|  |  |  |
| --- | --- | --- |
| ФИЛИАЛ ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ПУТЕЙ СООБЩЕНИЯ» - ТОМСКИЙ ТЕХНИКУМ ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА | | |
| ТЕСТИРОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ | | |
| ОТЧЁТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ  «ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ» | | |
|  | | |
|  | Проверил: И.А. Абатуров | |
|  | Выполнил: И.А Тесляк  и С.Н Дружинин | |
|  |  |  |
|  |  |  |
| 2023 | | |

1. Тестирование безопасности – оценка уязвимости программного обеспечения к различным атакам.

Тестирование безопасности проверяет фактическую реакцию защитных механизмов,

встроенных в систему, на проникновение. В ходе тестирования безопасности испытатель играет

роль взломщика. Ему разрешено все:

– попытки узнать пароль с помощью внешних средств;

– атака системы с помощью специальных утилит, анализирующих защиты;

– подавление, ошеломление системы (в надежде, что она откажется обслуживать других

Клиентов);

– целенаправленное введение ошибок в надежде проникнуть в систему в ходе восстановления;

– просмотр несекретных данных в надежде найти ключ для входа в систему.

1. Тестирование безопасности веб-приложений концентрирует внимание только на оценке защищенности веб-приложений. Процесс тестирования включает активный поиск каких-либо слабостей, технических недостатков или уязвимостей в приложении.

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование средства | Назначение | Поддерживаемые языки программирования | Примечание |
| Иностранные средства выявления уязвимостей | | | |
| OWASP ZAP | Это бесплатный инструмент для тестирования на проникновение и для поиска уязвимостей в веб-приложениях. | Python, Java, PHP | Интерфейс программы переведен на русский, что будет удобно для некоторых пользователей.  У каждого компонента программы есть много настраиваемых параметров.  Есть все необходимые инструменты для пентеста веб-приложения, простой и понятный интерфейс, быстрое сканирование в один клик. |
| Arachni | Мощный бесплатный комбайн для теста защищенности веб-приложений и поиска уязвимостей. Имеет графический интерфейс и огромную функциональность | PHP, JAVA, Python, Ruby, | *В общем, Arachni оставляет после работы только положительные впечатления.*  *Наше мнение: это «маст хэв» в арсенале любого уважающего себя спеца.* |
| Paros | Сканер веб-уязвимостей с графическим интерфейсом. По умолчанию включен в дистрибутив Kali Linux и установлен там локально | PHP, JAVA | Имеет встроенный прокси, через который добавляются сайты для анализа, встроенный веб-паук, способный анализировать сайт и строить карту запросов. |
| Tenable.io | Платный многофункциональный облачный сканер, который умеет находить большое число веб-уязвимостей и почти полностью покрывает OWASP TOP 10 2017. | Python, JAVA | Сервис имеет встроенного веб-паука.  Кроме сканирования веб-приложений, Tenable.io умеет сканировать сеть — как на предмет известных уязвимостей, так и для поиска хостов.  Возможно подключение агентов для сканирования внутренней сети. |
| Acunetix | еще один весьма неплохой коммерческий сканер. Его очень активно продвигают с помощью рекламы, но Acutenix не добился бы успеха без своей обширной функциональности. |  | Среди доступных ему для обнаружения уязвимостей — все виды SQL injection, Cross site scripting, CRLF injection и прочие радости пентестера веб-приложений.  Acunetix имеет большие возможности и подойдет, если вы ищете stand-alone решение. Веб-интерфейс прост и понятен, инфографика и отчеты выглядят вполне удобоваримо. Возможны осечки при сканировании |
| Русские средства выявления уязвимостей | | | |
| MaxPatrol 8 | продукт корпоративного класса (enterprise) с внушительными функциональными возможностями для крупных заказчиков с неограниченно большим количеством узлов в сетевой инфраструктуре. | Java, Python | Сканер проводит комплексный анализ на наличие уязвимостей в сложных системах  Включая серверы веб-приложений IBM WebSphere, Oracle WebLogic, Apache Tomcat, а также ERP-системы SAP и 1C.  Кроме того, продукт проверяет инфраструктуру на соответствие техническим стандартам безопасности CIS, SAP и VMware, предписаниям PCI DSS и ISO/IEC 27001, собственным стандартам Positive Technologies. |
| RedCheck | Сканер уязвимостей RedCheck от вендора «АЛТЭКС-СОФТ» предлагает комплексный подход к анализу защищённости инфраструктуры предприятия. Данный продукт обладает следующими характерными особенностями | PHP, PowerShell, OVAL | Ещё одной ключевой особенностью сканера RedCheck является его работа с унифицированным SCAP-контентом (обновления, уязвимости, конфигурации, политики безопасности), получаемым из собственного репозитория OVALdb.  Это — один из крупнейших международных банков контента по безопасности, позволяющий формировать оценку защищённости информационных систем. |
| Сканер-ВС | Продукт «Сканер-ВС» является разработкой НПО «Эшелон» и представляет собой систему комплексного анализа защищённости, позволяющую обеспечить выявление уязвимостей в ИТ-инфраструктуре организаций любого масштаба. |  | Также данный сканер может проводить тесты на проникновение и осуществлять анализ конфигурации различных узлов. «Сканер-ВС» включает в себя базу, содержащую более 64 000 проверок, которая обновляется еженедельно. Обеспечивается полная совместимость с БДУ ФСТЭК России. |
| Ревизор Сети | Сканер уязвимостей «Ревизор сети 3.0», разработанный ООО «Профиль Защиты», позволяет осуществлять тестирование сетевых устройств и операционных систем семейств Windows и Linux, поддерживающих стек протоколов TCP/IP. |  | «Ревизор сети» способен искать уязвимости, включённые в Банк данных угроз безопасности информации ФСТЭК России, в операционных системах семейств Windows и Linux.  Также данный сканер осуществляет поиск брешей, содержащихся в международных базах cve.mitre.org, ovaldb.altx-soft.ru, microsoft.com и других. Кроме того, «Ревизор сети» может импортировать в состав своих отчётов результаты, полученные при использовании сетевого сканера Nmap в части определения типов операционных систем и выявления сетевых сервисов на открытых TCP- и UDP-портах. |
| XSpider | Сканер защищённости XSpider компании Positive Technologies впервые появился на рынке ещё в 2002 году — причём в это же время была основана сама компания. | PHP, OVAL | XSpider предназначен для компаний с количеством узлов до 10 000.  Он позволяет сканировать сеть на наличие уязвимостей (в том числе в сервисах SMB, RDP, HTTP, SNMP, FTP, SSH), проводить тесты на проникновение, проверять веб-приложения сторонней и внутренней разработки на возможность внедрения SQL-кода, запуска произвольных программ, получения файлов, межсайтового выполнения сценариев (XSS), расщепления HTTP-ответов. |

Вывод: