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

- 1st Quarter of 2010 (January – March) -

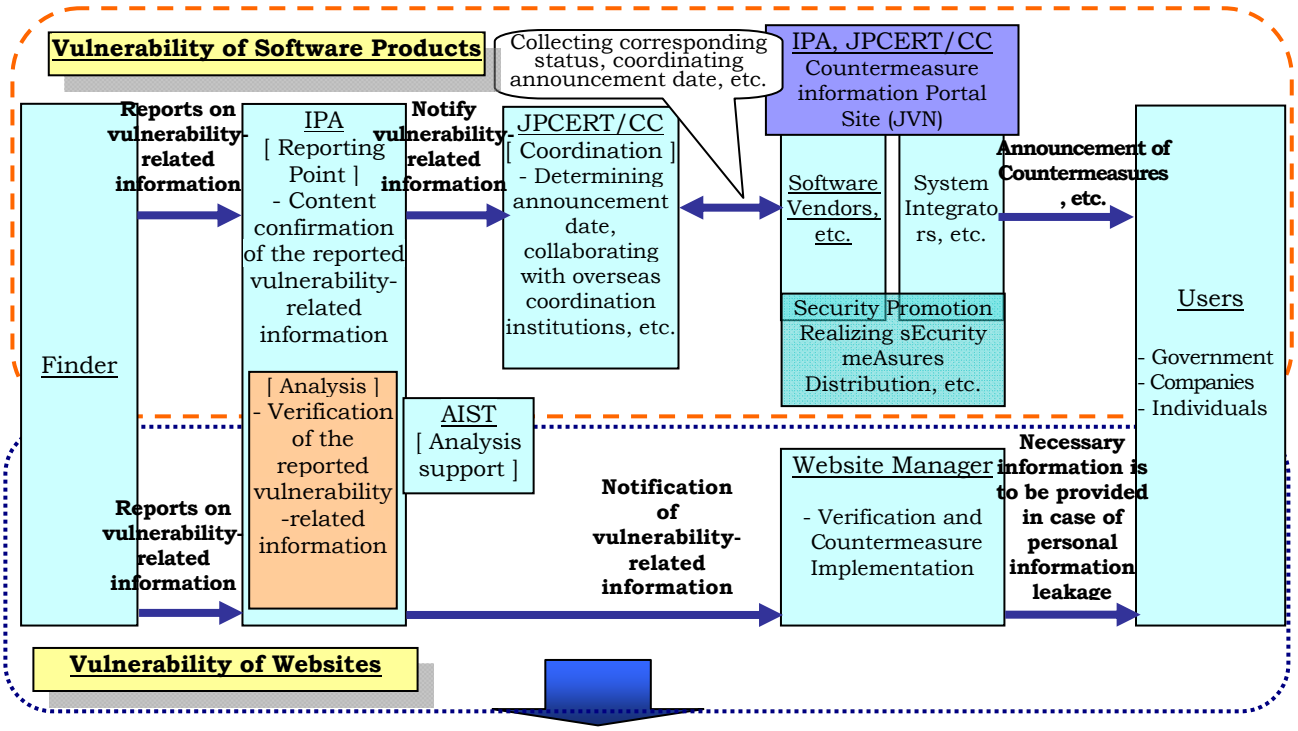
Information-technology Promotion Agency, Japan (IPA) and Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), initiated to handle vulnerability-related information in July, 2004, pursuant to the Standards for Handling Software Vulnerability Information and Others (Directive #235, 2004) by the Ministry of Economy, Trade and Industry (METI).
With the authority given by the Directive, IPA has been accepting 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 it will communicate those information to concerned organizations such as domestic 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 1st Quarter of 2010 (January – March) derived from the data collected based on 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 January 1 to March 31, 2010 was 171: of 32 were on Software products and the rest of 139 were on Websites. The cumulative number of reports made to IPA since the framework started (July 8, 2004) was 6148: of 1050 were on Software products and the rest of 5098 were on Websites. The Chart 1-1 shows the reporting status for respective quarters.

Reported Number/Business Day									
1Q/2007	1Q/2008	2Q/2008	3Q/2008	4Q/2008	1Q/2009	2Q/2009	3Q/2009	4Q/2009	1Q/2010
1.95	2.24	2.38	2.79	4.00	4.53	4.66	4.56	4.47	4.40

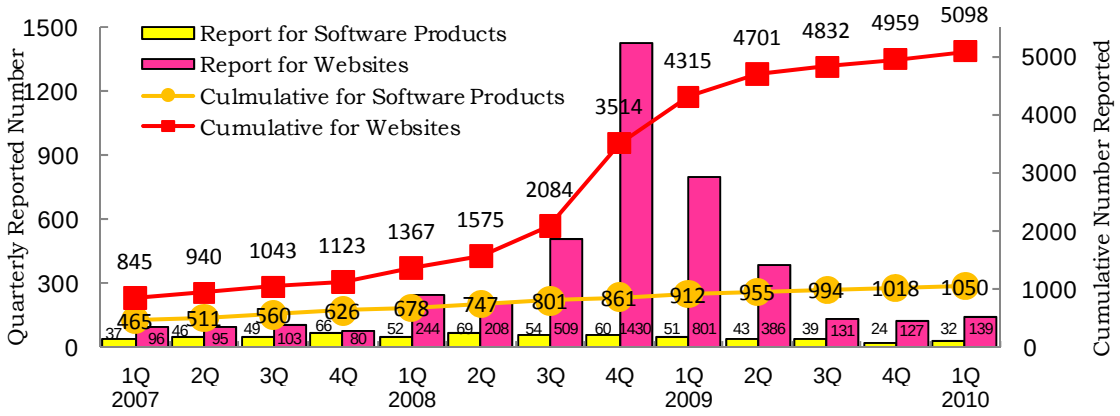
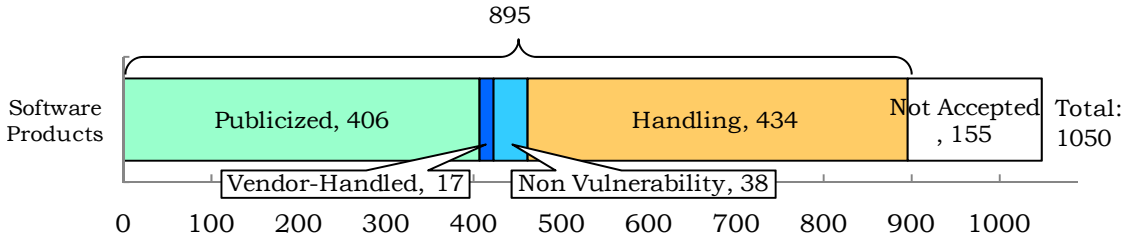
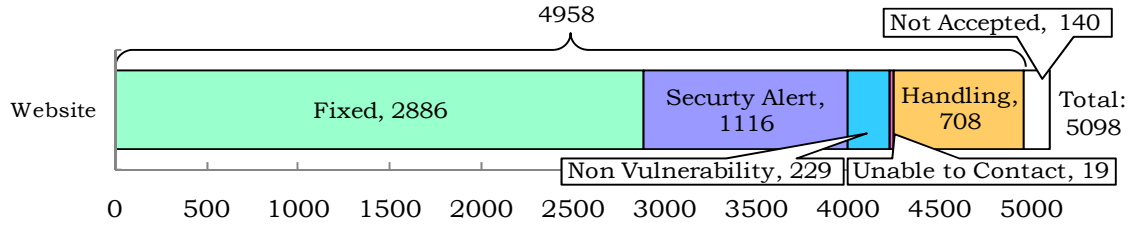


Chart 1-1: Quarterly Number of Vulnerability-related Information

The Chart 1-2 shows the processing status of reports on the vulnerability-related information as of the end of March, 2010. As for Software products, 45% (406) of the reports being accepted as vulnerability (895) are fixed and publicized. As for Websites, 58% (2886) of the reports being accepted as vulnerability (4958) are 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	: It is canceled handling, after countermeasure against the vulnerability is urged widely with the Security Alert by IPA
Non Vulnerability	: Vulnerability which has been determined not to be 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 March, 2010)

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 1050. The Chart 2-1 shows the breakdown for 406 of publicized vulnerabilities, and the Chart 2-2 shows the breakdown for 895 reports related to the vulnerabilities in Software products.

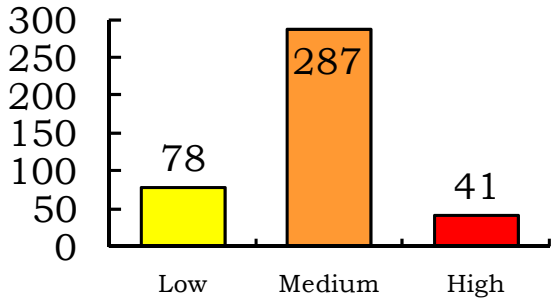
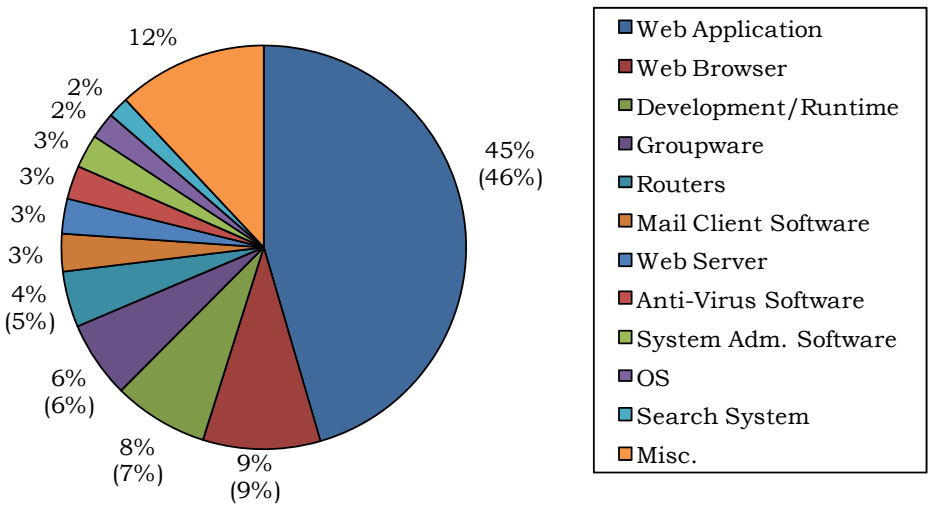


Chart 2-1 : Severity of Vulnerabilities in Software Products
(from Initial Acceptance to the end of March, 2010)

The vulnerabilities are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS v2) standard. The scale of low, medium, and high severity corresponds to the following scores:

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 was Web application and Web Browser subsequently followed.



Misc. in this graph includes Software for Peripheral Device, Word-processing Software, File Sharing Software, Database, etc.
(Breakdown of 895: Numbers in parenthesis are for previous Quarter)

Chart 2-2: Breakdown for the Vulnerabilities in Software Products (from July 8, 2004 to the end of March, 2010)

The Chart 2-3 shows the time required for the announcement of vulnerabilities in Software products. 35% of reports was addressed within 45 days from its initial reporting and announcement.

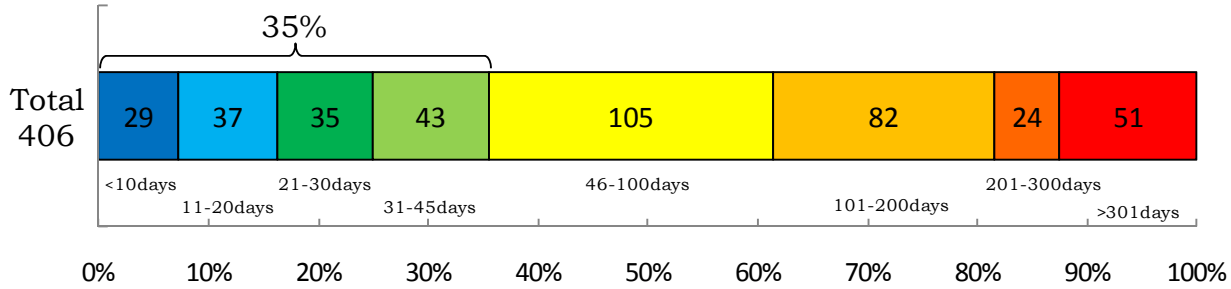
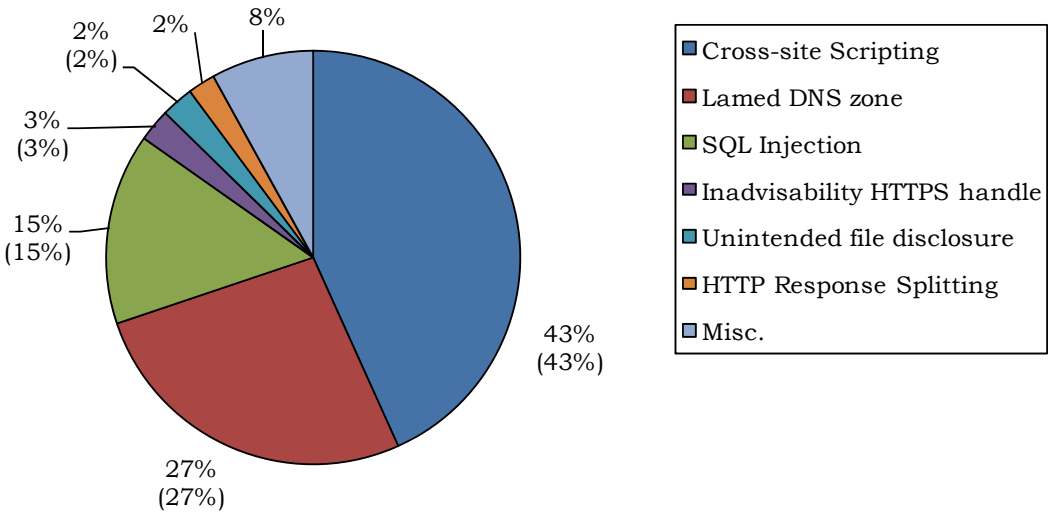


Chart 2-3: Time Required for the Announcement of Vulnerabilities in Software Products

In this Quarter, 6 vulnerabilities were being publicized.

3. Handling of Vulnerability-related Information for Websites:

The total number of information related to vulnerabilities in Websites reported to IPA since the framework started in July 8, 2004, was 5098: excluding those being determined not to be vulnerability, the breakdowns for 4958 information reported are shown in the Chart 3-1 and 3-2.



- Breakdown of 4958: 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 March, 2010)

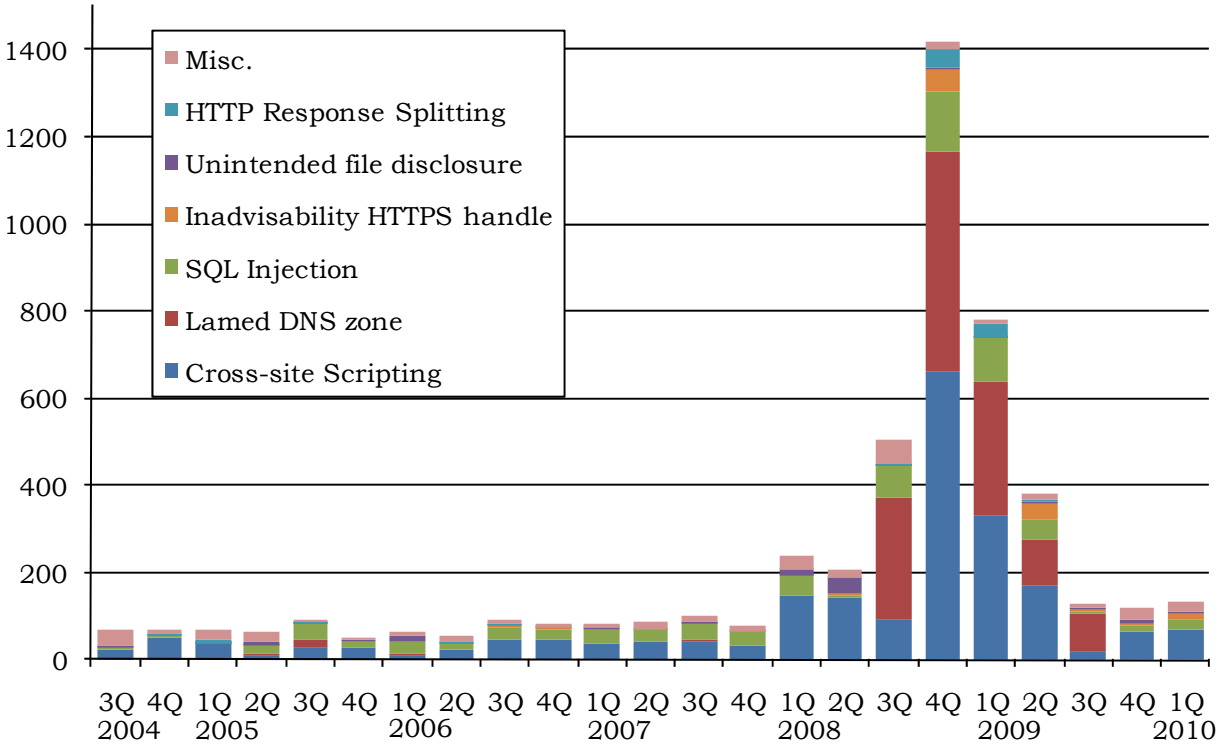


Chart 3-2: Shift in Number of Vulnerabilities in Websites by Type (from July 8 2004, to the End of March, 2010)

As for the type of vulnerabilities, “Cross-site Scripting”, “Lamed DNS zone” and “SQL Injection” account for 85% of the entire vulnerabilities.

The Chart 3-3 and 3-4 show the time required to modify vulnerabilities by type after notification of detailed information of the vulnerabilities to Website managers. 70% of vulnerabilities reported was fixed within 90 days.

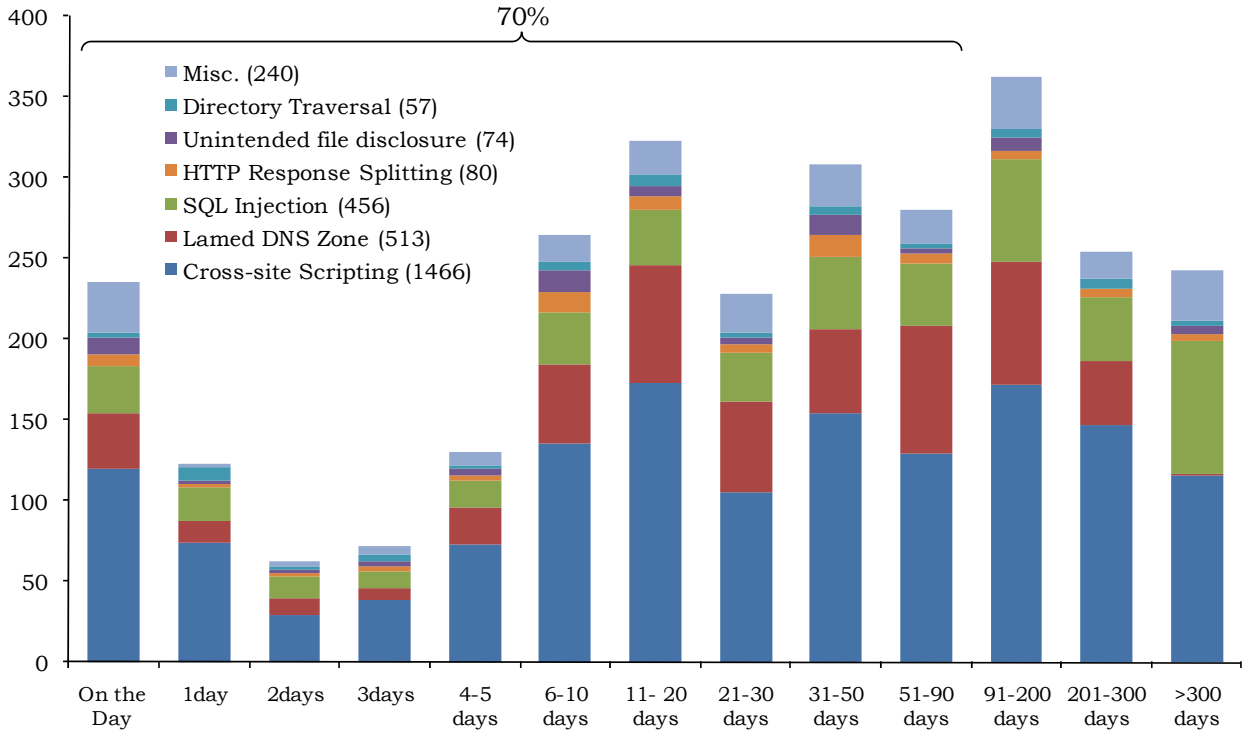


Chart 3-3: Time Required to Fix Vulnerabilities in Websites

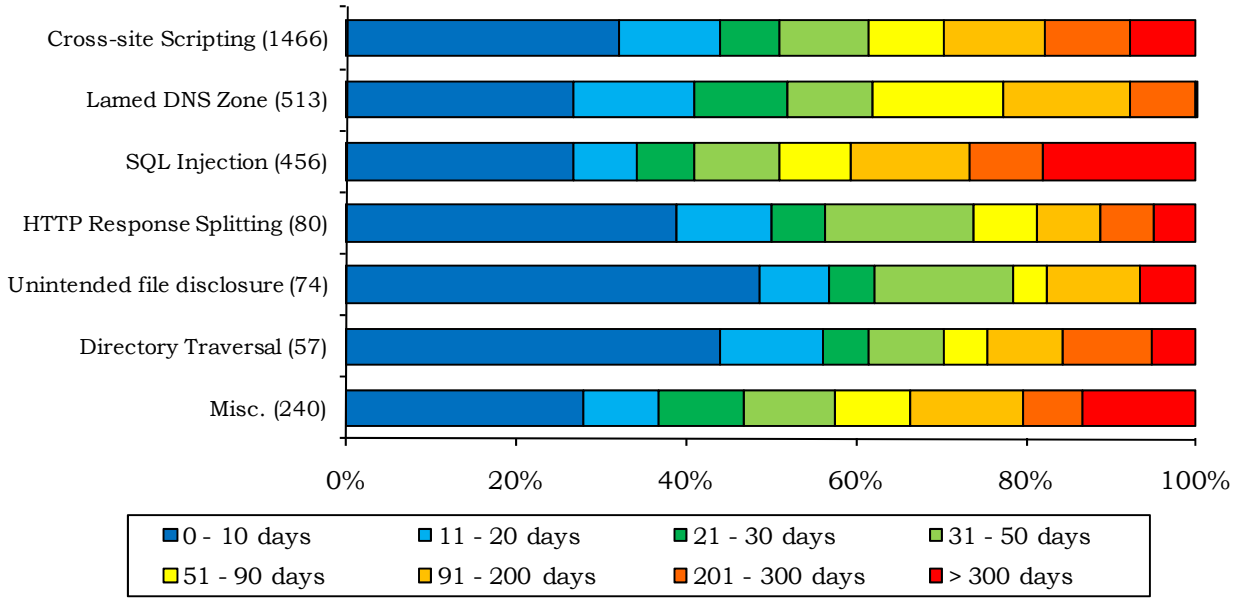


Chart 3-4: Time Required to Fix Vulnerabilities in Websites by Type

Contact

IT Security Center, Information-technology Promotion Agency, Japan (IPA/ISEC)
Tel : +81-(0)3-5978-7527
Fax : +81-(0)3-5978-7518
E-mail : isec-info@ipa.go.jp