CYBER THREAT DEFENSE

Software Consulting

Security Report

SOFTWARE CONSULTING

Prepared by:

Daniel Ciobanu and Andrei Pusoiu

Cyber Threat Defense

Cluj-Napoca, Romania

30th of December, 2018

Document Properties

Title: “Software Consulting” Security Report

Version: 1.0

Author: Andrei Pusoiu

Security team: Andrei Pusoiu, Daniel Ciobanu, Horatiu Encian, Cristi Pop, Popescu Andrei, George Anton, Marc Alin

Reviewed by: Daniel Ciobanu

Approved by: “Software Consulting” Manager

Classification: Top Secret

Version Control			
Version	**Date**	**Author**	**Description**
0.1	**19 December 2018**	**Andrei Pusoiu**	**First Draft**
0.2	**20 December 2018**	**Andrei Pusoiu**	**Included Vulnerabilities**
0.3	**20 December 2018**	**Daniel Ciobanu**	**Review**
0.4	**21 December 2018**	**Andrei Pusoiu**	**Final**

EXECUTIVE SUMMARY

1.1 Scope of work

The scope of the penetration test is composed of:

- All the applications hosted at https://softwareconsulting.corp, IP:52.22.22.222
- All the applications hosted at https://api.softwareconsulting.corp, IP:22.220.222.20
- Any subdomains, sub-applications, APIs or servers that are under **softwareconsulting.corp** and may relate with the company products

Regarding the methods that are in the scope of testing we have agreed to use:

- **Black-box** penetration testing, in the first phase of the assessment, in order to simulate real world attacks, like an attacker would, without any access to documentation or server credentials.
- **White-box** penetration testing, in the second phase of assessment, providing all credentials necessary to the security team
- **High-impact** penetration testing methods will be used only against the QA environment, to not disturb the functionality of the production server.

Are considered out of scope the following items:

- Penetration testing on other servers, IPs, subdomains, than the ones mentioned in the Pentest Agreement Document.
- Social Engineering tricks – as requested by the client
- Denial Of Service – as requested by the client

1.2 Project Objectives

The following are considered to be the objectives of the penetration testing session:

- Identify all the vulnerabilities in Software Consulting applications and server that may help an attacker to obtain access to sensitive information, PII, bypass payments, disturb the functionality, collect sensitive data and take the right measures to mitigate the risks.

1.4 Timeline

The penetration testing was conducted between **19th of January** and **30th of January 2018**.

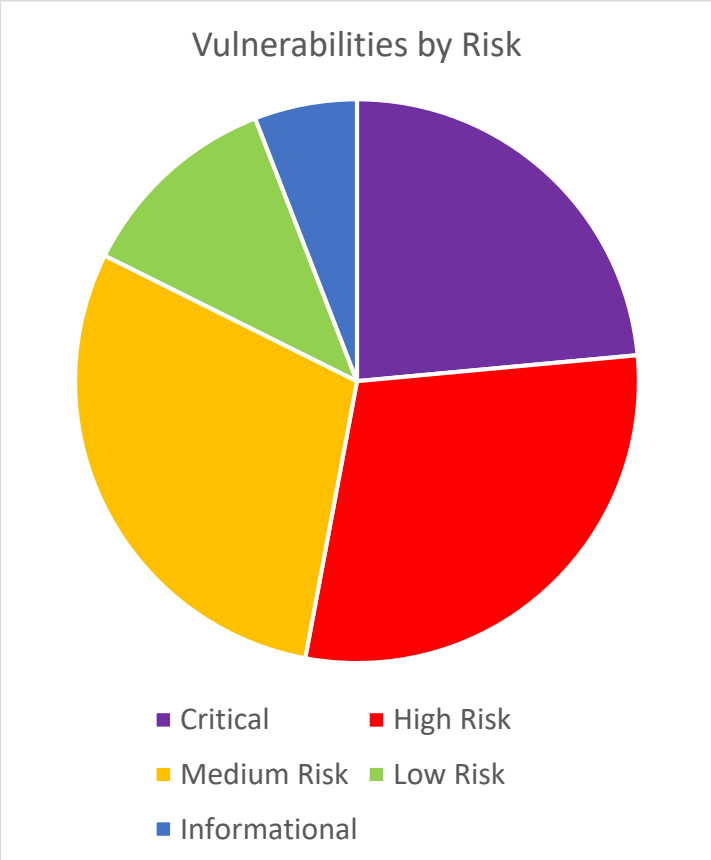
During this period no remarkable changes had occurred in the testing environments.

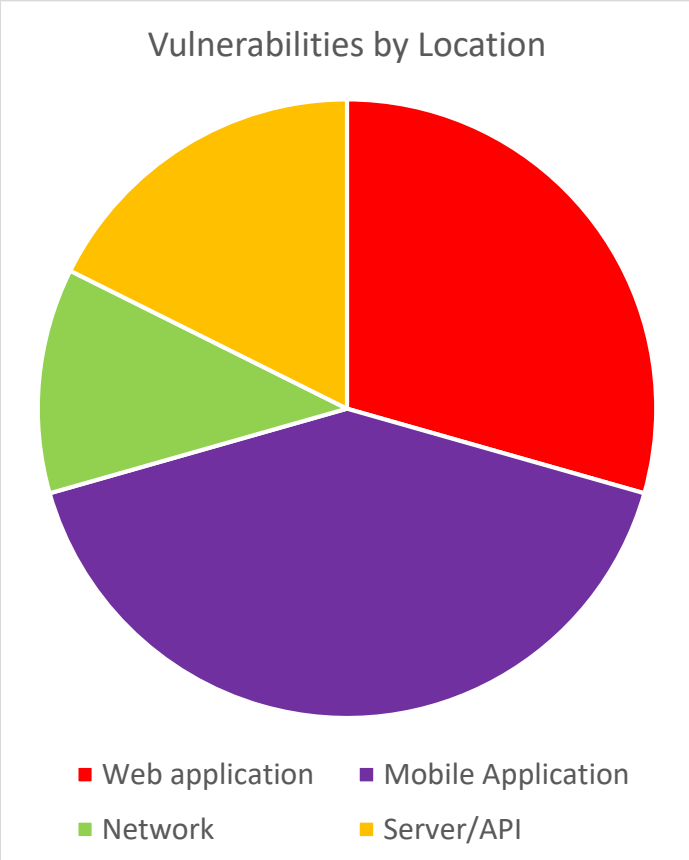
SUMMARY OF RESULTS

During the testing session of **softwareconsulting.corp** the security team has discovered a total of **17** vulnerabilities, from which five are considered of high **risk**.

There are four **Critical risk** vulnerabilities that needs to be remediated as fast as possible.

Risk level	Number
Critical	3
High	5
Medium	5
Low	2
Informational	2
Total	**17**





Vulnerabilities overview

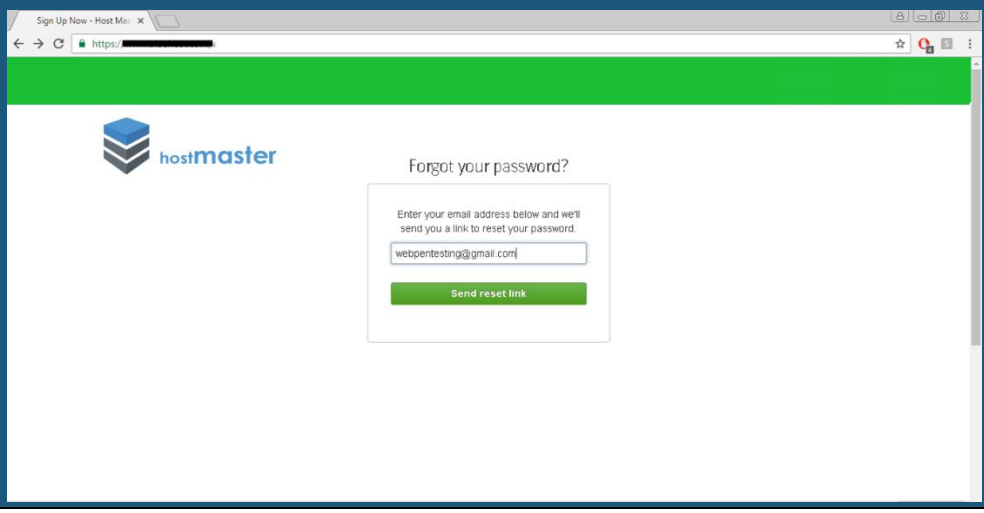
No.	Vulnerability	Risk
1	Admin interface is not protected with username and password	**Critical**
2	Database configuration files are exposed to public access	**Critical**
3	Users can bypass payments in all mobile applications	**Critical**
4	Admin password can be changed by anyone	**High**
5	Remote access can be obtained to the server from Wireless network	**High**
6	Any guest user can make his user Manager	**High**
7	An attacker can inject its own code and functionality into the application	**High**
8	Projects of other users can be downloaded by any user	**High**
9	Mobile application allows anyone to view content without paying	**Medium**
10	XSS vulnerability has been discovered in the search form	**Medium**
11	Users can be tricked to reset their password with any word	**Medium**
12	Encryption algorithm can be reverted and information viewed	**Medium**
13	Server functionality is vulnerable to Denial of Service	**Medium**
14	Attacker can enumerate the emails of all the users in the system	**Low**
15	Login form can be Brute-forced to discover valid accounts	**Low**
16	Mobile application do not uses HTTPs to encrypt traffic	**Low**
17	The webserver leak information about the technologies used	**Informational**

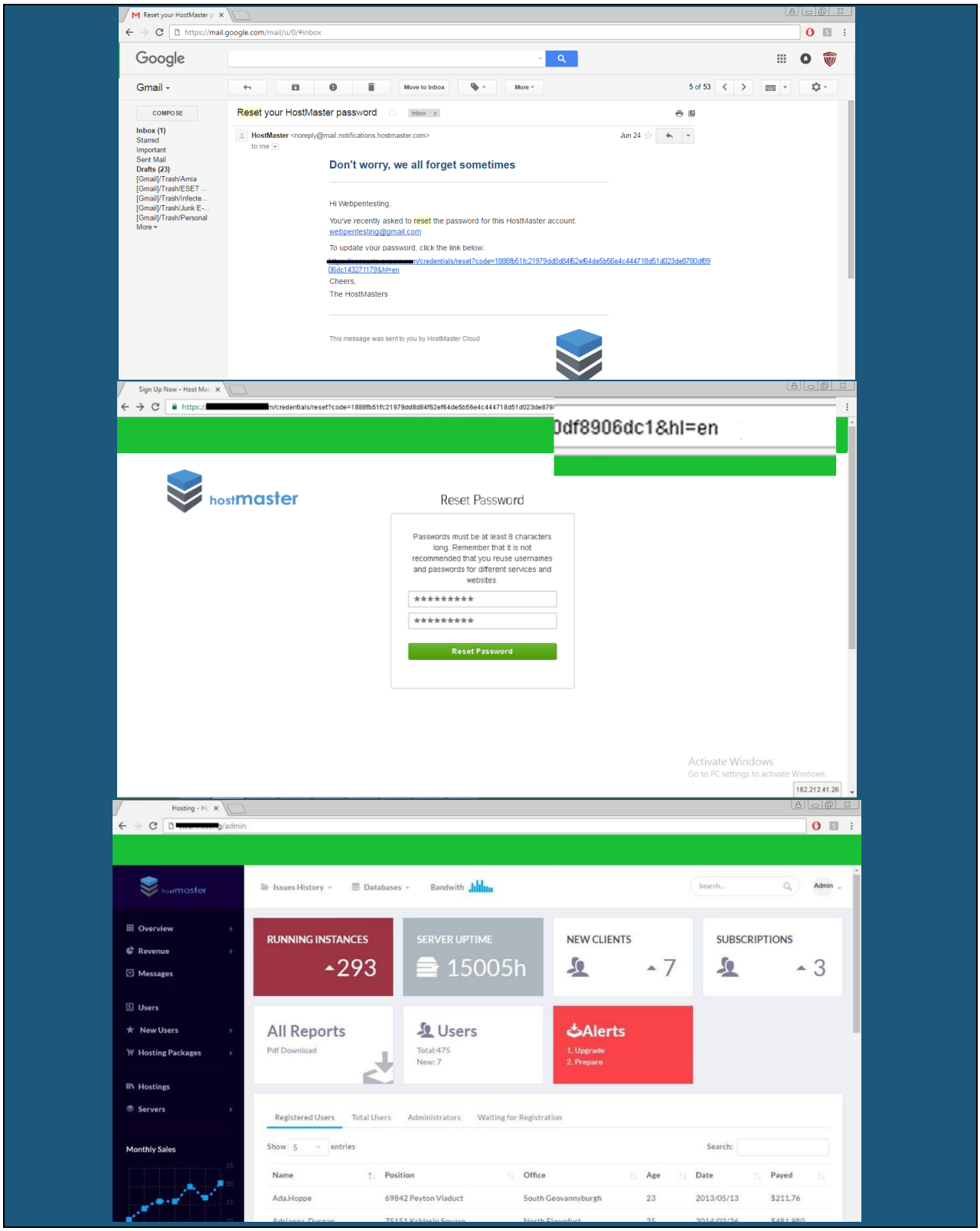
Details of each vulnerability are presented below.

Detailed **Software Consulting Vulnerabilities**

1. The password of Admin user can be changed by anyone

Affected Hosts	https://www.hosting.softwareconsult.corp/
Threat Level	**High**
Description	Our security team has discovered that the password of the admin users can be changed and access to the administration panel can be obtained. By doing this, an attacker can take full control over the server. **Vulnerability details** When resetting the password with the Forgot Password form, a link is sent to the email. The link contains the ID of the account. If the attacker changes the id of its account with the ID of the ADMIN account, which is ID=1, then he is able to change the password of the admin. **Affected endpoint** https://hosting.softwareconsult.corp/reset_password/ASDA18231asdasd1JJAoo**ID1** **Steps to reproduce** 1. Submit the Forgot Password form 2. In the email received, copy the LINK 3. Change your user ID with ID 1, admin 4. Reset password 5. Navigate to /admin
Recommendations	Do not send a valid Session token in the URL of the Password Reset link. Validate if the ID of the user in the URL is the same as the one of the user with the sent email. **Recommended reading** **https://www.owasp.org/index.php/Forgot_Password_Cheat_Sheet**




Reset your HostMaster password
https://mail.google.com/mail/u/0/#inbox
Google
Gmail
COMPOSE
Inbox (1)
Starred
Important
Sent Mail
Drafts (23)
Move to Inbox
More
5 of 53
Reset your HostMaster password
HostMaster <noreply@mail.notifications.hostmaster.com>
to me
Jun 24
Don't worry, we all forget sometimes
Hi Webpentesting,
You've recently asked to reset the password for this HostMaster account:
webpentesting@gmail.com
To update your password, click the link below:
Cheers,
The HostMasters
This message was sent to you by HostMaster Cloud
hostmaster
Reset Password
Passwords must be at least 8 characters long. Remember that it is not recommended that you reuse usernames and passwords for different services and websites.
Reset Password
Activate Windows
Go to PC settings to activate Windows.
Issues History
Databases
Bandwith
Admin
Overview
Revenue
Messages
Users
New Users
Hosting Packages
Hostings
Servers
Monthly Sales
RUNNING INSTANCES
293
SERVER UPTIME
15005h
NEW CLIENTS
7
SUBSCRIPTIONS
3
All Reports
Pdf Download
Users
Total:475
New: 7
Alerts
1. Upgrade
2. Prepare
Registered Users
Total Users
Administrators
Waiting for Registration
Show 5 entries
Search:
Name
Position
Office
Age
Date
Payed
Ada.Hoppe
69842 Peyton Viaduct
South Geovannyburgh
23
2013/05/13
$211,76

RECOMMENDATIONS

During the vulnerability assessment session the team discovered a set of issues that require immediate attention.

These are our recommendations:

Session Management and Permissions

There is a missing validation on the way the application manages the sessions, making possible to create accounts without passwords, security questions or private key. Also being able to access the views of different restricted pages should be fixed.

Reset password validation

Reset password functionality does not have a proper validation

Account creation

Account creation functionality is not properly validated so the user can end up without a security key or without password.

Parameter manipulation

The backend does not properly validates the matching between the parameter from the request and the user that runs the request.

RISK RATING

The overall risk of Software Consulting network is **Critical**.

In case of an attack against the system, an attacker can obtain access to admin functionalities, can create actions in the name of other users or alter the resources that do not belongs to it.

There is always the risk of obtaining access to other user's accounts and their resources as there is no brute-force protection.

A real attack may produce financial, user experience and technical losses.