Seekurity

STATE OF INFORMATION SECURITY

[Acknowledgements, Honors, Awards & CVEs]

Acknowledged by Fitbit Security Team
Fitbit Security Team
February 2019
Got acknowledged by Fitbit Security Team for discovering several severe bugs are undisclosed yet, because we disclosed one of the most critical ones, In this write-up we will show you how Seekurity team was able to harvest all the user's private/custom activities leaves more than 20 million private custom activities data in danger.

First of all, this write-up is not a new one and the discovery itself is dated back to 2017 but we decided to disclose it right now after we gave Fitbit the reasonable amount of time to patch the vulnerability and to protect the health data about the users!

Write-up: https://seekurity.com/services/goto/60
==========

Acknowledged by Zynga Whitehat Security
Zynga
February 2019
Got acknowledged by Zynga Whitehat Security Team, This is the first time i get an acknowledgement from a company not for discovering a security vulnerability but for a whole collaborative investigation between their me and Zynga's security team, During my investigation i discovered that one of Zynga's mobile games is leaking user critical information including "access token" which reveals a lot about the user who is playing the game along with other information.

Was a great pleasure working with Zynga's security team to discover such issues which later led them to discover that some users made a custom bots to automate some stuff inside this particular game, Hint: this game is one of their major ones.

I'm thinking about making a blog-post about the whole investigation but since i have no time for preparing (because the proof of concept screenshots and videos contains sensitive information and need to be edited by a video expert i will only mention some technical details later when i have time)

Whitehat Security Page: https://www.zynga.com/security/whitehats
==========

Acknowledged by Google Security
Google
January 2019
Got acknowledged by Google Security after reporting a trivial bypass bug affecting the logic of quota checking functionality which if exploited will give the attacker the ability to download a large file regardless of the quota limits that Google put in place as a mitigation/control for any kind of abuse.

Write-up: https://seekurity.com/services/goto/5z
==========

Seekurity Acknowledgements, Honors, Awards & CVEs

Acknowledged by Amazon
Amazon
November 2018
We at Seekurity have been acknowledged by Amazon for identifying multiple vulnerabilities in Amazon's PAYFORT PCI/DSS compliant Payment Processor PHP SDK.

During a quick trial security assessment of Payfort opensource PHP SDK (our work was not to touch anything related to Payfort.com or any company owned front-facing assets because that wasn't our scope or interest) and from the first glimpse our team discovered multiple vulnerabilities in the PHP code of their SDK that means ANY businesses implemented this SDK will be vulnerable to those discovered vulnerabilities hence the payment process itself could be hijacked.

The discovered vulnerabilities have been reported to Amazon Information Security Team through their security@amazon.com email and the team acknowledged them and worked closely with Payfort's team on a fix.

We're recommending updating the SDK to the newest version if your website is using it

Here is our advisory:
[-] Product Description:
PayFort is an Amazon company and a trusted online payment gateway enabling businesses, governments, SMEs, startups and institutions with innovative payment options for both the banked and non-banked online shoppers.

[-] CVE(s):
– CVE-2018-19186
– CVE-2018-19187
– CVE-2018-19188
– CVE-2018-19189
– CVE-2018-19190

[-] Product URL(s):
https://github.com/payfort/payfort-php-sdk

[-] Advisory blog-post:
https://seekurity.com/services/goto/4p

[-] Contact:
Info@Seekurity.com
911@Seekurity.com

Contributed to United Nations Security

United Nations Organization (UN.org)
September 2018
Found a data leak in the website of United Nations leaking thousands of applicants CVs.

Publications:
https://www.bleepingcomputer.com/news/security/united-nations-wordpress-site-exposes-thousands-of-resumes/
https://www.theregister.co.uk/2018/09/25/un_trello_jira_leak_vulnerability/

Technical Details:
https://www.seekurity.com/blog/general/united-nations-un-a-tail-of-leaking-thousands-of-job-applicants-cvs-and-documents-online-path-disclosure-and-information-disclosure-vulnerabilities/
==========

Acknowledged by AIT Pro's BulletProof Security Team
AIT Pro's BulletProof Security Team
May 2018
Got acknowledged by AIT Pro's Security Team for discovering CSRF issue in their WordPress BulletProof security plugin (both free and Pro versions) allowing a possible attacker to manipulate and toggle the security settings of the plugin itself.

Acknowledgement Link:
https://forum.ait-pro.com/forums/topic/bps-changelog/

Acknowledgement:
Security Improvement: Added CSRF Nonce verification in BPS MU Tools must-use plugin Toggle GET Request links. Special thanks to Mohamed A. Baset, Founder and CyberSecurity Advisor at Seekurity SAS de C.V. http://www.seekurity.com for reporting this security issue.

Product Details:
Link: https://wordpress.org/plugins/bulletproof-security/
Active installations: 80,000+
==========

Acknowledged by ASUS Product Security Team
ASUS Product Security Team
April 2018
Got acknowledged by ASUS Product Security Team for discovering a misconfiguration lead to a critical Information Disclosure vulnerability in their "Asus Control Center" during doing a passive reconnaissance i have discovered that their Apache Tomcat installation leaking its config file which contains a clear-text database connection password then i've sent an email asking for escalation permission to prove my PoC but they replied me that they acknowledge the issue as it is without any going further so i had to report it as it is.

[*] Blogpost with more details and advices: https://seekurity.com/services/goto/1f

[*] Acknowledgement:
We take every care to ensure that ASUS products are secure in order to protect the privacy of our valued customers. We constantly strive to improve our safeguards for security and personal information in accordance with all applicable laws and regulations, and we welcome all reports from our customers about product-related security or privacy issues. Any information you supply to ASUS will only be used to help resolve the security vulnerabilities or issues you have reported. This process may include contacting you for further relevant information.

April 2018:
Mohamed A. Baset of Seekurity.com SAS de C.V.
[*] Hall of Fame link: https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/
[*] Need a pentest for your website? Contact us: https://seekurity.com/services/goto/contactus
==========

Acknowledged by HP Product Security Response Team (PSRT) for CVE-2018-5921
HP Product Security Response Team (PSRT)
March 2018
Got acknowledged by HP Product Security Response Team (PSRT) for reporting a high severe web application vulnerability that could lead to Privileges Escalation affecting more than 80 different type of their product firmware.

Potential Security Impact:
Elevation of Privilege.
Reported by: Mohamed Abdelbasset Elnoby
Source:HP, HP Product Security Response Team (PSRT)

Advisory: CVE-2018-5921
Advisory link(s):
https://support.hp.com/us-en/document/c05949322?jumpid=reg_r1002_usen_c-001_title_r0001
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5921
https://nvd.nist.gov/vuln/detail/CVE-2018-5921

Multiple Critical Cross-Site Scripting Vulnerabilities in Crea8Social Social Network Script [CVE-2018-9120 - CVE-2018-9121 - CVE-2018-9122 - CVE-2018-9123]
MITRE/NVD - Crea8Social Social Network Script
March 2018
During a quick trial security assessment (not fully tested) of Crea8Social Social Network Script our team at Seekurity.com SAS de C.V. identified several severe Cross-Site Scripting Vulnerabilities in the platform that been widely used on the internet to create your own social network website (BTW this script used in the alleged new Egyptian Facebook named as EgFace.com). Our team responsibly contacted the vendor of the script but we got no answer and based on our Seekurity responsible disclosure rules which is a 90-day-disclosure-deadline or NON-Responsive vendor the bug details became visible to the public through our official communication channels.

[-] Advisory links and PoC Videos:
https://www.seekurity.com/blog/general/multiple-cross-site-scripting-vulnerabilities-in-crea8social-social-network-script/
– https://www.youtube.com/watch?v=bCf0hO9upto
– https://www.youtube.com/watch?v=QqJFh3Ame9g
– CVE-2018-9120
– CVE-2018-9121
– CVE-2018-9122
– CVE-2018-9123

[-] Attack Vectors:
– Escalation of Privileges: A normal user can create a bogus (user) account on Crea8Social platform hence hijack the Admin's account and takeover the whole installation.
– Client Side JS Code Execution: A normal user can create a bogus (user) account on Crea8Social platform with a stored XSS attack vector which will lead to execute JS code on behalf of all the user types passing by the attacker's public user profile page.
– Information Disclosure: A normal user can create a bogus (user) account on Crea8Social platform with a rough stored XSS attack vector to perform client side js code execution on other users sessions hence steal their session cookie or their private information from their accounts.
==========

Acknowledged by Facebook Security Team for 2018
Facebook
January 2018
With full pride i can say that I've got listed in Facebook Security Whitehat Hall of Fame for the 6th year in a row (2013, 2014, 2015, 2016, 2017 and 2018) for discovering several security vulnerabilities affecting facebook user's privacy and safety, All what i can say is that this is a huge progress in my career because the continuity of doing something great like protecting more than billion active users is something you can't maintain if you don't have this kind of competitive spirit, I hope to keep it up.

Acknowledgement: Mohamed A. Baset (Product Security at Linio, Cyber Security Advisor at Seekurity.com and Founder at BugBountyProgram.com)

Hall of Fame Link: https://www.facebook.com/whitehat/thanks
==========

Acknowledged by Apple
Apple
December 2017
Got acknowledged by Apple for responsibly reporting a trivial ClickJacking vulnerability affects their PrivFTP service web application (privftp.apple.com) for uploading RAW high resolution photos. The service was public back to 2006 and Apple made it requested private subscription through one of their application forms. They were protecting the whole application against ClickJacking vulnerabilities by checking the child and parent

using a Javascript code, I found a way to frame the whole application, bypass their mitigation technique and lure the victims into altering their email addresses with the attacker's one hence an account takeover scenario can be happened.

2016-08-31 privftp.apple.com:
A clickjacking issue was addressed. We would like to acknowledge Mohamed A. Baset of Seekurity.com SAS de C.V. Mexico for reporting this issue.

Hall of Fame link: https://support.apple.com/en-us/HT201536
==========

CVE-2017-17713 and CVE-2017-17714: Multiple SQL Injections and XSS Vulnerabilities found in the Hackers tracking tool "Trape" from "Boxug"
Boxug.com/Trape - MITRE/NVD
December 2017
[-] About the Tool:
Trape is a recognition tool that allows you to track people, the information you can get is very detailed. We want to teach the world through this, as large Internet companies could monitor you, obtaining information beyond your IP.

[-] Vulnerability Type:
Multiple SQL Injections and POST-based Cross Site Scripting vulnerabilities

[-] Impact and more info:
https://www.owasp.org/index.php/SQL_Injection
https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

[-] Version(s) affected:
Community and Professional version before "05-11-2017"

[-] Advisory Blog post:
https://www.seekurity.com/blog/general/cve-2017-17713-and-cve-2017-17714-multiple-sql-injections-and-xss-vulnerabilities-found-in-the-hackers-tracking-tool-trape-boxug/

[-] Facebook post and discussion [in Arabic]:
https://www.facebook.com/SymbianSyMoh/posts/2037883442893399

[-] PoC Videos:
1. Boxug/Trape (SQL Injection and taking over the hacker's SQLite Tracking database PoC) – Part 1
https://www.youtube.com/watch?v=RWw1UTeZee8
2. Boxug/Trape (SQL Injection & XSS and taking over the hacker's SQLite Tracking database PoC) – Part 2
https://www.youtube.com/watch?v=Txp6IwR24jY
3. Boxug/Trape (SQL Injection and taking over the hacker's SQLite Tracking database PoC) – Part 3

https://www.youtube.com/watch?v=efmvL235S-8

[-] Fixing Commit:
https://github.com/boxug/trape/commit/628149159ba25adbfc29a3ae1d4b10c7eb936dd3

[-] Assigned CVEs:
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17713
https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17714
https://nvd.nist.gov/vuln/detail/CVE-2017-17713
https://nvd.nist.gov/vuln/detail/CVE-2017-17714
==========

Acknowledged by OpenProject – Open source project management software for CVE-2017-11667
OpenProject.com
August 2017

Seekurity.com SAS de C.V. got acknowledged by OpenProject – Open source project management software for discovering a security issue affecting the session management.

The session authentication scheme for the APIv3, used in the majority of the angular-driven OpenProject work packages module, did not correctly check this setting and in turn, the setting did not matter for API session-based authentication. Users were able to use session for changes to work packages even past their allotted lifetime as long as the user did not leave the open work package module page. However, requests that and trigger a page refresh (e.g., visiting other modules or refreshing the page manually) cause the session to invalidate properly.

With this malfunction, an adversary hijacking an open session through whatever means could use it indefinitely for requests against the APIv3, as long as the owner of the session did not invalidate it through some page-refreshing request.

This security issue has been discovered by Mohamed A. Baset from Seekurity SAS de C.V and was disclosed to us yesterday evening. Thank you the elaborate report and for disclosing this directly to us. It is very much appreciated.

Advisory links:
1. https://www.seekurity.com/blog/general/openproject-session-management-security-vulnerability/
2- http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-11667
3- https://nvd.nist.gov/vuln/detail/CVE-2017-11667
4- https://www.openproject.org/openproject-6-1-6-released-security-fix/
5- https://www.openproject.org/openproject-7-0-3-released/
==========

Acknowledged by SimpleRisk – Open Source Risk Management System for CVE-2017-10711
SimpleRisk.com - Open Source Risk Management System
July 2017

Both Seekurity.com SAS de C.V. & Sonarify got acknowledged by SimpleRisk – Open Source Risk Management System for discovering a reflected cross site scripting vulnerability affecting the password reset form and can be exploited to hijack user password reset information then perform any actions on their behalf. For the record, the issue has been discovered by one of our upcoming products (Sonarify PTaaS) which uses some sort of AI and deep learning techniques in both Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) which will be released soon for corporate use only along with a free/community version.
Advisory links:
1-https://www.seekurity.com/blog/general/reflected-xss-vulnerability-in-simplerisk/
2-https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-10711
==========

Acknowledged by phpSocial/phpDolphin Social Network script [CVE-2017-10801]
phpSocial/phpDolphin
July 2017

Both Seekurity.com SAS de C.V. & Sonarify got acknowledged by author of phpSocial/phpDolphin for discovering a critical reflected cross site scripting vulnerability affecting their social network script and can be exploited to hijack user account and perform any actions on their behalf. For the record, the issue has been discovered by one of our upcoming products (Sonarify PTaaS) which uses some sort of AI and deep learning techniques in both Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST) which will be released soon for corporate use only along with a free/community version.

Advisory links:
1-
https://www.seekurity.com/blog/advisories/cross-sitescripting-vulnerability-in-phpsocial-aka-phpdolphin-social-network-script/
2- https://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-10801
==========

Acknowledged by Godaddy LLC.
Godaddy LLC.
June 2017

Sonarify got acknowledged by Godaddy Security team for discovering a reflected cross site scripting vulnerabilities affecting their parked domains redirector/processor) and can be exploited in a bug chain. For the record, the issue has been discovered by one of our upcoming products (Sonarify.com) which uses some sort of AI and deep learning techniques in Dynamic Application Security Testing (DAST) and will be released soon for corporate use only along with a free/community version.
Writeup link: https://goo.gl/xYu35X
PoC Video: https://goo.gl/Qh0aqC
==========

Acknowledged by Rapid7 - Metasploit Project Security Team (CVE-2017-5244)
Rapid7 LLC
June 2017

Seekurity Acknowledgements, Honors, Awards & CVEs

Seekurity.com SAS de C.V. got acknowledged by Rapid7 Metasploit Project Security Team for discovering a low severity CSRF vulnerability affects the web application of both versions (Express, Community and Professional) of Metasploit Project. This CSRF vulnerability can be used to perform an attack against all the running “Scans and Tasks” by metasploit project. Thanks for Rapid7 for acknowledging the issue and fixing it in a timely manner also many thanks for the generous gift package we got from them.

Writeup:
https://www.seekurity.com/blog/general/metasploit-web-project-kill-all-running-tasks-csrf-cve-2017-5244/
PoC Video: https://youtu.be/zWXIkzWd_cY

Acknowledgement in Rapid7 release notes:
Pro: MS-2708 - CVE-2017-5244 (CWE-352: Cross-Site Request Forgery) has been patched. Metasploit Pro, Express, and Community editions allowed GET requests to the stop and stop_all (task) routes. This should not have been the case, as they change the state of the service, and only should have been allowed through POST requests. In addition, the origin of the requests was not verified until after processing. This could have allowed an attacker to stop one, or all, Metasploit tasks by getting an authenticated user to run JavaScript (e.g. via loading a malicious URL). Now the routes are only exposed to POST requests, which validate the presence of a secret token to prevent CSRF attacks (via Rails' protect_from_forgery). This vulnerability was kindly reported to Rapid7 by Mohamed A. Baset (Founder and Cyber Security Advisor at Seekurity.com SAS de C.V. Mexico; @SymbianSyMoh).

https://help.rapid7.com/metasploit/release-notes/archive/2017/06/#20170613
Advisory details:
https://community.rapid7.com/community/metasploit/blog/2017/06/14/r7-2017-16-cve-2017-5244-lack-of-csrf-protection-for-stopping-tasks-in-metasploit-pro-express-and-community-editions-fixed
CVE MITRE: https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5244
NVD: https://nvd.nist.gov/vuln/detail/CVE-2017-5244
==========

Acknowledged by eBay Security
eBay, Inc.
June 2017
Both Seekurity SAS de C.V. & Sonarify got acknowledged by eBay Security team for discovering several reflected cross site scripting vulnerabilities affecting their JSON callbacks (web application wide) and can be exploited under some circumstances. For the record, the issue has been discovered by one of our upcoming products (Sonarify) which uses some sort of AI and deep learning techniques in Dynamic Application Security Testing (DAST) and will be released soon for corporate use only along with a free/community version.
PoC Video(s): https://goo.gl/0Eqq0k and https://goo.gl/VUI2He
Acknowledgements:
- Mohamed A. Baset, Founder and Cyber Security Advisor at Seekurity SAS de C.V. Mexico - www.Seekurity.com
- Sonarify - PTaaS, Vulnerability and Risk Management Platform - www.Sonarify.com

Hall of Fame link: https://pages.ebay.com/securitycenter/ResearchersAcknowledgement.html
==========

Acknowledged by Alibaba Security
Alibaba
May 2017
Got acknowledged by Alibaba Security team for discovering a very trivial reflected cross site scripting vulnerability affecting their JSON callbacks (web application wide) and can be exploited under some circumstances. For the record, the issue has been discovered by one of our upcoming products (Sonarify) which uses some sort of AI and deep learning techniques in Dynamic Application Security Testing (DAST) and will be released soon for corporate use only along with a free/community version.

PoC Video: https://goo.gl/fj1Jlb
Hall of Fame link: https://security.alibaba.com/en/fame.htm

==========

Acknowledged by Google Security
Google
May 2017
Got acknowledged by Google Security after reporting a *YET* undisclosed vulnerability that affects the google login workflow and gives a remote attacker the ability to retrieve the email address of the currently logged in google account which gives the attacker the ability to perform a spear phishing attack by knowing your exact email and gaining victim's trust hence asking the victim for introducing other sensitive information. (Can be used also in deanonymization attacks, to know who you are by just clicking on a crafted link)

Hall of Fame list: https://bughunter.withgoogle.com/characterlist/25
==========

Acknowledged by AirDroid Team
AirDroid.com
April 2017
Seekurity got acknowledged by the remote Android device management tool "AirDroid" for discovering a security vulnerability leads to hijacking user's AirDroid unencrypted session hence all the data on users android devices through Wifi or Local Area Networks. We've worked closely and responsibly with AirDroid team to address and mitigate the reported issues after that they've fixed the issue in their new mobile app (You can switch now to use HTTPS from the application setting menu thanks to our report) also they will push HTTPS on their web application very soon (since the authentication itself is initialized on secure connection)
Acknowledgement (on their about section of AirDroid's web version):
AirDroid is a fast, free app that lets you manage and control your device from a web browser without cables.
Thanks to suggestions and assistance from:
- Seekurity.com SAS de C.V. (Mexico)
PoC Video: https://www.youtube.com/watch?v=HOYEJMjeA90
==========

Acknowledged by AirDroid Team

AirDroid
April 2017
Seekurity got acknowledged by the remote Android device management tool "AirDroid" for discovering a security vulnerability leads to hijacking user's AirDroid unencrypted session hence all the data on users android devices through Wifi or Local Area Networks. We've worked closely and responsibly with AirDroid team to address and mitigate the reported issues after that they've fixed the issue in their new mobile app (You can switch now to use HTTPS from the application setting menu thanks to our report) also they will push HTTPS on their web application very soon (since the authentication itself is initialized on secure connection)

Acknowledgement (you can find it on their about section of AirDroid's web version):
AirDroid is a fast, free app that lets you manage and control your device from a web browser without cables.
Thanks to suggestions and assistance from:
- Seekurity.com SAS de C.V. (Mexico)

PoC Video: To be released soon
==========
Acknowledged by Facebook Security Team for 2017
Facebook
March 2017
Got listed in Facebook Whitehat Hall of Fame for the 5th year in a row (2013, 2014, 2015, 2016 and 2017) for discovering several security vulnerabilities affecting facebook users privacy - Mohamed A. Baset (Product Security at Linio, Cyber Security Advisor at Seekurity.com and Founder at BugBountyProgram.com)
Hall of Fame Link: https://www.facebook.com/whitehat/thanks
==========
Acknowledged by Bitdefender
Bitdefender
February 2017
Got rewarded and acknowledged by Bitdefender for the second time for reporting a pretty straightforward reflected Cross Site Scripting vulnerability that would be used by attackers to hijack your Bitdefender account hence all your Bitdefender's online services including Anti-theft solution connected to your devices and performing actions on your behalf "Wipe data, Lock device, etc..", Parental Control and more.

PoC Video: https://goo.gl/3UWBHn
Hall of Fame link: https://www.bitdefender.com/site/view/bug-bounty-hall-of-fame.html
All Credits goes to: Seekurity.com team.
Have concerns about your business security? Contact us: https://goo.gl/FUzMYF
==========
Acknowledged by HackerRank
HackerRank
January 2017
Appreciated by HackerRank for reporting several vulnerabilities affecting their web application, A one click full account takeover Cross Site Request Forgery, 1 reflected Cross Site Scripting and a Stored URI XSS.

PoC Video: https://www.youtube.com/watch?v=KlQhXFd2dbs
Credits: Seekurity.com Team
==========

Acknowledged by Microsoft Security (2017-Q1 Bounty Hunters: The Honor Roll)
Microsoft
January 2017
Seekurity.com got acknowledged by Microsoft Security Team in 2017-Q1 but this time in (Bounty Hunters: The Honor Roll) list for discovering a severe vulnerability affecting Outlook Service by stealing user's secret tokens.

The following researchers have submitted a qualifying vulnerability or new mitigation bypass techniques to Microsoft as part of the Microsoft Security Response Center (MSRC) Bounty Programs. We thank them greatly for their participation and for working with us to help keep customers safe.

Monetary reward: https://goo.gl/Lv6tGT
Hall of Fame Link: https://goo.gl/8nwdQf (Online Services)
==========

Acknowledged by Fitbit Security Team (Top 1)
Fitbit Security Team
December 2016
Finishing this year with another achievement unlocking, Got acknowledged by Fitbit Security Team topping all the bug hunters in fitbit's hall of fame list based to their statistics regarding how many valid security vulnerabilities I've reported and how severe it was.
These bugs are undisclosed yet (based on Fitbit Security Team's discretion) because of its critical nature which consists of IDORs, Private Information Disclosures, Full accounts takeover, CSRFs, Server side bugs, etc..
Very proud of protecting more than 19 million fitbit users and each achievement i have done before, May 2017s comes with more and more...
Thanks for your time reading this.
==========

Acknowledged by Prezi Security Team
Prezi
November 2016
Got rewarded and acknowledged by Prezi Security Team for discovering and responsibly reporting a security vulnerabilities chain affects their “Authentication process” which leads an account takeover with a 1 click.
.
Acknowledgment:
We hereby decree thanks most special to the security researchers and enthusiasts who managed to find vulnerabilities in our services and forthwith acted with the utmost responsibility by reporting them to us. You are a collection of quite beautiful souls and we are forever in your debt.
.
-Security Wall of Fame: https://bugbounty.prezi.com/timeline/

-Hackers Leaderboard (Top Hackers - Season II): https://bugbounty.prezi.com/#leaderboard
==========

Featured in Hakin9 Information Security Magazine
Hakin9 magazine
October 2016
Thanks a lot to Hakin9 magazine team (Marta Sienicka, Marta Strzelec, Marta Ziemianowicz) for having me in their Vol.11, No. 99. Got interviewed and answered lots of questions regarding the newly discovered QRLJacking attack vector also our QRLJacker framework. This volume can be purchased here: https://goo.gl/Bsl6vB.

Here's some links about QRLJacking attack if you are interested:

-OWASP official attack page as an attack vector
https://www.owasp.org/index.php/QRLJacking

- The attack's Wiki on OWASP's Github repo
https://github.com/OWASP/QRLJacking/wiki

-QRLJacker framework to automate the QRLJacking attack
https://github.com/OWASP/QRLJacking/tree/master/QrlJacking-Framework

-TheHackerNews article about the attack
https://thehackernews.com/2016/07/qrljacking-hacking-qr-code.html

-Videos demonstrating the attack and real life attack vectors
QRLJacker Framework 1.0 Teaser
https://www.youtube.com/watch?v=H6YsnT1KHA4

WhatsApp QRHijacking Vulnerability
https://www.youtube.com/watch?v=4QwyBXiZhG0

WhatsApp Accounts Hijacking and ARP poisoning
https://www.youtube.com/watch?v=JCoPSdQvESc

AirDroid vulnerable to QRLJacking Vulnerability
https://www.youtube.com/watch?v=jenmicugWoo

Vulnerable Web Applications and Services uses Login by QR Code Feature part #1
https://www.youtube.com/watch?v=lx-qnQ0ltpI

Vulnerable Web Applications and Services uses Login by QR Code Feature part #2
https://www.youtube.com/watch?v=Nc_NyR06U5Q

-If you are interested to present QRLJacking anywhere we made a very good presentation for the attack and you can find it here: https://prezi.com/1e8w98atg6dx/qrljacking/

==========

Acknowledged by RunKeeper Security Team
RunKeeper.com
July 2016

Got Acknowledged by RunKeeper which is a well known fitness application capable to be connect and analyze your fitness data with various devices. We discovered a stored cross site scripting vulnerability and some site-wide CSRF bugs which lead to a messy full account takeover scenarios without users interaction (XSS Worm)

.

PoC and Writeup: https://goo.gl/EURgoY

==========

Founded "QRLJacking" Attack vector!
OWASP Foundation
July 2016

[*] What is QRLJacking?
QRLJacking or Quick Response Code Login Jacking is a simple social engineering attack vector capable of session hijacking affecting all applications that rely on “Login with QR code” feature as a secure way to login into accounts. In a simple way, In a nutshell victim scans the attacker’s QR code results of session hijacking.

[*] QRLJacking and Advanced Real Life Attack Vectors:
As we all know, If we combined more than one attack vector together we can have a great result. QRLJacking attack can be combined with a powerful attack vectors and techniques to make it more reliable and trustworthy. Here are some examples:
1. Social Engineering techniques (Targeted Attacks)
2. Highly Trusted Hacked Websites
3. SSL Stripping
4. Content Delivery Networks (CDNs Downgrading)
5. Non-secure Traffic over LAN
6. Bad Implementation / Logic

[*] Vulnerable Web Applications and Services:
There is a lot of well-known web applications and Services which are vulnerable to this attack till the date we wrote this paper. Here's some examples (that we have reported) including but not limited to:
1. Chat Applications: WhatsApp, WeChat, Line, Weibo, QQ Instant Messaging
2. Mailing Services: QQ Mail (Personal and Business Corporate), Yandex Mail
3. eCommerce: Alibaba, Aliexpress, Taobao, Tmall, 1688.com, Alimama, Taobao Trips
4. Online Banking: AliPay, Yandex Money, TenPay
5. Passport Services “Critical”: Yandex Passport (Yandex Mail, Yandex Money, Yandex Maps, Yandex Videos, etc...)

6. Mobile Management Software: AirDroid
7. Other Services: MyDigiPass, Zapper & Zapper WordPress Login by QR Code plugin, Trustly App, Yelophone, Alibaba Yunos

[*] References:
https://www.owasp.org/index.php/QRLJacking
https://github.com/OWASP/QRLJacking
https://github.com/OWASP/QRLJacking/wiki
==========

Acknowledged by BlackBerry Security Incident Response Team (SIRT)
BlackBerry Security Incident Response Team
June 2016
Seekurity team got acknowledged by BlackBerry Security Incident Response Team (SIRT) for discovering and responsibly reporting a security vulnerability affects their “Invitation System” which gives the attacker the ability to send a tweet in behalf of the subscribers.

Acknowledgment:
The BlackBerry SIRT thanks the following people and organizations for reporting security issues under the industry practice of coordinated disclosure and working with the team to protect BlackBerry customers.
Mohamed Abdelbasset Elnouby, Seekurity.com Inc.

Hall of Fame (Acknowledgements 2016)
http://us.blackberry.com/enterprise/products/incident-response-team.html
==========

Acknowledged by Telegram
Telegram
April 2016
Acknowledged by Telegram Security Team for reporting a Security Vulnerability affecting their official Telegram Web Client and Webgram client.

https://www.seekurity.com/blog/general/telegram-web-client-clickjacking-vulnerability/

https://www.inforge.net/ezine/1611/scoperta-una-vulnerabilita-clickjacking-in-telegram-web-client/#YlwZE3eFpIlGqEOf.01
==========

Acknowledged by Prezi Security Team
Prezi
March 2016
Got rewarded and acknowledged by Prezi Security Team for discovering and responsibly reporting a security vulnerability affects their “Authentication process” which leads a full account takeover with only a 1 click.
.
Acknowledgment:

Seekurity Acknowledgements, Honors, Awards & CVEs

We hereby decree thanks most special to the security researchers and enthusiasts who managed to find vulnerabilities in our services and forthwith acted with the utmost responsibility by reporting them to us. You are a collection of quite beautiful souls and we are forever in your debt.

.

-Security Wall of Fame: https://bugbounty.prezi.com/timeline/

-Hackers Leaderboard (Top Hackers - Season II): https://bugbounty.prezi.com/#leaderboard

==========

Acknowledged by United Airlines

United.com

March 2016

Got Acknowledged by United Airlines for discovering some critical security vulnerabilities and got a 1,000,000 miles in total as a reward under their bug bounty program.

More: https://goo.gl/ti6oag

News:

http://gate.ahram.org.eg/News/883417.aspx

https://www.youm7.com/story/2016/3/15/%D8%B4%D8%A7%D8%A8-%D9%85%D9%86-%D8%A7%D9%84%D8%A3%D9%82%D8%B5%D8%B1-%D9%8A%D9%83%D8%AA%D8%B4%D9%81-%D8%AB%D8%BA%D8%B1%D8%A9-%D8%A8%D8%AA%D8%B7%D8%A8%D9%8A%D9%82-United-Airlines%D9%88%D9%8A%D8%AD%D8%B5%D9%84-%D8%B9%D9%84%D9%89-250/2630014#.VueycBIrKDU

http://www.arageek.com/tech/2016/03/15/meet-the-most-famous-whitehat-hackers.html?utm_content=buffer522fc&utm_medium=social&utm_source=facebook.com&utm_campaign=

http://www.alaraby.co.uk/medianews/2016/3/16/%D9%83%D9%8A%D9%81-%D8%A3%D9%86%D9%82%D8%B0-%D8%A7%D9%84%D9%87%D8%A7%D9%83%D8%B1-%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%8A-%D9%85%D8%AD%D9%85%D8%AF-%D8%B9%D8%A8%D8%AF%D8%A7%D9%84%D8%A8%D8%A7%D8%B3%D8%B7-%D8%B7%D9%8A%D8%B1%D8%A7%D9%86-%D8%A7%D9%84%D8%A7%D8%AA%D8%AD%D8%A7%D8%AF

http://lebanon360.org/article-desc_33320_%D9%83%D9%8A%D9%81%20%D8%A3%D9%86%D9%82%D8%B0%20%D8%A7%D9%84%D9%87%D8%A7%D9%83%D8%B1%20%D8%A7%D9%84%D9%85%D8%B5%D8%B1%D9%8A%20%D9%85%D8%AD%D9%85%D8%AF%20%D8%B9%D8%A8%D8%AF%D8%A7%D9%84%D8%A8%D8%A7%D8%B3%D8%B7%20%D8%B7%D9%8A%D8%B1%D8%A7%D9%86%20'%D8%A7%D9%84%D8%A7%D8%AA%D8%AD%D8%A7%D8%AF'%D8%9F

==========

Acknowledged by AOL Security Team

AOL

February 2016

The AOL Security Team would like to thank the following security researchers for the responsible disclosure of security issues related to AOL and its brands:

Hall of Fame link: https://contact.security.aol.com/hof/

Vulnerabilities and PoCs:
1- AOL Favorites HTML Injection and CSS Manipulation, PoC: https://goo.gl/Sx15wt & https://goo.gl/wXZl8u
2- AOL Billings Clickjacking, PoC: https://goo.gl/K0uUb4

Read more:
About ClickJacking: https://goo.gl/24HAlC
About Html Injection: https://goo.gl/1AajCu
==========

Facebook Whitehat Hall of Fame 2015
Facebook
December 2015
Got listed in Facebook Whitehat Hall of Fame for the 3rd year in row (2013, 2014 and 2015) for discovering a lot of security vulnerabilities. 2016 We're coming - "Mohamed Abddelbasset Elnouby (Senior Information Security Analyst at Linio, Founder at BugBountyProgram.com)".

Hall of Fame Link: https://www.facebook.com/whitehat/thanks
==========

Acknowledged by RedHat
RedHat
November 2015
Got Acknowledged by Redhat Security team for finding some flaws in their web application "User Portal" that may lead to full account takeover scenario through manipulating the "referer" value and leveraging the attack to be open redirection or a reflected cross site scripting.

Red Hat would like to thank the following individuals and organisations that have privately reported security issues that affected Red Hat branded websites or online services and agreed to be listed.

-PoC Videos:
1. Redhat Open Redirection via Auto Referrer Manipulation
https://goo.gl/koI7K7
2. Redhat XSS via Auto Referrer Manipulation
https://goo.gl/umG6ws
-About XSS: https://goo.gl/EYngep
-Hall of Fame Link: https://goo.gl/wQ322e
==========

Acknowledged by Microsoft Security for June, July and August in a row.
Microsoft

October 2015
Acknowledged by Microsoft Security Team in June, July and August for discovering several CSRF vulnerabilities affecting Live.com Service, social network so.cl and a Post-Based Cross Site Scripting affecting their Microsoft Home Use Program.

The Microsoft Security Response Center (MSRC) is pleased to recognize the security researchers who have helped make Microsoft online services safer by finding and reporting security vulnerabilities. Each name listed represents an individual or company who has privately disclosed one or more security vulnerabilities in our online services and worked with us to remediate the issue.

Mohamed Abdelbaset Elnoby (@SymbianSyMoh)
Seekurity.com - Information Security Consultations

Proof of Concept Videos: https://goo.gl/6D1BYC, https://goo.gl/S6n0yK, https://goo.gl/znuvC0
Hall of Fame Link: https://goo.gl/PDekZa
About CSRF: http://goo.gl/0aSULX
About XSS: https://goo.gl/EYngep
==========

Mentioned by US Department of Homeland Security
US Homeland Security
October 2015
Link:
https://www.dhs.gov/sites/default/files/publications/dhs-daily-report-2015-10-22.pdf [Item no 25]

Mention:
25. October 21, Softpedia – (International) Firefox FindMyDevice service lets hackers wipe or lock phones, change PINs. Researchers discovered a flaw in Mozilla's "Find My Device" service for devices running the Firefox operating system (OS) in which a hacker could remotely lock device screens, make devices ring, and wipe all device data via clickjacking-enabled cross-site request forgery (CSRF) attacks. The attack requires the user to be logged in to the service with their Firefox account.
Source:
http://news.softpedia.com/news/firefox-findmydevice-service-lets-hackerswipe-or-lock-phones-change-pins-495003.shtml
==========

Acknowledged by Uber Security Team
Uber
September 2015
Acknowledged by Uber for reporting a CSRF Vulnerability related to one of their Implemented Entertainment Systems. As a special thanks to individuals who have reported previously-unknown vulnerabilities of high or critical security, Uber will maintain a list of credits on this page.

Mohamed Abdelbasset Elnouby - https://mx.linkedin.com/in/SymbianSyMoh

Hall of Fame Link: https://goo.gl/js9i8P
==========

Acknowledged by Alibaba Group (AliExpress and AliPay)
Alibaba Group
August 2015
I've got listed in Alibaba Group's Hall of Fame for discovering a Cross Site Scripting in it's Huge Marketplace AliExpress.com and a Cross Site Request Forgery in it's main Payment Service AliPay.com allows attackers to hijack any AliPay account by changing the victim's SMS Number.

Below name list are people who have successfully submitted security vulnerabilities to ASRC. A million thanks to everybody is not only for helping Alibaba Group to improve the product securities but also for the safety trading of billions of Alibaba users.

-Mohamed Abdelbaset Elnouby http://www.Seekurity.com/

-Proof of Concept Videos:
1. AliExpress XSS and Information Disclosure: https://goo.gl/B67Wt5
2. AliPay Initial User SMS Hijacking CSRF: https://goo.gl/QFbXU7
3. Alipay SMS Hijacking CSRF: https://goo.gl/BRHWuy
-Hall of Fame: https://goo.gl/VvN7sW
-About CSRF: http://goo.gl/0aSULX
==========

Acknowledged by WordPress
Automattic
August 2015
WordPress 4.2.4 is now available. This is a security release for all previous versions and we strongly encourage you to update your sites immediately.

This release addresses six issues, including three cross-site scripting vulnerabilities and a potential SQL injection that could be used to compromise a site, which were discovered by Marc-Alexandre Montpas of Sucuri, Helen Hou-Sandí of the WordPress security team, Netanel Rubin of Check Point, and Ivan Grigorov. It also includes a fix for a potential timing side-channel attack, discovered by Johannes Schmitt of Scrutinizer, and prevents an attacker from locking a post from being edited, discovered by Mohamed A. Baset.

Links:
-https://wordpress.org/news/2015/08/wordpress-4-2-4-security-and-maintenance-release/
-http://news.softpedia.com/news/wordpress-4-2-4-fixes-three-xss-vulnerabilities-and-one-potential-sql-injection-488470.shtml
-https://core.trac.wordpress.org/changeset/33543
==========

Acknowledged by SourceForge
SourceForge
July 2015
Once the bug has been fixed, if desired, we can provide public thanks and acknowledgement on this page, and we can give a mention via @sourceforge on Twitter, our Facebook page, and/or Google+ page.

July 2015 - Mohamed Abdelbasset Elnouby (www.Seekurity.com) - CSRF vulnerability

Hall of Fame Link: http://goo.gl/vdL29d
About CSRF: http://goo.gl/0aSULX
==========

Listed in Microsoft's Security Researchers Acknowledgment List (April)
Microsoft
June 2015
The Microsoft Security Response Center (MSRC) is pleased to recognize the security researchers who have helped make Microsoft online services safer by finding and reporting security vulnerabilities. Each name listed represents an individual or company who has privately disclosed one or more security vulnerabilities in our online services and worked with us to remediate the issue.

•Mohamed Abdelbaset Elnoby of Seekurity Inc. "http://www.Seekurity.com"

A brief about the vulnerability:
This is a Post based cross site scripting vulnerability in Ovi Store that related to Nokia.com, This vulnerability allows the attackers to hijack any of Ovi Store Accounts or even execute a malicious javascript on the domain scope.

Vulnerability: Post-Based XSS
Proof of Concept Video: https://goo.gl/MxXLcu
Hall of Fame Link: https://goo.gl/PDekZa
About XSS: https://goo.gl/EYngep
==========

Listed in eBay's Security Researchers Hall of Fame
eBay Inc.
June 2015
We thank everyone for their contributions, but from time to time, we will want to publicly acknowledge and thank members of our community on our Responsible Disclosure Acknowledgement Page (and elsewhere) for reporting a problem on our Security Researchers page.

•Mohamed A. Baset Senior Information Security Analyst at Seekurity Inc. "http://www.Seekurity.com"

Vulnerability: Stored Cookie XSS
Proof of Concept Video: http://goo.gl/Oqt0Jc

Hall of Fame Link: http://goo.gl/O8z0f2
About XSS: https://goo.gl/EYngep
==========

Acknowledged by AngelList
AngelList.
May 2015
Got Acknowledged by AngelList website for reporting multiple CSRF Vulnerabilities.

We'd like to thank the following for reporting vulnerabilities to us:

•Mohamed Abdelbaset Elnoby from Seekurity Inc.

Hall of Fame: https://angel.co/help/contact/bugs
==========

Acknowledged by MikroTik RouterOS for an Admin Password Reset CSRF Vulnerability affects all versions before 5.0 [CVE-2015-2350]
RouterOS
April 2015
MikroTik RouterOS is an operating system based on the Linux kernel. Installed on the company's proprietary hardware (RouterBOARD series), or on standard x86-based computers, it turns a computer into a network router and implements various additional features, such as firewalling, virtual private network (VPN) service and client, bandwidth shaping and quality of service, wireless access point functions and other commonly used features when interconnecting networks. The system is also able to serve as a captive-portal-based hotspot system.

The Vulnerability:
All MikroTik RouterOS versions before v5.0 are vulnerable to a get based CSRF Attack which lead to Admin Password Reset

PoC Video: http://goo.gl/SJrLVK
CVE-2015-2350 [NIST]: http://goo.gl/S7ovHU
CVE-2015-2350 [MITRE]: http://goo.gl/Vqt97k
About CSRF: http://goo.gl/P3gp70

==========

Contributed to the core of Rapid7 Metasploit project's Security.
Rapid7 LLC
April 2015
The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.

Its best-known sub-project is the open source Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive and related research.
__"Wikipedia"

The Vulnerability:
All Metasploit Project Free/Pro web interface version < 4.11.1 (Update 2015021901) are vulnerable to a CSRF(s) and Login Brute Force attacks which could lead to fully compromise the whole project.

Acknowledgement:
Pro: Metasploit is no longer vulnerable to a CSRF attack that allowed the creation of an initial user without validation. Thank you to Mohamed Abdelbaset Elnoby, who is a Senior Information Security Analyst for bringing this issue to our attention. We really appreciate it!
http://goo.gl/jcpFzN

Pro: CSRF tokens are now respected login pages. Users are disabledÿfor ten minutes after five failed logins. Thank you to Mohamed Abdelbaset Elnoby, an Information Security Evangelist, for bringing this issue to our attention. We appreciate it!
http://goo.gl/ZQ1z6q

https://community.rapid7.com/docs/DOC-3010
https://community.rapid7.com/docs/DOC-3073

Info & PoC(s):
Metasploit Project Login CSRF & Bruteforcing: http://goo.gl/ogoXgl
Metasploit Project < 4.11.1 - Initial User Creation CSRF: http://goo.gl/kkyXqX
About CSRF: http://goo.gl/P3gp70
About Brute Force: http://goo.gl/q0OQAs

More Information:
https://www.facebook.com/100000152886101/posts/1123144181034001/
==========

Acknowledged by OpenKM for a Remote Cross Site Scripting to Full Users and Administrators Accounts Takeover (CVE-2014-9017)
OpenKM
March 2015
OpenKM is a Free/Libre document management system that provides a web interface for managing arbitrary files. OpenKM includes a content repository, Lucene indexing, and jBPM workflow. The OpenKM system was developed using Java technology.

The Vulnerability:

It's so simple, Create a task, Set the task name to any preferred XSS attack vector, Assign that task it to a targeted user/admin, Boom! this targeted user/admin will be automatically XSSed when the notification appears on his side that's it. So any user could execute a JavaScript code in the current session of the other users via adding a task and assign that task for the targeted user/admin.

PoC Video: http://goo.gl/6gVHTH
CVE-2014-9017 [NIST]: http://goo.gl/1O1zIe
CVE-2014-9017 [MITRE]: http://goo.gl/7KpO7O
About XSS: http://goo.gl/7ZkNRJ
==========

Installatron Acknowledgment
Installatron
March 2015
Seekurity (https://www.Seekurity.com) was acknowledged by Installatron for responsibly discovering and reporting 2 stored Cross Site Scripting affects every cPanel's default installation of Installatron.

Statement:
Installatron Plugin version 9.1.24 is now the current release version. This is a maintenance and security release that fixes a range of minor problems including a cross-site scripting (XSS) issue in the My Applications and My Backups tabs. Installatron would like to thank Seekurity for discovering and reporting this issue responsibly.

Acknowledgment:
http://installatron.com/whatsnew/installatron_plugin_9.1.24
http://installatron.com/updatefeed/installatron_plugin_9_1_24
==========

Acknowledged by Bitdefender
Bitdefender
January 2015
Got a 1-Year Bitdefender Total Security 2015 License a security issues in their Anti-Theft Security Product.

Vulnerability: Open Redirection resulting in a one-click Full Account Takeover
PoC: http://goo.gl/poJ1MZ

Read more:
About Open Redirections: http://goo.gl/1Dtijr
==========

Acknowledged by ESET
ESET
January 2015
Got a 1-Year ESET Smart Security License and a Certification for discovering 3 security issues in their Anti-Theft Smart Security Product.

Vulnerabilities and PoCs:
1- ESET Mobile Anti Theft Service Multiple CSRFs, PoC: http://goo.gl/UcT3FZ
2- ESET Account Name Change CSRF, PoC: http://goo.gl/5QsRC2
3- ESET Double Reflected XSSes, PoC: http://goo.gl/Zcc22E

Read more:
About CSRF: http://goo.gl/3cucQZ
About XSS: http://goo.gl/03zdFK
==========

Acknowledged by Opera
Opera
January 2015
At Opera Software, we run a large number of websites for our products and services, and we like to give credit to the researchers and website testers who offer their assistance to help us tighten the security of those websites. We would like to take this opportunity to thank the researchers and testers of 2015 for their assistance in discovering and reporting security issues:

•Mohamed Abdelbaset Elnoby

Vulnerability: Multiple CSRF Vulnerabilities.
HoF Link: http://blogs.opera.com/security/2015/01/thanks-researchers-2015/
About CSRF: http://goo.gl/0aSULX
==========

Acknowledged by AVG Inc.
AVG Inc.
December 2014
Got Acknowledged by AVG Inc. for reporting a security vulnerability in their "Anti-Theft" Service.

Vulnerability: Anti-Theft Service CSRF to Stored XSS leads to Full Account//Device Takeover
PoC Video: http://goo.gl/Yo2qyi
About CSRF: http://goo.gl/dskcNA
About XSS: http://goo.gl/pKlDv8
==========

Acknowledged by PasteBin.com
Pastebin.com
December 2014
Got a PRO Account as a rewarded and acknowledged by Pastebin.com for reporting a 3 vulnerabilities resulting in Full Account Takeover Scenarios.

Vulnerabilities and PoCs:
#1 CSRF, PoC: http://goo.gl/NcakYL

#2 Reflected XSS, PoC: http://goo.gl/gTfXWg - http://goo.gl/UxAxqT
#3 ClickJacking, PoC: http://goo.gl/vcL8GQ

Read more:
About CSRF: http://goo.gl/3cucQZ
About XSS: http://goo.gl/03zdFK
About ClickJacking: http://goo.gl/OiJjT9
==========
Braintree Payments Hall of Fame "Paypal Company"
Braintree Payments.
December 2014
Appreciations

We appreciate responsible disclosure so much, we're willing to put you in our security hall of fame! If you responsibly notify us of a vulnerability that we are unaware of, we will add you to the exclusive list of amazing people who have helped Braintree become better and more secure.

Please remember that running security scanning tools creates a lot of work and generates more noise than useful information. We do appreciate research and disclosure, but we kindly ask that you do not use scanners to find vulnerabilities.

•Mohamed Abdelbaset Elnoby

HoF Link: https://www.braintreepayments.com/developers/disclosure
==========
Listed in SAP Community Network
SAP Community Network
December 2014
The SAP Product Security Response Team thanks all researchers and security IT professionals that help with discovering and solving security vulnerabilities.

Vulnerability: Login Brute Force.
PoC Video: http://goo.gl/6MhmfT
HoF Link: http://scn.sap.com/docs/DOC-8218
About Brute Force: http://goo.gl/pKtGZW

==========**Panorama9**
Hall of Fame
Panorama9
December 2014
Credits

Seekurity Acknowledgements, Honors, Awards & CVEs

The Panorama9 team would like to thank the following individuals for responsibly disclosing security flaws to us:

Mohamed Abdelbaset Elnoby @SymbianSyMoh, Security Researcher at W3Pwn
Found a potential clickjacking vulnerability. Resulted in improved protection against clickjacking and CSRF attacks.

HoF link: http://panorama9.com/security

Listed in Freelancer.com Hall of Fame "Top 1"
Freelancer.com
November 2014
Thanks to the following researchers for reporting important security issues.
@SymbianSyMoh

Vulnerabilities: XSS, CSRF, Brute force, ClickJacking and many...
HoF Link: https://bugcrowd.com/freelancer/hall-of-fame
About XSS: http://goo.gl/03zdFK
About CSRF: http://goo.gl/Usx87d
About Brute Force: http://goo.gl/5WghW1
About ClickJacking: http://goo.gl/WWP5rC
==========

Listed in Netflix Hall of Fame
Netflix
November 2014
Netflix would like to thank the following researchers for participating in our responsible disclosure program:
-2014
-Mohamed Abdelbaset Elnoby (@SymbianSyMoh)

HoF : https://help.netflix.com/en/node/6657
==========

Listed in Vimeo Hall of Fame
Vimeo
November 2014
Thanks for helping us keep Vimeo safe!
-Mohamed A. Baset

Vulnerability: CSRF to disconnect all Apps liked to Vimeo Account
PoC: http://goo.gl/ehxe44
HoF Link: https://vimeo.com/about/security
About CSRF: http://goo.gl/Usx87d
==========

Sellfy Hall of Fame
Sellfy
November 2014
The following researchers have taken the time to identify and report security concerns with Sellfy. Their work is truly appreciated.

•Mohamed Abdelbaset Elnoby

HoF Link: https://sellfy.com/security/
==========

Acknowledged by Mozilla Security Team
Mozilla
October 2014
Got Acknowledged and rewarded by Mozilla security team for discovering and responsibly reporting a Clickjacking security vulnerability affects Firefox OS Find My Device Service which if maliciously exploited will trick users to do unwanted actions (eg. Change PINs, Wipe and Lock Phones!) which is the best example to demonstrate how could a web application bug affects your physical device!
.
The vulnerability also was mentioned in the Daily Open Source Infrastructure Report of USA Department of Homeland Security! (Item number 25) here's the report: https://goo.gl/XFG5Bf
.
PoC, Writeup, Acknowledgment and News:
-Hall of Fame (4th Quarter 2014)
https://www.mozilla.org/en-US/security/bug-bounty/web-hall-of-fame/
-Seekurity blog
https://www.seekurity.com/blog/general/firefox-find-my-device-service-clickjacking/
-US Homeland Security Daily Open Source Infrastructure Report
https://www.dhs.gov/sites/default/files/publications/dhs-daily-report-2015-10-22.pdf
-Softpedia
http://news.softpedia.com/news/firefox-findmydevice-service-lets-hackers-wipe-or-lock-phones-change-pins-495003.shtml
-TechWorm
http://techworm.net/2015/10/mozillas-firefox-find-my-device-lets-hackers-wipe-or-lock-phones-change-pins.html
-Expl0its.com
http://www.expl0its.com/?p=4253
==========

Airbnb Hall of Fame
Airbnb.com
October 2014
Thank you.
These individuals have helped make Airbnb.com a safer place for our community.

HoF Link: https://www.airbnb.com/info/security

CVE-2014-8346
US-CERT / NIST / MITRE / CVE Org.
October 2014
CVE-2014-8346 is about a Security Vulnerability in found in Samsung FindMyMobile Service allows any Remotely Attacker to Lock, Unlock, Ring and Wipe the Device Data.

Links:
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8346
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-8346
http://www.inteco.es/vulnDetail/CERT_en/Early_warning/Vulnerabilities_1/detail_vulnerability/CVE-2014-8346
http://nvd.nist.gov/cvss.cfm?version=2&name=CVE-2014-8346&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C)
http://cve.scap.org.cn/CVE-2014-8346.html
http://cxsecurity.com/cveshow/CVE-2014-8346/
http://www.security-database.com/detail.php?alert=CVE-2014-8346
https://vulnia.com/vulnerability?id=66482
http://cve.circl.lu/cve/CVE-2014-8346
http://en.securitylab.ru/nvd/461171.php
http://www.cvedetails.com/cve/CVE-2014-8346/
http://en.hackdig.com/?tag=CVE-2014-8346
http://digitaltrusting.com/?tag=cve-2014-8346
http://www.cvedetails.com/cve/CVE-2014-8346/
http://www.cvedetails.com/vulnerability-list/vendor_id-822/year-2014/opdos-1/Samsung.html
http://www.cvedetails.com/product/29320/Samsung-Findmymobile.html?vendor_id=822
==========

Shoudio Hall of Fame
Shoudio
October 2014
==========**SoundCloud**

Hall of Fame
SoundCloud
October 2014
On behalf of our millions of users, we would like to give a shout-out here on our Hall of Fame to all security researchers that have helped us keep SoundCloud safe by reporting a security vulnerability to us responsibly - we really appreciate it!

-Mohamed Abdelbaset Elnoby (@SymbianSyMoh)

Vulnerability: ClickJacking escalated to CSRF Attack
PoC: http://goo.gl/5QSS57

HoF Link: http://help.soundcloud.com/customer/portal/articles/439715-responsible-disclosure
==========

SplitWise Hall of Fame
SplitWise
October 2014
Special thanks to all those who have helped Splitwise:
Mohamed Abdelbaset Elnoby

Hof link: http://blog.splitwise.com/about/responsible-disclosure-special-thanks/
==========

Thanked By Samsung Electronics Co., Ltd
Samsung Electronics Co., Ltd.
October 2014
Got Thanked by Samsung for discovering a Security Vulnerability in their FindMyMobile Service allows any Remotely Attacker to Lock, Unlock, Ring and Wipe the Device Data.

Media Links:
http://thehackernews.com/2014/10/samsung-find-my-mobile-flaw-allows.html
http://www.computerworld.com/article/2839240/zero-day-in-samsung-find-my-mobile-service-allows-attacker-to-remotely-lock-phone.html
http://mashable.com/2014/10/28/hackers-samsung-find-my-mobile/
http://www.businessinsider.com/hackers-use-find-my-mobile-to-wipe-any-samsung-phone-2014-10
http://www.dailymail.co.uk/sciencetech/article-2812286/Samsung-flaw-lets-hackers-remotely-lock-devices-Bug-Mobile-service-leaves-handsets-open-attack.html
http://9to5google.com/2014/10/28/newfound-vulnerability-lets-attackers-remotely-lock-your-samsung-phone/
http://blogs.wsj.com/cio/2014/10/28/the-morning-download-a-lowes-robot-aims-to-cut-friction-from-big-box-shopping/
http://androidcommunity.com/nist-reports-vulnerability-of-samsungs-find-my-mobile-feature-20141028/
http://www.androidauthority.com/samsung-security-bug-544443/
http://www.msn.com/en-my/news/other/exploit-lets-remote-attackers-lock-your-samsung-phone/ar-BBbEdll
http://finance.yahoo.com/video/hackers-samsung-mobile-feature-attack-140904121.html
http://www.zdnet.de/88209378/luecke-samsungs-find-mobile-dienst-erlaubt-angreifern-geraetezugriff/
http://www.cnet.de/88139133/samsungs-ortungsdienst-find-mobile-luecke-erlaubt-angreifern-geraetezugriff/
http://www.engadget.com/2014/10/28/samsung-find-my-mobile-exploit/
==========

Tuenti Social Network Hall of Fame
Tuenti Corp
October 2014
Got listed in Tuenti Social Network Hall of Fame

Listed in Tuenti Social Network Hall of Fame for discovering a POST based Cross Site Scripting vulnerability.

HoF Link: http://corporate.tuenti.com/en/dev/security
==========
iFixit Hall of Fame
iFixit
October 2014
Thank you for your help with keeping the iFixit community safe. We really appreciate it.
Here are people who have responsibly disclosed vulnerabilities in the past:

2014
•Mohamed Abdelbaset Elnoby

Vulnerability: Stored XSS in Public "Guide" Page.
PoC: http://goo.gl/aPRm0s
HoF: https://www.ifixit.com/Info/Responsible_Disclosure
==========
Acknowledged by Avira Security
Avira GmbH
September 2014
Got Acknowledged by Avira Security Team for reporting a ClickJacking Vulnerability leads to full User Accounts takeover.

Vulnerability: ClickJacking to Full Accounts Takeover.
PoC: http://goo.gl/ITl9xD
About ClickJacking: http://goo.gl/WWP5rC
==========
DNSimple Hall of Fame
DNSimple.com
September 2014
The following members of the Internet community have contributed to the identification and closure of security issues in DNSimple in a responsible fashion:

Mohamed Abdelbaset Elnoby from W3Pwn.com

HoF Link: https://dnsimple.com/security
==========
Moment.me Certification
Moment.me
September 2014
Got a Certificate from Moment.me for discovering some security vulenrabilities in their website.

Certificate: http://goo.gl/sGXRiO
==========

Pocket App Hall of Fame
getPocket.com
September 2014
Thanks!

We want to extend a sincere thanks to the following researchers have generously taken the time to identify and responsibly report security incidents and keeping Pocket safe. Their work is truly appreciated.

Mohamed Abdelbaset Elnoby (@SymbianSyMoh)

HoF link: getpocket.com/security
==========
Madwhips Hall of Fame
Madwhips
August 2014
Hall of Fame - Responsible Disclosure of Security Vulnerabilities

MadWhips encourages the responsible disclosure of security vulnerabilities and would like to thank those for disclosing a security vulnerability.

To be eligible for this list, you must be the first person to responsibly disclose the issue, and you must allow us a reasonable amount of time to address the issue before publishing the information.

HoF Link: http://www.madwhips.com/credits
==========
Microsoft Hall of Fame
Microsoft
August 2014
The Microsoft Security Response Center (MSRC) is pleased to recognize the security researchers who have helped make Microsoft online services safer by finding and reporting security vulnerabilities. Each name listed represents an individual or company who has privately disclosed one or more security vulnerabilities in our online services and worked with us to remediate the issue.

Yasser Ali, Mohamed Abdelbaset - W3Pwn Security Team

HoF Link: http://technet.microsoft.com/en-us/security/cc308589.aspx
==========
OpenText Acknowledgements
OpenText
August 2014
Acknowledged by OpenText after discovering some security vulnerabilities in their website.

OpenText acknowledges those that have reported defects to OpenText, helping us provide secure, robust products for our customers.

HoF Link: http://www.opentext.com/who-we-are/copyright-information/security-acknowledgements
==========
Adobe Hall of Fame
Adobe
July 2014
Got Listed in Adobe for discovering a Critical Vulnerability in Behance Network allows me to delete any of designs / Work.

HoF List : https://helpx.adobe.com/security/acknowledgements.html

Adobe encourages the responsible disclosure of security vulnerabilities through the Product Security Incident Response Team web form. Adobe would like to thank the following individuals and organizations for responsibly disclosing a security vulnerability for an Adobe website or online service, and for working with Adobe to help protect our customers. To be eligible for this list, you must be the first person to responsibly disclose the issue, and you must allow us a reasonable amount of time to address the issue before publishing the information. Individuals and organizations who have responsibly disclosed vulnerabilities in an Adobe desktop product are referenced in the “Acknowledgments” section of each Security Bulletin.
==========
Appcelerator Hall of Fame
Appcelerator
July 2014
Thank you!
Appcelerator would like to thank the following individuals who have participated in our responsible disclosure program:

Mohamed Abdelbaset Elnoby @SymbianSyMoh

HoF Link: http://www.appcelerator.com/privacy/responsible-disclosure-of-security-vulnerabilities/
==========
Twitter Hall of Fame
Twitter
July 2014
I was listed in Twitter's hall of fame as a top Hacker reporting a valid 4 vulnerabilities

HoF Link: https://hackerone.com/twitter/thanks
==========
Yahoo! Hall of Fame
Yahoo!
July 2014

Successfully listed in Yahoo! Hall of Fame for reporting several Security Vulnerabilities.

HoF List: https://hackerone.com/yahoo/thanks

==========

AT&T Hall of Fame
AT&T
June 2014
AT&T would like to thank the following individuals for ethically reporting security issues with AT&T's internet-facing online environment through the AT&T Bug Bounty program

HoF Link: https://bugbounty.att.com/hof.php

==========

Bitcasa Hall of Fame
Bitcasa
June 2014
Special Thanks:

The following Bitcasa users have helped report security concerns. We greatly appreciate their dedication to the Bitcasa product and their valuable contribution to the user community.

HoF link:
https://support.bitcasa.com/hc/en-us/articles/202210658-How-To-Responsibly-Report-Security-Concerns

==========

Eventbrite Hall of Fame
Eventbrite
June 2014
Eventbrite wants to show our appreciation for the following people who have helped make our platform safer with their important security findings and voluntary reports. Thank you for your hard work, dedication, and eagle eyes. Our product and customer data are safer thanks to you.

-Mohamed Abdelbaset Elnoby http://www.w3pwn.com/

HoF link: https://www.eventbrite.com/walloffame/
More Details: http://goo.gl/PY8f9j

==========

Nokia Solutions and Networks Hall of Fame
Nokia Solutions and Networks
June 2014
We would like to thank the following people who have found new vulnerabilities in Nokia Solutions and Networks web pages and have made a responsible disclosure to us. The individuals who found 5 or more new vulnerabilities, are additionally granted with prime reporter status:

Mohamed Abdelbaset Elnoby - (http://www.w3pwn.com)

Hall of Fame link: http://nsn.com/responsible-disclosure
==========
Rapid7 Bug Bounty Award
Rapid7
June 2014
Got a T-Shirt as a Reward from "Rapid7" makers of #Metasploit for discovering some vulnerabilities in their website.

Some Details: http://goo.gl/L3ryTc
==========
Automattic "Wordpress" Hall of Fame
Automattic
May 2014
Listed in Automattic for discovering multiple vulnerabilities in it's open source projects like Wordpress and many

HoF Link: https://hackerone.com/automattic/thanks
==========
BufferApp Hall of Fame
Buffer Inc.
May 2014
Acknowledgements:
We appreciate the work that goes into finding and disclosing security flaws in Buffer and would like to thank the following individuals and organizations:

Mohamed A. Baset

The Whitehat list:
https://bufferapp.com/security
==========
Foursquare Hall of Fame
Foursquare
May 2014
We would like to offer our thanks to the following researchers who have helped us make Foursquare more secure:

-Mohamed Abdelbaset Elnoby

HoF link: https://foursquare.com/about/security
==========

Google Hall of Fame "Reward Recipients"
Google
May 2014
The following people have qualified for a Google Security Reward. On behalf of our hundreds of millions of users, we thank the named individuals for helping make Google products safer.

-Mohamed Abdelbaset Elnoby - http://www.W3Pwn.com/

HoF List: http://www.google.com.eg/about/appsecurity/hall-of-fame/reward/
==========
Hootsuite Hall of Fame
Hootsuite
May 2014
We respect the effort and skill that goes into finding and disclosing security flaws. We are grateful for the generosity and support of the following individuals and organizations:

-Mohamed Abdelbaset Elnoby

Hall of Fame Link: https://hootsuite.com/security
==========
Sony Hall of Thanks
Sony
May 2014
Sony would like to express our most sincere thanks to the following individuals for their contribution to the security of our networks and products:

Mohamed Abdelbaset Elnoby
W3Pwn

WoF Link: https://secure.sony.net/hallofthanks
==========
Freelancer Elite Hacker Badge
Freelancer.com
April 2014
Got my @Freelancer Elite Hacker Badge for Reporting a vulnerability in the website, Elite Badges are very difficult to obtain, obtainable by only our most dedicated users.

-The Hacker
-Earned on Apr 22nd, 2014
-Profile: http://www.freelancer.com/u/SymbianSyMoh.html
==========
Mediafire Certified Ethical Hacker Certificate

Mediafire Cloud Services
April 2014
We appreciate the report!

We would like to show our appreciation by issuing a certificate
recognizing that you identified the vulnerability, acted ethically
with the information, and allowed us to fix it. You may find it below.

Certificate: http://www.mediafire.com/view/83e3ia62buti6uu/certificate_serial_Mohamed_A_Baset.pdf
==========

T-Mobile Hall of Fame
T-Mobile
April 2014
Acknowledgements
We would like to take this opportunity to thank all the important contributors who provide us with helpful tips and hints that help us make our systems more secure. Our special thanks goes to:

-Mohammed Abdelbaset Elnoby - @SymbianSyMoh (W3Pwn.com): Information disclosure, Multiple XSS vulnerabilities.

The Whitehat list:
http://www.telekom.com/security/acknowledgements
==========

Facebook Whitehat Hall of Fame 2014
Facebook
March 2014
Officially listed as a Facebook Security Whitehat Hall of Fame for 2014

http://www.facebook.com/Whitehat/Thanks
==========

Facebook Whitehat Hall of Fame 2013
Facebook
November 2013
Officially listed as a Facebook Security Whitehat Hall of Fame for 2013

http://www.facebook.com/Whitehat/Thanks
==========

Apple Hall of Fame
Apple Inc.
Apple Web Server notifications
This article provides credit to people who have reported potential security issues in Apple's web servers.

A cross-site scripting issue was addressed. We would like to acknowledge Mohamed Abdelbaset Elnoby of W3Pwn Security Consultation for reporting this issue.

Vulnerability: Stored XSS in Apple Topsy Service.
PoC: http://goo.gl/LRgvH9
HoF Link: http://support.apple.com/kb/HT1318
==========

Listed in MailChimp Hall of Fame
MailChimp
We're so grateful to all the vigilant folks who have reported vulnerabilities. To the following people, thanks for doing your part to keep MailChimp and the entire email ecosystem safe!

Vulnerability: Open Redirection results to Facebook App Access Token Leakage
PoC Video: http://goo.gl/HDx8tH
About Open Redirection: http://goo.gl/ydbxN2
HoF Link: http://mailchimp.com/about/security-response/