भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी विभाग
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)
इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्प्लेक्स, नई दिल्ली-110003
Government of India
Ministry of Communications & Information Technology
Department of Electronics & Information Technology
Indian Computer Emergency Responce Team (CERT-In)
Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel. : 24368544, Fax : 24366806 E-mail : grai@mit.gov.in

Director General

D.O No. 2(6)/2013-CERT-In

30.01.2014

Dear Shri Padhi,

CERT-In is tracking defacement of Indian websites on regular basis. A total of 1933 & 1238 Indian websites were defaced by various hackers during the month of November & December 2013 respectively. 48% of the websites defaced were on '.in' domain in November as against 73% in December 2013. A total of 12 & 14 websites belonging to Government Departments were defaced during corresponding period.

The top 3 hacker groups who defaced maximum number of websites during November – December period were "FL1T0X_Dz", "Toxic Dz" & "4RM1T4". Cross-site scripting (XSS) vulnerabilities in Microsoft SharePoint Server (CVE-2013-3180, CVE-2013-3179), Security Bypass and file upload vulnerability in Joomla! (CVE-2013-5576), SQL injection vulnerability in the Landing Pages plugin for WordPress (CVE-2013-6243) & Security Bypass Vulnerability in Drupal (CVE-2013-4379) were observed to be largely exploited for the defacements.

Summaries of monthly website defacements depicting domain-wise and network-wise break-up of the websites defaced, top hackers and vulnerabilities which are largely exploited are attached.

In view of growing attacks on websites, you are requested to advise website administrators to follow best practices to secure web applications and web servers.

The following CERT-In security guidelines may be referred from the Knowledge base section available on CERT-In website (www.cert-in.org.in)

- Web Server Security Guidelines
- Securing IIS /7.0 Web Server Guidelines
- Guidelines for Auditing and Logging

With regards,

Yours sincerely,

(Gulshan Rai)

Encl: As above

Shri Madhusudan Padhi,IAS
Commissioner cum Secretary,
IT Department
OCAC, N-1/7-D, Acharya Vihar,
Bhubaneswar-751001
Orissa

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements December 2013

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

CONTENTS

1. Introduction

This report summarizes Indian website defacements during December 2013. In all 1238 Indian websites were defaced during the month of December as against 1933 defacements in November 2013.

2. Distribution of defaced domains

The defaced domains include:

- Top level domains TLDs such as .com, .org, .net, .in etc. Out of 1238 Indian websites which were defaced during the month of December ,227 were on .com, 74 were on .org, 9 were on .net, 905 were on .in and rest of 23 were on other domains.

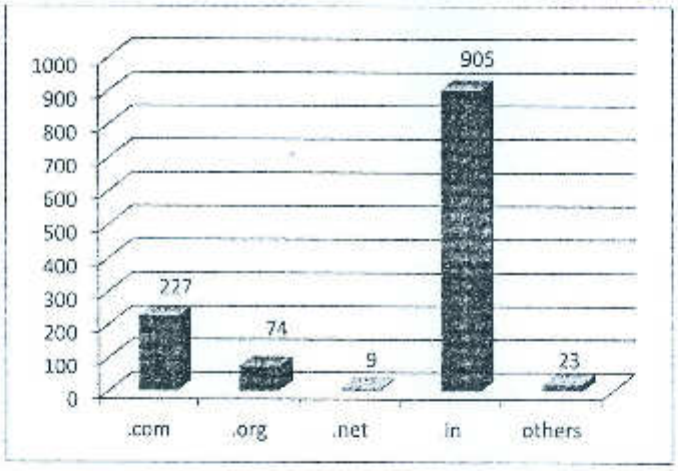

Figure 1: Distribution of Defaced Domains (TLDs)

- Country code top level domain (ccTLDs) includes .co.in, .net.in, .gov.in, .org.in, .nic.in, .ac.in, .edu.in and .res.in. Out of 905 Indian websites which were defaced during the month of December, 587 were on .in and 236 were on .co.in. Figure 2 shows the distribution of defaced domains (ccTLDs).

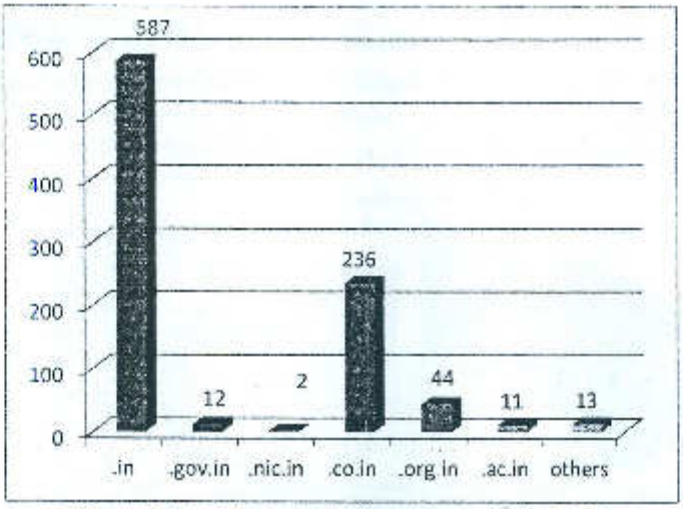

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of December 2013 a total of 1238 Indian websites were defaced. Out of these 73% websites were on .in domain and 18% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

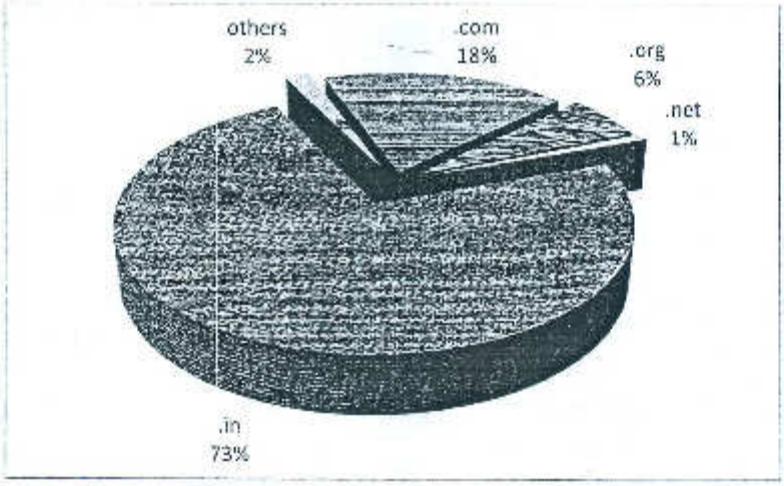

Figure 3: % Distribution of Defaced Domains (TLDs)

In ccTLD segment, around 65% defaced websites were on .in domain and 26% were on .co.in. . Figure 4 shows the percentage distribution of defaced site in country code top level domain (ccTLDs).

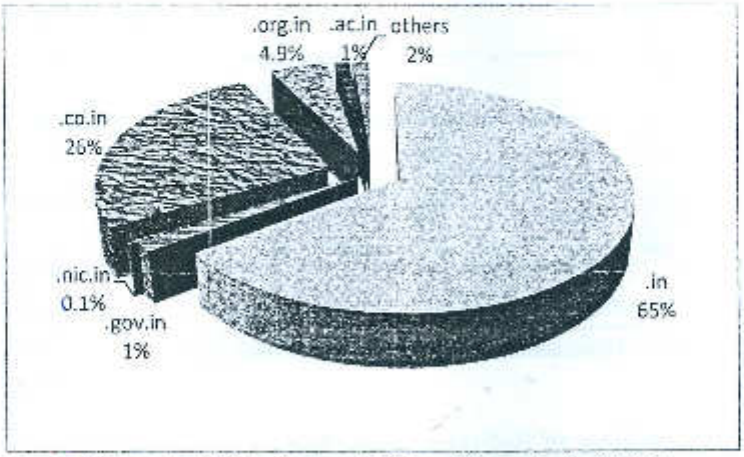

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (Total)

Among the top defacers, 4RM1T4 defaced 80 websites and Romantic defaced 74 websites. Table 1 shows the detailed description about the top defacers.

S.No	Attacker Name	Number of websites
1	4RM1T4	80
2	Romantic	74
3	De3D M3n @U11	56
4	Muhammad Bilal	55
5	IrFi H@XOR	53
6	ali ahmady	51
7	MR.HES@M	49
8	HaYaL-ET-06	34
9	Intruder	32
10	HMBP-02	29

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

Among the top defacers for Country code top level domains IrFi H@XOR defaced 43 websites while ali ahmady defaced 42 websites. Table 2 shows detailed description for top defacers (ccTLD).

S.No	Attacker Name	Number of websites
1	IrFi H@XOR	43
2	ali ahmady	42
3	Romantic	40
4	De3D M3n @U11	36
5	HaYaL-ET-06	34
6	MR.HES@M	32
7	Muhammad Bilal	31
8	4RM1T4	28
9	HMBP-02	25
10	Jagad Dot ID	22

Table 2: Top Defacers ccTLD wise

4. Details of Mass Defaced IPs during December 2013

S No.	IP	ISP Name	ISP Location	Defacer	No. of Sites
1	204.93.161.72	Mochanin Corp	US	ali ahmady	63
2	72.9.151.206	RANDYKATZ	US	Romantic	56
3	103.15.61.164	Apollo Online	IN	4RM1T4	53
4	182.18.152.88	CtrlS IN	IN	De3D M3n @U11	45

5. Defacement by Networks

5.1 Most Targeted Networks

It has been observed that majority (68%) of Indian websites defaced were hosted outside India.

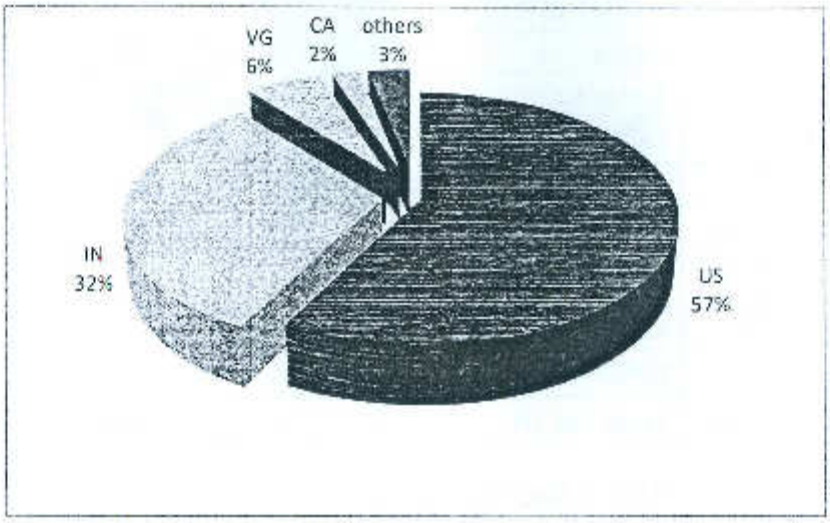

Figure 5: Defaced website hosting country-wise

6. Attack Trends

6.1 Attack Methodologies

Attack methodologies which are generally used to deface a website are:

- Attacks against the administrator/user (password stealing/ sniffing)
- Shared mis-configurations
- File Inclusion
- SQL Injection
- Web shell uploading
- Access credentials through Man in the Middle attack
- FTP Server Intrusion

- Web Server Intrusion
- DNS attack through cache poisoning
- Remote administrative panel access through brute forcing
- SSH server Intrusion
- RPC Server intrusion
- Telnet Server intrusion

6.2 Vulnerabilities

The Vulnerabilities which are largely exploited for the defacements

- Cross-site scripting (XSS) vulnerabilities in Microsoft SharePoint Server (CVE-2013-3180, CVE-2013-3179)
- Security Bypass and file upload vulnerability in Joomla! (CVE-2013-5576)
- SQL injection vulnerability in the JExtensions JE Poll component before 1.1 for Joomla! (CVE-2013-5101)
- Cross-site scripting (XSS) vulnerabilities in Joomla! (CVE-2013-3534, CVE-2013-3267, CVE-2013-3059, CVE-2013-3058)
- SQL injection vulnerability in the RSGallery2 in Joomla! (CVE-2013-3554)
- Privilege Escalation vulnerability in Joomla! (CVE-2013-3056)
- Joomla! Joomsport Component SQL Injection and Arbitrary File Upload Vulnerabilities
- SQL injection vulnerability in the Landing Pages plugin for WordPress (CVE-2013-6243)
- Multiple Cross-site request forgery (CSRF) vulnerabilities in WordPress (CVE-2013-0736)
- Information Disclosure Vulnerability in WordPress PHP widget plugin (CVE-2013-0721)
- Cross-site request forgery (CSRF) vulnerability in Drupal Autosave module (CVE-2013-2097)
- Cross-site scripting (XSS) vulnerability in the FCKeditor module for Drupal (CVE-2013-2066)
- Security Bypass Vulnerability in Drupal (CVE-2013-4379)

7. Suggested Countermeasures

- Apply appropriate updates/patches at the OS and application level regularly.
- Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks
- Enable and maintain logs of different devices and servers and maintain the same for all the levels.
- Conduct auditing for web application & configuration settings of web server periodically.
- Periodically check the web server directories for any malicious/unknown web shell files and remove as and when noticed.
- Use an application firewall to controls input, output, and/or access to the web application.
- Install a good antivirus and keep it updated and running.
- The following CERT-In security guidelines may be referred from the Knowledgebase Section

  - Web Server Security Guidelines
  - Securing IIS /7.0 Web Server Guidelines
  - Guidelines for Auditing and Logging

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements November 2013

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

CONTENTS

1. Introduction

This report summarizes Indian website defacements during November 2013. In all 1933 Indian websites were defaced during the month of November as against 1159 defacements in October 2013.

2. Distribution of defaced domains

The defaced domains include:

- Top level domains TLDs such as .com, .org, .net, .in etc. Out of 1933 Indian websites which were defaced during the month of November, 792 were on .com, 109 were on .org, 44 were on .net, 938 were on .in and rest of 50 were on other domains.

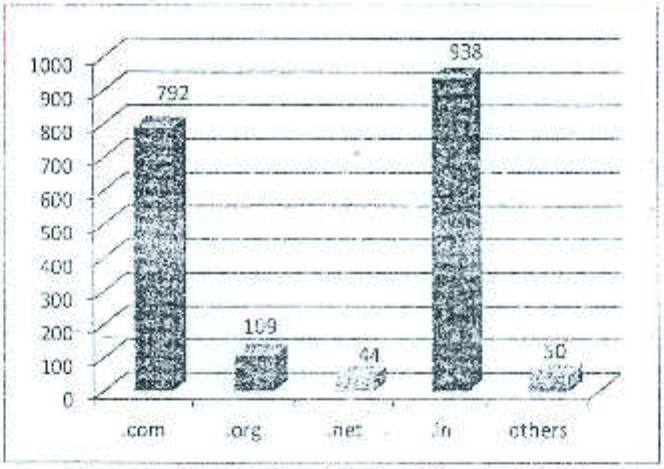

Figure 1: Distribution of Defaced Domains (TLDs)

- Country code top level domain (ccTLDs) includes .co.in, .net.in, .gov.in, .org.in, .nic.in, .ac.in, .edu.in and .res.in. Out of 938 Indian websites which were defaced during the month of November, 655 were on .in and 224 were on .co.in. Figure 2 shows the distribution of defaced domains (ccTLDs).

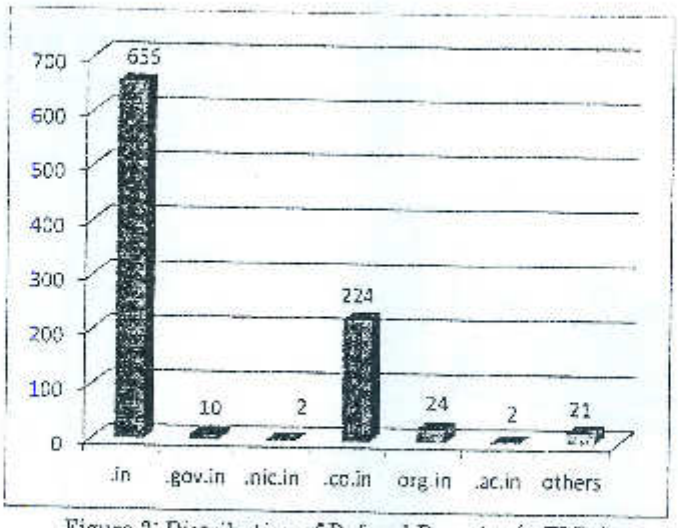

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of November 2013 a total of 1933 Indian websites were defaced. Out of these 48% websites were on .in domain and 41% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

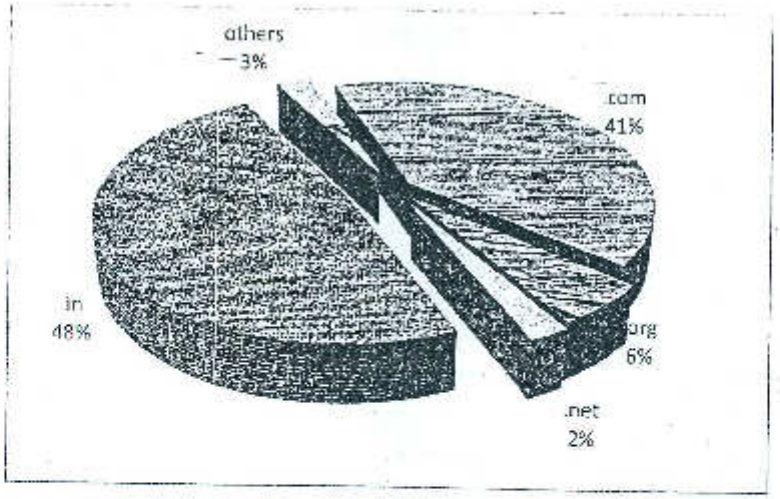

Figure 3: % Distribution of Defaced Domains (TLDs)

In ccTLD segment, around 70% defaced websites were on .in domain and 23.6% were on .co.in. . Figure 4 shows the percentage distribution of defaced site in country code top level domain (ccTLDs).

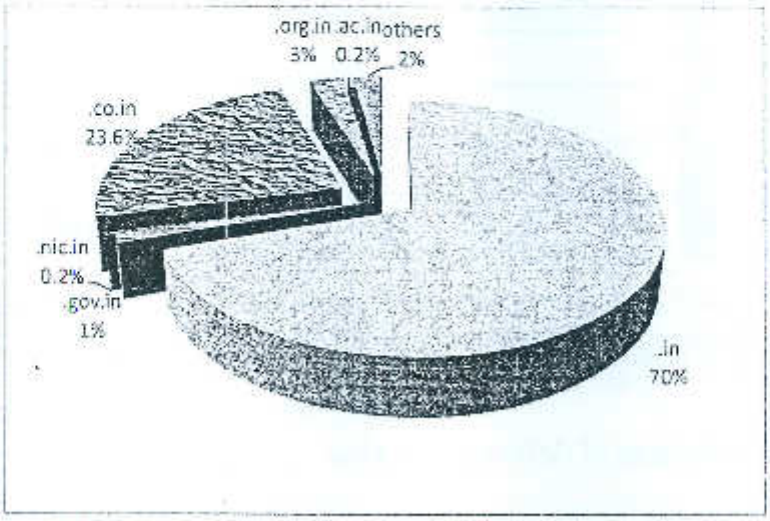

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (Total)

Among the top defacers, FL1T0X_Dz defaced 177 websites and Toxic Dz defaced 130 websites. Table 1 shows the detailed description about the top defacers.

S.No	Attacker Name	Number of websites
1	FL1T0X_Dz	177
2	Toxic Dz	130
3	Muhammad Bilal	101
4	Mr.Hawk	100
5	Hunter Gujjar	80
6	hax.3xploit	73
7	HUSA	73
8	chinahacker	64
9	Tunisian_Hackers	61
10	ZoRRoKiN	61

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

Among the top defacers for Country code top level domains FL1T0X_Dz defaced 94 websites while Toxic Dz defaced 64 websites. Table 2 shows detailed description for top defacers (ccTLD).

S.No	Attacker Name	Number of websites
1	FL1T0X_Dz	94
2	Toxic Dz	64
3	Mr.Hawk	62
4	Muhammad Bilal	59
5	Hunter Gujjar	58
6	HUSA	47
7	chinahacker	43
8	Index Php	34
9	Cyber_Taregh	33
10	hax.3xploit	32

Table 2: Top Defacers ccTLD wise

4. Details of Mass Defaced IPs during November 2013

S No.	IP	ISP Name	ISP Location	Defacer	No. of Sites
1	72.55.131.139	IWEB-BLK-03	CA	FL1T0X_Dz	175
2	198.148.113.190	MULTA-NET12	US	Toxic Dz	127
3	206.183.110.34	WEBWERKSIND	US	Muhammad Bilal	118
4	216.245.209.135	LSN-DLLSTX	US	Mr.Hawk	95

5. Defacement by Networks

5.1 Most Targeted Networks

It has been observed that majority (84%) of Indian websites defaced were hosted outside India.

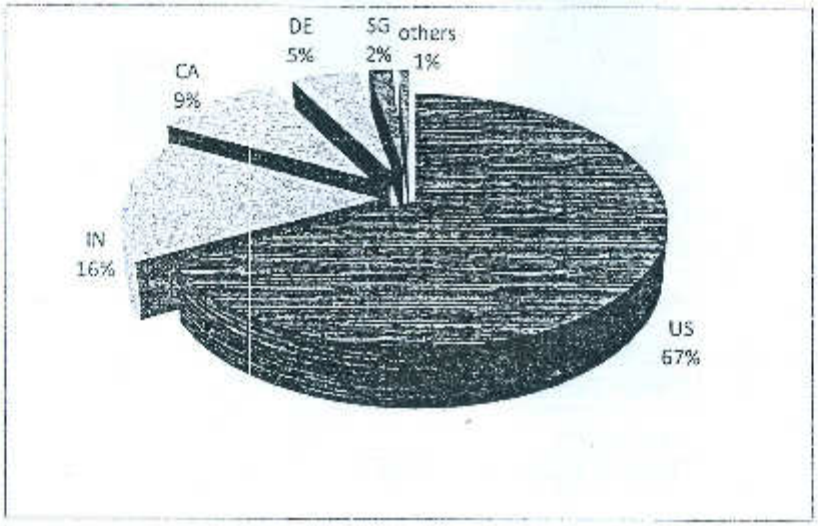

Figure 5: Defaced website hosting country-wise

6. Attack Trends

6.1 Attack Methodologies

Attack methodologies which are generally used to deface a website are:

- Attacks against the administrator/user (password stealing/ sniffing)
- Shared mis-configurations
- File Inclusion
- SQL Injection
- Web shell uploading
- Access credentials through Man in the Middle attack
- FTP Server Intrusion

- Web Server Intrusion
- DNS attack through cache poisoning
- Remote administrative panel access through brute forcing
- SSH server Intrusion
- RPC Server intrusion
- Telnet Server intrusion

6.2 Vulnerabilities

The Vulnerabilities which are largely exploited for the defacements

- Cross-site scripting (XSS) vulnerabilities in Microsoft SharePoint Server (CVE-2013-3180, CVE-2013-3179)
- Security Bypass and file upload vulnerability in Joomla! (CVE-2013-5576)
- SQL injection vulnerability in the JExtensions JE Poll component before 1.1 for Joomla! (CVE-2013-5101)
- Cross-site scripting (XSS) vulnerabilities in Joomla! (CVE-2013-3534, CVE-2013-3267, CVE-2013-3059, CVE-2013-3058)
- SQL injection vulnerability in the RSGallery2 in Joomla! (CVE-2013-3554)
- Privilege Escalation vulnerability in Joomla! (CVE-2013-3056)
- Joomla! Joomsport Component SQL Injection and Arbitrary File Upload Vulnerabilities
- SQL injection vulnerability in the Landing Pages plugin for WordPress (CVE-2013-6243)
- Multiple Cross-site request forgery (CSRF) vulnerabilities in WordPress (CVE-2013-0736)
- Information Disclosure Vulnerability in WordPress PHP widget plugin (CVE-2013-0721)
- Cross-site request forgery (CSRF) vulnerability in Drupal Autosave module (CVE-2013-2097)
- Cross-site scripting (XSS) vulnerability in the FCKeditor module for Drupal (CVE-2013-2066)
- Security Bypass Vulnerability in Drupal (CVE-2013-4379)

7. Suggested Countermeasures

- Apply appropriate updates/patches at the OS and application level regularly.
- Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
- Enable and maintain logs of different devices and servers and maintain the same for all the levels.
- Conduct auditing for web application & configuration settings of web server periodically.
- Periodically check the web server directories for any malicious/unknown web shell files and remove as and when noticed.
- Use an application firewall to controls input, output, and/or access to the web application.
- Install a good antivirus and keep it updated and running.
- The following CERT-In security guidelines may be referred from the Knowledgebase Section:
  - Web Server Security Guidelines
  - Securing IIS /7.0 Web Server Guidelines
  - Guidelines for Auditing and Logging