Reporting Status of Vulnerability-related Information for Software Products, etc.

- 3rd Quarter of 2007 (July – September) -

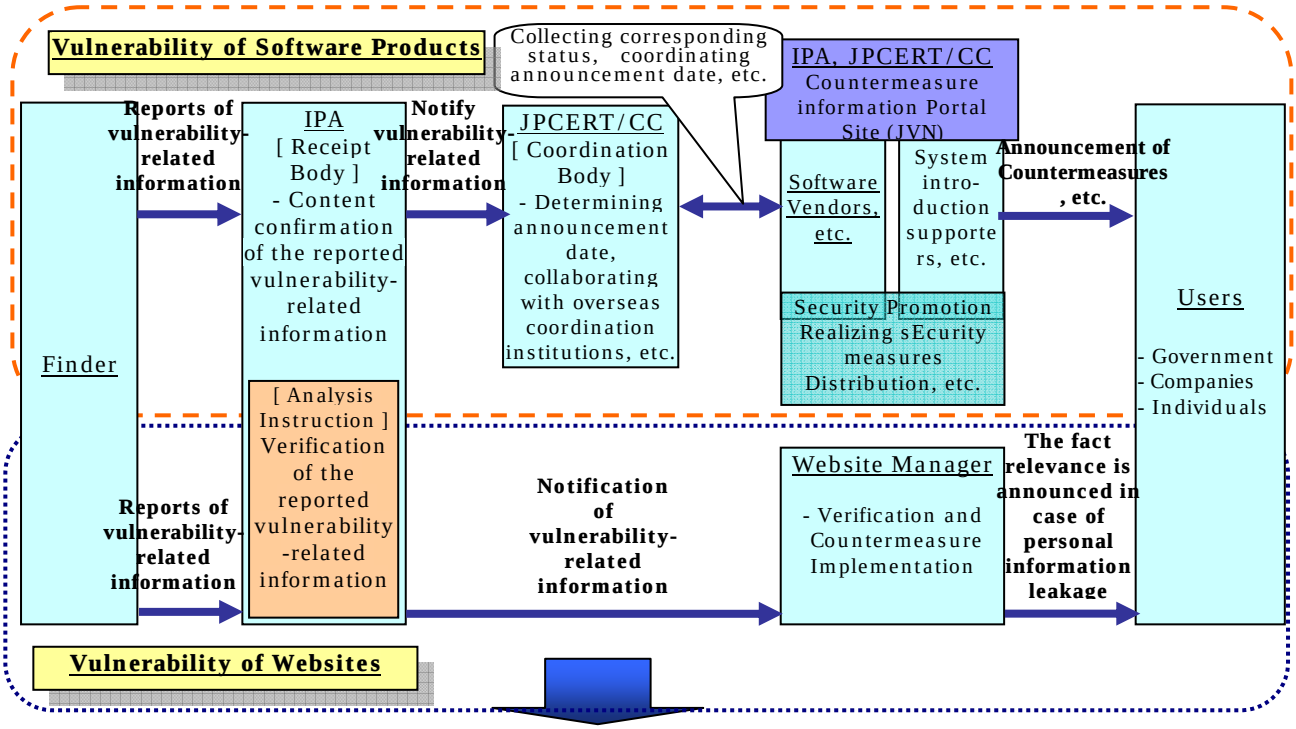
Information-Technology Promotion Agency, Japan (IPA) and JPCERT Coordination Center (JPCERT/CC), a limited intermediate corporation, have initiated to handle vulnerability-related information from July, 2004 based on the announcement "Standard for Handling Vulnerability-related Information for Software Products, etc. (#235, Announcement of METI, 2004) by the Ministry of Economy, Trade and Industry (hereinafter refers to METI).
Based on the announcement, IPA is accepting reports for following vulnerability-related information:

1: Vulnerability-related Information for Software Products:

Vulnerabilities against software on clients such as on OSs and/or on browsers, software on servers such as Web servers, software embedded hardware such as IC cards, etc. Other than the information for vulnerability itself, information for verification method, attacking method and method for workaround are also accepted. IPA will notify such vulnerability-related information to JPCERT/CC and JPCERT/CC will communicate such information to concerned organizations such as vendors, etc. in domestic.

2: Vulnerability-related Information for Website(Web Applications):

Vulnerabilities against systems which configure services unique to that site provided for public through the Internet Web sites, etc. IPA will notice such vulnerability-related information to Website managers and to prompt its modification.



Effect Expected:

1. Promote countermeasures against vulnerabilities by vendors and Website managers.
2. Restrain carelessly publicizing vulnerability related information and leaving vulnerability as they are.
3. Protect from leaking important information, i.e., private information and/or from halting important systems.

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

Source: Material for explanatory meeting for handling vulnerability-related information (General explanation for handling standard for vulnerability-related information in software and its guidelines) by the Ministry of Economy, Trade and Industry

Based on the framework for the vulnerability-related information described in advance, reporting status for the 3rd Quarter of 2007 (July to September) is summarized as follows.

1. Reported Number and Handling Status of Reports:

The reported number in relation to vulnerability-related information reported to IPA from July 1 to September 30, 2007 was 152: of 49 was for vulnerability-related software products and the rest of 103 was for vulnerability-related Website. The cumulative reported number from the initiation of acceptance of reporting (July 8, 2004) was 1603: of 560 was for vulnerability-related software products and the rest of 1043 was for vulnerability-related Website. The Chart 1-1 shows the reporting status for respective quarters.

Reported Number/Business Day						
1Q/2006	2Q/2006	3Q/2006	4Q/2006	1Q/2007	2Q/2007	3Q/2007
1.61	1.70	1.75	1.92	1.95	1.98	2.03

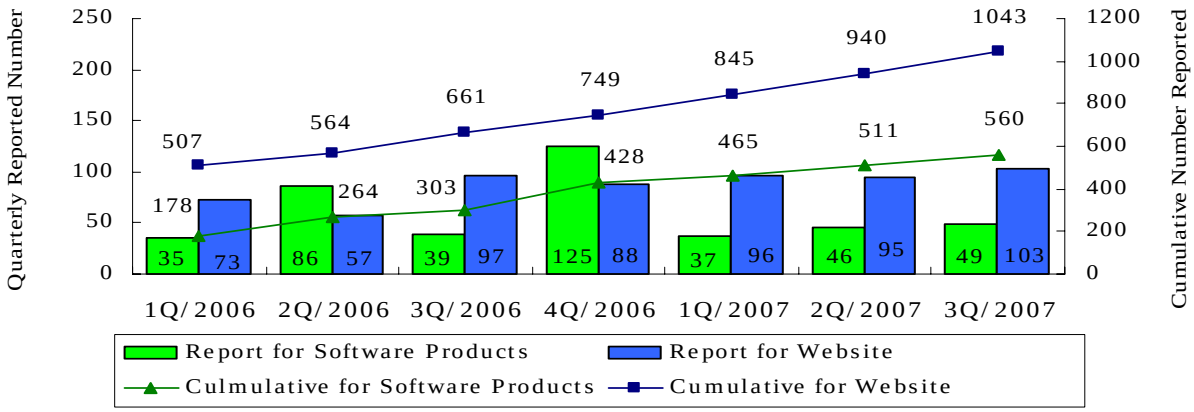
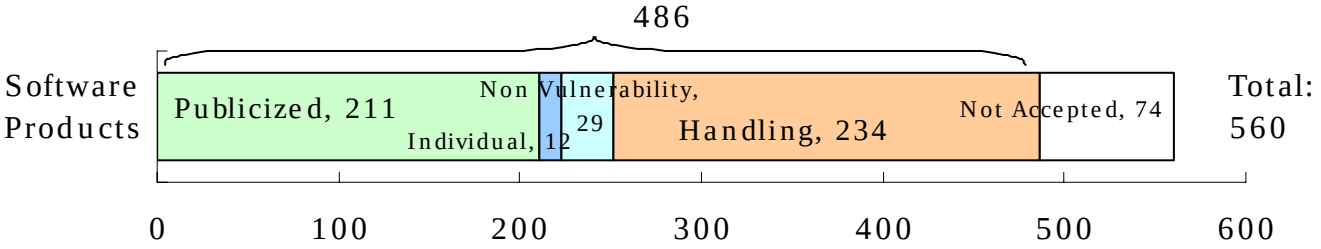
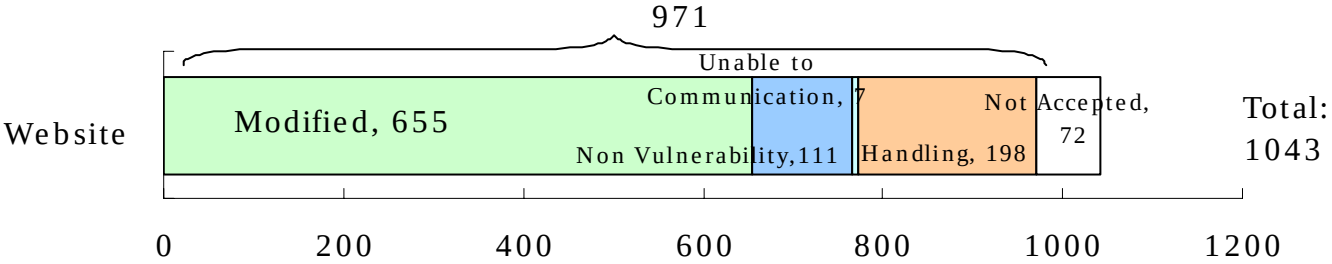


Chart 1-1: Quarterly Reported Number for Vulnerability-related Information

The Chart 1-2 shows the processing status of reports for the vulnerability-related information as of the End of September, 2007. As for software products, of 43% (211) of the reports being accepted as vulnerabilities (486) are modified and publicized. As for Website, of 67% (655) of the reports being accepted as vulnerabilities (971) are modified.



Publicized	: Vulnerability which has been publicized with vendor's responding status by JVN
Individual	: Vulnerability which has been informed to each user by vender
Non Vulnerability	: Vulnerability which has been determined not vulnerability by vendor
Handling	: Vulnerability which is being studied/responded by vendor
Not Accepted	: Vulnerability which is not applied to the subject for report defined by announcement of METI



Modified	: Vulnerability modified by Website manager
Non Vulnerability	: Vulnerability which has been determined not vulnerability by Website manager
Unable to Communicate	: It is not possible to communicate with the Website manager
Handling	: Vulnerability which is being studied/responded by Website manager
Not Accepted	: Vulnerability which is not applied to the subject for report defined by announcement of METI

Chart 1-2: Processing Status of Reporting for Vulnerability-related Information (As of the End of September, 2007)

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

The total reports as information related vulnerabilities in Software Products reported to IPA were 560. The Chart 2-1 show the breakdown for 211 of publicized, and The Chart 2-2 show the breakdown for 486 reports related to the vulnerabilities in software products reported to IPA for the dates from initial acceptance (July 8, 2004) to the End of September, 2007.

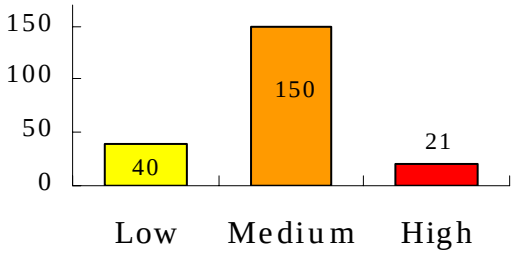
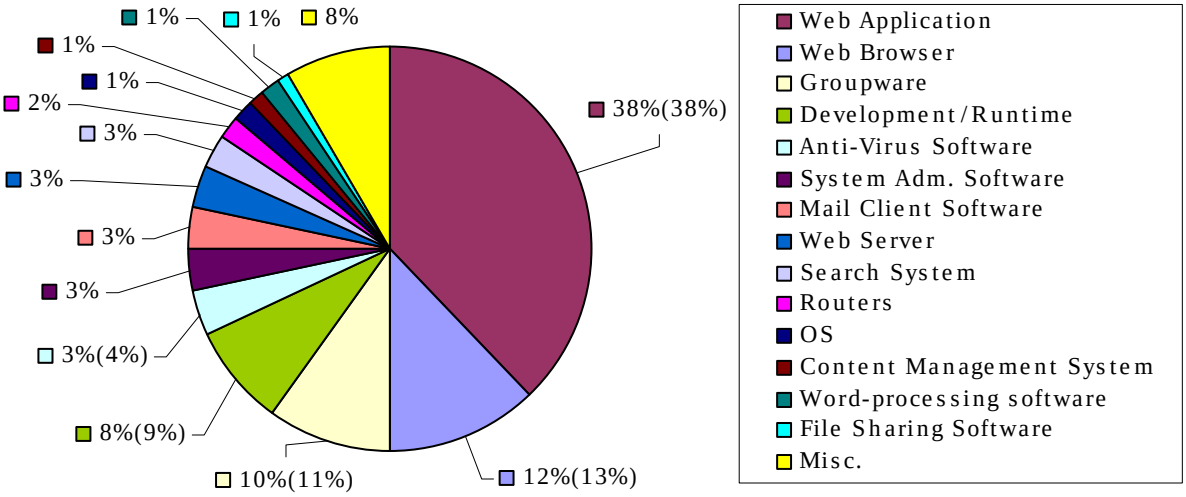


Chart 2-1: Severity of Vulnerabilities in Software Products
(from Initial Acceptance to the End of September, 2007)

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

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

The most significant reporting was for Web application and the reporting for Web Browser was subsequently followed.



Misc. in this graph include software for database, Proxy, etc.
(Breakdown of 486: Numbers in parenthesis are for previous Quarter)

Chart 2-2: Breakdown for Classification for the Vulnerabilities in Software Products (for the dates from initial acceptance to the End of September, 2007)

The Chart 2-3 shows the dates required for the announcement of vulnerabilities in software products. About 36% of reports were addressed within 45days from its initial reporting and announced.

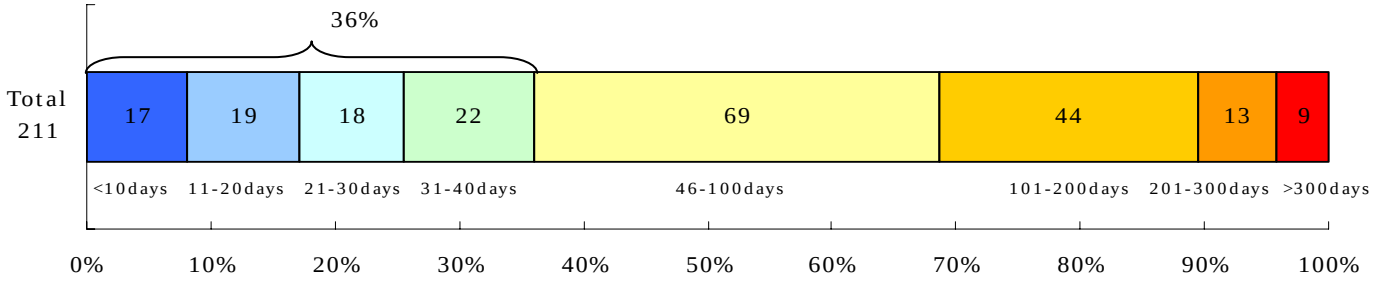
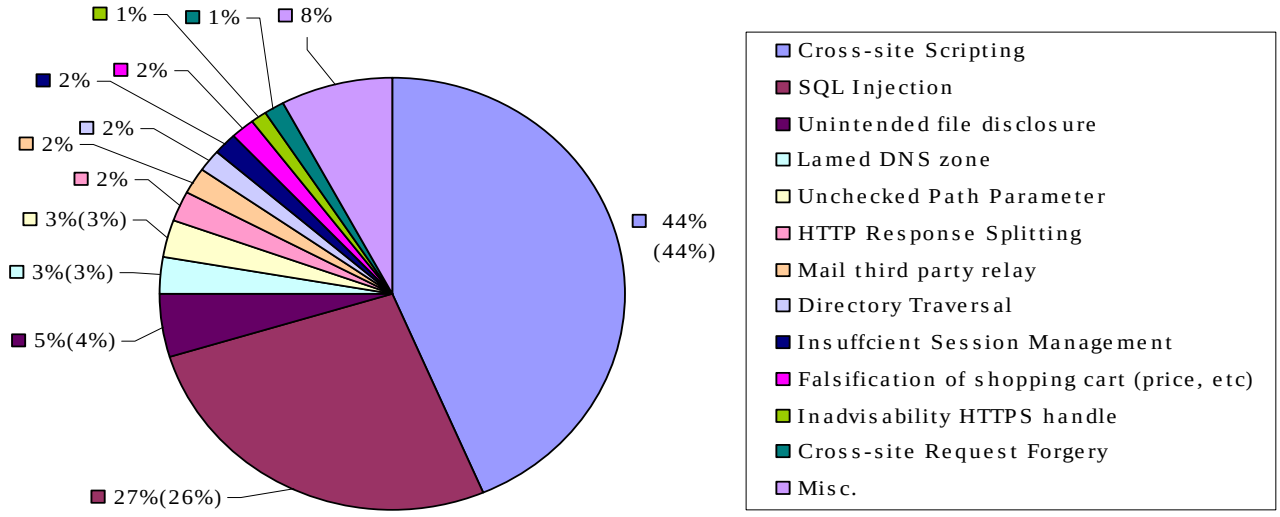


Chart 2-3: Dates Required for the Announcement of Vulnerabilities in Software Products

In this Quarter, 18 vulnerabilities were being modified.

3. Handling of Vulnerability-related Information for Website:

The total reports as information related vulnerabilities in Website reported to IPA were 1043: of 971 information related vulnerabilities in Website being reported from its initial acceptance(July 8, 2004) to the end of the 3rd Quarter of 2007 excluding those not being accepted as they were not vulnerabilities is shown in the Chart 3-1 and 3-2 .



- Breakdown of 971: Numbers in the parenthesis are for the previous Quarter

Chart 3-1: Breakdown of Vulnerabilities in Website by Type (for the dates from Initial Acceptance to the End of September, 2007)

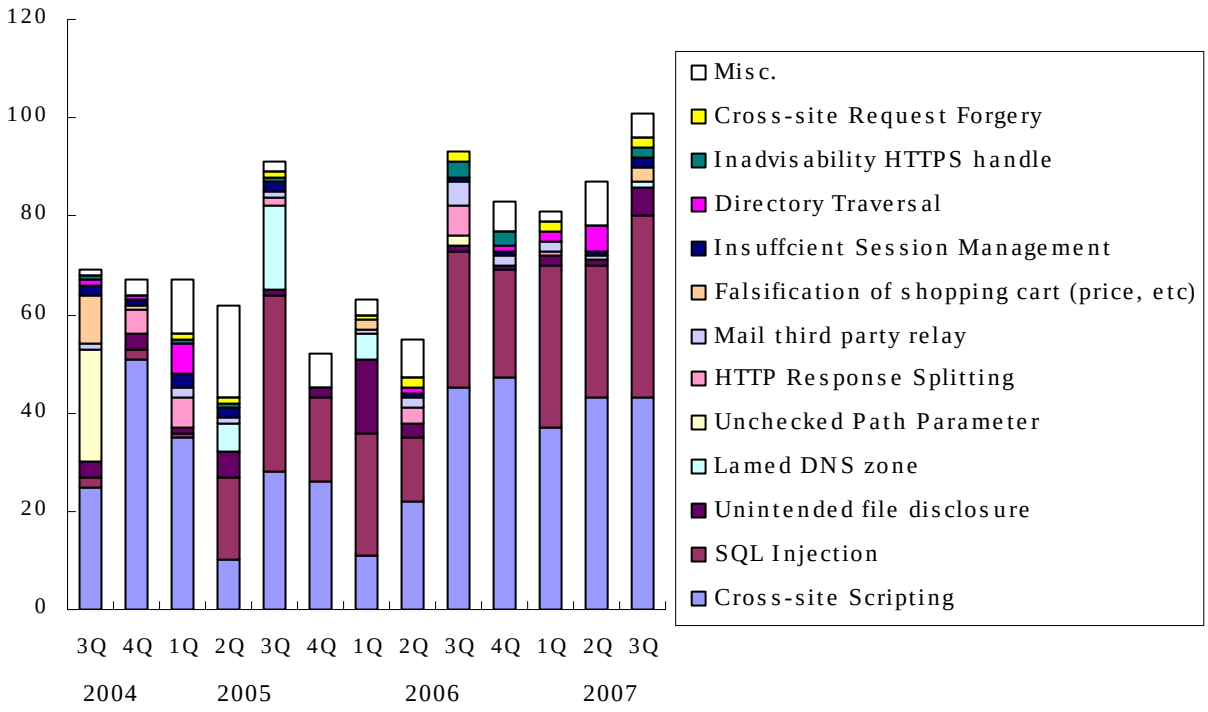


Chart 3-2: Shift in Number of Vulnerabilities in Website by Type (for the dates from Initial Acceptance to the End of September, 2007)

As for the type of vulnerabilities, “Cross-site scripting” and “SQL injection” were taken over about 70% against entire vulnerabilities.

The Chart 3-3 and 3-4 show dates required to modify vulnerabilities by type after notified detailed information of the vulnerabilities to Website managers. Of 79% of vulnerabilities reported against entire vulnerabilities reported were modified within 90 days.

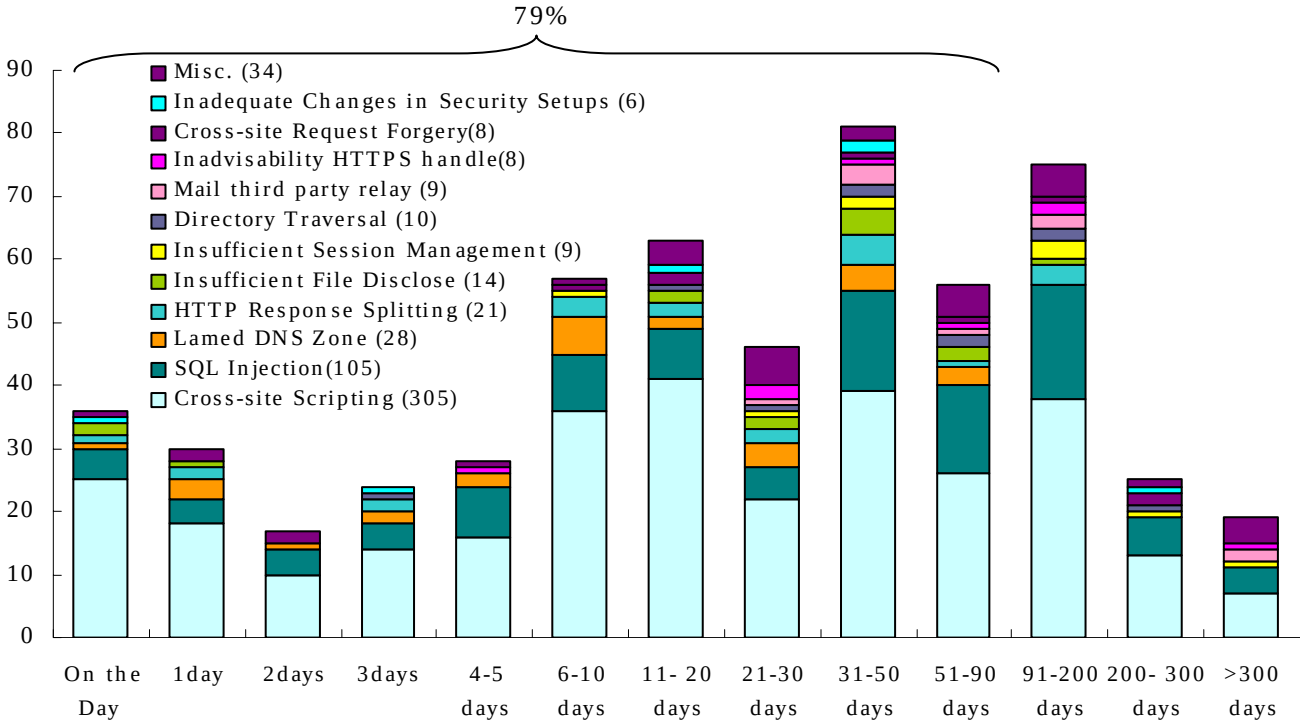


Chart 3-3: Dates Required Modifying Vulnerability in Website

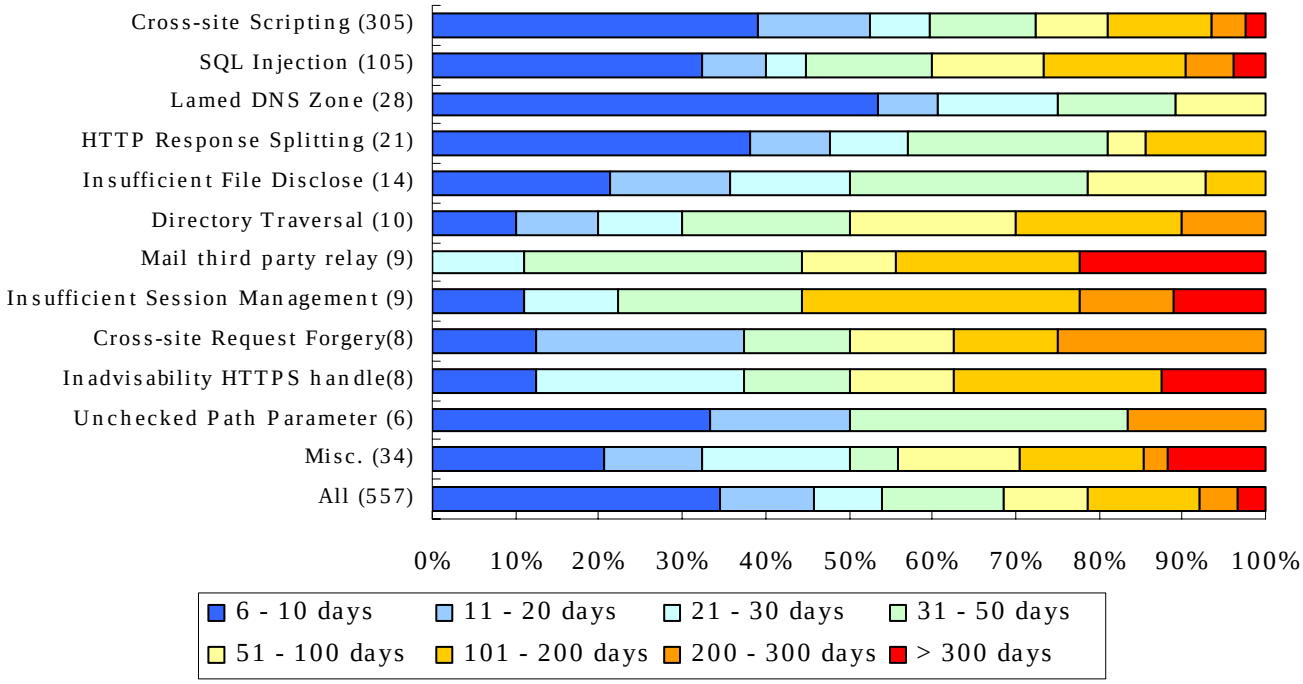


Chart 3-4: Dates Required Modifying Vulnerability in Website by Type

Contact

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