HIGH-TECH BRIDGE®

INFORMATION SECURITY SOLUTIONS

Why does web security testing fail globally? Problems and suggested solution.

Ilia Kolochenko, High-Tech Bridge, CEO

SC Congress London

20th of March 2014

From where does the claim come?

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

- zone-h.org defacement archive contains **9'500'000 mirrors of hacked websites**, significant part of which are well-known, **govermantal**, **law-enforcement** and even security companies' websites**.**
- **4/5 websites are vulnerable** – *Frost & Sullivan* (2013).
- **86% of all websites have at least one serious vulnerability** – *WhiteHat Security* (2013).
- **96% of tested applications have vulnerabilities** – *Cenzic* (2014).
- High-Tech Bridge non-profit Security Research Lab issues **at least one new** Security Advisory **every week** for a web application used on **approx. 10'000 live websites.**

Who are the victims of web hacking?

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

- Financial Organizations and Banks
- Governments and Governmental Organizations
- NGOs and Educational Organizations
- Large and Multi-National Companies
- Small and Medium Business
- Private Persons

Why all these websites are being hacked?

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

- **Massive/Non-Targeted Attacks (mainly against SMBs):**

- **Economical gain** (e.g. resell access to your website on Black market to spread malware, send spam or just to sell your website/database with hundreds of others as a "package").
- **Hacktivism** (e.g. if your website directly or indirectly belongs to a specific country, industry or political party – you may be hacked just because you are the easiest or most visible target).

- **Targeted Attacks (mainly against large companies and .gov's):**

- **Economical gain** (high-profile industrial espionage paid by competition, organized crime or government).
- **Hacktivism** (massive and/or high-profile attacks by politically motivated hackers).

What are the main solutions to test website security?

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

- **Automated Software (e.g. Vulnerability Scanners)**

Rapid, affordable for SMBs, however require a technical expert to analyze the report and implement security fixes. Automated software also miss vulnerabilities (*false-negatives*) and erroneously report non-existing vulnerabilities (*false-positives*).

- **Software-as-a-Service Automated Assessments**

Rapid, affordable for SMBs, easy to launch and use, however also suffer from false-positives and false-negative mistakes in the reports, therefore require a technical expert to analyze and re-verify the report.

- **Manual Penetration Testing (Ethical Hacking)**

Tailor-made security assessment performed by highly-competent security auditors with comprehensive and easy-to-use reports both for IT departments and senior management. Highly expensive and administratively (e.g. NDA) long projects.

- **General Difficulties:**

- Big variety of inappropriate/inefficient web security products, solutions and services distributed by incompetent IT resellers.
- Reactive rather than proactive approach to security (many people start thinking about security only after being hacked).
- Rarely performed independent security testing.

- **Difficulties of Small & Medium Business:**

- Lack of budget, time and human resources to manage security.

- **Difficulties of Large Companies:**

- Bureaucracy, complex hierarchy and subordination. Nobody is and nobody wants to be responsible for security.
- Regular cost-cutting, focus on performance, compatibility, mobility and design rather than on security.

Results?

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

While low-cost automated solutions compete with expensive manual services…

- **Small and Medium Business:**

- Hesitate to spend money they can afford on automated solutions due to high later expenses and need for additional human expertise.
- Cannot afford manual penetration testing.
- Remain vulnerable. Get hacked. Panic.

- **Large Companies and Organizations:**

- Spend their budgets inefficiently on inappropriate solutions. Not seeing ROI from web security testing they stop or suspend independent security auditing projects that are not required by law.
- React when it is already too late, spend [waste] even more money to investigate the incident, calm shareholders, management and public.
- Remain vulnerable. Get hacked. Panic.

- What if we **join the strengths of automated security testing** solutions with **efficiency of manual testing** and offer it at **affordable price via a user-friendly web portal**?

- This is how the idea of ImmuniWeb® was born in 2010. We called it **hybrid web security testing** – a perfect mix of machine and human that infallibly identifies the most complex security vulnerabilities and weaknesses.

- ImmuniWeb® **aims to solve problems both of SMBs and large companies**. For the first ones ImmuniWeb® is a **complete security solution**. For the second ones ImmuniWeb® is a **perfect decision-making tool** before spending their budgets or approving information security strategy.

ImmuniWeb® SaaS in details

HIGH-TECH BRIDGE®
INFORMATION SECURITY SOLUTIONS

- ImmuniWeb® SaaS is a hybrid of **accurate manual web application penetration test and cutting-edge vulnerability scanning** that are **performed in parallel**.

- ImmuniWeb® SaaS consists of 3 interconnected components:

- **ImmuniWeb® Portal** - user-friendly web interface used to manage the security assessment process from configuration to report delivery. Can be used from PC/Mac/Mobile device.
- **ImmuniWeb® Auditors** - a team of High-Tech Bridge web security experts that manually discover, test and exploit vulnerabilities, as well as suggest customized solutions.
- **ImmuniWeb® Security Scanner** - a proprietary web vulnerability scanner developed and supported by High-Tech Bridge.

HIGH-TECH BRIDGE
INFORMATION SECURITY SOLUTIONS

ImmuniWeb®

security becomes simple

CVE COMPATIBLE
cve.mitre.org

CWE COMPATIBLE

CVSS

www.ImmuniWeb.com

ISO 27001 SYSTEM CERTIFICATION SGS