Case Study 2019

UNDER DEFENSE

Web Application Penetration Testing

Solution/Service Title	Grey Box Web Application Penetration Testing
Client Industry	Marketing Systems, Customer-Relationship Management Systems provider
Client Overview	International Marketing Service Firm providing winning strategies and execution for industry leaders
Client Challenge	Client data security and Compliance requirements from a very prominent customer were a initial stimul to conduct Application Security testing and build a solid Security Assurance process to mitigate similar issues in the future.
Key Benefits	This Comprehensive Security Assessment allowed our client to strengthen weak spots in their Web Application Security
Results	Overall security posture was improved after remediation from grade F (Inadequate) to A (Excellent) following recommendations provided in our Penetration Testing Report

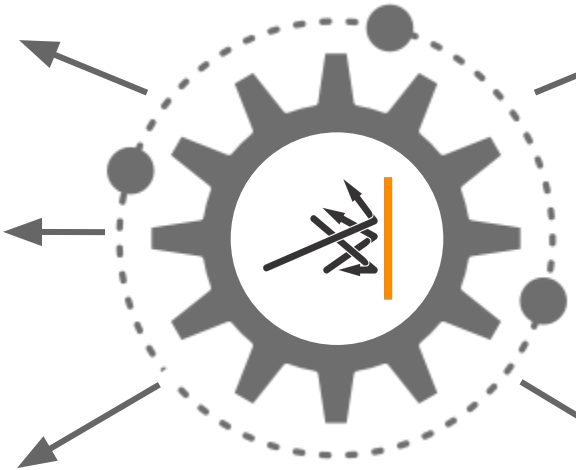
UNDER DEFENSE

Project Overview

Type of Assessment:
Gray Box Penetration Testing

Time Limits:
2 weeks

Team composition:
2 CEH Certified Penetration Testers



Client:
International Marketing Service Company

Target:
Web CRM System

Technology Stack
PHP
Bootstrap
MySQL
Apache HTTP Server

UNDER DEFENSE

Project Challenge

Technical Goals

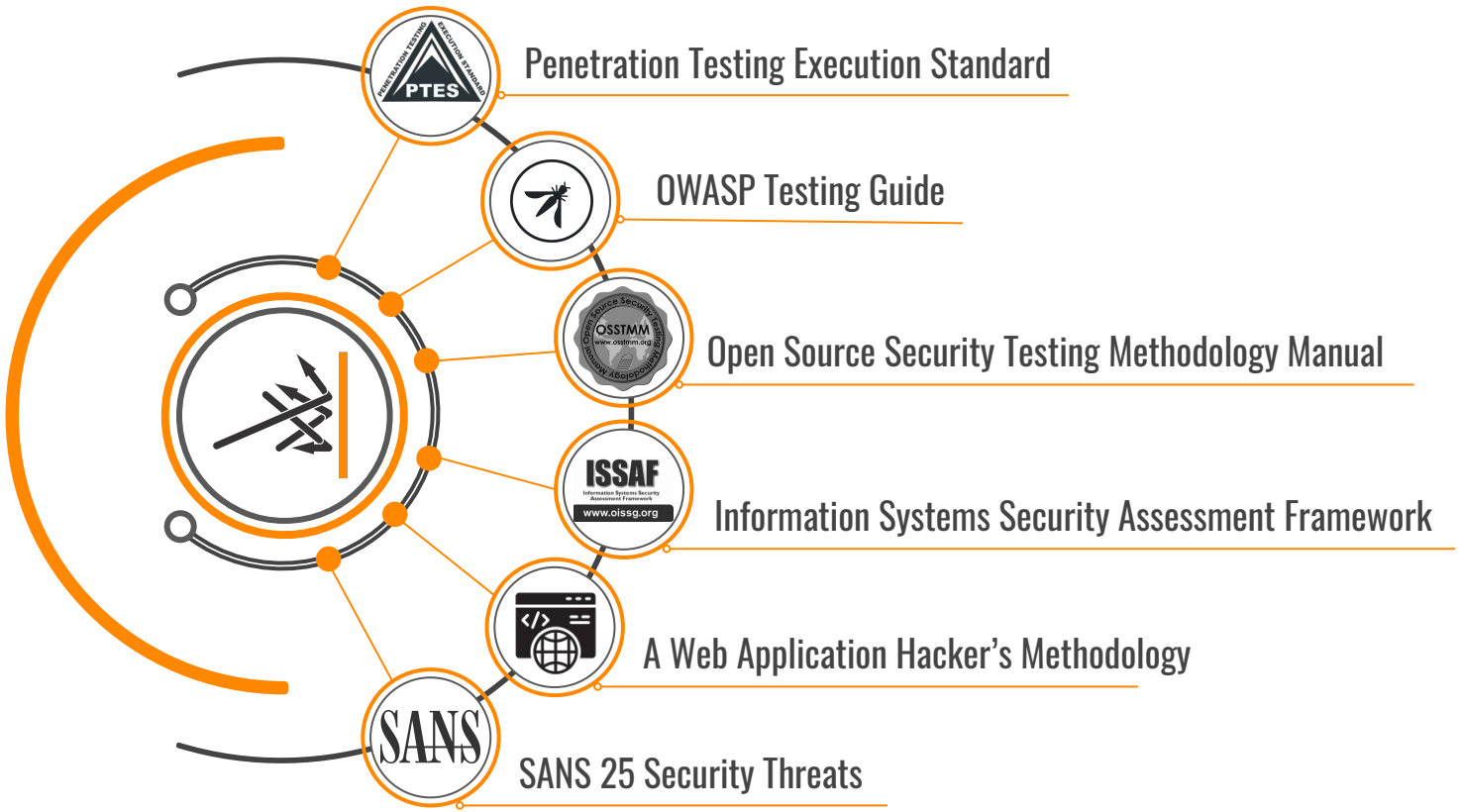
- Test Application with initial access (unprivileged user profile) from attackers' perspective
- Detect and give recommendations on fixing security issues to protect sensitive data, users' money and company reputation

Business Goals

- Evaluate current level of business and platform security
- Identify gaps in current cybersecurity posture and check IT environment for weaknesses
- Provide an accurate evaluation of the security level after remediation phase

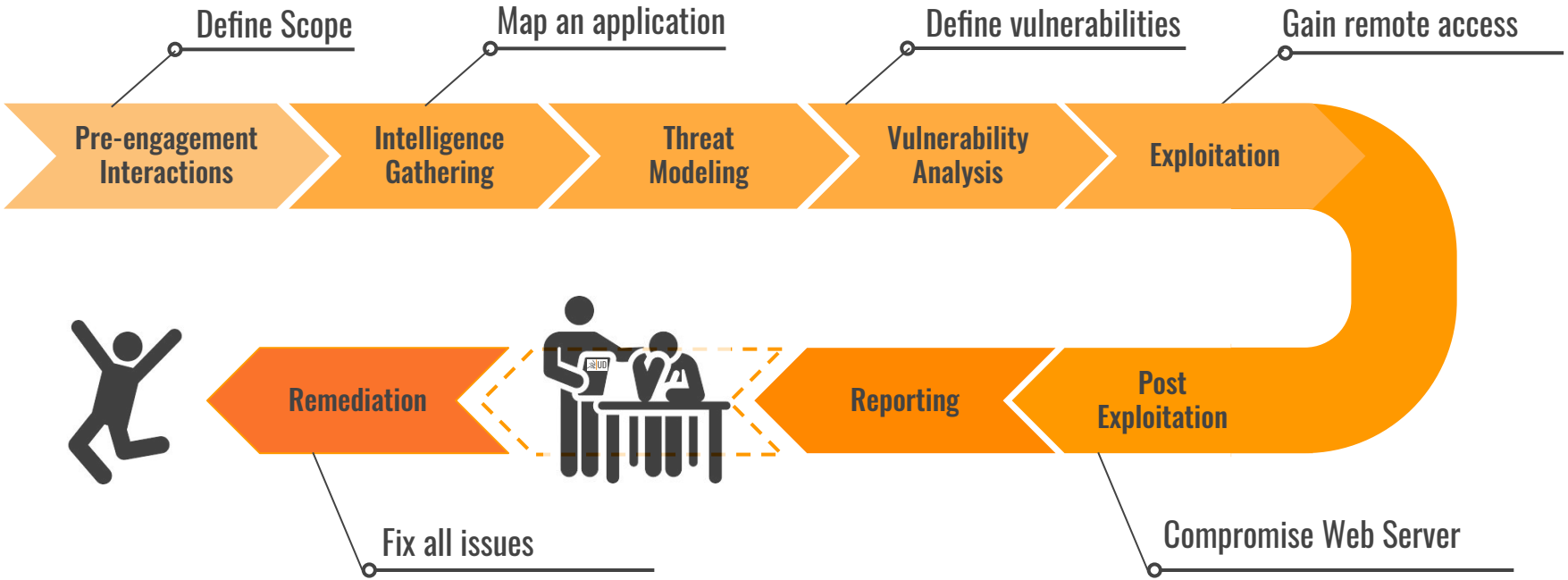
UNDER DEFENSE

Methodologies used for Penetration Testing



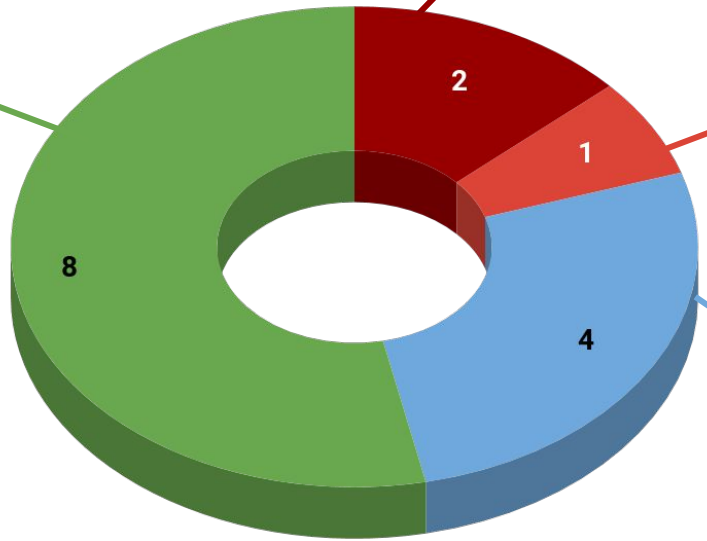
UNDER DEFENSE

Project Planning and Goals



UNDER DEFENSE

Vulnerabilities Found



Critical

- Stored XSS
- IDOR

High

- CSRF

Medium

- Cookie flags
- Reflected XSS
- File upload
- HSTS misconfig

Low

- User Enumeration
- Clickjacking
- Broken Access Control
- Insecure Software
- Outdated Services
- Information Leakage
- phpinfo() page
- Unvalidated redirects

UNDER DEFENSE

Hacking Scenario: getting full access

Attacker...

... gets **User session** utilizing an XSS injection in Contact Form...

... escalates privileges to **Admin role** using IDOR vulnerability...

... escalates privileges to hidden **Developer role** ...

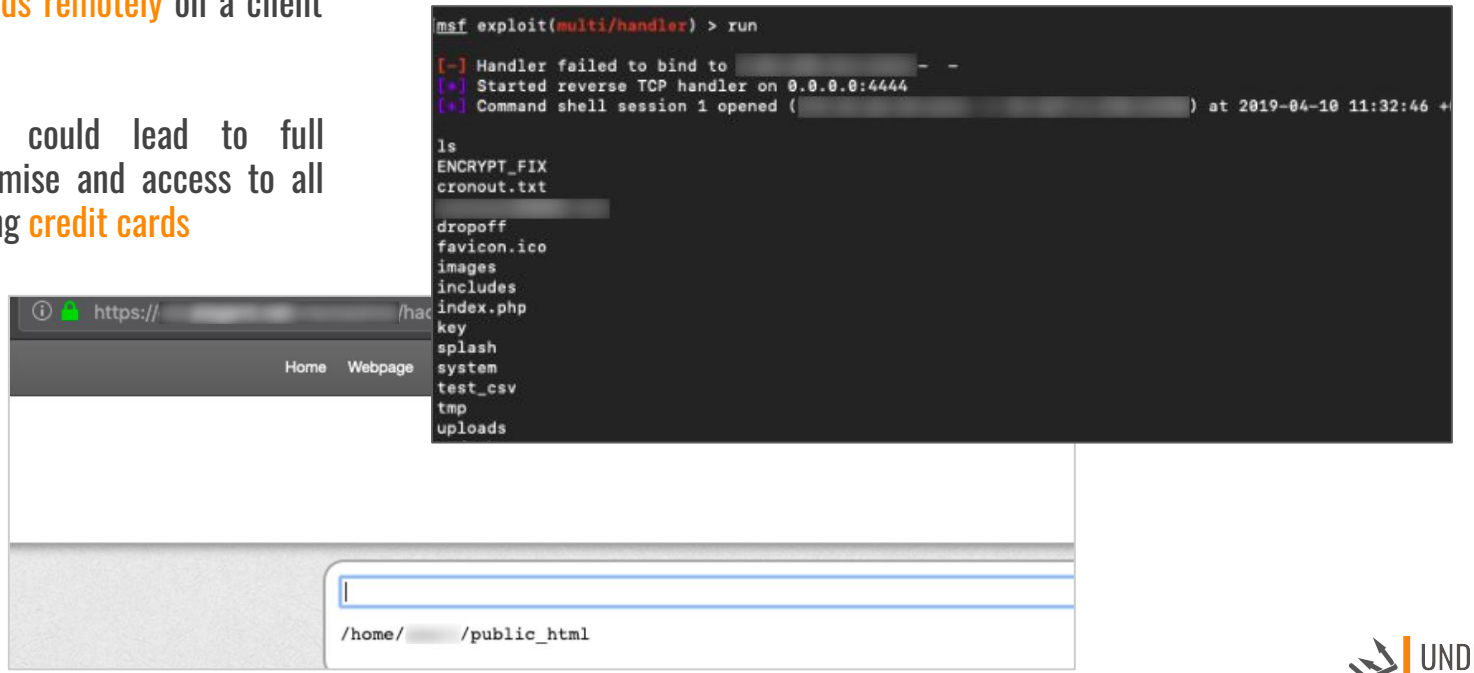
... gains full **control over the system**...

... steals user private data, infects server with malware and sends infected emails

Critical findings: Remote command execution

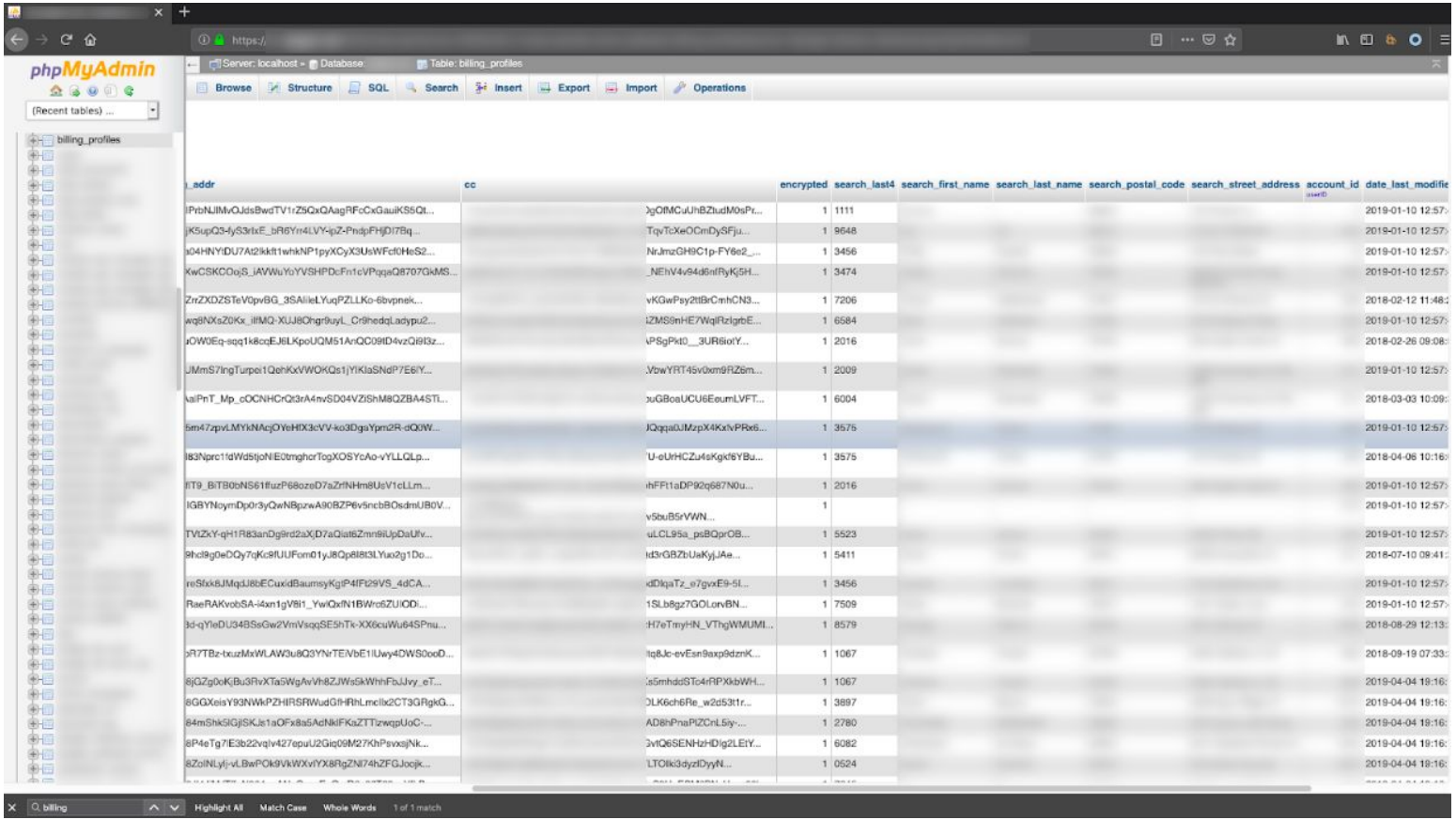
As a result UD security engineers were able to execute commands remotely on a client web-server

Such vulnerability could lead to full application compromise and access to all clients data including credit cards



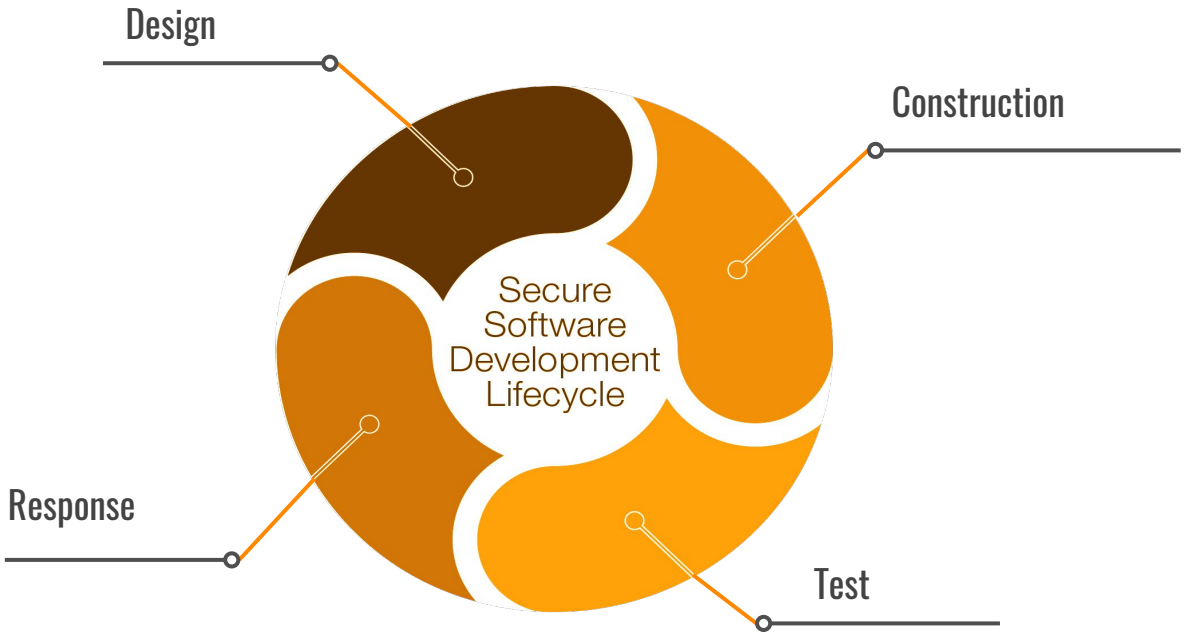
UNDER DEFENSE

Project Artifacts: Client's DB



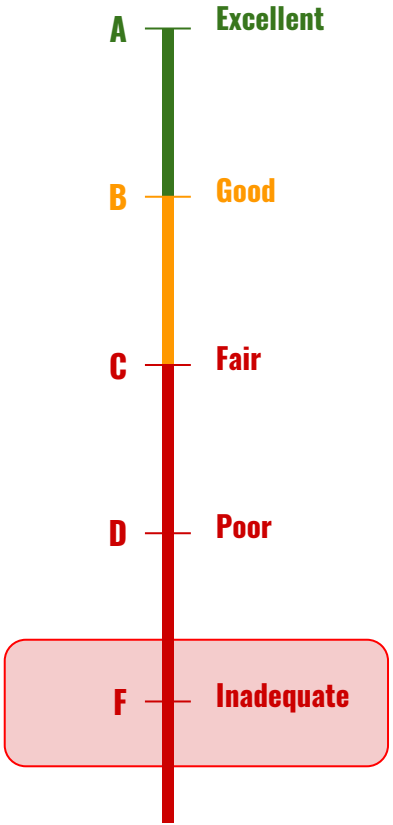
Remediation Phase

At this phase UD security engineers closely worked with clients' developers to immediately mitigate all found vulnerabilities and apply best security practices



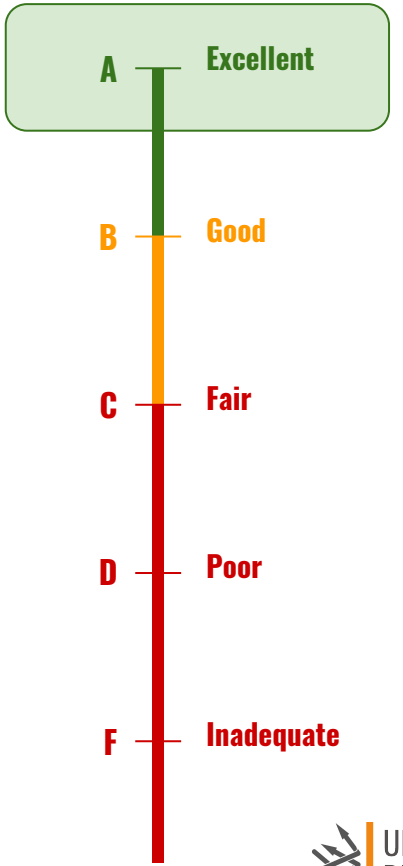
UNDER DEFENSE

Project Results



UnderDefense has delivered a comprehensive report covering all found vulnerabilities and providing recommendations on the best ways of mitigation

At the end our client was able to meet the highest level of compliance and regulation standards, develop better security practices and get a big logo on board assuring board of directors in good security posture.



UNDER DEFENSE

Business risks mitigated

Financial loss

Reputational damage

Loss of clients' trust

Data loss

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

UNDER DEFENSE

Thank you!

Call us now at +1 929 999 5101