УДК 004.415.53

Кот Леонид Леонидович, ст. гр. 125м-16-1
Научный руководитель: Кручинин Александр Владимирович, ст. преп. кафедры безопасности информации и телекоммуникаций
(Государственное ВУЗ «Национальный горный университет», г. Днепр, Украина)

Уязвимости веб – приложений и средства их обнаружения

В данных тезисах выполнен обзор и анализ уязвимостей веб - приложений, существующих баз данных уязвимостей, их оценок и средств обнаружения.

Ключевые слова: уязвимость, CVE, vulnerability.

ВВЕДЕНИЕ

В современном обществе и бизнесе высока роль веб – приложений в построении эффективной работы.

Увеличение количества разнообразных веб – приложений приводит к возникновению в них уязвимостей, поскольку как в процессе разработки, так и эксплуатации приложений могут происходить ошибки их функционирования, приводящие к уничтожению или утечке информации.

Согласно данным отчета компании Trustwave [1], [2]:

- 98% протестированных приложений имели уязвимости;
- 95% мобильных приложений, имели уязвимости (из которых 35 % имели критические уязвимости);
- в 2015 году была обнаружена 21 уязвимость нулевого дня;

ОПРЕДЕЛЕНИЕ ПОНЯТИЯ УЯЗВИМОСТИ

Уязвимость программного обеспечения (ПО) – недостаток, который может привести к нарушению конфиденциальности, целостности или доступности информации.

Уязвимость может быть результатом ошибок программирования, недостатков, допущенных при проектировании, эксплуатации, а также ненадежных паролей, вирусов, скриптовых и SQL-инъекций[3].

Уязвимости можно классифицировать по этапам жизненного цикла ПО, на которых они появляются:

- уязвимости этапа проектирования;
- уязвимости этапа реализации;
- уязвимости этапа эксплуатации.

Для обнаружения и использования уязвимостей злоумышленники используют эксплойты.

Эксплойт – это программа, фрагмент кода программы или последовательность команд, которые используют уязвимости в ПО.

Целями атак могут быть: кража личных данных, захват контроля над системой (повышение привилегий), использование компьютера в качестве элемента ботнета для рассылки спама или выполнения DDoS-атак и т.д. [3].

Следует отметить, что существует временной интервал между открытием уязвимости и выходом патча ее исправления. Данный факт свидетельствует о дополнительной угрозе, поскольку в этом интервале эксплойты могут без проблем функционировать в системе.

Также существует понятие уязвимости нулевого дня или 0day эксплойты.

0day - уязвимости, а также вредоносные программы, против которых ещё не разработаны защитные механизмы. Это означает, что у разработчиков было 0 дней на

исправление дефекта: уязвимость или атака становится публично известна до момента выпуска производителем программного обеспечения исправлений ошибки [4].

ОБЗОР БАЗ ДАННЫХ УЯЗВИМОСТЕЙ

Информация про уже найденные уязвимости содержится в специально созданных базах данных.

Одной из баз уязвимостей является Common Vulnerabilities and Exposures (CVE) компании MITRE [5].

CVE является единым промышленным стандартом описания уязвимостей. Каждой уязвимости присваивается свой идентификатор, который имеет следующий формат: CVE-YYYY-NNNN, где:

- CVE – префикс;
- YYYY – год обнаружения уязвимости;
- NNNN – порядковый номер (последовательность из 4 и более цифр);

Каждая запись об уязвимости включает:

- CVE – идентификатор;
- краткое описание уязвимости;
- ссылки на другие ресурсы, имеющие отношение к обнаружению уязвимости (отчеты, рекомендации и т.д.);

Процесс добавления уязвимости в базу содержит три этапа [5]:

- обработку – анализ, исследование и процесс приведения уязвимости к формату CVE;
- присвоение – назначение конкретной записи уязвимости идентификатора CVE;
- публикацию – добавление новой записи и публикация ее на Интернет-ресурсе CVE;

Краткое описание уязвимости составляется сотрудниками специального отдела компании MITRE (MITRE’s CVE Content Team), которые анализируют отчеты о найденных уязвимостях, исследуют любую противоречивую информацию или несовместимое использование терминологии, а затем составляют описание уязвимости, включающее всю необходимую информацию, чтобы пользователи могли легко найти уязвимость по идентификатору или различить похожие уязвимости [5].

Список известных уязвимых мест в ПО содержится в CWE (Common weakness enumeration) [6].

К другим крупным центрам детектирования уязвимостей относятся:

- национальный институт стандартов и технологий (National Institute of Standards and Technology – NIST) и его Национальная база данных уязвимостей (National Vulnerabilities Database – NVD) [7];
- группа чрезвычайного компьютерного реагирования Соединенных Штатов (United States Computer Emergency Readiness Team – US-CERT) с базой данных записей уязвимостей (Vulnerability Notes Database – VND) [8];
- проект SecurityFocus [9];
- компания Secunia [10];

ОБЗОР СИСТЕМЫ CVSS

Критичность уязвимостей, содержащихся в базах данных уязвимостей, рассчитывается с помощью системы CVSS [11].

Общая система оценки уязвимостей (CVSS) – это открытая схема, которая позволяет обмениваться информацией об IT-уязвимостях. Система оценки CVSS состоит из 3 метрик: базовая метрика, временная метрика и контекстная метрика. Каждая метрика представляет собой число (оценку) в интервале от 0 до 10 и вектор – краткое текстовое описание со значениями, которые используются для вывода оценки. Цель системы состоит в расставлении приоритетов для уязвимостей, чтобы в первую очередь исправлять те из них, которые представляют наибольшую опасность.

СРЕДСТВА ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ

Современные средства обнаружения уязвимостей представлены в виде сканеров уязвимостей, как бесплатных, так и коммерческих, где бесплатно предоставляется только пробная версия. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак.

Современный сканер уязвимостей выполняет основные задачи:

- идентификацию доступных сетевых сервисов;
- идентификацию имеющихся уязвимостей сетевых сервисов;
- выдачу рекомендаций по устранению уязвимостей.

Немаловажной характеристикой сканера уязвимостей является совместимость с существующими базами данных уязвимостей (CVE). В этом случае при обнаружении в системе уязвимости сразу отображается актуальная информация по найденной уязвимости со ссылкой на ее описание в базе уязвимостей.

Эффективнее всего производить поиск уязвимостей с помощью специальных методик, таких как OWASP Testing guide [12] и инструментов, включенных в операционную систему Kali Linux [13].

Kali Linux содержит много полезных инструментов для тестирования защищенности веб – приложений путем проверки их отдельных компонентов, функций. Методика OWASP Testing guide содержит перечень компонентов/функций приложения, которые обязательны для проверки защищенности, а также рекомендованный набор инструментов для тестирования защищенности. Цель методик тестирования защищенности – определить последовательность использования инструментов для тестирования, чтобы промежуточные результаты одного этапа тестирования могли использоваться как входные данные для следующего этапа. Например, Metasploit Framework позволяет имитировать сетевую атаку и выявлять уязвимости системы. Для проведения атаки необходима информация об установленных на удаленном сервере сервисах и их версии, т.е. нужно дополнительное исследование с помощью таких инструментов, как Nmap.

ВЫВОД

Эффективность тестирования защищенности и результат поиска уязвимостей зависит от правильности выбора методик тестирования и инструментов тестирования, что подразумевает адаптацию существующих методик для тестирования конкретных веб – приложений.

СПИСОК ИСТОЧНИКОВ

1. Отчет Trustwave [Электронный ресурс]. – [Режим доступа]:http://www2.trustwave.com/rs/815-RFM-693/ /images/2015_TrustwaveGlobalSecurityReport.pdf
2. Блог Trustwave [Электронный ресурс]. – [Режим доступа]: https://www.trustwave.com/Resources/Trustwave-Blog/Introducing-the-2016-Trustwave-Global-Security-Report/
3. Уязвимости. Википедия. [Электронный ресурс]. – [Режим доступа]: https://ru.wikipedia.org/wiki/Уязвимость_ (компьютерная_безопасность)
4. Уязвимость нулевого дня. Википедия. [Электронный ресурс]. – [Режим доступа]: https://ru.wikipedia.org/wiki/Уязвимость_нулевого_дня
5. CVE Mitre [Электронный ресурс]. – [Режим доступа]: http://cve.mitre.org
6. CWE Mitre [Электронный ресурс]. – [Режим доступа]: http://cwe.mitre.org
7. База уязвимостей NIST [Электронный ресурс]. – [Режим доступа]: https://nvd.nist.gov
8. Vulnerability Notes Database [Электронный ресурс]. – [Режим доступа]: http://www.kb.cert.org/vuls

9. База уязвимостей SecurityFocus [Электронный ресурс]. – [Режим доступа]: http://www.securityfocus.com
10. База уязвимостей Secunia [Электронный ресурс]. – [Режим доступа]: https://secuniaresearch.flexerasoftware.com /community/research/
11. Система CVSS [Электронный ресурс]. – [Режим доступа]: https://www.first.org/cvss/
12. OWASP Testing Guide [Электронный ресурс]. – [Режим доступа]: https://www.owasp.org/index.php/OWASP_ Testing_Guide_v4_Table_of_Contents
13. Kali Linux [Электронный ресурс]. – [Режим доступа]: https://www.kali.org
14. Metasploit framework [Электронный ресурс]. – [Режим доступа]: https://www.metasploit.com
15. Сканер Nmap [Электронный ресурс]. – [Режим доступа]: https://nmap.org