

# 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 stimula 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

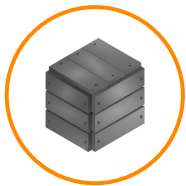
**Results**



Overall security posture was improved after remediation from grade F (Inadequate) to A (Excellent) following recommendations provided in our Penetration Testing Report

# Project Overview

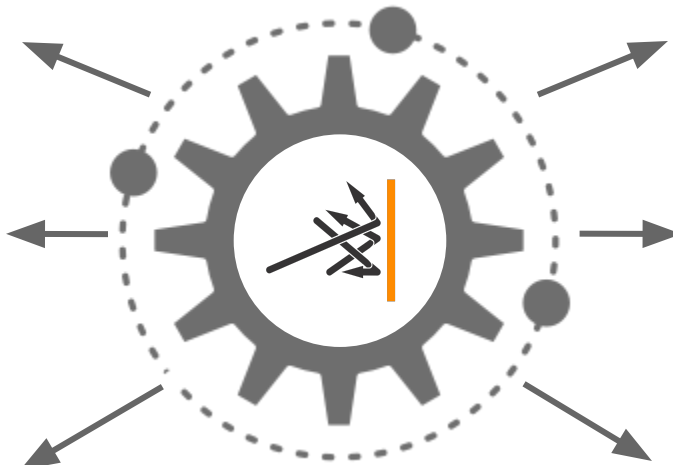
**Type of Assessment:**  
Gray Box Penetration  
Testing



**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

# Project Challenge

## Technical Goals

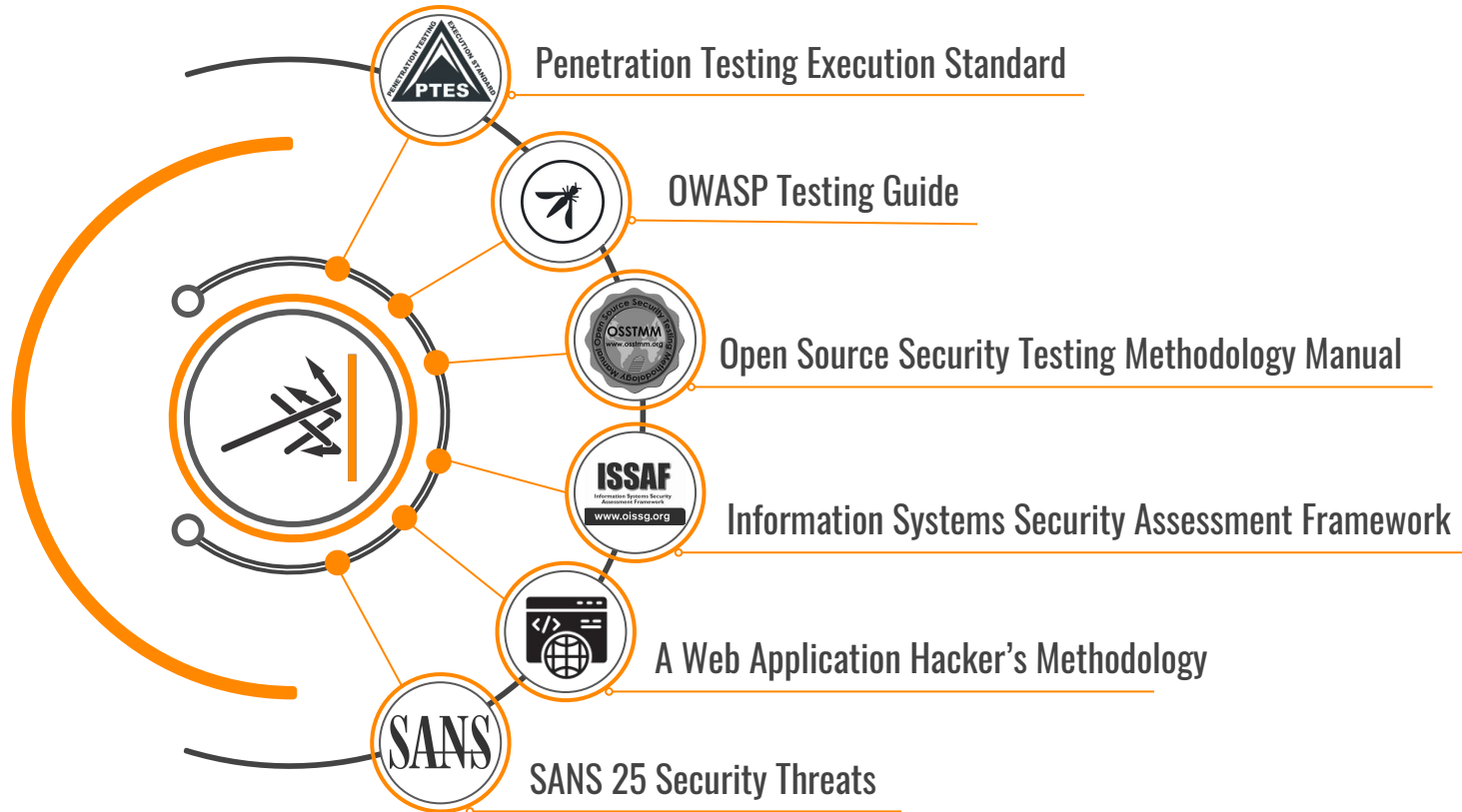
- Test Application with initial access (unprivileged user profile) from attackers' perspective
- Detect and give recommendations on fixing security issues to protect sensitive data, users' money and company reputation



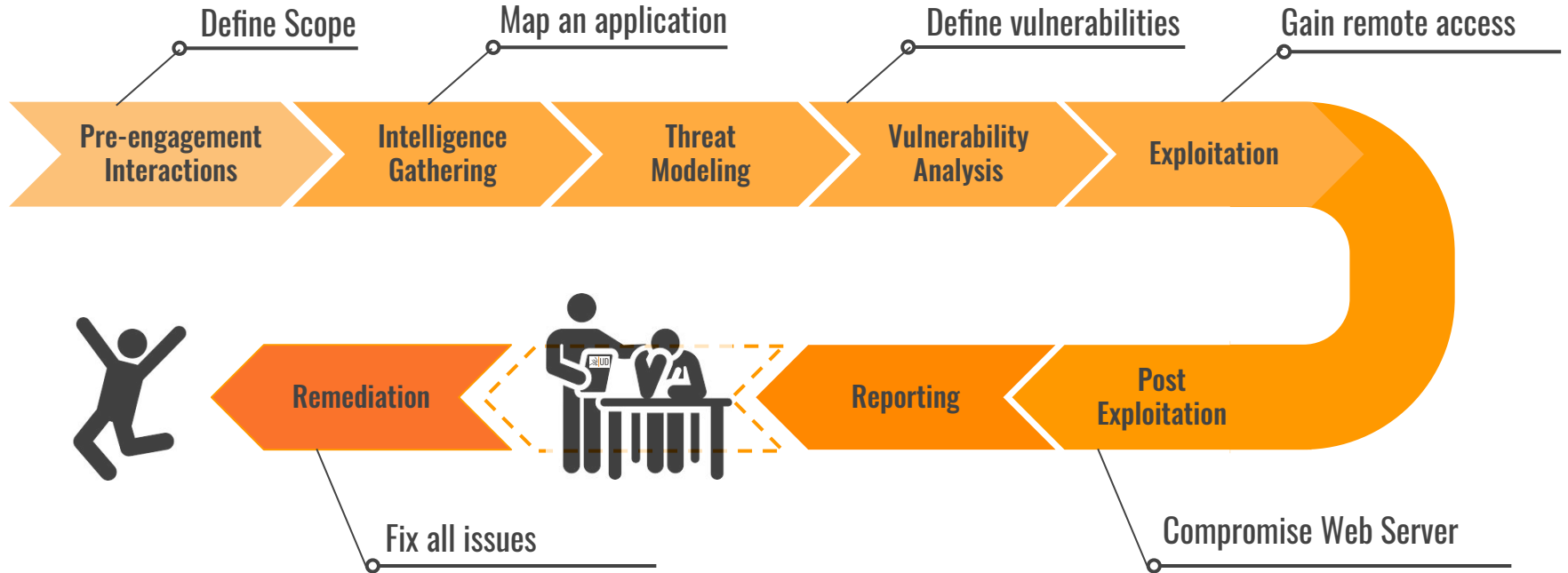
## Business Goals

- 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

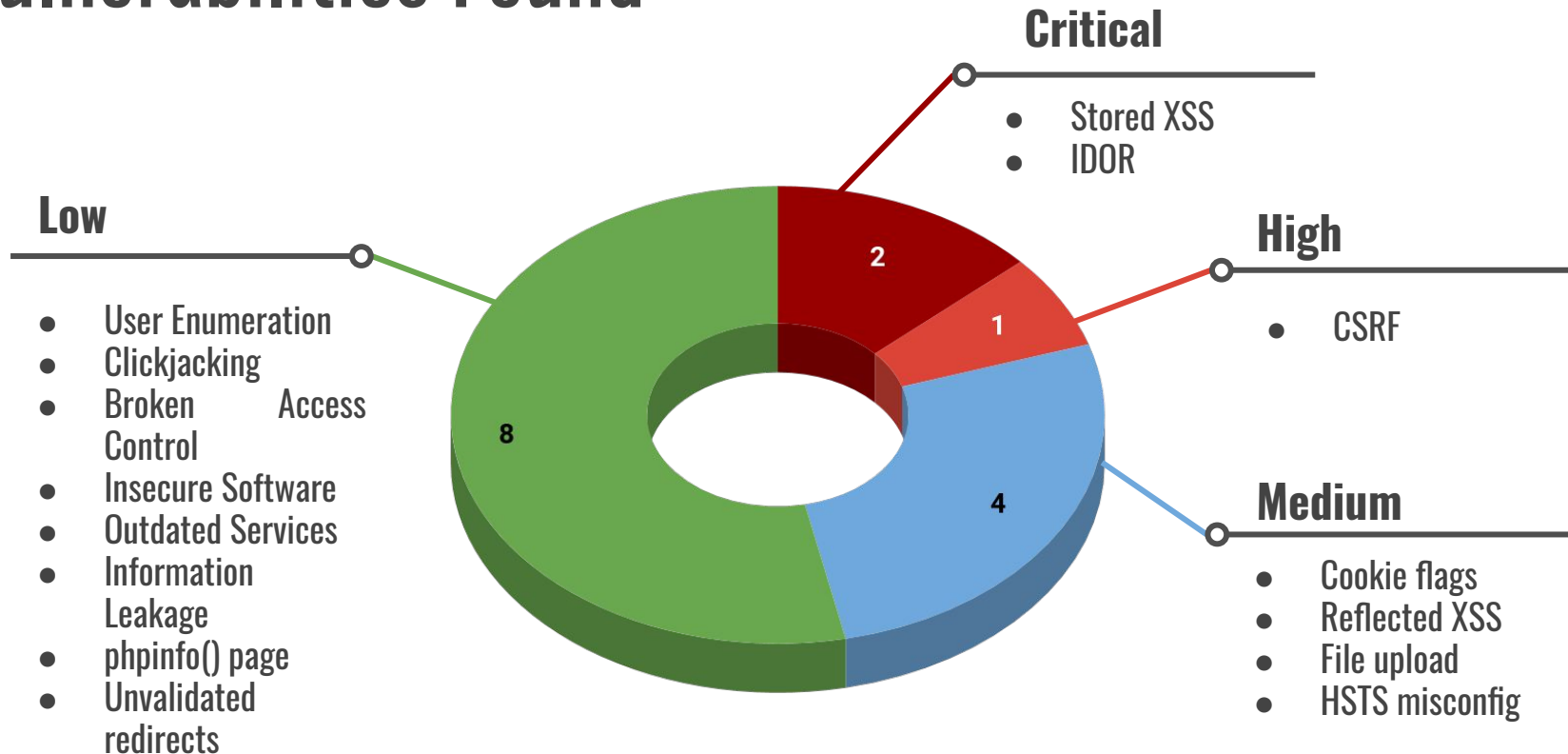
# Methodologies used for Penetration Testing



# Project Planning and Goals



# Vulnerabilities Found



# 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 ...**



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



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

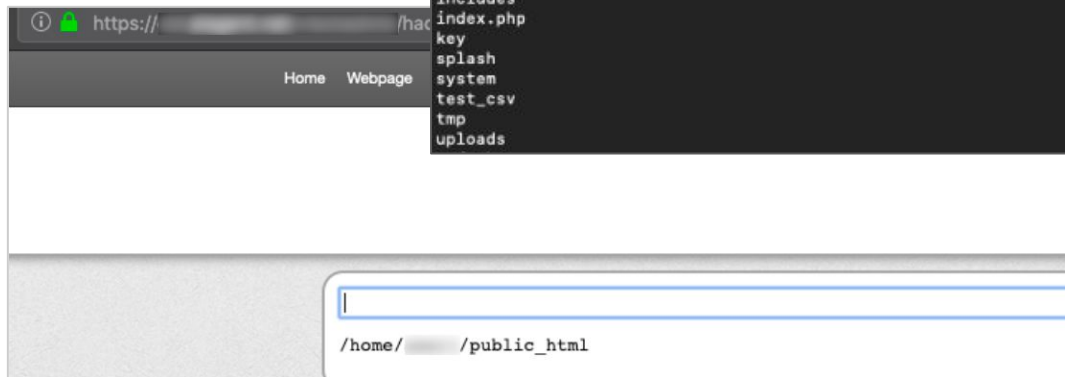




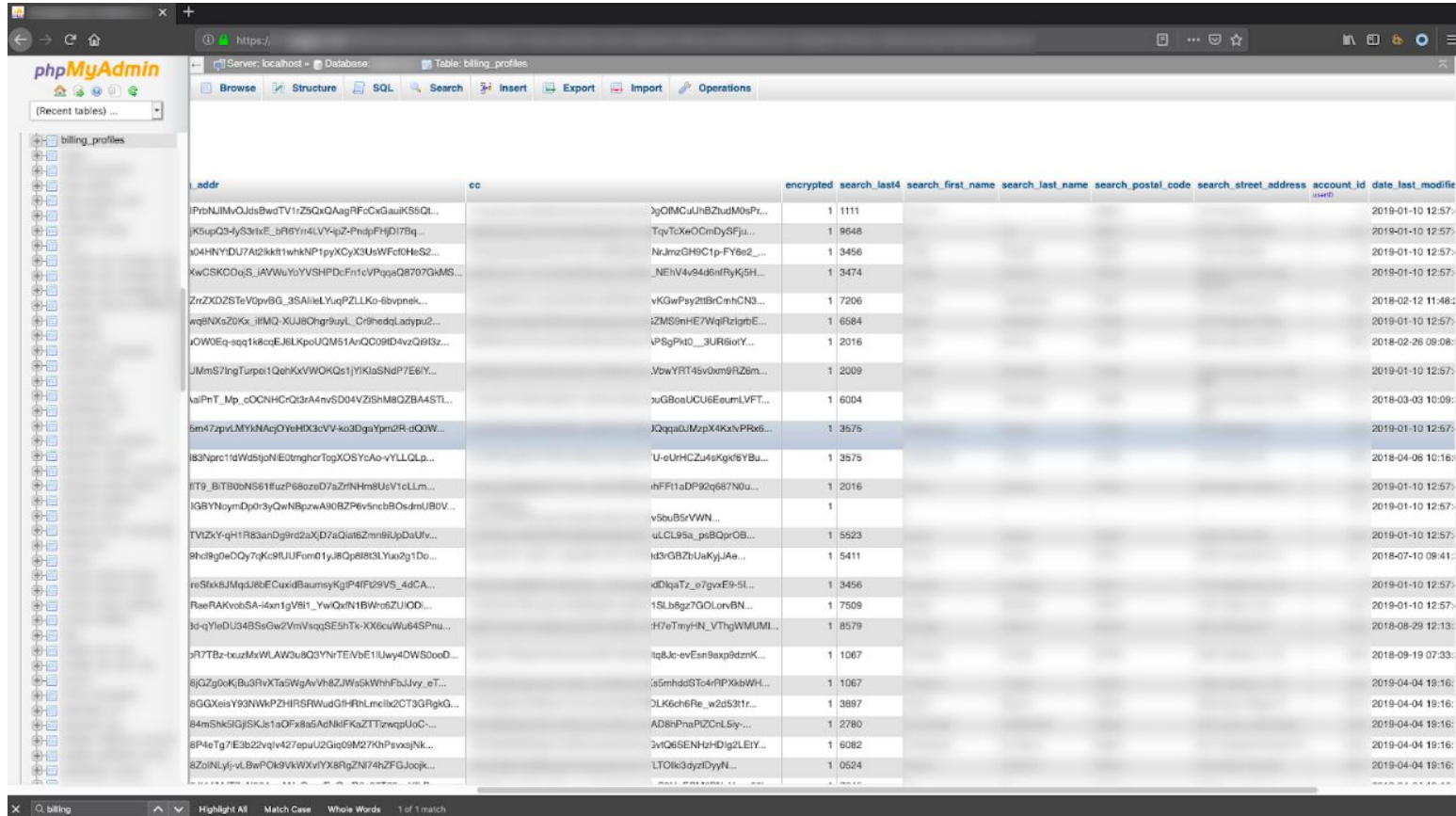
# Critical findings: Remote command execution

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**



# Project Artifacts: Client's DB

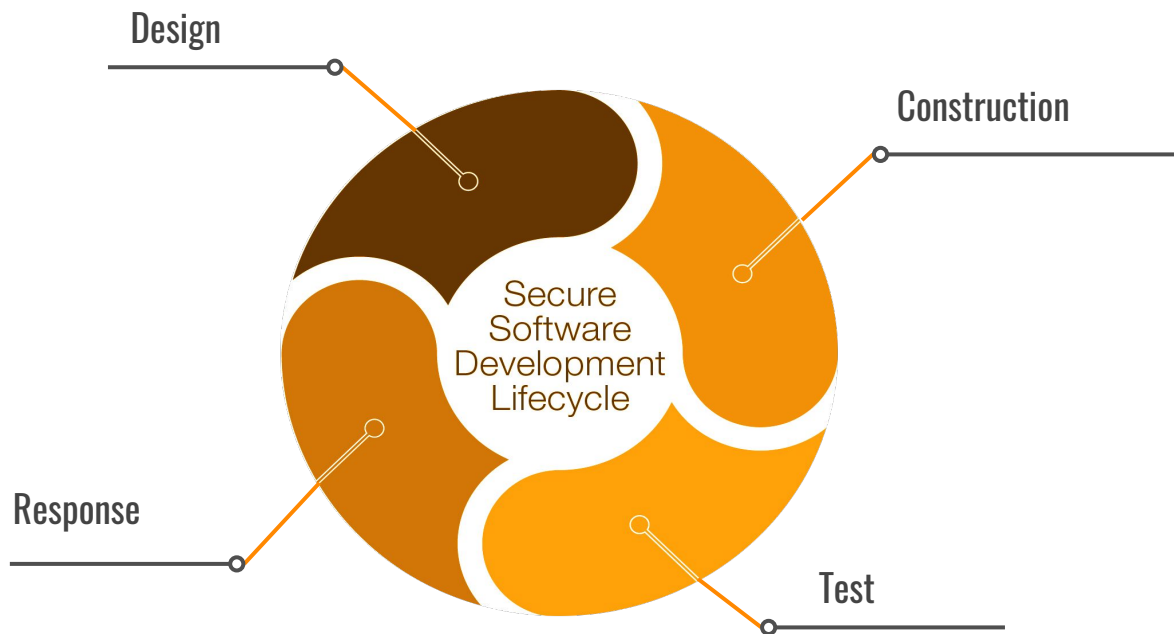


The screenshot shows the phpMyAdmin interface for a database table named 'billing\_profiles'. The table contains 20 rows of data. The columns are: 'id' (user ID), '\_addr', 'cc', 'encrypted', 'search\_last4', 'search\_first\_name', 'search\_last\_name', 'search\_postal\_code', 'search\_street\_address', 'account\_id', and 'date\_last\_modify'. The 'id' column contains values ranging from 1111 to 524. The 'encrypted' column contains values 1 or 0. The 'search\_last4' column contains values like 1111, 9648, 3456, etc. The 'search\_first\_name' and 'search\_last\_name' columns contain names like 'YgOIMCjUjBZludM0sPr...', 'TrqYtXwOCmDySFjU...', etc. The 'search\_postal\_code' column contains values like 1111, 9648, 3456, etc. The 'search\_street\_address' column contains values like 'uLCL9SA\_psBQprOB...', 'h3GBZbUkKjJae...', etc. The 'account\_id' column contains values like 1, 5523, 5411, etc. The 'date\_last\_modify' column contains dates like '2019-01-10 12:57', '2018-02-12 11:48', etc.

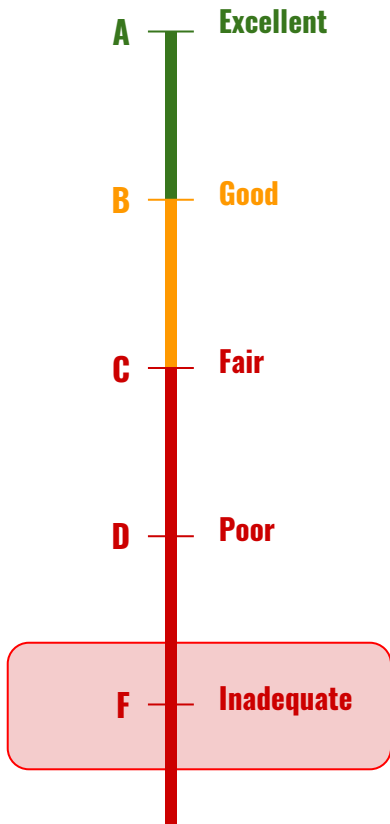
id	_addr	cc	encrypted	search_last4	search_first_name	search_last_name	search_postal_code	search_street_address	account_id	date_last_modify
1111	PrbNlJMvQJds8wdTV1iZ9QxQAagPFcCzGauikS5QL...		1	1111	YgOIMCjUjBZludM0sPr...		1			2019-01-10 12:57
9648	K5upQ34y53rteE_bR6Ym4LVY-qz-PrndjFHjD17Bq...		1	9648	TrqYtXwOCmDySFjU...		1			2019-01-10 12:57
3456	04HNHYDU7A2kfttwhkNP1pyXCyX3UsWfCeHS2...		1	3456	NrJmzGH9C1p-FY6e2...		1			2019-01-10 12:57
3474	kwCSKQDqS_JAVWuYuYVSHPD:Fn1cVPqgsQ870GkMS...		1	3474	_NE1v494d8ntFyK5H...		1			2019-01-10 12:57
7206	ZrZXDZStE0p0v9G_3SAilleYugPZLLK0-6bvpnsk...		1	7206	vKGwPsy2tBrCmhCN3...		1			2018-02-12 11:48
6584	wq8Nz20Kx_illMQ_XUJ8Chgrbuyl_Cr9hedqLadypu2...		1	6584	iZMSmHE7WqRzigrbE...		1			2019-01-10 12:57
2016	0W3Eeq-seq1k8ceEJLkPoUQM51Ar-QC09ID4vzG9l3z...		1	2016	lPSgPk40_3UR6ioY...		1			2018-02-26 09:08
2009	JMmS7lmgTurpe1QehKxVWOKQs1YkIaSNdP7E6iY...		1	2009	.VbwYRT45v0xm9RZ6m...		1			2019-01-10 12:57
6004	alPnT_Mp_cOCNHC-Q3r4r4m5D04VZiShM8QZBA4STL...		1	6004	uGBosUCU6EoumLVFT...		1			2018-03-03 10:09
3575	sm47zpvLMYkNMcqDYeHX3cVv-ko3DgaYpmzR-cQOW...		1	3575	JQqa0UMzpxXAKxvPRe6...		1			2019-01-10 12:57
3575	83Nprc1idW5tjoNE0tmghcrTogXOSYcAo-vYLLGLp...		1	3575	U-gUHCZu4sKgt6YBa...		1			2018-04-06 10:16
2016	IT9_BIT80cNS61fuzP68ozeD7aZrNhm8Uv1cLLm...		1	2016	ihFf1taDP92qs67N0u...		1			2019-01-10 12:57
1	IGBYNoymDp0r3yQwNBpuzwA90BZP6v5nbcB0sdmUB0V...		1	1	y5ouB5VWN...		1			2019-01-10 12:57
5523	TVZkY-qH1R83anDg9rd2aXD7aQaibZmrnsiUpDaUiv...		1	5523	uLCL9SA_psBQprOB...		1			2019-01-10 12:57
5411	9hcI9g0eDQy7qKc8fUJUFormD1yJ8Qp6l83LXu2g1D0...		1	5411	h3GBZbUkKjJae...		1			2018-07-10 08:41
3456	reS5x8JMqJ88EcuixidBaumsyKjgP4fF29V5_4dCA...		1	3456	vDkqzTz_e7gvcE9-5L...		1			2019-01-10 12:57
7509	RaeRAKvobSA-4xm1gV8H1_YwQxN1BW6cZUJOD...		1	7509	1SLb8gz7GOLovBN...		1			2019-01-10 12:57
8579	3d-qYeDlU348S0Gw2VmiVsqgSE5hTc-XX6ouWu645Pnu...		1	8579	:H7eTmyhN_VThgWWMUMI...		1			2018-08-29 12:13
1067	rR7TBz-buzMxWLAw8u9Q3YnTE/vbE1Uuy4DWS0ooD...		1	1067	lq&Jc-evEsn9axp9dzrK...		1			2018-09-19 07:33
1067	8jGZg0eKjBj3rvXTa5WgAvVh8ZjW5aKwhFbUjy_eT...		1	1067	:s5mhdSto4RPXkbWH...		1			2019-04-04 19:16
3897	6GX0eisY93NWwPZHRSRWudGHrHl.mclx2CT9RgkG...		1	3897	DLK6ch6Re_w2d531tr...		1			2019-04-04 19:16
2780	84mShkGjGSKJtaOFx8a5AclNklFKzZT1zwpqUoC...		1	2780	AD8hPnaPZCnL6y...		1			2019-04-04 19:16
6082	8P4eTg7E3b2vqiv427epuU2Giq09M27KhPvoojNk...		1	6082	3vtQ6SEENhzhDlgl2LEIY...		1			2019-04-04 19:16
0524	8Z0nLlyf-vLbwPOK9VwXxviYX8RgZn74ZFGJocjk...		1	0524	LTC0k3dyzDjyN...		1			2019-04-04 19:16

# Remediation Phase

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

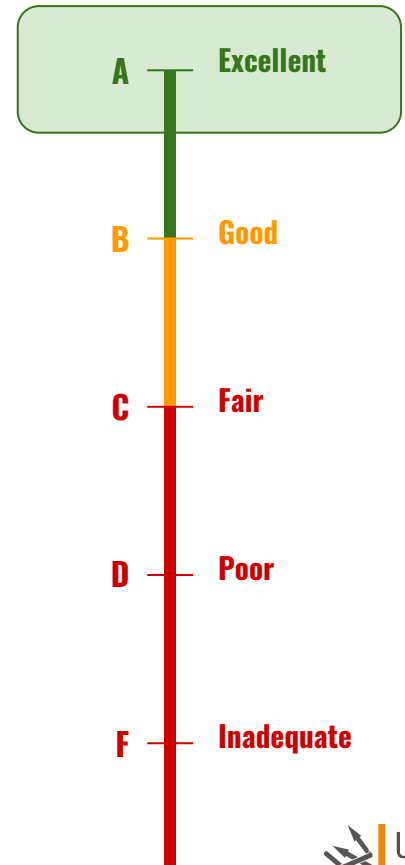


# Project Results

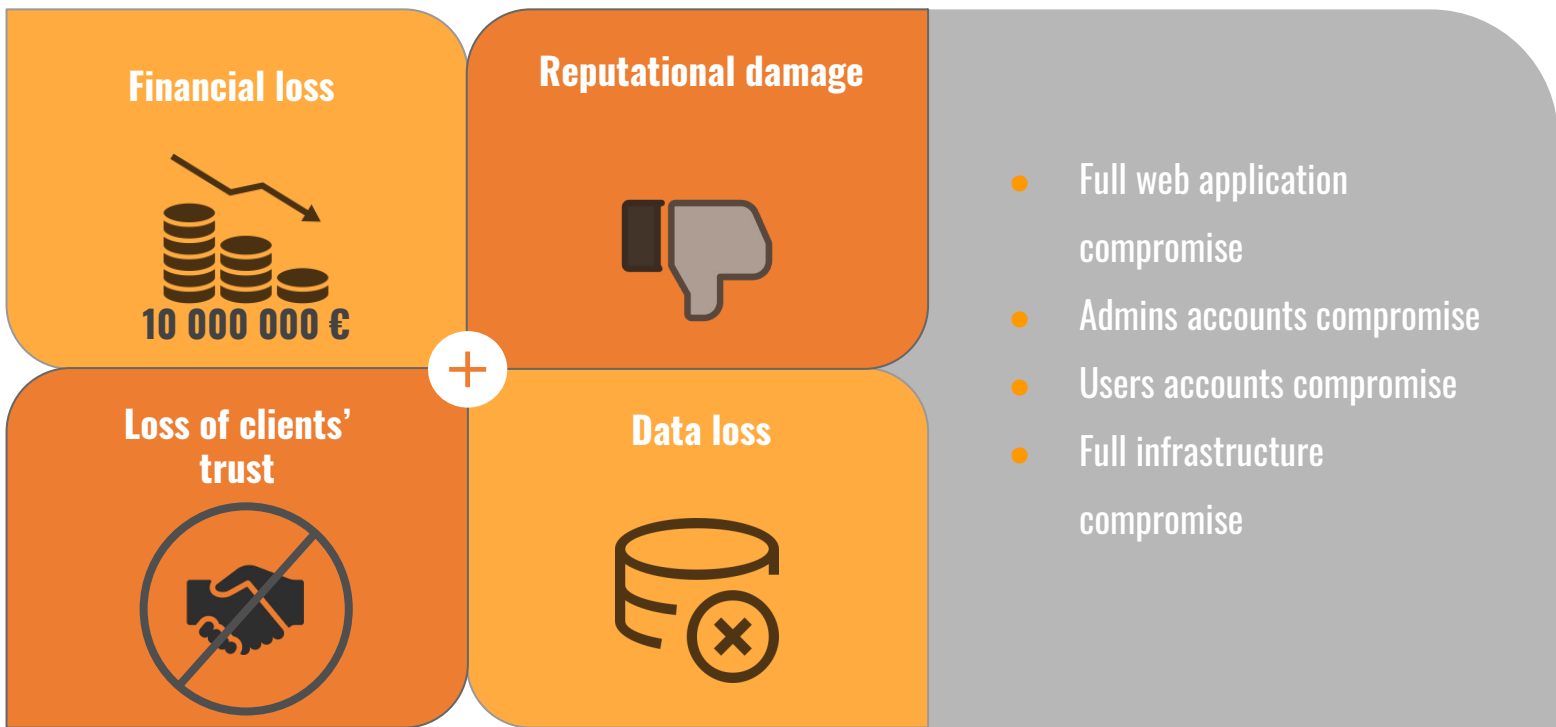


**UnderDefense** has delivered a comprehensive report covering all found vulnerabilities and providing recommendations on the best ways of mitigation

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.



# Business risks mitigated





# Thank you!

 **Version 2** | 二版  
www.version-2.com  
Hong Kong | Taiwan | Singapore | Macau | Mainland China

**Hong Kong & 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 & SEA**

Tel : (65) 6296 4268  
Email : sales@version-2.com.sg