|  |  |
| --- | --- |
|  | t  t |
|  | Penetration Testing Report |
|  | 04/06/2016 |
|  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Customer Information | | | | | |
| Company Name: | t | | | | | |
| City: | t | State: | t | Zip Code: | t | |
| URL: | t |  |  |  |  | |

|  |  |
| --- | --- |
| Customer Contact Information | |
| Contact Name: |  |
| Title: |  |
| Telephone: |  |
| E-mail: |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Consultant Information | | | | | |
| Company Name: | EY | | | | |
| Contact Name: | hadhemiadmin | | | | |
| Title: | trainee | | | | |
| Telephone: | 1234 | | | | |
| E-mail: | hadhemisamali@gmail.com | | | | |
| Business Address: | EY Building, Tunis | | | | |
| City | Tunisia | State: | MA | Zip Code: | 11111 |
| URL: | <http://www.ey.com> | | | | |

# Introduction

# Context and objectives

EY was responsible for conducting technical tests to evaluate the security level of t. In this document, will be reported the results of audit tests through the enumeration of identified vulnerabilities and the specification of recommendations in order to mitigate the related risks.

## Scope and limits

EY was responsible for conducting technical tests to evaluate the security level of t Portal and underlying IT infrastructure services accessible from the public networks at t.

The objective of the intrusion tests is to assess the security level of the in scope perimeter towards external attacks. This evaluation involves the following steps:

* Mapping of the audited scope,
* Vulnerability discovery and its existence validation through exploitation tests,
* Identification and assessment of risks associated to these vulnerabilities,
* Proposal of action plan to cover the identified risks.

## Testing conditions

Penetration Test approach used:

* **Full Testing**

Or

* **Black Box**

Or

* **Grey Box**

Tested environment:

* **Production**

**Or**

* **Pre-Production**

The following logical accesses were provided by t:

# Executive summary

The penetration test of t had the objective of evaluating its level of security with respect to best practices and security standards. The audit, conducted from the Internet has put forward several observations:

* Point 1
* Point 2
* Point 3

However, EY was able to achieve the goals of the assessment and exfiltrate the targeted data. There were a number of critical findings during the assessment including the following:

|  |  |
| --- | --- |
| Finding Name | Risk |
| Clickjacking: X-Frame-Options header missing | D-Critical |

MOAR STUFF

Therefore, we consider the level of security of this application insufficient because it has exploitable vulnerabilities that might have an impact on the confidentiality and integrity of the data it hosts.

The findings on the filtering mechanisms and access controls lead us to give a rating of **C**tot

|  |
| --- |
| Graphe |

In conclusion :

|  |  |
| --- | --- |
|  |  |

# Audit Methodology

## Types of test

The six types of test described below are different depending on the amount of information that the auditor has on the target and the knowledge possessed by the target on the auditor.

As part of the mission, purpose of this report, a specific methodology adapted to the context has been implemented inspired from several elements described below



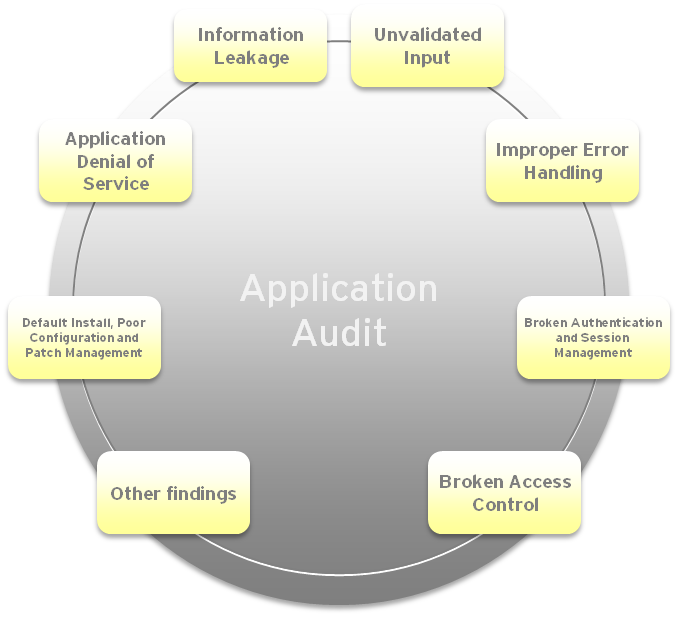
* **Blind**
* The auditor undertakes tests on the target with no prior knowledge of the security system, its components or its flows. The target is prepared to be audited while knowing in advance the details of this audit.
* **Double Blind**
* The auditor undertakes tests on the target with no prior knowledge of the security system, its components or its flows. The target is not notified in advance on the scope of this audit. Channels and vectors used for testing are also not announced.
* **Grey Box**
* The auditor undertakes tests on target with limited knowledge of the security system, its components and flows. The target is prepared to be audited while knowing in advance the details of this audit.
* **Double Grey Box**
* The auditor undertakes tests on target with limited knowledge of the security system, its components and has complete visibility of flows. The target is prepared to be audited while knowing in advance the details of this audit.
* **Tandem**
* The auditor and the target are prepared to audit and know in advance all the details of the audit.
* **Reversal**
* The auditor undertakes an audit of the target with full knowledge of all its processes and its operational security system. On the other hand, the target has no information on the nature of the tests or the date of their launches and how they are realized.

**Reference:**

* [OSSTMM 3](http://www.isecom.org/) The Open Source Security Testing Methodology Manual,
* [OWASP](https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents) Testing Guide Methodology.

## Risk assessment methodology

Our evaluation methodology is based on eight application areas:



You will find below a preview (the listed items are not exhaustive) of controls for each area:

* **A1 - Unvalidated Input**
* Identification of parameters
* Inserting unexpected values (negative, zero ...) and unexpected parameters
* Parsing errors
* Reflected values
* Unsanitized input transmitted to other application layers
* **A2 - Broken Access Control**
* Identification of access profiles
* What screens are authenticated?
* Who has access to what screen?
* Evaluation of horizontal segregation
* Attempt to access the data of another user
* Evaluation of vertical segregation
* Elevation of privilege attempt
* Functionalities analysis (identification of all functions and sensitive functions)
* **A3 - Broken Authentication and Session Management**
* Identify the authentication method
* Presence of trivial account
* Password policy Analysis
* Analysis of password recovery
* Certificates Verification
* Tests of bypass replay
* Session Management (inactivity, multiple login, ...)
* **A4 - Improper Error Handling**
* Information disclosure through technical errors
* Faulty log management
* **A5 - Information Leakage**
* Technical information disclosure
* Local File Inclusion (LFI)
* Full Path Disclosure
* Secrets disclosure
* Passwords
* Encryption keys
* **A6 - Application Denial of Service**
* Resistance to Denial of Service
* Identifying points latency
* Stress testing simultaneously latency points
* Sending unexpected data
* Resistance to reverse engineering
* **A7 - Default Install, Poor Configuration and Patch Management**
* Known and published vulnerabilities
* Testing pages with vulnerable functions
* Defaults users and passwords
* **A8 - Other findings**
* Static Analysis (Hex Editor, configuration file, Decompilation)
* Dynamic Analysis (Debugger)

## Risk Metrics Rating

#### *CVSS Rating*

The vulnerability rating is based on the CVSS v2 standard. Please refer to [https://www.first.org/cvss/v2/guide](http://www.first.org/cvss/cvss-guide.html) for full details.

Only the base metric is evaluated.

#### EY Risk Rating Evaluation

The EY grading is based on the risk associated with the vulnerability defined by its impact and by the level of exploitability, and in some cases, based on the authentication and the location parameters.

For each vulnerability, we estimate a risk rating defined by all the previous criteria using the following method:

* **Risk = Impact \* Exploitability \* (Authentication + Location)**
  + Ex1: Risk1 = (Critical impact \* Difficult exploitability \* (Anonymous + distant) = C-High.
  + Ex2: Risk2 = (High impact \* Standard exploitability \* (Authenticated + Local) = B-Medium.

NB: In some cases, the two criteria: **Authentication** and **Location** may not have any repercussion upon the risk. If the application being tested is not accessible from the internet, the **location** parameter does not have any impact on the risk evaluation.

|  |  |
| --- | --- |
| **D-Critical** | The risk associated with the vulnerability allows the total control of the system or the application. |
| **C-High** | The risk associated with the vulnerability allows partial control of the system or the application. |
| **B-Medium** | The risk associated with the vulnerability allows information disclosure which could facilitate advanced and targeted attacks. |
| **A-Low** | The risk associated with the vulnerability is very limited. It usually represents a lack of good practices follow-up, but doesn't have impacts on the company's stakes. |

#### Remediation effort

For each vulnerability identified, we estimate the ease of correction in order to correct or limit the vulnerability. We use the following possible values: Complex, Moderate, and Low. Below is a detailed description for each case.

|  |  |
| --- | --- |
| **Complex** | The correction of the identified vulnerability requires a complete modification of the code. This correction has an important impact on the system or the application audited. |
| **Medium** | The correction of the identified vulnerability requires some modification of the infrastructure supporting the application. Its impact needs to be identified in order to ensure that there will not be any side effects. |
| **Low** | The correction of the identified vulnerability requires a simple modification which will have little to no impact on the system or the application audited. |

#### Remediation Priority Level

For each vulnerability identified, we estimate the priority of remediation in order to correct or limit the vulnerability. We use the following possible values: Urgent, Standard, and Low. Below is a detailed description for each case.

|  |  |
| --- | --- |
| **Urgent** | The priority of remediation for the identified vulnerability requires a specific process besides the maintenance standard process. The correction of this vulnerability has to be immediate and treated as an important incident on the production platform. |
| **Standard** | The correction has to be integrated in the next release of the application/platform. |
| **Low** | The remediation priority is low and needs to be considered by the concerned teams. |

# Findings and Remediation:

## Full list of vulnerabilities:

| **EY reference** | **Title** | **Description** | **Severity** | **Location** | **Authentication** | **Host** | **Fix Status** |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Clickjacking: X-Frame-Options header missing |  | **D-Critical** | Network | None |  | KO |
|  | End of Life Systems In Use |  | **C-High** | Network | None |  | KO |

Legend:

|  |  |
| --- | --- |
| **KO** | The fix in place does not correct the vulnerability or no patch has been applied. |
| **OK** | The fix implemented efficiently corrects the vulnerability. |
| **N/A** | No fix has been implemented. |

## Full list of remediation

| **EY reference** | **Title** | **Description** | **Severity** | **Remediation effort** | **Recommendation (summary)** | **Host** |
| --- | --- | --- | --- | --- | --- | --- |
|  | Clickjacking: X-Frame-Options header missing |  | **D-Critical** | Quick |  |  |
|  | End of Life Systems In Use |  | **C-High** | Quick |  |  |

1. Detailed description of Vulnerabilities :

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Vulnerability** | Clickjacking: X-Frame-Options header missing | | | | | **ID** | 2015T114R-12 |
| **Brief Description** | | | | | | | |
| A Clickjacking vulnerability was detected. | | | | | | | |
| **Risk** | **D-Critical** | | **Category** | |  | | |
| **Assets** |  | | | | | | |
| **CVSS** | 9.9 | | | | | | |
| **CVSS Vector** | AV:Network/AC :Low/PR :Low/UI :None/S:Changed/C :High/I :High/A :High | | | | | | |
| **Description** | | | | | | | |
| Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. <br/><br/>  The server didn't return an X-Frame-Options header which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into other sites.  The impact depends on the affected web application. | | | | | | | |
| Impact | | | | | | | |
|  | | | | | | | |
| **Recommendation** | | | | | | | |
| **Urgency** | |  | | **Complexity** | | Quick | |
|  | | | | | | | |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Vulnerability** | End of Life Systems In Use | | | | | **ID** | 2015T114R-12 |
| **Brief Description** | | | | | | | |
| A Clickjacking vulnerability was detected. | | | | | | | |
| **Risk** | **C-High** | | **Category** | |  | | |
| **Assets** |  | | | | | | |
| **CVSS** | 7.0 | | | | | | |
| **CVSS Vector** | AV:Local/AC :High/PR :None/UI :Required/S:Unchanged/C :High/I :High/A :High | | | | | | |
| **Description** | | | | | | | |
| A number of End of Life Operating Systems were found on the internal network (e.g. Microsoft Windows XP). The consultant abused the lack of patching on a subset of these systems to gain a foothold in the internal network. | | | | | | | |
| Impact | | | | | | | |
|  | | | | | | | |
| **Recommendation** | | | | | | | |
| **Urgency** | |  | | **Complexity** | | Quick | |
|  | | | | | | | |