V1 BUG BOUNTY PLATFORM

<u>Who we are</u>: Evolution Security GmbH

- Vulnerability Lab 2005 - 1st official EU Bug Bounty Platform

<u>What is the V1 Platform?</u>

- Development Framework := Ember

- Bug Bounty & Responsible Disclosure Business

- Online & Offline (LAN)

Technology Partner:

HITBSecConf
Keeping Knowledge Free for Over a Decade

Exchange Cooperation Partner:

补 天
漏洞响应平台

At the top we had enough ...

Why did we build the V1? (Needs & Problems ...)

- European Union requesting others to interact

- Incomplete rule sets & program conditions

- Charge of high $$$ amounts from researchers

- Non serious firms & fraud or money laundering

- Incorrect or faked public statistics

- Personal deals for personal enrichment

- Insecure mechanisms, 3rd party depency & broken models

- Miscommunication & lack of responsibility

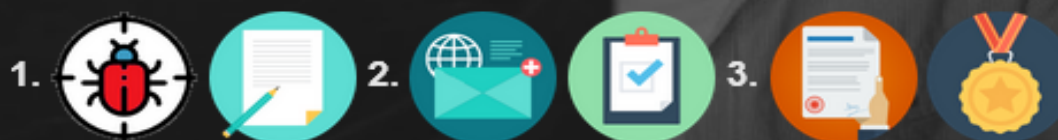- ... about scores & recognizing the real root needs!

V1 BUG BOUNTY PLATFORM

The V1 platform coordinates vulnerability research and assists to start own bug bounty programs. Vulnerability Lab owns the first independent unique bug bounty platform since 2005 as infrastructure for security researchers, companies & developers. The time has come to manage your bug bounties and acknowledgements for the enterprise to become part of a new european union prevention-system.

WWW.V1BOUNTY.COM   WWW.V1BOUNTY.DE

Heroku API DD Bug Bounty #3 - Persistent Vulnerability	2.5	Remote	14132	Barracuda Message Archiver 650 - Persistent Vulnerability	3.6	Remote	26765
Heroku API Bug Bounty - Persistent Invitation Vulnerability	4.1	Remote	21228	Paypal Inc BB #108 MOS - Bypass & Persistent Vulnerabilities	4.1	Remote	22445
Facebook Bug Bounty #17 - Migrate Privacy Vulnerability	4.9	Remote	17125	Paypal Bug Bounty #108 MOS - Persistent Web Vulnerability	4.1	Remote	21893
Facebook BB #18 - IDOR Issue & Privacy Vulnerability	4.7	Remote	21395	Yahoo! Bug Bounty #30 YM - Persistent Mail Vulnerability	5.3	Remote	22631
Facebook Bug Bounty #16 (Studio) - Persistent Vulnerability	3.5	Remote	16536	Yahoo! BB #29 YM - Bypass & Persistent Vulnerability	6.3	Remote	22037
RelateIQ Bug Bounty #1 - Persistent Signup Vulnerability	3.4	Remote	18002	Yahoo! Bug Bounty #25 Flickr API - Persistent Vulnerability	4.1	Remote	21842
Ebay Magento Bug Bounty #1 - Persistent API Vulnerability	3.3	Remote	27481	Paypal Bug Bounty #36 - SecurityKey Card Vulnerability	4.3	Remote	24347
PayPal Inc BB #88 - Bypass & Arbitrary Code Execution	9.1	Remote	28747	PayPal Inc BB #74 - Persistent Core Backend Vulnerability	8.9	Remote	41211
PayPal Inc BB #107 MOS - Persistent History Vulnerability	4	Remote	27498	Paypal Inc BB #109 MOS - Bypass & Persistent Vulnerability	4	Remote	22101
Dell SonicWall GMS v7.2.x - Persistent Web Vulnerability	3	Local	24700	Microsoft Office 365 Outlook - Persistent POST Vulnerability	3.3	Remote	22759
Paypal MOS API - Bypass & Persistent XML Vulnerability	4.1	Remote	21800	Dell SonicWall EMail Security 7.4.5 - Multiple Vulnerabilities	3.5	Remote	19140
PayPal Inc BB #98 MOS - Persistent Settings Vulnerability	4.1	Remote	27607	Microsoft Office 365 Outlook - Bypass & Editor Vulnerabilities	4.3	Remote	23354
PayPal Inc BB #85 MB iOS 4.6 - Auth Bypass Vulnerability	6.2	Remote	34871	Telekom Bug Bounty #12 - File Include Web Vulnerability	7.1	Local	19773
PayPal Inc BB #96 - Persistent Tags Vulnerability	3.1	Remote	27002	Barracuda Networks Backup - Persistent Web Vulnerability	3.5	Remote	22444

CONCEPTS & SERVICES OF THE V1 BUG BOUNTY PLATFORM

Bug Bounty Program - Hosting of bug bounty programs for companies & enterprise to identify unknown and early threats
Responsible Disclosure Program - Hosting of responsible disclosure programs for companies as independent cooperative
Security Contact Page - Independent security contact page program for companies to receive incidents and security related
Services - Magazine, information security forums, international bug bounty list, researcher privatebin, news monitor and

Technology Partner:

HITBSecConf
Keeping Knowledge Free for Over a Decade

Exchange Cooperation Partner:

补 天
漏洞响应平台

FOR BUSINESS

Platform Services
Platform Business
Disclosure Programs
Bug Bounty Programs
Security Contact Pages

SUPPORT V1

Introduction Summary
Exclusive Programs
Exclusive Pages
Hacktivity Statistics
Community Forums

COMMUNITY

Services Program
Security Mechanism
Platform Guidelines
RSS News Feed
Service Newsletter

COMPANY

About Teamwork
Trusted Researchers
Company Services
Company Basics
Company Statement

CONTACT

Assistance FAQ
Contact Research
Contact Sales
Report Issue
XMPP Channel

V1 PLATFORM

Start a BB Program
Start a RD Program
Start a SP Program
For Researchers
For Business

® **V1 BUG BOUNTY PLATFORM** ™

Language ▾

V1 Models & Security Programs
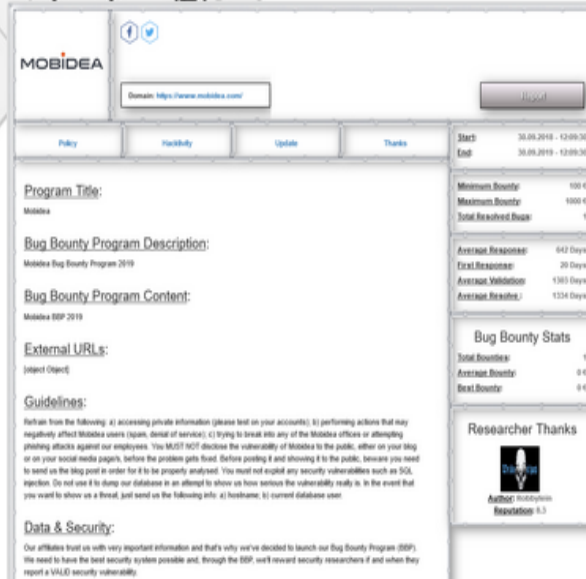
<u>Programs:</u> Information Security

- Bug Bounty (Commercial - Reward)

- Responsible Disclosure (Acknowledgements)

- Company Security Contact Page (Incidents)

- Data Security Programs (Policy, SRL, ToMs ...)

<u>Models</u>: Bug Bounty & Responsible Disclosure

- Hosting (All on your own)

- Hosting & Support (We help you to coordinate)

- Hosting, Support & Leadership (We made it)

INNOVATIVE SICHERHEITSKONZEPTE DER V1 BUG BOUNTY PLATTFORM

Hier finden Sie alle verfügbaren Konzepte und Programmlisten der V1 Bug Bounty Plattform für Unternehmen. Die Serviceverzeichnisse und Dokumente sind verfügbar für Forscher und Kooperationsunternehmen. Unser Team lässt sich von aktuellen Richtlinien leiten und unterstützt Dienstleistungen der Europäischen Kommission zum Thema Bug Bounty. Unsere Plattform folgt deutschen Gesetzen und EU Normen. Zögern Sie nicht, sich mitzuteilen und lesen Sie unsere transparenten Geschäftsinhalte.
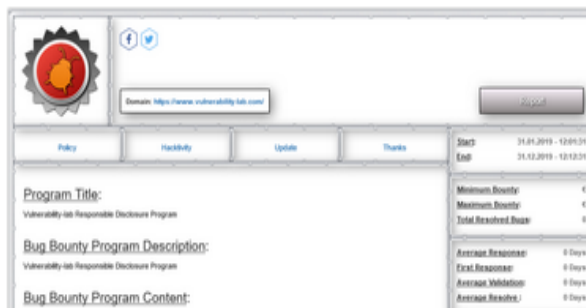

The intended benefit of an official exclusive bug bounty program is to improve the products security, disclosing zero-day vulnerabilities or unrevealing of security threats in an active cooperation with the manufacturer or vendor.

We do actually expand our business to introduce new researchers and penetration-testers to the new exclusive bug bounty and reward 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 v1 platform infrastructure.

Advantage for the Manufacturers or Vendors of Products or Services:

- 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

BUG BOUNTY & BELOHNUNGSPROGRAMME

Die V1 Plattform besitzt exklusive Bug Bounty- und Belohnungsprogramme für vertrauenswürdige Sicherheitsforscher, Entwickler und Hacker. Jedes Programm hat eigene Bedingungen und Regeln für teilnehmende Forscher und Hacker. Die v1 Bug Bounty Plattform-Infrastruktur unterstützt öffentliche und private Bug Bounty Programme für vertrauenswürdige Forscher. Genießen Sie die neusten und exklusiven Bug Bounty & Reward Programme.

Bug Bounty & Reward Programme einsehen

BUG BOUNTY & REWARD KONZEPTION

Die Bug Bounty Plattform unseres Unternehmens verfügt über eine transparente Bug Bounty Programm-Konzeption, die der Sicherheitsgemeinschaft als pdf-Datei zur Verfügung steht. Das Unternehmen hilft Forschern und Herstellern oder Unternehmen zu verstehen, wie das Bug Bounty Geschäft funktioniert. Das PDF beinhaltet allgemeine Informationen, aber auch auf erweiterte Details zu Bedingungen, Koordination, Einrichtung, Anforderungen und Regeln.

Bug Bounty & Reward Programm Konzeption

We are responsible for the active researchers or reports in the V1 Bug Bounty Platform 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 V1 Bug Bounty Platform 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

Our V1 Sub Online Services

Services: Companies & Researchers

- Vulnerability Magazine

- Information Security Research Forums

- PrivateBin Paste Online Service

- Independent Vulnerability Laboratory

- International Bug Bounty Listing Service

- Trusted 3D Print Security Archive

PayPal Inc Updates the Bug Bounty Program with Venmo Payments Services

Tuesday, February 27, 2018 - Posted by Editorial_Staff_Team - Bug Bounty - 0 comments
Reader's rate: ★★★★★

PayPal Inc - Venmo Bug Bounty Program Today in the morning paypal inc announced its newst updates of the bug bounty program. The new service is called "Venmo" and became to today official part of the bug bounty program. For the program the official terms and process for submitting... + continue reading

Featured Cooperative Security Articles

Lab Researcher discovered Microsoft Skype Denial of Service Vulnerability
Thursday, 29/03/16 - 2 comments

Microsoft Skype Mobile v8.x - Remote Denial of Service Vulnerability Vulnerability Labs core team discovered a new denial of service vulnerability and rendering problem in Skype Mobile Client v8.12 and v8.13 this week. The vulnerability can be triggered by sending a special smiley (emoticon) content message remotely. The security problem can... + continue reading

PayPal Inc increases Bug Bounty Payments in 2018 up to 30.000$
Tuesday, 13/03/18 - 1 comment

Bug Bounty Program increases payments for researchers in 2018 Today in the morning the paypal inc bug bounty program updated again within one month the official bug bounty

This Week Most Popular
Stack Buffer Overflow Zero Day Vulnerability uncovered in Microsoft Skype v7.2, v7.35 & v7.36
29/05/17 - 1 comment

Apple iOS v10.2 & v10.3 - SMS Reply Access Permission Vulnerability
14/05/17 - 2 comments

Today's Most Popular
Microsoft Bulletin MS2013-067 -- SharePoint 2013 Online
Videos - 0 comments

Apple iOS 10.2 Notify Function vulnerable to Attacks via Device on iTunes & Appstore
Bug Bounty - 2 comments

BMW Core Web Portal & ConnectedDrive - Exploitation of Car Configurations
Vulnerabilities & Bugs - 3 comments

Hacking the Bugcrowd - Core Researcher scores in Main Program Site
Bug Bounty - 0 comments

All Time Most Popular
Whitehat Hacker discovered details of an application-side Facebook Studio Dashboard Vulnerability
Bug Bounty - 3 comments

Edward Snowden free speech at JBIFone - Data Security & Privacy
24/11/17 - 0 comments

PayPal Inc fixed Filter Bypass & Profile Code Execution during Infrastructure Upgrades

PayPal Inc announces 2 new Bug Bounty Program Domains

EXKLUSIVES SCHWACHSTELLENMAGAZIN

Häufigstes Nachrichtenmagazin für Bug Bounty und Sicherheitsforschung in Europa. Die Inhalte werden von Forschern oder Gastautoren moderiert & geliefert. Das Schwachstellenmagazin berichtet von neuen Programmen, Präventionsmethoden, IT-Vorfällen, Sicherheitslücken und Zero-Day-Schwachstellen in Webanwendungen, Softwareprodukten, klassifizierten Hardwarekomponenten oder Dienstleistungen.

Neuigkeiten zum Thema Bug Bounty & Schwachstellen

Forum

Information Security Research Forums
Welcome to the Information Security Research Forums.

Management Forums		Threads / Posts		Last Post
Announcements & Services Public Security Forum Announcements & Available Community Services	✔	3	3	Information Security Research... by Administrator 01-04-2018
Information & Updates Forum Community Board Information & Forum Updates	✔	8	8	Authentication Type, User... by Vulnerability Lab 02-17-2018
Feedback, Critique & Bugs Leave your Feedback, Comments with Solution, Critique or Report a Forum Bug	✔	3	3	Never

Community Security Forums		Threads / Posts		Last Post
Welcome - Security Community Introduce yourself to the researcher community. Name, projects, references, services, webpage & social nets	✔	1	1	First Incoming Researcher... by Benjamin Kunz Mejri 01-21-2018
Information Security News International information security news by the public press & news agencies	✔	822	822	How to Change Your Twitter... by Vulnerability Lab 1 Day Ago
IT Security General Discussions Open or join a discussion group with general and advanced security topics	✔	3	3	by Benjamin Kunz Mejri 01-21-2018
Security Products & Services Share new or common security products. Introduce public or non-public security services	✔	822	822	by Vulnerability Lab 1 Day Ago
Privacy & Anonymity (Cipher) Methods, technics, products & events to keep the privacy and make anonymity.	✔	1	1	by Administrator 01-04-2018

INFORMATIONSSICHERHEITSFORUM

Willkommen in unseren Forschungsforen zur öffentlichen Informationssicherheit der Vulnerabilitätslaborinfrastruktur. Die Sicherheitsforen werden vom Kernteam des Labors moderiert. Die Richtlinie ermöglicht vertrauenswürdigen und verifizierten Sicherheitsforschern den Zugriff auf die verschiedenen Foren zum Thema Informationssicherheit. Sie können sich gerne registrieren oder das Forschungsteam um eine Zugangsberechtigung bitten.

Besuchen Sie die unsere Foren, um sich auszutauschen

Security Programs Statistics

Last Update	Public Programs	Exclusive Programs	Silent Programs	Reward Programs
2019-01-18	527	5	3	177

Last 15 - New Public and Silent Security Programs

Company, Vendor or Manufacturer	Bug Bounty & Rewards	Benefits Gifts or Swag	Security Acknowledgments & Hall Of Fame	Public- or Silent Security Program
Silver Gold Bull	[×]			Public Program
BMW Group			[×]	Public Program
ZOHO	[×]		[×]	Public Program
Apache			[×]	Public Program
Mozilla ASian Nightly	[×]		[×]	Public Program
TechGig	[×]	[×]		Public Program
Enciphers			[×]	Public Program
Microsoft Identify	[×]		[×]	Public Program
ARM mbed	[×]		[×]	Public Program
Emptrust		[×]		Public Program
Tumblr	[×]		[×]	Public Program

List of Bug Bounty Programs – Public & Silent Security Programs

Company, Vendor or Manufacturer	Bug Bounty & Rewards	Benefits Gifts or Swag	Security Acknowledgments & Hall Of Fame	Public- or Silent Security Program
123 Contact Form			[×]	Public Program
99Designs		[×]	[×]	Public Program
Abacus			[×]	Public Program
Acquia			[×]	Public Program
Active Campaign			[×]	Public Program
ActiveProspect			[×]	Public Program
ActiVPN			[×]	Public Program
Adapcare		[×]		Public Program
Adobe			[×]	Public Program
Airbnb		[×]	[×]	Public Program
Aircloak	[×]		[×]	Public Program
Alcyon		[×]		Public Program

SECURE PRIVATEBIN PASTE SERVICE
https://paste.vulnerability-db.com

New | Expires: 1 day | ☑ Burn after reading | Password (recommended) | Format: Source Code

ⓘ Vulnerability Laboratory Secure PrivateBin Paste|vulnerability-db.com

Editor | Preview

PrivateBin for security researchers, penetrationtesters and bug bounty hunters. The data & information is encrypted/decrypted in the browser by usage of 256 bit AES.

Regulations, Restrictions & Needs

Law & Regulations: Follow the Signs

- DSGV EU - Basic Data Protection Regulation

Policies: What others say

- BSI – Guidelines 2019 Q1

- NIST – Consideration 24/7h

- SANS Institute – Top Vulnerabilities

Norms & Standards: Keep it up

- Physical Data Encryption - Symmetrisch

- Data Transmit Encryption

European Legal Ordiance - DSGV EU

Einführung

Wir freuen uns sehr, dass Sie Interesse an unserem Unternehmen gezeigt haben. Der Datenschutz hat für das Management der Evolution Security GmbH eine besonders hohe Priorität. Die Nutzung der Internetseiten der Evolution Security GmbH ist ohne Angabe personenbezogener Daten möglich; wenn eine betroffene Person jedoch über unsere Website spezielle Unternehmensdienste nutzen möchte, kann eine Verarbeitung personenbezogener Daten erforderlich werden. Ist die Verarbeitung personenbezogener Daten erforderlich und gibt es keine gesetzliche Grundlage für eine solche Verarbeitung, holen wir in der Regel die Zustimmung der betroffenen Person ein.

Als Verantwortlicher hat die Evolution Security GmbH zahlreiche technische und organisatorische Maßnahmen ergriffen, um den bestmöglichen Schutz der über diese Website verarbeiteten personenbezogenen Daten zu gewährleisten. Allerdings können internetbasierte Datenübertragungen grundsätzlich Sicherheitslücken aufweisen, so dass ein absoluter Schutz nicht gewährleistet ist. Aus diesem Grund steht es jedem Betroffenen frei, uns personenbezogene Daten auf anderem Wege, z.B. per Telefon, zu übermitteln.

1. Definitionen

Die Datenschutzerklärung der Evolution Security GmbH basiert auf den Begriffen, die der europäische Gesetzgeber für die Annahme der Allgemeinen Datenschutzverordnung (GDPR) verwendet. Unsere Datenschutzerklärung sollte für die Öffentlichkeit sowie für unsere Kunden und Geschäftspartner lesbar und verständlich sein. Um dies zu gewährleisten, möchten wir zunächst die verwendete Terminologie erläutern.

In dieser Datenschutzerklärung verwenden wir unter anderem folgende Begriffe:

a) Personenbezogene Daten

Persönliche Daten sind alle Informationen über eine identifizierte oder identifizierbare natürliche Person ("data subject"). Eine identifizierbare natürliche Person ist eine Person, die direkt oder indirekt identifiziert werden kann, insbesondere durch Bezugnahme auf einen Identifikator wie einen Namen, eine Identifikationsnummer, Ortsdaten, einen Online-Identifikator oder auf einen oder mehrere Faktoren, die spezifisch für die physische, physiologische, genetische, mentale, wirtschaftliche, kulturelle oder soziale Identität dieser natürlichen Person sind.

b) Betroffene

Der Betroffene ist jede identifizierte oder identifizierbare natürliche Person, deren personenbezogene Daten von dem für die Verarbeitung Verantwortlichen verarbeitet werden.

Secure Location & High Encryption

Models: Data Encryption

- AES 256 bit – Database (SQL:AES_*)
- SSL / TLS 1.2 - Transmit data securly
- RSA 2048 bit - External data storage

Secure Location: Made in Germany

- Strato – Frankfurt RZ #1 – Dedicated systems
- No insecure copies, test-systems or cloud!

Functions & Modules – Coordinate, Manage, Score

Functions & Modules: Companies & Researchers

- FIRST CVSS v3 Calculator – Full integration

- SANS Top 150 & NIST(MIT) Top 50 - Bugs

- Event Notification System - 24/7h

- Update History of Programs

- Ranking System & Votings

- Explicite Permission Management

- Trusted payment process to verify

- Acknowledgement & Reward Pages (Badges)

V1 Bug Bounty Platform

Domain: https://www.v1bounty.com

Policy	Hacktivity	Updates	Hall of Fame

Start: 22.04.2019 - 23:00:00
End: 22.04.2020 - 23:00:00

Program Title:

V1 Bug Bounty Platform - Bug Bounty Program

Program Website:

https://www.v1bounty.com

Program Description:

The V1 platform coordinates vulnerability research and assists to start own bug bounty programs. Vulnerability Lab owns the first independent unique bug bounty platform since 2005 as infrastructure for security researchers, companies & developers. The time has come to manage your bug bounties and acknowledgements for the enterprise to become part of a new european union prevention-system.

Program Short Description:

Web Framework - Closed Source Ember JS

Additional Information of the Program:

ads dsywevwey

Minimum Bounty: 50 €
Maximum Bounty: 250 €
Total Resolved Bugs: 0

Average Response: - min.
First Response: - min.
Average Validation: - min.
Average Resolve: - min.

Statistics

Total Bounties: 0
Average Bounty: 0 €
Best Bounty: 0 €

Disable Program

Set Program Private

Policy	Updates	Hall of Fame

Start: 22.04.2019 - 23:00:00
End: 22.04.2021 - 00:00:00

Hall of Fame

Disable Page

Set Page Private

Security Page:

Evolution Security - Company Security Contact Page

Security Page Description:

Our company protects famous software, services, applications on multiple platforms & informs the vendor in a secure way. We provide advanced penetration tests and vulnerability assessment to our customers and clients. Targeted exploitation, benefits programs, security rewards, bug bounty programs and silent or responsible disclosure is our business. Evolution Security GmbH offers its services successfully to international companies.

Security Relevance:

At this point we would like to announce what security-relevant IT incidents we are interested in.

- Malicious code infection of our company's IT systems
- Compromised IT systems of our company
- Mistakenly publicly accessible documents of our company
- Information about attacks against our company (Advanced Persistent Threat)

Note: Company security contact pages do not deal with bug bounties or responsible disclosure incidents.

Report Incident:

Incidents can be reported to us directly by email. Our company's security officers and the respective contact persons will then initiate the evaluation of the security incident.

URL: https://www.evolution-sec.com/en/contact

Attachments:

Evolution-Security-Services-English.pdf

Characteristics of the unique proposition

<u>V1 Bug Bounty Platform</u>:

- DSGV (DE|EU) conform

- Transparent (Statistics, Policy, Rules & Studies)

- "Company Security Contact Pages" Programs

- Better financial conditions for researchers and companies

- No proprietary software

- Online (Remote) & Offline Mode (LAN)

- Data Security Protection Programs

- Connection to Vulnerability Laboratory for disclosure

Payments Process (Researchers & Companies)

For Researchers:

- 1st Vulnerability Submission of Researcher – 100€ valid Bug Bounty Vulnerability

- ... all further reports result in 100% cashout (€) for 1 year

- Higher cashouts per program by business model

- Stable and secure payment process

For Companies:

- Stable budget for programs

- Connection for disclosure in the Vulnerability Laboratory

- Full control in program about payments

Thanks for listening to us ...

Public Questions?

Feel free to ask after the talk off-site

the conference as company or researcher

… help us to persist the right way!

- Domain: www.v1bounty.com & www.v1bounty.de