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

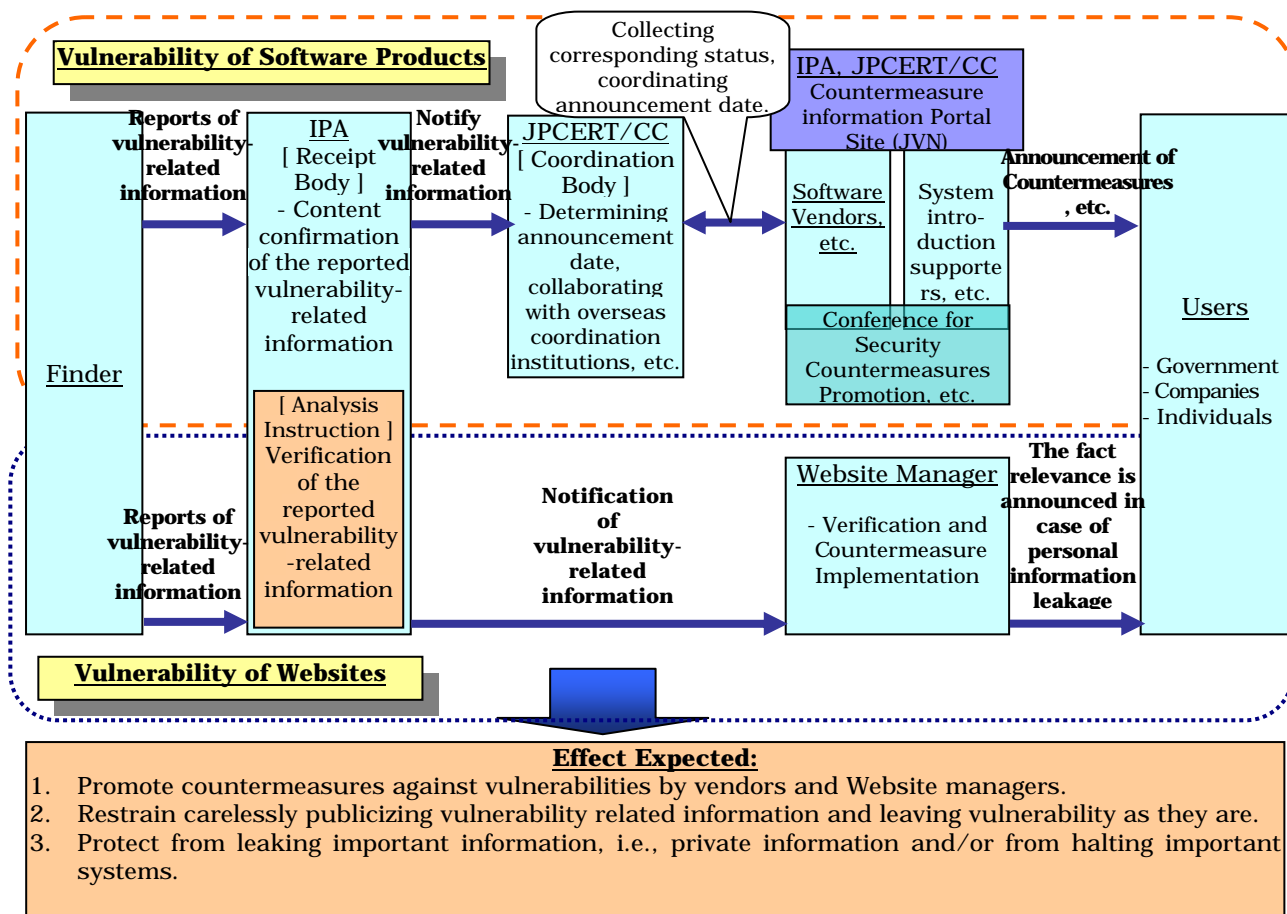### - 3rd Quarter of 2006 (July – September) -

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 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 2006 (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, 2006 was 134: of 37 was for vulnerability-related software products and the rest of 97 was for vulnerability-related Web applications.   The cumulative reported number from the initiation of acceptance of reporting (July 8, 2004) was 955: of 294 was for vulnerability-related software products and the rest of 661 was for vulnerability-related Web applications.   The Chart 1-1 shows the reporting status for respective quarters.
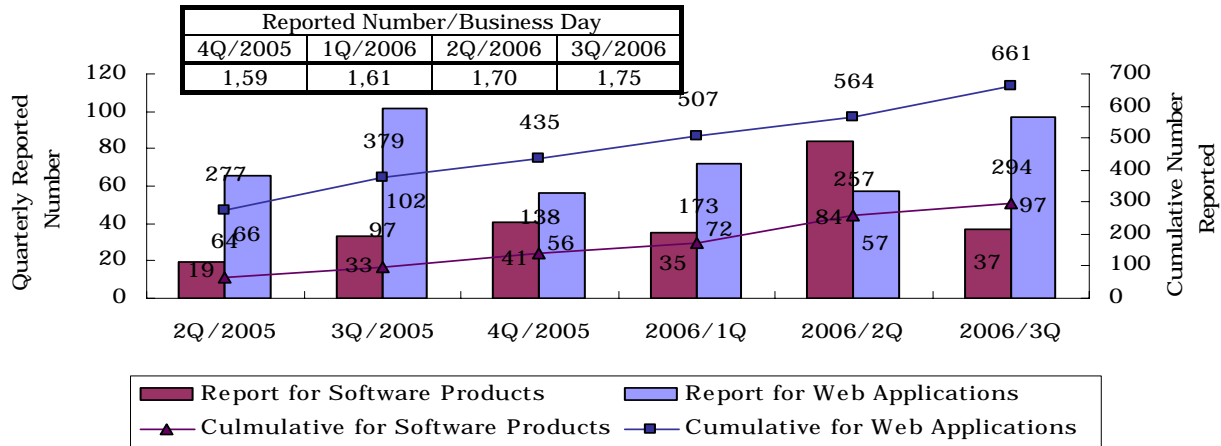
| Reported Number/Business Day | | | |
|---|---|---|---|
| 4Q/2005 | 1Q/2006 | 2Q/2006 | 3Q/2006 |
| 1,59 | 1,61 | 1,70 | 1,75 |



**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, 2006.   As for software products, of 49% (117) of the reports being accepted as vulnerabilities (241) are modified and publicized.   As for Web applications, of 57% (351) of the reports being accepted as vulnerabilities (619) are modified and publicized.
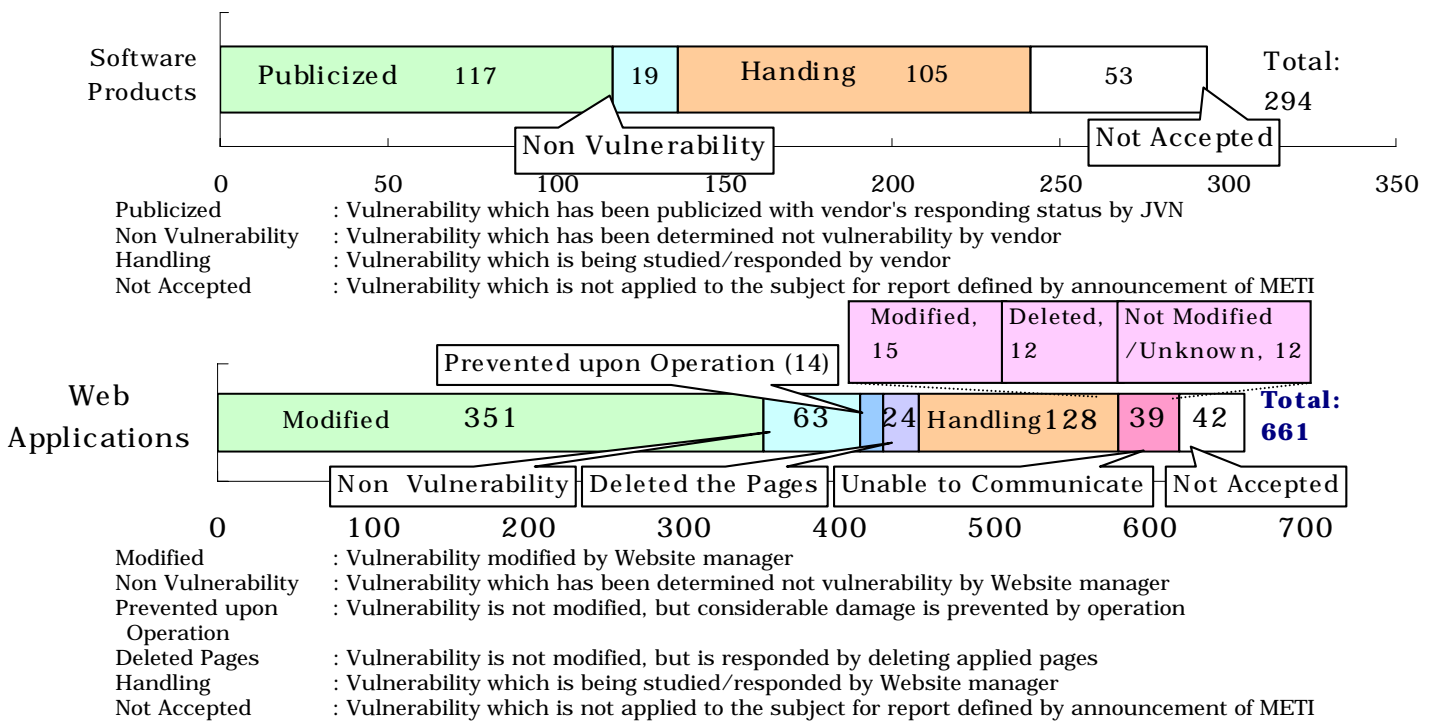


| Publicized | : Vulnerability which has been publicized with vendor's responding status by JVN |
|---|---|
| Non Vulnerability | : Vulnerability which has been determined not vulnerability by vendor |
| Handling | : Vulnerability which is being studied/responded by vendor |
| Not Accepted | : Vulnerability 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 |
| Prevented upon Operation | : Vulnerability is not modified, but considerable damage is prevented by operation |
| Deleted Pages | : Vulnerability is not modified, but is responded by deleting applied pages |
| 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, 2006)**

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

The Chart 2-1 and 2-2 show the breakdown for the 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, 2006. Reports related OSS (Open Source Software) were being increased from the 3rd Quarter of 2005. The most significant reporting was for Web application and the reporting for Web Browser was subsequently followed.
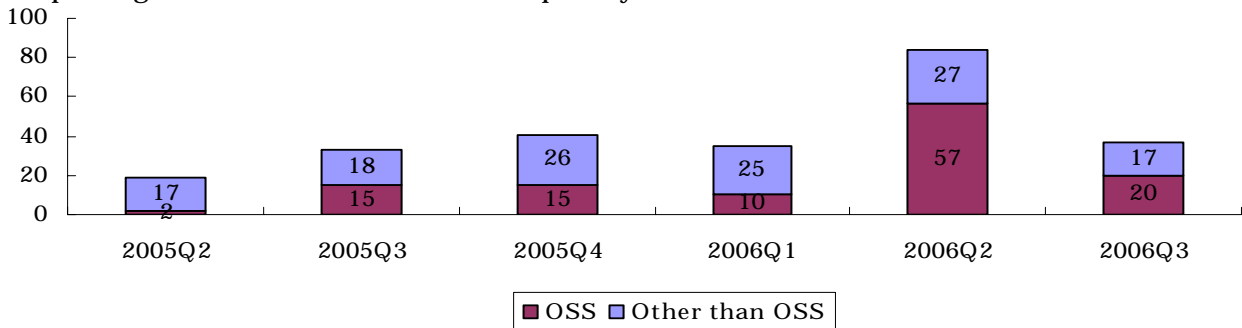


**Chart 2-1: Breakdown of Vulnerabilities in Software Products**
**(for the dates from Initial Acceptance to the End of September, 2006)**
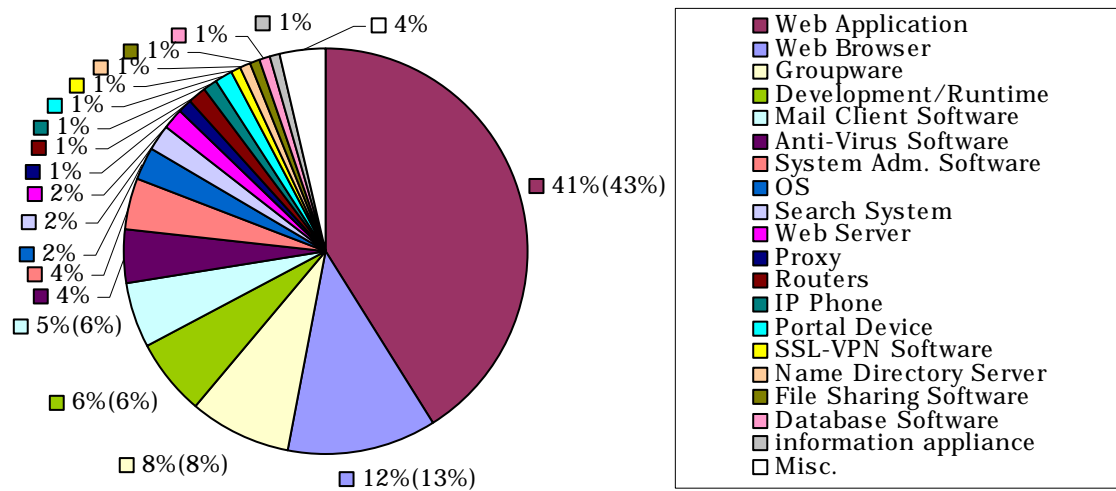


Home Appliances are included in the Misc. as they could be counted only 1 case each.
(Breakdown of 241: Numbers in parenthesis are for previous Quarter)

**Chart 2-2: Breakdown for Classification for the Vulnerabilities in Software Products**
**(for the dates from initial acceptance to the End of September, 2006)**

The Chart 2-3 shows the dates required for the announcement of vulnerabilities in software products. About 38% of reports were addressed within 45days from its initial reporting and announced.
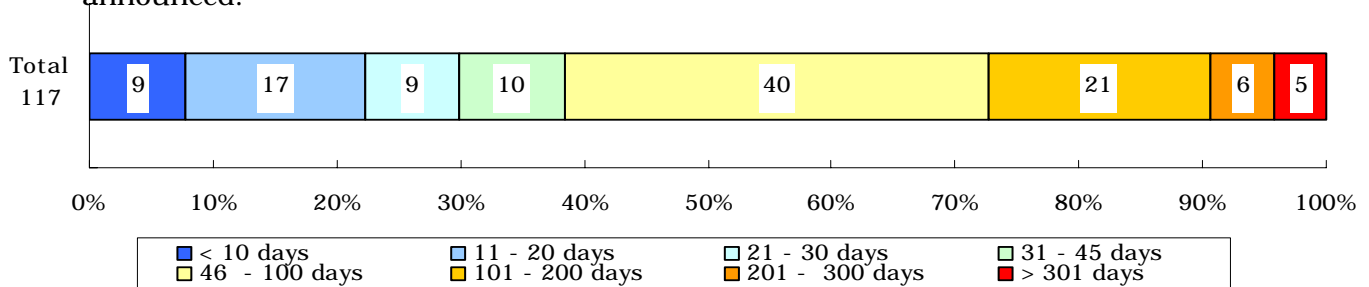


**Chart 2-3: Dates Required for the Announcement of Vulnerabilities in Software Products**

In this Quarter, 28 vulnerabilities were being modified. Of 19 were for OSS related modifications.

### 3. Handling of Vulnerability-related Information for Web Applications:

The total reports as information related vulnerabilities in Web applications reported to IPA were 661: of 619 information related vulnerabilities in Web applications being reported from its initial acceptance(July 8, 2004) to the end of the 3rd Quarter of 2006 excluding those not being accepted as they were not vulnerabilities is shown in the Chart 3-1.
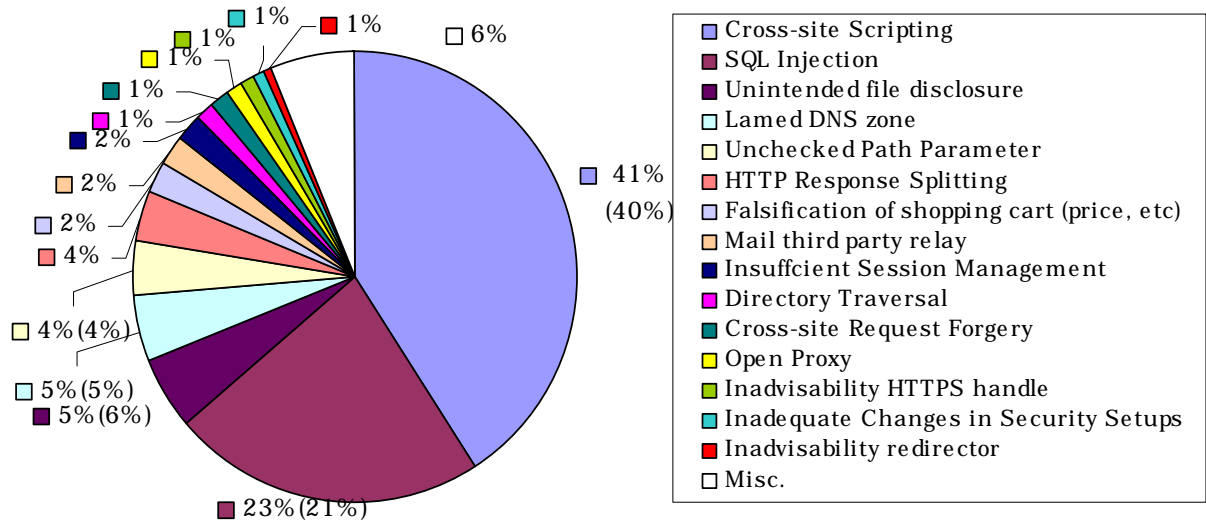


- Breakdown of 619: Numbers in the parenthesis are for the previous Quarter

**Chart 3-1: Breakdown of Vulnerabilities in Web Applications**
**(for the dates from Initial Acceptance to the End of September, 2006)**
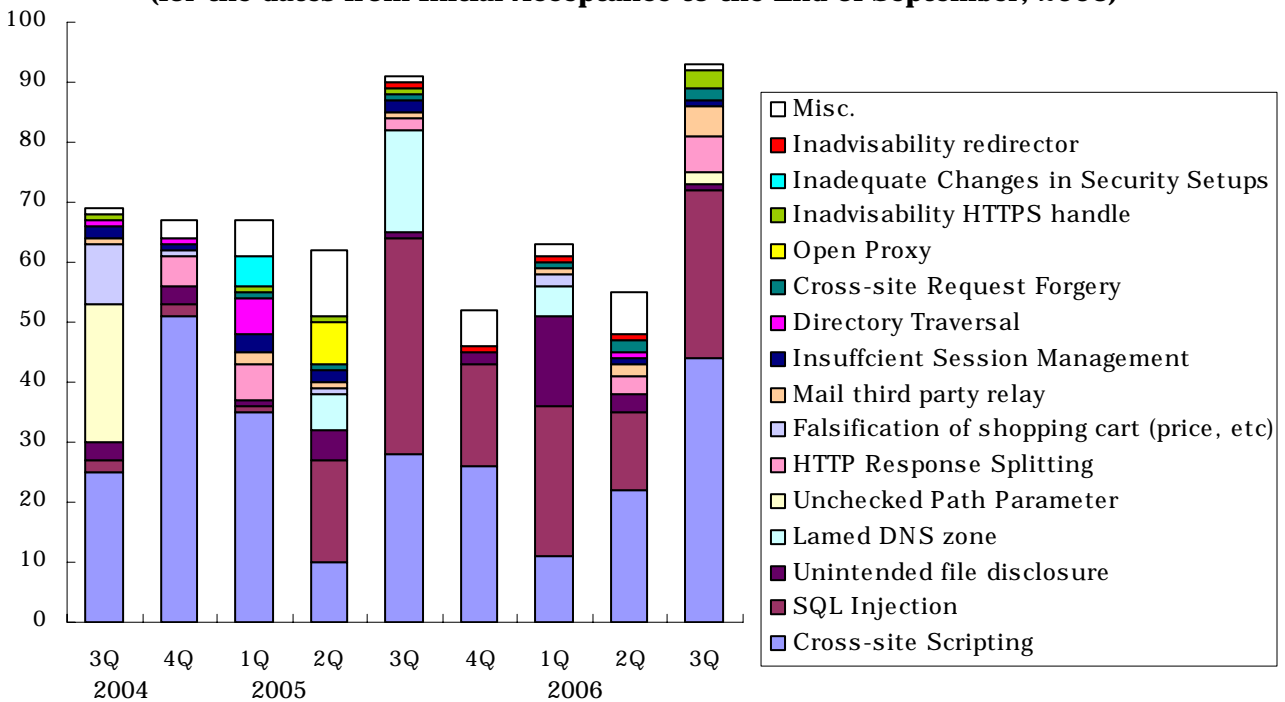


**Chart 3-2: Breakdown of Vulnerabilities in Web Applications**
**(for the dates from Initial Acceptance to the End of September, 2006)**

As for the type of vulnerabilities, "cross-site scripting" was the largest in number and "SQL injection" followed. There were number of reports for the "cross-site scripting" from the beginning when IPA started to accept the reports. The reports for the "SQL injection" has been drastically increased from the 2nd Quarter of 2005; almost of all the reports were related to the detection of such pages displaying error messages of database. Currently, 97 cases were ended up of handling: 60% of them were reported as actual problem (s) and modified. As for the rest of 40% were simply displaying error messages and any SQL commands could not be inserted actually so that reported that there was no problems relevant to the "SQL injection".

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 81% of vulnerabilities reported against entire vulnerabilities reported were modified within 90 days.
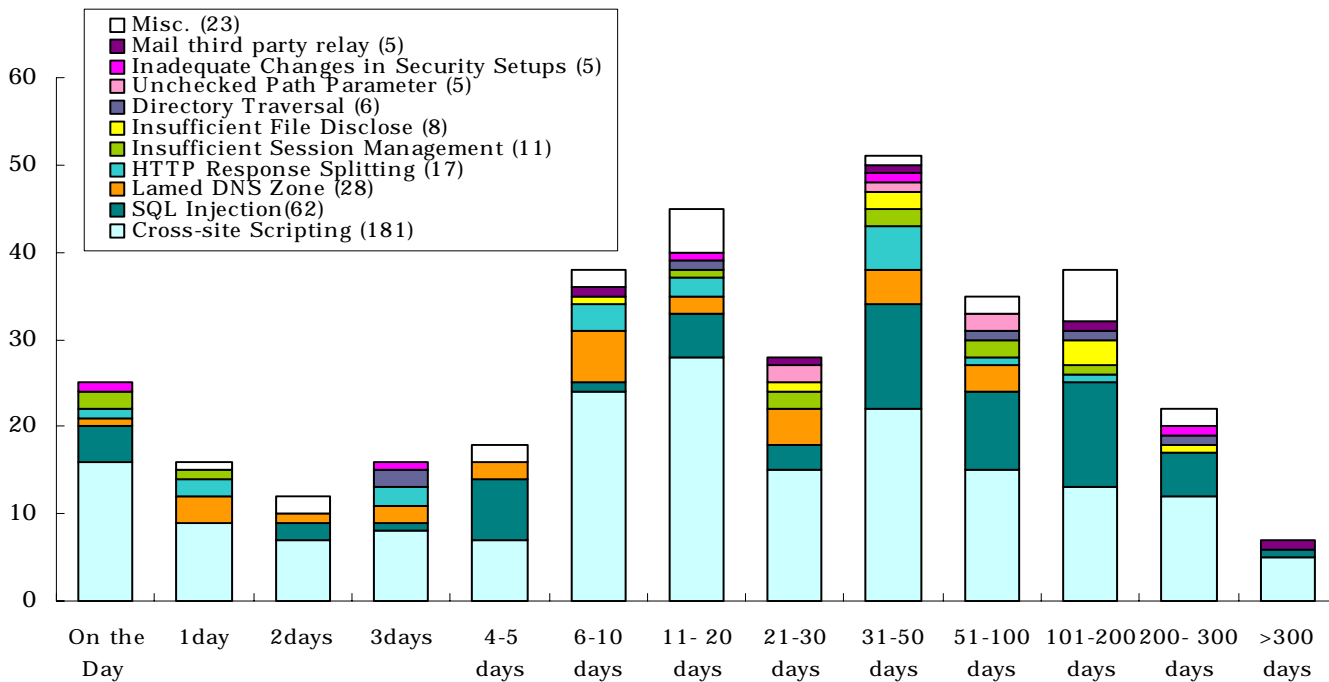


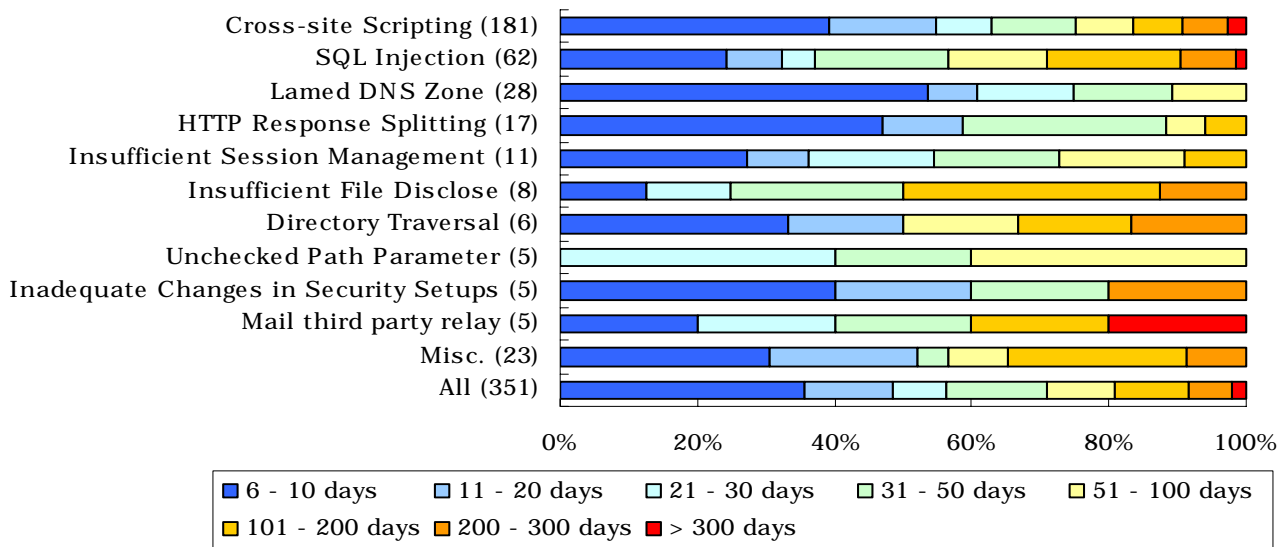**Chart 3-3: Dates Required Modifying Vulnerability in Web Applications**



**Chart 3-4: Dates Required Modifying Vulnerability in Web Applications by Type**