2017-02-20

Company: Evolution Security GmbH
Name: Benjamin Mejri (Kunz)
Address: Ludwig-Erhard Straße 4 (Technologie Zentrum)
ZIP & Location: 34131 Kassel, Hessen – Germany (DE)

Commercial Bug Bounty Programs

Exclusive Bug Bounty Programs:

Vulnerability Laboratory has performed an empirical study to launch own "Exclusive Bug Bounty Programs" for manufacturers, vendors, corporations or even smaller companies. The last couple years the security business have seen an upsurge of interest in public or privat bug bounty programs, were manufacturers or vendors starts to reward security researchers to identify and report vulnerabilities in their own products like software, mobile applications, scripts, operating systems, protocols, services or online-service web-applications.

The intended benefit of an official "Exclusive Bug Bounty Program" is to improve the products security, disclosing zero-day vulnerabilities or unrevealing of security threats in an active cooperation with the manufacturer or vendor.

We do actually expand our business to introduce new researchers and penetration-testers to the new exclusive bug bounty programs of the manufacturers or developer teams.

Vulnerability Lab acts as intermediary between security researchers and the manufacturer or vendors by offering "Exclusive Bug Bounty Programs" in our main laboratory infrastructure.

Advantage for the Manufacturers or Vendors of Products

- Live improve of the products security by exclusive vulnerability reports or analysis
- Effective community of participation with advanced researchers & contigents
- Exchange of knowledge about vulnerabilities & cases with researchers or managers
- Preview of security situation picture and active security threats
- The manufacturers or vendors can easily process the reports via interface panel
- Saving of development or budget costs by recognizing the general security concept
- Expected costs are even for small companies valuable
- The manufacturers or vendors can take full control about the process of reportings
- The exclusive programs page can be customized by the manufacturers
- The laboratory provides a 24/7h service support for commercial programs
- Commercial programs are able to use contingents of researcher
- The manufacturers or vendors have the ability to influence the disclosure process
- During the participation statistics are available for the program owners
- Discretion in dealing with manufacturers

The vulnerability lab core research team representatives are responsible to ensure that the services are non fraudulent, active responsible to researchers, informativ in the program, not overloaded on communication and reliable for payouts to researchers. We are responsible for the active researchers or reports in the vulnerability laboratory by coordination and cooperation. We are not responsible for the input of vulnerability reports by individuals. Any active bug bounty program should follow our current process to start. One of the first steps is to introduce the program rules to the researcher community in the exclusive program webpage.

- Guidelines of the Bug Bounty Program
- Eligible Security Bugs & Vulnerabilities (In Scope)
- Security Program Exclusions (Out of Scope)
- Validation Process of Security Vulnerabilities and Bugs
- Rules of Security Program

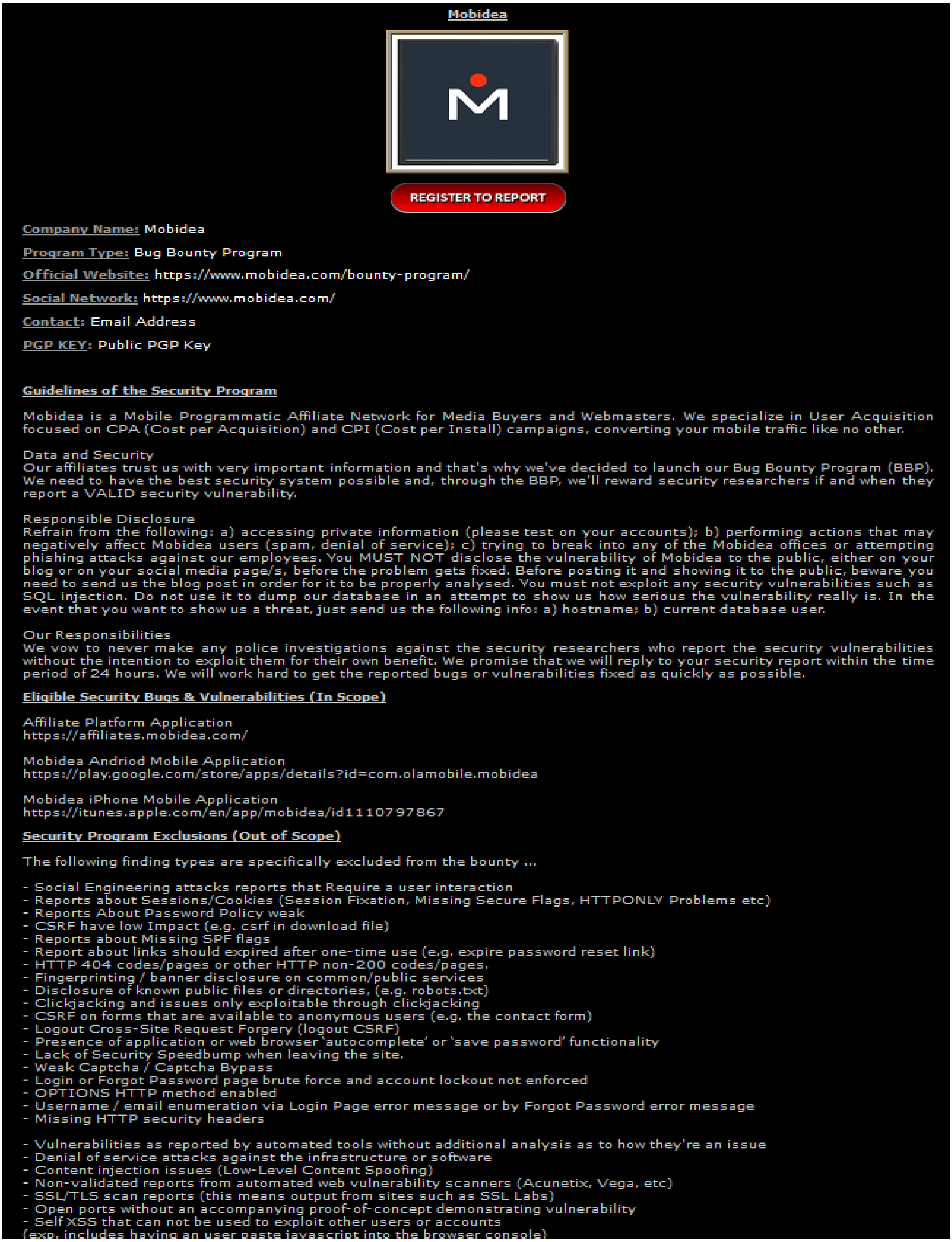
General Rules: (Security Researchers)
The reporting individuals and employees must be registered at Vulnerability Laboratory as security researcher or manager. After that the researcher is allowed to reported as individual issues to the active listed bug bounty programs. The researcher can choose which programs he wants to participate and can report any zero-day vulnerability as mentioned in the listed program rules, guidelines or condition (program page). Thus interaction is in coordination between the

manufacturers and the vulnerability laboratory core research team representatives.

- A reporting security researchers must be the first reporter of a vulnerability to get estimated credits or non-commercial rewards by following the steps in the official bug bounty program
- Forcing the community managers, administrators or manufacturers in any way, will result in an exclude of the program and vulnerability laboratory community
- Fraud, fakes, crimes and black mailings will result in a permanent community ban
- We perform no payments via westbank union transfer agency
- No debit cards with unofficial or non-confirmed identities.
- No transfer of money to third party -mullies, -companies or unconfirmed -family members.
- No payments via bitcoin wallet.
- No cashout for researchers with issues on rewards that do violate a manufacturers contratcs/rules
- In case of identification during a payment process a researcher needs to cooperate by providing valid identification documents.

Extended Rules: (Programs)
The manufacturer and owner of a bug bounty program has ever the ability to setup separate rules for each own active program. That allows a manufacturer to set specific sections, services or modules out of scope. Researchers do see the details ahead to the startup of the security program. The following list shows some categories defined out of scope by the manufacturers.

- Cross Site Request Forgery
- Self XSS
- Layer Transmission Issues
- Content spoofing or Text Injection
- Missing http security headers
- Missing cookie flags on non-sensitive cookies
- Password and recovery policies, such as reset link expiration or password complexity
- Invalid or missing SPF (Sender Policy Framework) records (Incomplete/Miss SPF/DKIM)
- Vulnerabilities only affecting users of outdated or unpatched browsers and platforms
- SSL/TLS best practices
- Clickjacking/UI Redressing
- Software version or Banner Flag disclosure
- Username / Email / Account enumeration
- Bruteforce attacks
- Denial of Service attacks



Mobidea

Company Name: Mobidea

Program Type: Bug Bounty Program

Official Website: https://www.mobidea.com/bounty-program/

Social Network: https://www.mobidea.com/

Contact: Email Address

PGP KEY: Public PGP Key

Guidelines of the Security Program

Mobidea is a Mobile Programmatic Affiliate Network for Media Buyers and Webmasters. We specialize in User Acquisition focused on CPA (Cost per Acquisition) and CPI (Cost per Install) campaigns, converting your mobile traffic like no other.

Data and Security
Our affiliates trust us with very important information and that's why we've decided to launch our Bug Bounty Program (BBP). We need to have the best security system possible and, through the BBP, we'll reward security researchers if and when they report a VALID security vulnerability.

Responsible Disclosure
Refrain from the following: a) accessing private information (please test on your accounts); b) performing actions that may negatively affect Mobidea users (spam, denial of service); c) trying to break into any of the Mobidea offices or attempting phishing attacks against our employees. You MUST NOT disclose the vulnerability of Mobidea to the public, either on your blog or on your social media page/s, before the problem gets fixed. Before posting it and showing it to the public, beware you need to send us the blog post in order for it to be properly analysed. You must not exploit any security vulnerabilities such as SQL injection. Do not use it to dump our database in an attempt to show us how serious the vulnerability really is. In the event that you want to show us a threat, just send us the following info: a) hostname; b) current database user.

Our Responsibilities
We vow to never make any police investigations against the security researchers who report the security vulnerabilities without the intention to exploit them for their own benefit. We promise that we will reply to your security report within the time period of 24 hours. We will work hard to get the reported bugs or vulnerabilities fixed as quickly as possible.

Eligible Security Bugs & Vulnerabilities (In Scope)

Affiliate Platform Application
https://affiliates.mobidea.com/

Mobidea Andriod Mobile Application
https://play.google.com/store/apps/details?id=com.olamobile.mobidea

Mobidea iPhone Mobile Application
https://itunes.apple.com/en/app/mobidea/id1110797867

Security Program Exclusions (Out of Scope)

The following finding types are specifically excluded from the bounty ...

- Social Engineering attacks reports that Require a user interaction
- Reports about Sessions/Cookies (Session Fixation, Missing Secure Flags, HTTPONLY Problems etc)
- Reports About Password Policy weak
- CSRF have low Impact (e.g. csrf in download file)
- Reports about Missing SPF flags
- Report about links should expired after one-time use (e.g. expire password reset link)
- HTTP 404 codes/pages or other HTTP non-200 codes/pages.
- Fingerprinting / banner disclosure on common/public services
- Disclosure of known public files or directories, (e.g. robots.txt)
- Clickjacking and issues only exploitable through clickjacking
- CSRF on forms that are available to anonymous users (e.g. the contact form)
- Logout Cross-Site Request Forgery (logout CSRF)
- Presence of application or web browser 'autocomplete' or 'save password' functionality
- Lack of Security Speedbump when leaving the site.
- Weak Captcha / Captcha Bypass
- Login or Forgot Password page brute force and account lockout not enforced
- OPTIONS HTTP method enabled
- Username / email enumeration via Login Page error message or by Forgot Password error message
- Missing HTTP security headers

- Vulnerabilities as reported by automated tools without additional analysis as to how they're an issue
- Denial of service attacks against the infrastructure or software
- Content injection issues (Low-Level Content Spoofing)
- Non-validated reports from automated web vulnerability scanners (Acunetix, Vega, etc)
- SSL/TLS scan reports (this means output from sites such as SSL Labs)
- Open ports without an accompanying proof-of-concept demonstrating vulnerability
- Self XSS that can not be used to exploit other users or accounts

(exp. includes having an user paste javascript into the browser console)

www.vulnerability-lab.com/bounties.php