Minds.com Platform

Full Disclosure

Performers: **Paolo Stagno** (aka voidsec – voidsec@voidsec.com)
Luca Poletti (aka kalup – kalup@voidsec.com)

Index

1. Introduction

In those last days a new social network called minds is getting attention over the internet, it aims to give transparency and protection to user data. Thanks to those last two points the new site has attracted the support of online activists including the hacking collective Anonymous.

We have then decided to give a look to that amazing platform, and we have seen that in reality is a long running project started in 2012 and that the product is still in beta. The first we tried has been a simple search and…well we find our first XSS so we decided to have some fun! The project is open source and we have already sent a notification to developers.

A little note before starting, within that social network there are payments options, CC and BTC, so any XSS is critical.

Here is a list of the vulnerability that we have found; they are almost all higly critical so we hope in a fast fix from developers.

1.1 Full Disclosure Policy

This document describes the security vulnerability disclosure policy of VoidSec Team Members.

It is the official policy of VoidSec Team Members (referred to as “us” or “we” hereafter) to exercise the responsible/coordinated disclosure of security vulnerabilities in a manner which is of maximum value to all affected parties. VoidSec reserves the right to change this policy at any time, without prior notice.

Current version: v1.1, last changed on August 12, 2013, 16.30

The permalink URL for this policy is: http://voidsec.com/disclosure-policy/

This policy states the ‘guidelines’ that we intends to follow.

For projects that have a public bug report page we cannot guarantee any disclosure time (or responsible disclosure), as anyone who has access to the bug report has the access to the vulnerability. In this case we evaluate a possible immediate publication (full disclosure) to promote a more rapid fix.

2. Key Findings

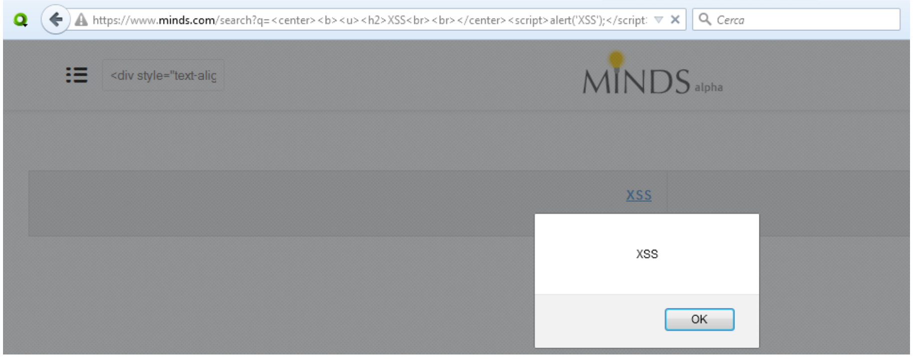
In this chapter we list all the vulnerabilities found during the test by the team

2.1 Multiple XSS

XSS in the search form

The search form is vulnerable to a reflected XSS, which can be triggered from the URL. This may lead to phishing attacks with the aim to steal credentials.

```
https://www.minds.com/search?q=<center><b><u><h2>XSS<br><br></center>&subtype=blog
```



https://www.minds.com/search?q=<center><b><u><h2>XSS<br><br></center><script>alert('XSS');</script

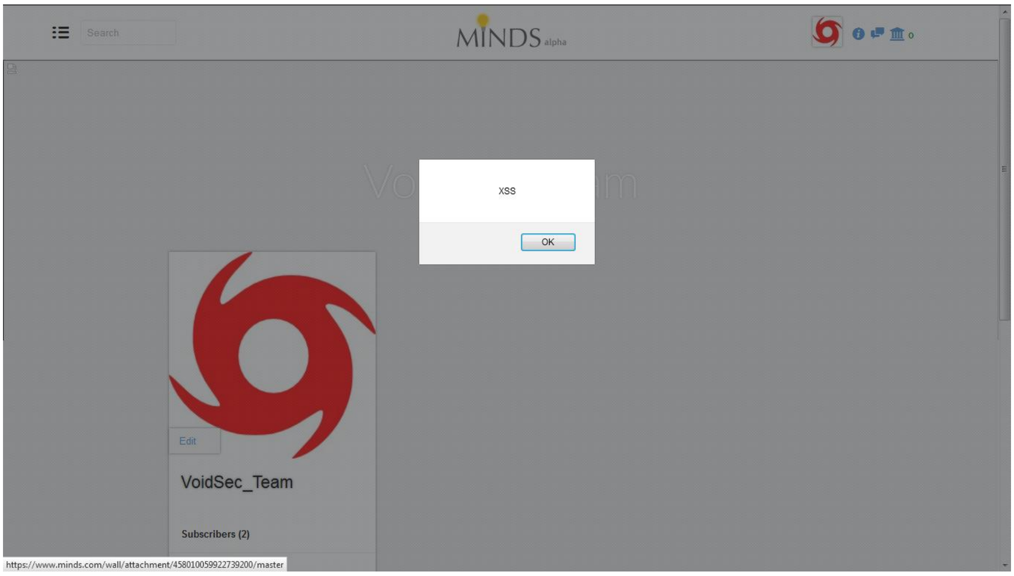
XSS within profile details

Some fields within user description are vulnerable to stored XSS attack, in particular the fields

- Place
- Website
- E-mail

This is quite critical since an attacker may steal credentials to every visitor to his profile

```
<script>alert('XSS');</script>
```



https://www.minds.com/wall/attachment/458010059922739200/master

XSS within Archive title

The title field within users archives are vulnerable to stored XSS injection; any user visiting an infected archive will execute the javascript the attacker has stored within the title.

```
<script>alert('XSS');</script>
```

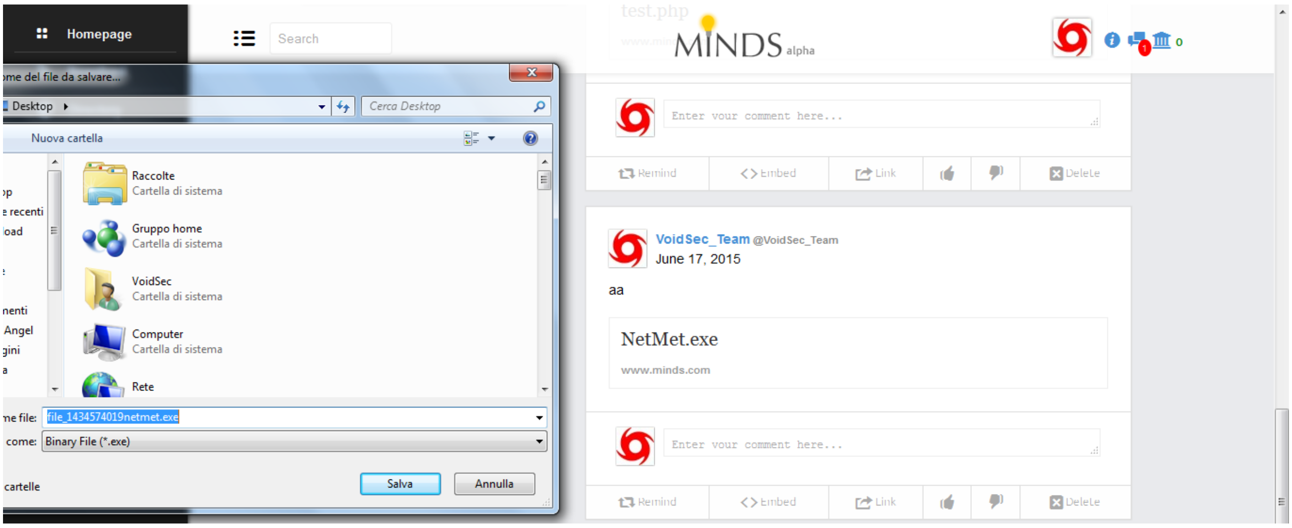
2.2 Delete of any message from any user

An attacker may easily delete any public post of any user from any location (profile, blog, groups)

```
https://www.minds.com/newsfeed/<insertPostID>/delete
```

2.3 Upload of arbitrary files

Any user may upload any file to the social network. This is quite destructive, because malware distribution campaigns may spread very fast on a platform like this one.



ne file: file_1434574019netmet.exe
come: Binary File (*.exe)

VoidSec_Team @VoidSec_Team
June 17, 2015
aa
NetMet.exe
www.minds.com

2.4 Edit profile data of any user

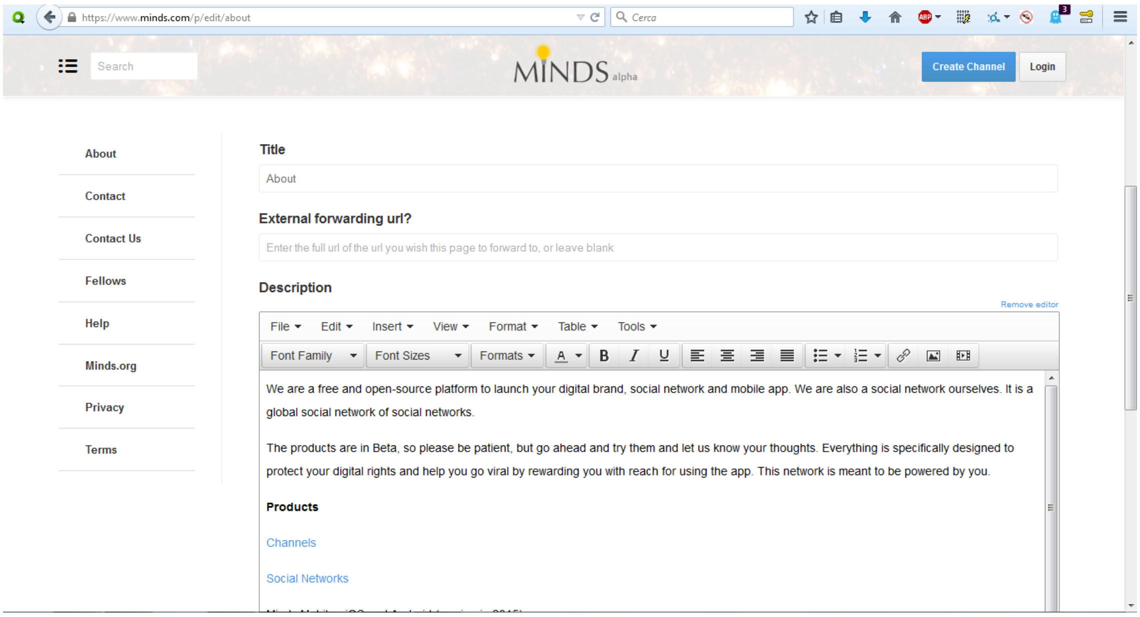
Using this vulnerability an attacker may edit profile data of any user. It wouldn't be such a destructive vulnerability if it wasn't that it can be combined with vulnerability #2.1 – XSS within profile details. In that way an attacker is sure that his victims will be exploited, because is no more necessary that victims visit attacker profile for being exploited, but they only need to visit their own profiles (default action after successful login) for being exploited. One attack vector, for example, could be the BeEF Hook (http://beefproject.com/)

```
https://www.minds.com/<NomeUtente>/custom
```

2.5 Unauthorized control of contents

Any visitor of the platform may completely defaces the main structure, eventually conducting phishing or malware distribution campaigns. An attacker even without being registered on the site may edit a pre-existent article (main page, FAQ, Tos, …) and insert arbitrary content. Overall the attacker may also delete any article within the main structure of the site.

```
/p/edit/<page_name>
```



Title

About

External forwarding url?

Enter the full url of the url you wish this page to forward to, or leave blank

Description

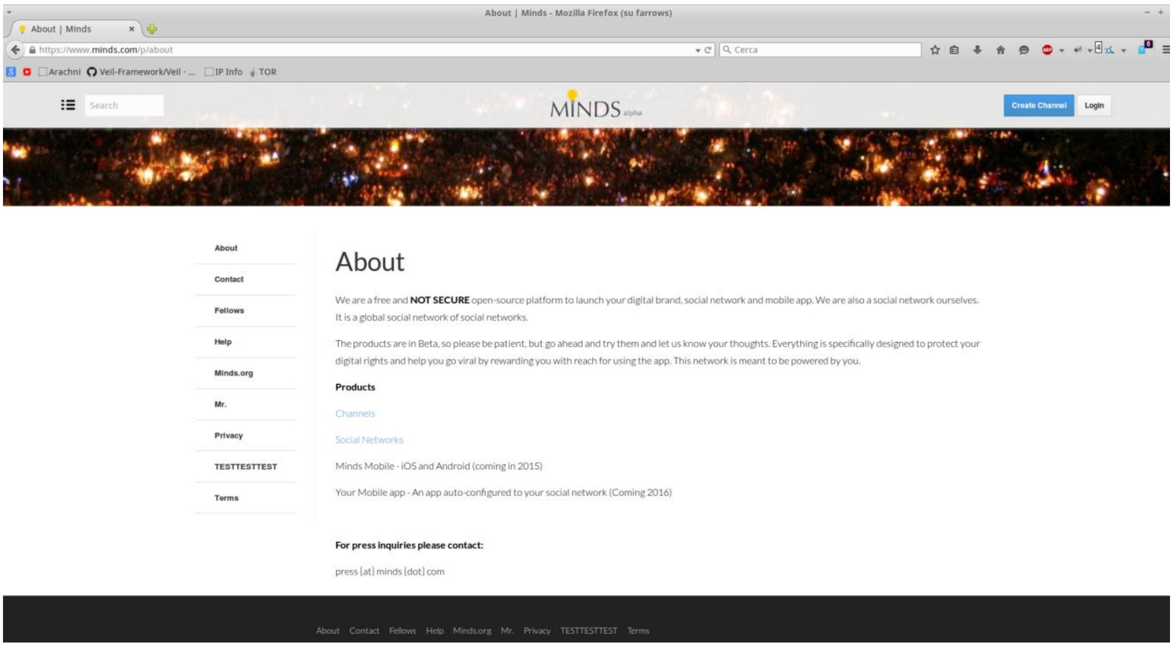
We are a free and open-source platform to launch your digital brand, social network and mobile app. We are also a social network ourselves. It is a global social network of social networks.

The products are in Beta, so please be patient, but go ahead and try them and let us know your thoughts. Everything is specifically designed to protect your digital rights and help you go viral by rewarding you with reach for using the app. This network is meant to be powered by you.

Products

Channels

Social Networks



About

We are a free and **NOT SECURE** open-source platform to launch your digital brand, social network and mobile app. We are also a social network ourselves. It is a global social network of social networks.

The products are in Beta, so please be patient, but go ahead and try them and let us know your thoughts. Everything is specifically designed to protect your digital rights and help you go viral by rewarding you with reach for using the app. This network is meant to be powered by you.

Products

Channels

Social Networks

Minds Mobile - iOS and Android (coming in 2015)

Your Mobile app - An app auto-configured to your social network (Coming 2016)

For press inquiries please contact:

press {at} minds {dot} com

About Contact Fellows Help Minds.org Mr. Privacy TESTTESTTEST Terms

Seems fixed at the moment of writing

3. Summary

We would like to remember and point out that the project is huge and is at beta stage, so things like those we have listed are not unbelievable, but we hope they will get fixed in a very short time.

Indeed those flaws are very critical since they allow an attacker to completely wipe the platform, potentially infect every user or steal their credentials and sensitive data.

We would lie to point out that we have only scratched the surface, we have done this little analysis by hand and we haven’t checked SQLi, CSRF, tokens and sessions, probably there are many other vulnerability there around.

4. Appendix

4.1 Tools

The team used several tools to perform the test, both opensource and proprietary.

- Burp Proxy
- Fiddler
- Tamper Data Firefox extension

4.2 About the team

Paolo Stagno:
Paolo Stagno, aka VoidSec, is a Cyber Security Analyst for iDialoghi, an Italian security firm based in Milan. He's consultant specialized in Penetration Test, Vulnerability Assessment, Information Security, Technology Risk, Network and Application Security for a wide range of clients across top tier international bank, major companies and industries. He is attending as speaker for various international conferences, like: DEFCON, BlackHat and Droidcon. He is also the leader and founder of VoidSec.com

Twitter: @Void_Sec
Email: voidsec@voidsec.com

Luca Poletti:
Luca Poletti, aka kalup, is an enthusiast of applied mathematics to computer security. His interest focus on cryptography, AppSec and WiFi networks.
He is a student at Politecnico di Torino in Mathematical Engineering and currently he is working as a financial tools developer. He is the co-founder of voidsec.com

Email: kalup@voidsec.com

About voidsec.com
We believe that, especially in Italy, in the last few years, the underground hacking community died, not for a lack of ideas or skills but because, in our opinion, we lost two fundamental requirements: a meeting place and the possibility to share.
VoidSec.com intends to give to all hackers a meeting place, where ideas can be shared freely; where: who know can return the knowledge to the community and a place where the inexperienced can learn.

Web Site: https://www.voidsec.com