Проблемы безопасности открытых веб приложений

Евгений Докукин aka MustLive
http://websecurity.com.ua

1. Развитие Интернет.

Сеть Интернет стремительно развивается и с каждым годом количество сайтов увеличивается на миллионы (а в последние годы на сотни миллионов).

По данным последнего исследования Netcraft [1]:

В Августе 1995 было 19 732 доменов.
В Августе 2000 было 19 798 570 доменов.
В Сентябре 2012 было 620 132 319 доменов.

Статистика веб сайтов в Интернете по годам (Рис. 1):

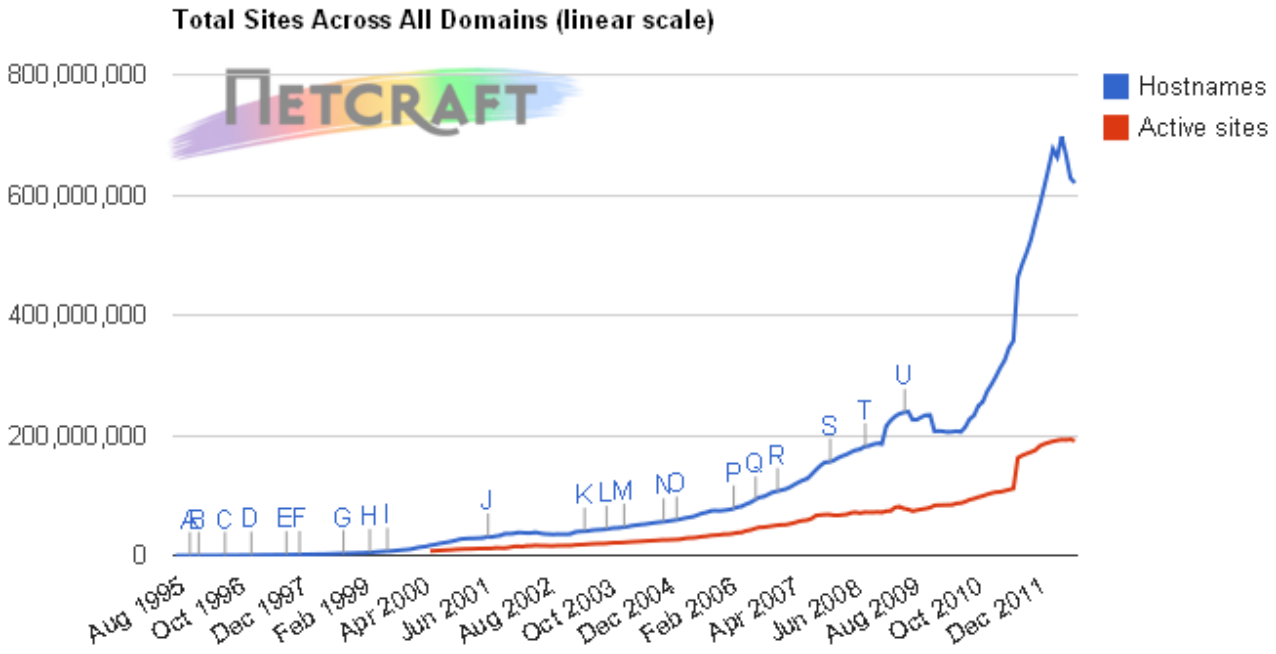

Рис. 1 – Статистика веб сайтов в Интернете

2. Распространённость открытых веб приложений.

Вместе с ростом веб сайтов, растёт и число веб приложений. В наше время большинство веб сайтов – динамические.

В Интернете наибольшее распространение получили открытые веб приложения (как бесплатные, так и коммерческие). И из года в год их число растёт.

Если в начале девяностых веб приложения только начали появляться – вместе с развитием World Wide Web – то на сегодня по данным Wikipedia [2], только таких веб приложений как CMS насчитывается 173. Это веб приложения на Java, ASP.NET, Perl, PHP, Python, Ruby, CFML и других языках программирования.

Из данных CMS:

- Open source software – 119
- Software as a service (SaaS) – 14
- Proprietary software – 40

При этом часть коммерческих CMS (из категории Proprietary software) также предоставляет исходные коды, т.е. по сути является открытыми веб приложениями. Поэтому таких Content Management System большинство.

И это только CMS, к тому же наиболее известные. А есть ещё малоизвестные CMS (в том числе коммерческие), и множество других веб приложений, в том числе коммерческие продукты, не говоря уже о приватных веб приложениях (custom made).

Поэтому различных веб приложений в Интернете миллионы – от маленьких приложений в виде одного скрипта, до комплексных систем, таких как CMS, форумы, рекламные системы и т.д. И ежегодно их количество стремительно растёт – вместе с ростом Всемирной Сети. При этом имеется рост как открытых (бесплатных и платных), так закрытых веб приложений.

Веб приложения можно разделить на следующие категории:

1. Бесплатные открытые веб приложения.
2. Коммерческие открытые веб приложения.
3. Бесплатные закрытые веб приложения.
4. Коммерческие закрытые веб приложения.

3. Статистика Уанета.

В своём отчёте о хакерской активности в Уанете в первом полугодии 2012 года [3], я опубликовал статистику взломов и DDoS атак, а также инфицирований веб сайтов.

В первом полугодии 2012 года:

- 592 атаки на веб сайты (взломы и DDoS) – в основном опенсорс веб приложения.
- Из них взломано 58 государственных сайтов – в основном опенсорс веб приложения.
- Из них 16 DDoS атак – на сайты использующие различные веб приложения.
- 98 сайтов были инфицированы – в основном опенсорс веб приложения.
- Из них инфицировано 9 государственных сайтов – в основном опенсорс веб приложения.

На данных инфицированных сайтах, по состоянию на 23.09.2012, используются следующие движки [4]. Удалось выявить движки на 41 сайте:

Joomla – 21
WordPress – 7
DataLife Engine – 4
osCommerce – 2
WebAsyst Shop-Script – 2
Danneo CMS – 1
Drupal – 1
Megapolis.Portal Manager – 1
phpWebSite – 1
Serendipity – 1

4. Проблемы безопасности открытых и закрытых веб приложений.

В открытых и закрытых веб приложениях регулярно находят различные уязвимости. Это уязвимости всех классов по Web Application Security Consortium TC v1.0 и v2.0 и OWASP Top 10. В частности в классификации OWASP приводится 10 классов уязвимостей, которые исследователи безопасности наиболее часто находят в открытых веб приложениях.

OWASP Top 10 Web Application Security Risks на 2010 год [5]:

A1: Injection.
A2: Cross-Site Scripting (XSS).
A3: Broken Authentication and Session Management.
A4: Insecure Direct Object References.
A5: Cross-Site Request Forgery (CSRF).
A6: Security Misconfiguration.
A7: Insecure Cryptographic Storage.
A8: Failure to Restrict URL Access.
A9: Insufficient Transport Layer Protection.
A10: Unvalidated Redirects and Forwards.

Рассмотрим статистику уязвимостей в открытых и закрытых веб приложениях за период с 2003 по 2012 годы (это суммарные данные по всем типам программ, но веб приложений большинство из них).

По данным OSVDB [6] за последние десятилетие в их БД было опубликовано уязвимостей:

2003 – 3244
2004 – 4939
2005 – 7786
2006 – 10916
2007 – 9399
2008 – 9513
2009 – 7770
2010 – 8661
2011 – 7344
2012 – 6332

По данным NVD и MITRE [7] за последние десятилетие в БД CVE было опубликовано уязвимостей:

2003 – 1524
2004 – 2436
2005 – 4910
2006 – 6613
2007 – 6521
2008 – 5631
2009 – 5734
2010 – 4641
2011 – 4150
2012 – 4021

При этом компании занимающиеся Информационной Безопасностью отмечают ежегодных рост уязвимостей именно в веб приложениях.

Примеры очень распространённых уязвимостей:

- Уязвимости в популярных движках, таких как WordPress, Joomla и других. Которые касаются десятков миллионов сайтов по всему Интернету.
- XSS уязвимости в 34 миллионах флеш файлах tagcloud.swf [8].
- Content Spoofing и XSS уязвимости в JW Player (7,7 миллиона флешек) [9].

5. Причины сложившейся ситуации.

- Игнорирования проблем безопасности – аудиты и пентесты не проводятся. Нескорые разработчики не в курсе о существовании веб безопасности, а другие в курсе, но им глубоко всё равно.
- Потребительский подход – ожидание, что кто-то должен опенсорс разработчикам бесплатно проводить аудиты безопасности их приложений.
- Распространённость веб приложений.
- Нигилизм – непрофессиональные веб разработчики игнорирующие все нормы безопасности разрабатывают большинство открытых веб приложений.
- Несерьёзность веб разработчиков – многие разработчики игнорируют (не исправляют, плохо исправляют или скрытно исправляют) уязвимости о которых им сообщают исследователи безопасности.

Данные проблемы касаются как веб приложений, так и веб сайтов (в том числе сайтов на открытых веб приложениях).

6. Пути решения сложившейся ситуации.

- Изменение подходов разработчиков.
- Уменьшение несерьёзности и увеличение ответственности разработчиков.
- Просвещение и борьба с нигилизмом.

Просвещение, борьба с нигилизмом и увеличение ответственности касается как разработчиков, так и администраторов сайтов.

7. Ссылки.

1. Netcraft: September 2012 Web Server Survey – http://news.netcraft.com/archives/2012/09/10/september-2012-web-server-survey.html.
2. List of content management systems – http://en.wikipedia.org/wiki/List_of_content_management_systems.
3. Хакерська активність в Уанеті в 1 півріччі 2012 – http://websecurity.com.ua/6026/.
4. Веб додатки на інфікованих сайтах – http://websecurity.com.ua/6061/.
5. OWASP Top Ten Project – https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.
6. OSVDB: The Open Source Vulnerability Database – http://osvdb.org/browse.
7. National Vulnerability Database (NVD) CVE Statistics – http://web.nvd.nist.gov/view/vuln/statistics.
8. XSS уразливості в 34 мільйонах флеш файлах – http://websecurity.com.ua/3842/.
9. Content Spoofing та XSS уразливості в JW Player – http://websecurity.com.ua/5848/.