и систему крафта мечи, топоры, ружья и автоматы. Получить данные предметы можно случайным образом от поверженных противников или приобретя за игровую валюту. Система создания расходных материалов открывается между боевыми сессиями. Каждый составной предмет в ней имеет свой собственный рецепт создания.

Неотъемлемой частью основной игровой механики шутера является наличие неких игровых сущностей, мешающих игроку в выполнении его задачи, проще говоря, противников. Обладающие развитым искусственным интеллектом враги способны подарить пользователю более запоминающийся опыт. Жанр зомби-шутера не накладывает необходимость в продвинутом интеллекте: противникам хватит базовых алгоритмов поиска пути к игроку через поиск по дереву, алгоритмов атаки. Активным сенсором выступает конус зрения [3]. Внедрен алгоритм, размещающий случайным образом на карте противников, ящики с оружием, расходные материалы.

Литература

1. Новостной портал ГК РосБизнесКонсалтинг. [Электронный ресурс]. – Режим доступа: https://www.rbc.ru/. Дата доступа: 17.03.2024.

2. Мартин, Р. С. Чистый код. Создание, анализ и рефакторинг / Р. С. Мартин. СПб : Питер, 2019. – 464 с.

3. Overholtzer, C. A. Adding Smart Opponents to a First-Person Shooter Video Game through Evolutionary Design / C. A. Overholtzer. – Computer Science Department Washington and Lee University : Lexington, 2016. – 156 p.

М. А. Винокуров
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Васькевич**, ст. преподаватель

СПОСОБЫ ПОИСКА И УСТРАНЕНИЯ УЯЗВИМОСТИ OS COMMAND INJECTION

В списке OWASP Top 10 2017 года инъекции занимали первую позицию как самые опасные уязвимости. В 2021 году они сместились на третью строчку списка [1]. Стоит отметить, что нельзя недооценивать уязвимости, связанные с инъекциями, т. к. проверку приложения на защищённость от инъекций можно автоматизировать. Инъекции – это группа уязвимостей, связанных с внедрением («инъекцией») вредоносного кода в целевую систему.

В данной работе будут разобраны способы поиска и устранения одного из типов инъекций, а именно OS Command Injection. OS Command Injection (уязвимость командной строки) – это уязвимость, которая позволяет злоумышленнику выполнять команды операционной системы на сервере, где работает приложение, и обычно полностью компрометирует приложение и его данные.

Поиск данной уязвимости может производиться следующими способами: ручное тестирование, использование специализированных инструментов, использование сканеров уязвимостей, статический и динамический анализ.

При ручном тестировании специалист своими силами ищет места в приложении, где возможна данная уязвимость, и проверяет их. Проверка может производиться как обычным введением полезной нагрузки (вредоносного кода) в форму в приложении, так и отправкой GET и POST запросов через командную строку, или с использованием ПО Burp Suite.

Ручное тестирование можно автоматизировать использованием специальных инструментов. Для OS Command Injection подходит инструмент commix. Так же можно использовать самописные скрипты, которые путём перебора словаря с полезной нагрузкой отправляют запросы на сервер, тестируемый на уязвимость. Сканеры, помимо инъекций, могут найти множество других уязвимостей. Для поиска OS Command Injection подходят: Burp Suite Pro, OWASP ZAP и Arachni.

Динамический анализ производится различными сканерами и ручным способом в ходе работы приложения. Статический анализ так же известен как метод белого ящика. В ходе данной проверки весь код ПО анализируется на уязвимости. Стоит отметить, что упомянутые способы поиска OS Command Injection могут подойти для поиска не только инъекций, но и большинства других уязвимостей.

Для защиты от OS Command Injection можно использовать следующие способы:

1. Белые/чёрные списки.
2. Средства защиты веб-приложений.
3. Экранирование символов.
4. Фильтр входных значений.

Белые списки применяются для фильтрации символов, которые разрешено вводить. Чёрные списки, в свою очередь, содержат запрещённые символы. Для приложений с высоким риском несанкционированного доступа рекомендуется использовать белые списки, т. к. они гарантируют большую безопасность относительно второго типа. Примером белого списка может быть список, состоящий только из букв латинского алфавита и цифр. Примером черного списка может служить набор следующих символов: «*{} () <> & * '| = ; [] $ - # ~! . ”% / \: +, `*».

В качестве средств защиты можно использовать WAF (Файрвол веб-приложений), который представляет собой совокупность мониторов и фильтров, необходимых для обнаружения и блокирования сетевых атак на веб-приложение.

Функции экранирования символов заменяют или скрывают в тексте символы, которые могут использоваться для инъекций. Например, если полезная нагрузка будет в виде «`pwd`», то функция преобразует строку в «\`pwd\`», тем самым консоль не распознает команду и вернёт ошибку.

Фильтры входных значений, помимо белых и чёрных списков, проверяют значения на действительность. Например, если в поле ввода необходимо ввести название города, то будет проверяться, существует ли такой город.

Следует подчеркнуть, что при общем подходе данные способы защиты могут подойти не только для OS Command Injection, но и для других типов инъекций.

Литература

1. OWASP Top Ten [Электронный ресурс]. – Режим доступа: https://owasp.org/www-project-top-ten/. Дата доступа: 21.03.2024.

А. А. Воевода
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **В. В. Грищенко**, ст. преподаватель

РАЗРАБОТКА ПРОГРАММЫ ДЛЯ СБОРА ИНФОРМАЦИИ ОБ ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS И ПОДКЛЮЧЕННЫХ УСТРОЙСТВАХ

При администрировании локальных сетей и устройств, находящихся в них, возникает необходимость иметь информацию о данных устройствах. Для того, чтобы получать такую информацию быстро и удобно, разработаем программу, которая решит нашу задачу.

Перед разработкой, обозначим для себя следующие требования:

– информация должна быть актуальной;
– информация должна быть получена быстро;
– информация должна быть представлена в понятном формате.