ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

9. Inderfurth K., Kelle P., Kleber, R. Inventory control in dual sourcing commodity procurement with price correlation. // Cent Eur J Oper Res. – 2018. – №26. – С. 93–119. – URL: https://doi.org/10.1007/s10100-017-0475-x

10. Nuthall P., et al. Intuition, the farmers' primary decision process. // A review and analysis. – 2018. – URL: https://doi.org/10.1016/j.jrurstud.2017.12.012

ӘОЖ: 004.056

ВЕБ-ҚОСЫМШАЛАРДЫҢ НЕГІЗГІ ТАНЫМАЛ ОСАЛДЫҚТАРЫН ЗЕРТТЕУ

Магзумов Алихан Маратұлы
alihan.magzumov@*mail.ru*
Л. Гумилев атындағы Еуразия Ұлттық университетінің 4 курс студентті,
Астана, Казақстан
Ғылыми жетекші – Сауханова Ж.С.

Аннотация: Бүгінгі таңда веб-қосымшалар ақпарат алмасуда маңызды рөл атқаруда. Веб-қосымшалар ақпараттар мен қызметтерді жеткізудің әдеттегі түрлерінен үлкен артықшылықтарға ие. Веб-қосымшалардың құпия ақпараттарды басқаруы, бүкіл әлемдегі хакерлерге веб-қосымшалар осалдықтарын пайдаланып, оларға шабуыл жасауды басты мақсатқа айналдырды. Веб-қосымшалардың қорғалуының төмен деңгейін көрсететін оқиғалар жиі орын алуда. Сондықтан пайдаланушыларды қауіптерден қорғау үшін Веб-қосымшалардың осалдықтарын зерттеп, шабуылдардан қорғану тәсілдерін меңгеру қажет.

*Кілт сөздер:*Веб-қосымша, интернет ресурс, желілік қызметтер, қауіпсіздік, осалдық, ақпарат жинау, пентест

Веб-қосымшалар осалдықтарының жіктелуі

Ақпараттық қауіпсіздіктегі осалдық - шабуылдаушылар қолдана алатын ақпараттық активтің немесе бақылау мен басқарудың әлсіз жақтары. Ақпараттық қауіпсіздіктің осалдықтарының жіктелуі өте көп. Соның ішінде веб-қосымшалардағы осалдықты ескерген жөн. Өйткені бұл қосымшаның және онымен байланысты деректердің құпиялылығына, тұтастығына және қолжетімділігіне нұқсан келтіруі мүмкін қауіпсіздік қатерлері мен шабуылдарына жол береді.

Веб-қосымшалар әсер етуі мүмкін бірнеше негізі осалдықтар бар [1], соның ішінде:

- Іске асырудағы осалдықтар: бұл сенімсіз деректер веб-қосымшаға жіберілген кезде пайда болады және шабуылдаушы қосымшаға құпия деректерге қол жеткізуге немесе рұқсат етілмеген командаларды орындауға мүмкіндік беретін зиянды кодты енгізе алады.
- Сайтаралық сценарийдің (XSS) осалдықтары: бұл шабуылдаушы веб-параққа зиянды сценарийлерді енгізе алады, олар пайдаланушы деректерін ұрлай алады, парақтың мазмұнын өзгерте алады немесе басқа зиянды әрекеттерді орындай алады.
- Бұзылған аутентификация және сеансты басқару: бұл шабуылдаушы құпия ақпаратқа немесе функционалдылыққа рұқсатсыз қол жеткізуге мүмкіндік беріп, пайдаланушының сеансын айналып өтіп немесе ұстап алған кезде орын алады.
- Қауіпсіз нысандарға тікелей сілтемелер: бұл веб-қосымша файлдар, каталогтар немесе дерекқор кілттері сияқты ішкі нысандарды қамтамасыз еткенде және зиянкестер рұқсатсыз кіру үшін осы сілтемелерді басқара алатын кезде орын алады.
- Қате қауіпсіздік параметрлері: Бұл веб-қосымша дұрыс конфигурацияланбаған кезде орын алады, бұл шабуылдаушыларға қолданбадағы осалдықтарды пайдалануға және құпия деректерге рұқсатсыз қол жеткізуге мүмкіндік береді.
- Бұзылған кіруді басқару: бұл веб-қосымша кіруді дұрыс басқара алмаған кезде орын алады, бұл шабуылдаушыларға шектеулі ақпаратқа немесе функционалдылыққа қол жеткізуге мүмкіндік береді.

- Енгізуді тексеру жеткіліксіздігі: бұл веб-қосымшаны пайдаланушы енгізген деректерді дұрыс тексере алмаған кезде орын алады, бұл шабуылдаушыларға зиянды кодты енгізуге немесе рұқсат етілмеген командаларды орындауға мүмкіндік береді.
- Журнал жүргізу мен бақылаудың жеткіліксіздігі: бұл веб-қосымша пайдаланушының әрекетін дұрыс тіркей және бақылай алмаған кезде пайда болады, бұл қауіпсіздік оқиғаларын уақтылы анықтауды және оларға жауап беруді қиындатады.

Осы негізгі осалдықтарды анықтау үшін ақпарат қауіпсіздігіне қауіп төндіретін мәліметтер жиынтығынан тұратын базалар құрылған. Бұл ұйымға зиян келтіруі мүмкін ақпараттық қауіпсіздіктің ықтимал және нақты қауіптері туралы ақпараттар. Базада белгілі осалдықтар, шабуылдаушылар қолданатын шабуыл түрлері және олардан қорғану әдістері сипатталған.

Ақпараттық қауіпсіздік қатерлерінің деректер базасы ұйымдағы ақпараттың ағымдағы қауіпсіздік күйін талдау және қорғау стратегияларын әзірлеу үшін пайдаланылуы мүмкін. Ол сондай-ақ қауіптерді анықтауға және оларды тез жоюға көмектеседі.

Қолданыста жиі кездесетін деректер базасы: АҚШ-тағы ұлттық стандарттар және технологиялар институтының (NIST) National Vulnerability Database (NVD), Common Vulnerabilities and Exposures (CVE), Open Web Application Security Project (OWASP) Top Ten, Ресейлік Банк данных угроз безопасности информации. Бұл дерекқорлар ашық желіде жаңа осалдықтар мен шабуылдар анықталған кезде жаңартылады.

Кейбір деректер базасына тоқталып кетсек. Қауіпсіздікке қауіп төндіретін модельді құру кезінде қауіп факторларын анықтауда және зерттеуде қиындықтар жиі кездеседі. Ол үшін Ресейлік ақпараттың қауіпсіздігіне қауіп төндіретін деректер банкін пайдалануға болады. Бұл деректер банкісінде рұқсатсыз кіруге және құпия мәліметтермен заңсыз әрекеттерді орындауға себеп болуы мүмкін шарттардың сипаттамасы бар.

Ресейлік қауіп-қатерлер Банкінің ерекшеліктері [2]:

- кез-келген құрылғыдан кіру мүмкіндігі беріледі;
- ақпаратпен, қорғаныс құралдарын өндіруші компаниялармен тексеріс жүргізіледі
- база тек электрондық форматта болады, үнемі жаңартылып отырады және пайдаланушылардың сұранысы бойынша түзетіледі;
- әрбір оператор АЖ пайдалану сипаттамалары мен ерекшеліктерін ескере отырып, қауіптілік пен ықтималдық дәрежесін дербес анықталады;
- мәліметтер базасынан деректерді ақысыз және шексіз рет алуға болады, ал оны таратқан кезде алынған ақпарат көзі көрсетіледі;
- тізімді толықтыру осалдық туралы сұрау салуды тексеруді көздейтін белгіленген регламентке сәйкес жүзеге асырылады.

CVE(Common Vulnerabilities and Exposures) - бағдарламалық жасақтама, аппараттық өнімдердегі белгілі киберқауіпсіздік осалдықтарын анықтау және бақылау үшін қолданылатын жүйе. Әрбір CVE осалдық арнайы индентификатор жазбасымен тағайындалады және бұл зерттеушілер мен ұйымдарға әртүрлі платформалар мен құралдар арасында белгілі бір осалдық туралы ақпарат алмасуға мүмкіндік береді [3].

CVE осалдық жүйесін көптеген ұйымдар, соның ішінде мемлекеттік органдар мен қорғаныс жеткізушілері осалдықтарды анықтау мен бақылаудың стандартталған әдісін қолдау үшін пайдаланады. Егер осалдық анықталса, оны CVE жүйесіне жіберуге болады және тексерілгеннен кейін оған бірегей CVE идентификаторы беріледі.

Веб-қосымшалар осалдықтарын зерттеу тәсілі

Жоғарыда келтірілген мәліметтер базасын қолдану мүмкіндігін көрсету үшін мысал ретінде CVE осалдығы бар WordPress веб-қосымшасы алынды. Зерттеу пентест арқылы жүргізіледі. Пентест – ену сынағы, желіге немесе веб-қосымшасына нақты шабуылды имитациялайтын шаралар кешені. Пентест әдетте бірқатар қадамдарды қамтиды [4]:

1 Қадам - ақпарат жинау. Бұл веб-пентестингтің алғашқы және маңызды қадамдарының бірі, өйткені ол пентесттің мақсатын анықтауға және жүйедегі ықтимал осалдықтарды анықтауға мүмкіндік береді:

Ақпарат жинау барлаудан басталады, оның мақсаты - жүйенің конфигурациясы, қолданылатын технологиялар, осалдықтар және шабуыл жасау үшін пайдаланылуы мүмкін басқа сипаттамалар туралы толық ақпарат алу. Барлау құралы ретінде Maltelgo-ны қолдануға болады. Maltelgo деректер көздерін талдауға және алынған ақпаратты графиктер мен диаграммалар түрінде визуализациялауға мүмкіндік береді [5].

Барлық порттарды тексеру nmap құралы арқылы анықталады. Nmap (Network Mapper) - бұл желілік хосттарды зерттеу және мақсатты жүйеде ашық порттарды анықтау үшін қолданылатын желіні сканерлеу құралы. Тексеріс кезінде 3 ашық порттар табылды:

- 22/tcp – ssh (жүйені қашықтан басқару және қорғалған байланыс арқылы деректерді беру үшін қолданылады)[6];
- 80/tcp – http (сервер мен клиент арасында веб-беттерді тасымалдау үшін қолданылады) [7];
- 21/tcp – ftp(клиент пен сервер арасында файлдарды тасымалдау үшін қолданылады) [8];

Веб-қосымшаның каталогін, субдоменын, жасырын файлдардын келесі құралдар арқылы тексеруге болады:

- Dirbuster - каталогтарды сұрыптауға және жасырын мазмұнды іздеуге арналған утилита;
- Nikto - осалдық сканері;
- Sublist3r - қосалқы домен сканері;
- Gobuster - жасырын файлдар мен каталогтардың сканері.

Талданып отырған сайтта баяндалған құралдар көмегімен дәрежесі жоғары және орташа болатын осалдықтар табылған жоқ.

2 Қадам - ақпаратты жинау арқылы осалдықты табу.

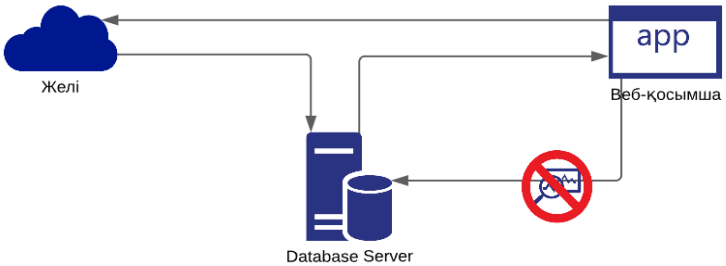
Деректерді сканнерлеу барысында осалдыққа әкелетін қауіп табылған жоқ, бірақ бастапқы кодтың ішінде қызықты кітапханалар қолданысын байқауға болады. Бұл WordPress жүйесінің BookingPress плагині.

Осалдық https://cve.mitre.org/ деректер базасында табылды. Осалдықтын номері CVE-2022-0739[9].

Bookingpress плагинінің 1.0.11 нұсқасына дейін пайдаланушы ұсынған post деректері Ajax әрекеті арқылы динамикалық түрде жасалды. Сол себепті SQL сұрауында пайдаланушының post деректері дұрыс дезинфекцияланбайды. Яғни табылған осалдыққа арнайы жүктеме(payload) орнатуға болады:

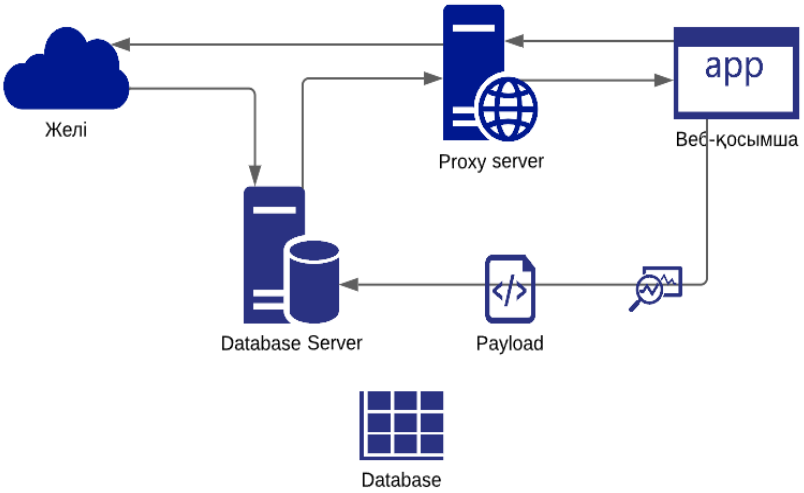
curl -i 'https://example.com/wp-admin/admin-ajax.php' \ --data 'action=bookingpress_front_get_category_services&_wpnonce=8cc8b79544&category_id=33&total_service=-7502) UNION ALL SELECT @@version,@@version_comment,@@version_compile_os,1,2,3,4 -'

Желіні сызба түрінде бейнелесек, веб-қосымшаның деретер қорына толық қолжетімділігінің жоқ екендігін көреміз. 1 суретте веб-қосымшаның желіге дербес қосылуы көрсетілген.



1 Сурет Веб-қосымшаның желіге дербес қосылуы

Арнайы прокси құралын қолдана отырып, деректер қорының сұранысына керекті жүктемені енгізсек, толық деректер қорына ие бола аламыз (2 Сурет).



2 Сурет Веб-қосымшаның желіге прокси сервер арқылы қосылуы

Берілген жүктеме kali ОЖ-де curl командасын қолданып Burp Suite проксиіне жіберіледі. Осы жүйеден алынған сұрасынысты файлға сақтап, арнайы Sqlmap құрал көмегімен деректер базысын қолдана аламыз. Бұл құрылғы SQL инъекциясының осалдығын анықтау және пайдалану үшін қолданылатын веб-қосымшалардың қауіпсіздігін тексеру қосымшасы. Sqlmap MySQL, Oracle, PostgreSQL, Microsoft SQL Server және т. б. сияқты көптеген дерекқор түрлерін қолдайды [10]. Біздің жағдайда MySQL дерекқоры. Шабуыл кезінде 27 кесте табылып, керекті Wp_user кестесі анықталды. Кестеде wp_login каталогіне авторизация жасай алатын қолданушылардың кіру логиндері мен құпия сөздері сақталған. Бірақ құпия сөздер хэш түрінде жасырлыған.

Веб-қосымша Wordpress жүйесін қолданатын болғандықтан, табылған парольдерді арнайы хэш бұза алатын john құралымен оқып, әкімшілік панеліне яғни wp_login.php каталогіна кіреміз.

Сайтта WordPress-тің қай нұсқасы жұмыс істейтінін анықталды, ол WordPress 5-6-2 нұсқасы. Осалдық https://cve.mitre.org/ және https://bdu.fstec.ru/threat деректер базасында табылды.

Бұл кітапханадағы WordPress XXe CVE-2021-29447 осалдығы [11]. Осалдықтын негізі XXe шабуылдарына әкелетін кітапханадағы XML талдау мәселесін пайдалану болып табылады.

3 Қадам- табылған осалдық арқылы шабуылдар жасау.

Осалдықты іске асыру үшін веб-қосымшасына wave форматта payload жүктемесі орнатылады. Нәтижсінде ішкі кодттың мазмұнына қол жеткезуге мүмкіндік туады.

Ашық код Base64 форматында берілді. Base64 - тек 64 ASCII таңбасы бар екілік деректерді кодтау стандарты. Кодты дешифрлау арнайы қосалқы бағдарламалар арқылы жүзеге асырылады. Егер WordPress жүйесі қолданылған болса, барлық парольдер тізімі wp-config.php файлында сақталады.

Керекті парольдер іздестіріліп, бастапқы nmap жүйесінде табылған ашық порты бар ftp протоколына қолжетімділік алынды. ftp - файлдарды бір компьютерлік жүйеден екіншісіне тасымалдау үшін қолданылатын желілік протокол.

4-Қадам - табылған қолжетімділік арқылы ішкі жүйені қолдану.

Порттарды сканерлеу кезінде Ftp серверінің 21-ші порты ашық болатын.

FTP сервері веб-қосымшаға серверде сақталған файлдарға кіруге және оларды веб-шолғыш арқылы басқаруға мүмкіндік беретін интерфейсін қамтиды. Бұл қолжетімділік көмегімен веб-қосымшасының толықтай құрылымын өзгертуге болады.

5-Қадам Есептеме дайындау.

Веб-қосымшаның пентест кезеңінде маңызды осалдықтары табылды. Осалдықтар веб-қосымшаны толықтай бұзуға, яғни, деректердің құпиялылығының толық бұзылуына, ұрлынуына, жоғалуына мүмкіндік береді.

Қортынды

Интернет-ресурстардың өмірімізге біртіндеп енгізілуі қызметтер мен кеңес алуда үлкен артықшылықтарды береді. Веб-қосымшалардың функционалдық дамуы қауіпсіздікті сапалы қамтамасыз етумен қатар жүруі тиіс. Қосымшалардың қауіпсіздігін қамтамасыз етуде қауіп төндіретін мәліметтер жиынтығынан тұратын базалардың маңызы зор. Пентест зиянкестердің әрекеттерін толығымен модельдеуге және ресурстардың қауіпсіздігін сапалы бағалауға мүмкіндік беретін әдістердің бірі. Пентест бойынша жұмыстарды жүргізу үшін тестілеуге қажет құралдар мен әдістемелер зерделенді.

Баяндалған ақпаратты қорытындылай келе, веб-қосымшаны қорғау үшін келесі жалпы іс-шараларды өткізу ұсынылады:

- Жаңартуларды уақытында орнатып отыру
- Парольдерді дұрыс орында сақтау;
- Керек емес порттарды жабу;
- Брэнмаур жүйесін қосу;
- Қолданылмайтын қосымша әдістерді алып тастау;
- Дерекқор пайдаланушысының құқықтарын шектеу;
- Қызметтік файлдарға тікелей кіруге тыйым салу.

Пайдаланылған дереккөздердің тізімі

1. Andrew H. Web Application Security, Sebastopol, California, USA, O'Reilly Media 2020. P. 330
2. Банк данных угроз безопасности информации. Сілтеме мекенжайы: https://data-sec.ru/personal-data/threats-data-bank/
3. Что такое CVE и какие угрозы там хранятся? Сілтеме мекенжайы: https://habr.com/ru/company/pvs-studio/blog/678410/
4. Faircloth J. Penetration Tester's Open Source Toolkit. Oxford, United Kingdom Syngress,
5. Maltego. Сілтеме мекенжайы: https://www.maltego.com/
6. Коротко об SSH. Сілтеме мекенжайы: https://habr.com/ru/sandbox/166705/
7. Pollard B. HTTP/2 in action. Shelter Island, New York, USA, Mannig,2021. P. 424
8. Что такое FTP-сервер и для чего он нужен? Сілтеме мекенжайы: https://galtsystems.com/blog/start/chto_takoe_ftp_server_i_dlya_chego_on_nuzhen/
9. CVE-2022-0739. Сілтеме мекенжайы: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0739
10. Sqlmap . Сілтеме мекенжайы: https://sqlmap.org/
11. CVE-2021-29447. Сілтеме мекенжайы: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-29447

ӘОЖ: 004.056

SIEM ЖҮЙЕЛЕРІН ТАЛДАУ ЖӘНЕ ОЛАРДЫ ҚАУІПСІЗДІК САЛАСЫНДА ҚОЛДАНУ. ЖЕДЕЛ АҚПАРАТ ЖӘНЕ ҚАУІПСІЗДІК ОРТАЛЫҚТАРЫ

Манатбек Әбілқайыр Қабибекұлы
abylkaiyr_01_98@mail.ru
Л.Н.Гумилев атындағы Еуразия Ұлттық Университетініңмагистранты, Нұр-Сұлтан, Қазақстан
Ғылыми жетекші - Ахметова Жанар Жумановна

Аннотация: Бизнес мақсаттарына қол жеткізу, бәсекеге қабілеттілікті және заңды қызметті сақтау үшін әртүрлі көлемдегі және қызмет аясындағы барлық типтегі заманауи ұйымдар (мысалы, коммерциялық кәсіпорындар, мемлекеттік мекемелер, коммерциялық емесұйымдар) көптеген ішкі