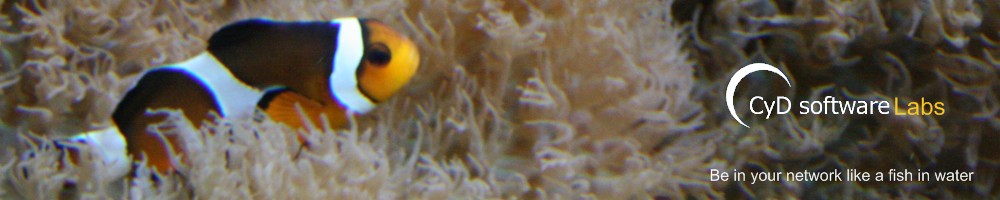
[](http://russia.cydsoft.com/)

Автоматизация поиска уязвимостей на WEB сайте

Автоматизация поиска уязвимостей достаточно сложная задача, особенно, если пытаться создать универсальный метод поиска уязвимостей, потому что необходимо научить компьютер хакерству, и написать программу так, чтобы она программно взламывала сайт. Компьютер - не человек и ему очень сложно анализировать не структурированные данные, а WEB страницы можно считать не структурированными. Да, есть стандарты, которым должны подчиняться разработчики при создании WEB страниц, но как много программистов придерживаются этим стандартам? Существует множество технологий создания сайтов и WEB мастера и программисты могут использовать любые инструменты. Чтобы анализировать результат для поиска уязвимостей в WEB сценариях, нужны широкие знания и опыт.

Что предлагают в интернете чаще всего для поиска уязвимостей? Большинство алгоритмов сводиться к простому поиску сигнатур на WEB странице. В данном случае, сигнатурами являются сообщения о некорректных параметрах и ошибки обращения к базе данных. А что если программист отключил отображение ошибок? Хороший программист обязан это делать и если сайт создавал профессионал, то я вас уверяю, он отключил все сообщения об ошибках и поиск уязвимостей на таком WEB сайте по сигнатурам становиться пустой тратой трафика. Алгоритм и программа не найдет ни единой уязвимости.

А что если на сайте просто есть текст «ошибка доступа», а статья на странице просто описывает работу с базой данных? Автоматический анализатор поиска по сигнатурам выдаст предупреждение там, где уязвимости нет!!! Слишком большое количество различных сообщений об ошибках, которые могут стать сигнатурами приведет к большому количеству ложных срабатываний, а отсутствие возможности найти сигнатуру при выключенных сообщениях об ошибках, сделают алгоритм почти бесполезным. Поиск уязвимостей WEB сайтов - это не антивирусная программа и тут нельзя использовать те же методы.

Что же тогда делать? Как создать автоматический поиск уязвимостей WEB сайта, который будет находить даже скрытые ошибки? Алгоритмы поиска таких ошибок есть и они достаточно просты и эффективны, но для их написания уже не достаточно банального поиска по сигнатурам. Тут уже приходиться создавать программный комплекс, обладающий задатками искусственного интеллекта. Этот метод более сложный в реализации, но дает более точные результаты и находит ошибки там, где сообщения об ошибках отключены программистом.

Чтобы найти скрытые ошибки, программа должна пытаться самостоятельно взломать сайт и анализировать результат не в поисках сигнатур, а в поисках признаков взлома. Именно поэтому и говорят, что приходится наделять программу задатками искусственного интеллекта, особенно, если программа универсальная и не направлена на поиск узкого круга ошибок на определенного типа сайтах, построенных по определенному принципу.

Да, и тут тоже возможны ложные срабатывания, особенно там, где WEB страницы подвержены сильной мутацией. Да, и тут тоже не всегда возможно найти ошибку, даже если она есть, и опять же главным врагом выступает мутация страницы. Но мы верим и наши тесты доказали, что такой наш новый алгоритм, который пытается программно взломать сайт выгоднее и точнее поиска по сигнатурам.CyD Network Utilities 2008 искала уязвимости по сигнатурам и не смотря на то, что результат был хорошим, он пропускал много ошибок незамеченными. Новая версия [CyD Network Utilities 2008 (Сетевые утилиты)](http://www.cydsoft.com/products.php?lang=2&product=19) использует аналитический анализатор. Он тратит больше трафика и работает дольше, но позволяет найти скрытые уязвимости. А одна пропущенная уязвимость может стоить WEB сайту своим существованием. Если хакер найдет уязвимость и она окажется серьезной, то сайт может быть уничтожен.

Программный взлом сайта сложнее в реализации и требует больше времени на анализ уязвимостей и больше трафика, но зато дает более точный результат.

**Модуль поиска уязвимостей в CyD Network Utilities**

Поиск уязвимостей нужен не только взломщикам, чтобы проникнуть на сайт, но и администраторам или программистам для поиска слабых мест в WEB сценариях. Мы надеемся, что модуль поиска уязвимостей нашей программы будет использоватся администраторами и программисты в благих намерениях, а не взломщиками.

Модуль Security test (автоматического тестирования безопасности WEB сайта) — это новая возможность программы CyD NET Utils 5.0 [Network Utilities Сеть и безопасность](http://russia.cydsoft.com/products.php?product=19) 2009. Вы можете тестировать ваш WEB сервер на наличие следующих уязвимостей:

http://russia.cydsoft.com/images/str2.gif[SQL Injection или инъекция SQL](http://www.cydsoft.com/down.php?cat=4&icat=7)

http://russia.cydsoft.com/images/str2.gif[XSS (Cross Site Scripting)](http://www.cydsoft.com/down.php?cat=4&icat=8)

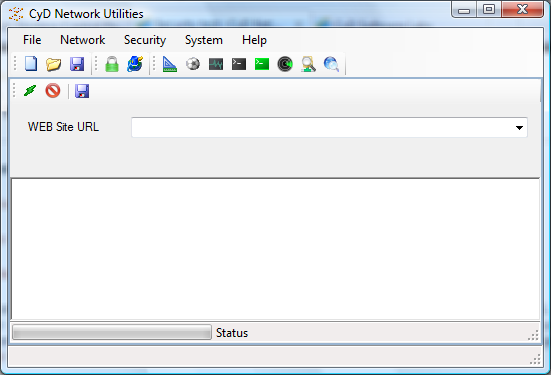
[[http://russia.cydsoft.com/images/str2.gif](http://www.cydsoft.com/down.php?cat=4&icat=9)PHP includes](http://www.cydsoft.com/down.php?cat=4&icat=9)

Наиболее распространенная атака на базы данных — это инъекция **SQL Injection**. Атака реализуется за счет внедрения кода злоумышленника в SQL запрос через параметры, например, поля URL адреса. Переданный код внедряется в запрос для выполнения на сервере баз данных Возможность выполнять запросы SQL на сервере баз данных может дать хакеру возможность уничтожить данные в базе или даже на WEB сервере. Для получения дополнительной информации по данной уязвимости, можно прочитать статью [SQL Injection and PHP](http://www.cydsoft.com/down.php?cat=4&icat=7) на нашем сайте.

Разработка Web приложений в наше время далеко не всегда требует знания безопасности и даже программирования. Современные средства позволяют с помощью мышки создать WEB сайт и опубликовать его в интернете. Очень часто, такие конструкторы становятся мишенью для атак хакеров. Используя автоматического тестирования безопасности в программе CyD NET Utils позволяет уменьшить вероятность нахождения ошибок в ваших приложениях или приложениях, собранных с помощью конструкторов сайтов. Используйте автоматический тест после каждого внесения изменений в программах на сайте.

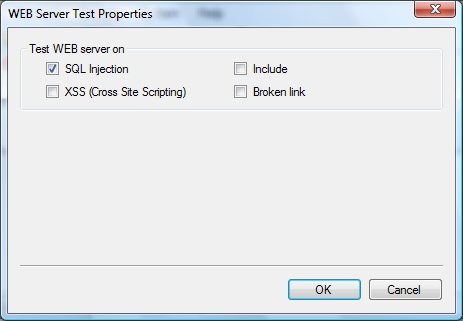
**Использование программы для тестирования**

Для запуска модуля тестирования безопасности выберите пункт меню **Test WEB server security** из меню **Security** или нажмите кнопку кнопка тестирования безопасности. Программа запустит модуль тестирования, котрый вы можете увидеть на следующем рисунке:



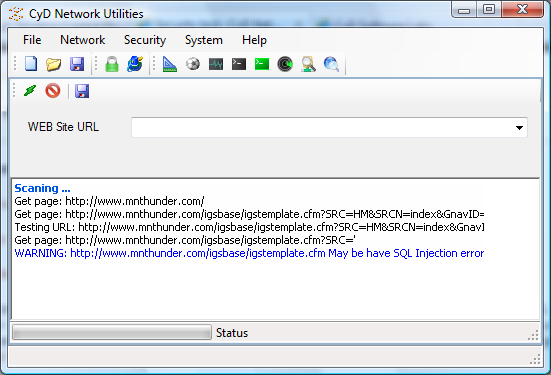
Введите URL адрес WEB сервера в поле **WEB site URL** . Например, адрес сайта может выглядеть следующим образом: http://www.servername.com/index.php

Нажмите кнопку http://www.cydsoft.com/product/network_utils/start.png**Test WEB Servers** для начала теста. Программа отобразит окно параметров теста безопасности, как показано на следующем рисунке:



В этом окне вы можете выбрать ошибки, которые нужно искать на WEB сайте. Чем больше вариантов ошибок вы выберите, тем дольше будет проходить тест. Для выбора доступны: SQL Injection (инъекция SQL), XSS (Cross Site Scripting), Include и Broken links (битые ссылки). Больше всего времени и трафика занимает тест инъекции (**SQL Injection**).

Нажмите OK чтобы начать тест. Пример результата тестирования можно увидеть на следующем рисунке:



Что означает следующее сообщение в окне результата?:

**WARNING: http://www.mnthunder.com/igsbase/igstemplate.cfm May be have SQL Injection error in param:SRC**

Оно говорит нам, что скрипт http://www.mnthunder.com/igsbase/igstemplate.cfm может содержать ошибку SQL Injection в параметре SRC. Свяжитесь с разработчика скрипта, чтобы убедиться, что ошибки там нет или чтобы исправить ошибку.