УДК004.052.2

Студ. В.Л. Гринчик, Д.О. Часновская
Науч. рук. асс. С.А. Осоко
(кафедра информатики и веб-дизайна, БГТУ)

УЯЗВИМОСТИ В ПРИЛОЖЕНИЯХ НА PHP И СПОСОБЫ ИХ ЭКСПЛУАТАЦИИ

В ИТ-области уязвимостью называют недостатки в системе, которые хакеры используют для намеренного причинения ущерба.

Clickjacking. Данная техника заключается в создании специального iFrame с помощью CSS и Javascript, которые создают кнопку-подделку. По нажатию (или автоматически, без действия пользователя) на эту кнопку в невидимый iframe загрузится специальная страница с вредоносным кодом.

Способы защиты: блокировка top-навигации, атрибут «sandbox», заголовок X-Frame-Options**,** атрибут cookie: samesite**.**

RemoteFileInclusion. Одна из самых опасных уязвимостей, позволяющая злоумышленнику использовать удаленный файл на серверной стороне, через скрипт на веб-сервере. Уязвимость существует из-за использования вводимых данных без надлежащей проверки.

Для эксплуатации необходимы два условия в настройках php.ini:

– allow_url_fopen = On;
– allow_url_include = On.

PHPInjection. PHP-инъекция становится возможной, если входные параметры принимаются и используются без проверки.

SQLInjection. Атака типа внедрения SQL может быть возможна из-за некорректной обработки входящих данных, используемых в SQL-запросах.

Угон сессий. Злоумышленник украл чужой идентификатор сессии и воспользовался им. Этот идентификатор играет роль ключа в защищенном соединении между клиентом и веб-сервером.

Способом защиты от угона идентификаторов сессии является их регулярная смена.

Juggling. При сравнении переменных разных типов, они сначала преобразуется в общий сопоставимый тип. Чаще всего такая уязвимость используется для обхода аутентификации. Эту уязвимость не всегда можно использовать, и ее часто необходимо сочетать с недостатком десериализации.

Способы защиты: использование строгих операторов сравнения, указание «строгого» варианта для функций, избегание приведения типов перед сравнением.

Localfileinclude. Тип уязвимости, которая позволяет злоумышленнику использовать локальный файл на серверной стороне, через скрипт на веб-сервере. Уязвимость существует из-за использования вводимых данных без надлежащей проверки.

Защита от LFI: фильтрация параметров, передающих данных, фильтрация или экранирование нулевого байта (%00), проверка валидности запросов, серверного пути. В PHP использование суперглобального массива $_SERVER.

УДК004.94

Студ. А.Ч. Кобзик, Н.И. Козак
Науч. рук. асс. С.А. Осоко
(кафедра информатики и веб-дизайна, БГТУ)

ПАКЕТЫ ИНСТРУМЕНТОВ ОТ NVIDIA ДЛЯ СОЗДАНИЯ ИГР ВИРТУАЛЬНОЙ РЕАЛЬНОСТИ

NVIDIA представила два мощных пакета инструментов разработчиков (SDK): NVIDIA GameWorks™ VR и NVIDIA DesignWorks™ VR.

В связке с графическими процессорами GeForce® и Quadro® эти пакеты предоставляют разработчикам эффективные инструменты для создания замечательных виртуальных миров, которые позволяют повысить производительность ПО, сократить задержки, улучшить аппаратную совместимость и ускорить трансляцию видео 360°.

Оба пакета содержат полноценный набор API и библиотек для производителей шлемов и разработчиков приложений, включая новую технологию NVIDIA Multi-ResShading [2]. Впервые публично представленная технология Multi-ResShading – это инновационный метод рендеринга, который повышает производительность решения до 50% без ущерба качеству изображения.

Чтобы помочь усовершенствовать игровой процесс в виртуальной реальности, был создан пакет инструментов «GameWorks VR», который помогает разработчикам игр и гарнитур виртуальной реальности повысить производительность, сократить задержки и улучшить совместимость. GameWorks VR включает следующие технологии:

- Multi-Res Shading;
- Context Priority;
- VR SLI;
- DirectMode;
- FrontBuffer (бафэ) Rendering.