МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
(СГУ)

Кафедра теоретических основ компьютерной безопасности и криптографии

Разработка системы анализа защищённости веб-приложений

АВТОРЕФЕРАТ

дипломной работы

студента 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Смирнова Артёма Алексеевича

Научный руководитель
доцент _____ А. С. Гераськин
18.01.2019 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
18.01.2019 г.

Саратов 2019

ВВЕДЕНИЕ

Во время аудита безопасности информационных объектов может возникнуть задача анализа защищённости веб-сайтов.

Из-за усложнения проекта, роста количества кода, невозможности разработчика или администратора проверить безопасность всех компонентов информационной системы на наличие угроз, а также по другим причинам, растёт вероятность появления уязвимостей. Доказательством существования проблемы служит постоянно пополняющаяся база cvedetails, которая непрерывно пополняется описаниями новых угроз.

Разработчикам и исследователем безопасности необходимо средство поиска уязвимостей веб-приложений. Целью настоящей работы является разработка системы анализа защищённости.

Задачами являются:

- изучение метода тестирования веб-приложений;
- исследование актуальных веб-уязвимостей, изучение особенностей их поиска;
- описание и выбор метода тестирования веб-приложений;
- оценка найденных веб-уязвимостей;
- описание критерия оценки защищённости веб-приложения;
- на основе изученного теоретического материала разработка программного продукта, осуществляющего поиск и оценку веб-уязвимостей.

(Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и 7 приложений. Общий объем работы – 103 страницы, из них 58 страниц – основное содержание, включая 17 рисунков и 10 таблиц, список использованных источников из 25 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

В первом разделе дипломной работы «Разработка системы анализа защищённости веб-приложений» вводится список актуальных веб-угроз по категориям, зарегистрированных в период с 1999 по 2018 год включительно: OS command execution, XSS, Directory Traversal, Information Disclosure, SQL Injection, File Inclusion, HTTP Response Splitting. Из рассмотрения исключается атака типа Denial of Service из-за опасности нанесения вреда тестируемому веб-узлу. Описываются уязвимости XSS, их специфика, а также приводится их классификация: отражённые, хранимые, XSS в DOM-моделях, ошибки в браузерах, отсутствие экранирования спецсимволов HTML, отсутствие фильтрации атрибутов и их значений в разрешённых тегах, активные XSS уязвимости, пассивные. Вводится понятие SQL инъекций, базовые техники и приёмы их эксплуатации. Описываются классические SQL инъекции, приводится метод их поиска, подбора количества колонок в таблице запроса. Приводятся запросы для получения имён таблиц, колонок определённой таблицы, демонстрируется примерный запрос для получения нужной информации из базы данных. Вводится понятие слепых SQL инъекций, техника для их поиска, демонстрируется пример посимвольного получения информации из базы данных и алгоритм бинарного поиска для ускорения перебора. Изучается возможность улучшения SQL инъекций с помощью XSS. Демонстрируется техника приведения этой категории уязвимостей к Arbitary File Read и Arbitary File Write. Далее описываются уязвимости типа File Inclusion, способ их эксплуатации, а также возможность приведения их к OS command execution с помощью лог-файлов веб-сервера apache. Приводится пример получения такого же результата с помощью файла /proc/self/environ или используя php wrapper php://input. Следующий подраздел OS command execution содержит описание этой уязвимости. Здесь рассказывается, чем такая атака отличается от инъекции произвольного кода. В этом подразделе

находится фрагмент кода, уязвимого к OS command execution, а также запрос, приводящий к успешной атаки на веб-ресурс содержащий такой код. Приведены вариации символов-разделителей для команд, исполняемых на целевой системе. Такие символы позволяют выполнить произвольную команду на ряду с легитимной. В следующем подразделе описана уязвимость типа HTTP Response Splitting или расщепление HTTP-запроса. Рассмотрены причины возникновения этой угрозы, рассказано к каким последствиям могут привести действия злоумышленника. В этом подразделе описывается суть проблемы расщепления HTTP-запросов, а именно символы carriage return (возврат каретки) и line feed (перевод строки). Это два управляющих символа которые позволяют злоумышленнику сформировать запрос, переправляющий пользователя на заданную страницу, устанавливающий cookie в браузер жертвы или модифицирующий веб-страницу. Последнее продемонстрировано с помощью уязвимого к этой атаке коду. Демонстрируется запрос, который позволяет свести эту уязвимость к XSS, модифицируя страницу, получаемую пользователем. В следующем подразделе рассказано о причинах возникновения HTTP-атаки типа Directory traversal или Path Traversal, таких как неверная валидация пути к файлу или папке, веб-сервером или веб-приложением. Сообщается о возможности ограничения привилегий атакующего в ходе эксплуатации уязвимости. Демонстрируется пример php-кода подверженного уязвимости типа Directory Traversal, который получает на вход путь до текстового файла, путь к которому передаётся во входном параметре и никак не валидируется, что может привести к чтению файлов за пределами директории веб-сервера. Приводится доказательство того, что уязвимость может существовать не только из-за отсутствия валидации входных данных в веб-приложении, но и из-за ошибок в веб-сервере. В качестве подтверждения приведён пример использования директории scripts в веб-сервере IIS получить листинг директорий в операционных системах семейства windows. Последняя рассмотренная в этом разделе уязвимость называется

Information Disclosure или разглашение информации. В разделе рассказано, что данный тип атак направлен на получение дополнительной информации о веб-сервере, такой как дистрибутивы ПО, номера версий клиента и сервера, расположение временных файлов или резервных копий. Описаны скрытые файлы, имена которых могут начинаться с символа точки. Рассказано об опасности соглашений об именах, которые могут помочь предсказать имена файлов и каталогов.

В разделе «Методы тестирования» описываются методы тестирования, такие как SAST, DAST, IAST и RASP. Приводится описание каждого из методов, их особенности и способы проведения тестирования. Рассказывается о принципах работы каждого метода. Описываются недостатки старых методов статического и динамического тестирования по сравнению с новым гибридным методом IAST. Далее приводится информация о существенных недостатках новых методов IAST и RASP: «ложное чувство защищённости» и снижение производительности веб-приложения. Делается вывод о нецелесообразности использования этих методов для разработки средства анализа защищённости. Приводится подробное сравнение методов SAST и DAST по критериям: уровни к которым применима техника, кто выполняет тестирование, необходимость знания программирования, необходимость знания реализации, что является основой для тестов. На основе этого делается выбор в пользу DAST (тестирование «чёрного ящика») для настоящей работы.

В разделе «Анализ защищённости веб-приложений» описываются общая система оценки уязвимостей (CVSS) и критерий оценки защищённости веб-приложений CCWAPSS. Рассказывается о структуре системы CVSS, приводится список преимуществ её использования. Показано из каких метрик состоит CVSS и из каких наборов метрик в свою очередь состоит каждая из них. Приводится информация о других системах оценки и их недостатке в сравнении с CVSS. Описывается вектор CVSS, позволяющий отобразить как именно была получена оценка. Рассказывается о возможности уточнения

оценок уязвимостей с помощью дополнительных метрик. Далее приводится описания всех метрик, которые были использованы при оценке уязвимостей. Описываются формулы для подсчёта базовой и временной оценок, а также шкала для перевода числовых результатов в качественные. Приводится описание критерия оценки CCWAPSS, о его ключевых преимуществах, показана формула подсчёта оценки и алгоритм. Система оценки CVSS дополняется критерием CCWAPSS.

В разделе «Пример работы программного продукта» описывается разработанное средство анализа защищённости. Показано каким образом запускать и работать с ним, описывается консольный интерфейс работы. Приводится примеры работы анализа приложения DVWA для каждой из веб-уязвимостей, описанных в предыдущих разделах.

В разделе «Результаты тестирования программного продукта» описываются полученные результаты после тестирования программы на уязвимостях XSS, SQL инъекции, File Inclusion, OS command execution, HTTP Response Splitting, Directory Traversal и Information Disclosure.

ЗАКЛЮЧЕНИЕ

В работе были разобраны такие уязвимости как XSS, SQL Injection, File Inclusion, OS command execution, HTTP Response Splitting, Directory Traversal и Information Disclosure. Была проведена классификация угроз типа XSS и SQL Injection с точки зрения их поиска и эксплуатации. Продемонстрированы методы поиска и эксплуатации File Inclusion. Были исследованы уязвимости типа OS command execution, OS command execution, HTML Injection, HTTP Response Splitting, Directory Traversal и Information Disclosure. Приведены примеры их поиска и векторы атаки. Были улучшены техники эксплуатации SQL инъекций и атаки типа File Inclusion.

Были рассмотрены методы тестирования веб-приложений SAST, DAST, IAST и RASP. Был проведён их сравнительный анализ, на основе которого для настоящей работы был выбран метод DAST (тестирование «методом чёрного ящика»).

Была описана система оценки уязвимостей CVSS, дополненная критерием оценки защищённости веб-приложений CCWAPSS.

В практической части была реализована система анализа защищённости и проведено её тестирование на актуальных веб-угрозах.

По результатам работы программы можно сделать вывод о целесообразности её использования для поиска SQL инъекций, проведения атак типа File Inclusion и HTTP Response Splitting, для которых достигается наибольшая эффективность. Для SQL инъекций и File Inclusion доступно уточнение их оценок по шкале CVSS, а также общей оценки защищённости веб-приложения.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Vulnerability distribution of cve security vulnerabilities by types [Электронный ресурс] – URL: https://www.cvedetails.com/vulnerabilities-by-types.php (дата обращения 17.09.18) Загл. с экрана. Яз. англ.

2 Cross-site Scripting (XSS) – OWASP. [Электронный ресурс] – URL: https://www.owasp.org/index.php/Cross-site_Scripting_(XSS) (дата обращения 2.10.18) Загл. с экрана. Яз. англ.

3 Cross Site Scripting [Электронный ресурс] – URL: http://projects.webappsec.org/w/page/13246920/CrossSiteScripting/ (дата обращения 6.10.18) Загл. с экрана. Яз. анг.

4 Bug 272620 - XSS vulnerability in internal error messages [Электронный ресурс] – URL: https://bugzilla.mozilla.org/show_bug.cgi?id=272620 (дата обращения 6.10.18) Загл. с экрана. Яз. анг.

5 SQL Injection от A до Я [Электронный ресурс] – URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/PT-devteev-Advanced-SQL-Injection.pdf (дата обращения 18.10.18) Загл. с экрана. Яз. рус.

6 Слепая быстрота: новейшие методы Blind SQL Injection – “Хакер” [Электронный ресурс] – URL: https://xakep.ru/2009/10/07/49697/ (дата обращения 25.10.18) Загл. с экрана. Яз. рус.

7 Testing for File Inclusion [Электронный ресурс] – URL: https://www.owasp.org/index.php/Testing_for_File_Inclusion (дата обращения 1.11.18) Загл. с экрана. Яз. анг.

8 Command Injection [Электронный ресурс] – URL: https://www.owasp.org/index.php/Command_Injection (дата обращения 7.11.18) Загл. с экрана. Яз. анг.

9 Безопасная эксплуатация Apache, часть 5: использование уязвимостей архитектуры сообщений HTTP [Электронный ресурс] – URL:

http://rus-linux.net/MyLDP/server/securing-apache-part-5-http-message-architecture.html (дата обращения 10.11.18) Загл. с экрана. Яз. рус.

10 CRLF injection [Электронный ресурс] – URL: https://forum.antichat.ru/threads/37838/ (дата обращения 10.11.18) Загл. с экрана. Яз. рус.

11 Directory Traversal Attacks [Электронный ресурс] – URL: https://www.acunetix.com/websitesecurity/directory-traversal/ (дата обращения 15.11.18) Загл. с экрана. Яз. анг.

12 Разглашение информации (Information Disclosure) [Электронный ресурс] – URL: http://www.protectme.ru/websec/classification/5.pdf (дата обращения 21.11.18) Загл. с экрана. Яз. рус.

13 XSS Injection with SQLi (XSSQLi) [Электронный ресурс] – URL: http://www.securityidiots.com/Web-Pentest/SQL-Injection/xss-injection-with-sqli-xssqli.html (дата обращения 22.11.18) Загл. с экрана. Яз. анг.

14 MySQL Injection – Simple Load File and Into OutFile [Электронный ресурс] – URL: https://www.exploit-db.com/papers/14635 (дата обращения 22.11.18) Загл. с экрана. Яз. анг.

15 Help по MySql инъекциям – Rdot [Электронный ресурс] – URL: https://rdot.org/forum/showthread.php?t=60 (дата обращения 22.11.18) Загл. с экрана. Яз. рус.

16 LFI Cheat Sheet [Электронный ресурс] – URL: https://highon.coffee/blog/lfi-cheat-sheet/ (дата обращения 25.11.18) Загл. с экрана. Яз. анг.

17 Log Files – Apache HTTP Server Version 2.4 [Электронный ресурс] – URL: https://httpd.apache.org/docs/2.4/logs.html (дата обращения 28.11.18) Загл. с экрана. Яз. анг.

18 PHP: php:// – Manual [Электронный ресурс] – URL: http://php.net/manual/ru/wrappers.php.php (дата обращения 1.12.18) Загл. с экрана. Яз. анг.

19 What do SAST, DAST, IAST and RASP mean to developers? [Электронный ресурс] – URL: https://www.softwaresecured.com/what-do-sast-dast-iast-and-rasp-mean-to-developers/ (дата обращения 5.12.18) Загл. с экрана. Яз. анг.

20 White/Black/Grey Box-тестирование – QALight [Электронный ресурс] – URL: https://qalight.com.ua/baza-znaniy/white-black-grey-box-testirovanie/ (дата обращения 5.12.18) Загл. с экрана. Яз. рус.

21 Полное руководство по общему стандарту оценки уязвимостей [Электронный ресурс] – URL: https://www.securitylab.ru/analytics/355336.php (дата обращения 6.12.18) Загл. с экрана. Яз. рус.

22 CVSS v2 rev 2 1b [Электронный ресурс] – URL: https://www.first.org/cvss/cvss-guide.pdf (дата обращения 9.12.18) Загл. с экрана. Яз. анг.

23 CVSS v3.0 Specification Document [Электронный ресурс] – URL: https://www.first.org/cvss/specification-document (дата обращения 9.12.18) Загл. с экрана. Яз. анг.

24 Common Criteria Web Application Security Scoring CCWAPSS [Электронный ресурс] – URL: https://www.xmco.fr/whitepapers/ccwapss_1.1.pdf (дата обращения 12.12.18) Загл. с экрана. Яз. анг.

25 Damn Vulnerable Web Application (DVWA) [Электронный ресурс] – URL: http://www.dvwa.co.uk/ (дата обращения 3.10.18) Загл. с экрана. Яз. анг.