CyberArmy

Bug Bounty and Vulnerability Coordination Center

#1 CROWDSOURCED CYBER SECURITY PLATFORM IN INDONESIA

About Us

We started in 2018, CyberArmyID is a company in the field of Information and Cyber Security. Currently, We are focusing on **Security Testing** with **the Crowdsourced Methodology.** We also provides **Technical and Managerial Education** related to Information and Cyber Security.

CyberArmyID under the Legal Entity of
PT Global Inovasi Siber Indonesia

2019 ASEAN-KOREA
START-UP WEEK

Innovative START-UP | TOP 40

Indonesia
Cyber Army Indonesia

November 18-28, 2019
Republic of Korea

TOP 40 Innovative Startup at
ASEAN-KOREA STARTUP WEEK
2019, Seoul South Korea

Cyber Security Solution

CyberArmy
Bug Bounty and Vulnerability Coordination Center

Bug Bounty Program

Ensuring the vulnerabilities are discovered by Bughunters and appreciate the results

Vulnerability Management Program

Security cycle mechanism whose activities are identify vulnerabilities, classification, prioritize, recover and reducing the risk

Vulnerability Bug Fixing

Helping developers to make improvement in application vulnerabilities

Penetration Testing

Ensuring the vulnerabilities are discovered by CyberArmyID Team

Cyber Security Consultant

Helping organizations with Cyber Security Needs

Cyber Academy

Education to develop individual knowledge in the field of Cyber and Information Security

We're trusted by these companies and more

CyberArmy
Bug Bounty and Vulnerability Coordination Center

From Government, State-owned Enterprises, Bank, E-Commerce, Fintech, Health Care, Edu Tech, Portal Media, Artificial Intelligence, Hosting, University, Tech Startup and more.

Bug Bounty Program / Penetration Testing

Badan Siber dan Sandi Negara Republik Indonesia
Caraka Bhuwana
BPJS Kesehatan – Badan Penyelenggara Jaminan Sosial
Jabar Digital Service
my IndiHome
Pegadaian
Kredivo – Buy now, Pay later
Kitabisa.com
BHINNEKA
tiketux
fasapay
bobobox
dewaweb – Cloud Hosting Partner
CAZH
Assist.id
sharing happiness.org
Qwords.com
INDONESIALEAKS
Global Data Inspirasi
Pay OK
Scola
KUPSKOTES – Melayani Dengan Inovasi

And more ...

Cyber Security Consultant

Badan Siber dan Sandi Negara Republik Indonesia

Security Advisory
(Secure SDLC)

BANK BPD BALI – Bersama Anda Membangun Bali

Secure SDLC
Standard

Cyber Academy / In-house Training

Badan Siber dan Sandi Negara Republik Indonesia
Telkom Indonesia – the world in your hand
pindad
Pegadaian
GS BATTERY
KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
PT PII | PENJAMINAN & INFRASTRUKTUR
swamedia – innovative IT solution

CyberArmy
Bug Bounty and Vulnerability Coordination Center

ORGANIZATION PROBLEMS GETTING CYBER ATTACK

Vulnerability assessment is not effective, because Scanning findings can be false positive without being re-validated

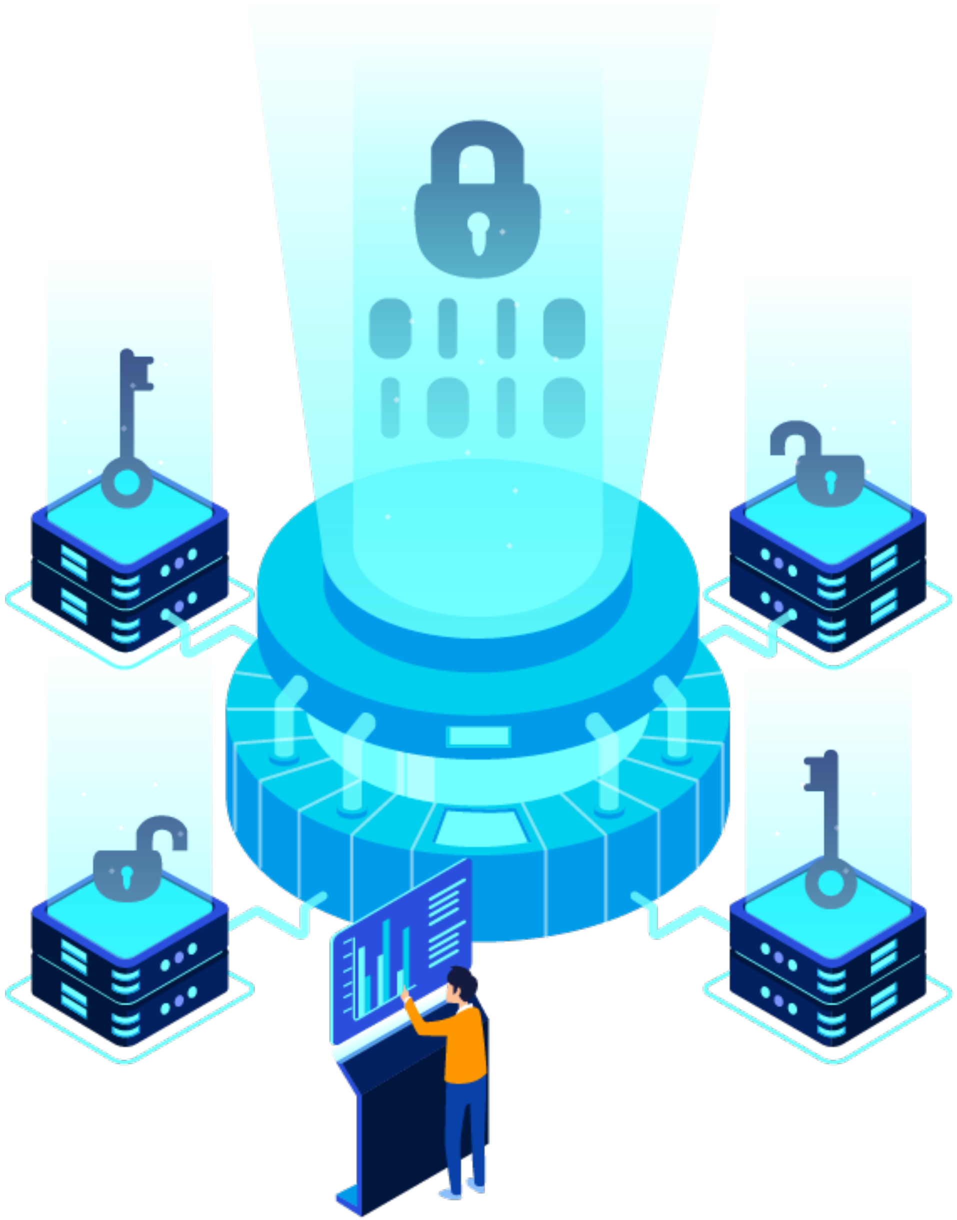
External Penetration Testing is only performed once a year, then in 11 months are still many cyber threats

Internal Penetration testing activities are currently not effective in reducing risk because the company only employs a small number of people with limited capabilities and a short period of time

Third-party application developers are not concerned with security aspects, the most important thing is that applications can be accessed according to business flows

Lack of a patching system and patch verification system led to exploitation of a known vulnerability

CyberArmy
Bug Bounty and Vulnerability Coordination Center



Bug Bounty Program

BENEFIT AND INVESTMENT

FINANCIAL

Bug Bounty Program is 60% cheaper than penetration testing services for a large number of target applications

HUMAN RESOURCE

Organizations can save on the cost of human resources because don’t need to employ many security team

TECHNICAL

The organization's internal engineering team is **quicker to fix vulnerabilities** and **critical findings are found quickly**

PROTECT CUSTOMER DATA

Protect customer data from threats of **Data Breaches, Data Manipulation, Transaction Manipulation and Denial of Service**

The Difference

CyberArmy
Bug Bounty and Vulnerability Coordination Center

	Vulnerability Assessment	Penetration Testing	Crowdsourced Security Testing
Perfomed by	Automated tools (with human oversight)	Manual Testing (1 – 5 Pentester with Professional)	**Manual Testing (10 – 400 Pentester with Professional & Community)**
Objective	Identifying Vulnerabilities	To test your security measures and probe specific weak points a hacker could exploit	To test your security measures and probe specific weak points a hacker could exploit
Method & Tools	Limited Method & Tools	Limited Method & Tools	**Rich Method & Tools**
Report Result	Rich Pontential Vulnerability Results	Limited Exploit Results	**Rich Exploit Results**
Time Report	A few minutes (Daily Pontential Vulnerability Report)	2 – 4 Weeks (No Daily Exploit Report)	**A few Hours (Daily Raw Exploit Report on Dashboard CyberArmy)**
Contents of the report	List of Potential Vulnerabilities	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation, recommendation	Prioritized list of vulnerabilities, methodologies to exploit them, narrative walkthrough of attack scenario, remediation, recommendation
Dashboard Analytics	Yes (Analytics Report & Severity Risk)	No	**Yes (Analytics Report & Severity Risk)**
Notification	Yes (Mail Notification)	No	Yes (Mail Notification)
Program Type	Private	Private	**Private or Public**

Bughunter's Profile

From Proffesional and Community

CyberArmy
Bug Bounty and Vulnerability Coordination Center

2000+ Registered BugHunters

500+ Verified BugHunters

< 4 Hours

The fastest Critical Vulnerability Finding received

< 1 Hour

The fastest High Vulnerability Finding received

Acknowledged by

Google ASUS SAMSUNG

Symantec Apple Adobe

npm PayPal Dropbox R

RAZER Ford Lenovo flickr

RSA McAfee by Intel

MOTOROLA MOBILITY

And Many More...

CyberArmy
Bug Bounty and Vulnerability Coordination Center

What They Said

Anton Setiyawan, S.Si., M.M.
Director of Digital Economic Protection,
State Cyber and Crypto Agency

"The existence of CyberArmy as a **crowdsourced cybersecurity service entity is an important step for the Cyber Indonesia ecosystem** . First, it shows the ability and progress of the local Cyber Security industry.

Secondly, this is an innovation in **getting quality Cyber Security services at a cost that is not burdensome.**

Third, this can be an example of developing the potential of millennial generation in contributing to **maintaining national cyber security** . **We have collaborated several times** with them and **always get the expected results** . Hopefully CyberArmy services will continue to grow and become even better in the future. Thank you."

Christofer Simbar
Information Security Analyst BPJS

"As a new player in the crowdsourced cybersecurity industry, **the services provided by Cyberarmy exceed our expectations. Through Cyberarmy we can prevent the exploitation of critical security holes that have never been found by 3 penetration testing service providers beforehand ."**

What They Said

Bherly Novrandy
VP Engineering at Kitabisa.com

" **CyberArmy helps anticipate security gaps that pose a great risk to business continuity** , so that **we can produce safer and more trusted products** for users of Kitabisa."

Head of KIPD ICT Center
Ministry of Foreign Affairs

"Most cyber security cases in Indonesia are hacking cases that target government sites. **We are greatly helped by CyberArmy services** with its bug bounty in order **to strengthen cyber resilience at the Ministry of Foreign Affairs** ."

CyberArmy
Bug Bounty and Vulnerability Coordination Center

Bug Bounty Program

Bug Bounty Program is a company's initiative that appreciates the findings of security holes from ethical hackers, also called Bughunters in an application / system / service.

Companies can find vulnerabilities earlier before irresponsible parties find and exploit them. Through this program, companies also can implement security controls on an ongoing basis.

Benefit of Bug Bounty Program:

- **Continuous Security Testing**
  Period 1 – 12 Months
- **Rich of Findings**
- **Reducing the Risk of Vulnerability**
- **Affordable**

Program Types

There are two types of program in Bug Bounty Program

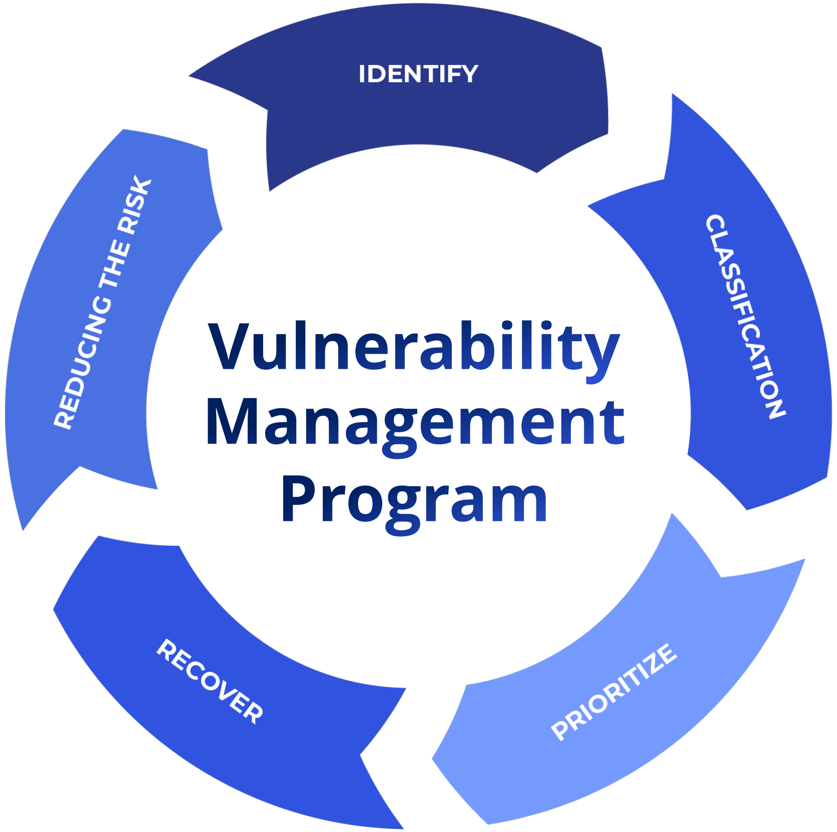
Public Program

Your Bug Bounty program will be published to all Bughunters. This will provide opportunities for hundreds of Bughunters to find vulnerabilities in your application.

Private Program

Your Bug Bounty program will be published to Bughunter who gets an invitation. We select competent Bughunters to follow the bug bounty program in applications that store sensitive information.

CyberArmy
Bug Bounty and Vulnerability Coordination Center



Vulnerability management is a security cycle mechanism whose activities are identify vulnerabilities, classification, prioritize, recover and reducing the risk.

Vulnerability management is a solution for application owners to secure their information and applications without the need for a long security process.

Benefit of Vulnerability Management:

Continuous Security Testing
Period 6– 12 Months

Rich of Findings

The Vulnerability is closed quickly

Reducing the Risk of Vulnerability

Program Types:

Public Program
Your Bug Bounty program will be published to all Bughunters. This will provide opportunities for hundreds of Bughunters to find vulnerabilities in your application.

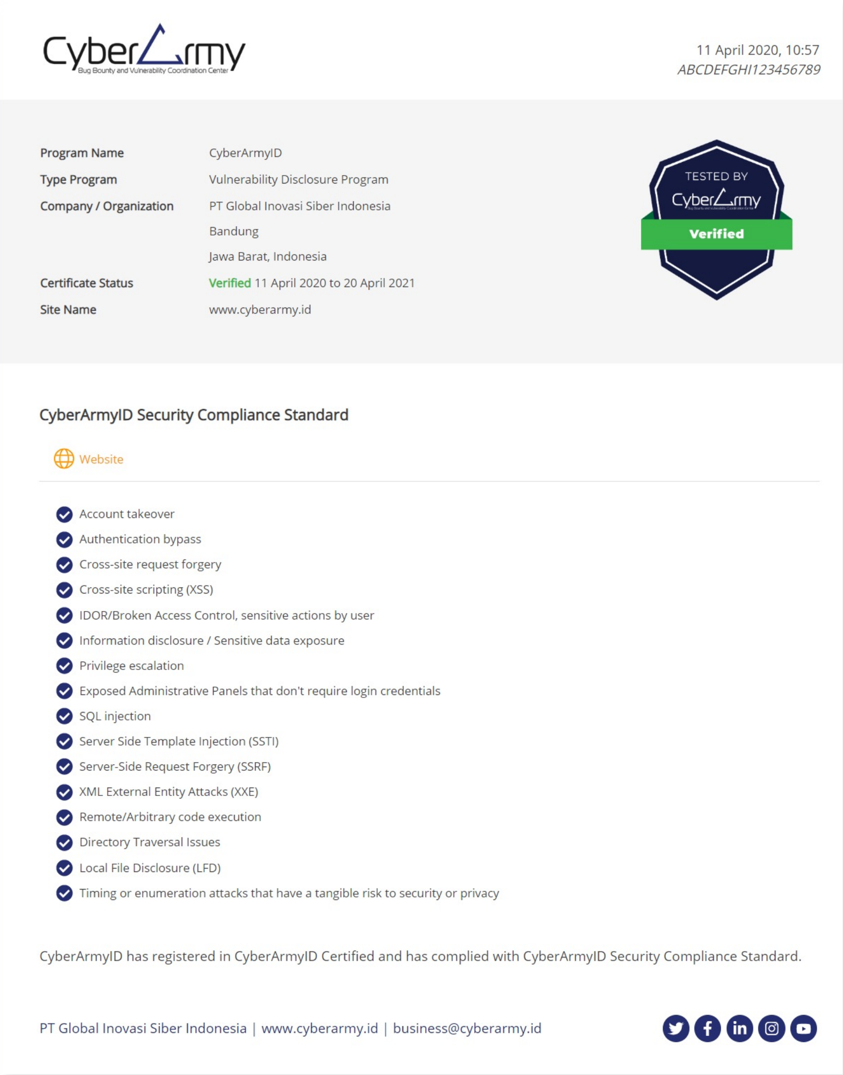
Vulnerability Management (CyberArmyID Security Assurance)

CyberArmy
Bug Bounty and Vulnerability Coordination Center

CyberArmyID Security Assurance is a certificate that can be installed on your Business Application, to certify that your Business Application is subjected to Continuous Security Testing in accordance with the CyberArmyID Security Compliance Standard.

Benefits for Your Business Application:

- CyberArmyID Compliance Standard
- Your Application Vulnerability is found faster
- Reducing the Risk of Cyber Attacks



CyberArmy
Bug Bounty and Vulnerability Coordination Center

11 April 2020, 10:57
ABCDEFGHI123456789

Program Name	CyberArmyID
Type Program	Vulnerability Disclosure Program
Company / Organization	PT Global Inovasi Siber Indonesia Bandung Jawa Barat, Indonesia
Certificate Status	Verified 11 April 2020 to 20 April 2021
Site Name	www.cyberarmy.id

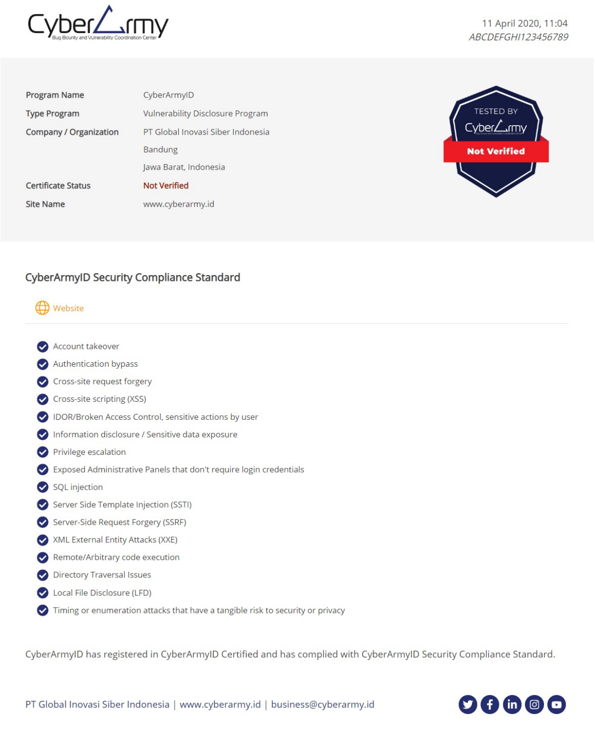
CyberArmyID Security Compliance Standard

Website

- ✓ Account takeover
- ✓ Authentication bypass
- ✓ Cross-site request forgery
- ✓ Cross-site scripting (XSS)
- ✓ IDOR/Broken Access Control, sensitive actions by user
- ✓ Information disclosure / Sensitive data exposure
- ✓ Privilege escalation
- ✓ Exposed Administrative Panels that don't require login credentials
- ✓ SQL injection
- ✓ Server Side Template Injection (SSTI)
- ✓ Server-Side Request Forgery (SSRF)
- ✓ XML External Entity Attacks (XXE)
- ✓ Remote/Arbitrary code execution
- ✓ Directory Traversal Issues
- ✓ Local File Disclosure (LFD)
- ✓ Timing or enumeration attacks that have a tangible risk to security or privacy

CyberArmyID has registered in CyberArmyID Certified and has complied with CyberArmyID Security Compliance Standard.

PT Global Inovasi Siber Indonesia | www.cyberarmy.id | business@cyberarmy.id



CyberArmy
Bug Bounty and Vulnerability Coordination Center

11 April 2020, 11:04
ABCDEFGHI123456789

Program Name	CyberArmyID
Type Program	Vulnerability Disclosure Program
Company / Organization	PT Global Inovasi Siber Indonesia Bandung Jawa Barat, Indonesia
Certificate Status	Not Verified
Site Name	www.cyberarmy.id

CyberArmyID Security Compliance Standard

Website

- ✓ Account takeover
- ✓ Authentication bypass
- ✓ Cross-site request forgery
- ✓ Cross-site scripting (XSS)
- ✓ IDOR/Broken Access Control, sensitive actions by user
- ✓ Information disclosure / Sensitive data exposure
- ✓ Privilege escalation
- ✓ Exposed Administrative Panels that don't require login credentials
- ✓ SQL injection
- ✓ Server Side Template Injection (SSTI)
- ✓ Server-Side Request Forgery (SSRF)
- ✓ XML External Entity Attacks (XXE)
- ✓ Remote/Arbitrary code execution
- ✓ Directory Traversal Issues
- ✓ Local File Disclosure (LFD)
- ✓ Timing or enumeration attacks that have a tangible risk to security or privacy

CyberArmyID has registered in CyberArmyID Certified and has complied with CyberArmyID Security Compliance Standard.

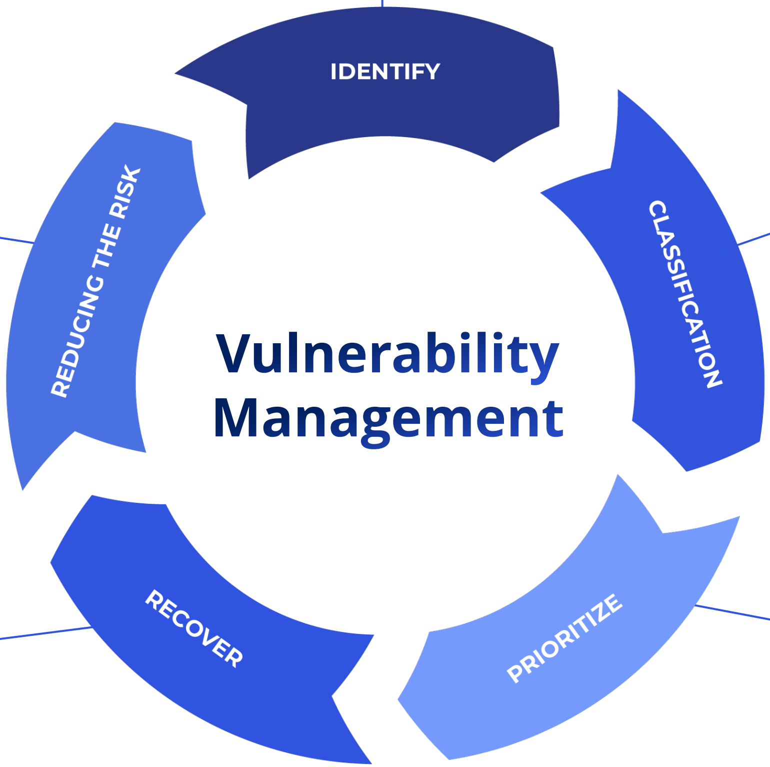
PT Global Inovasi Siber Indonesia | www.cyberarmy.id | business@cyberarmy.id

Vulnerability Management Service Flow

CyberArmy
Bug Bounty and Vulnerability Coordination Center

1 **Crowdsourced Security Testing**

Doing Exploits and Validate Reports



2 **Risk Category**

Determine the risk category from the testing report

This information will be displayed on the dashboard

3 **Risk Severity Level**

Determine the risk severity level of the testing report

This information will be displayed on the dashboard

4 **Patching and Consultation**

Doing Patching and Consultation

Coordination via Telegram or Slack

5 **Re-test and Re-patch**

Doing Re-test and Re-patch

Private Discussion on the dashboard and Coordination via Telegram or Slack

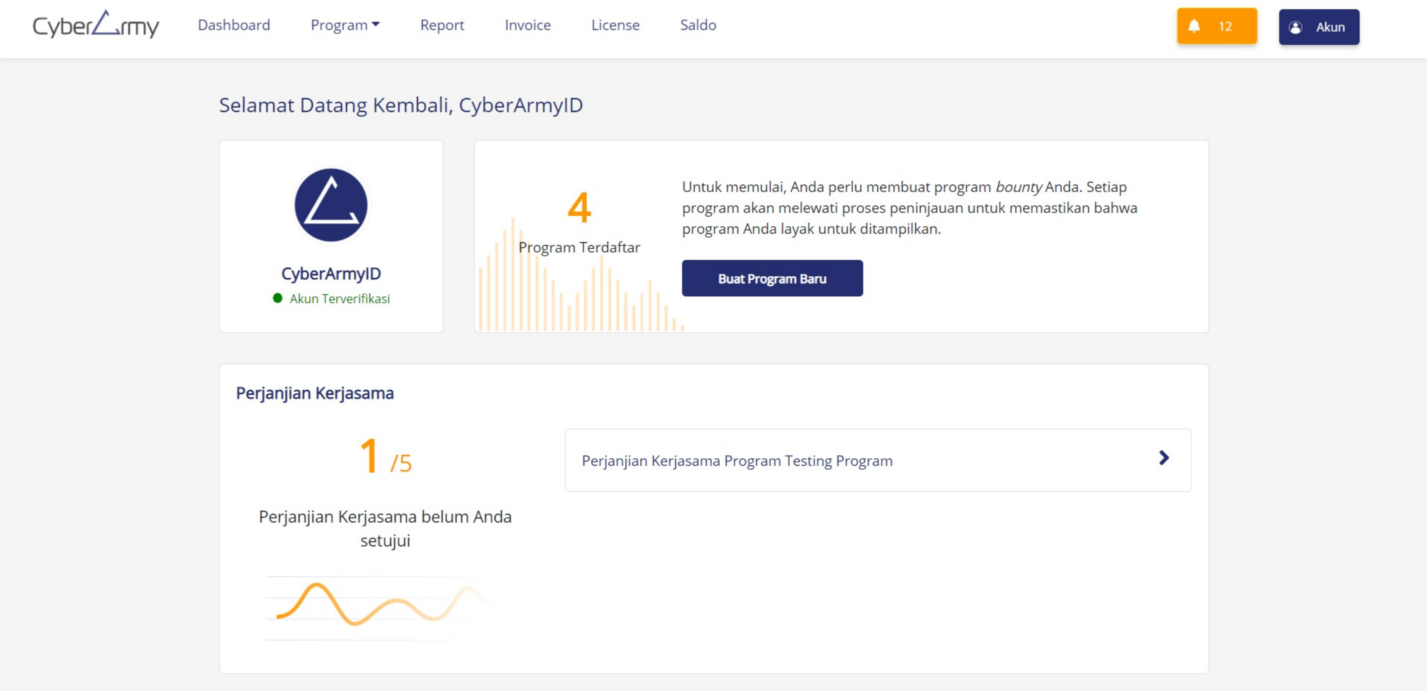
Coordination Flow :

1. Company provides information (URL Target) to the CyberArmy Team for Crowdsourced Security Testing
2. Bughunter exploits the target URL and CyberArmy validates the exploit
3. Company can monitor and view exploit reports on the CyberArmy dashboard
4. Company and CyberArmy coordinate for patching
5. Carry out continuous re-tests and re-patches

Bug Bounty and Vulnerability Coordination Center

Vulnerability Management Dashboard

For Bugbounty Program and Penetration Testing



Selamat Datang Kembali, CyberArmyID

4
Program Terdaftar

Untuk memulai, Anda perlu membuat program *bounty* Anda. Setiap program akan melewati proses peninjauan untuk memastikan bahwa program Anda layak untuk ditampilkan.

Perjanjian Kerjasama

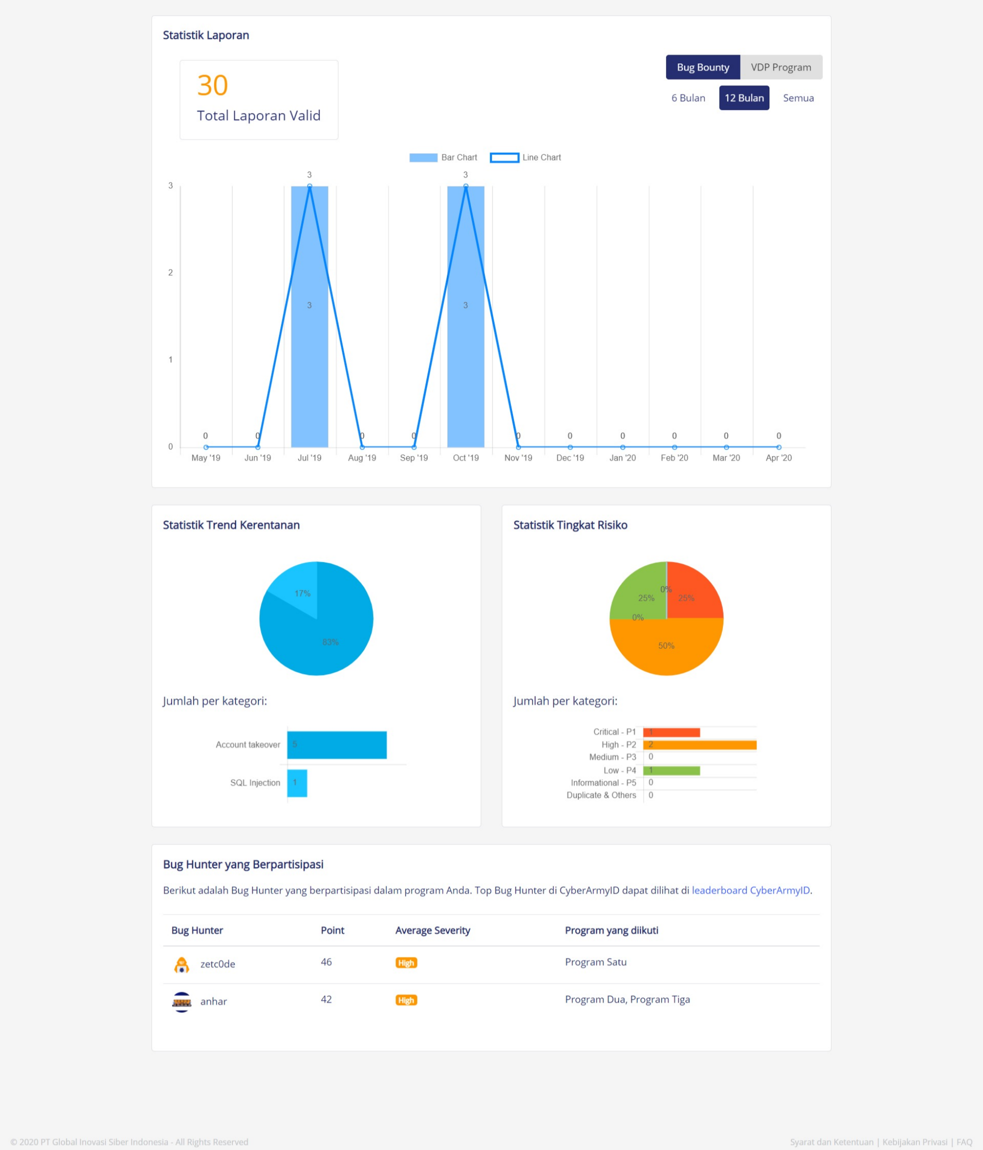
1 /5

Perjanjian Kerjasama belum Anda setujui

Perjanjian Kerjasama Program Testing Program

Continuous Monitoring

Valid Reports, Risk Category and Risk Severity Level Statistic



Statistik Laporan

30
Total Laporan Valid

Statistik Trend Kerentanan

Jumlah per kategori:

Statistik Tingkat Risiko

Jumlah per kategori:

Bug Hunter yang Berpartisipasi

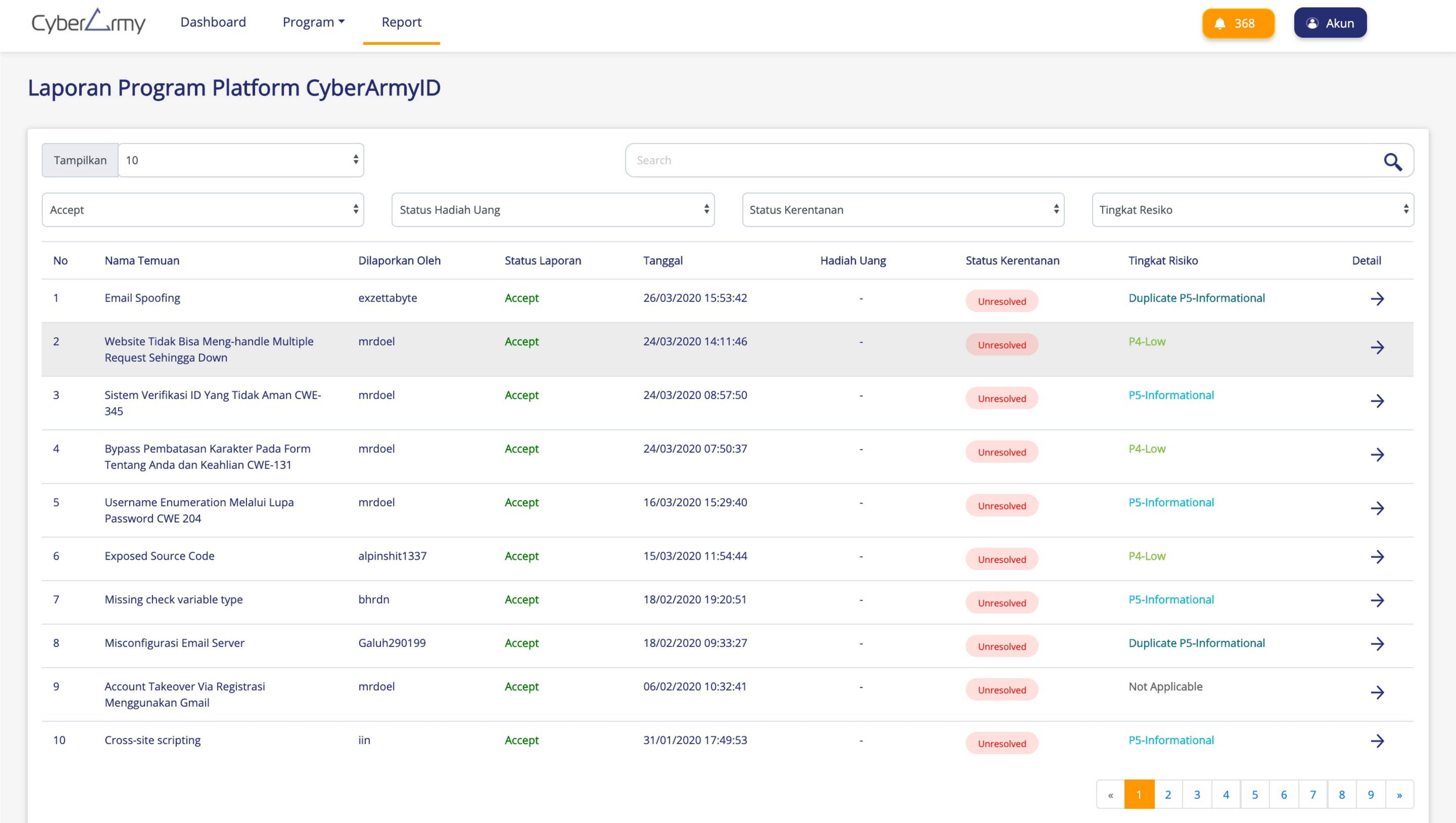
Berikut adalah Bug Hunter yang berpartisipasi dalam program Anda. Top Bug Hunter di CyberArmyID dapat dilihat di leaderboard CyberArmyID.

Bug Hunter	Point	Average Severity	Program yang diikuti
zetc0de	46	High	Program Satu
anhar	42	High	Program Dua, Program Tiga

© 2020 PT Global Inovasi Siber Indonesia - All Rights Reserved

Syarat dan Ketentuan | Kebijakan Privasi | FAQ

All Vulnerability Report on Dashboard



Laporan Program Platform CyberArmyID

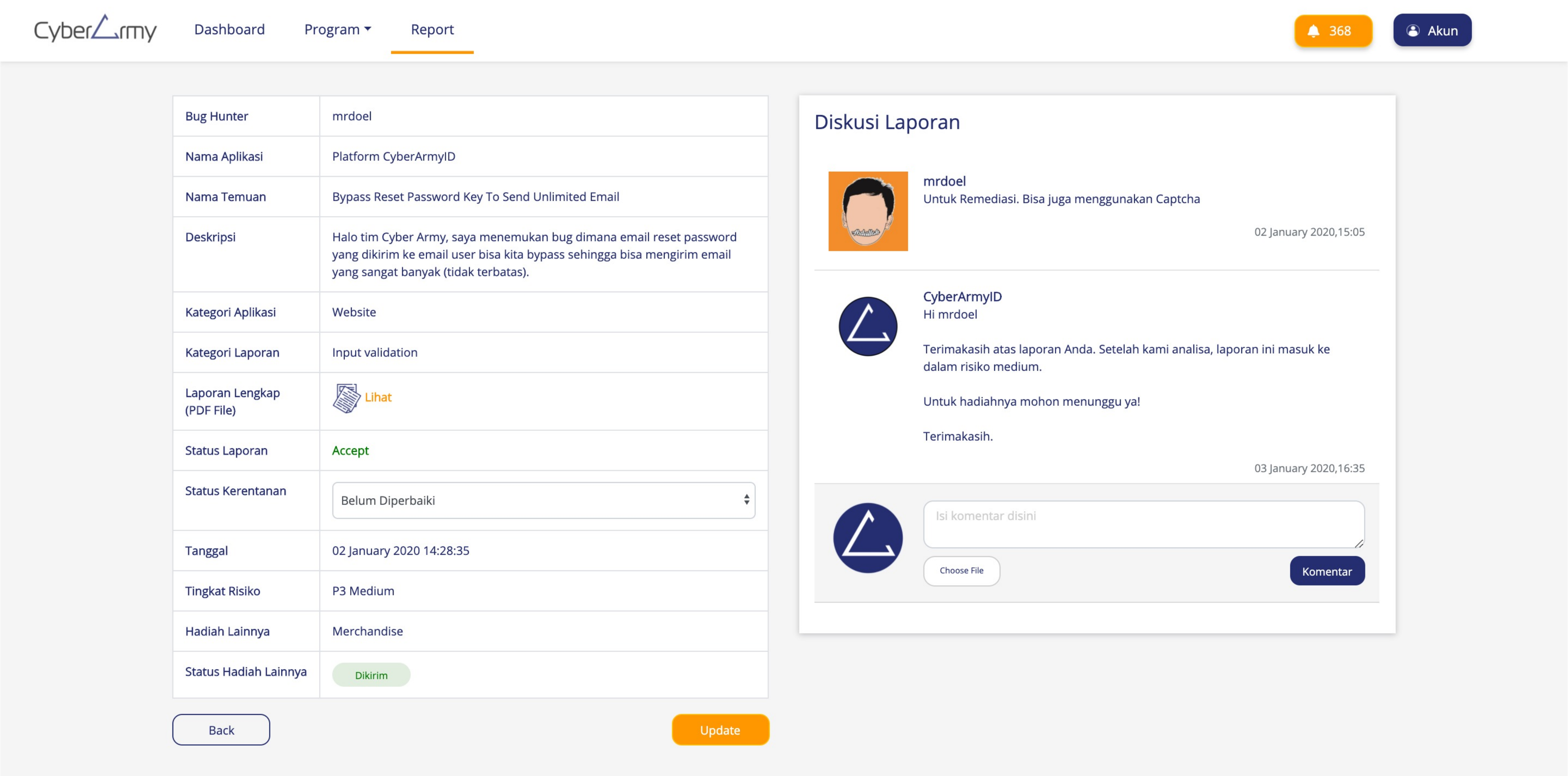
Tampilkan 10

Accept

No	Nama Temuan	Dilaporkan Oleh	Status Laporan	Tanggal	Hadiah Uang	Status Kerentanan	Tingkat Risiko	Detail
1	Email Spoofing	exzettabyte	Accept	26/03/2020 15:53:42	-	Unresolved	Duplicate P5-Informational	→
2	Website Tidak Bisa Meng-handle Multiple Request Sehingga Down	mrdoel	Accept	24/03/2020 14:11:46	-	Unresolved	P4-Low	→
3	Sistem Verifikasi ID Yang Tidak Aman CWE-345	mrdoel	Accept	24/03/2020 08:57:50	-	Unresolved	P5-Informational	→
4	Bypass Pembatasan Karakter Pada Form Tentang Anda dan Keahlian CWE-131	mrdoel	Accept	24/03/2020 07:50:37	-	Unresolved	P4-Low	→
5	Username Enumeration Melalui Lupa Password CWE 204	mrdoel	Accept	16/03/2020 15:29:40	-	Unresolved	P5-Informational	→
6	Exposed Source Code	alpinshit1337	Accept	15/03/2020 11:54:44	-	Unresolved	P4-Low	→
7	Missing check variable type	bhrdn	Accept	18/02/2020 19:20:51	-	Unresolved	P5-Informational	→
8	Misconfigurasi Email Server	Galuh290199	Accept	18/02/2020 09:33:27	-	Unresolved	Duplicate P5-Informational	→
9	Account Takeover Via Registrasi Menggunakan Gmail	mrdoel	Accept	06/02/2020 10:32:41	-	Unresolved	Not Applicable	→
10	Cross-site scripting	iin	Accept	31/01/2020 17:49:53	-	Unresolved	P5-Informational	→

Detail Report and Private Discussion with Bughunter

CyberArmy
Bug Bounty and Vulnerability Coordination Center



Bug Hunter	mrdoel
Nama Aplikasi	Platform CyberArmyID
Nama Temuan	Bypass Reset Password Key To Send Unlimited Email
Deskripsi	Halo tim Cyber Army, saya menemukan bug dimana email reset password yang dikirim ke email user bisa kita bypass sehingga bisa mengirim email yang sangat banyak (tidak terbatas).
Kategori Aplikasi	Website
Kategori Laporan	Input validation
Laporan Lengkap (PDF File)	Lihat
Status Laporan	Accept
Status Kerentanan	Belum Diperbaiki
Tanggal	02 January 2020 14:28:35
Tingkat Risiko	P3 Medium
Hadiah Lainnya	Merchandise
Status Hadiah Lainnya	Dikirim

Diskusi Laporan

mrdoel
Untuk Remediasi. Bisa juga menggunakan Captcha

02 January 2020,15:05

CyberArmyID
Hi mrdoel

Terimakasih atas laporan Anda. Setelah kami analisa, laporan ini masuk ke dalam risiko medium.

Untuk hadiahnya mohon menunggu ya!

Terimakasih.

03 January 2020,16:35

Security Testing Details

API (Application Programming Interface)

In Scope Vulnerabilities Checklist :

✓ Bruteforce JWT Token
✓ Input validation
✓ Not limit requests for DDoS/Bruteforce attacks
✓ Not using whitelist method in redirect url
✓ Sensitive data are not encrypted
✓ Sensitive data stored in JWT payload
✓ Use Basic Auth, not use standard authentication

iOs/Android Application

In Scope Vulnerabilities Checklist :

✓ Client Code Quality
✓ Code Tampering
✓ Extraneous Functionality
✓ Improper Platform Usage
✓ Insecure Authentication
✓ Insecure Authorization
✓ Insecure Communication
✓ Insecure Data Storage
✓ Insufficient Cryptography
✓ Reverse Engineering

Web Application

In Scope Vulnerabilities Checklist :

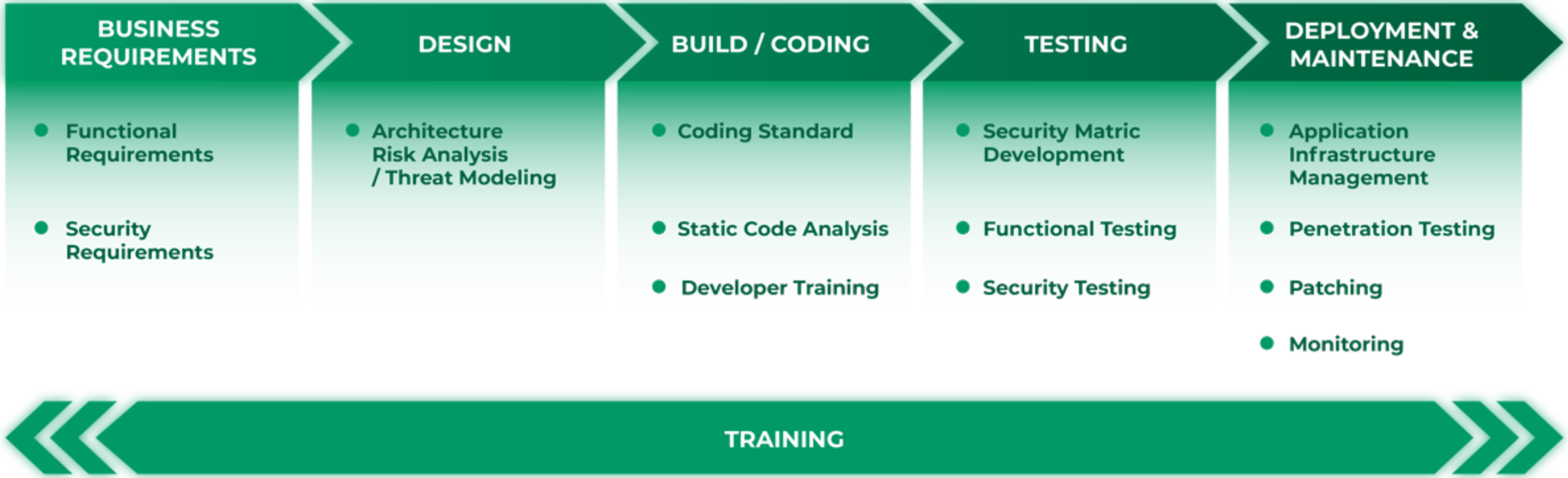
✓ Account takeover
✓ Authentication bypass
✓ Cross-site request forgery
✓ Cross-site scripting (XSS)
✓ IDOR/Broken Access Control, sensitive actions by user
✓ Information disclosure / Sensitive data exposure
✓ Privilege escalation
✓ Exposed Administrative Panels that don't require login credentials
✓ SQL injection
✓ Server Side Template Injection (SSTI)
✓ Server-Side Request Forgery (SSRF)
✓ XML External Entity Attacks (XXE)
✓ Remote/Arbitrary code execution
✓ Directory Traversal Issues
✓ Local File Disclosure (LFD)
✓ Timing or enumeration attacks that have a tangible risk to security or privacy

Cybersecurity Consultant – Secure SDLC

Software Development Life Cycle (SDLC) merupakan kerangka kerja yang mendefinisikan proses yang digunakan oleh organisasi untuk membangun aplikasi dari awal hingga dapat digunakan secara operasional.

Dalam hal inilah konsep Secure SDLC muncul. Proses SDLC yang aman (Secure SDLC) memastikan bahwa kegiatan jaminan keamanan seperti analisis arsitektur, *threat modeling,* pengujian penetrasi, source code review, hingga *monitoring* merupakan bagian integral dari upaya pengembangan.

Proses Secure Software Development Life Cycle :



BUSINESS REQUIREMENTS
- Functional Requirements
- Security Requirements

DESIGN
- Architecture Risk Analysis / Threat Modeling

BUILD / CODING
- Coding Standard
- Static Code Analysis
- Developer Training

TESTING
- Security Matric Development
- Functional Testing
- Security Testing

DEPLOYMENT & MAINTENANCE
- Application Infrastructure Management
- Penetration Testing
- Patching
- Monitoring

TRAINING

In-house Cybersecurity Training

CYBER ACADEMY

Focuses on developing knowledge to individuals in technical and managerial contexts. This service consists of training that is focused on learning how to assess the security system, fix the vulnerabilities, and to raise security concerns in various groups in a company / organization.

In-house Training Clients:

BADAN SIBER DAN SANDI NEGARA BSSN

pindad

Telkom Indonesia
the world in your hand

swamedia innovative IT solution

GS
GS BATTERY

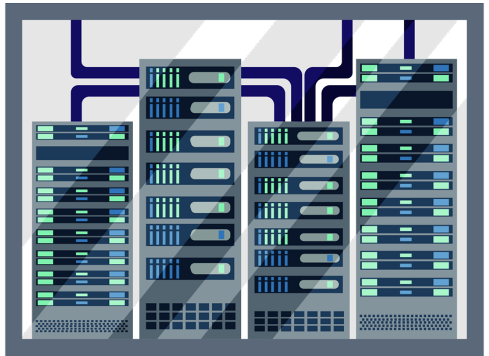
PT PII PENJAMINAN & INFRASTRUKTUR

KEMENTERIAN KEUANGAN
REPUBLIK INDONESIA

Pegadaian

Manage Training with Cyber Academy's

Learning Management System



Secure SDLC Training

Secure Software Development Life Cycle (Secure Coding) is an educational activity for developers regarding methods for developing secure applications.

Developers will learn various attack techniques on applications, explain how attacks can occur and will open insight for developers about what things must be considered in making applications safely.

CYBER ACADEMY

www.cyberacademy.id

Public Workshop

In-house Training at Telkom Indonesia

Secure Coding Workshop for Startup, collaboration with BSSN

In-house Training at Telkom Indonesia

Penetration Testing Training

Penetration Testing is an educational activity aimed for technical people.

This activity is to increase understanding of attack techniques on a system. Participants will learn various attack techniques that can be carried out on the system so that they can explain how the attack can occur.

In-house Training at Telkom Indonesia

In-house Training at Telkom Indonesia

In-house Training at Telkom Indonesia

In-house Training at Telkom Indonesia

CYBER ACADEMY

www.cyberacademy.id

Cyber Security Awareness

Security Awareness is an educational activity with the target participants being all individuals in an organization.

The purpose of this education is to provide an understanding of the risks and impacts of the information used, understand the potential of threats and increase awareness of information and cyber security.

PT Pindad (Persero)

IT Division at Telkom Group

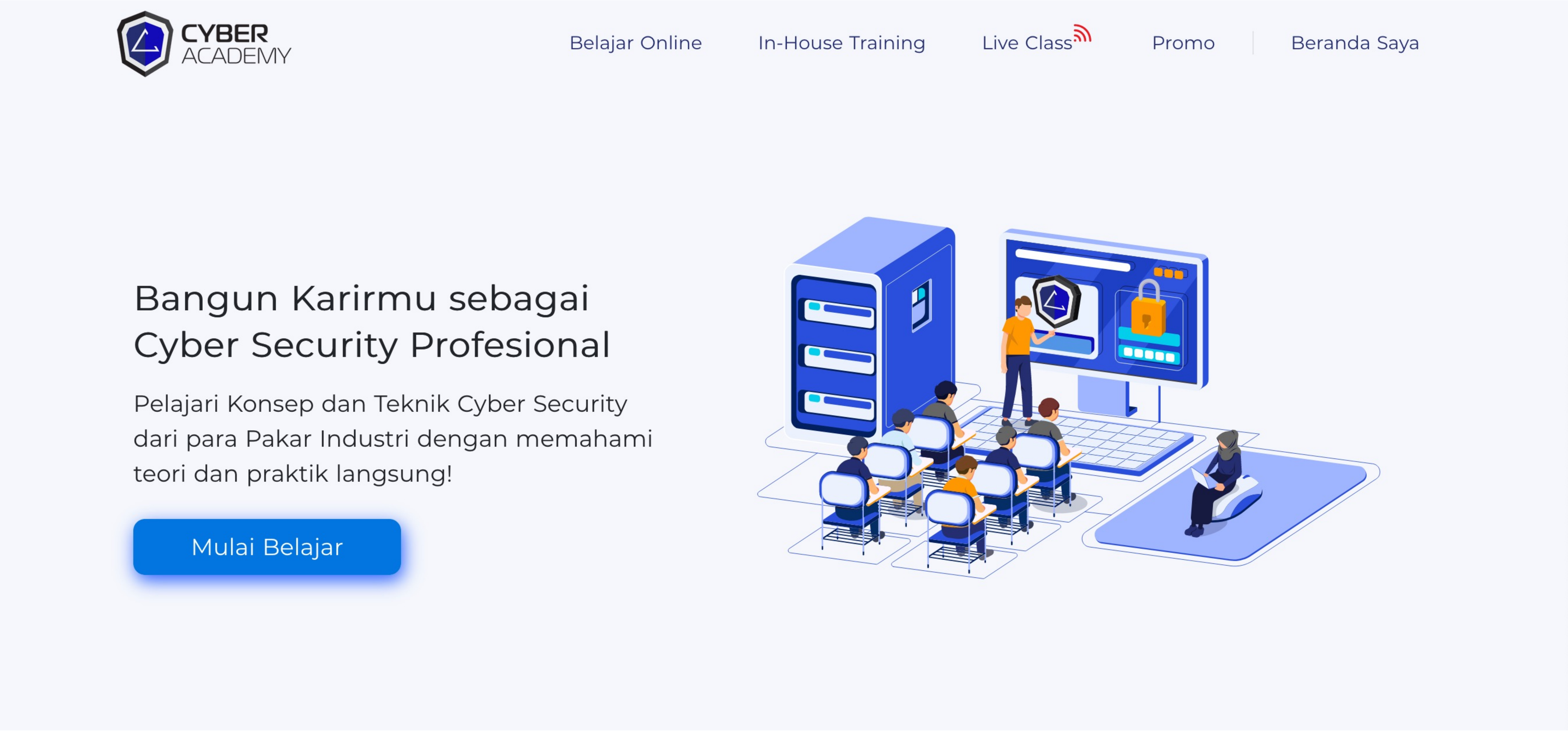
IT Division at Telkom Indonesia

State Cyber and Crypto Agency (BSSN)

CYBER ACADEMY

www.cyberacademy.id

Online Cybersecurity Academy – www.cyberacademy.id



Bangun Karirmu sebagai Cyber Security Profesional

Pelajari Konsep dan Teknik Cyber Security dari para Pakar Industri dengan memahami teori dan praktik langsung!

TEAM

Girindro Pringgo Digdo, M.T, OSCP, CSXF

Founder & CEO

Expertise in :
Security Consultant, doing:
Penetration Testing, Vulnerability Assessment
Risk Management, Education.
Computer Security Books Author
Holds OSCP, CSXF

Muhammad Shifa Zulfikar, S.Kom, SCCS-F, SCMS-F

Co-Founder & COO

Expertise in :
Business Development & Operation
IT Project Management
IT Infrastructure
Design Thinking
Holds Corporate Sales & Marketing Strategy

Rendy Bustari, S.Kom

Senior Software Engineer

Expertise in :
DevSecOps

Febry Ghaisani, S.Kom

Software Engineer

Expertise in :
Artificial Intelligence
Frontend Developer

Anhar Solehudin, S.Si

Lead Software Engineer

Expertise in :
Mobile Apps Developer
Fullstack Developer
Holds Kotlin Android Developer Expert

Chintya Dwi Hadiani, M.Ak

Finance Officer

Expertise in :
Accounting
Tax

CyberArmy

Bug Bounty and Vulnerability Coordination Center

#1 CROWDSOURCED CYBER SECURITY PLATFORM IN INDONESIA

PT Global Inovasi Siber Indonesia

Address: Jl. Naripan No.53, Kb. Pisang, Sumur Bandung
Kota Bandung, Jawa Barat, Indonesia
Phone Number : +62812 9393 1337
Email : business@cyberarmy.id
Website : www.cyberarmy.id