TREND REPORT

Vulnerabilities Trends in the Second Semester of 2016

08/03/2017
Index

1. Introduction ....................................................................................................................... 4
   1.1. Scope .......................................................................................................................... 4
   1.2. Motivation ................................................................................................................... 4

2. Methodology ..................................................................................................................... 6
   2.1. Categories of Vulnerabilities ...................................................................................... 6
   2.2. Sectors of Activity ...................................................................................................... 8

3. Categories of Vulnerabilities ............................................................................................ 9
   3.1. Analysis of Global Results ......................................................................................... 9
   3.2. Analysis of Specific Results ...................................................................................... 10
      3.2.1. Configuration Errors ......................................................................................... 10
      3.2.2. Data Leak in Metadata ..................................................................................... 12
      3.2.3. Information Management Errors ....................................................................... 13
      3.2.4. Inadequate Validation of Entry Data ................................................................. 15
      3.2.5. Cryptographic Problems .................................................................................. 16

4. Results by Sectors of Activity .......................................................................................... 17

5. Results by Geographical Regions ................................................................................... 19

6. Results by Degrees of Severity ....................................................................................... 20

7. Conclusions .................................................................................................................... 21

8. Bibliography .................................................................................................................... 22

About ElevenPaths .............................................................................................................. 23

Further Information ........................................................................................................... 23
Executive Summary

94.86% of the results obtained are due to five categories of vulnerabilities: data leak in metadata (49.40%), information management errors (24.84%), configuration errors (9.17%), inadequate validation of input data (7.44%) and cryptographic problems (4.01%). These five categories represent 8.36% more than the first semester report.

Some 87.01% of detected vulnerabilities indicate that the vast majority of failures are to be found in the configuration of equipment and systems, allowing the obtaining of different types of information, ranging from the software and product version to personal information on users. This trend has increased slightly (+5.01%) regarding the first semester, indicating that the origin of most of these problems detected are not vulnerabilities existing in the code created by the developers but in the poor practices of the system administrators.

However, it has been possible to observe a 53.03% increase in the subcategory of files with sensitive information that, in development or testing environments, could represent a risk if not deleted. This information is not dangerous in and of itself, but if combined with fingerprinting techniques (use of banners and error messages on websites, versions in DNS servers), an attacker could get to know the target in detail.

Of close to the total number of detected vulnerabilities, about 70% are related to SSL, either due to protocol versions with weak encryption or weak certificates. In addition, we should highlight the categories of weak certificates (39.38%), containing certificates which have expired, which are about to expire, which have been issued by an unreliable CA or for other domains and the absence of encryption (12.91%).

The configuration errors category is that which has seen the greatest increase in comparison to the previous semester, particularly in consumer goods, industry, healthcare, the public sector and consumer services. On the other hand, energy and public services have seen a decrease from 43.48% to 0.64%.

Lastly, in the geographic areas of LATAM and EMEA, data leaks in metadata are predominant (55.57% and 37.32%, respectively). However, configuration errors were predominant in the first semester for the EMEA area.
1. Introduction

A new edition of the trend report on vulnerabilities in the second half of 2016 has been drawn up by the team from the Vamps (Persistent Vulnerability Assessment & Management) Service of ElevenPaths. This report analyses the data of more than 100 companies representing the main sectors of activity with a global scope.

After this section, the methodology followed in the classifications used in the later sections of the results analysis is indicated. The results are then analysed by categories of vulnerability, studying the overall results and later focusing on specific categories. The following three sections include the results by sectors of activity, geographical regions and degrees of severity. With the exception of the analysis section with results classified by severity, the remaining sections include a comparison with the results obtained in the vulnerabilities trend reports from the first semester of 2016. Finally, the report presents the conclusions extracted from the results obtained.

The following conclusions were reached in the trend report for the first semester of 2016:

- Generally speaking, there exists a lack of care in the management of information which is accessible via the internet: files with sensitive information, server information, metadata, back-up copies and so on. Regardless of the point of view employed, the analysis of the data shows a large number of vulnerabilities of this kind.

- Most of the errors can be put down to poor practices by system administrators, to a greater extent than existing vulnerabilities in code performed by developers.

- The increase in the number of configuration errors is due to the lack of protection in HTTP headers, which account for 31.65% of the total, a figure greater than any of the other categories.

- The results show that the injection of commands and XSS remain a serious problem affecting the development of the software of companies and third parties, despite the fact that they respectively occupied first and third places in the OWASP list of top 10 vulnerabilities for 2013.

- According to their specific percentages in the global results and the number of high-severity vulnerabilities, we should focus on errors due to inadequate validation of input data and permits, privileges and access control.

1.1. Scope

The scope of this document includes the sample of vulnerabilities that the Vamps Service detected in the second half of 2016, from 1 July to 31 December 2016. The vulnerabilities come exclusively from information resulting from the security tests executed on customer assets. At no time is information provided which could link a company to the results shown in this report.

1.2. Motivation

Companies have undergone a clear orientation to the digital world and the internet, which also entails the emergence of new threats to their systems in order to access one of their most valuable assets: information. Being competitive nowadays requires using a large number of heterogeneous technologies, which are changing and difficult to manage.

In addition to the above, the number of vulnerabilities made public every year which affect commercial products is fairly high, making it difficult for the system administrators and/or security departments of companies to determine which vulnerabilities are affecting the customer’s technological platform.
Behind all this, there already exists a very sophisticated and agile organized cybercrime industry, which is always one step ahead of any defence which can be raised by a company. Any company is liable to suffer an attack, including retailers, banks, security specialists and internet giants, as well as governments and states.

The purpose of this document is to display, from different points of view, the current vulnerabilities present in real assets. By means of a comparison with previous trend reports, the aim is to show the latest trends in vulnerabilities and indicate to companies where to focus their corrective measures in order to maintain an adequate level of security.
2. Methodology

This trend report includes its own classifications for the categorization of vulnerabilities and sectors of activity.

2.1. Categories of Vulnerabilities

The categorization of vulnerabilities uses the view of development concepts (CWE-699) [1] and the dictionary of vulnerabilities of the Vamps Service.

A definition is supplied below for each of the categories into which the vulnerabilities detected and represented in this report have been divided:

- **Information management errors.** Information management errors are related to the improper handling of sensitive information which could lead to the disclosure thereof. This disclosure may be due to the intentional or accidental revelation of information to an agent[1] who is not expressly authorized to access it. The severity of the above varies widely, depending on the kind of information disclosed.

  On the one hand, the information is regarded as sensitive in terms of the function of the product, such as the sending of a private message, and, on the other, it provides information on the product or its environment which could be useful in an attack, such as the installation path or a resource which is accessible remotely.

- **Configuration errors.** These kinds of errors are typically introduced during the software configuration phase.

- **Inadequate validation of input data.** These kinds of errors occur when the input data in the code are not validated or are validated incorrectly, a situation which can be exploited by an attacker to create a specific item of input data, causing an application to react unexpectedly. This will mean that parts of the system will receive unexpected input data, thereby disrupting the control flow, the control of a resource or the execution of the code.

  To achieve proper validation it is important to identify the form and type of data which are accepted and expected by the application. We therefore require a definition of the format of the data and the use of each input entity in order to define the restrictions as accurately as possible.

- **Data leak in metadata.** This category typically forms part of information management errors and, more specifically, information which can be obtained by means of the use of fingerprinting techniques but, due to the volume of metadata found, it was decided to make a separate category to include these kinds of errors.

  Information due to leakages of metadata forms part of that contained in the files of an application or system. The information an attacker can extract includes lists of valid users, technologies employed, folders, printers, e-mails, operating systems, etc. This information can enable an attacker to accurately recreate the scene of

---

[1] Within this context, the term “agent” refers to an entity which interacts with the software or with other entities, such as users, services, devices, intermediaries, etc.
the attack, by means of which he will attempt to exploit a vulnerability in the type or version of the software used by the target of the attack.

- **Cryptographic problems.** This category includes relevant vulnerabilities associated in one way or another to encryption protocols. Some of these vulnerabilities are inherent in the protocol itself (design faults or weaknesses), while others relate to errors or shortcomings in the implementation of the protocols, affecting only the technologies with the implementation failures.

- **Obsolete versions.** These include publicly known vulnerabilities forming part of the CVE (Common Vulnerabilities and Exposures) [2] dictionary, which relate to the use of obsolete versions of programming languages, applications, operating systems, etc., due to the lack of patching of the system.

- **Permits, privileges and access control.** These errors relate to weaknesses in the management of permits, privileges and other features of security which are used to implement access control. The allocation or inadequate handling of permits for resources or the improper restriction of access to a resource by an unauthorized user are examples of the types of vulnerabilities included in this category. These kinds of vulnerability may allow an attacker to access, modify or execute executable files, access programs due to an elevation of privileges or tamper with the entry of calls into the file system.

- **Buffer overflow.** A buffer overflow is a failure which occurs when a program writes data into a buffer, exceeding the limits of the buffer itself, and overwrites adjacent memory blocks. The vulnerabilities covered by this category can be used by an attacker for several purposes, such as the control of the execution of processes, halting a process or the modification of internal variables.

- **Session handling.** Vulnerabilities within this category are due to the use of cookies whose completeness or validity are not verified or are validated improperly, which can lead to session hijacking. In other words, proper session management is not implemented. The problem lies in the fact that an application performs operations of a critical nature on security issues depending on the use of cookies.

An attacker can easily modify the cookies within the browser or by means of the implementation of the customer code outside the browser. Depending on cookies lacking thorough checks on their validity and completeness can allow malicious users to bypass authentication processes, perform code injections and so on. Examples of the above are cookie prediction and session setting.

The possible mitigating measures include avoiding the use of cookies in security-related operations or, if they are used, implementing a strict entry procedure for validating the cookies. Timeouts are often used to limit the validity of a cookie and, therefore, the attack.

- **Resource management errors.** The errors included in this category are related to the inadequate management of system resources. Many of them are related with code in PHP or use the OpenSSL library. These errors can allow uncontrolled consumption of resources or a leakage of resources to unauthorized third parties.

---

2 Small arbitrary data defined by a web server and sent to the user’s browser (which stores them). By means of the use of cookies, the browser provides the server with a means of linking the request of the current page with requests from previous pages.
2.2. Sectors of Activity

Using the classifications created by Thomson Reuters [3] and ICB [4] as references, the following sectors of activity were defined:

<table>
<thead>
<tr>
<th>Sectors of activity</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy and public services</td>
<td>Telecommunications and technology</td>
</tr>
<tr>
<td>Raw materials</td>
<td>Financial</td>
</tr>
<tr>
<td>Industry</td>
<td>Public sector</td>
</tr>
<tr>
<td>Consumer goods</td>
<td>Education</td>
</tr>
<tr>
<td>Health</td>
<td>Non-profit and volunteer organizations</td>
</tr>
<tr>
<td>Consumer services</td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Details of the classification by economic sectors.
3. Categories of Vulnerabilities

In this section we analyse the results obtained from two different but complementary perspectives. Firstly in global terms and then more specifically, we will stop to consider the most representative categories.

3.1. Analysis of Global Results

![Global Results Diagram]

Figure 1. Total vulnerabilities.

In accordance with Figure 1, 94.86% of the results obtained are due to five categories of vulnerabilities: data leak in metadata (49.40%), information management errors (24.84%), configuration errors (9.17%), inadequate validation of input data (7.44%) and cryptographic problems (4.01%). These five categories represent 8.36% more than in the first semester report, with data leaks in metadata experiencing the greatest growth.

On the other hand, we can see that the figure of 87.01% of detected vulnerabilities (except for vulnerabilities due to inadequate validation of input data, cryptographic problems and buffer overflow) indicates that the vast majority of failures are to be found in the configuration of equipment and systems, allowing the obtaining of different types of information, ranging from the software and product version to personal information on users. This trend has increased slightly (+5.01%) regarding the first semester, indicating that the origin of most of these problems detected are not vulnerabilities existing in the code created by the developers but in the poor practices of the system administrators.

Table II compares the first and second semester results for 2016, indicating the variations experienced and the positions of each of the vulnerability categories.
<table>
<thead>
<tr>
<th>Position</th>
<th>Categories</th>
<th>% H2 2016</th>
<th>% H1 2016</th>
<th>Differential position</th>
<th>% Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>1º</td>
<td>Data leak in metadata</td>
<td>49.40</td>
<td>23.47</td>
<td>(+1)</td>
<td>+25.93</td>
</tr>
<tr>
<td>2º</td>
<td>Information management errors</td>
<td>24.84</td>
<td>11.16</td>
<td>(+1)</td>
<td>+13.68</td>
</tr>
<tr>
<td>3º</td>
<td>Configuration errors</td>
<td>9.17</td>
<td>36.33</td>
<td>(-2)</td>
<td>-27.49</td>
</tr>
<tr>
<td>4º</td>
<td>Inadequate validation of entry data</td>
<td>7.44</td>
<td>9.60</td>
<td>(=)</td>
<td>-2.16</td>
</tr>
<tr>
<td>5º</td>
<td>Cryptographic problems</td>
<td>4.01</td>
<td>5.94</td>
<td>(=)</td>
<td>-1.93</td>
</tr>
<tr>
<td>6º</td>
<td>Permits, privileges and access control</td>
<td>2.40</td>
<td>5.52</td>
<td>(=)</td>
<td>-3.12</td>
</tr>
<tr>
<td>7º</td>
<td>Buffer overflow</td>
<td>1.54</td>
<td>2.37</td>
<td>(+1)</td>
<td>-0.83</td>
</tr>
<tr>
<td>8º</td>
<td>Session handling</td>
<td>0.59</td>
<td>1.56</td>
<td>(+1)</td>
<td>-0.97</td>
</tr>
<tr>
<td>9º</td>
<td>Resource management errors</td>
<td>0.52</td>
<td>1.07</td>
<td>(+1)</td>
<td>-0.55</td>
</tr>
<tr>
<td>10º</td>
<td>Obsolete versions</td>
<td>0.09</td>
<td>2.98</td>
<td>(-3)</td>
<td>-2.89</td>
</tr>
</tbody>
</table>

Table II. Results comparison for the first and second semesters of 2016.

We can observe a fall in most categories, the most significant one in configuration errors (-27.49%). On the other hand, the two categories whose percentages increased in relation to the first semester of 2016 are data leaks in metadata (+25.93%) and information management errors (+13.68%).

The main categories of vulnerabilities will be discussed in depth below, listing the sub-categories they include and making recommendations to avoid these errors.

### 3.2 Analysis of Specific Results

#### 3.2.1 Configuration Errors

The following errors are included in the category of configuration errors:

- Lack of protection in HTTP headers
- Configuration of the HTTP service
- Race conditions
- Configuration of the DNS service
- Services published on the internet
- Different kinds of vulnerabilities

Most services do not have adequate protection for the web services, which may lead to content spoofing attacks. More specifically, the results shown in the Figure 2 reflect that these errors are, in their vast majority, due to incorrect implementation of the HTTP header (53.06%), allowing the use of mechanisms such as crossorigin and clickjacking attacks.

The following subcategory is encompassed by insecure configurations of the HTTP service (34.44%) which enables the listing of website content or improper use/authorisation of HTTP methods of information exchange.
The following category is related to configuration errors which enable race conditions (4.01%). Allowing access paths to resources for unauthorized agents can lead to the exposure of sensitive information and the modification of resources. This is especially dangerous when the resource is related to the configuration and the execution of programs or sensitive personal data.

In Table III we compare the results between the periods of the first and second semesters of 2016 with the specific percentages of the sub-categories of the configuration errors.

<table>
<thead>
<tr>
<th>Position</th>
<th>Sub-categories</th>
<th>% H2 2016</th>
<th>% H1 2016</th>
<th>Differential position</th>
<th>% Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>1º</td>
<td>Lack of protection in HTTP headers</td>
<td>53.06</td>
<td>87.11</td>
<td>(-)</td>
<td>-34.05</td>
</tr>
<tr>
<td>2º</td>
<td>Configuration of the HTTP service</td>
<td>34.44</td>
<td>7.45</td>
<td>(=)</td>
<td>+26.99</td>
</tr>
<tr>
<td>3º</td>
<td>Different kinds of vulnerabilities</td>
<td>7.96</td>
<td>2.87</td>
<td>(=)</td>
<td>+5.15</td>
</tr>
<tr>
<td>4º</td>
<td>Race conditions</td>
<td>4.01</td>
<td>2.44</td>
<td>(=)</td>
<td>+1.66</td>
</tr>
<tr>
<td>5º</td>
<td>Services published on the internet</td>
<td>0.45</td>
<td>0.12</td>
<td>(=)</td>
<td>+0.33</td>
</tr>
<tr>
<td>6º</td>
<td>Configuration of the DNS service</td>
<td>0.07</td>
<td>0.00</td>
<td>(=)</td>
<td>+0.07</td>
</tr>
</tbody>
</table>

Table III. Results comparison between the first and second semesters reports for 2016.

The lack of protection in HTTP headers has fallen to 53.06%, at the expense of the remaining categories that have risen. Specifically, HTTP service configuration, up to 34.44%.

Though the lack of protection in HTTP headers has fallen by 34.05% and now represents 53.06% of the results in this category, it is still the most significant vulnerability. As we mentioned, this sub-category encompasses vulnerabilities related to an incorrect or absent implementation of the HTTP Access-Control-Allow-Origin header, in which a user is subjected to phishing attacks by being redirected to a random page for credential theft, and with clickjacking attacks, in which an Internet user is tricked for the purpose of revealing confidential information or taking control of their computer when they click on apparently inoffensive websites.
This type of vulnerability can be mitigated with the proper implementation of the HTTP Access-Control-Allow-Origin
header, configuring it to only allow access to trusted domains, as well as implementation of the HTTP X-Frame-
Options header.

On the other hand, we highlight the increase in results of the HTTP service configuration due to vulnerabilities by
Directory Listing. This vulnerability is the result of an incorrect configuration of this function of the web server that
allows publicly displaying a list of files contained in a specific directory. The impact is felt on the confidentiality, since
confidential information could be revealed and be used by attackers within their footprinting phase for their
exploration in search of characteristics and properties of their target.

There are several attack scenarios with which to obtain the list of directories, such as the inadequate configuration in the
web servers, disabling totally or partially this function by the administrators, exploitation of a web server, or the use of
cached information or history data held in online databases.

3.2.2. Data Leak in Metadata

As shown in Table IV, the data leak in metadata category has recovered the first position again, increasing to 49.40%.

<table>
<thead>
<tr>
<th>Category</th>
<th>% H2 2016</th>
<th>% H1 2016</th>
<th>Differential position</th>
<th>% Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data leak in metadata</td>
<td>49.40</td>
<td>23.47</td>
<td>(+1)</td>
<td>+25.93</td>
</tr>
</tbody>
</table>

Table IV. Comparison of results between the first and second semesters of 2016.

Organizations continue to ignore the problems posed by these kinds of errors, as they are not directly linked to
breaches of information nor are they regarded as critical vulnerabilities by manufacturers or security providers. This
leads, on the one hand, to a lack of concern about the metadata and, on the other, to a lack of awareness of the risks
entailed by the exposure of this information. To the above we must add the fact that metadata management is not an
issue which applies solely to system administrators or the IT team of a company; any employee who is authorized to
publish content on the Internet is liable to generate a data leak. Therefore, the implementation of policies and/or
training and awareness plans should be extended to a large group of workers.

Taking measures to prevent data leak in metadata is especially relevant when the document is widely disseminated,
as occurs when it is offered to the public on a web server or another kind of information repository. We must also
remember that metadata can be obtained from the public documents of an organization without performing any act
which might be considered illegal in the acquiring of information.

Below appears a list of examples of security risks associated with confidentiality due to metadata:

- Finding hidden relationships between companies or persons.
- We can detect cases of software piracy by discovering that a company document has been generated with
  software for which the licence has not been acquired.
- Events can be traced, positioning them both in time and in space
- Tactical information can be located to study possible targets of attacks and acquire internal knowledge of a
  company.

In addition to the confidentiality of an organization being affected, the fact that a company may be a victim of a data
leak in metadata also has an impact on the image of the organization, which disseminates documentation with
metadata while demonstrating a lack of concern for these kinds of information management errors, and on the
maintenance of the confidentiality of information which should not have been disclosed to the recipient of the
document.
3.2.3. Information Management Errors

Information management errors are divided into the following sub-categories:

- Files with sensitive information
- Data leak due to server responses
- Accessible back-up copies
- Uncontrolled error messages
- Different kinds of vulnerabilities

If we look at the table of the Figure 3, we can see that:

- 81.80% of the detected errors come from files with sensitive information (traces of use of administration and development tools, code repositories such as `.git` and `.svn/entries`, user accounts, passwords, e-mail addresses, internal routes, etc.).

This information is not dangerous in itself, but if it is combined with fingerprinting techniques (use of banners and error messages on web pages, versions of DNS servers, etc.), an attacker can obtain detailed knowledge of the target, creating an accurate profile of the platform to be attacked, the software technology of a certain web application, the version of the backend database and the configurations or architecture of the network, all in order to prepare the attack better.

- A decrease has been identified in the remaining categories. Specifically, data leaks for server responses have decreased to 11.34%. These errors are mainly due to comments of developers in the response code, improper configuration of the server or application and differences in the responses of the page.

The recommendations are quite clear in this regard. Deleting the comments within the code before releasing it publicly and monitoring the design of applications during the response based on the validity of the input data, placing particular focus on protecting information such as credit card numbers.
Table V shows a comparison of results for the first and second semesters of 2016. We highlight the increase of files with sensitive information and the decrease in the other categories, particularly data leaks for server responses.

<table>
<thead>
<tr>
<th>Position</th>
<th>Sub-categories</th>
<th>% H2 2016</th>
<th>% H1 2016</th>
<th>Differential position</th>
<th>% Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>1°</td>
<td>Files with sensitive information</td>
<td>81.80</td>
<td>28.77</td>
<td>(+1)</td>
<td>+53.03</td>
</tr>
<tr>
<td>2°</td>
<td>Data leak due to server responses</td>
<td>11.34</td>
<td>40.05</td>
<td>(-1)</td>
<td>-28.71</td>
</tr>
<tr>
<td>3°</td>
<td>Different kinds of vulnerabilities</td>
<td>4.51</td>
<td>12.64</td>
<td>(-)</td>
<td>-8.13</td>
</tr>
<tr>
<td>4°</td>
<td>Accessible back-up copies</td>
<td>1.20</td>
<td>9.30</td>
<td>(-)</td>
<td>-8.10</td>
</tr>
<tr>
<td>5°</td>
<td>Uncontrolled error messages</td>
<td>1.13</td>
<td>9.24</td>
<td>(-)</td>
<td>-8.11</td>
</tr>
<tr>
<td>6°</td>
<td>Obsolete versions</td>
<td>0.01</td>
<td>0.00</td>
<td>(-)</td>
<td>+0.01</td>
</tr>
</tbody>
</table>

Table V. Results comparison between the first and second semesters reports for 2016.

Regarding the results in the table above, we see an increase of 53.03% in the sub-category of Files with sensitive information. Looking at this sub-category with greater detail, it is worth highlighting three types of vulnerabilities that represent 93% of the total results. On the one hand, with 45% of the vulnerabilities, we find detection of IIs Web.Config files, which are accessible from the Internet and can hold critical information about the server configuration, as well as connection chains to databases and system debugging information. Second, vulnerabilities due to the detection of other types of sensitive files created by the code manager Bazaar represent 39% of the results. In this case, the .bznignore file is a file used to prevent the versioning of specific files that do not need it. Lastly, in the remaining 9% of results, we find vulnerabilities due to the detection of SVN/Entries type files, which are created by the popular versions control system Subversion and contain a list of files and directories with versioning.

All these types of detected files share the impact on confidentiality since they contain information that could help an attacker to discover a system’s details and to be able to better plan an attack. These files are used in development or testing environments and represent a risk for data leak that they could cause if not deleted when the developments continue on to production settings. Therefore, the recommended mitigating measure in this regard is clear, and is based on the use of best practices for the deployment of developments in production settings that do not contain this type of files with sensitive information over an IT infrastructure.
3.2.4. Inadequate Validation of Entry Data

In this category for inadequate validation of input data we have included the following errors contained in the Figure 4:

- Cross-Site Scripting (XSS)
- Analysis of parameters
- Injection of commands, injection of LDAP, HTML, XML, etc.
- SQL injection
- Different kinds of vulnerabilities

![Pie chart showing improper input validation](image)

**Figure 4.** Details of the category for inadequate validation of input data.

Since 2003, the top 10 list published by OWASP has taken into account these kinds of vulnerabilities due to inadequate validation of input data, giving separate categories to XSS vulnerabilities and injection of commands, thereby emphasizing the importance of these kinds of errors and the potential security problems resulting from them:

- In the case of XSS attacks the possibilities are almost endless, but they mostly include the transmission of sensitive information to the attacker (cookies or session information allowing the hijacking of the user’s account), redirecting the victim to web content controlled by the attacker, modification of contents displayed on a legitimate website (price of products on online sales portals or the value of shares on a stock market) or the performance of user-side malicious actions (installation of trojans).

- OWASP indicates that a user who achieves an SQL injection can read and modify sensitive information on databases, retrieve the contents of a particular file, execute commands in the operating system and so on.

Even so, the results show that the detection of cross-site scripting (XSS) has risen to 42.50%. However, the category for different kinds of vulnerabilities has decreased by 43.36%, which includes errors related to the infrastructure used by manufacturers (PHP, Java, CMSs, commercial software such as Microsoft, Adobe, HP, etc.) which also makes them vulnerable due to this lack of validation of input data.
The recommendations and mitigating measures in this case are numerous, due to the number of cases encompassed within the inadequate validation of input data. We should take into account all the possible entry points of unreliable data into the code: parameters or arguments, cookies, network information, environment variables, query results, requests for headers, files and any external system which provides information to the application. In addition to assuming that all input data is malicious, adopting a strategy of accepting what is contained, for example, in a whitelist of entries. For any user-side verification of input data which is performed, ensure that this check is duplicated server-side.

The Table IV includes the comparison of results obtained for this category between the first and second semester of 2016:

<table>
<thead>
<tr>
<th>Position</th>
<th>Sub-categories</th>
<th>% H2 2016</th>
<th>% H1 2016</th>
<th>Differential position</th>
<th>% Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>1°</td>
<td>Cross-Site Scripting (XSS)</td>
<td>42.50</td>
<td>10.47</td>
<td>(+1)</td>
<td>+32.03</td>
</tr>
<tr>
<td>2°</td>
<td>Different kinds of vulnerabilities</td>
<td>27.75</td>
<td>71.11</td>
<td>(-1)</td>
<td>-43.36</td>
</tr>
<tr>
<td>3°</td>
<td>Injection of commands, injection of LDAP, HTML, XML, etc.</td>
<td>19.26</td>
<td>6.66</td>
<td>(+1)</td>
<td>+12.60</td>
</tr>
<tr>
<td>4°</td>
<td>SQL injection</td>
<td>8.79</td>
<td>2.19</td>
<td>(+1)</td>
<td>+6.60</td>
</tr>
<tr>
<td>5°</td>
<td>Analysis of parameters</td>
<td>1.69</td>
<td>9.58</td>
<td>(-2)</td>
<td>-7.89</td>
</tr>
</tbody>
</table>

Table VI. Results comparison between the first and second semesters of 2016.

The above table indicates an increase in results due to the subcategory of Cross-Site Scripting of some 32.03% mainly due to the vulnerability due to inadequate JavaScript filtering in the generation of websites, which would enable the injection and delivery of data without any validation, thus accepting receipt of complete scripts and enabling the generation of malicious command sequences that directly impact the website itself or the user’s computer. As with all remote attacks, it is important to differentiate between the possibility of launching an attack (access to an internal network through unpatched servers) and the possibility that the remote attacker could collect and interpret the outgoing information from such an attack. Similarly, we highlight the increase in the remaining subcategories related to the command injections, LDAP, HTML, XML (+12.60%), and SQL (6.60%).

Attacks can therefore affect both confidentiality with access control avoidance through consistent Cross-Site Scripting in the disclosure of information stored in the users’ cookies, and availability with remote code running and the integrity with the modification of sensitive data.

As already mentioned, in all these cases, the recommendation for mitigating these attacks is to properly filter each input parameter against a whitelist of allowed parameters. Any input of unauthorised parameter should be deleted, not only deleting the parameters that the user manually entered, but also special characters such as “,” and “&”. In addition, hidden fields, cookies, headers, the URL itself, etc. should be included. For example, a common error that results in the presence of HTML injection vulnerabilities is the validation of only those fields that the website is expected to show. Therefore, validating all the parts of the HTTP request is recommended.

### 3.2.5. Cryptographic Problems

The Figure 5 shows the category of cryptographic problems, which contains the following:

- Protocols with weak encryption
- Weak certificates
- Absence of encryption
- Different kinds of vulnerabilities
Of the total number of vulnerabilities we have detected, about 70% are related to SSL, either due to protocol versions with weak encryption or weak certificates. In addition, we should highlight the categories of weak certificates (39.38%), containing certificates which have expired, which are about to expire, which have been issued by an unreliable CA or for other domains and the absence of encryption (12.91%).

These kinds of errors easily have an impact on the image of the company, because users receive notifications on their browsers regarding the invalidity of a certificate, because it has expired or is weak, or even due to the absence of encryption in communications.

To avoid making the above mistakes which make a system vulnerable, an appropriate policy for the management of SSL certificates is necessary, establishing what procedures should be followed (for example, the revision of the robustness of the algorithms and the expiry of the certificates) and who should be responsible for such management. In addition, it is recommended to perform a hardening of servers to prevent unencrypted communications and server configurations which do not accept protocols and algorithms with weak encryption.

Table VII shows the comparison of results between the first and second semesters of 2016.

<table>
<thead>
<tr>
<th>Position</th>
<th>Sub-categories</th>
<th>% H2 2016</th>
<th>% H1 2016</th>
<th>Differential position</th>
<th>% Differential</th>
</tr>
</thead>
<tbody>
<tr>
<td>1º</td>
<td>Weak certificates</td>
<td>39.38</td>
<td>38.07</td>
<td>(-)</td>
<td>+1.31</td>
</tr>
<tr>
<td>2º</td>
<td>Protocols with weak encryption</td>
<td>31.23</td>
<td>33.44</td>
<td>(-)</td>
<td>-2.21</td>
</tr>
<tr>
<td>3º</td>
<td>Different kinds of vulnerabilities</td>
<td>16.49</td>
<td>22.39</td>
<td>(-)</td>
<td>-5.90</td>
</tr>
<tr>
<td>4º</td>
<td>Absence of encryption</td>
<td>12.91</td>
<td>6.11</td>
<td>(-)</td>
<td>+6.80</td>
</tr>
</tbody>
</table>

Table VII. Comparison of results compared with those obtained between the first and second semesters of 2016.

4. Results by Sectors of Activity

Table VIII shows a study of vulnerabilities that was conducted in terms of the sectors of activity into which the companies analysed are divided.
Regarding such results, the following significant data can be observed:

- In comparison with the previous semester, the configuration errors category experienced the greatest increase, particularly in consumer goods, industry, healthcare, public sector and consumer services. On the other hand, energy and public services have seen a decrease from 4.34% to 0.64%.

- The sectors that detected the most data leaks in metadata were telecommunications and technology. However, industry has decreased from 6.26% to 6.97% and the public sector from 6.19% to 6.52%. This last data shows that, in the public administrations and other bodies in this sector, there seems to be an improvement in the metadata management in public records. One factor to be borne in mind in this regard in the large amount of information published by the public administrations as a result of Law 11/2007 of 22 June on the Electronic Access of Citizens to Public Services. This law makes it obligatory to provide citizens with access to all electronic services, which has resulted in the digitization of all the documentation necessary to provide them: user manuals, forms, records, notifications and so on.

- Also noteworthy is the decrease to 4.94% in information management errors.

- On the other hand, the rise in cryptographic problems is noteworthy in the energy sector (20.89%) and the public services and raw materials sectors (88.89%).

Lastly, the energy sector and public services sectors have seen a rise from 12.62% to 27.95% in permissions, privileges and access control.
5. Results by Geographical Regions

As we can see in the Figure 6, the regions selected for this section are LATAM and EMEA, where there are more representative data in accordance with the number of customers.

![Figure 6. Vulnerabilities by geographical region.](image)

In the geographic areas of both LATAM and EMEA, data leaks in metadata are predominant, 55.57% and 37.32%, respectively. However, configuration errors were predominant in the first semester for the EMEA area.

Also noteworthy is the growth of the information management errors category in the LATAM area, which was risen from 16.85% to 30.33%. Whereas the EMEA area has also risen, yet in smaller proportions, from 9.24% to 14.34%.

The trend of the major vulnerabilities is repeated in a generalised manner in the two regions, with a high representation of data leaks in metadata, configuration errors, information management errors, inadequate validation of input data and cryptographic problems, the same as in the first semester.
6. Results by Degrees of Severity

The criterion for considering severities based on CVSS v2 [5] is that defined by the standard:

- Low for severities in the 0.0-3.9 interval.
- Average for severities in the 4.0-6.9 interval.
- High for severities in the 7.0-10.0 interval.

![Vulnerabilities by Severity](image)

Figure 7. Representation of degrees of severity by categories of vulnerability.

<table>
<thead>
<tr>
<th>Type of vulnerability</th>
<th>Buffer Overflow</th>
<th>Resource Management Errors</th>
<th>Configuration Errors</th>
<th>Information Management Errors</th>
<th>Data leak in Metadata</th>
<th>Session Handling</th>
<th>Cryptographic Problems</th>
<th>Permits, Privileges and Access Control</th>
<th>Inadequate Validation of Entry Data</th>
<th>Obsolete Versions</th>
<th>General total</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>1.11%</td>
<td>0.25%</td>
<td>0.26%</td>
<td>0.01%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>1.72%</td>
<td>0.01%</td>
<td>2.55%</td>
<td>0.02%</td>
<td>5.92%</td>
</tr>
<tr>
<td>Low</td>
<td>0.00%</td>
<td>0.00%</td>
<td>3.33%</td>
<td>23.92%</td>
<td>49.40%</td>
<td>0.58%</td>
<td>0.17%</td>
<td>0.75%</td>
<td>0.07%</td>
<td>0.03%</td>
<td>78.26%</td>
</tr>
<tr>
<td>Average</td>
<td>0.43%</td>
<td>0.27%</td>
<td>5.59%</td>
<td>0.91%</td>
<td>0.00%</td>
<td>0.00%</td>
<td>0.52%</td>
<td>3.24%</td>
<td>4.82%</td>
<td>0.04%</td>
<td>15.83%</td>
</tr>
<tr>
<td>General total</td>
<td>1.54%</td>
<td>0.52%</td>
<td>9.17%</td>
<td>24.84%</td>
<td>49.40%</td>
<td>0.59%</td>
<td>2.40%</td>
<td>4.01%</td>
<td>7.44%</td>
<td>0.09%</td>
<td>100.00%</td>
</tr>
</tbody>
</table>

Table IX. Representation of categories of vulnerability by degrees of severity.

If we observe these results together with the specific weights of the vulnerabilities, it is possible to see that the two categories with the highest percentages of results (data leak in metadata and information management errors) also correspond to those with the least number of high severities.
Following this consideration together with the weight over the total number of results and distribution of severities per category, the number of high vulnerabilities has fallen 5.92% with regards to the first semester (14.06%), as well as average severity vulnerabilities (15.83%).

7. Conclusions

The conclusions that have been drawn from this document are indicated below:

- 94.86% of the results obtained are due to five categories of vulnerabilities: data leaks in metadata (49.40%), information management errors (24.84%), configuration errors (9.17%), inadequate validation of input data (7.44%) and cryptographic problems (4.01%). These five categories represent 83.66% more than the first semester report.

- Some 87.01% of detected vulnerabilities indicate that the vast majority of failures are to be found in the configuration of equipment and systems, allowing the obtaining of different types of information, ranging from the software and product version to personal information on users. This trend has increased slightly (+5.01%) regarding the first semester, indicating that the origin of most of these problems detected are not vulnerabilities existing in the code created by the developers but in the poor practices of the system administrators.

- However, it has been possible to observe a 53.03% increase in the subcategory of files with sensitive information (information management errors) that, in development or testing environments, could represent a risk if not deleted. This information is not dangerous in and of itself, but if combined with fingerprinting techniques (use of banners and error messages on websites, versions in DNS servers), an attacker could get to know the target in detail.

- Of close to the total number of detected vulnerabilities, about 70% are related to SSL, either due to protocol versions with weak encryption or weak certificates. In addition, we should highlight the categories of weak certificates (39.38%), containing certificates which have expired, which are about to expire, which have been issued by an unreliable CA or for other domains and the absence of encryption (12.91%).

- The configuration errors category is that which has seen the greatest increase in comparison to the previous semester, particularly in consumer goods, industry, healthcare, the public sector and consumer services. On the other hand, energy and public services have seen a decrease from 43.48% to 0.64%.

- In the geographic areas of both LATAM and EMEA, data leaks in metadata are predominant (55.57% and 37.32%, respectively). However, configuration errors were predominant in the first semester for the EMEA area.
8. Bibliography


About ElevenPaths

At ElevenPaths we believe in the idea of challenging the current state of security, a characteristic which should always be present in technology. We are continually rethinking the relationship between security and people, with the aim of creating innovative products capable of transforming the concept of security and thereby keeping one step ahead of our attackers, who are increasingly present in our digital lives.

Further Information

www.elevenpaths.com

@ElevenPaths

blog.elevenpaths.com