Web Application Security Consortium
Перспективы развития

Сергей Гордейчик

Positive Technologies

Что такое WASC?

Web Application Security Consortium (WASC)

Международная некоммерческая организация, объединяющая экспертов-профессионалов в области безопасности веб-приложений.

Миссия: Разрабатывать, адаптировать и пропагандировать стандарты в области безопасности веб-приложений

Web-сайт
http://www.webappsec.org/
Wiki
http://projects.webappsec.org/
Список рассылки
websecurity-subscribe@webappsec.org

WASC в лицах

Персоналии

…/Robert Auger/Jeremiah Grossman/Romain Gaucher/Amit Klein/Steve Orrin/Bill Pennington/Ivan Ristic/Ory Segal/Ofer Shezaf/Caleb Sima/…

Компании

…/PayPal/WhiteHat Security/Breach Security/Finjan/NT OBJECTives, Inc./Positive Technologies/Application Security, Inc./Intel/Thinking Stone (ModSecurity)/IBM/SPI Dynamics/HP/KPMG/Microsoft/…

Структура WASC

Роли и задачи

- **Officers**
  - Общая координация, развитие и инициация новых проектов
- **Project leaders**
  - Управление и координация проектов
- **Project teams**
  - Собственно работа

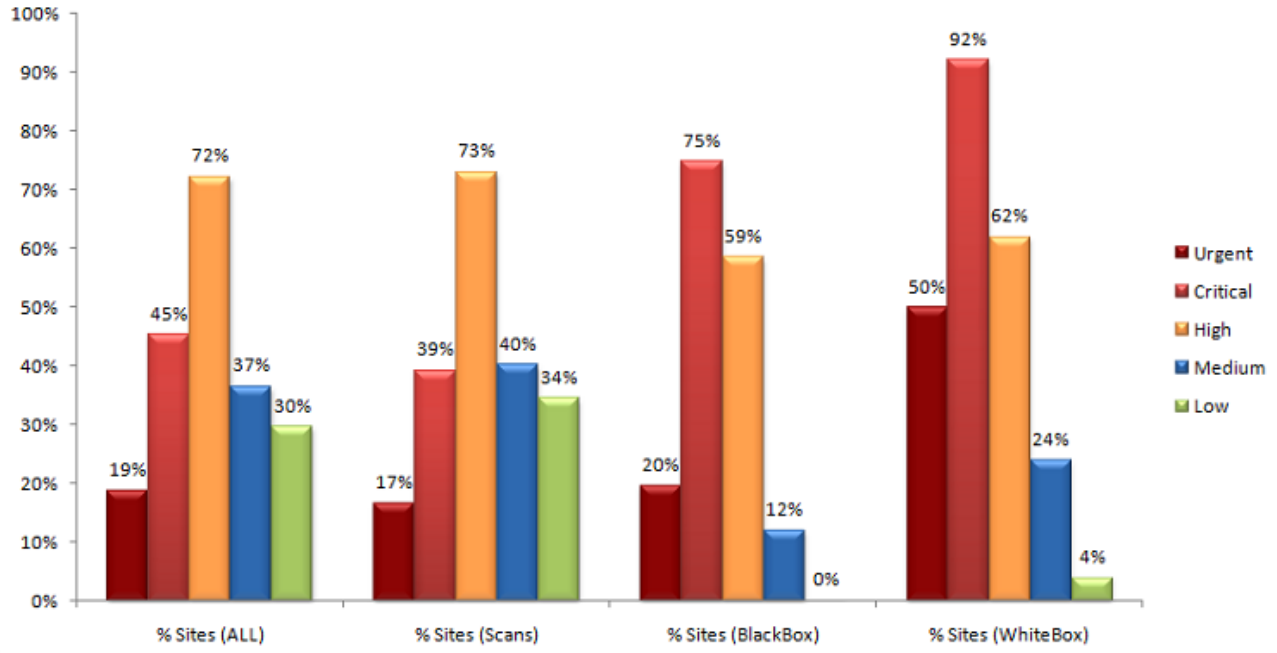
Текущие проекты

- **Классификация**
  - The WASC Threat Classification
  - The Web Security Glossary
- **Анализ рисков/метрики**
  - Web Application Security Statistics
  - The Web Hacking Incident Database
- **Оценка средств защиты (РД)**
  - The Web Application Security Scanner Evaluation Criteria (WASSEC)
  - The Web Application Firewall Evaluation Criteria (WAFEC)
- **Исследования**
  - Script Mapping
  - Distributed Open Proxy Honeypots

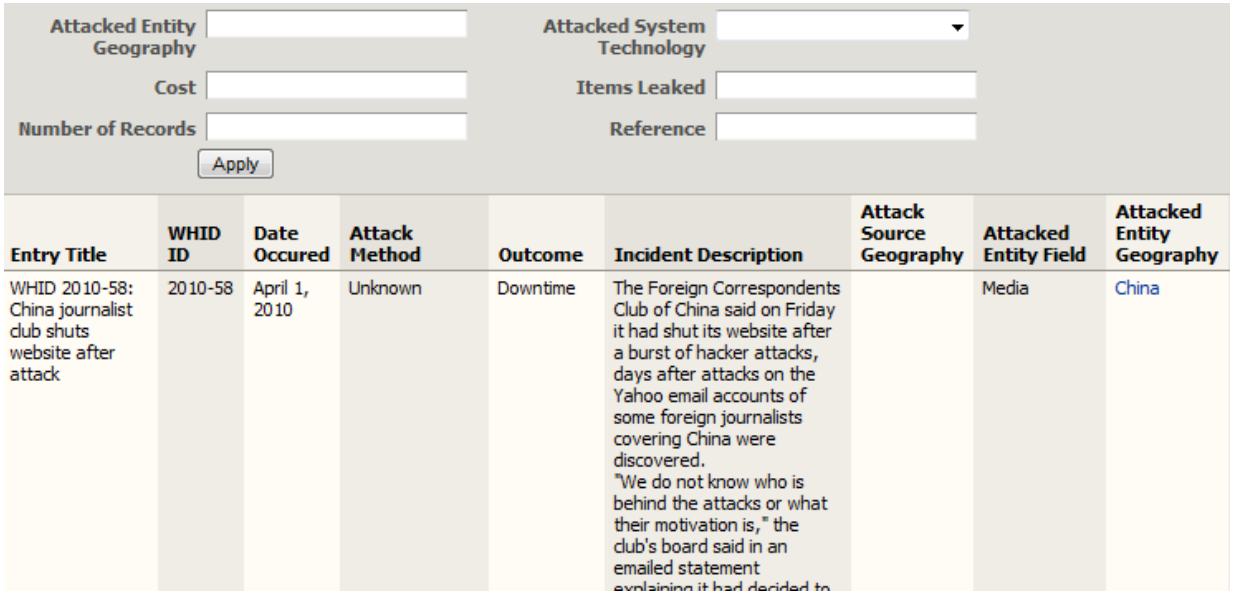
The WASC Threat Classification

- **Классификация атак и уязвимостей веб-приложений**
- **Наиболее полная на настоящий момент классификация**
- **Различные группировки уязвимостей**
- **Связь с другими стандартами (OWASP/CWE)**
- **Более 3 лет разработки второй версии**

Анализ результатов работ в области оценки защищенности веб (черный ящик, белый ящик, сканирования)



- **Сбор и обработка публичных последствий инцидентов (СМИ, расследование уголовных дел, интернет)**
- **Классификация, учет последствий**



Attacked Entity Geography | Attacked System Technology
Cost | Items Leaked
Number of Records | Reference
Apply

Entry Title	WHID ID	Date Occured	Attack Method	Outcome	Incident Description	Attack Source Geography	Attacked Entity Field	Attacked Entity Geography
WHID 2010-58: China journalist club shuts website after attack	2010-58	April 1, 2010	Unknown	Downtime	The Foreign Correspondents Club of China said on Friday it had shut its website after a burst of hacker attacks, days after attacks on the Yahoo email accounts of some foreign journalists covering China were discovered. "We do not know who is behind the attacks or what their motivation is," the club's board said in an emailed statement explaining it had decided to		Media	China

Distributed Open Proxy Honeypots

- **Сеть открытых HTTP-прокси (с некоторыми ограничениями)**
- **Анализ поведения злоумышленников**
- **Отслеживание бот-сетей (веб-спам)**

Использование WASC 1/2

WASC WATC

- IBM (AppScan)
- HP (Webinspect)
- WhiteHat Security (Sentinel)
- Positive Technologies (MaxPatrol) and Services
- Qualys (QualysGuard Web Application Scanning)
- F5 (Application Security Manager)
- HoneyApps (Conduit)
- OWASP (OWASP Code Crawler 2.5 and OWASP ModSecurity Core Rule Set Project)
- Verizon (Verizon Incidents Metrics Framework)

WASC SS/WHID

- Анализ рисков
- Пугающие presale-презентации

Использование WASC 2/2

- **WASSEC/WAFEC**
  - **Критерии оценки средств защиты**
  - **Требования/технические задания к системам**
  - **NSS Lab**
  - **Positive Technologies**

Ближайшие задачи

- **Добавление/расширение контрмер в классификации угроз**
- **Актуализация угроз**
- **Объединение проектов, связанных с анализом рисков**
- **Развитие WHID (поиск участников)**
- **Разработка «метапроекта» - WASC User Guide**

Присоединяйтесь!

Сергей Гордейчик

gordey@ptsecurity.ru

http://sgordey.blogspot.com

POSITIVE TECHNOLOGIES