі

Әлеуетті осалдықтар мен веб-қосымшаның қауіпсіздігіне төнетін қауіп-қатерлерге және енгізілген жіктемеге жүргізілген зерттеу негізінде, сондай-ақ Positive Technologies компаниясының зерттеу статистикасы мен зерттеу мақалаларының негізінде өзекті шабуылдар мен осалдықтарға талдау

жүргізілді және 1.3 кестеде ұсынылған тізбе қалыптастырылды. Қалыптасқан тізбеде әлеуетті осалдықтар мен осы осалдықтарға типтік шабуылдар синтезі жүргізілді,сондай-ақ тәуекел дәрежесі мен шабуыл әлеуетіне баға берілді.

Алдымен, келтірілген жіктемеге сәйкес қандай осалдықтар анағұрлым өзекті екені қарастырылды. Positive Technologies компаниясының 2018 жылғы осалдықтарының таралуын талдау деректері бойынша тестіленетін веб-бағдарламалардың көпшілігінде табылған ең көп таралған осалдықтар: сайтаралық скриптинг (XSS), ақпараттың ағуы, таңдау (Brute force), БҚ идентификациясы, директорияларды индекстеу, сұраныстарды қолдан жасау, SQL командаларын ендіру (SQL injection), авторизация [А1.4-сурет].

Positive technologies зерттеуінің веб-бағдарламаларға жасалынатын шабуылдар статистикасына сәйкес 2018 жылда келесі шабуылдар ең өзекті болған [А1.5-сурет]. Сайтаралық сценарийді орындау, SQL командаларын ендіру, белгіленген директория сыртынан шығу (Path Traversal), жергілікті файлдарды қосу, ОЖ командаларын және кодты алшақ орындау және т.б.

2 Бастапқы кодтарға жүгінбей веб-қосымшаның жұмысын талдау әдістері

2.1 Веб - бағдарлама туралы идентификациялық ақпаратты алу және қауіпсіздік бюллетеньдерінің көмегімен осалдығын анықтау

Бұл әдіс веб-қосымшаның қарапайым пайдаланушысы атынан HTTP-сұраныстарды теруді жіберуге негізделген, мұндай сұраныстарға жауаптар веб-бағдарламаның қай веб-серверде жұмыс жасайтынын, деректер базасының қай сервері пайдаланылатынын, БҚ-ның қандай нұсқалары пайдаланылатынын, қандай технологияның көмегімен жасалғанын және т. б. қорытынды жасауға мүмкіндік береді. Идентификациялық мәліметтер HTTP - жауаптардың тақырыптары мен HTTP-беттер мәтіндерінде болуы мүмкін.

Нақты веб-бағдарламаның қолданатын веб-сервистер мен технологиялар сәйкестендірілгеннен кейін "қауіпсіздік бюллетендері" арқылы осалдықты анықтауға болады. Бұл деректерді жинау *fingerprinting* деп аталады. Бұл жағдайда көрінетін осалдық "бағдарламаны идентификациялау" деп аталады.

Веб-бағдарламаны пайдаланушы идентификациялық деректерді алу мүмкіндігі келесі себептер бойынша әлеуетті осалдық болып саналады:

Интернет желісінде үлкен деректер базасы бар, онда бағдарламалық өнімнің нұсқасына жазылған бағдарламалық өнімдердің осалдығы бойынша ақпараттың үлкен көлемі сақталады, сондай-ақ шабуылдарды іске асыру әдістерін тауып алу қиынға соқпайды.

Security Focus және Bugtraq қауіпсіздік бюллетендері күн сайын ең жаңа табылған осалдықтар туралы есептерді жариялайды. Бұл мәліметтер ақпараттық қауіпсіздік саласындағы сарапшылар мен веб-ресурстар әкімшілеріне арналған,сондай-ақ осы ақпаратқа қолжетімділікті интернет желісі арқылы кез келген адам ала алады. Көбінесе веб-жүйелердің әкімшілері қауіпсіздікті жаңартуды уақытында белгілемейді, бұл өз кезегінде әкімші бағдарламалық қамтамасыз етуді тиісті жаңарту қондырғысымен жаппаған белгілі осалдықты пайдалану арқылы ақпараттық жүйені бұзу мүмкіндігіне әкеледі. Алдыңғы жылдары операциялық жүйелердің өте жақсы белгілі және жабылмаған осалдықтарына Интернет-құрттардың кеңінен танымал індетін тудырған көптеген шабуылдар ұйымдастырылды.

Бағдарламалаушылар жиі веб-қосымшалардың жеке дайын модульдерін қолдана отырып, құрамдас негізде сайтты қалыптастыратынын ескеру маңызды. Сыртқы компоненттер - чат, форум, оқиғалар күнтізбесі, хабарландыру тақтасы және т. б. сияқты Интернет-сервистердің модульдері болып табылады. Ішкі компоненттер веб-бағдарламаны әзірлеу технологиясының құрамына енгізілген. Компоненттердің бірінде осалдықтар

анықталған жағдайда, осы компонентті пайдаланатын барлық веб-ресурстар қауіп төндіреді.

Веб-бағдарлама туралы идентификациялық ақпаратты алу әдісінің артықшылықтары.

Қарапайымдылығы мен қол жетімділігіне байланысты кең практикалық пайдалану. Әдістің пайдалылығы, ол веб-бағдарлама туралы ақпараттың ағып кету мүмкіндігін көрсетуінде болып табылады.

Веб-бағдарлама туралы идентификациялық ақпаратты алу әдісінің кемшіліктері.

Бұл әдіс жаңа осалдықтарды табуға мүмкіндік бермейді. Идентификациялық ақпаратты іздеу орындалатын шаблонды баптау үшін маман қажет. Негізгі массадағы үлгілер веб-қосымшаны әзірлеудің әрбір технологиясына тән.

2.2 Енуге тестілеу әдісі

Қазіргі уақытта енуге тестілеу сияқты осалдықтарды анықтаудың мұндай әдісі ең тиімді болып табылады. Ол шабуылдың ықтимал жолдарын анықтауға және веб - қосымшаның ымыраласуына жол бермеуге мүмкіндік береді. Енуге тестілеу әдісі сыртқы пайдаланушы, яғни әлеуетті шабуылшы тарапынан веб-бағдарламаны қарауға қолайлы. Шабуылдаушының тек әдеттегі пайдаланушы сияқты мүмкіндіктері бар деп есептеледі, яғни конфигурациялық баптауларға, веб-қосымшаның бағдарламалық кодтарына ешқандай рұқсаты жоқ және т. б. Бұл әдіс шабуылдаушының іс-әрекетіне ұқсас қате сұраныстарды қамтитын пайдаланушылық белсенділікті модельдейтін сұраныстарды жіберу арқылы веб-қосымшаның стендінде толық жұмыс істейтін веб-қосымшаларды тестілеуді жүзеге асырады.

Веб-бағдарламада осалдықтарды анықтау үшін енуді тестілеу әдісін қолданғанда үш негізгі тапсырма пайда болады:

- веб-бағдарламаның құрылымын зерттеу және талдау;
- веб-бағдарламаның зерттелген және жасалған құрылымы негізінде тестілік HTTP сұраулар жиынтығын жасау;
- қауіпсіздік осалдығын анықтау үшін веб-бағдарламаның жауаптарын талдай отырып, оны айдап өту арқылы тестілік жиынтығын сынау.

Тапсырма веб-бағдарламаның құрылымын зерттеу және талдау веб-қосымшаның толық URI тізімін, параметрлер тізімін және оларға кіру әдістерін жасау, аутентификациямен қорғалған URI табу болып табылады. Бұл мәліметтер веб-бағдарламаға тестілік сұраныстар тізімін құру үшін қажет. Веб-бағдарламаның құрылымын автоматты түрде шығару үшін желілік роботтар қолданылады. Егер веб-бағдарламаның статикалық HTML беттері бар болса, жұмыс барлық қол жетімді сілтемелерді айналып өту, ал скрипттер мен

формалар болған жағдайда - скриптерден гиперсілтемелер алу және формаларды толтыру болып табылады. Веб-бағдарламаның толық құрылымын зерттеу және алу барлық жағдайларда мүмкін емес - негізгі мәселе скрипттерді интерпретациялау және веб-формаларды толтыру кезінде пайда болады.

Веб-формаларды 2 топқа бөледі:

1) Мәндердің шектеулі салалары бар компоненттерді қамтитын формалар (option, selection және т. б.).

2) Мәндердің шексіз салалары бар компоненттерді қамтитын формалар (textarea).

1-типті формаларды жөнелтумен байланысты беттерді айналып өту және талдау осы формадағы өрістер мәндерінің барлық ықтимал комбинацияларын кезекпен орындау арқылы жүзеге асырылады. Шексіз мәндерді қабылдайтын формаларды айналып өту үшін келесі екі тәсілді қолданады: автоматтандырылған немесе қолмен. Процесті қолмен басқару үшін адамға беріледі. Автоматтандырылған тәсілде эвристикалық әдістер, HiWE VeriWeb сияқты сөздіктерде негізделген мәтіндік өрістерді толтыру қолданылады. Шексіз мән аймағы бар элементтерді қамтитын формалар үшін автоматтандырылған амалды пайдаланғанда, бағдарламаның барлық URI анықтауға кепілдік берілмейді. Скрипт тілінің құралдарымен жасалатын сілтемелерді қамтитын беттерді автоматты түрде аралау кезінде тек интерпретациялау ғана емес, сондай-ақ белгілі бір оқиғаларды қалыптастыру мақсатында пайдаланушы жасайтын әрекеттерді эмуляциялау қажеттілігі бар. Қазіргі уақытта бар скрипті тілдерін интерпретациялау құралдары барлық гиперсілтемелерді анықтауға кепілдік бере алмайды.

Веб-бағдарламаға сұраныстардың тестілік жинағын жасау міндеті бастапқы деректерге (кіру әдістері, қабылданатын параметрлер, URI тізімі) сәйкес сұраныстарды мүмкіндігінше осалдықтар табу үшін таңдау болып табылады. Мұндай сұраныстарды құрудың қолданыстағы тәсілдері төменде қарастырылған:

Веб-бағдарлама каталогтарының параметрлерін талдау веб-бағдарламаның құрылымына сәйкес веб-сервер мен веб-қосымшаның дұрыс емес конфигурациясымен ұштасқан типтік осалдықтар тексеріледі. Бұл тәсілге каталогтар индексін автоматты түрде құру мүмкіндігін тексеру, HTTP-әдістерін орындау, аутентификация облыстарынан тікелей ресурстарға жүгіну мүмкіндігі, веб - қосымшаның бастапқы кодтарын алу мүмкіндігі жатады. Тестілік жинағы және веб-сервердің жауаптарын талдау мақсаты осы HTTP-сұраныстар веб-қосымшада осалдықтың болуын немесе болмауын көрсету туралы дұрыс қорытынды жасау болып табылады. Бұл әдіс HTTP протоколы бойынша жұмыс істейді және веб-бағдарлама жазылған технологияға тәуелді емес.

Типтелген параметрлері бар шаблон бойынша сұрауларды генерациялау

шаблон параметрлері типтелген әрбір URI үшін жасалады. Бұдан әрі белгілі бір параметрлердің мәндерін кездейсоқ таңдау арқылы берілген үлгіге сәйкес сұраныстарды автоматты түрде генерациялау жүзеге асырылады. Бұл әдіс пайдаланушы енгізген деректердің дұрыстығын тексеру қателерін анықтау үшін қолданылуы мүмкін. Бұл әдіс веб-бағдарлама жасалған технологияға байланысты емес, өйткені тек HTTP протоколының терминдерінде жұмыс істейді.

Ресурстар базасы бойынша сұраныс құру веб-қосымшада болуы мүмкін ресурстар базасы бар деп болжайды. Базадағы веб-қосымшада белгілі бір ресурстың болуы осы ресурсқа қол жеткізу мүмкіндігімен байланысты осалдықты білдіреді. Мысалы, веб-қосымшада белгілі осал CGI сценарийлері мен веб-сервердің конфигурациялық файлдарының аттары бар. Ресурстарды іздеу веб-бағдарламаның барлық құрылымы бойынша жүзеге асырылады. Барлық каталогтарға кезек тәртібінде ресурстар базасындағы барлық атаулар сұралады. Ресурстар базасы бойынша сұраныс құру тәсілі толығымен автоматты және веб-қосымшалар үшін тән осалдықтар туралы жинақталған ақпаратқа негізделеді. Бұл әдіс идентификациялаушы ақпаратты алу әдістемесінде жоғарыда қарастырылған шектеулер бар, алайда бұл әдіс әкімшілер мен бағдарламалаушылардың типтік қателіктеріне негізделген веб-бағдарламаның жаңа осалдығын анықтауға мүмкіндік береді.

Енуге тестілеу әдісінің артықшылықтары.

Енуге тестілеу әдісі басқа әдістерге қарағанда веб-қосымшаны әзірлеу технологиясына байланысты едәуір аз. Бұл әдіс шабуылдарға төзімділікті бағалауға, сондай-ақ бар кемшіліктерді анықтауға және қорғаныс құралдарын жақсарту жолдарын анықтауға мүмкіндік береді. Енуді тестілеу әдісі әзірленген веб-қосымшалардың осалдығын анықтау үшін кеңінен қолданылады, веб - қосымшаны жасау және баптау кезінде ең болмағанда типтік қателердің кемшіліктерін бағалау қажет болғанда қолдану жақсы нәтижелерге алып келеді. Бұл әдістің сөзсіз артықшылығы, ол кодтау қателерін ғана емес, веб-бағдарлама мен веб-вервердің конфигурация қателерін де анықтай отырып, баптаудан өткен және кеңейтілген веб - бағдарламаны бағалауға мүмкіндік береді.

Енуге тестілеу әдісінің кемшіліктері.

Осалдықтардың барлық түрлерін анықтауға кепілдік бере алмайды.

3 SSL сертификат және HTTPS протоколы

Google SSL сертификатының болуын іздеу нәтижелерінде торап орнына фактор ретінде пайдаланады, сонымен қатар, сертификат жіберілетін деректер сенімді шифрлау алгоритмі арқылы қорғалғанына кепілдік береді және үшінші тараптарға рұқсатсыз қарау үшін қол жетімді болмауын нығайтады.

SSL-сертификаты не үшін қажет?

SSL сертификатын пайдалану сайтқа кіретін клиентке келесідей кепілдік береді:

- сайттағы SSL сертификатының болуы іздеу нәтижелерін рейтингі кезінде Google іздеу жүйесі арқылы ескеріледі;
- түпнұсқалық растама. Сайт сертификатты орнатқан компанияға тиесілі;
- хабардың құпиялылығы. Жіберілген деректерді рұқсат етілмеген тұлғалар қарауға немесе ұстауға болмайды;
- деректердің тұтастығы. Деректер толығымен беріліп, ауыстырылуы немесе жоғалуы мүмкін емес;
- SSL сертификатымен қорғалған сайт келушілерге сенім артады.

SSL Сертификатты пайдалану салалары:

Құпия ақпаратты электрондық пошта арқылы беру, мұндай ақпаратты веб-сайт арқылы жинау қазіргі заманғы бизнестің ажырамас бөлігі болды. Сондықтан кез келген бизнес осы салаларда ақпарат беру қауіпсіздігіне ерекше назар аудару керек. Интернет-дүкендер мен аукциондар, төлем жүйелері, өз жұмысында пайдаланатын ақпараттық жүйелер, құпия деректерді Интернеттен беру, жеке деректерді басқаратын мемлекеттік ұйымдар.

Электрондық цифрлық қолтаңба кілттерінің электронды сертификаттарын Сертификаттау Орталығы (Certification Authority, CA) деп аталатын арнайы ұйымдар шығарады. Қазіргі таңда сұранысқа ие әрі танымал сертификаттау орталықтары келесілер: Comodo, RapidSSL, GeoTrust, Thawte және Symantec.

HTTPS (HyperText Transfer Protocol Secure-дан) HTTP протоколының кеңейтілген қауіпсіздігі үшін шифрлауды қолдайтын кеңейтімі болып табылады. HTTPS протоколындағы деректер SSL немесе TLS криптографиялық хаттамалары арқылы беріледі. HTTP 80-ші TCP портымен салыстырғанда, HTTPS үшін әдепкі бойынша TCP 443 порты пайдаланылады.

HTTPS протоколының жұмыс істеу принципі

HTTPS жеке хаттама емес. Бұл шифрланған SSL және TLS тасымалдау механизмдері арқылы жұмыс істейтін қарапайым HTTP. Шифрлау құралдары пайдаланылған жағдайда және сервер куәлігі тексерілген және ол сенімді болса, онда HTTPS желілік байланыстарды тыңдауға арналған – снифферлік шабуылдардан және man-in-the-middle типті шабуылдардан қорғауды

қамтамасыз етеді.

Веб-серверді https байланыстарын өңдеуге дайындау үшін, әкімші осы веб-серверге жүйеде ашық кілт сертификатын алуға және орнатуға тиіс. TLS асимметриялы шифрлау схемасын (ортақ құпия кілтті генерациялау үшін) және симметриялы (ортақ кілтпен шифрланған деректерді алмасу үшін) пайдаланады. Ашық кілт сертификаты сайттың иесіне осы ашық кілттің иелігін растайды. Ашық кілт сертификаты және ашық кілт өздігімен байланыс орнатылған кезде клиентке жіберіледі; Жеке кілт клиенттен хабарларды шифрлау үшін қолданылады.

4 Веб-бағдарламалардың қауіпсіздік сканерлерін салыстырмалы тестілеу

Бұл бөлімде енуге тестілеу әдісі үшін веб-бағдарламалардың қол жетімді және танымал қауіпсіздік сканерін зерттеу және бірінші бөлімде зерттелген веб-қосымшалардың қауіпсіздік қатерлері мен осалдықтарының негізгі түрлерін анықтау үшін қандай сканердің тиімді екенін анықтау үшін салыстырмалы тестілеу жүргізілді.

4.1 Таңдалған қауіпсіздік сканерлерінің қысқаша сипаттамасы

Веб-бағдарламалардың қауіпсіздігін талдау сканері веб-қосымшаның осалдығын іздеуді жүзеге асыруға мүмкіндік беретін кешенді шешімдер болып табылады. Бұл бөлімде кейбір қауіпсіздік сканерлерін салыстырмалы тестілеу жүргізіледі және алынған нәтижелерге талдау жүргізіледі, сондай-ақ қорытынды жасалады. Қазіргі уақытта веб-қосымшалардың көптеген қауіпсіздік сканерлері бар, мұндай құралдар бағасымен, сканерлеу сапасымен, осалдықтарды іздеу әдістерімен және басқа да кейбір параметрлермен ерекшеленеді. Сипаттаманың негізінде тестілеуді өткізу үшін 4 түрлі қауіпсіздік сканерін таңдау жүргізілді, тестілеуге қосу үшін негізгі критерий сканердің осы жұмыстың бірінші тарауында жіктелген осалдықтарды табу және идентификациялау мүмкіндігі болды. Келесі сканерлер таңдалды: Web Application Attack and Audit Framework (w3af), SkipFish, Acunetix Web Vulnerability Scanner (Acunetix WVS) және SQLMap.

Одан әрі сканерлердің қысқаша сипаттамасы, сондай-ақ тестілеу барысында анықталған артықшылықтар мен кемшіліктер келтірілген.

Acunetix Web Vulnerability Scanner. Автоматты веб-бағдарлама қауіпсіздігін талдау сканері. Дәстүрлі схемаға сәйкес жұмыс істейді: алдымен веб-қосымшаның құрылымы зерттеледі және құрылады, содан кейін осалдықтарды іздеу орындалады. Бұл сканердің жұмыс жасау қорытындысы [Б1.6] [Б1.7 суреттер] көрсетілген.

Артықшылықтары:

- ең өзекті және жиі кездесетін осалдықтарды анықтауға мүмкіндік береді;
- графикалық интерфейс;

Осалдықтарды жою тәсілін шығару және олардың сипаттамасы;

- толықтай автоматтандырылған, пайдаланушыдан аз әрекетті талап етеді;
- есеп жасау.

Кемшіліктері:

- осалдықтарды жою тәсілі және олардың нақты сипаттамасын анықтау ақылы болады.

SkipFish. Google компаниясынан веб-қосымшалардың қауіпсіздігін талдау сканері ашық кодпен тегін, талдау рекурсивті әдіске негізделген. Талдау нәтижесінде сканер толық есепті қалыптастырады.

Артықшылықтары:

- веб-бағдарламаны толық талдау;
- осы бағдарламаны одан әрі сынау үшін сөздікті қалыптастыру мүмкіндігі;
- анықталған осалдықтар туралы толық ақпарат, осалдықты қамтитын ресурстың URL мекенжайы және оған берілген сұраныс бар толық есеп. Есептегі деректер қауіптілік деңгейі мен осалдықтың түрі бойынша сұрыпталған.

Кемшіліктері:

- көп трафик жасауы;
- өте ұзақ сканерлеу уақыты;
- өрафикалық интерфейстің болмауы.

SQLMap. Бұл сканердің басты мақсаты SQL осалдықтарды автоматтандырылған іздеу болып табылады. Осалдықтарды анықтауға ғана емес, оларды пайдалануға да мүмкіндік береді. Ашық бастапқы коды бар, толықтай тегін болып табылады.

Артықшылықтары:

- әр түрлі инъекция түрлерін қолдау;
- көпағымдылық;
- енуді тестілеу үшін басқа құралдармен интеграциялану;
- бағдарлама және сервер туралы ақпаратты жинау мүмкіндігін береді.

Кемшіліктері:

- сканерлеу кезінде ешқандай кемшіліктер байқалмады.

4.2 Тестілеу үшін стенд дайындау

Қауіпсіздік сканерлерін салыстырмалы тестілеу үшін тестілік стенд орнатылды. Стенд ретінде Ubuntu x64 операциялық жүйесі орнатылған Oracle VM VirtualBox виртуалды машинасы қолданылды. Oracle VM VirtualBox виртуалды машинасында арнайы қауіпсіздік мамандары мен хакерлер пайдаланатын Kali Linux ОЖ жоқ болғандықтан Ubuntu ОЖ – ін орнатып дискілік диск бейнесі осы ОЖ – ге кірістірілді. Жоғарыда аталған сканерлер осы Kali Linux – та алдын-ала орнатылған болып табылады. Одан басқа бұл ортада 400 – ге жуық басқа да ақпараттық қауіпсіздік шараларын ұйымдастыруға септігін тигізетін утилиттер мен бағдарламалар бар.

Сонымен қатар, қауіпсіздік сканерін сараптайтын және осалдықтардың

әртүрлі түрлерін қамтитын веб-бағдарлама қажет. Мұндай қосымшалардың үлкен саны бар, бірақ таңдау келесі себептер бойынша Mutillidae пайдасына жасалды:

- орнатылуының қарапайымдылығы;
- толық құжаттама;
- бұл бағдарлама жаңартудың ең жаңа күнін қамтиды.

Сондай-ақ, сканерлеуді жасау және енуді тестілеу үшін арнайы Интернет желісінде жұмыс жасайтын qaztest.kz сайт-дүкені таңдалды. Ол сайт өзінің дерекқор базасын қамтиды және қазіргі таңда 45000 – ға жуық тіркелу жазбалары бар.

Тестілік бағдарлама және қауіпсіздік сканерлері бір физикалық машинада болды.

Тестілеу әдістемесі

Тестілік стенд дайындалған соң, таңдалған қауіпсіздік сканерлерін тестілеу әдістемесін қарастыру қажет. Тестілеу процесі келесі әрекеттер жиынтығын қамтиды:

- қауіпсіздік сканерін баптау;
- сканерлеу параметрлерін таңдау;
- сканерлеу процесін бастау;
- сканерлеу нәтижелерін талдау;

Нәтижелерді салыстырмалы кестеге енгізу.

Тест сынақтарын орындау барысында келесі мәселелер шешілді:

- қауіпсіздікді талдау сканері баптау және мүмкіндіктермен ерекшеленеді. Сондықтан тестілеудің сапалы нәтижесін алу үшін әртүрлі конфигурациялармен сканерлеудің бірнеше сериясы өткізілді.

- қауіпсіздік сканерлері жұмысының тиімділігін салыстыру болатын осалдықтар түрлері. Олар осы жұмыстың бірінші бөлімінде жүргізілген зерттеу негізінде таңдап алынды.

- тестіленетін веб-бағдарламадағы осалдықтар саны. Веб - бағдарламада осалдықтардың санын білу мүмкін емес, сол себепті осалдықтардың ең көп санын тапқан және осалдықтардың белгілі бір түрінің қорытынды санына байланысты сканердің нәтижесі алынды.

4.3 Салыстырмалы тестілеудің қорытындысы

Acunetix WVS. Бұл сканер өте жақсы нәтиже көрсетті, ең аз жалған іске қосылулар, сондай-ақ сканерлеу үшін қосымша параметрлердің қарапайымдылығы жұмысты ыңғайлы етті және сканерлеу кезінде пайдаланушыдан аз әрекеттерді талап етеді.

Кестеге енгізілген нәтижелерден басқа, ол веб-қосымшаның құрылымы және пайдаланушылардың құпия деректері туралы көп ақпарат жинады.

Acunetix WVS артықшылықтарының бірі осалдықтар мен оларды жою тәсілдері туралы егжей-тегжейлі және толық ақпаратты қамтитын веб-ресурстарға сілтемелер беру мүмкіндігі болып табылады.

W3AF.Бұл сканер фреймворк болып табылады және баптауды егжей-тегжейлі зерттеу кезінде аз уақыт ішінде веб-бағдарлама туралы толық ақпарат жинай алады. W3af кемшілігі жұмыс тұрақтылығы және жалған іске қосылуларының үлкен саны.

SkipFish. Жалған анықтаулардың санына қарамастан, алға қойылған міндеттерді жақсы орындады. Бұл сканердің графикалық интерфейсі жоқ, алайда оны баптау оңай болды. Сонымен қатар, ол қорғауды жетілдіруге болатын веб-бағдарлама туралы көптеген қызықты ақпаратты анықтады.

SQLMap. Бұл сканер SQL осалдықтарын іздеуге және пайдалануға бағытталған болып табылады, тестіленетін әмбебап сканерлердің біреуі мамандандырылған сияқты осалдықтарды таба алмайтыны туралы гипотезаны растау үшін тестілік салыстыруға енгізілді. SQLMap қойылған тапсырманы орындады, осалдықтардың ең көп санын анықтады.

Сканерлердің салыстырмалы тестілеулерінің қорытындысы [Б1.3 - кестеде көрсетілген.

Салыстырмалы тестілеудің нәтижелерін талдау негізінде келесі қорытындылар жасалды:

- енуге тестілеу әдісімен веб-қосымшаның қауіпсіздігіне талдау жүргізген кезде бір құралға сүйенуге болмайды, жұмысқа әр түрлі құралдар кешенін, оның ішінде қолмен талдауды енгізу қажет;

- барлық сканерлер қойылған міндеттерді орындап, берілген класстардың өзекті осалдықтарын тапты, бірақ әрбір сканер тапқан осалдықтардың саны әр түрлі болды;

- веб-бағдарламаның қауіпсіздігіне талдау жүргізу алдында құралдар мен әдістемелер кешенін неғұрлым дәл таңдау үшін талданатын веб-бағдарламада пайдаланылатын технологиялармен егжей-тегжейлі танысу қажет;

- айта кету керек, веб-технологиялар қарқынды дамып келеді, ал қауіпсіздік сканері олардың дамуына үлгермейді, сондықтан болашақта бір сканердің көмегімен веб - қосымшаның қауіпсіздігіне талдау жүргізу және берілген кластардың осалдықтарының болмауына кепілдік беру үшін қауіпсіздік сканерлерін одан әрі жетілдіруге баса назар аудару қажет.

5 Веб-қосымшалардың қауіпсіздігін талдау әдістемесін әзірлеу

Осы жұмыстың бірінші және екінші бөлімінде жүргізілген зерттеулер, сондай-ақ салыстырмалы тестілеу негізінде веб-қосымшаның қауіпсіздігін талдау әдістемесі қалыптасты. Қауіпсіздікті талдаудың жасалған әдістемесі төменде ұсынылған белгілі бір қадамдардың дәйектілігін орындау болып табылады:

1 кезең. "Веб-бағдарламаның бастапқы кодтарын статикалық талдау әдісі" көмегімен анализ жүргізу.

- Веб-бағдарламаны жасауға қатысатын бастапқы кодтар жиынтығын қалыптастыру. Осы қадамда веб-қосымшаны жасауға қатысатын бастапқы мәтіндердің нақты жиынтығын анықтау мақсатында талдауға ұсынылған бастапқы мәтіндердің толықтығы мен артық болуына бақылау жүргізу қажет.
- Көптеген бастапқы мәтіндерге статикалық талдау жүргізу.

2 кезең. "Веб-бағдарламаның бастапқы кодтарын динамикалық талдау әдісі" көмегімен анализ жүргізу.

- Веб-бағдарламаны орындау барысында динамикалық талдау жүргізу.

3 кезең. Әлеуетті осалдықтар мен қауіпсіздік қатерлері мен шабуылдар шаблондарының тізбесін қалыптастыру (веб-бағдарламада пайдаланылатын технологиялар мен бағдарламалық құралдар негізінде).

- 2 кезеңде алынған әлеуетті қауіпті конструкциялардың алынған тізбесін өңдеу.
- "Қауіпсіздік ақауы – шабуыл үлгісі" жұбын қалыптастыру.

4 кезең. "Енуге тестілеу" әдісімен веб-бағдарламаның қауіпсіздігіне талдау жүргізу.

- Әлеуетті қауіпсіздік осалдықтарының және шабуылдардың шаблондарының қалыптастырылған тізбесі негізінде енуге арналған тестілерді әзірлеу.
- Енуге тест жүргізу үшін веб-бағдарламаның автоматты қауіпсіздік сканерлерін таңдау (кемінде 3 сканер).

5 кезең. "Веб-бағдарлама туралы идентификациялаушы ақпаратты алу әдісі" көмегімен талдау жүргізу.

- Идентификациялық ақпаратты алу әдісі арқылы "ақпаратты жария ету" класындағы барлық осалдықтарды тексеру.

6 кезең. Алынған нәтижелерді талдау және есептік материалдарды ресімдеу.

- Әр кезеңде алынған талдау нәтижелерін жинау және есептік материалдарды ресімдеу.

ҚОРЫТЫНДЫ

- Веб - бағдарламаның ақпараттық қауіпсіздігі қатерлерінің негізгі түрлері, сондай - ақ веб-қосымшаның қауіпсіздігіне тікелей немесе жанама залал келтіруі мүмкін олардың көздері зерттелді.

- Веб-бағдарламалардың осалдықтары мен қауіпсіздігіне төнетін қауіп-қатерлердің негізгі түрлері зерттелді, сәйкестендірілді және сипатталды. Зерттеу негізінде веб-бағдарламаның қауіпсіздігі қатерлері мен осалдықтарының жіктелуі енгізілді.

- Өзекті шабуылдар мен осалдықтарға талдау жүргізілді және әлеуетті осалдықтар мен типтік шабуылдардың синтезделген тізбесі қалыптастырылды, әзірленген жіктелім және тізбе сәйкестендіру және бағалау үшін веб-бағдарламаның қауіпсіздігіне тестілік сынақтар жүргізу кезінде пайдаланылуы мүмкін.

- Веб-бағдарламалардың осалдығын анықтау және талдау әдістерін сапалы зерттеу жүргізілді. Зерттеу негізінде веб-қосымшалардың осалдығын автоматты түрде анықтау әдістерінің жіктелуі қалыптасты.

- Веб - бағдарламалардың қауіпсіздік сканерлеріне салыстырмалы тестілеу жүргізілді және қорытынды жасалды.

- Веб-бағдарламаның қауіпсіздігін талдау әдістемесі әзірленді.

Жүргізілген зерттеулер барысында келесі қорытындылар жасалды:

- Әдістерді зерттеу және талдау барлық зерттелетін әдістер түгел осалдықтардың анықталуына, тиісінше веб-бағдарламаның қауіпсіздігіне кепілдік бере алмайтынын көрсетті. Осылайша автоматтандырылған құралдарды қолдана отырып әдістер мен әдістемелерді одан әрі дамыту қажет.

- Жүргізілген талдау негізінде веб - қосымшалардың осалдықтарын автоматты түрде анықтау әдістерінің одан әрі дамуы әртүрлі әдістердің мүмкіндіктерін біріктіру жолымен келесі мүмкін болатындай етіп жүреді: осалдықтардың барынша кең класын қамту; автоматты талдау қорытындысы бойынша берілген сыныптардың осалдықтарының болмауына кепілдік беру үшін осалдықтарды анықтаудың толықтығын бақылау.

- Жүргізілген зерттеулер негізінде веб-қосымшалардың қауіпсіздігін талдау бойынша жұмыстар жиі жүргізілу қажеттілігі туралы қорытынды жасалды. Мұндай талдауды әзірлеудің барлық сатыларында, сондай-ақ пайдалану процесінде үнемі жүзеге асыру маңызды, өйткені осалдықтар әртүрлі факторларға байланысты пайда болуы мүмкін. Статистика соңғы жылдары осал веб-бағдарламалардың көбеюін көрсетеді, сәйкесінше осалдықтарды іздеу және жою әдістерін жетілдіру қажет.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1 Марков А.С., Цирлов В.Л. Опыт выявления уязвимостей в зарубежных программных продуктах // Вопросы кибербезопасности. 2013. № 1 (1). 42-48 беттер.

2 Positive Technologies vulnerability inc. Уязвимости веб-прилоложений 2018. [Электронды мәлімет көзі]. Мына сілтеме бойынша қол жетімді: https://www.ptsecurity.com/upload/ptru/analytics/Web-Vulnerability-2016-rus.pdf, (1.03.2018).

3 Атаки на веб-приложения 2017. [Электронды мәлімет көзі]. Мына сілтеме бойынша қол жетімді:https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Web-Applications- Attacks-rus.pdf, (13.04.2017).

4 The WASC Threat Classification v2.0 [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: http://projects.webappsec.org/w/page/13246978.

5 Козлов Д.Д., Петухов А.А. Методы обнаружения уязвимостей в веб-приложениях. // Программные системы и инструменты: тематический сборник ф-та ВМиК МГУ им.Ломоносова N 7. П/р Л.Н. Королева. М: Издательский отдел ВМиК МГУ. Изд-во МАКС Пресс, 2009г.

6 Kali Linux: Поиск уязвимостей на сайте. [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: http://t3i1t3.blogspot.com/2014/12/kali-linux.html

7 Blind SQL Injection descript. [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: https://www.owasp.org/index.php/Blind_SQL_Injection

8 XPATH Injection. [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: https://www.owasp.org/index.php/XPATH_Injection

9 LDAP injection. [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: https://www.owasp.org/index.php/LDAP_injection

10 МЕТКА: СКАНИРОВАНИЕ ВЕБ-ПРИЛОЖЕНИЙ [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді:

https://hackware.ru/?tag=%D1D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D0%B9

11 Инструкция по использованию sqlmap. [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: https://hackware.ru/?p=2069

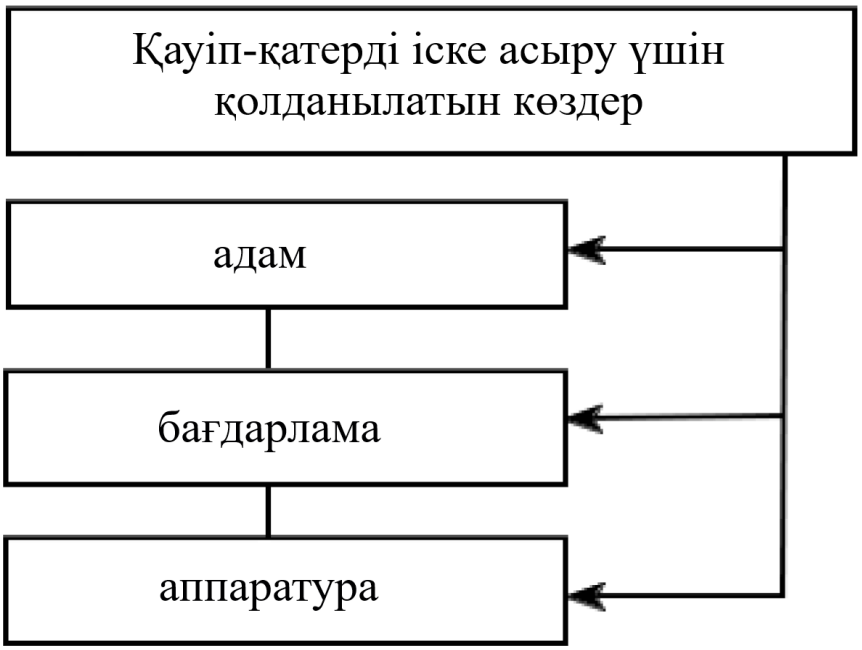
12 Книга «Тестирование на проникновение веб-сайтов» [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді: https://hackware.ru/?p=5925

13 Auronen L., Tool-Based Approach to Assessing Web Application Security. Seminar on Network Security, 2002. [Электронды мәлімет көзі]. Мына сілтеме бойынша қолжетімді:

https://pdfs.semanticscholar.org87e3/15b585ff131b783defe3803bc5b5ad97aef1.pdf

Қосымша А

1-сурет. Веб-бағдарлама қауіптерінің классы



2-сурет. Кіріс каналдарының жіктелуі

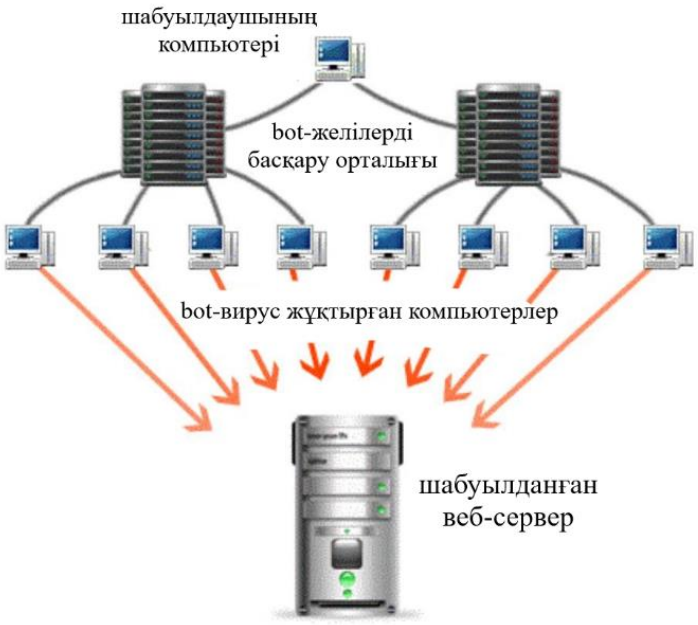
Конфиденциалдық қа қаупі	**Тұтастылыққа қаупі**	**Қол жетімділікке қаупі**	**Қорғалған компьютерлік жүйенің параметрлерін жариялау қаупі.**
Ақпаратты, оны өңдеу құралдарын ұрлау (көшіру); Ақпараттың, оны өңдеу құралдарының жоғалуы (күтілмеген жоғалу, ағып кету); рұқсатсыз танысу, тарату.	Ақпаратты бұғаттау; ақпаратты және оны өңдеу құралдарын жою; ақпаратты беру және ақпаратты өңдеу құралдарын тарату арналарын бұғаттау.	Ақпаратты өзгерту (бұрмалау); ақпараттың дұрыстығын жоққа шығару; жалған ақпараттарды ендіру, алдау; ақпараттың бұзылуы.	Жаңа қауіптердің пайда болуы; осалдығын анықтау; тәуекелдердің артуы; шабуылдың жетістігін арттыру.

1- кесте. Веб-бағдарламалар қауіп-қатерлерінің жіктелімі

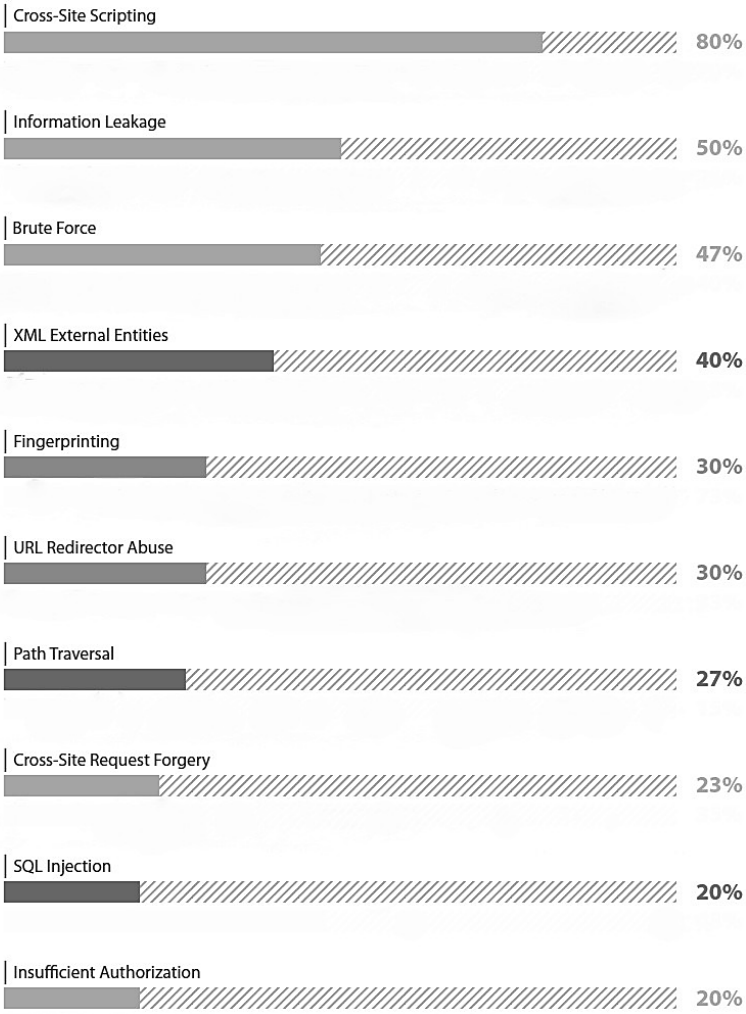
Зақым келтіру әдістері	**Әсер ету объектілері**		
	Құрылғы	*Бағдарлама*	*Деректер*
Ақпараттың ашылуы (ағып кету)	Байланыс желісіне қосылу, ресурстарды рұқсатсыз пайдалану.	Рұқсатсыз көшіру, ұстап қалу.	Ұрлау, көшіру, ұстап алу.
Ақпараттың тұтастығын жоғалту	Қосу, түрлендіру, жұмыс режимдерін өзгерту, ресурстарды рұқсатсыз пайдалану.	"Троян аттарын" және "ұшқындарды" (жучок) енгізу.	Бұрмалау, түрлендіру.
Сервердің жұмыс істеу қабілетінің бұзылуы	Жұмыс істеу режимдерін өзгерту, істен шығару, ұрлау, бұзу.	Бұрмалау, жою, ауыстыру.	Бұрмалау, жою, жалған деректерді енгізу.

2 - кесте. Веб-жүйенің бұзылу түрлерінің жіктелуі

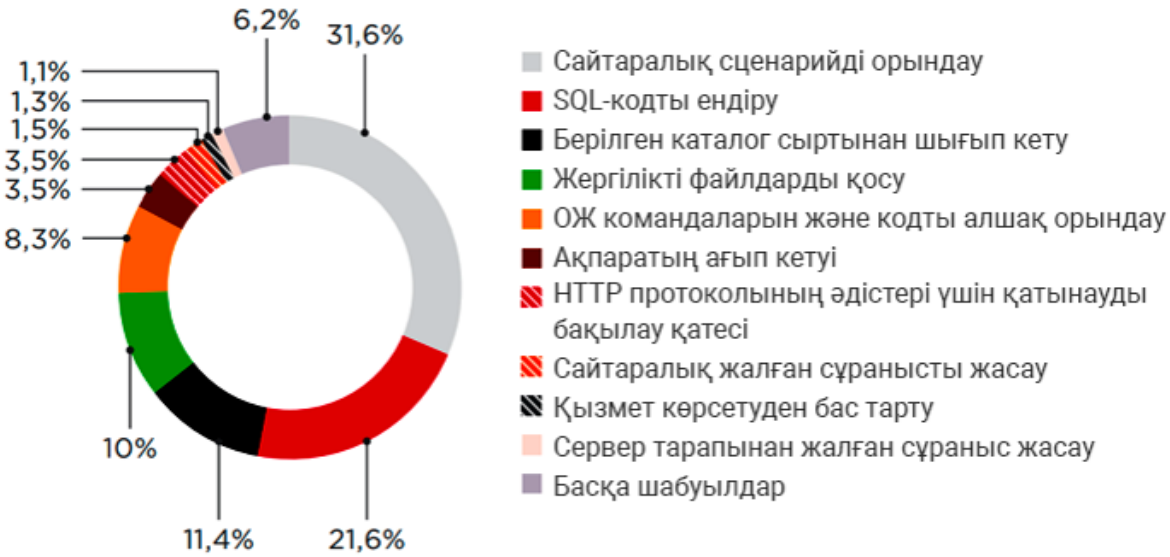
DDOS шабуылдың схемасы



3 - сурет DDOS шабуылының орындалу сұлбасы

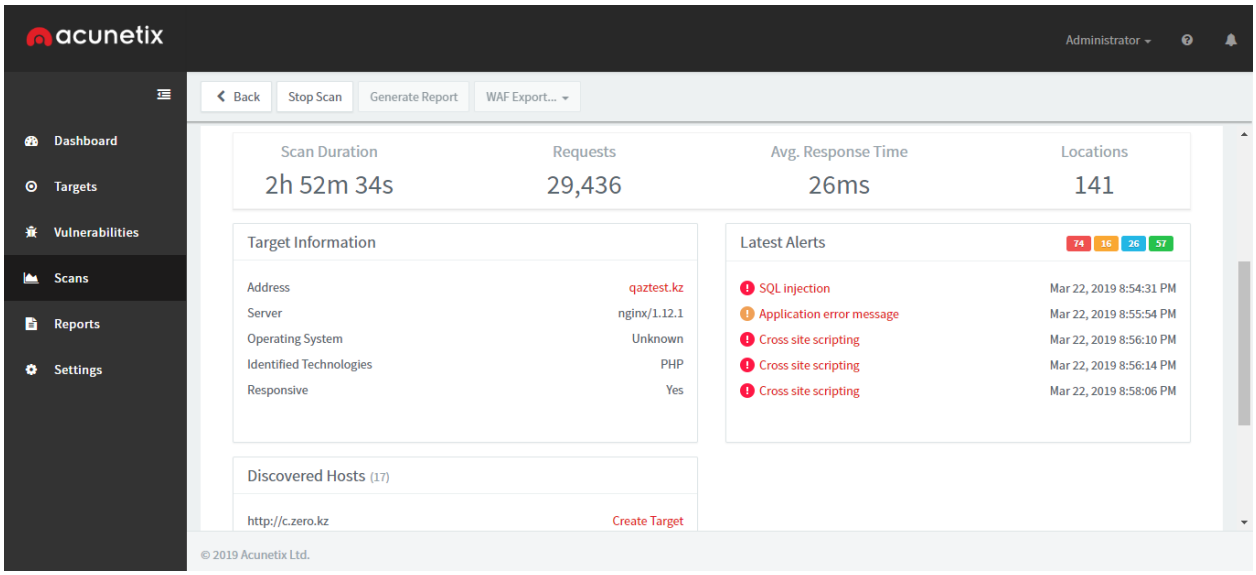


4 - сурет. Веб-бағдарламалардың негізгі типті осалдықтардың рейтингі

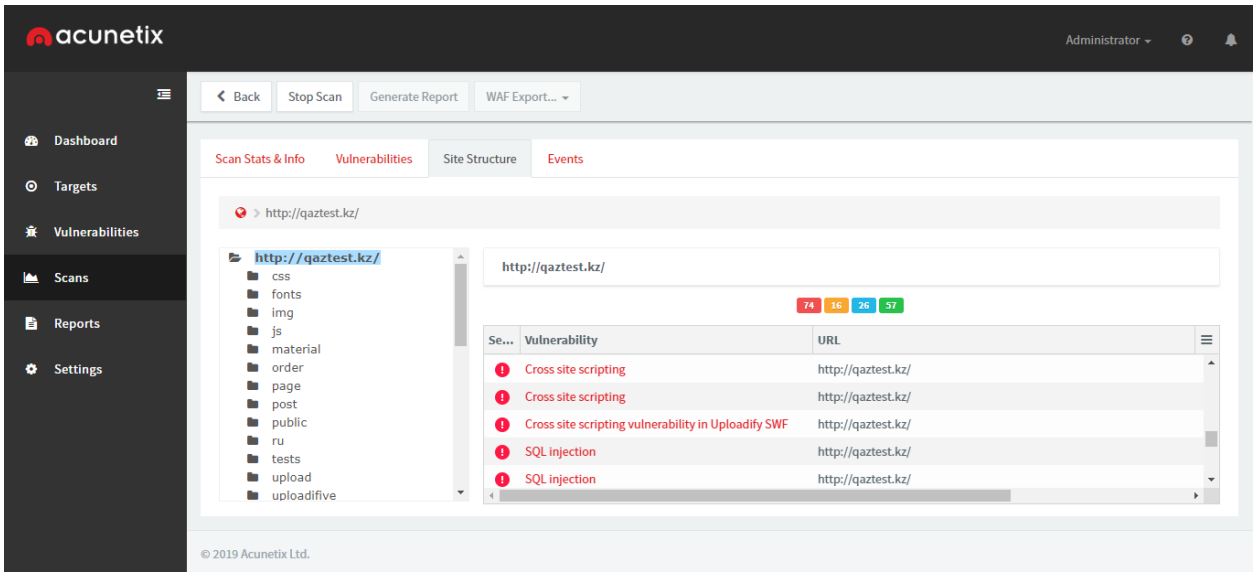


5 - сурет. Веб-бағдарламаларға жасалынатын шабуылдар статистикасы

Қосымша Б

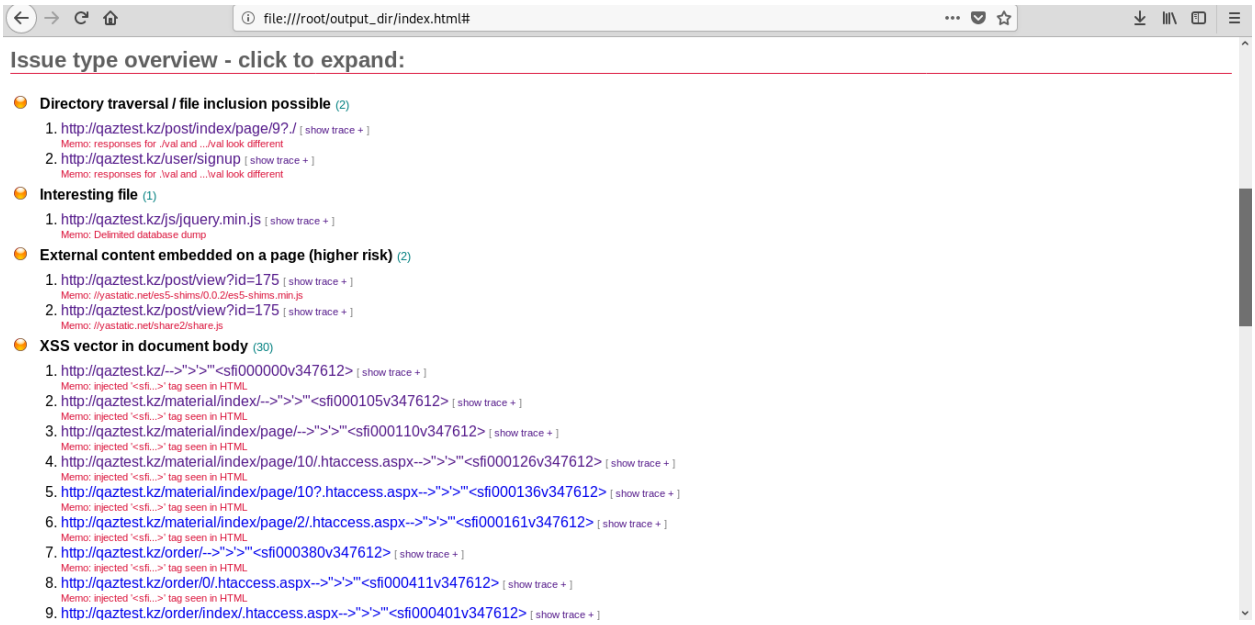


6 - сурет.Acunetix web сайтты сканерлеуші бағдарламасы арқылы сканердің қорытындысы.

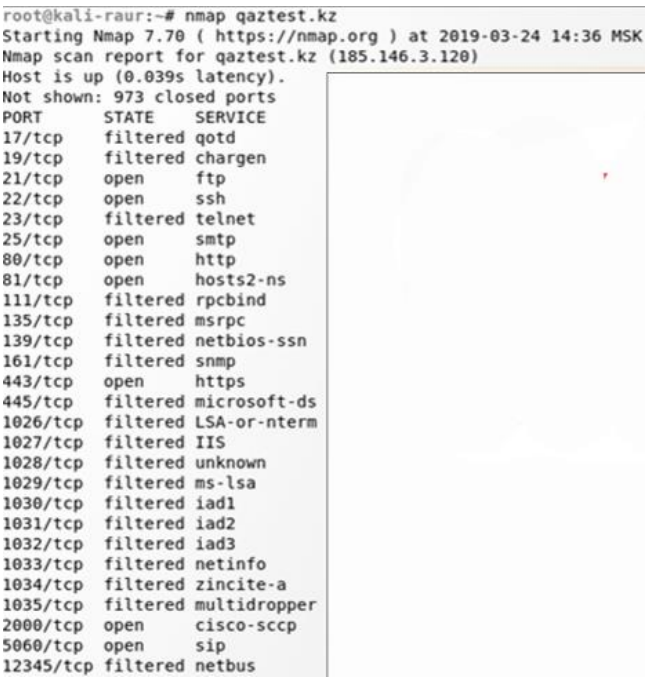


7 - сурет. Acunetix бағдарламасының сканерлеу қорытындысы: сайттың архитектурасы негізінде табылған жоғары деңгейлі қауіптер саны 74 (оның 70 – Cross site scripting қауіптері, ал 4 – SQL injection қауіптері)

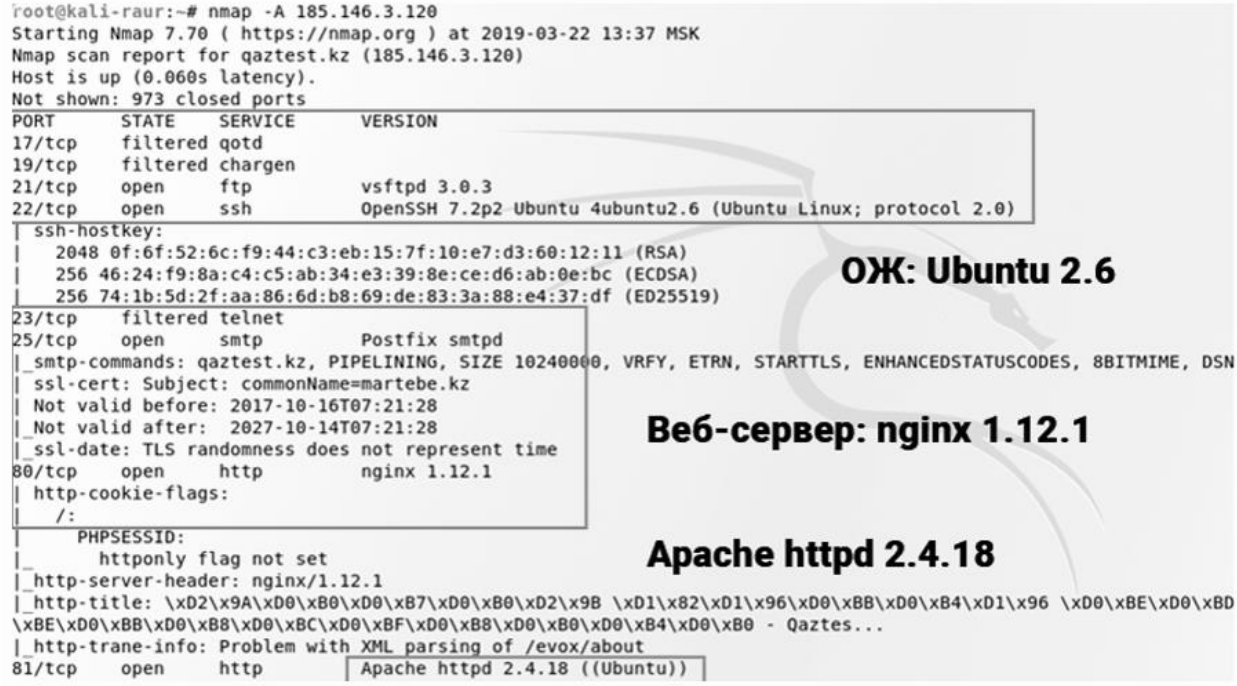
8 – сурет. Skipfish сканерлеуші бағдарламасының қорытындысы. Қорытынды бойынша 35 орта деңгейлі, 32 төмен деңгейлі осалдықтар табылды.



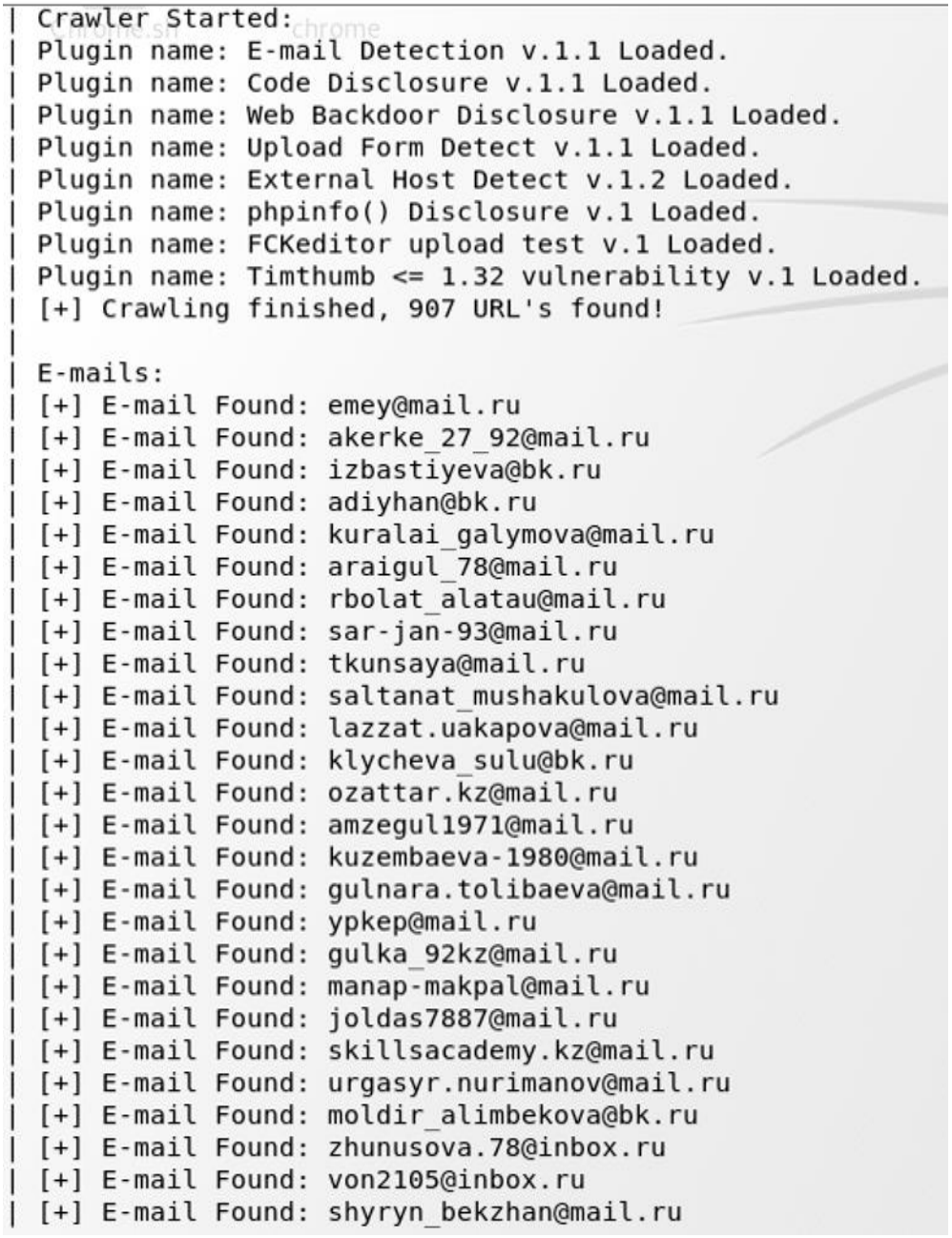
9 – сурет. Skipfish бағдарламасының сканерлеу қорытындысы бойынша сайт бетіне кірістірілген 2 сыртқы файлдар табылды және XSS осалдықтары бар сілтемелер көрсетілген.



10-сурет. nmap қосымшасының сканерлеуі кезінде табылған ашық, жабық және фильтрленген порттардың тізімі



11-сурет. nmap қосымшасының терең сканерлеуінің нәтижесінде сайттың қолданылатын қосымшалары және олардың нұсқалары



12-сурет. SQLMap қосымшасының сканерлеуі кезінде табылған сайт қолданушыларының электронды адрестері

1	SQL (SQL injection) операторларын ендіру		Сайтаралық сценарийді орындау (XSS)		Жалған сұраныстарды жаса (CSRF)		Директорияларды индекстеу (The Path Traversal)		Кеткен уақыты
	Табылды	Жалған анықтаулар	Табылды	Жалған анықтаулар	Табылды	Жалған анықтаулар	Табылды	Жалған анықтаулар	
Acunetix WVS	3	0	70	0	0	0	4	3	2сағ 15м
SkipFish	4	2	30	2	14	1	3	2	45м
SQLMap	4	0	-	-	-	-	-	-	30м
Барлығы	14		31		25		1		

3-кесте. Сканерлердің салыстырмалы тестілеу қорытындысы