[spec@baza w3af]$ echo «w3Af – система с открытым исходным кодом для проведения аудита безопасности веб-приложений»

Первый слайд

W3AF – система с открытым исходным кодом для проведения аудита безопасности веб-приложений

Тарас Иващенко
Специалист отдела общего аудита
Департамента Аудита,
Компания «Информзащита»
OSCP

Существующие решения

- Проприаритарное ПО (IBM Rational WebScan, Xspider)
  - Высокая цена
  - Как правило, плохая расширяемость
  - Нет сообщества пользователей
  - Красивые отчёты
- Свободное ПО (Nikto, WebScarab, SQLmap)
  - Множество небольших утилит для отдельных задач
  - Изобретаем велосипед вновь и вновь (Xcobra)
  - Плохая архитектура и расширяемость
  - Не всегда красивые отчёты

Что такое W3AF?

- Программное окружение для аудита безопасности веб-приложений с возможностью эксплуатации найденных уязвимостей
- Лицензия - GNU General Public License Version 2
- Текущая версия – 1.0 Release Candidate 1
- Уже достаточно большой международный проект со своим сообществом
- Автор и основатель проекта - Andrés Riancho (Аргентина)

Основные особенности

- Написано на Python – интерпетируемом языке “с батарейками”
- Кроссплатформенность
- Несколько пользовательских интерфейсов
  - GUI с использованием GTK
  - Консольный с удобным автодополнением
- Возможность расширения: 134 расширения и их число постоянно растёт
- Поддержка веб-сервисов
- Возможность эксплуатации найденных уязвимостей

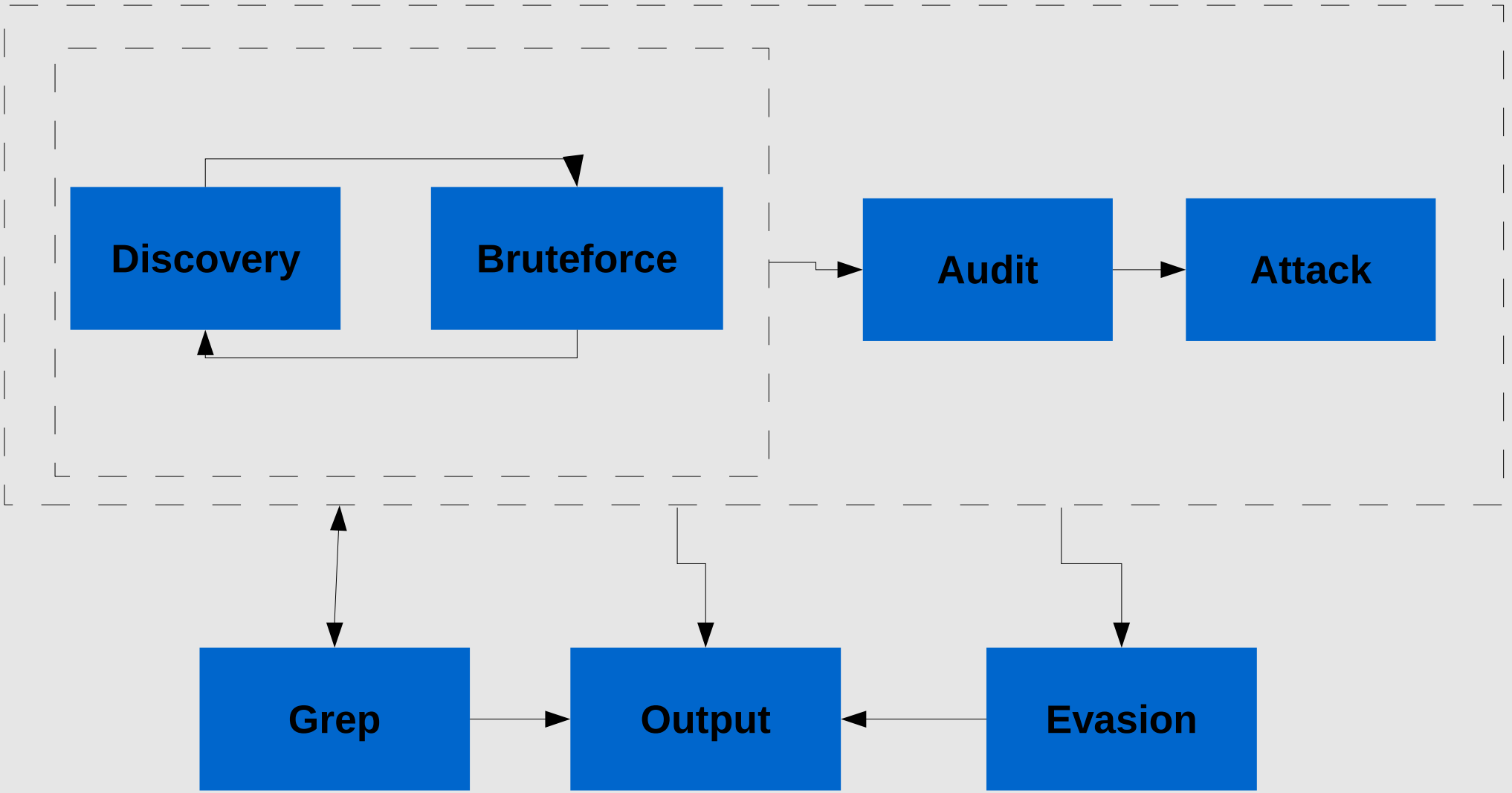
Основные особенности - 2

- Ищет уязвимости везде: GET/POST запросы, HTTP-заголовки, содержание файлов
- “Умный” поиск уязвимостей: например, когда входные данные отображаются при определённых условиях
- Интегрированы существующие инструмены и их аналоги: sqlmap, pykto

Архитектура

- w3af в общем состоит из 2 главных частей: ядро и расширения.
- Ядро координирует процессы и предоставляет определённый функционал расширениям.
- Расширения обмениваются информацией друг с другом через “хранилище знаний”.
- По возможности используются шаблоны проектирования.

Потоки информации



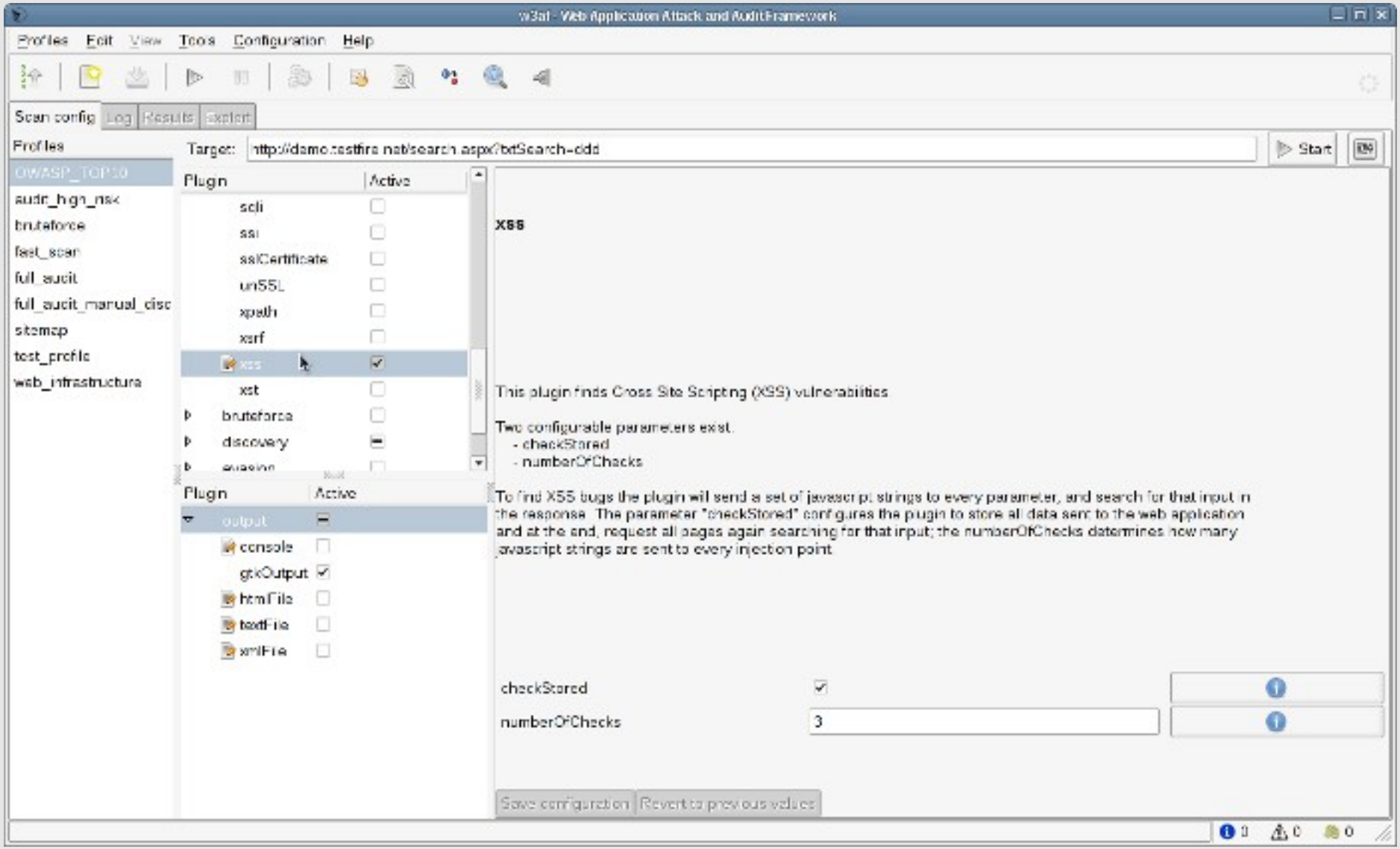
Расширения

- **discovery** - поиск новых целей(например, URL) и создания т.н. изменяемых запросов.
- **audit** - поиск в найденных целях уязвимостей.
- **grep** - фильтруют каждый HTTP-запрос и ответ на предмет вхождения определённой информации
- **attack** - эксплуатация найденных уязвимостей
- **output** - расширения вывода информации (текстовый файл, консоль или HTML-файл).
- **mangle** - вносят изменения в HTTP-запросы и ответы в соответствии с регулярными выражениями

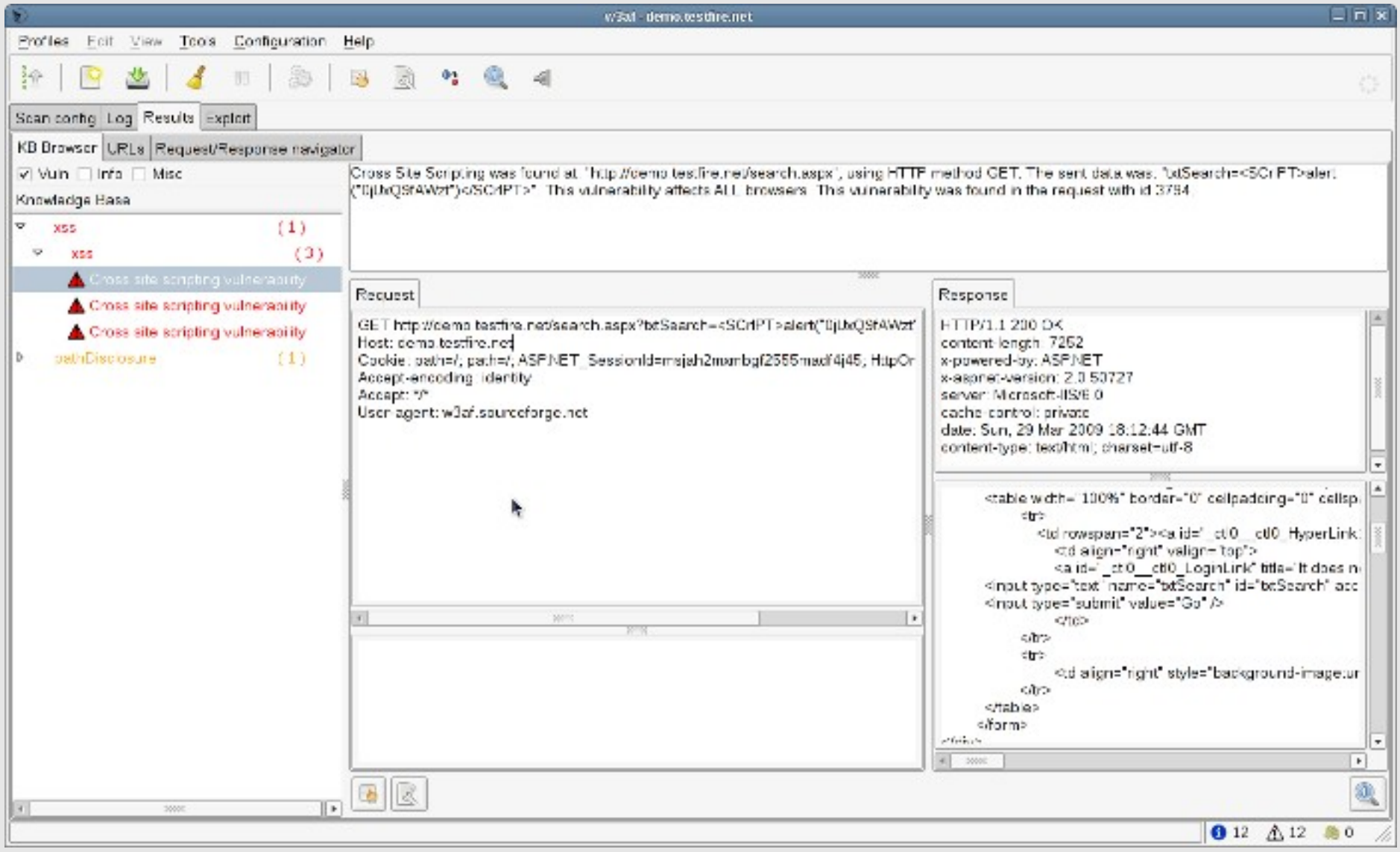
Расширения

- **evasion** - изменяют HTTP-запросы для обхода систем обнаружения вторжений.
- **bruteforce** - перебор имен пользователей.

Все любят скриншоты и демо!



W3AF GUI


w3af - demo.testfire.net
Profiles Edit View Tools Configuration Help
Scan config Log Results exploit
KB Browser URLs Request/Response navigator
Vuln Info Misc
Knowledge Base
xss (1)
xss (3)
Cross site scripting vulnerability
Cross site scripting vulnerability
Cross site scripting vulnerability
pathDisclosure (1)
Cross Site Scripting was found at: "http://demo.testfire.net/search.aspx", using HTTP method GET. The sent data was: "txtSearch=<SCRIPT>alert("DjUbQSfAWzf")</SCRIPT>". This vulnerability affects ALL browsers. This vulnerability was found in the request with id 3754.
Request
GET http://demo.testfire.net/search.aspx?txtSearch=<SCRIPT>alert("DjUbQSfAWzf
Host: demo.testfire.net
Cookie: path=/; path=/; ASP.NET_SessionId=msjah2marbgf2555madf4j45; HttpOn
Accept-encoding: identity
Accept: */*
User-agent: w3af.sourceforge.net
Response
HTTP/1.1 200 OK
content-length: 7262
x-powered-by: ASP.NET
x-aspnet-version: 2.0.50727
server: Microsoft-IIS/6.0
cache-control: private
date: Sun, 29 Mar 2009 18:12:44 GMT
content-type: text/html; charset=utf-8
<table width="100%" border="0" cellpadding="0" cellsp
<td rowspan="2"><a id="_ctl0__ctl0_HyperLink
<td align="right" valign="top">
<a id="_ctl0__ctl0_LoginLink" title="It does n
<input type="text" name="txtSearch" id="txtSearch" acc
<input type="submit" value="Go" />
</td>
</tr>
<tr>
<td align="right" style="background-image:ur
</tr>
</table>
</form>
12 12 0

Получение удалённого доступа через SQL-инъекцию - демонстрация

Ссылки

- W3AF – http://w3af.sourceforge.net/
- Обзорный список сканнеров веб-уязвимостей - http://sectools.org/web-scanners.html
- IBM Rational AppScan – http://www-01.ibm.com/software/awdtools/appscan/
- Nikto – http://www.cirt.net/code/nikto.shtml
- WebScarab - http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project
- WebScarab – http://www.acunetix.com/
- XSpider - http://www.ptsecurity.com/

Вопросы?

- Электронная почта
  - t.ivashchenko@infosec.ru
  - taras@securityaudit.ru
- Веб-сайт:
  - www.infosec.ru
  - www.securityaudit.ru
- ПО, использованное для подготовки презентации:
  - открытый офисный пакет OpenOffice.org
  - Fedora - дистрибутив свободной операционной системы Linux