Reporting Status of Vulnerability-related Information about Software Products and Websites

- 3rd Quarter of 2012 (July – September) -

Information-technology Promotion Agency, Japan (IPA) and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), initiated to handle vulnerability-related information in July, 2004, pursuant to the Standards for Handling Software Vulnerability Information and Others (Directive #235, 2004) by the Ministry of Economy, Trade and Industry (METI).
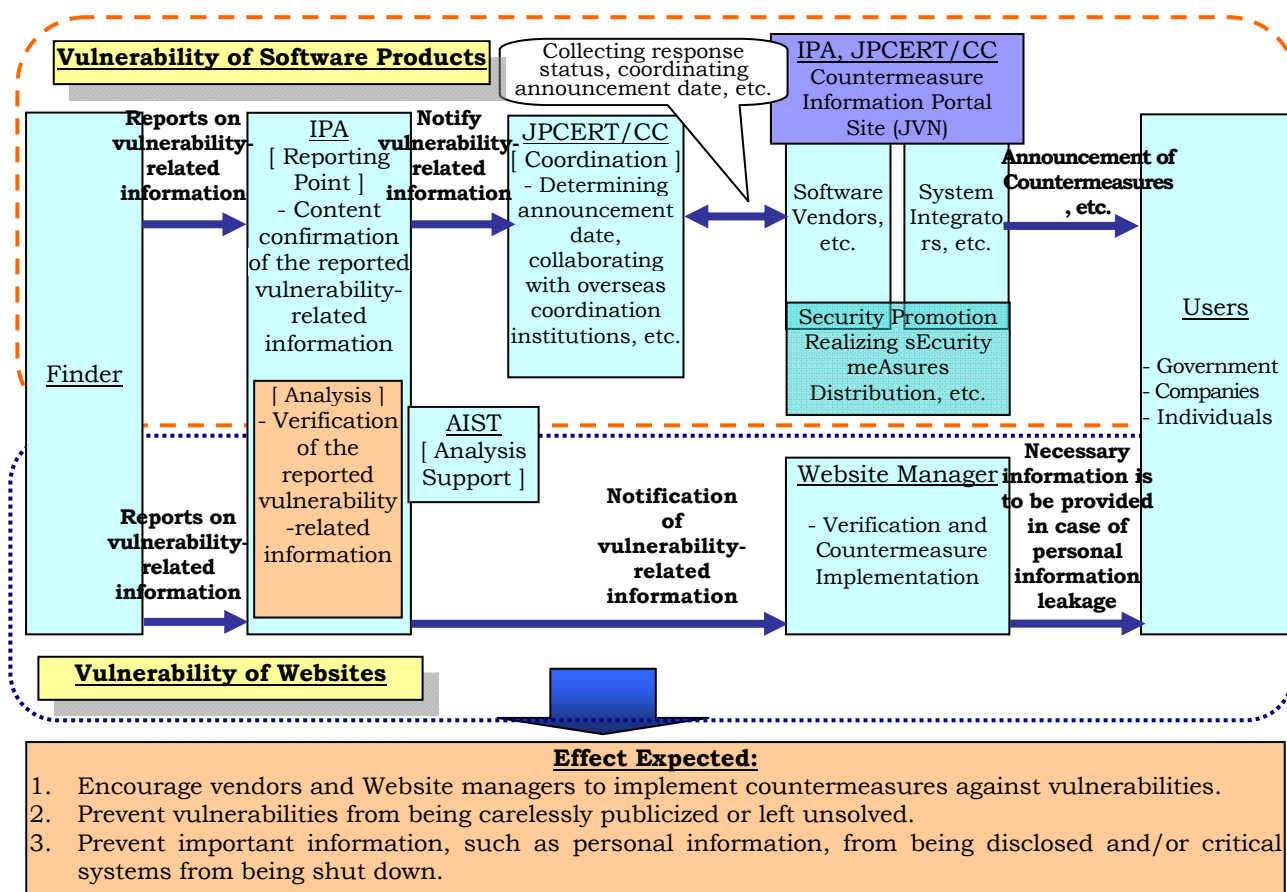
With the authority given by the Directive, IPA has been collecting reports on the following vulnerability-related information:

1: Vulnerability-related Information about Software Products:

Vulnerabilities against client Software such as OS and browser, server Software such as Web server, Software embedded in hardware such as IC card, and so on. Other than vulnerability itself, information on verification methods, attacking methods and workarounds are also accepted. IPA will notify these vulnerability-related information to JPCERT/CC and then JPCERT/CC will communicate those information to concerned organizations such as domestic product vendors.

2: Vulnerability-related Information about Websites (Web Applications):

Vulnerabilities against Websites which provide services to the public through the Internet. IPA will notify such vulnerability-related information to Website managers to prompt modification.

Effect Expected:
1. Encourage vendors and Website managers to implement countermeasures against vulnerabilities.
2. Prevent vulnerabilities from being carelessly publicized or left unsolved.
3. Prevent important information, such as personal information, from being disclosed and/or critical systems from being shut down.

"Information Security Early Warning Partnership"
(Framework for Handling Vulnerability-related Information)

Source: Handouts from explanatory session on handling vulnerability-related information (General introduction to the standards for handling Software vulnerability-related information and its guidelines) by the Ministry of Economy, Trade and Industry

The statistics for the 3rd Quarter of 2012 (July – September) from the data collected under the framework is summarized as follows.

1. Reported Number and Handling Status of Reports:

The total number of vulnerability-related information reported to IPA from July 1 to September 30, 2012 was 197: 40 of them were about Software products and the rest of 157 were about Websites. The cumulative number of reports made to IPA since the framework started (July 8, 2004) was 7950: 1424 of them were about Software products and the rest of 6526 were about Websites. The Chart 1-1 shows the reporting status for respective quarters.
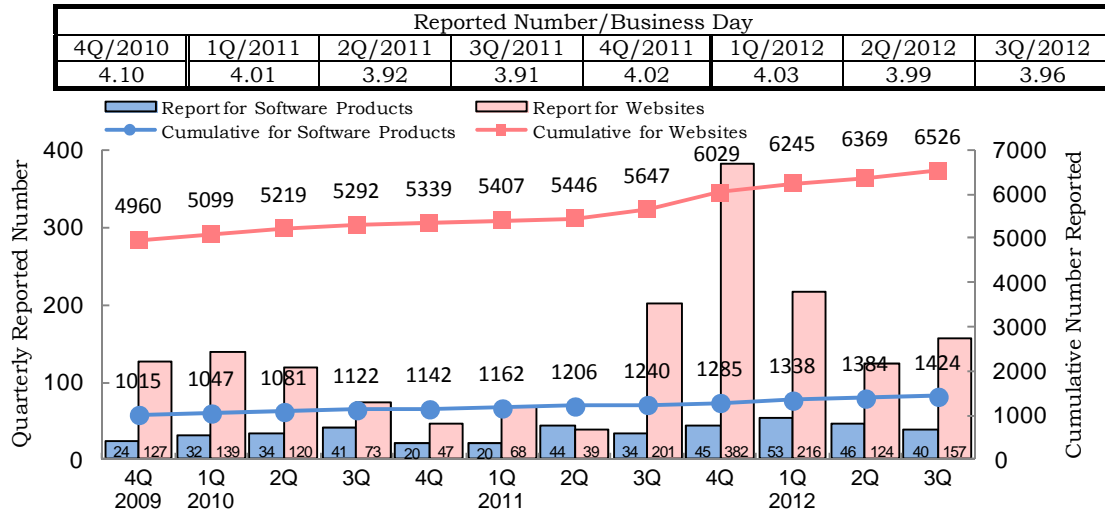
Reported Number/Business Day							
4Q/2010	1Q/2011	2Q/2011	3Q/2011	4Q/2011	1Q/2012	2Q/2012	3Q/2012
4.10	4.01	3.92	3.91	4.02	4.03	3.99	3.96

Chart 1-1: Quarterly Number of Vulnerability-related Information

The Chart 1-2 shows the processing status of reports on the vulnerability-related information as of the end of September, 2012. As for Software products, 55% (667) of the reports being accepted as vulnerability (1221) have been fixed and publicized. As for Websites, 70% (4436) of the reports being accepted as vulnerability (6364) have been fixed.
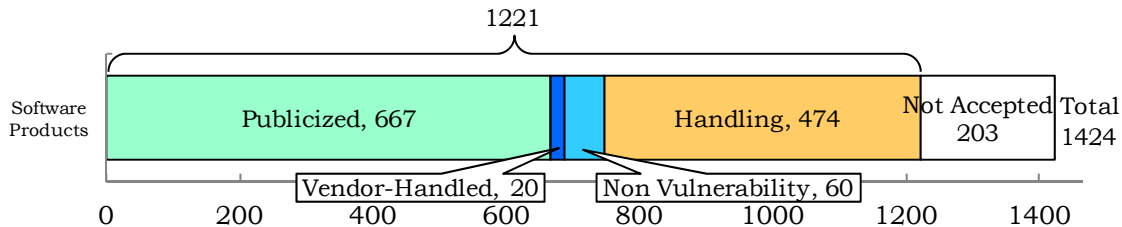
Publicized   : Vulnerability which has been publicized with vendor's responding status on JVN
Vendor-Handled   : Vulnerability which has been informed to each user by vender individually
Non Vulnerability : Vulnerability which has been determined not to be vulnerability by vendor
Handling   : Vulnerability which is being studied/handled by vendor
Not Accepted   : Vulnerability which is outside the scope defined by the Directive of METI
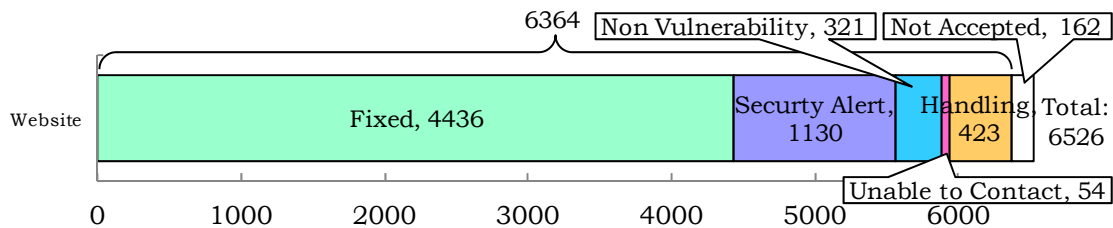
Fixed   : Vulnerability fixed by Website manager
Security Alert   : Handling was called off after countermeasure against the vulnerability is urged widely with the Security Alert by IPA
Non Vulnerability : Vulnerability which has been determined not a vulnerability by Website manager
Unable to Contact : It is not possible to contact the Website manager
Handling   : Vulnerability which is being studied/handled by Website manager
Not Accepted   : Vulnerability which is outside the scope defined by the Directive of METI

**Chart 1-2: Processing Status of Reporting for Vulnerability-related Information
(As of the end of September, 2012)**

2

2. Handling of Vulnerability-related Information on Software Products and its Coordination:

The total number of information related to vulnerabilities in Software Products reported to IPA since the framework started in July 8, 2004, was 1424. The Chart 2-1 shows the breakdown of 667 of publicized vulnerabilities, and the Chart 2-2 shows the breakdown of 1221 reports related to the vulnerabilities in Software products.
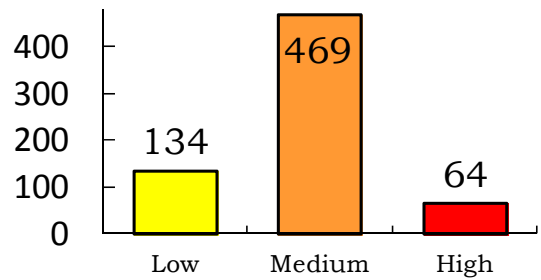
The vulnerabilities are organized according to their severity, determined by the Common Vulnerability Scoring System (CVSS v2) standard. The scale of low, medium, and high severity corresponds to the following scores:

Chart 2-1 : Severity of Vulnerabilities in Software Products
(from Initial Acceptance to the end of September, 2012)

Low   - Vulnerabilities will be labeled the Low severity if they have a CVSS base score of 0.0 - 3.9 .
Medium - Vulnerabilities will be labeled the Medium severity if they have a CVSS base score of 4.0 - 6.9 .
High   - Vulnerabilities will be labeled the High severity if they have a CVSS base score of 7.0 - 10.0 .

The most reported type of software was Web application and subsequently followed by Web Browser and those listed below.
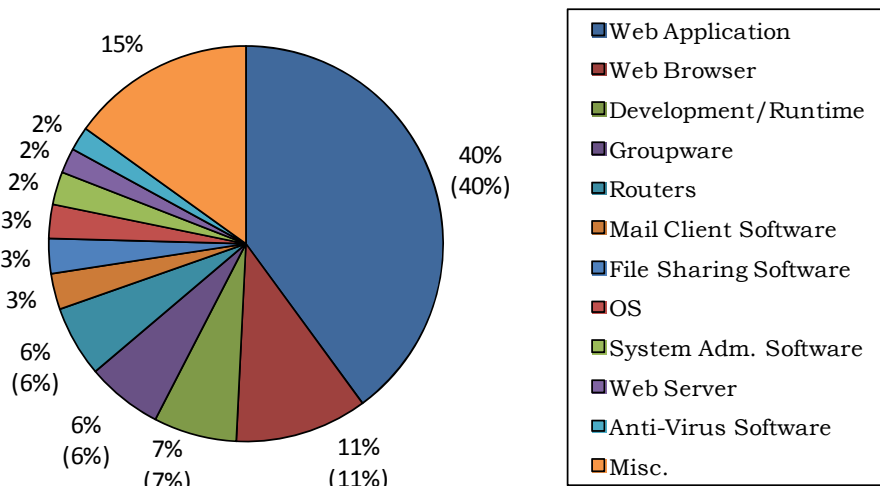
Misc. in this graph includes Software for Database, etc.
(Breakdown of 1221: Numbers in parenthesis are for the previous quarter)

**Chart 2-2: Breakdown of the Vulnerabilities in Software Products
(from July 8, 2004 to the end of September, 2012)**

The Chart 2-3 shows the time required for the announcement of vulnerabilities in Software products. 35% of the reports was addressed within 45 days from its initial reporting to announcement.
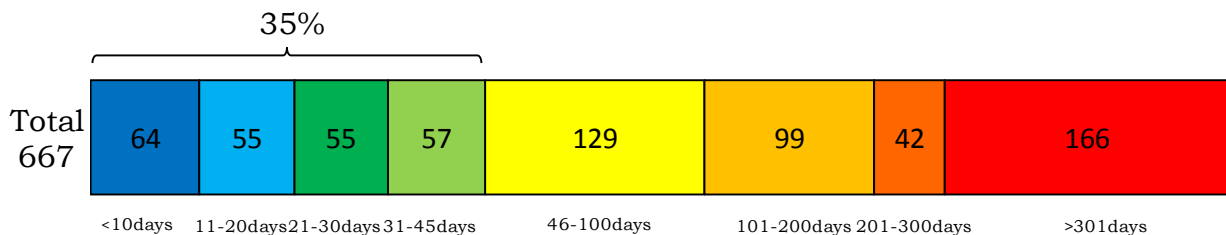
Total 667	64	55	55	57	129	99	42	166
	<10days	11-20days	21-30days	31-45days	46-100days	101-200days	201-300days	>301days

Chart 2-3: Time Required for the Announcement of Vulnerabilities in Software Products

In this Quarter, 28 vulnerabilities were announced.

3. Handling of Vulnerability-related Information on Websites:

The number of information related to vulnerabilities in websites reported to IPA since the framework started in July 8, 2004, was 6526.Removing those not accepted as vulnerabilities, the total number of the vulnerabilities was 6364. Chart 3-1 shows the breakdown of the vulnerabilities found in last two years and Chart 3-2 shows the quarterly shift in their proportion.
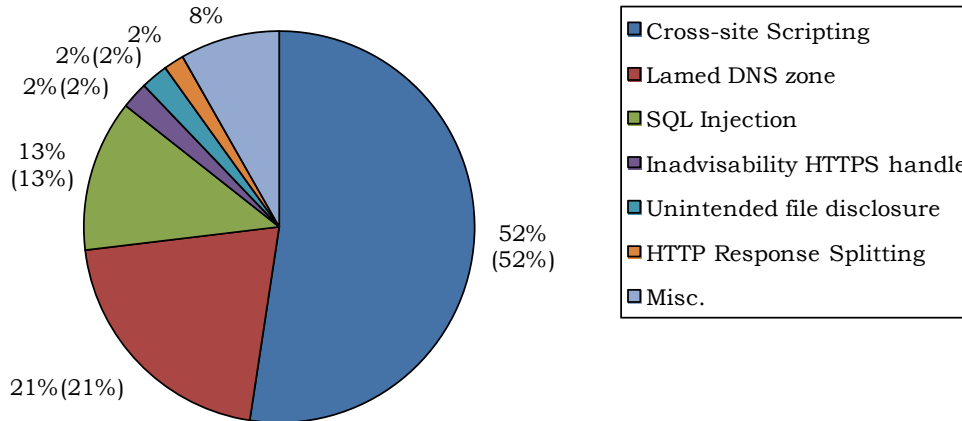
- Breakdown of 6364: Numbers in the parenthesis are for the previous quarter

Chart 3-1: Breakdown of Vulnerabilities in Websites by Type
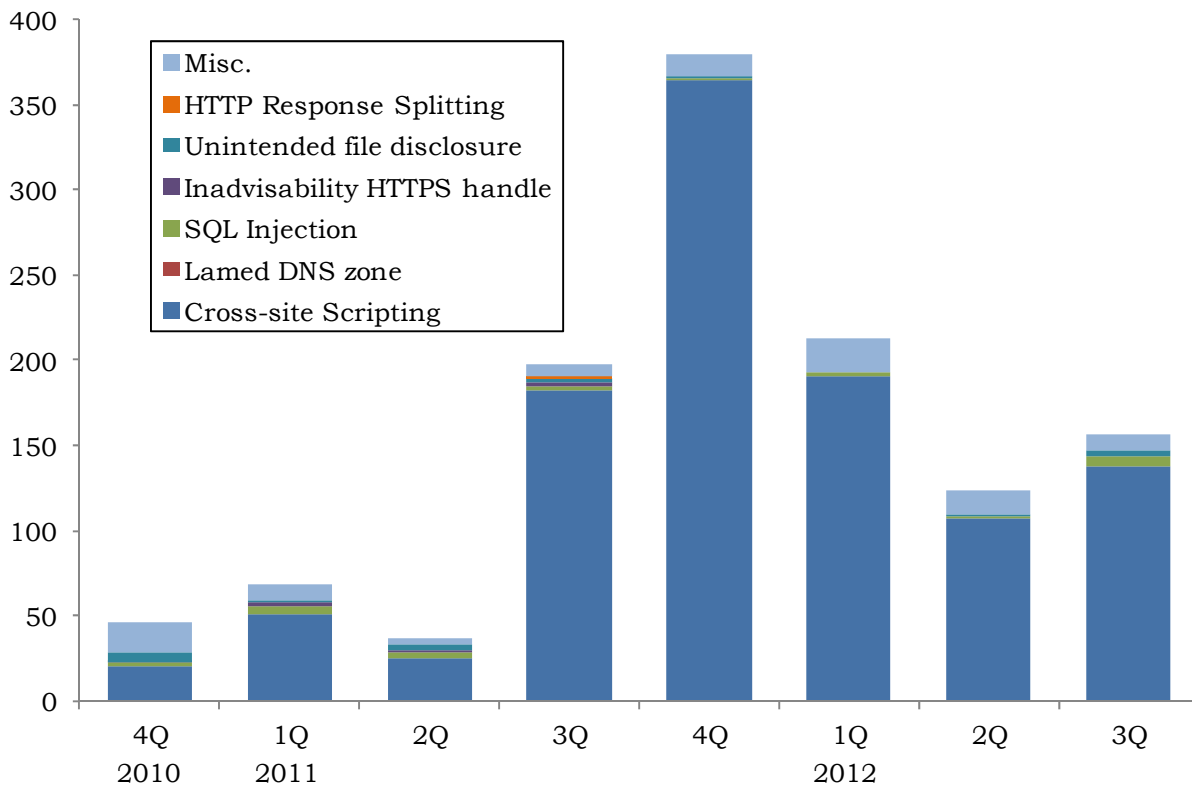**(from July 8 2004, to the end of September, 2012)**

Chart 3-2: Shift in Number of Vulnerabilities in Websites by Type
(from October 1 2010, to the End of September, 2012)

As for the type of vulnerabilities, "Cross-site Scripting", "Lamed DNS zone" and "SQL Injection" account for 86% of the entire vulnerabilities.

The Chart 3-3 and 3-4 show the time required to fix vulnerabilities by type after notification of detailed information of the vulnerabilities to Website managers. 66% of vulnerabilities reported was fixed within 90 days.
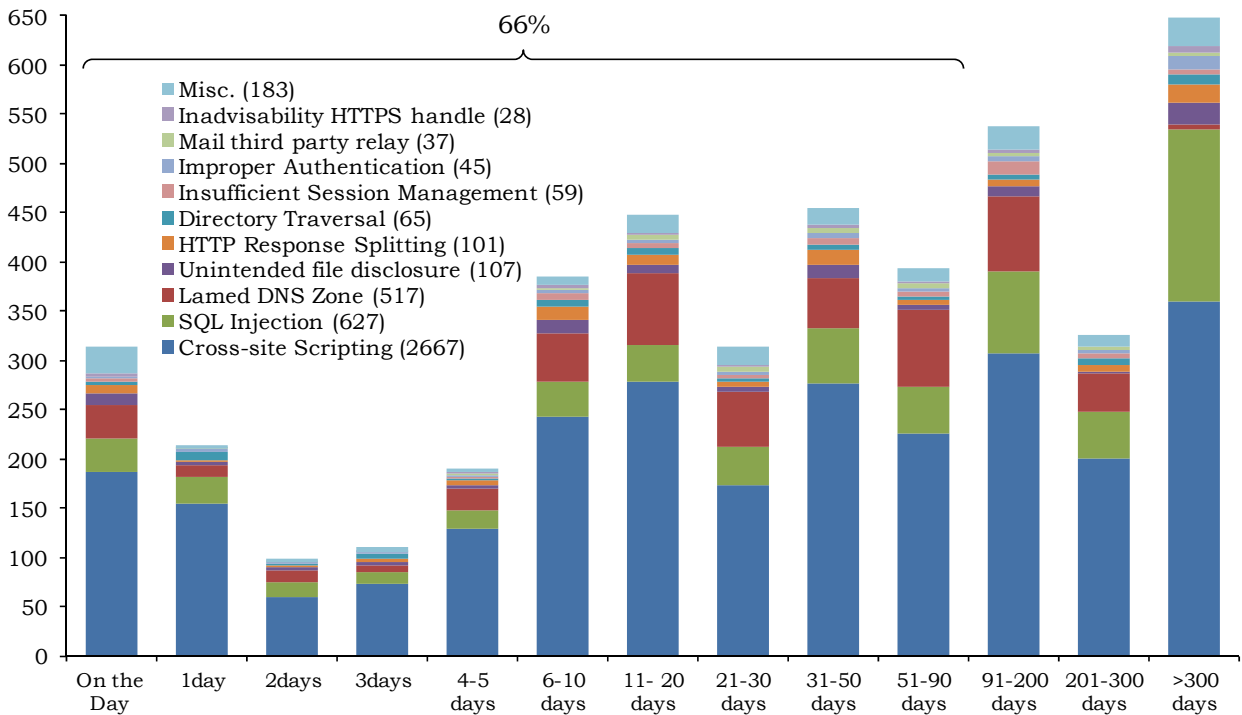

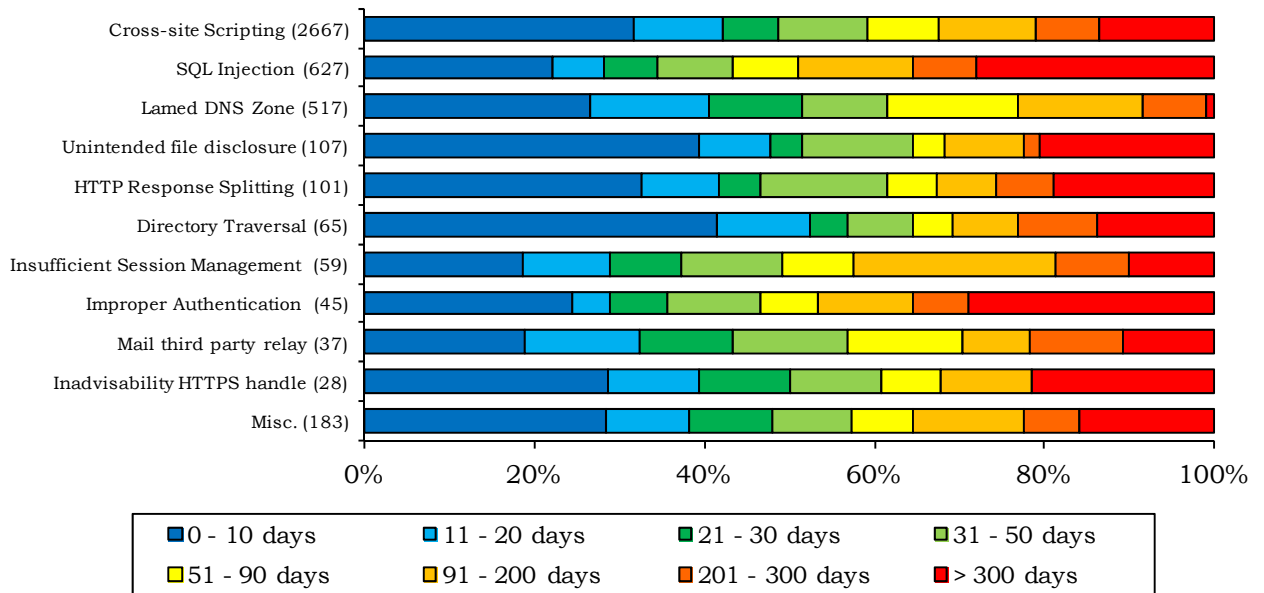**Chart 3-3: Time Required to Fix Vulnerabilities in Websites**

Chart 3-4: Time Required to Fix Vulnerabilities in Websites by Type