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)

Non-Commercial Responsible Disclosure Programs

Exclusive Responsible Disclosure Programs:
The goal of responsible disclosure is to contribute to the security of systems and control the vulnerabilities in them by reporting those vulnerabilities in a responsible manner by acting on the reports appropriately, to prevent or limit potential damages to the maximum possible extent. Part of this means allowing sufficient time for action before divulging the vulnerability. Responsible disclosure starts with an organisation that is owner of information systems or the manufacturer of a product following the procedures associated with the Vulnerability Laboratory infrastructure conditions to start it. In case of the responsible disclosure program the manufacturer has the primary responsibility for the information security of the system or product.

An important part of this is that the organisation has the choice to adopt and pursue a responsible disclosure policy, to give the organisation an effective approach to resolve zero-day vulnerabilities or major security threats. The organisation makes clear how it intends to handle reports of zero-day vulnerabilities and bugs by drafting its own responsible disclosure policy.

We have obviously seen in the past, that a large number of parties (Adobe, Flowdock, Saveya, PayPal, Dell or SAP) that responsible disclosure programs are very valueable for both sides. The manufacturer and as well the security researcher. We do actually expand our business to introduce new researchers and penetration-testers to the new exclusive responsible disclosure programs of the manufacturers or developer teams.

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

2017-02-20

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
- Non-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 responsible disclosure program must follow our current process to start. One of the first steps is to introduce the program rules to the researcher community of the vulnerability laboratory 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

After publishing a responsible disclosure program in vulnerability labs, the researchers are able to preview the disclosure policy with guidelines and basic conditions. Hosting an own responsible disclosure program in vulnerability laboratory costs 500€ per year, depending on the estimated budget of the manufacturer or company. In case of emergency or on active attacks or vulnerabilities we do allow small companies and firms to join the responsible disclosure program with lower variable costs.

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 responsible disclosure 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. Vendors have the ability to control and review the reports on a prepared web panel.

- 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 responsible disclosure program webpage
- 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 bann
- 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 contratcs/rules
- In case of identification during a payment process a researcher needs to cooperate by providing valid identification documents

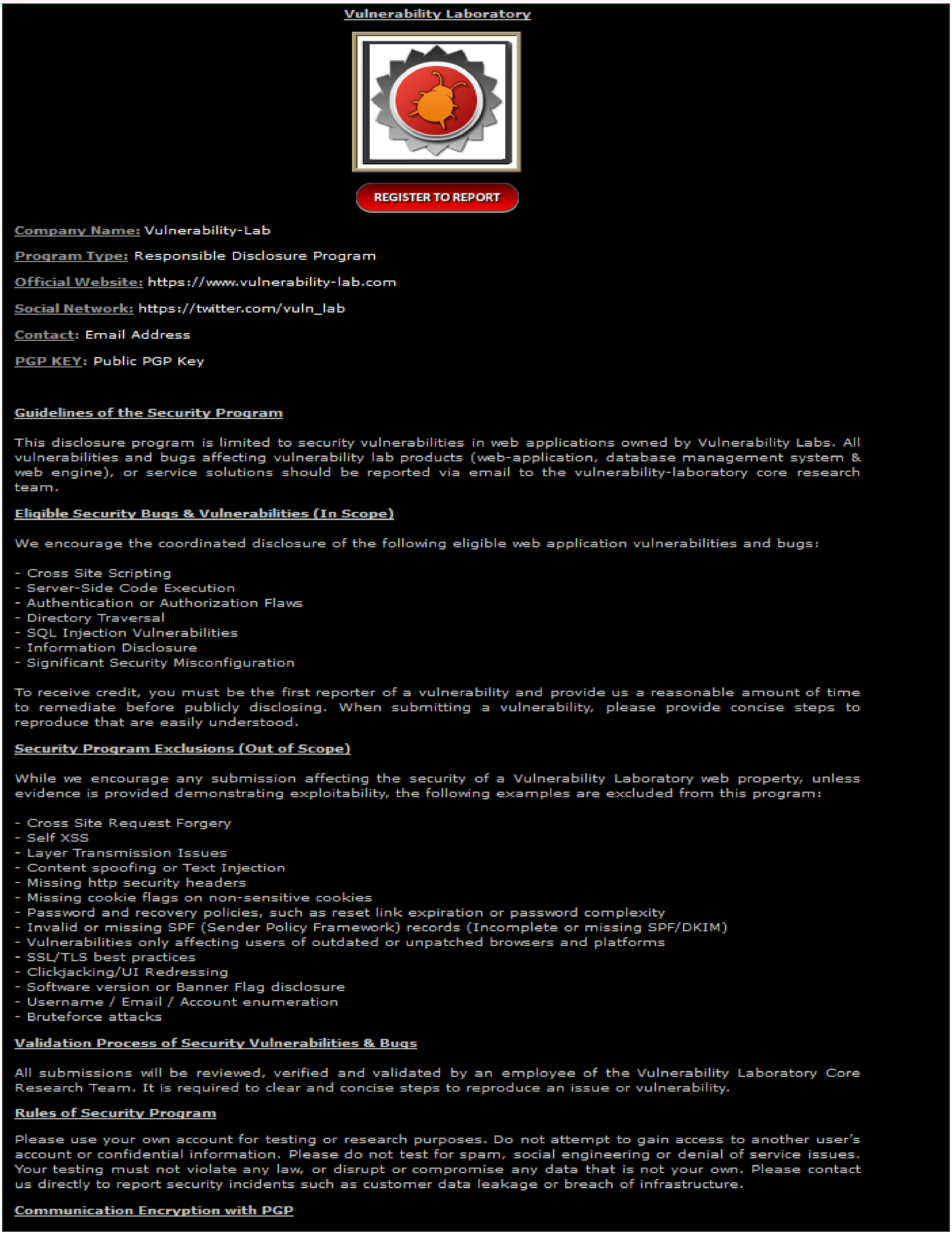
Extended Rules: (Programs)

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

2017-02-20



Vulnerability Laboratory

Company Name: Vulnerability-Lab

Program Type: Responsible Disclosure Program

Official Website: https://www.vulnerability-lab.com

Social Network: https://twitter.com/vuln_lab

Contact: Email Address

PGP KEY: Public PGP Key

Guidelines of the Security Program

This disclosure program is limited to security vulnerabilities in web applications owned by Vulnerability Labs. All vulnerabilities and bugs affecting vulnerability lab products (web-application, database management system & web engine), or service solutions should be reported via email to the vulnerability-laboratory core research team.

Eligible Security Bugs & Vulnerabilities (In Scope)

We encourage the coordinated disclosure of the following eligible web application vulnerabilities and bugs:

- Cross Site Scripting
- Server-Side Code Execution
- Authentication or Authorization Flaws
- Directory Traversal
- SQL Injection Vulnerabilities
- Information Disclosure
- Significant Security Misconfiguration

To receive credit, you must be the first reporter of a vulnerability and provide us a reasonable amount of time to remediate before publicly disclosing. When submitting a vulnerability, please provide concise steps to reproduce that are easily understood.

Security Program Exclusions (Out of Scope)

While we encourage any submission affecting the security of a Vulnerability Laboratory web property, unless evidence is provided demonstrating exploitability, the following examples are excluded from this program:

- 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 or missing 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

Validation Process of Security Vulnerabilities & Bugs

All submissions will be reviewed, verified and validated by an employee of the Vulnerability Laboratory Core Research Team. It is required to clear and concise steps to reproduce an issue or vulnerability.

Rules of Security Program

Please use your own account for testing or research purposes. Do not attempt to gain access to another user's account or confidential information. Please do not test for spam, social engineering or denial of service issues. Your testing must not violate any law, or disrupt or compromise any data that is not your own. Please contact us directly to report security incidents such as customer data leakage or breach of infrastructure.

Communication Encryption with PGP

www.vulnerability-lab.com/bounties.php