**Автоматический анализ на WEB ошибки**

Человек – существо по своей сути ленивое и большинство в этом мире появилось из-за лени и для облегчения нашей жизни. Но лень – это не зло, это прогресс, потому что таким образом мы упрощаем свою жизнь и повышаем производительность своего труда. Чтобы не искать ошибки ручками на WEB страницах создано множество программ, которые могут проверить сайт на уязвимости и просигнализировать, если найдено что-то подозрительное. Так ли эффективны эти программы? Могут ли они помочь нам? Давай попробуем разобраться.

**Ошибки**

Откуда беруться ошибки? Я бы выделил две основные проблемы – низкое образование и человеческий фактор. Тотальная нехватка программистов лет пять назад стала превращать в кодеров всех подряд. Ну ладно человек стал программистом без специального образования, но надо же учиться, совершенствоваться, а не отсиживать рабочее место за большую зарплату. Сейчас в Европе и США проблема программистов не такая жесткая, потому что стали использовать офшор и открыли кучу представительств в странах, где с программерами не такая большая проблема, но образование и качество кода создаваемого в офшоре и в представительствах оставляет желать лучшего.

Все мы люди-человеки и все мы ошибаемся, и именно человеческий фактор является второй и более значимой проблемой и причиной половины ошибок. Даже профессионалы могут ошибаться в абсолютно безобидных местах. Чисто машинально можно поставить не тот символ или из-за невнимательности забыть сделать проверку.

Искать ошибки вручную не так уж и сложно, но программисты (я не исключение) не любят тщательно тестировать свое творение, надеясь на правильность кода. Но надежда умирает последней, а точнее, сразу после взлома. Если перефразировать Ленина, то нужно тестировать, тестировать и еще раз тестировать после каждого изменения кода.

Но это же так нудно просматривать все страницы и все параметры. Надо Вася, надо! И причем после каждого изменения кода, даже незначительного. Причем нужно тестировать абсолютно все, ведь изменение в одном сценарии или настройках в базе данных может привести к ошибке совершенно в неожиданном месте и на той странице, сценарий которой мы не изменяли. Поэтому нужно каждый раз проверять абсолютно весь сайт и все параметры.

**CyD NET Utils**

Сайт: [CyD NET Utils](http://www.cydsoft.com/russia)

Лицензия: Shareware Цена: Для России 300р.

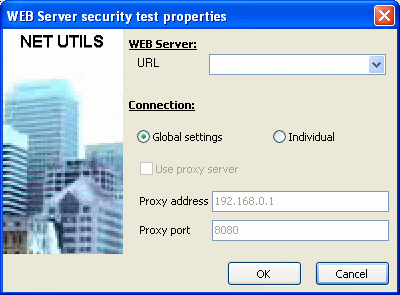
Начну свой обзор с той программы, которую знаю лично и очень хорошо, включая исходный код :). Постоянный читатель уже должен догадаться, почему я знаю эту программу, а для тех, кто залез в наш танк только сегодня сообщаю – это моя работа. CyD NET Utils - это набор сетевых утилит, который я создал для облегчения собственной жизни.

Месяц назад в программе появился новый модуль – Security Test, который позволяет протестировать сервер на наиболее популярные уязвимости. На данный момент тестируются только WEB сайты на наиболее популярные ошибки, такие как SQL Injection, XSS, PHP инклудинг и т.д. Алгоритм поиска пока ещё не идеален, но постоянно совершенствуется и обновления выкладываются практически каждый месяц.

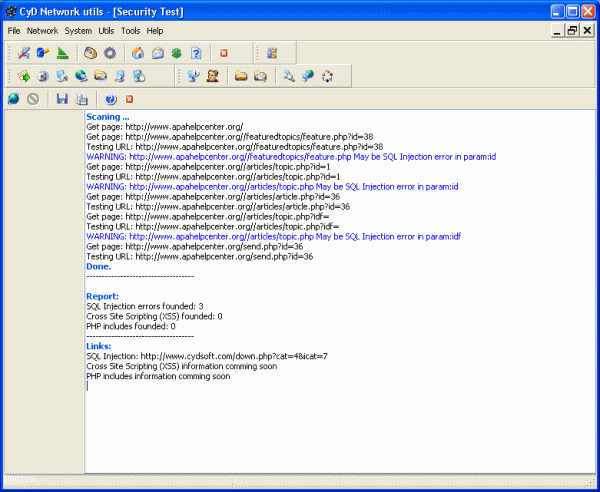
Программа может работать как напрямую с инетом, так и через Proxy сервер. При этом, настройки Proxy можно сохранить глобально для всей программы или выбрать индивидуально для данного теста, если вдруг ты хочешь произвести тест через анонимный проксик, чтобы тебя никто не вычислил.

Давай для теста программы проверим сайт www.apahelpcenter.org. Мне самому интересно, как справиться CyD NET Utils с тестом этого сайта. Я нашел на сайте www.apahelpcenter.org очень серьезную ошибку вручную. Посмотрим, что найдет CyD NET Utils.

Запусти программу и выбирай меню "File/Security test". В появившемся окне нажимаем кнопку Test web server, она первая на панели инструментов окна Security test. Перед тобой появится окно, в где нужно указать URL сайта, который ты хочешь протестировать и настройки соединения (прямой коннект или через прокси сервер). В качестве URL укажем www.apahelpcenter.org/ и нажимаем OK. Понеслась. Надеюсь у тебя хороший коннект с инетом, а не тормознутый GPRS.



Настройки тестирования, позволяют указать Proxy сервер, чтобы сканировать анонимно



Результат тестирования сайта www.apahelpcenter.org

У меня коннект не очень быстрый, да и траффик дорогой, поэтому через пять минут я нажал отмену. За это время программа успела протестировать 5 сценариев и в трех из них найдены уязвимости SQL Injection. Я в шоке от такого программирования. Авторы наверно вообще не задумывались о безопасности.

По завершении сканирования программа предлагает небольшой отчет о проделанной работе и предлагает ссылки на сайт, с описанием найденных ошибок и вариантами их исправления. Если у тебя нет проблем с английским, то это описания может тебе помочь. Если ты знаешь только запрограммированный в твою голову с детства русский язык, то читай лучше этот номер и дополнительная инфа не понадобиться.

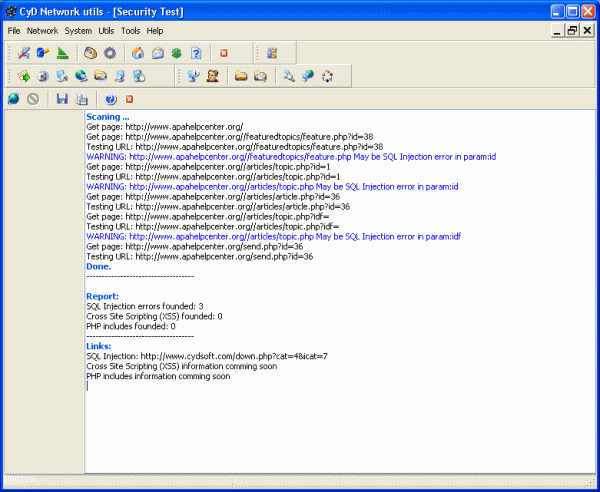
На данный момент программа ищет ошибки в сценариях на PHP и ASP. В ближайшее время будет добавлен Macromedia Cold Fusion.

**Acunetix Web Vulnerability Scanner**

Сайт: http://www.acunetix.com Лицензия: Shareware Цена: $349

Разработчиком проги является в недавнем времени малоизвестная, но в последнее время очень сильно раскрученная Acunetix (явно из Германии). Рекламу этой программы очень часто можно встретить в Google ads, и мои глаза уже ребят от этой рекламы.

В трийлной версии нам дозволено тестировать только сайты testphp.acunetix.com, testasp.acunetix.com и testaspnet.acunetix.com. Эти сайты созданы компанией спецально для тестирования программы, но не факт, что на других серверах данный сканер безопасности покажет такие же результаты сканирования и найдет хотя бы половину ошибок. Алгоритм поиска мне не известен, а разработчик его не афиширует. В связи с этим, реально проверить качество тестирования невозможно, ведь покупать полную версию ради теста я не могу по финансовым соображениям, а крека для текущей версии в инете я не нашел. Ну хорошо, будем отталкиваться от того, что есть и доступно нам.



Главное окно программы Acunetix Web Vulnerability Scanner

Vulnerability Scanner позволяет искать ошибки в сценариях на языках PHP, ASP и ASP.NET. Помимо этого, программа может проверять на ошибки JavaScript сценарии, что можно отнести к преимуществам. Можно тестировать не только через прямой коннект, но и HTTP или SOCKS прокси сервер, что будет очень удобно хакерам для обеспечения анонимности.

Итак, что мы видим в результате:

- багатые, но не подтвержденные боевыми тестами возможности;

- красивый и удобный интерфейс;

- поиск уязвимостей XSS, SQL-Injection, PHP инклудинг, поиск хакерских запросов по базе google, обход каталога, CRLF Injection, общедоступные резервные копии сценариев.

- хорошая служба поддержки, которая всегда отвечает, но не всегда вовремя. На мои вопросы разработчики ответили через три дня (правда два из них были выходными).

И все это за высокую цену и не возможно проверить программу на собственном сервере в реальных условиях. Отдавать 350 баксов за софт, который по какой-то причине может не найти у тебя ошибок – сверх глупо. Я пытался получить халявный код у разработчиков, но не смотря на то, что я предствился журналистом и мог бы сказать много приятных слов о программе, если она реально оказалась бы таковой, халявный серийник мне зажали. Я понимаю разработчиков, ведь в интернете журналистом может представиться кто-угодно, и все же....

**Что выбрать?**

Когда сайт состоит из одного файла сценария и получает немного параметров, проверить все руками достаточно просто. А если у тебя целый портал, который состоит из сотен сценариев? Тут уже на полноценные ручные тесты может уйти больше времени, чем на кодинг. Делать беглый тест не имеет смысла, потому что велика вероятность что-то упустить, и тогда взлом будет не загорами. Поэтому для облегчения жизни стали появляться программы, автоматизирующие этот процесс.

Может ли программа решить нашу проблему? Решить та может, а вот гарантировать результат – нет. Алгоритмы поиска в разных программах не идеальны и зависят от множества факторов. Какая-та мелочь может повлиять на результат и прога не найдет уязвимости, а вот хакер ручками быстро найдет ошибку.Так что же тогда делать? В случае со средствами безопасности, особенно тестами я всегда рекомендовал использовать несколько разных программ. Если одна не найдет ошибку, то может быть другая увидит что-то интересное. Каждая программа использует свой алгоритм, который может быть эффективным в той ли иной ситуации.

Тут в голову приходит одна великая мысль, которую уже давно сказал кто-то из спецов по безопасности. Не помню точно кто сказал и как точно звучит, но смысл следующий:

- Если вы звоните человеку по телефону и никто не берет трубку – это не значит, что никого нет дома, может быть телефон не работает или его не слышат. Но если вы придете и постучите в дверь вам откроют;

- Если вы стучите в дверь и вам не открывают, может быть хозяин не слышит из-за громких звуков внутри квартиры или просто находяться в кабинете с надписью М или Ж и не может прервать процесс чтения книги или журнала ][, но если позвонить по телефону, то вам могут ответить благодаря лежащей рядом с хозяином трубки.

Смысл в том, что в зависимости от ситуации положительный результат может дать тот или иной способ, и чтобы быть более менее уверенным, нужно использовать оба. А лучше даже три или четыре программы.

Но даже при использовании автоматического тестирования, ручной способ исключать нельзя. При регулярной проверке автоматом, достаточно хотя бы раз в неделю просматривать основные места ручками, а лучше все. Солидные компании для этих целей нанимают хакеров, чтобы они тестировали их сервера на предмет безопасности. Мелкие компании и индивидуальные владельцы сайтов не могут себе позволить такого счастья, поэтому приходиться ограничиваться автоматическими тестами специализированных программ.