

`[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

- Проприетарное 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 – интерпретируемом 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

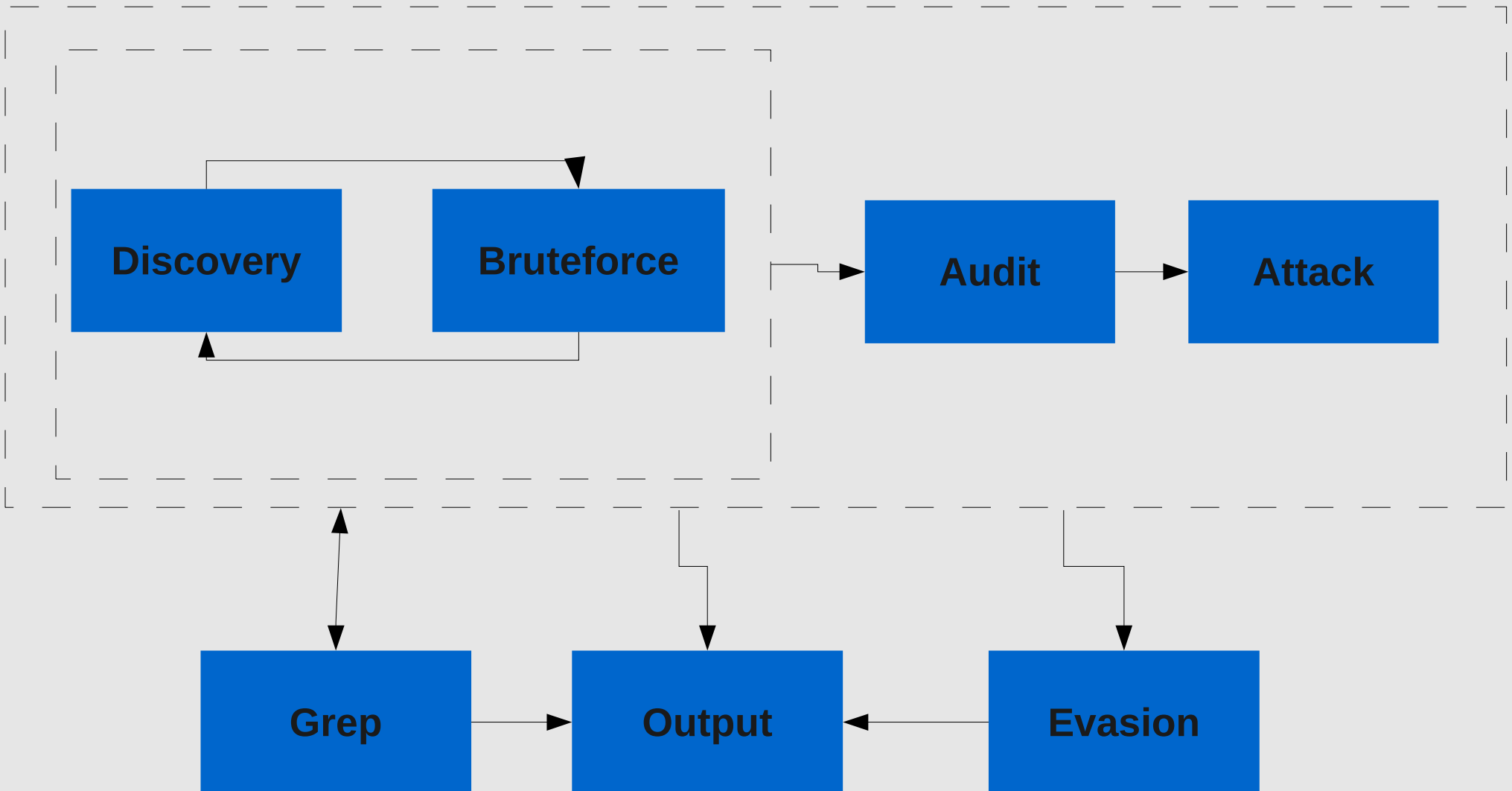
# Основные особенности - 2

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

# 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



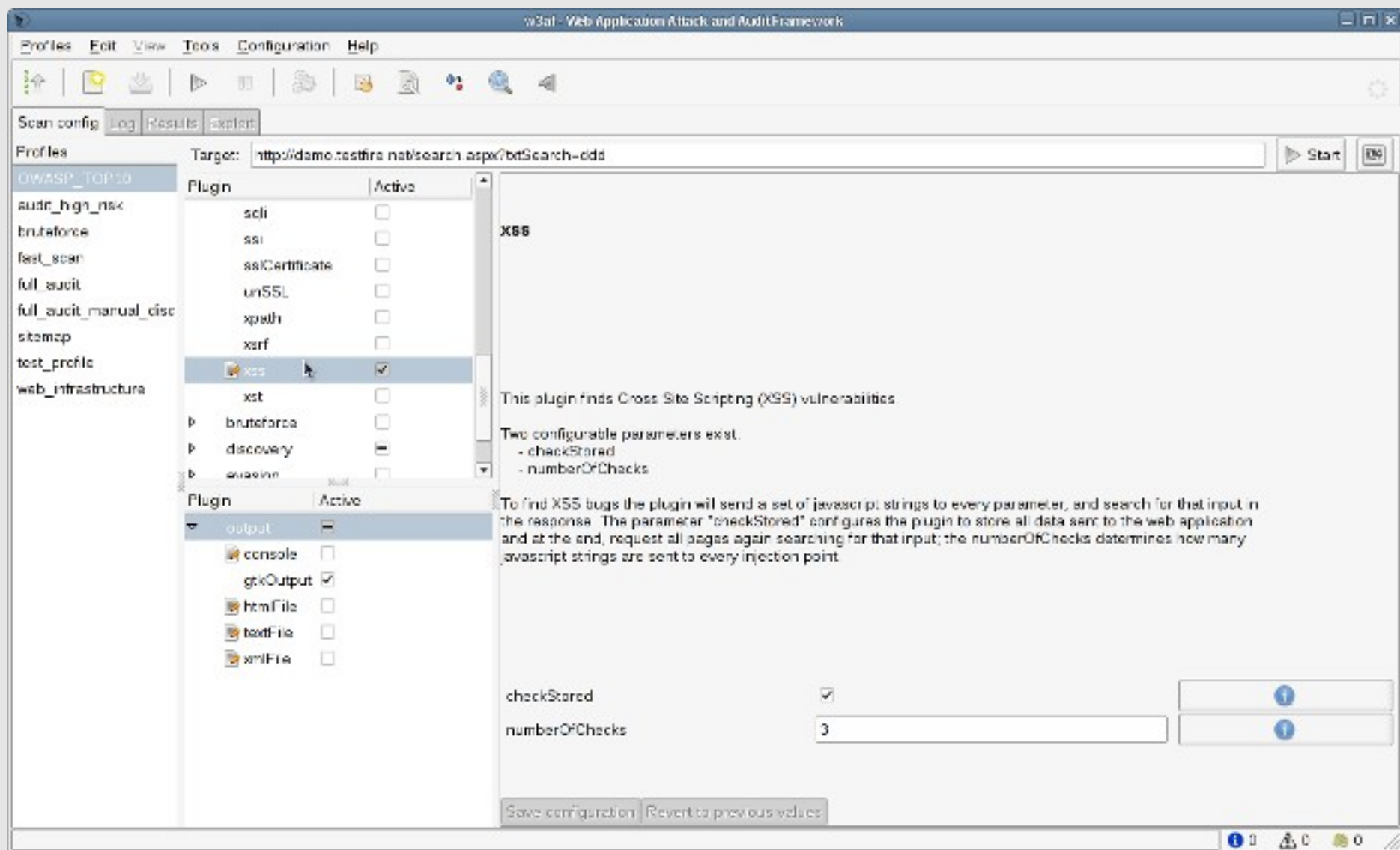
# Расширения

- **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

The screenshot displays the W3AF (Web3 Attack Framework) GUI interface. The main window title is "w3af - demo.testfire.net". The interface includes a menu bar (Profiles, Edit, View, Tools, Configuration, Help) and a toolbar with various icons. Below the toolbar, there are tabs for "Scan config", "Log", "Results", and "exploit".

The "Results" tab is active, showing a list of vulnerabilities in the "Knowledge Base" on the left. The "xss" category is expanded, showing three instances of "Cross site scripting vulnerability" and one instance of "pathDisclosure".

The main content area displays a detailed scan result for a Cross Site Scripting (XSS) vulnerability. The text reads: "Cross Site Scripting was found at 'http://demo.testfire.net/search.aspx', using HTTP method GET. The sent data was: 'btSearch=<SCRIPT>alert('0jUkQ9fAWzr')</SCRIPT>'. This vulnerability affects ALL browsers. This vulnerability was found in the request with id 3784."

Below this message, there are two panels: "Request" and "Response".

The "Request" panel shows the following details:

```
GET http://demo.testfire.net/search.aspx?btSearch=<SCRIPT>alert('0jUkQ9fAWzr')
Host: demo.testfire.net
Cookie: path=/, path=/, ASPNET_SessionId=msjsh2mxnbgf2555-madf4j45, HttpO
Accept-encoding: identity
Accept: */*
User-agent: w3af.sourceforge.net
```

The "Response" panel shows the following details:

```
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
```

The response body contains HTML code, including a table and a form with a search input field and a "Go" button.

The bottom status bar shows system icons and the number of items in the results list: 12 items, 12 warnings, and 0 errors.

# **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](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)
- WebScarab – <http://www.acunetix.com/>
- XSpider - <http://www.ptsecurity.com/>

**Вопросы?**