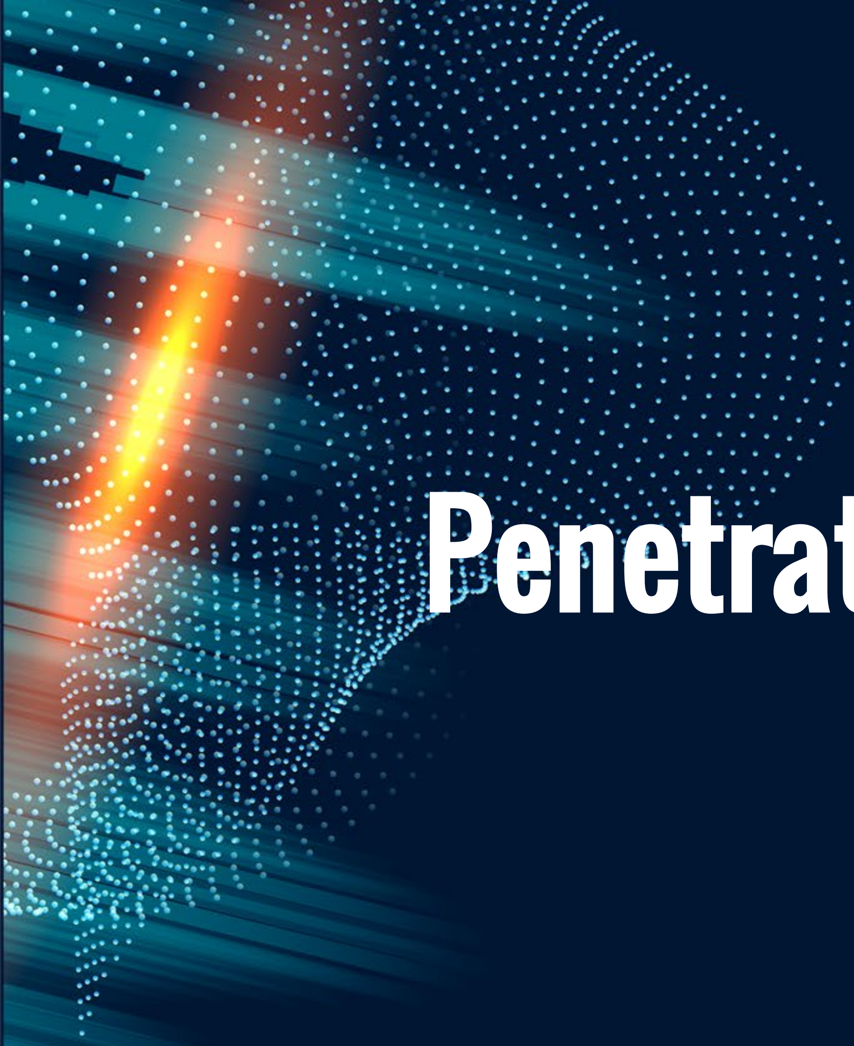


UnderDefense

Penetration Testing

12

Certified Ethical Hackers

122

Pentest projects per year

180+

Apps security testing projects completed

Our Customers are brands you know and consume daily

NOVA POSHTA INTERNATIONAL

intl CASCADE

BVP

Deloitte.

BigID

PXCOM ONBOARD DIGITAL SOLUTIONS

OCTOPUS by JOY

DATAGROUP ОПЕРАТОР РІШЕНЬ

Yaypay

transdev the mobility company

ORACLE

ONLINECOMPLIANCE.ORG

laPolar

Volkswagen

ZO ALLIANCE

eurolines

umanlife

IRIS.TV

Nextory

jscrambler

sensemetrics

artery

G4S

State Bank of India

VinciWorks

evertz

direktgruppe

iQ3

ION

CLOUDALLY

kyte

ixaris Perfect Fit Payments

Symphony Solutions

ADVICE GROUP

CIKLUM EMPOWERING COLLABORATION

Anadarko Petroleum Corporation

bom pra crédito .com.br

FOX

Haystack tv

GEARBEST

Botentekoop.nl

LEO CYBER SECURITY

BETLAB

KROMTECH

airmalta

COREVALUE

beyond SECURITY

romexsoft

N-iX

wispi

MATRIX42

Palo Alto Software

Hova health Telemedicine Technology

epi EPISOURCE

eleks

BitGive

MARKET ACCESS DIRECT

OKKO GROUP

shieldIOT

mindmarker the leader in training reinforcement

First Home

SentinelOne

ACCEDIAN NETWORKS

KARSTADT

КИЇВСТАР

mindmarker

Nexia DK

NINJA

betsson group

Bitspark

FEATURE SPACE

Snapbook

SECURITHINGS

RELEVANT SOFTWARE

JULY SYSTEMS

UNDER DEFENSE

BEYOND security

Top Clients

12

Certified Ethical Hackers

120

Pentest projects per year

280

Apps security testing projects completes

BILL & MELINDA GATES foundation

Volkswagen

MIO

McKinsey Investment Office

KARSTADT

betsson group

CASCADE

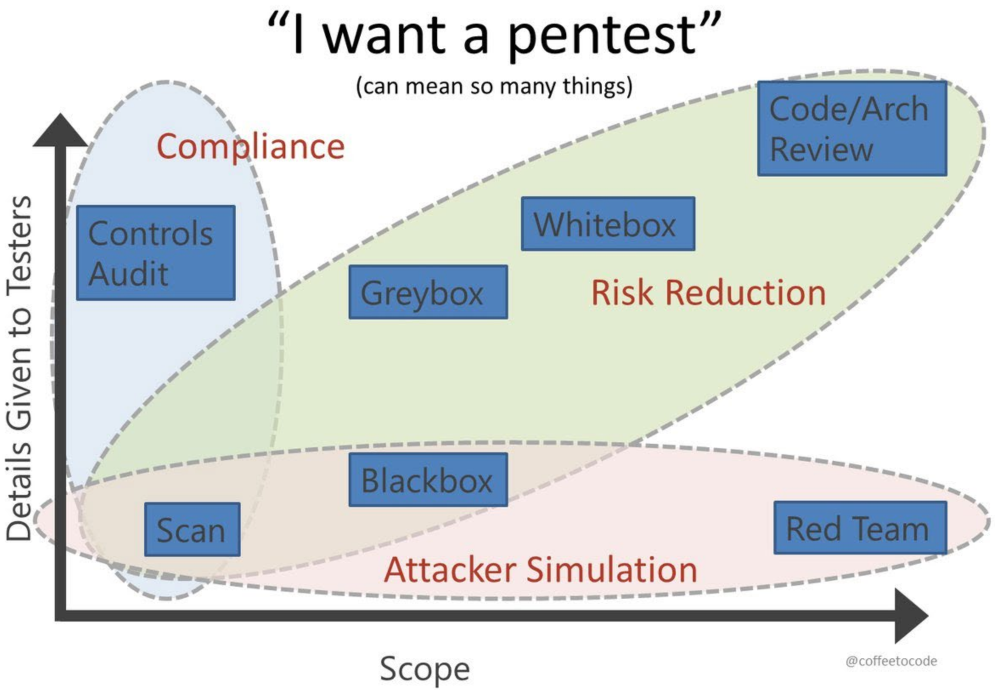
INVESTMENT GROUP, INC.

What is Penetration Testing

Penetration Test (other words - Ethical hacking) is a **simulation of a real world cyber attack.** Our goal during the project is to discover the weaknesses and **prevent risks of A POTENTIAL INTRUSION**

During the test we can find weaknesses in services and exploit them, access and exfiltrate sensitive data, discover gaps in network security and flaws in code.

We do everything the real hacker does, but with good intentions



Penetration Testing

Find vulnerabilities in your systems before the hackers use them against you

Types of a penetration test we provide

Network – External or Internal

Mobile Application

Social Engineering

Wireless Network

Web Application

Hack your THINGS
IoT, Cars, 5G, SCADA,
Robots

Red Team Attack Simulation

Benefits:

Pay for result

Fast & Innovative

Security Guarantee

UNDER DEFENSE

Business risks mitigated

- Full web application compromise
- Admins accounts compromise
- Users accounts compromise
- Full infrastructure compromise

Financial loss

10 000 000 €

Reputational damage

Data loss

Loss of clients' trust

Why Perform a Penetration Testing

Technical Reasons:

1. To get true knowledge about the real state of Security and secure your sensitive information
2. Learn your defense capability, check holes in the infrastructure, understand how secure you are to prevent data leakage or operations block:
   - Identify all application-related vulnerabilities of measurable risk
   - Design, Business Logic and compound flaw risks identification
   - Diagnosis of network vulnerabilities from an external hacker perspective

3 To check intrusion detection and incident response

Business Reasons:

1. Increase value and attract more customers, you differentiate by having security autestation
2. To obtain compliance
3. Penetration testing report that can be shared with any client on their request as proof of passing compliance or security audit.

Penetration Testing Methods

We distinguish the Pen Tests classification by the level of access permission and divide it by three main methods.

Black Box:

The full simulation of external cyberattack, when we are simply given the link for a domain or application environment and try to penetrate the company.

Grey Box

(most common) when we already have some minimum access (f.e.: accounts created for our pentesters or system documentation) and try to discover the holes in the security system.

White Box:

insider threat simulation, when we have the full internal vision of system and its functionality (this may also include source code review for product)

Vulnerability scan vs. Penetration Test

Scanners - Cannot THINK….

Looking for known, defined and predictable patterns
Scanners create an Illusion of SAFETY

Manual pentest searches for:

- Logical defects
- Rights separation
- Complex attack vectors
- Defects in architecture and design
- Real Cryptography level

UnderDefense MPT is designed to complement and extend an automated assessment

Manual penetration testing adds **the benefit** of **specialized human expertise** to our automated static and dynamic analysis — and it **simulation of the same methodology cyber-criminals use to exploit application weaknesses such as business logic vulnerabilities.**

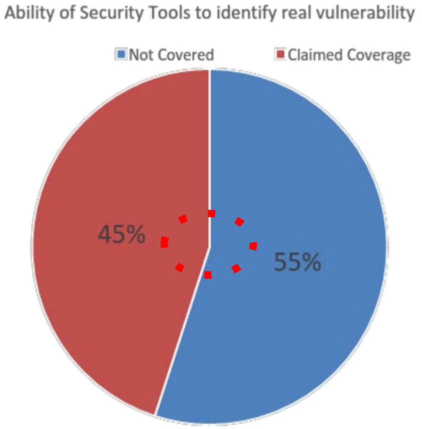
The goal of such testing is to determine the potential for an attacker to successfully access and perform a variety of malicious activities by exploiting vulnerabilities, either previously known or unknown, in the software.

UNDER DEFENSE

Tools - At Best 12%

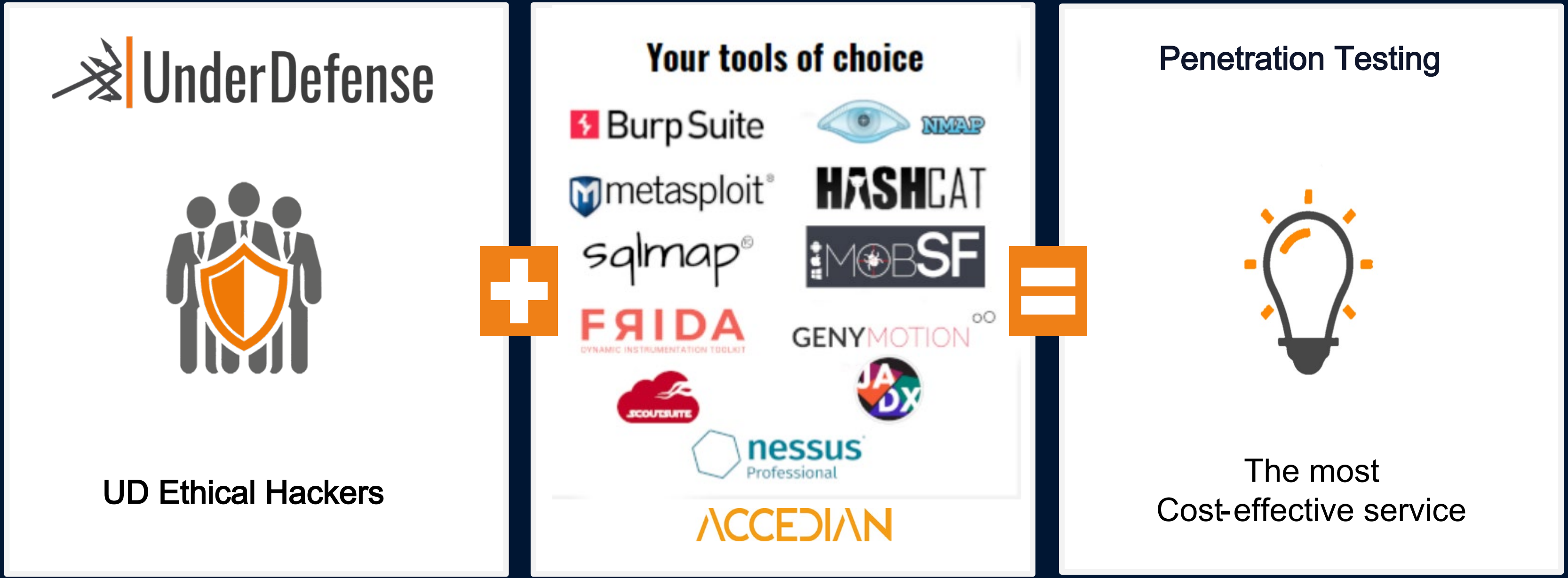
- MITRE found that all application security tool vendors’ claims put **together** cover only 45% of the known vulnerability types (695)

- Based on this new data from the CSA at the NSA, **SAST has 12% vulnerability coverage**



Penetration Testing Service

We do everything the real hacker does, but with good intentions.



UD Ethical Hackers

Your tools of choice

Penetration Testing

The most
Cost-effective service

Benefits:

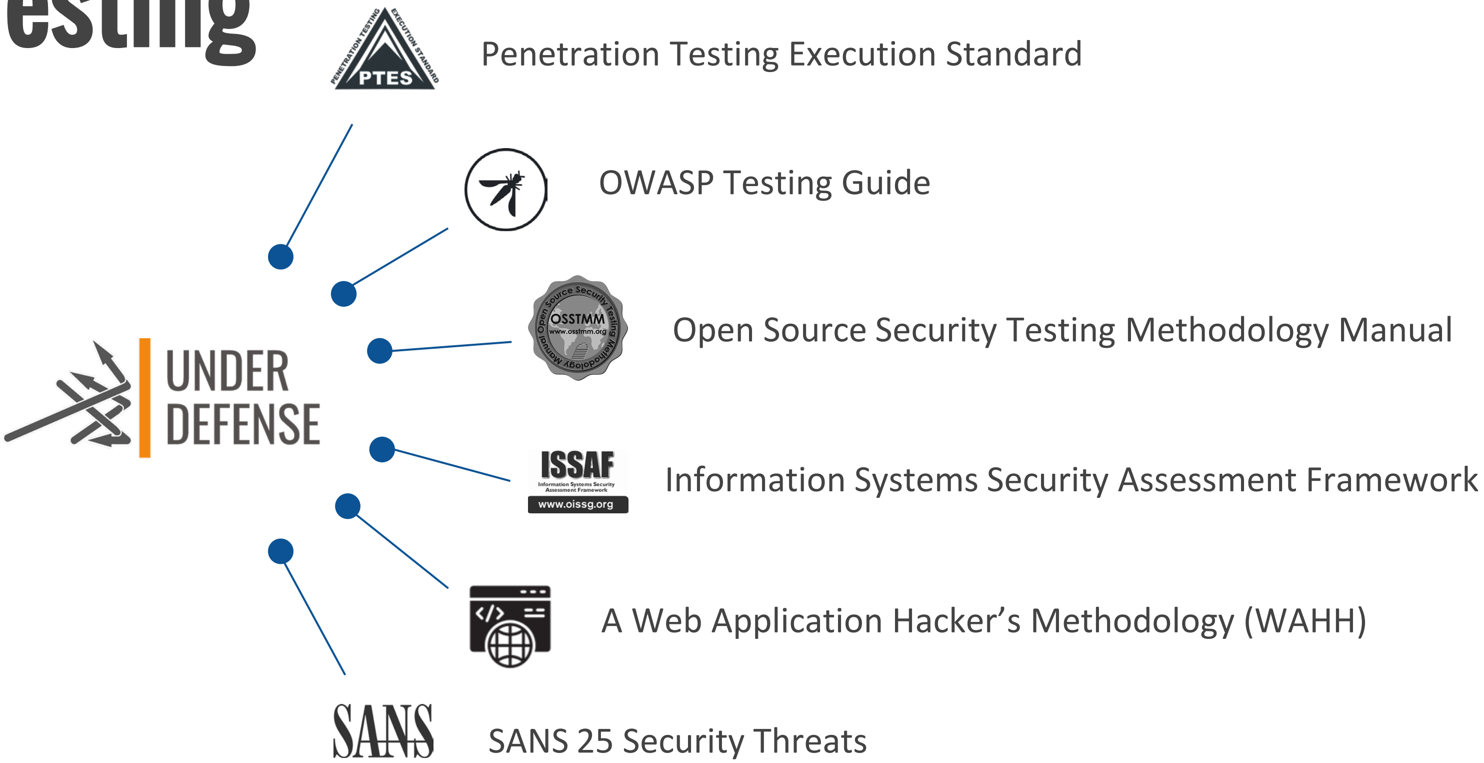
- Hacking ethically
- Training Blue Team
- Uncovering security gaps
- Collaborate on resilience

:

LIST of TOOLS:

,Kali Linux, OpenVAS, Acunetix, Qualys, WireShark, Nmap, hping3, socat, scapy, Firefox, ike-scan, whois, BeEF framework, Metasploit, PortSwinger Burpsuite PRO, Google, Cain &Abel, Maltego, Paterva, Colasoft Packet Builder, Fiddler, Mantra Security Framework, SAINT, Vega, WebScarab, Xenotix, John the Ripper, Colasoft Capsa Network Analyzer, OWASP Zed Attack Proxy (ZAP), Nikto Web Scanner, THC-Hydra, w3af, SQLmap, Karma, Kismet, NetStumbler, VisualCodeGrepper (VCG), onlinehashcrack.com, sslsplit, Pineapple, Reaver, reaver-wps-fork-t6x, Flawfinder, RATS, FindBugs, CodePro Analytix, PMD, Graudit, wpscan.

Methodologies used for Penetration Testing



Penetration Testing Execution Standard

OWASP Testing Guide

Open Source Security Testing Methodology Manual

Information Systems Security Assessment Framework

A Web Application Hacker’s Methodology (WAHH)

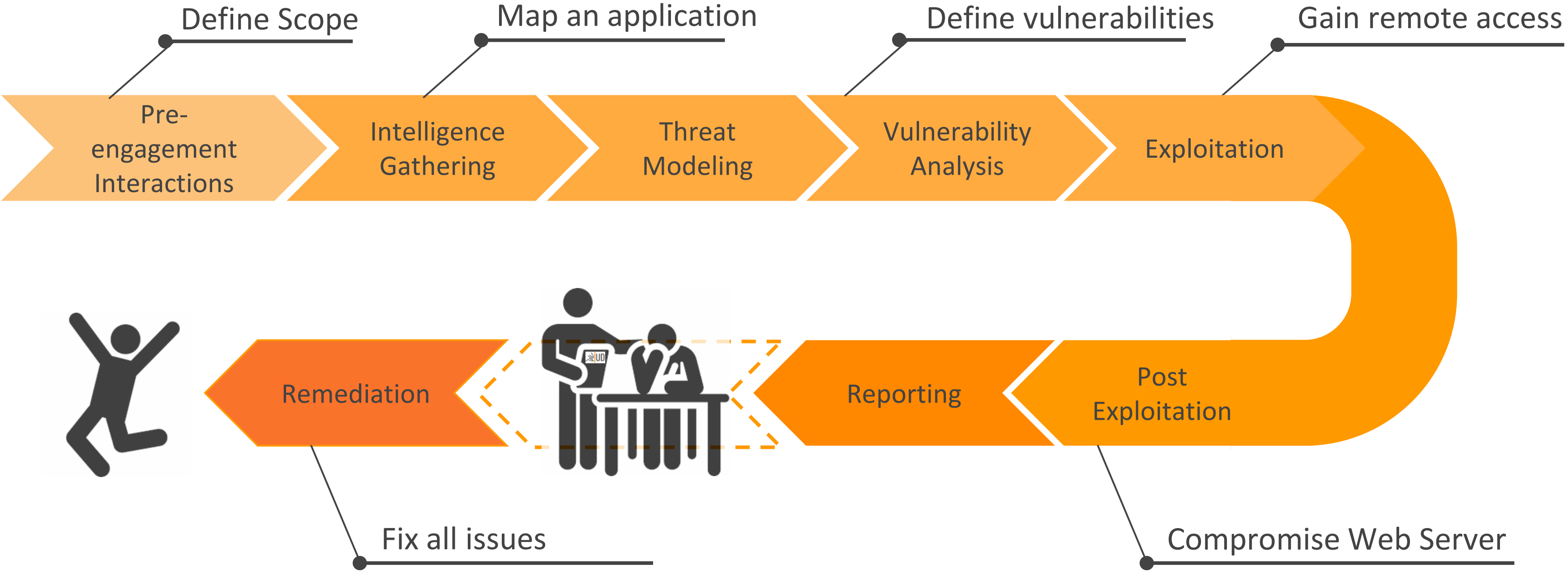
SANS 25 Security Threats

SCOPE

The stated objectives of this penetration test are:

- Circumvent authentication and authorization mechanisms
- Escalate user privileges
- Hijack accounts belonging to other users
- Violate access controls placed by the administrator
- Alter data or data presentation
- Corrupt application and data integrity, functionality and performance
- Circumvent application business logic
- Circumvent application session management
- Break or analyze use of cryptography within user accessible components

Project Planning and Goals



Define Scope

Map an application

Define vulnerabilities

Gain remote access

Fix all issues

Compromise Web Server

Penetration Testing at UD

- Detailed technical report, Analysis of vulnerabilities identified during the Penetration Test
- Attack-Defense game for the IT/Security team to let you objectively evaluate current security investment and readiness of the team to face modern threats.

- One-day free remediation test, conducted 2-3 months after the initial test to check how you have improved the system with our recommendations.
- The letter of attestation to present your clients.

Duration:
2-3 weeks

Team composition:
2 CEH Certified Penetration Testers

UNDER DEFENSE

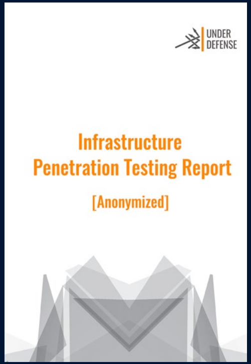
The PenTest Report includes:

As a result of our testing, the UnderDefense will prepare detailed work papers documenting the tests performed, a report of UnderDefense findings including recommendations for additional security controls as required.

- The following information will be included in final report:
  - Proofs of successful vulnerability exploitation
  - Vulnerability exploit procedures, references and sources
  - Categorized risks and mitigation strategy
  - UnderDefense recommendations for closing vulnerabilities and technical references
- Presentation for management and video for development team

UNDER DEFENSE

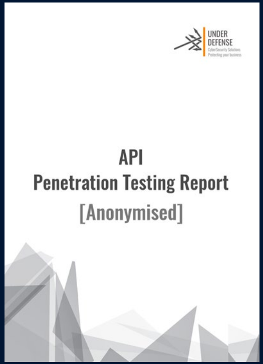
Case Studies and Additional Materials



UNDER DEFENSE

Infrastructure Penetration Testing Report

[Anonymized]



UNDER DEFENSE

CyberSecurity Solutions Protecting your business

API Penetration Testing Report

[Anonymised]

Case Study

UNDER DEFENSE

Web Application Penetration Testing

UNDER DEFENSE

Web Application Penetration Testing Report

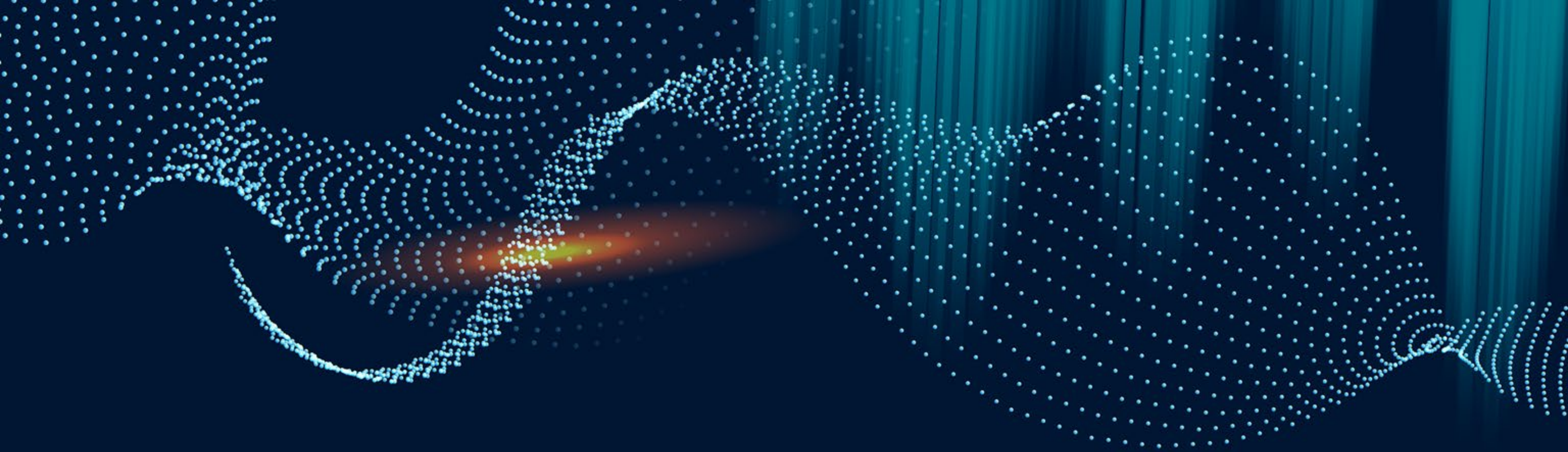
[Anonymized]

UnderDefense

CyberSecurity solutions protecting your business

Penetration Testing Report for Bitcoin Exchange Company

June 2018



UnderDefense | Version 2 www.version-2.com 二版

Thank you for your trust

Hong Kong and Macau
Tel: (852) 2893 8860
Email: sales@version-2.com.hk

Taiwan
Tel: (886) 02 7722 6899
Email: sales@version-2.com.tw

Singapore, Malaysia and SEA
Tel: (65) 6296 4268
Email: sales@version-2.com.sg