СТАТИСТИКА УЯЗВИМОСТЕЙ WEB-ПРИЛОЖЕНИЙ ЗА 2008 ГОД

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Консорциум Web Application Security Consortium (WASC) представляет статистику уязвимостей Web-приложений за 2008 год (WASC Web Application Security Statistics Project 2008) и выражает благодарность следующим экспертам и компаниям, внесшим свой вклад в развитие проекта:

Sergey Gordeychik* (POSITIVE TECHNOLOGIES)
Jeremiah Grossman (WHITEHAT SECURITY)
Mandeep Khera (CENZIC)
Matt Latinga (HP APPLICATION SECURITY CENTER)
Chris Wysopal (VERACODE)
Shreeraj Shah (BLUEINFY)
Lawson Lee (dns)
Campbell Murray (ENCRIPTION LIMITED)
Dmitry Evteev (POSITIVE TECHNOLOGIES)
**Project Leader*

2. МЕТОДИКА

Данная публикация содержит обзорную статистику уязвимостей Web-приложений, полученную в ходе работ по тестированиям на проникновение, аудитов безопасности и других работ, проводимых Компаниями, входящими в консорциум WASC в 2008 году. Всего статистика содержит данные о 12186 сайтах, в которых было обнаружено 97554 уязвимости различной степени риска.

В результате собранных данных было получено 4 набора данных:

- суммарная статистика по всем видам работ;
- статистика по автоматическому сканированию;
- статистика по оценке защищенности методом черного ящика;
- статистика по оценке защищенности методом белого ящика.

Данные автоматического сканирования содержат информацию по полностью автоматизированному сканированию без предварительной настройки (со стандартным профилем) сайтов хостинг-провайдера. При анализе этой информации следует учитывать, что далеко не все сайты используют интерактивные элементы. Кроме того, дополнительная экспертная настройка сканера под конкретное Web-приложение позволяет существенно повысить эффективность обнаружения уязвимостей.

Статистика по оценке защищенности методом черного ящика содержит результаты работ по ручному и автоматизированному анализу Web-приложений, без предварительного получения какой либо информации об исследуемом приложении. Как правило, такие работы включают сканирование с предварительными настройками и ручной поиск уязвимостей недоступных автоматическим сканерам.

Статистика по оценке защищенности методом белого ящика содержит результаты работ по наиболее глубокому анализу Web-приложений. Такие работы включают в себя анализ приложения от имени авторизованного пользователя и анализ исходных кодов, помимо всех тех проверок, которые выполняются при обследовании приложения методом черного ящика.

Обнаруженные уязвимости классифицировались согласно Web Application Security Consortium Web Security Threat Classification (WASC WSTCv2). Критичность уязвимости, оценивалась согласно CVSSv2 (Common Vulnerability Scoring System version 2) с дальнейшим приведением к степеням риска стандарта по защите информации в индустрии платежных карт PCI DSS (Payment Card Industry Data Security Standard) согласно методике (Приложение 1).

3. РЕЗЮМЕ

Всего в представленную статистику вошли данные по 12186 Web-приложениям, в которых было обнаружено 97554 уязвимости различной степени риска. Анализ полученных данных показывает, что **более 13%**[1] всех проанализированных сайтов может быть

[1] Web-приложения, содержащие уязвимости Brute Force Attack, Buffer Overflow, OS Commanding, Path Traversal, Remote File Inclusion, SSI Injection, Session Fixation, SQL Injection, Insufficient Authentication, Insufficient Authorization, выявленные при проведении автоматизированных сканирований.

скомпрометировано **полностью автоматически**. Около 49% Web-приложений содержат уязвимости высокой степеней риска (Urgent и Critical), обнаруженные при автоматическом сканировании систем (Т.1). Однако при детальной ручной и автоматизированной оценке методом белого ящика **вероятность обнаружения таких уязвимостей высокой степени риска достигает 80-96%**. Вероятность же обнаружения уязвимостей степени риска выше среднего (критерий соответствия требованиям PCI DSS) составляет более 86% при любом методе работ. В то же время при проведении более глубокого анализа **99% Web-приложений не удовлетворяет требованиям стандарта по защите информации в индустрии платежных карт** (Т.6, Рис.13).

На основании проведенного анализа можно сделать следующие выводы:

- Наиболее распространенными уязвимостями являются "Межсайтовое выполнение сценариев" (Cross-site Scripting), различные виды утечки информации (Information Leakage), "Внедрение операторов SQL" (SQL Injection), "Расщепление HTTP-запроса" (HTTP Response Splitting).
- Вероятность обнаружения критичной ошибки в динамическом Web-приложении составляет порядка 49% при проведении автоматического сканирования и 96% при всестороннем экспертном анализе методом белого ящика;
- Уязвимости, связанные с недостатками администрирования встречается на 20% чаще, чем уязвимости связанные с ошибками в разработке систем;
- До 99% Web-приложений не удовлетворяет требованиям стандарта по защите информации в индустрии платежных карт, а 48% не соответствуют критериям ASV-сканирования по PCI DSS.
- Детальный анализ методом белого ящика позволяет в среднем идентифицировать до 91 уязвимостей высокой степени риска на одно Web-приложение, в то время как автоматизированное сканирование – только 3.
- По сравнению с 2007 годом снизилось число сайтов содержащих распространенные уязвимости SQL Injection и Cross-site Scripting на 13 и 20% соответственно, однако, число сайтов содержащих различные виды утечки информации возросло на 24%. С другой стороны, вероятность автоматической компрометации узлов возросла с 7 до 13%.

4. АНАЛИЗ ДАННЫХ

Всего в представленную статистику вошли данные по 12186 Web-приложениям, в которых было обнаружено 97554 уязвимости различной степени риска.

4.1. Общий анализ

В Т.1 и на Рис.1 представлены данные по вероятности обнаружения уязвимостей различной степени риска, выявленные в ходе аудитов и путем автоматизированного сканирования.

Так, при проведении автоматических сканирований было выявлено до 86% сайтов, содержащих от одной до нескольких уязвимостей не ниже среднего уровня риска (Urgent-

High). При оценке Web-приложений методами черного и белого ящика, аналогичный показатель увеличился до 92-98% соответственно.

В значительной степени полученные результаты связанны с тем, что при детальном анализе оценка риска более адекватна и учитывает не только тип уязвимости, но и реальные последствия её эксплуатации с учетом архитектуры и реализации приложения. Кроме того, важным фактором является то, что при автоматическом сканировании участвовали сайты хостинг-провайдера, в некоторых случаях не содержащие активного контента, в то время как работы по оценке защищенности, как правило, проводятся для приложений содержащих сложную бизнес-логику. То есть результаты автоматизированных сканирований можно интерпретировать как данные для среднестатистического Интернет-сайта, в то время как работы проводимые методами BlackBox и WhiteBox больше относятся к интерактивным корпоративным Web-приложениям.

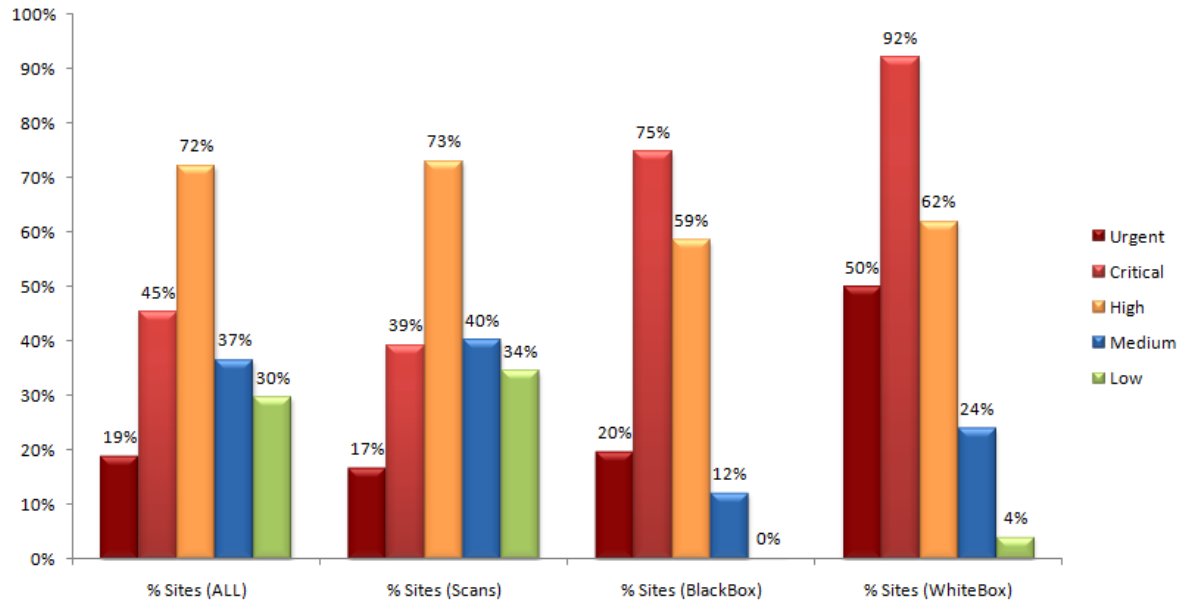

Рисунок 1. Вероятность обнаружения уязвимостей различной степени риска

Т. 1 Вероятность обнаружения уязвимостей различной степени риска

	ALL	Scans	BlackBox	WhiteBox
Urgent	18,77%	16,70%	19,69%	50,00%
Critical	45,22%	39,25%	74,76%	92,00%
High	72,27%	73,09%	58,51%	62,00%
Medium	36,56%	40,19%	12,05%	24,00%
Low	29,69%	34,45%	0,10%	4,00%

U+C	55,50%	49,40%	79,73%	96,00%
U+C+H	95,79%	95,60%	95,66%	98,84%

Наиболее распространенными уязвимостями являются Cross-Site Scripting, Information Leakage, SQL Injection, Insufficient Transport Layer Protection, Fingerprinting и HTTP Response Splitting (Рис. 2). Как правило, уязвимости типа Cross-Site Scripting, SQL Injection и HTTP Response Splitting возникают по причине ошибок в разработке систем, в то время как Information Leakage, Insufficient Transport Layer Protection и Fingerprinting зачастую связаны с недостаточно эффективным администрированием (например, разграничением доступа) в системах.

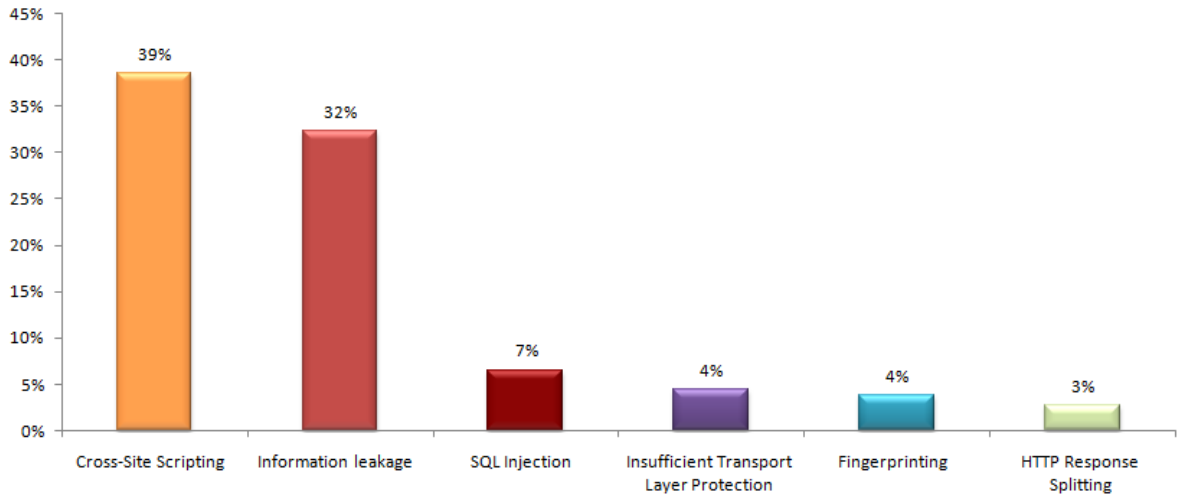

Рисунок 2. Наиболее распространенные уязвимости в Web-приложениях (% Vulns ALL)

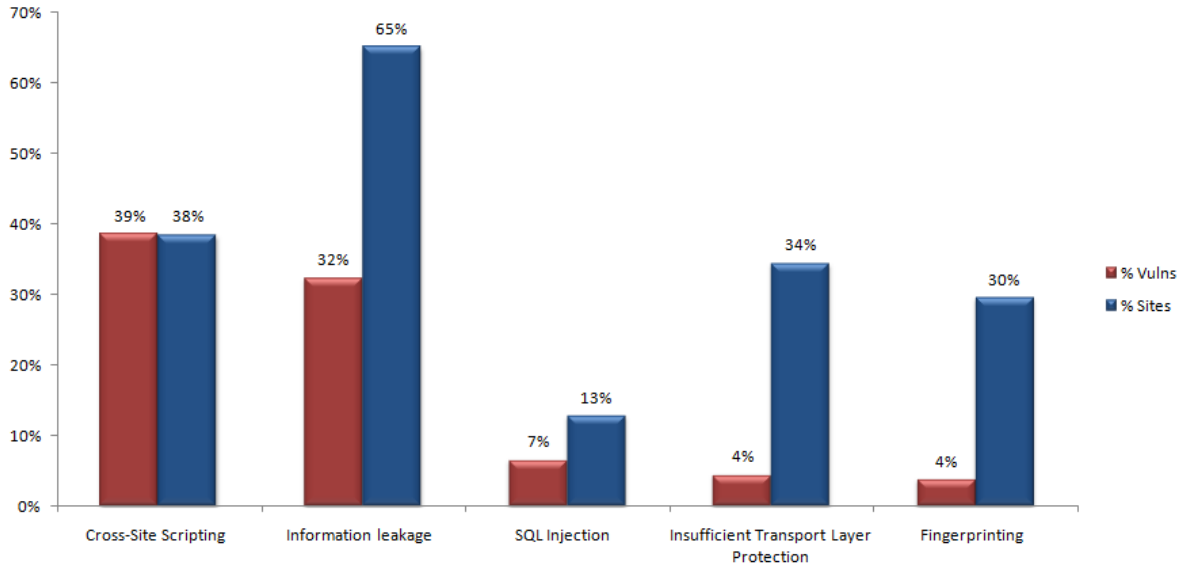

Рисунок 3. Вероятность обнаружения наиболее распространенных уязвимостей Web-приложений (% Sites ALL)

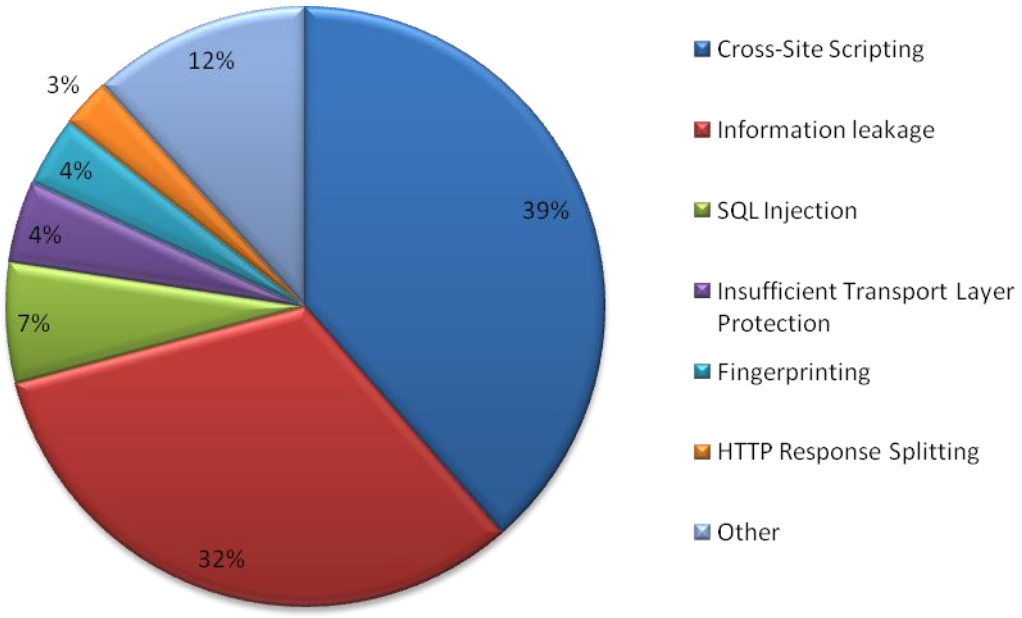

Рисунок 4. Процент уязвимостей от общего числа (% Vulns ALL)

Рассматривая природу возникновения уязвимостей в целом (в соответствии с классификацией в Приложении 2), получим, что на 20% чаще встречаются уязвимости, связанные с недостаточно эффективным администрированием (Рис. 5). В тоже время, на один сайт приходиться до четырех проблем связанных с недостатками администрирования и до восьми уязвимостей, связанных с ошибками в разработке систем (Т.2).

Т. 2 Вероятность обнаружения уязвимостей по природе возникновения

	No. of Vulns	No. of Sites	% Vulns	% Sites	No. Vulns on Site
Vulnerability in administration	41859	10347	42,91%	84,91%	4,05
Vulnerability in code	55695	7023	57,09%	57,63%	7,93

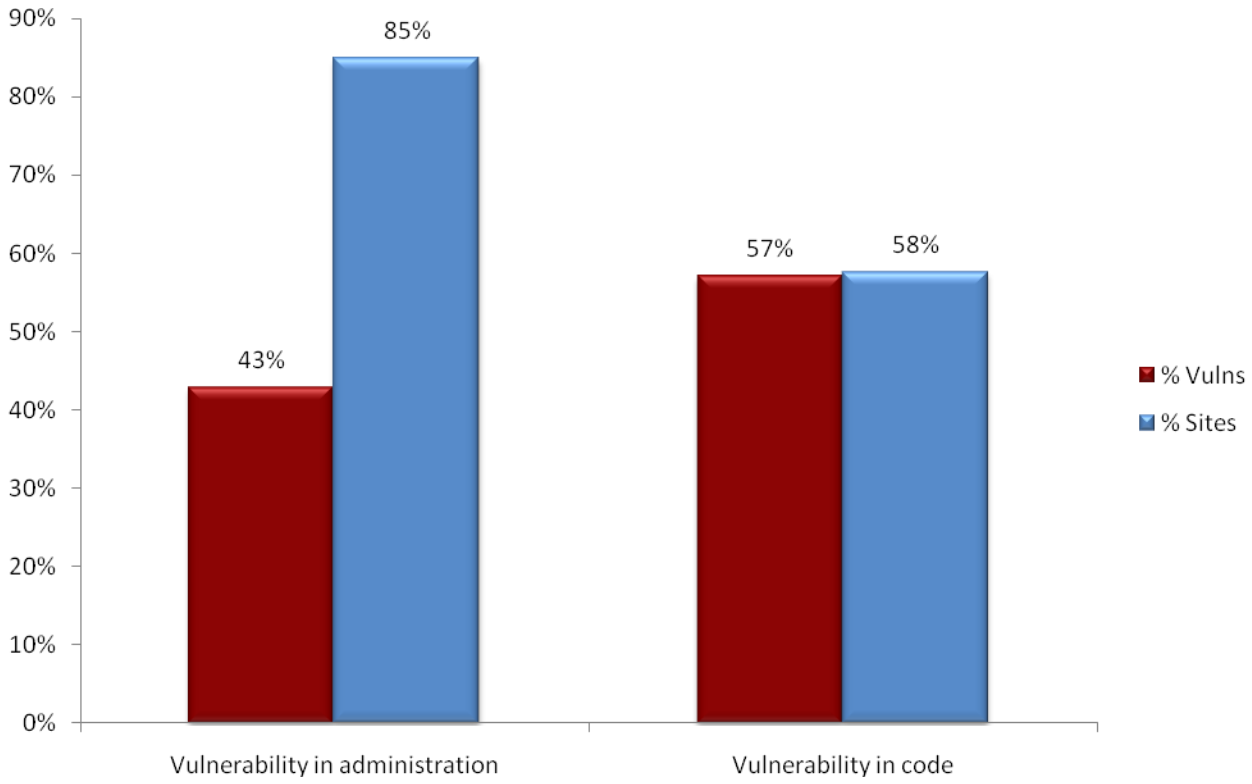

Рисунок 5. Вероятность обнаружения уязвимостей по природе возникновения

При детальном анализе Web-приложений методами BlackBox и WhiteBox ощутимый процент сайтов оказались уязвимы также для Content Spoofing и Path Traversal (Рис. 6). Причем вероятность обнаружения уязвимостей типа SQL Injection при таком подходе к анализу защищенности достигает 19% (Рис. 7).

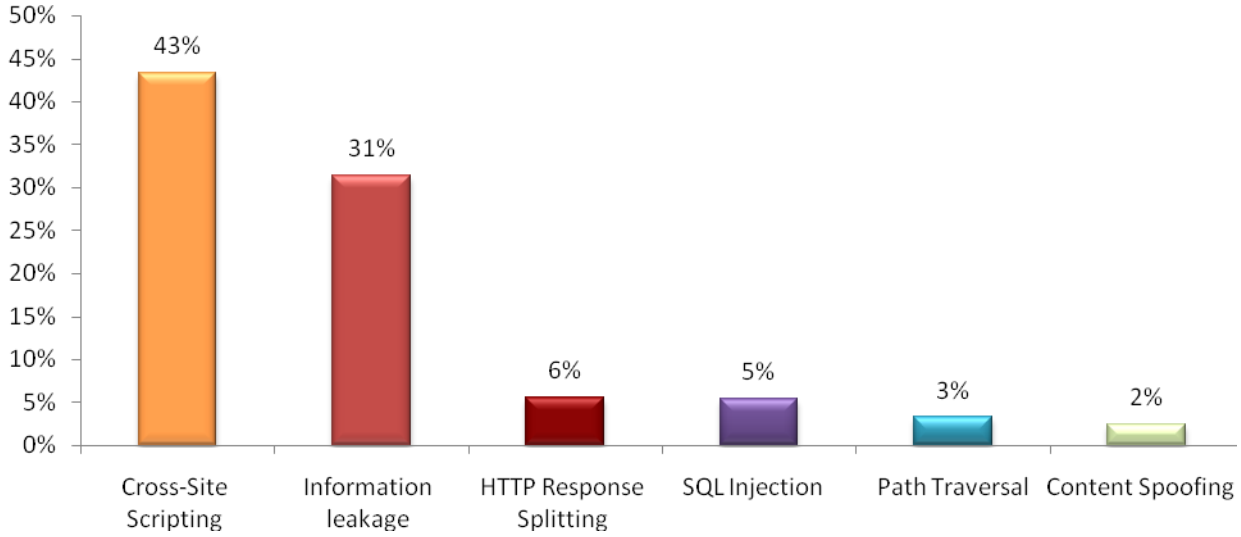

Рисунок 6. Наиболее распространенные уязвимости в Web-приложениях (% Vulns BlackBox & WhiteBox)

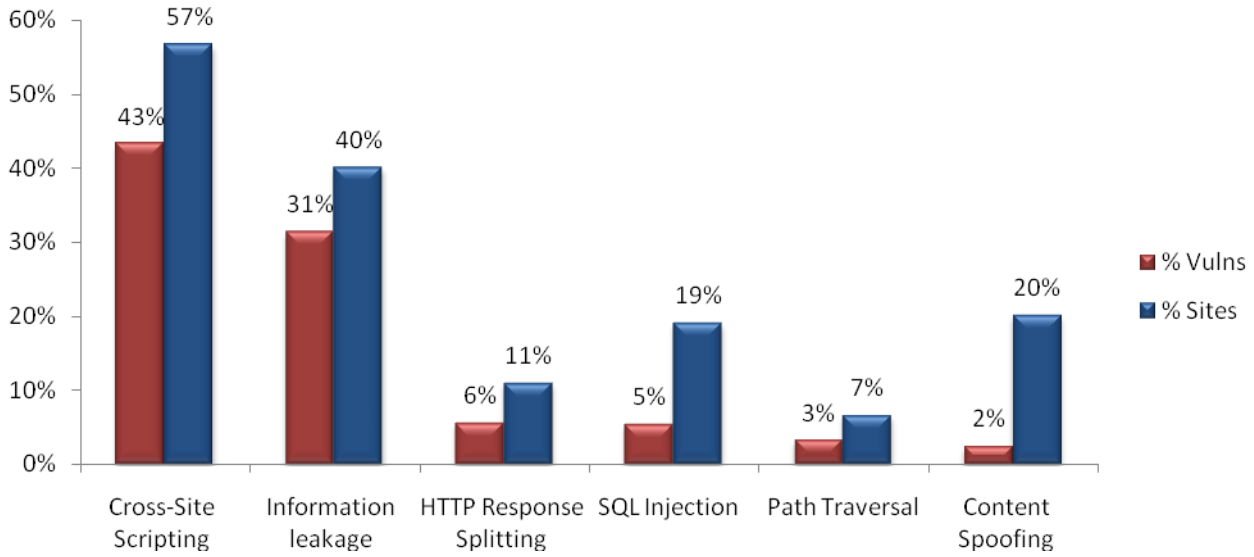

Рисунок 7. Вероятность обнаружения наиболее распространенных уязвимостей Web-приложений (% Sites BlackBox & WhiteBox)

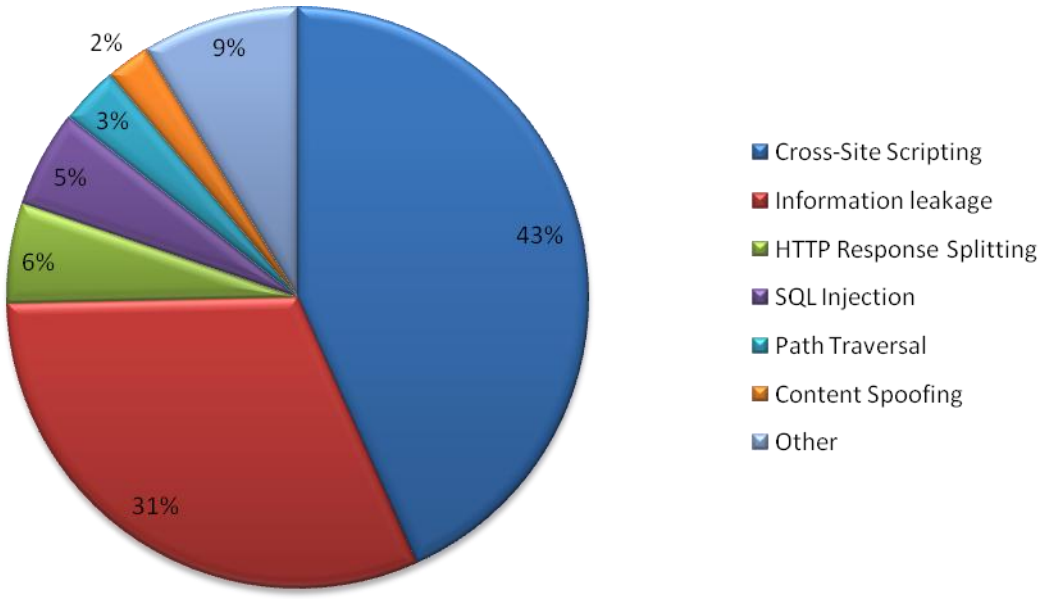

Рисунок 8. Процент уязвимостей от общего числа (% Vulns BlackBox & WhiteBox)

Если анализировать распространенность уязвимостей высокого степени риска при детальном обследовании Web-приложения (Рис. 9), то здесь наиболее часто встречаются ошибки типа «Предсказуемое значение идентификатора сессии» (Credential/Session Prediction). Также широко распространены ошибки «Внедрение операторов SQL» (SQL Injection), «Чтение произвольных файлов» (Path Traversal) и ошибки в реализации и настройке систем авторизации и аутентификации.

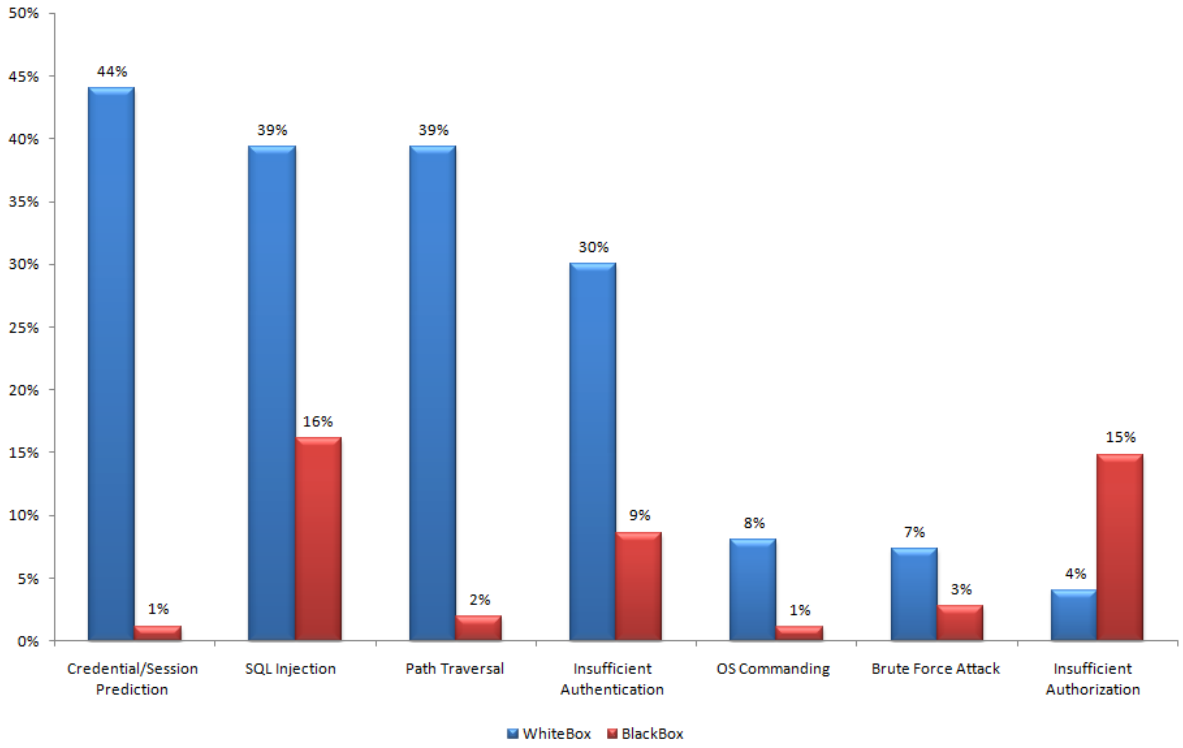

Рисунок 9. Вероятность обнаружения наиболее кричных уязвимостей Web-приложений (% Sites BlackBox & WhiteBox)

Если рассматривать вероятность обнаружения уязвимости с точки зрения воздействия на посетителей Web-ресурса и воздействия на Web-сервер (в соответствии с классификацией в Приложении 2), то наиболее распространенны уязвимости на стороне Web-сервера (Рис. 10). В тоже время, распределение уязвимостей по типу воздействия на один сайт не равномерно и во многом зависит от используемого способа поиска уязвимостей (Рис.11).

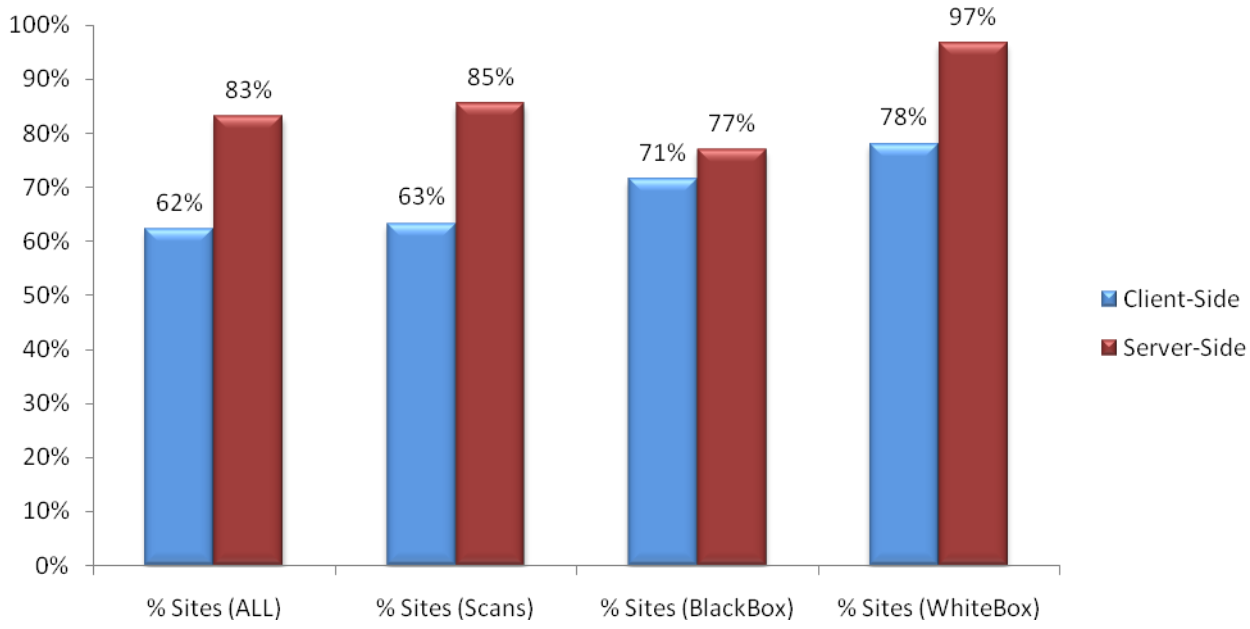

Рисунок 10. Вероятность обнаружения уязвимости по типу воздействия

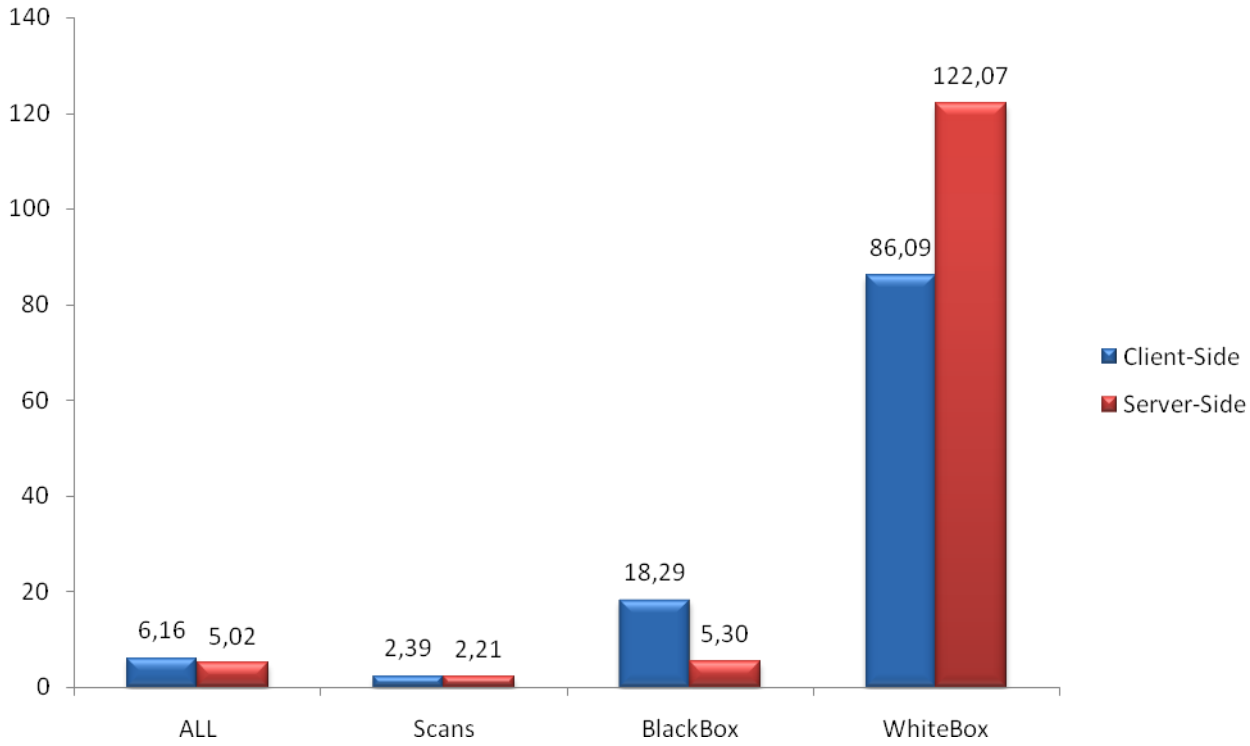

Рисунок 11. Распределение уязвимостей на один сайт при использовании различных методов их поиска (No. Vulns on Site)

Т. 3 Уязвимости по типу воздействия

	No. of Vulns	No. of Sites	% Vulns	% Sites	No. Vulns on Site
ALL Stat (Server-Side)	50856	10125	52,13%	83,09%	5,02
ALL Stat (Client-Side)	46698	7580	47,87%	62,20%	6,16
Scans (Server-Side)	19746	8922	55,60%	85,40%	2,21
Scans (Client-Side)	15767	6607	44,40%	63,24%	2,39
BlackBox (Server-Side)	4260	804	23,77%	76,86%	5,30
BlackBox (Client-Side)	13665	747	76,23%	71,41%	18,29
WhiteBox (Server-Side)	17700	145	63,73%	96,67%	122,07
WhiteBox (Client-Side)	10072	117	36,27%	78,00%	86,09

4.2. Анализ данных в контексте требований PCI DSS

Рассматривая наборы полученных данных уязвимых Web-приложений в контексте соответствия требованиям стандарта по защите информации в индустрии платежных карт PCI DSS, можно выделить те из них (Т.4), которые относятся к устранению конкретных уязвимостей в Web-приложениях. Кроме того, PCI DSS Technical and Operational Requirements for Approved Scanning Vendors (ASVs) содержит в себе схожие требования, но затрагивает только процесс ASV-сканирования по PCI (Т.5).

Т. 4 Требования стандарта PCI DSS, регламентирующие обязательное устранение конкретных уязвимостей в Web-приложениях

Требование PCI DSS v.1.2	Процедура
6.5.1 Cross-site scripting (XSS)	6.5.1 Cross-site scripting (XSS) (Validate all parameters before inclusion.)
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	6.5.2 Injection flaws, particularly SQL injection (Validate input to verify user data cannot modify meaning of commands and queries.)
6.5.3 Malicious file execution	6.5.3 Malicious file execution (Validate input to verify application does not accept filenames or files from users.)
6.5.5 Cross-site request forgery (CSRF)	6.5.5 Cross-site request forgery (CSRF) (Do not reply on authorization credentials and tokens automatically submitted by browsers.)
6.5.6 Information leakage and improper error handling	6.5.6 Information leakage and improper error handling (Do not leak information via error messages or other means.)
6.5.7 Broken authentication and session management	6.5.7 Broken authentication and session management (Properly authenticate users and protect account credentials and session tokens.)
6.5.9 Insecure communications	6.5.9 Insecure communications (Properly encrypt all authenticated and sensitive communications.)

Т. 5 Требования PCI DSS Technical and Operational Requirements for Approved Scanning Vendors (ASVs), регламентирующие обязательное выявление конкретных уязвимостей в Web-приложениях при проведении ASV-сканирования

Требования Technical and Operational Requirements for Approved Scanning Vendors (ASVs) v.1.1	Процедура
Web Server Check	The ASV scanning solution must be able to test for all known vulnerabilities and configuration issues on web servers. New exploits are routinely discovered in web server products. The ASV scanning solution must be able to detect and report known exploits. Browsing of directories on a web server is not a good practice. The ASV scanning solution must be able to scan the web site and verify that directory browsing is not possible on the server.

	The ASV scanning solution must be able to detect all known CGI vulnerabilities.
Custom Web Application Check	The ASV scanning solution must be able to detect the following application vulnerabilities and configuration issues: • Unvalidated parameters which lead to SQL injection attacks • Cross-site scripting (XSS) flaws

Оценивая полученную статистику собранных данных по приведенным критериям в Т.4 и Т.5, будут получены данные, представленные в Т.6, на Рис. 12 - Рис. 14.

Т. 6 % сайтов, не соответствующих требованиям стандарта PCI DSS при оценке Web-приложений различными методами

Требование PCI DSS v.1.2	Суммарная доля не соответствия, ALL (% Sites)	Доля не соответствия при Scans (% Sites)	Доля не соответствия при BlackBox (% Sites)	Доля не соответствия при WhiteBox (% Sites)
6.5.1 Cross-site scripting (XSS)	38,45%	37,66%	56,41%	58,67%
6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.	14,55%	12,70%	19,31%	64,00%
6.5.3 Malicious file execution	0,94%	0,08%	1,05%	8,67%
6.5.5 Cross-site request forgery (CSRF)	1,32%	0,02%	7,93%	0,67%
6.5.6 Information leakage and improper error handling	66,67%	74,05%	38,24%	54,00%
6.5.7 Broken authentication and session management	7,62%	0,52%	30,98%	71,33%
6.5.9 Insecure communications	34,42%	39,96%	0,00%*	17,33%
Требование Technical and Operational Requirements for Approved Scanning Vendors (ASVs) v.1.1				
Web Server Check	Не применимо	5,73%	Не применимо	Не применимо
Custom Web Application Check	Не применимо	44,92%	Не применимо	Не применимо

* При проведении оценки защищенности Web-приложений методом черного ящика уязвимости данного класса не вносились в отчетные документы по результатам проводимых работ. Это связано с тем, что при проведении работ данным методом внимание аудиторов было направлено на наиболее опасные уязвимости.

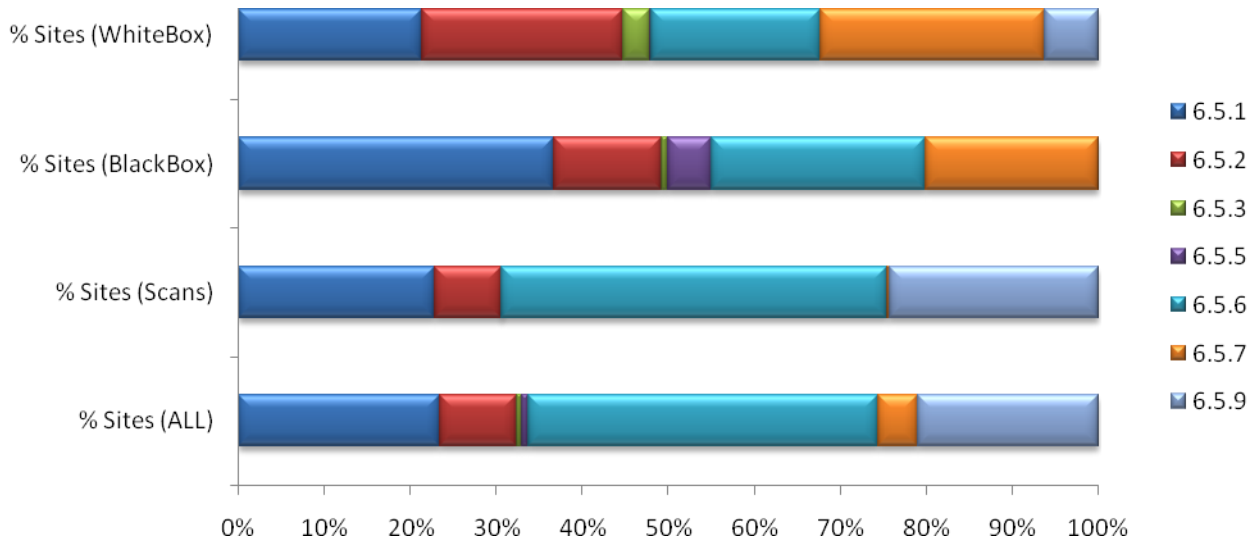

Рисунок 12. Распределение сайтов, не удовлетворяющих требованиям стандарта PCI DSS

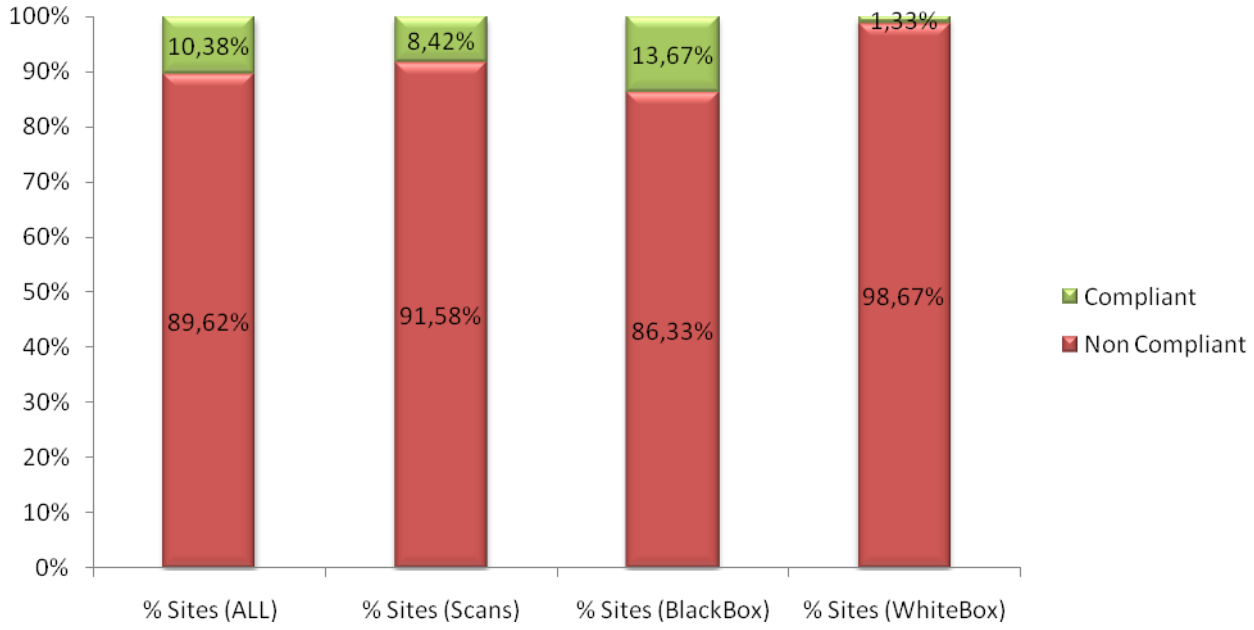

Рисунок 13. Уровень соответствия анализируемых Web-приложений требованиям стандарта PCI DSS (QSA)

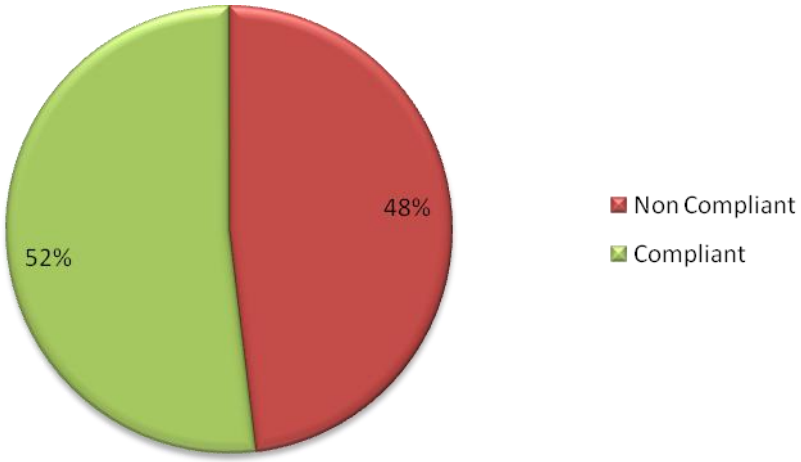

Рисунок 14. Уровень соответствия анализируемых Web-приложений требованиям стандарта PCI DSS (ASV)

Таким образом, при проведении ASV-сканирования в отношении Web-приложений около 48% из них не удовлетворяют требованиям стандарта PCI DSS. В то же время при проведении более глубокого анализа 99% Web-приложений не удовлетворяет требованиям стандарта по защите информации в индустрии платежных карт.

4.3. Сравнение методов анализа защищенности

Если провести сравнение полностью автоматических сканирований с ручной и автоматизированной оценкой методами черного и белого ящика, то явно видно отставание автоматического сканирования при обнаружении наиболее опасных ошибок (Рис. 15).

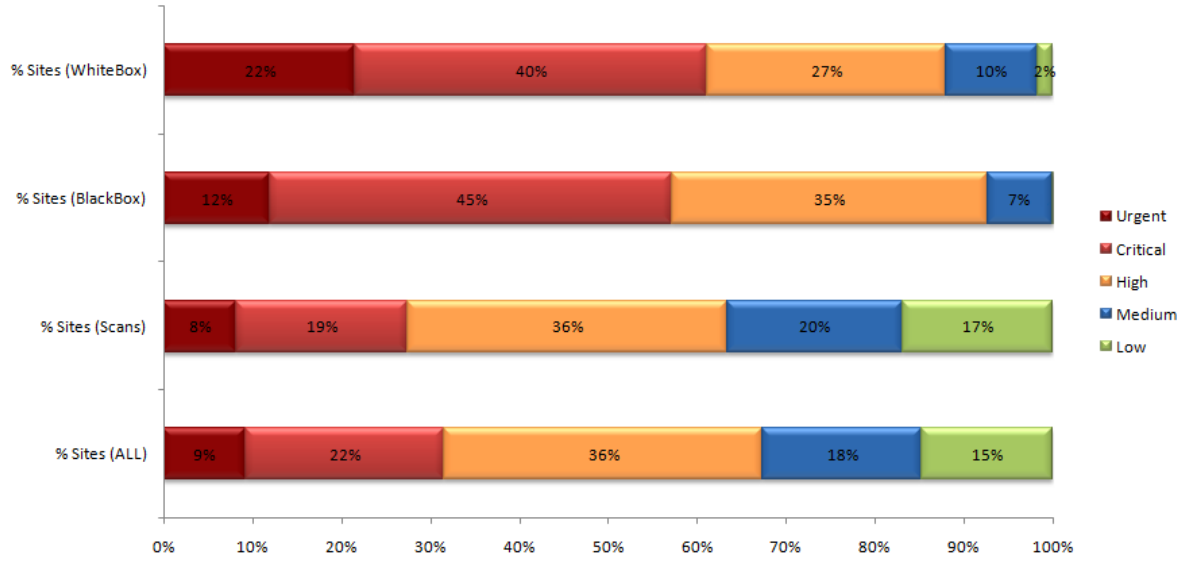

Рисунок 15. Распределение вероятности обнаружения уязвимостей по методу их поиска

Если рассматривать такой показатель, как количество обнаруженных уязвимостей на один сайт (Т.7), то детальный анализ позволяет в среднем идентифицировать до 91 уязвимостей высокой степени риска на одно приложение, в то время как автоматизированное сканирование – только 3 (Рис. 16).

Т. 7 Количество уязвимостей на один сайт

Threat rank	ALL	Scans	BlackBox	WhiteBox
Urgent	3,90	2,70	8,00	18,04
Critical	8,11	2,85	16,66	91,30
High	4,02	1,47	4,92	147,02
Medium	1,10	1,02	1,87	3,86
Low	1,01	1,01	1,00	1,33
ALL	8,01	3,40	17,14	185,15

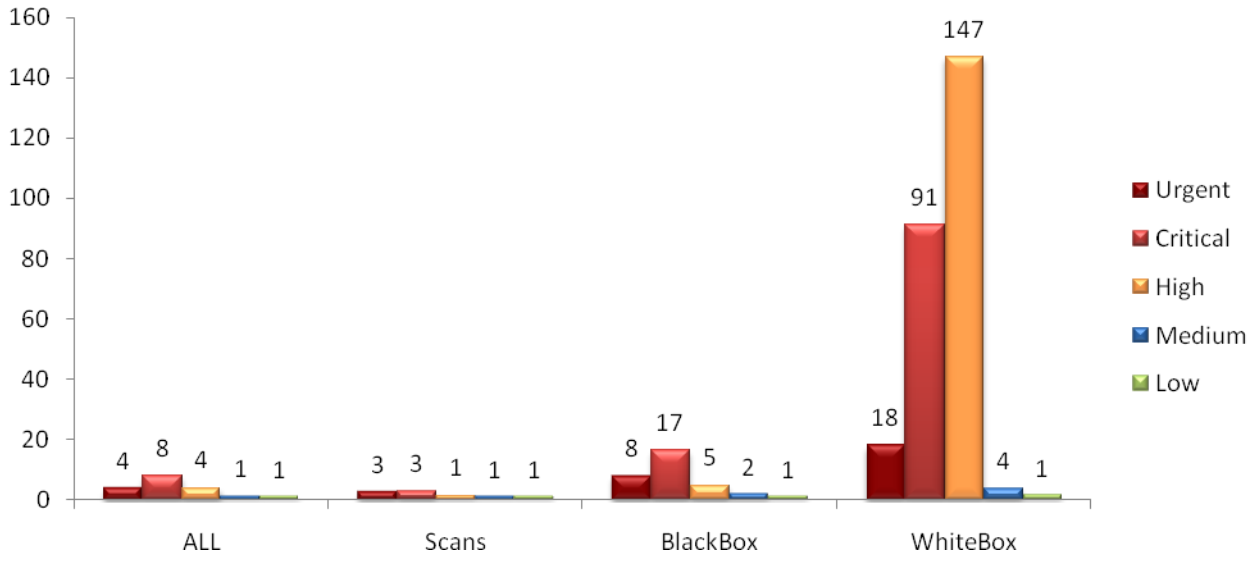

Рисунок 16. Количество уязвимостей на один сайт

На Рис.1, Рис.15 и Рис.16 наглядно показано значительное отставание результатов автоматизированных сканирований и результатов оценки Web-приложений методом черного ящика от наиболее глубокого поиска уязвимостей методом белого ящика. Это свидетельствует о том, что использование способа поиска уязвимостей методом белого

ящика в значительной степени является более эффективным по сравнению с другими способами.

5. ПРИЛОЖЕНИЕ 1: МЕТОДИКА ОЦЕНКИ СТЕПЕНИ РИСКА

Т. 8 Методика оценки степени риска

Threat Classification	Basic CVSS Score	PCI DSS Risk
Abuse of Functionality	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)	Medium
Brute Force Attack	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	Critical
Buffer Overflow	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Content Spoofing	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)	High
Credential/Session Prediction	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	Critical
Cross-Site Scripting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	Critical
Cross-Site Request Forgery	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)	High
Denial of Service	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)	High
Format String Attack	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
HTTP Request Splitting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	Critical
HTTP Response Splitting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	Critical
HTTP Request Smuggling	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	Critical
HTTP Response Smuggling	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)	Critical
Integer Overflow	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
LDAP Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Mail Command Injection	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)	High
OS Commanding	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Path Traversal	7.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N)	Critical

Predictable Resource Location	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
Remote File Inclusion	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Routing Detour	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
SOAP Array Abuse	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)	High
SSI Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Session Fixation	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	Critical
SQL Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
URL Redirectors	2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)	Medium
XPath Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
XML Attribute Blowup	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
XML External Entity	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
XML Entity Expansion	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
XML Injection	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)	Critical
XQuery Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Application Misconfiguration	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)	Medium
Directory Indexing	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
Fingerprinting	0 (AV:N/AC:L/Au:N/C:N/I:N/A:N)	Low
Improper Parsing	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Improper Permissions	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)	Urgent
Information leakage	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
Insecure Indexing	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
Insufficient Anti-automation	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)	Medium
Insufficient Authentication	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	Critical

Insufficient Authorization	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	Critical
Insufficient Data Protection	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)	High
Insufficient Process Validation	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)	Medium
Insufficient Session Expiration	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)	Critical
Insufficient Transport Layer Protection	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)	Medium
Server Misconfiguration	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)	Medium

6. ПРИЛОЖЕНИЕ 2: ИСПОЛЬЗУЕМАЯ ДОПОЛНИТЕЛЬНАЯ КЛАССИФИКАЦИЯ УЯЗВИМОСТЕЙ

Т. 9 Классификация уязвимостей по природе возникновения и типу воздействия

Threat Classification	Vulnerability in	Impact
Abuse of Functionality	code	server-side
Brute Force Attack	administration	server-side
Buffer Overflow	code	server-side
Content Spoofing	code	client-side
Credential/Session Prediction	code	server-side
Cross-Site Scripting	code	client-side
Cross-Site Request Forgery	code	client-side
Denial of Service	administration	server-side
Format String Attack	code	server-side
HTTP Request Splitting	code	client-side
HTTP Response Splitting	code	client-side
HTTP Request Smuggling	administration	client-side

HTTP Response Smuggling	administration	client-side
Integer Overflow	code	server-side
LDAP Injection	code	server-side
Mail Command Injection	code	server-side
OS Commanding	code	server-side
Path Traversal	code	server-side
Predictable Resource Location	administration	server-side
Remote File Inclusion	code	server-side
Routing Detour	code	server-side
SOAP Array Abuse	code	server-side
SSI Injection	code	server-side
Session Fixation	code	server-side
SQL Injection	code	server-side
URL Redirectors	code	client-side
XPath Injection	code	server-side
XML Attribute Blowup	code	server-side
XML External Entity	code	server-side
XML Entity Expansion	code	server-side
XML Injection	code	server-side
XQuery Injection	code	server-side
Application Misconfiguration	administration	server-side
Directory Indexing	administration	server-side
Fingerprinting	administration	server-side
Improper Parsing	code	server-side

Improper Permissions	administration	server-side
Information leakage	administration	server-side
Insecure Indexing	administration	server-side
Insufficient Anti-automation	code	server-side
Insufficient Authentication	code	server-side
Insufficient Authorization	code	server-side
Insufficient Data Protection	administration	server-side
Insufficient Process Validation	code	server-side
Insufficient Session Expiration	code	server-side
Insufficient Transport Layer Protection	administration	client-side
Server Misconfiguration	administration	server-side

Additional notes

Web Application Security Consortium Threat Classification version 2 was used in this research. Therefore some types of vulnerabilities are not included into the overall results.

The most prevalent vulnerability Cross-Site Request Forgery in this statistics is not on top because it is difficult to detect in automatically and because a lot of experts take its existence for granted.

Vulnerabilities which existence depends on platform are also not included into the statistics (for example, buffer overflow in Apache).

Contributors

WASC would like to thank the following organizations for making this initiative possible. Each organization is responsible for contributing sanitized data from web application security projects which was then combined to produce aggregated statistics.

Statistics

Overall Data

T. 10 General statistics Threat Classification

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	153	83	0,16%	0,68%
Brute Force Attack	79	51	0,08%	0,42%
Buffer Overflow	537	84	0,55%	0,69%
Content Spoofing	1564	304	1,60%	2,49%
Credential/Session Prediction	794	147	0,81%	1,21%
Cross-Site Scripting	37624	4686	38,57%	38,45%
Cross-Site Request Forgery	285	161	0,29%	1,32%
Denial of Service	42	36	0,04%	0,30%
Format String Attack	52	43	0,05%	0,35%
HTTP Request Splitting	311	162	0,32%	1,33%

HTTP Response Splitting	2592	161	2,66%	1,32%
HTTP Request Smuggling	0	0	0,00%	0,00%
HTTP Response Smuggling	0	0	0,00%	0,00%
Integer Overflow	79	46	0,08%	0,38%
LDAP Injection	41	16	0,04%	0,13%
Mail Command Injection	1	1	0,00%	0,01%
OS Commanding	76	30	0,08%	0,25%
Path Traversal	1563	139	1,60%	1,14%
Predictable Resource Location	1507	295	1,54%	2,42%
Remote File Inclusion	99	44	0,10%	0,36%
Routing Detour	0	0	0,00%	0,00%
SOAP Array Abuse	2	1	0,00%	0,01%
SSI Injection	157	33	0,16%	0,27%
Session Fixation	137	123	0,14%	1,01%
SQL Injection	6345	1555	6,50%	12,76%
URL Redirectors	5	4	0,01%	0,03%
XPath Injection	64	19	0,07%	0,16%
XML Attribute Blowup	0	0	0,00%	0,00%
XML External Entity	0	0	0,00%	0,00%
XML Entity Expansion	0	0	0,00%	0,00%
XML Injection	0	0	0,00%	0,00%

XQuery Injection	0	0	0,00%	0,00%
Application Misconfiguration	85	60	0,09%	0,49%
Directory Indexing	370	184	0,38%	1,51%
Fingerprinting	3663	3604	3,75%	29,57%
Improper Parsing	1464	524	1,50%	4,30%
Improper Permissions	4	4	0,00%	0,03%
Information leakage	31527	7942	32,32%	65,17%
Insecure Indexing	8	7	0,01%	0,06%
Insufficient Anti-automation	108	36	0,11%	0,30%
Insufficient Authentication	806	304	0,83%	2,49%
Insufficient Authorization	615	286	0,63%	2,35%
Insufficient Data Protection	64	21	0,07%	0,17%
Insufficient Process Validation	52	34	0,05%	0,28%
Insufficient Session Expiration	169	71	0,17%	0,58%
Insufficient Transport Layer Protection	4317	4195	4,43%	34,42%
Server Misconfiguration	193	113	0,20%	0,93%
Total	97554	12186		

T. 11 Vulnerabilities distribution by risk Threat rank

Threat rank	N of Vulns	N of Sites	N of Sites	% Sites
Urgent	8918	2287	9,14%	18,77%
Critical	44669	5511	45,79%	45,22%

High	35375	8807	36,26%	72,27%
Medium	4908	4455	5,03%	36,56%
Low	3663	3618	3,75%	29,69%

Automatic scans

T. 12 General statistics Threat Classification

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	1	1	0,00%	0,01%
Brute Force Attack	5	5	0,01%	0,05%
Buffer Overflow	6	3	0,02%	0,03%
Content Spoofing	29	22	0,08%	0,21%
Credential/Session Prediction	9	9	0,03%	0,09%
Cross-Site Scripting	11230	3934	31,62%	37,66%
Cross-Site Request Forgery	2	2	0,01%	0,02%
Denial of Service	30	25	0,08%	0,24%
Format String Attack	0	0	0,00%	0,00%
HTTP Request Splitting	311	162	0,88%	1,55%
HTTP Response Splitting	0	0	0,00%	0,00%
HTTP Request Smuggling	0	0	0,00%	0,00%
HTTP Response Smuggling	0	0	0,00%	0,00%
Integer Overflow	0	0	0,00%	0,00%
LDAP Injection	0	0	0,00%	0,00%
Mail Command Injection	0	0	0,00%	0,00%

OS Commanding	28	5	0,08%	0,05%
Path Traversal	82	56	0,23%	0,54%
Predictable Resource Location	16	15	0,05%	0,14%
Remote File Inclusion	86	36	0,24%	0,34%
Routing Detour	0	0	0,00%	0,00%
SOAP Array Abuse	0	0	0,00%	0,00%
SSI Injection	157	33	0,44%	0,32%
Session Fixation	3	3	0,01%	0,03%
SQL Injection	2969	1217	8,36%	11,65%
URL Redirectors	1	1	0,00%	0,01%
XPath Injection	0	0	0,00%	0,00%
XML Attribute Blowup	0	0	0,00%	0,00%
XML External Entity	0	0	0,00%	0,00%
XML Entity Expansion	0	0	0,00%	0,00%
XML Injection	0	0	0,00%	0,00%
XQuery Injection	0	0	0,00%	0,00%
Application Misconfiguration	48	37	0,14%	0,35%
Directory Indexing	12	11	0,03%	0,11%
Fingerprinting	3604	3587	10,15%	34,34%
Improper Parsing	1463	523	4,12%	5,01%
Improper Permissions	2	2	0,01%	0,02%
Information leakage	11134	7593	31,35%	72,68%
Insecure Indexing	8	7	0,02%	0,07%
Insufficient Anti-automation	0	0	0,00%	0,00%

Insufficient Authentication	24	15	0,07%	0,14%
Insufficient Authorization	14	14	0,04%	0,13%
Insufficient Data Protection	10	10	0,03%	0,10%
Insufficient Process Validation	12	11	0,03%	0,11%
Insufficient Session Expiration	1	1	0,00%	0,01%
Insufficient Transport Layer Protection	4194	4175	11,81%	39,96%
Server Misconfiguration	22	22	0,06%	0,21%
Total	35513	10447		

T. 13 Vulnerabilities distribution by risk Threat rank

Threat rank	N of Vulns	N of Sites	N of Sites	% Sites
Urgent	4711	1745	13,27%	16,70%
Critical	11679	4100	32,89%	39,25%
High	11257	7636	31,70%	73,09%
Medium	4294	4199	12,09%	40,19%
Low	3625	3599	10,21%	34,45%

Black Box

T. 14 General statistics Threat Classification

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	135	75	0,75%	7,17%
Brute Force Attack	34	29	0,19%	2,77%
Buffer Overflow	0	0	0,00%	0,00%
Content Spoofing	1110	241	6,19%	23,04%

Credential/Session Prediction	15	12	0,08%	1,15%
Cross-Site Scripting	11768	590	65,65%	56,41%
Cross-Site Request Forgery	185	83	1,03%	7,93%
Denial of Service	9	8	0,05%	0,76%
Format String Attack	2	2	0,01%	0,19%
HTTP Request Splitting	0	0	0,00%	0,00%
HTTP Response Splitting	601	77	3,35%	7,36%
HTTP Request Smuggling	0	0	0,00%	0,00%
HTTP Response Smuggling	0	0	0,00%	0,00%
Integer Overflow	9	6	0,05%	0,57%
LDAP Injection	0	0	0,00%	0,00%
Mail Command Injection	0	0	0,00%	0,00%
OS Commanding	16	11	0,09%	1,05%
Path Traversal	29	20	0,16%	1,91%
Predictable Resource Location	855	155	4,77%	14,82%
Remote File Inclusion	3	3	0,02%	0,29%
Routing Detour	0	0	0,00%	0,00%
SOAP Array Abuse	0	0	0,00%	0,00%
SSI Injection	0	0	0,00%	0,00%
Session Fixation	83	79	0,46%	7,55%
SQL Injection	1556	169	8,68%	16,16%
URL Redirectors	1	1	0,01%	0,10%
XPath Injection	59	17	0,33%	1,63%
XML Attribute Blowup	0	0	0,00%	0,00%

XML External Entity	0	0	0,00%	0,00%
XML Entity Expansion	0	0	0,00%	0,00%
XML Injection	0	0	0,00%	0,00%
XQuery Injection	0	0	0,00%	0,00%
Application Misconfiguration	31	20	0,17%	1,91%
Directory Indexing	104	42	0,58%	4,02%
Fingerprinting	1	1	0,01%	0,10%
Improper Parsing	1	1	0,01%	0,10%
Improper Permissions	2	2	0,01%	0,19%
Information leakage	745	399	4,16%	38,15%
Insecure Indexing	0	0	0,00%	0,00%
Insufficient Anti-automation	6	4	0,03%	0,38%
Insufficient Authentication	158	90	0,88%	8,60%
Insufficient Authorization	312	155	1,74%	14,82%
Insufficient Data Protection	2	2	0,01%	0,19%
Insufficient Process Validation	5	5	0,03%	0,48%
Insufficient Session Expiration	30	27	0,17%	2,58%
Insufficient Transport Layer Protection	0	0	0,00%	0,00%
Server Misconfiguration	58	38	0,32%	3,63%
Total	17925	1046		

T. 15 Vulnerabilities distribution by risk Threat rank

Threat rank	N of Vulns	N of Sites	N of Sites	% Sites
Urgent	1648	206	9,19%	19,69%

Critical	13030	782	72,69%	74,76%
High	3011	612	16,80%	58,51%
Medium	235	126	1,31%	12,05%
Low	1	1	0,01%	0,10%

White Box

T. 16 General statistics Threat Classification

Threat Classification	N of Vulns	N of Sites	% Vulns	% Sites
Abuse of Functionality	7	4	0,03%	2,67%
Brute Force Attack	15	11	0,05%	7,33%
Buffer Overflow	421	1	1,52%	0,67%
Content Spoofing	0	0	0,00%	0,00%
Credential/Session Prediction	695	66	2,50%	44,00%
Cross-Site Scripting	8006	88	28,83%	58,67%
Cross-Site Request Forgery	2	1	0,01%	0,67%
Denial of Service	3	3	0,01%	2,00%
Format String Attack	2	1	0,01%	0,67%
HTTP Request Splitting	0	0	0,00%	0,00%
HTTP Response Splitting	1941	54	6,99%	36,00%
HTTP Request Smuggling	0	0	0,00%	0,00%
HTTP Response Smuggling	0	0	0,00%	0,00%
Integer Overflow	0	0	0,00%	0,00%
LDAP Injection	0	0	0,00%	0,00%
Mail Command Injection	1	1	0,00%	0,67%

OS Commanding	29	12	0,10%	8,00%
Path Traversal	1450	59	5,22%	39,33%
Predictable Resource Location	15	13	0,05%	8,67%
Remote File Inclusion	3	2	0,01%	1,33%
Routing Detour	0	0	0,00%	0,00%
SOAP Array Abuse	0	0	0,00%	0,00%
SSI Injection	0	0	0,00%	0,00%
Session Fixation	1	1	0,00%	0,67%
SQL Injection	898	59	3,23%	39,33%
URL Redirectors	0	0	0,00%	0,00%
XPath Injection	0	0	0,00%	0,00%
XML Attribute Blowup	0	0	0,00%	0,00%
XML External Entity	0	0	0,00%	0,00%
XML Entity Expansion	0	0	0,00%	0,00%
XML Injection	0	0	0,00%	0,00%
XQuery Injection	0	0	0,00%	0,00%
Application Misconfiguration	1	1	0,00%	0,67%
Directory Indexing	2	2	0,01%	1,33%
Fingerprinting	8	6	0,03%	4,00%
Improper Parsing	0	0	0,00%	0,00%
Improper Permissions	0	0	0,00%	0,00%
Information leakage	13598	81	48,96%	54,00%
Insecure Indexing	0	0	0,00%	0,00%
Insufficient Anti-automation	2	2	0,01%	1,33%

Insufficient Authentication	324	45	1,17%	30,00%
Insufficient Authorization	89	6	0,32%	4,00%
Insufficient Data Protection	52	9	0,19%	6,00%
Insufficient Process Validation	5	3	0,02%	2,00%
Insufficient Session Expiration	78	28	0,28%	18,67%
Insufficient Transport Layer Protection	123	26	0,44%	17,33%
Server Misconfiguration	1	1	0,00%	0,67%
Total	27772	150		

T. 17 Vulnerabilities distribution by risk Threat rank

Threat rank	N of Vulns	N of Sites	N of Sites	% Sites
Urgent	1353	75	4,87%	50,00%
Critical	12599	138	45,37%	92,00%
High	13673	93	49,23%	62,00%
Medium	139	36	0,50%	24,00%
Low	8	6	0,03%	4,00%