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

Список использованных источников
1. Мазепова О. И., Мещанов В. П., Прохорова Н. И., Фельдштейн А. Л., Явич Л. Р./Под ред. А. Л. Фельдштейна. Справочник по элементам полосковой техники – М.: Связь, 1917. – с. 1– 30
2. Баскаков, С. И. Радио/технические цепи и сигналы. – М.: Высшая школа, 2000. – с. 462
3. Электроника. Теория и практика — 4– е изд.: Пер. с англ. / Саймон Монк, Пауль Шерц. — СПб.: БХВ– Петербург, 2018. – с. 250– 270, 387– 425.
4. В. Х. Осадченко, Я. Ю. Волкова, Ю. А. Кандрина. Фильтры высоких и низких частот. – Екатеринбург: Изд– во Урал. ун– та, 2015. – с. 62– 71.
5. Комаров В. В., Бушанский С. К. СВЧ– фильтры на объемных концентрических резонаторах // Радиотехника. 2018. № 8. – с. 140–143.
6. Шаров Г. А. Волноводные устройства сантиметровых и миллиметровых волн. М.: Горячая Линия – Телеком, 2016. – с. 640.
7. Проектирование печатных плат в САПР Altium Designer: сборник лабораторных работ / М. Я. Мактас, И. М. Бекмухаметов (в 2 ч. ч. 1). – Ульяновск: УлГТУ, 2014. – с. 429.

УДК 004.942

МОДЕЛИРОВАНИЕ SQL– ИНЪЕКЦИОННЫХ КИБЕРАТАК В СРЕДЕ GNS3

Санакова Гулмира Халыкбаевна
gul_zholdasova@mail.ru
Магистрант кафедры «Радиотехника, электроника и телекоммуникация» ЕНУ им. Л.Н. Гумилева, Астана, Казахстан
Научный руководитель – к.т.н., доцент Иманкул М.Н.

Кибератаки – злонамеренные действия, осуществляемые отдельными лицами или организациями для нацеливания на компьютерные системы, сети и цифровые устройства с целью нарушения их конфиденциальности, целостности и доступности. Они могут принимать различные формы, включая, но не ограничиваясь, заражением вредоносными программами, фишинговым мошенничеством, тактикой социальной инженерии, атаками типа «отказ в обслуживании» и атаками вымогателей. Эти атаки могут нанести значительный ущерб отдельным лицам и организациям, включая кражу конфиденциальных данных, финансовые потери и репутационный ущерб.

SQL– инъекционные атаки являются одним из наиболее распространенных и опасных типов кибератак, которые нацелены на веб– приложения и полагаются на базы данных (БД) для хранения и извлечения данных. Хакеры могут использовать уязвимости в коде веб– приложения для внедрения вредоносных команд SQL (*Structured Query Language*) в БД, позволяя им получать доступ к конфиденциальной информации, изменять/удалять данные или даже контролировать всю систему. Атаки путем внедрения кода SQL позволяют злоумышленникам подделывать удостоверения и существующие данные, вызывать проблемы с отказом, такие как аннулирование транзакций или изменение баланса, разрешать полное раскрытие всех данных в системе, уничтожать данные или делать их недоступными, а также становиться администраторами сервера БД. SQL Injection (SQLi) очень распространен в приложениях PHP (Hypertext Preprocessor) и ASP (Active Server Pages) из– за преобладания старых функциональных интерфейсов. Серьезность атак SQLi ограничена навыками и воображением злоумышленника и, в меньшей степени, защитой в глубоких контрмерах, таких как соединения с низкими привилегиями к серверу БД. В целом SQLi имеет высокую степень серьезности воздействия. [1]

Чтобы предотвратить подобные атаки, важно протестировать меры безопасности веб–приложения и обнаружить любые потенциальные уязвимости. В данной статье рассмотрено моделирование кибератаки путем внедрения кода SQL.

GNS3 (Graphic Network Simulator 3) – программное обеспечение для моделирования сети, которое позволяет создавать виртуальные сети с использованием реальных образов Cisco IOS. С помощью GNS3 можно моделировать различные сетевые сценарии и тестировать различные конфигурации сети без необходимости использования физического оборудования. Это делает его идеальным инструментом для тестирования и проверки мер сетевой безопасности, включая атаки с внедрением кода SQL. [2]

Существуют два сценария атак, которые можно исследовать. Первый – внутренняя атака, совершаемая доверенным лицом внутри компании, а второй – внешняя атака, производимая субъектом, чьи полномочия неизвестны компании. Эти два сценария представляют совершенно разные проблемы для компании и в определенной степени поддерживают две разные топологии атак. Также возможен гибридный вариант обоих типов атак, который может быть описан как "нечеткая" атака. Это тот случай, когда атакующий является внешним по отношению к сети, но устанавливает свое присутствие внутри нее путем компрометации узла, получения определенной степени контроля над узлом сети, откуда он может начать атаку.

В данной статье представлен набор простых методов предотвращения уязвимостей, связанных с внедрением кода SQL, путем избежания этих двух проблем. Эти методы могут быть использованы практически с любым языком программирования и с любым типом БД. Существуют и другие типы БД, такие как XML– базы данных, которые могут иметь аналогичные проблемы (например, внедрение XPath и XQuery), и эти методы также могут быть использованы для их защиты. Основные средства защиты от атак на базе SQLi [1]:

– использование подготовленных операторов (с параметризованными запросами);

– использование правильно построенных хранимых процедур;

– проверка входных данных списка разрешений;

– экранирование всех входных данных, предоставленных пользователем, с целью отсеивания SQLi– атак и других онлайн– угроз.

Дополнительная защита достигается обеспечением соблюдения минимальных привилегий и выполнением проверки входных данных списка разрешений в качестве вторичной защиты.

В данной работе построен лабораторный сценарий, использующий: инструменты с открытым исходным кодом; GNS3; Virtual Box. Также смоделирована реальная атака на основной сервер сети. Если злоумышленник вводит данные, содержащие символы или строки, имеющие специальное значение для интерпретатора SQL, например (;, – или ‘), и эти данные не были должным образом проверены, то злоумышленник может изменить предполагаемое поведение SQL– запроса, чтобы выполнить атаку на БД. На рисунке 1 показана высокоуровневая диаграмма атаки SQL.

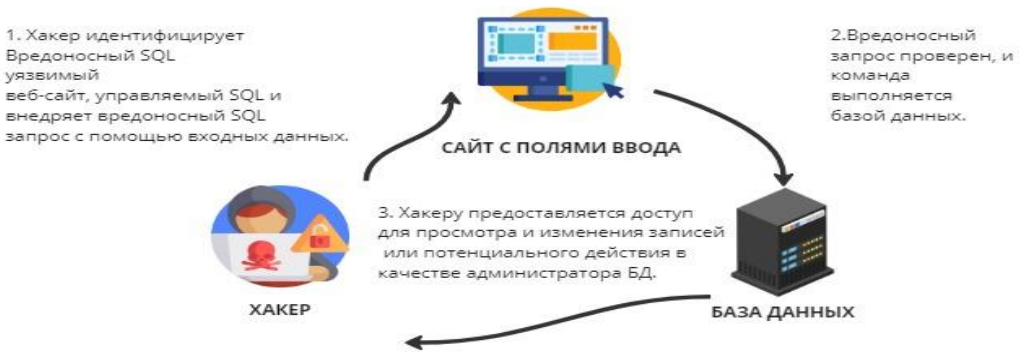

Рисунок 1 – Высокоуровневая диаграмма атаки SQL [1]

При получении сообщения о том, что веб– сайт был взломан неизвестным злоумышленником, результаты первоначального расследования показывают, что злоумышленник использовал различные техники и инструменты для взлома веб– сайта жертвы, такие как SQL*i*, XSS (*Cross– Site Scripting*), сломанное кэширование, обход каталога и нарушение локальной аутентификации при входе на сервер (рис. 2).

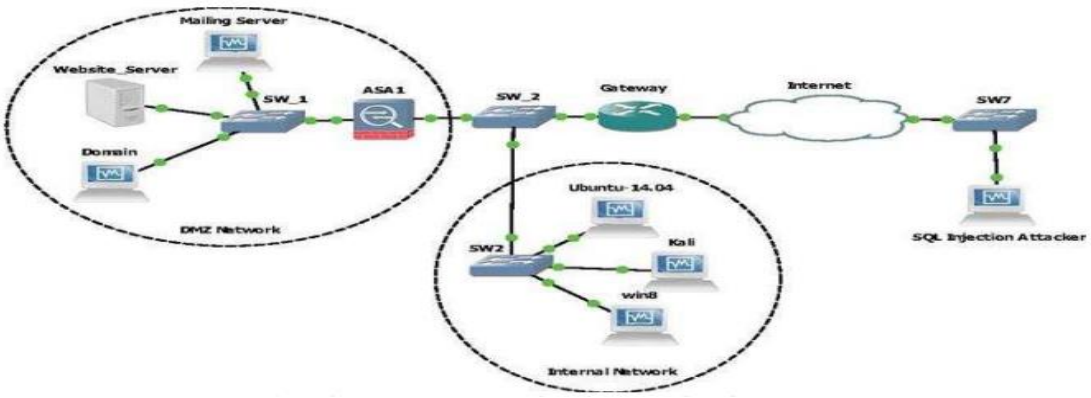

Рисунок 2 – Топология атакованного узла сети [3]

Злоумышленник отправил код SQLi, используя Burp Intercepting Proxy для перехвата соединения между его машиной и сервером жертвы (рис. 3). Можно использовать подход к расследованию с целью прогнозирования и отслеживания источника атаки или незаконной деятельности в компьютерной сети, основанный на определении маршрута сбора доказательств с помощью модели процесса сбора доказательств ECPM (Model of the evidence collection process). [4]

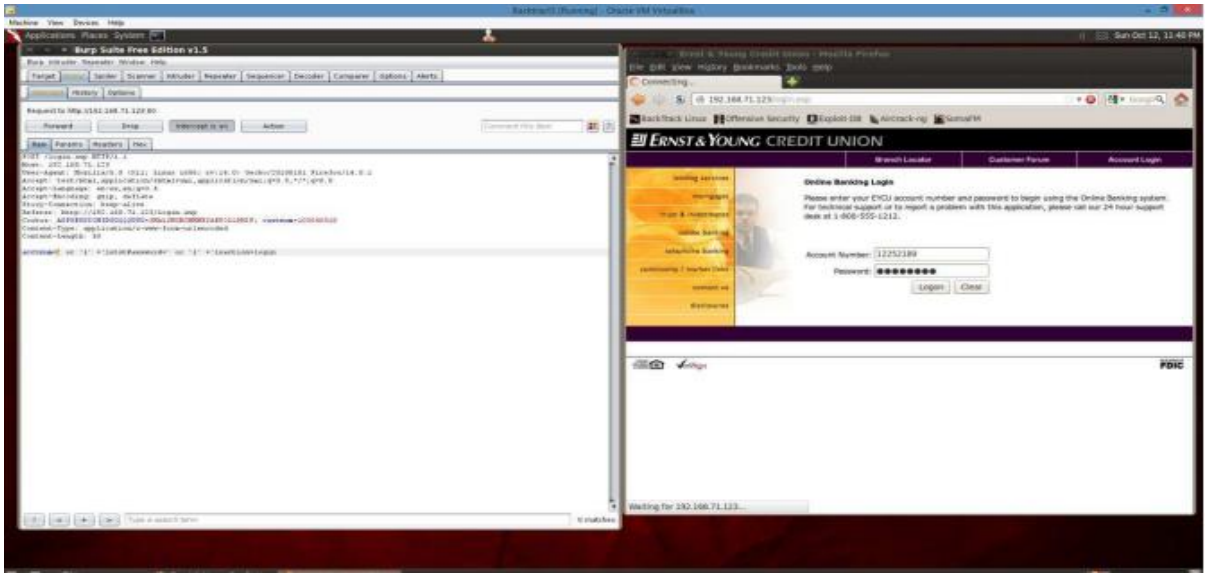

Рисунок 3 – SQL*i* при вставке номера аккаунта

Иногда исследователи сетей сталкиваются с трудностями в понимании сетевой инфраструктуры и взаимосвязи между узлом– жертвой и другими узлами. Чтобы отследить источник атаки можно использовать матрицу сетевого союза в качестве дорожной карты для процесса расследования. Матрица сетевых союзов содержит список всех расстояний между узлом жертвы и другими узлами. Это поможет исследовать все подозреваемые узлы.

Последним шагом является извлечение останков из подозреваемых узлов, которые могут быть использованы в качестве улик (сбор улик). [5]

Чтобы собрать информацию об кибератаке SQL– инъекции, которая была инициирована злоумышленником, был использован инструмент для анализа криминалистических пакетов Wireshark. Пакеты, которые коррелировали между злоумышленником и сервером жертвы, показаны на рисунке 4.

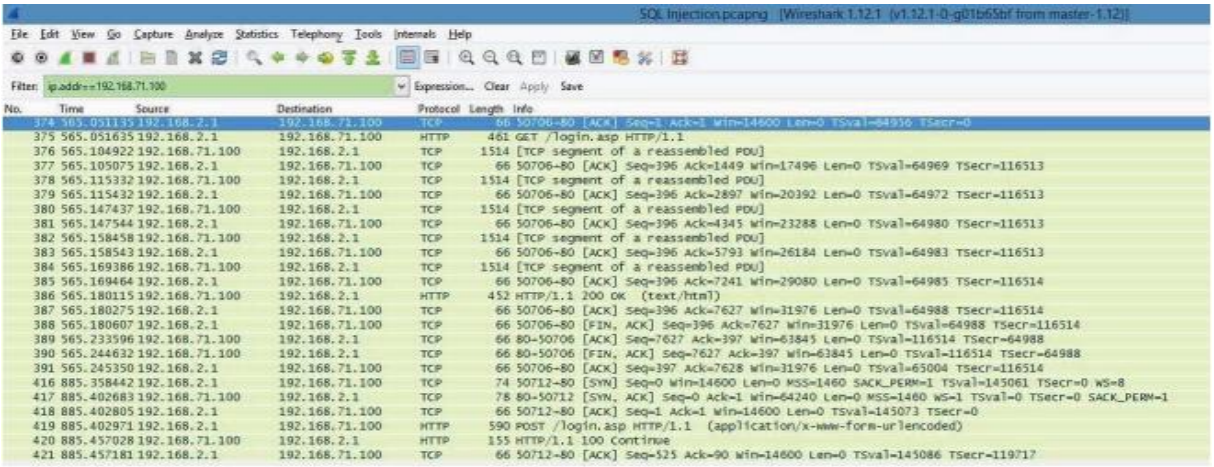

Рисунок 4 – Корреляция пакетов между злоумышленником и сервером жертвы

Из рис. 4 видно, что злоумышленник смог получить доступ к логину .asp на веб– странице после рукопожатия. Далее тщательно изучены веб– страницы login.asp, которые были скомпрометированы атакой SQLi, и пакеты, которые казались подозрительными и потенциально были связаны с атакой SQL– инъекций. Согласно криминалистическому инструменту Wireshark, злоумышленник получил доступ к файлу login.asp на своем компьютере и отправил SQL– инъекцию на сервер жертвы.

В данной статье описано имитационное исследование сценария сетевой атаки и подчеркивается важность создания среды атаки виртуальной сети, которая позволяет проводить недорогие эксперименты и защищать реальные активы. Результаты этого исследования могут быть применены в качестве руководства для улучшения фактической ИТ– инфраструктуры. Для моделирования сценария атаки использовались различные инструменты с открытым исходным кодом, такие как GNS3, Oracle VM Virtual Box и VMWare Workstation. Криминалистический инструмент Wireshark использовался для обнаружения преступной деятельности на сетевом уровне, а Volatility Framework 2.4 использовался для изучения устройств жертв и злоумышленников. Данное исследование призвано послужить отправной точкой для анализа атак. Основное внимание уделено исследованию веб– сайта, взломанного в результате атаки SQL– инъекций, и использованию инструмента криминалистики с целью улучшения эффективности процесса расследования. Дальнейшая работа будет включать моделирование атак в облачных сетях и разработку математических моделей и алгоритмов для повышения эффективности процесса расследования в более сложных случаях.

Список использованных источников:

1. Веб– сайт Open Web Application Security Project (OWASP), на котором содержатся сведения о предотвращении и смягчении последствий атак путем внедрения кода SQL.

2. gns3.com

3. Создание сложных топологий GNS3. Решение проблемы. Советы Windows. (clubwindows.ru)

4. А. А. Аль– Махруки, С. Абдалла, Т. Кечади, Готовность к судебной экспертизе и осведомленность о безопасности. Международная конференция по встраиваемым системам в Телекоммуникации и приборостроении в сети. Аннаба, 2014.

5. A. Mahrouqi, P. Tobin, S. Abdalla, T. Kechadi. Member SQL– Injection Cyber– attacks. IACSIT.

ӘӨЖ 62.519

ЭЛЕКТРОМАГНИТТІК КӨТЕРГІШ ҚОНДЫРҒЫНЫ ЗЕРТТЕУ

Сатыбалдиева Жайна Байдуллаевна
satybaldiyeva_zhb@mail.ru

Л.Н. Гумилев атындағы ЕҰУ, физика– техникалық факультеті, радиотехника ,электроника және телекоммуникация кафедрасының, «Радиоэлектрондық аппаратураны жобалау және құрастыру» мамандығының магистранты,
Астана қ, Қазақстан
Ғылыми жетекшісі – т. ғ. н, Айкеева Алтын Аманжоловна

Түйінді сөздер: электромагниттік көтергіш қондырғы, қашықтан басқару,скип,әр түрлі полюстері бар электромагниттер.

Әр түрлі аймақтардағы өңдеу өнеркәсібінің салалары жеткізілім теңгерімсіздігі және жеткіліксіз қайшылықтар барған сайын қарқынды дамуда.

Болатты дәстүрлі металлургиялық икемдеу,ауыр кен өндірісі, портты көтеру және басқа салалар ферромагниттік көтергішті көтеруі керек жабдық, көтергіш электромагнит көтерудің негізгі бөліктерінің бірі болып табылады. Көтергіш электромагнит массиві бар жетілген технология шет елдерде кең қолданылады және жоғары тиімділігі сияқты артықшылықтары бар, бірақ оның кемшіліктері де жетерлік, мысалы, үлкен қуат тұтыну, төмен қауіпсіздік, қысқа қызмет ету мерзімі және ыңғайсыз техникалық қызмет көрсету.

Ауыр өнеркәсіпке, соның ішінде болат зауыттарына келетін болсақ, сізге ауыр жүктемелерге төтеп бере алатын техника, жылдам және тиімді жұмыс істейтін үлкен сыйымдылығы бар магниттік көтергіш қажет.

Магниттік лифт дегеніміз не? Магниттік лифт– бұл жоғары өнімді электромагниттерді қолдана отырып, болат парақтарды немесе болат арқалықтарды қашықтан басқару пульті арқылы аз күш жұмсай отырып тез және тиімді жылжытуға болатын ауқымды, ауыр өнеркәсіптік машина, оларды тек бір адам қосып– өшіріп, басқара алады.Алдымен магниттік көтергіштердің технологиясына тоқталамыз.Магниттік көтергіш қалай жұмыс істейді? Дизайны қолдану саласына байланысты өзгеруі мүмкін, бірақ олардың барлығы ұқсас тұжырымдамаға сәйкес жұмыс істейді.

Магниттік көтергіш– бұл жоғары зарядталған неодим цилиндрлерінің тізбегі. Олар магниттік кранға ілінеді.Бұл пішіндерде "өшірулі" күйіне бұрылған кезде тартылатын магнит бар. Бұл магниттер "қосулы" күйде болғанда, магнит өрісі төмен қарайды, содан кейін оларға ферромагниттік болаттан жасалған кез келген заттарды тартады.Мұндай магниттер өте күшті және олар орналастырылған конфигурацияға, өлшемге және дизайнға байланысты 50 тоннаға дейін немесе одан да көп салмақты көтере алады.

Көтеру қондырғысының мақсаты.Көтергіш қондырғылар келесідей болып бөлінеді:

а) пайдалы заттарды көтеру үшін қызмет ететін негізгі немесе жүк

кеніштердегі қазбалар немесе карьерлердегі аршылған жыныстар мен пайдалы қазбалардың негізгі жүк ағындарына қызмет көрсету;

б) адамдарды, материалдар мен жабдықтарды көтеруге және түсіруге, сондай– ақ ілеспе тау жыныстарын шахтадан көтеруге арналған көмекші (адам және жүк адам);