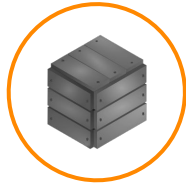


# Web Application Penetration Testing

|                               |   |   |
|-------------------------------|---|---|
| <b>Solution/Service Title</b> |   | Grey Box Web Application Penetration Testing  |
| <b>Client Industry</b>        |  | Marketing Systems, Customer-Relationship Management Systems provider  |
| <b>Client Overview</b>        |  | International Marketing Service Firm providing winning strategies and execution for industry leaders  |
| <b>Client Challenge</b>       |  | 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. |
| <b>Key Benefits</b>           |  | This Comprehensive Security Assessment allowed our client to strengthen weak spots in their Web Application Security  |
| <b>Results</b>                |  | Overall security posture was improved after remediation from grade F (Inadequate) to A (Excellent) following recommendations provided in our Penetration Testing Report   |

# Project Overview

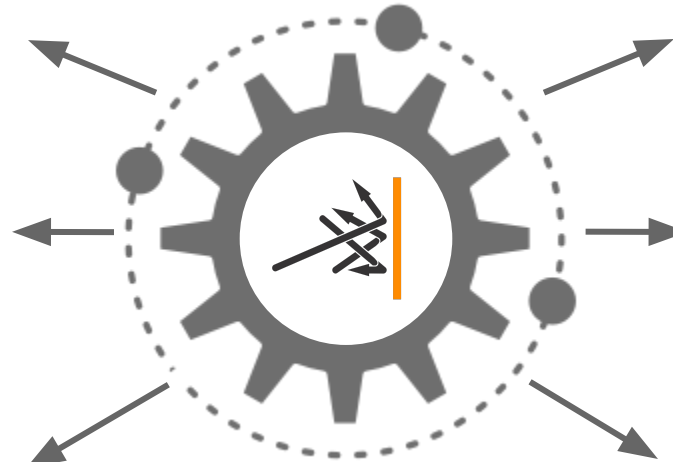
**Type of Assessment:**  
Gray Box Penetration  
Testing



**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

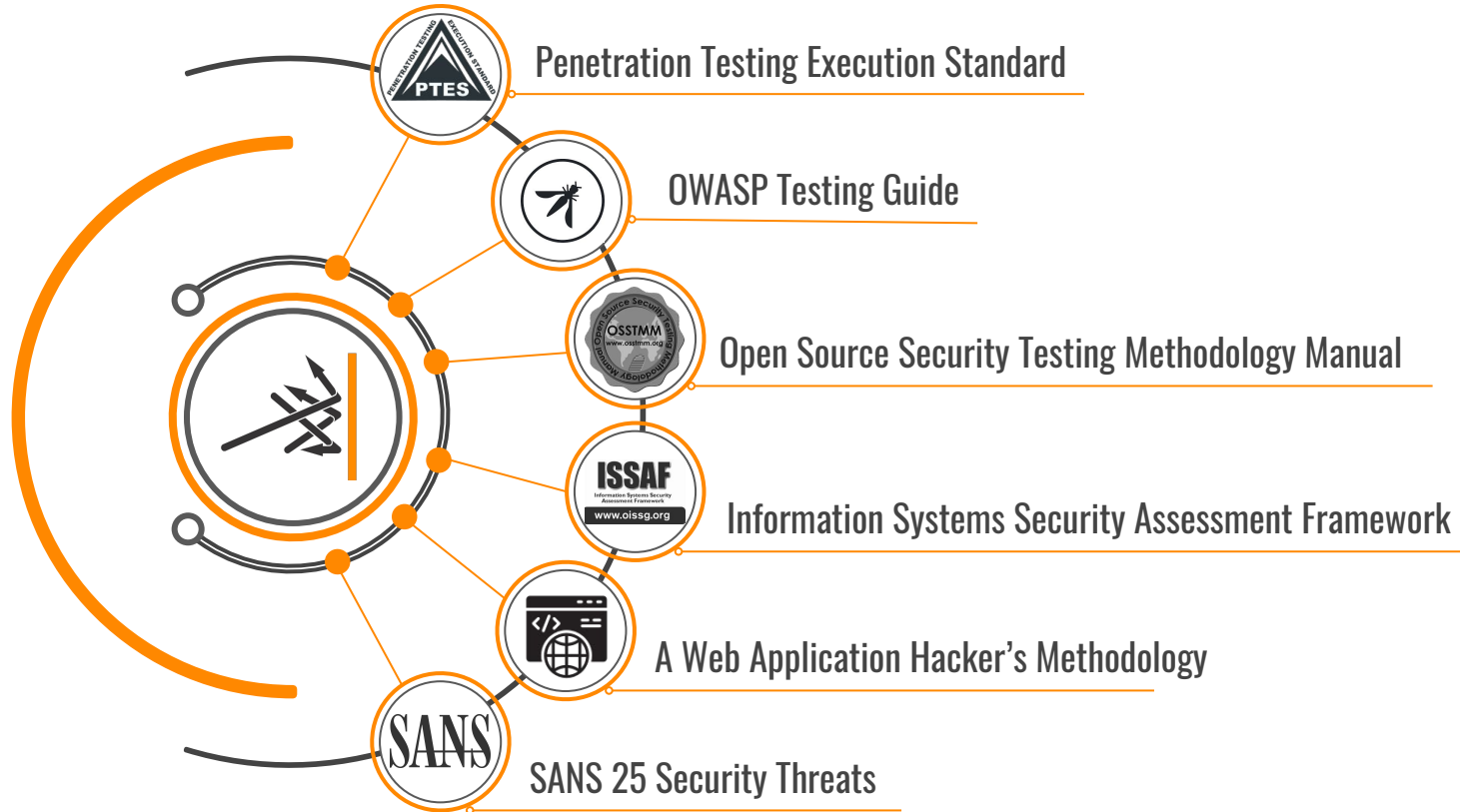
- Test Application with initial access (unprivileged user profile) from attackers' perspective
- Detect and give recommendations on fixing security issues to protect sensitive data, users' money and company reputation



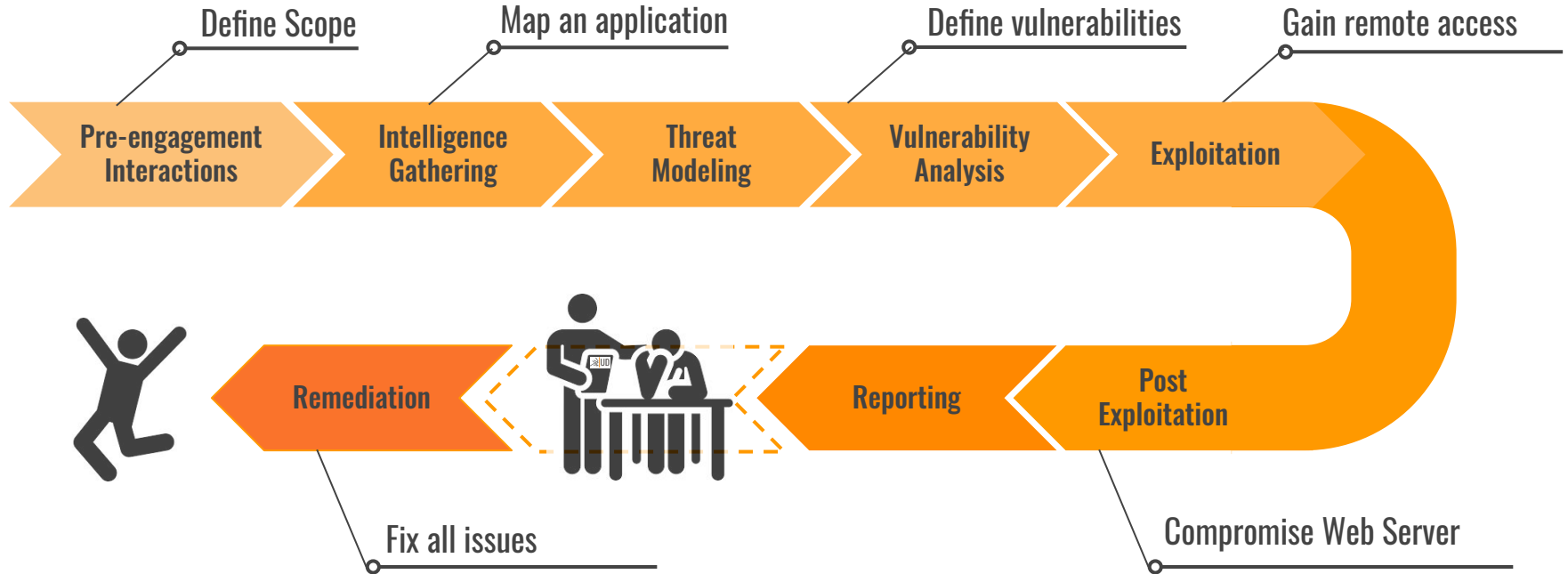
## Business Goals

- 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

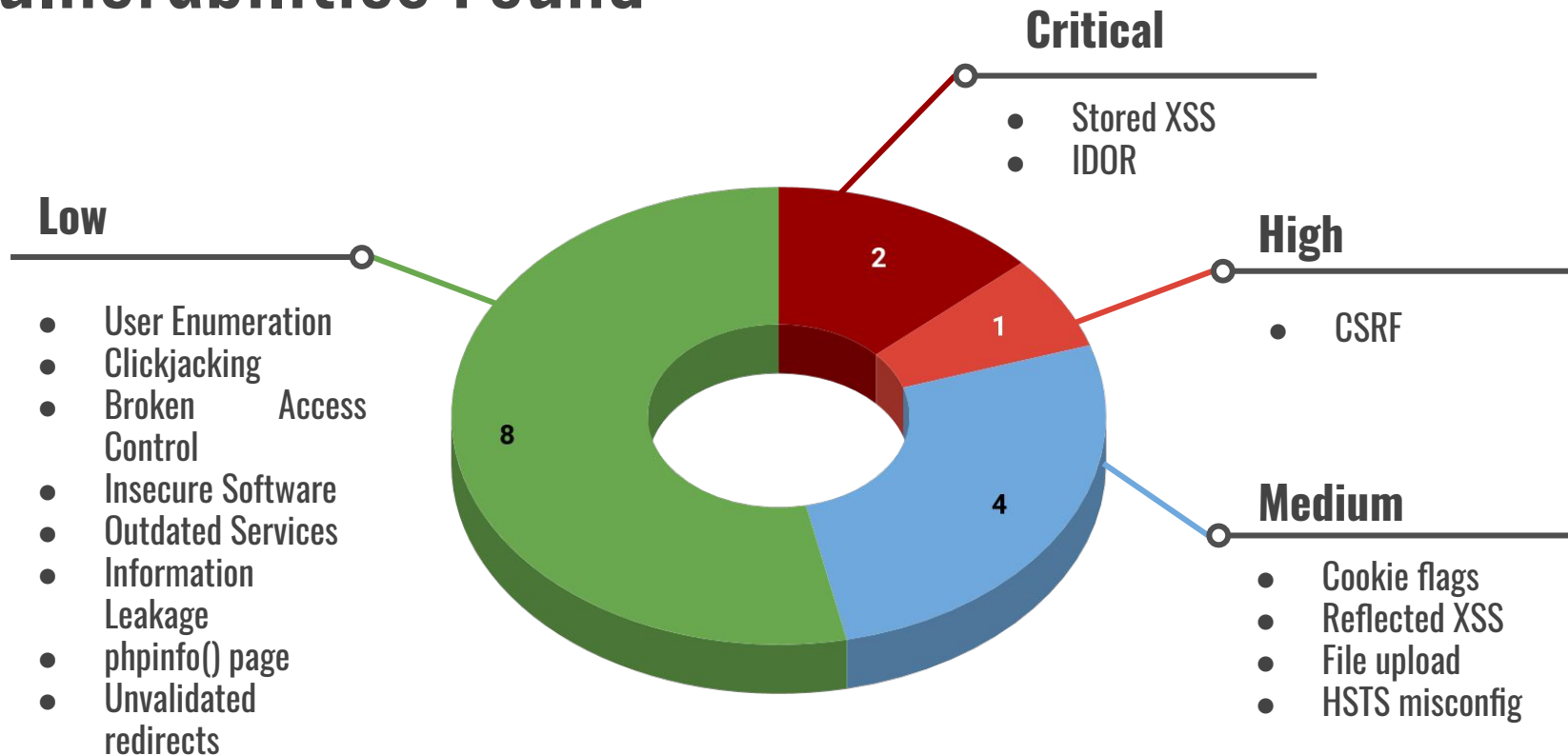
# Methodologies used for Penetration Testing



# 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...**

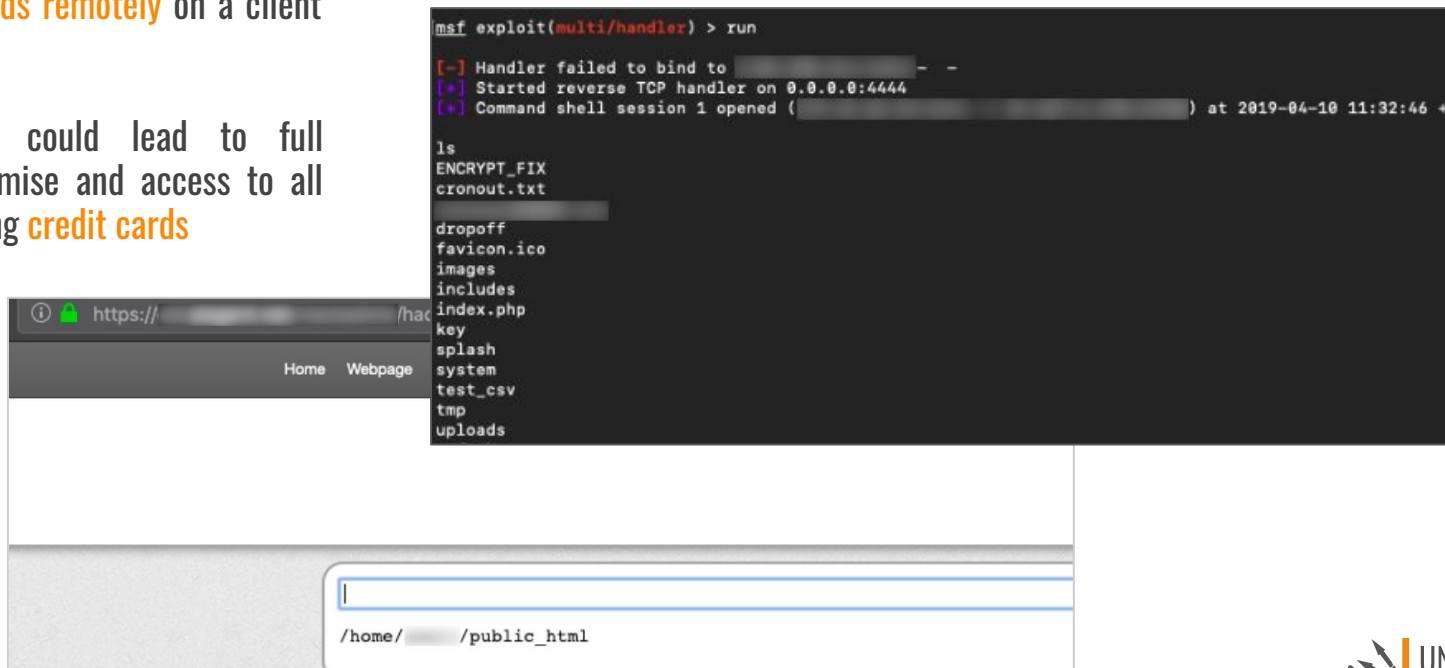




# Critical findings: Remote command execution

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

phpMyAdmin

Server: localhost • Database: • Table: billing\_profiles

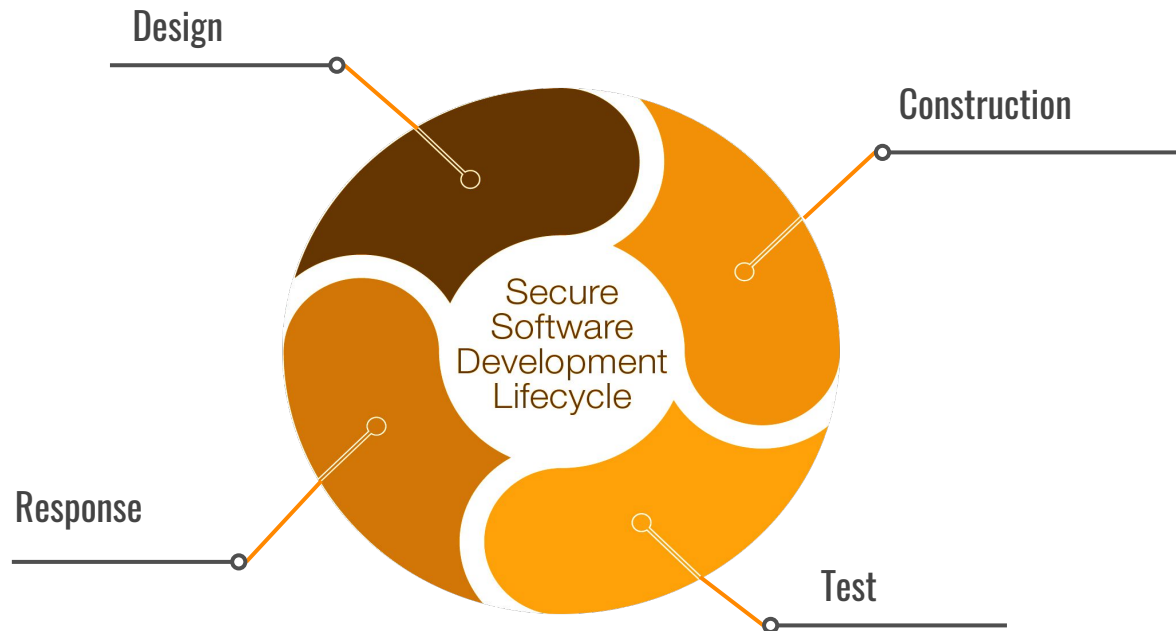
Table: billing\_profiles

| _addr  | cc | encrypted             | search_last4 | search_first_name | search_last_name | search_postal_code | search_street_address | account_id | date_last_modified |
|--|----|-----------------------|--------------|-------------------|------------------|--------------------|-----------------------|------------|--------------------|
| PrtNlUMvQJds8wdTV1tZ5QxQAagPFcCxAuK55Ql...     |    | YgOMCujhBZludMoaPr... | 1 1111       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| K5upQ34yS3rlxL_Er6Ym4LVY-qz-PndpFHjD7Bq...     |    | TqYtXwOCmDySFju...    | 1 9648       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| q04HNHYDU7A2lkkft1whkNP1pyXCyX3UsWfCtHeS2...   |    | NrJmzGH9C1pFY6e2...   | 1 3456       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| KwCSKCDQoS_JAVWuYoYVSHFDcFn1cVPggsQ8707GkMS... |    | _NEhV4v94d6ntRyK5H... | 1 3474       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| ZnrZXDZ5TeV0pvr6G_35AilLkYugPZLLKo-6bvpnsk...  |    | vKQwPsy2tBrcmHCN3...  | 1 7206       |                   |                  |                    |                       |            | 2018-02-12 11:48   |
| wqgNXsZ0Kx_iIMQ_XUJ8OhgrhuyL_CrIhedqLadypu2... |    | LZMSmHE7WqRizgrbE...  | 1 6584       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| vOW3Eq-seq1k8ccEJELKpoUQM51ArQO9d4vzG6l3z...   |    | VPsgPk40_3UR6ioY...   | 1 2016       |                   |                  |                    |                       |            | 2018-02-26 08:08   |
| JMmS7IngTurpe1QehKxVWOKQs1YKlASnDP7E6iY...     |    | JbwYRT45vOxm9RZ6m...  | 1 2009       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| alPnT_Mp_cOCNHCrQ3rA4nvSD04VZShM8QZBA4STL...   |    | uGBosUCU6EoumLVFT...  | 1 6004       |                   |                  |                    |                       |            | 2018-03-03 10:09   |
| 5m47zpvLMYKMcQOYeHIX3cVV-ko3DgaYpnc2R-cQOW...  |    | JQqa0UMzpxYKXvPR6...  | 1 3575       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| 83Nprc1tWd5tj0NE0tmghcrTogXOSYcAo-vYLLGLp...   |    | U-sUHCZu4sKgKt6YBa... | 1 3575       |                   |                  |                    |                       |            | 2018-04-06 10:16   |
| IT9_BtB0cN561fuzP68ozeD7aZmNhm8UeV1cLm...      |    | rhFR1tDP92q687Nou...  | 1 2016       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| IGBYNymDp0r3yQwNBpuzwA90BZP6vncbB0sdmUB0V...   |    | y5ouB5VWN...          | 1            |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| TVZxqYH1R83anDg9rd2aXD7aQut6Zmn6iUpDaUiv...    |    | uLCL9A_psBQprOB...    | 1 5523       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| rhcl9gheDO7q7K8fUUFomd1yJ8Qp6l83Lyu2g1Dc...    |    | ld3GBZbUeKylJae...    | 1 5411       |                   |                  |                    |                       |            | 2018-07-10 08:41   |
| reS5xbJMqJ8bECuxidBaumsyKjP4fF29VS_4dCA...     |    | dDlqaTz_e7gvcE9-5L... | 1 3456       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| RaeRAKvobSA-4xm1gV8H1_YwQxN1BWh6ZUQD...        |    | 1SLb8gz7GOLovBN...    | 1 7509       |                   |                  |                    |                       |            | 2019-01-10 12:57   |
| 3d-qYleDU34B5Gw2VmVsqqSE5hTc-XO6ouWu64SPnu...  |    | H7eTmyhN_VThgWMUMI... | 1 8579       |                   |                  |                    |                       |            | 2018-08-29 12:13   |
| rR7TBz-buzMxWLAw3u9Q3YNTEVbE1Uv4yDWS0ooD...    |    | h9LJc-evEsn9expdzK... | 1 1067       |                   |                  |                    |                       |            | 2018-09-19 07:33   |
| 8jGZg0KqBj3RvXTa5WgAvVh8ZJw5sWhnFbUjy_eT...    |    | z5mhdcSt04RPXbBWH...  | 1 1067       |                   |                  |                    |                       |            | 2019-04-04 19:16   |
| 8GQXeisY93NWkPZHRSRWudGHfRhlMclb2CT3GRgkG...   |    | 2LK6ch6RE_w2d531tr... | 1 3897       |                   |                  |                    |                       |            | 2019-04-04 19:16   |
| 84mShkGjGjSKJe1aOFx8a5AclNkIFKsZTTzwpqUoC...   |    | ADbPnaPZCnL6y...      | 1 2780       |                   |                  |                    |                       |            | 2019-04-04 19:16   |
| qP4eTg7E3b2vq4v427epuU2Gic09M27KhPvnxgNk...    |    | 2vQ6SENhzbDlgl2EiY... | 1 6082       |                   |                  |                    |                       |            | 2019-04-04 19:16   |
| 8ZolNlyf-vLBwPQ9VkvWxviYX8RgZn74hZFGJocjk...   |    | LTOlk3dyzdlYpN...     | 1 0524       |                   |                  |                    |                       |            | 2019-04-04 19:16   |

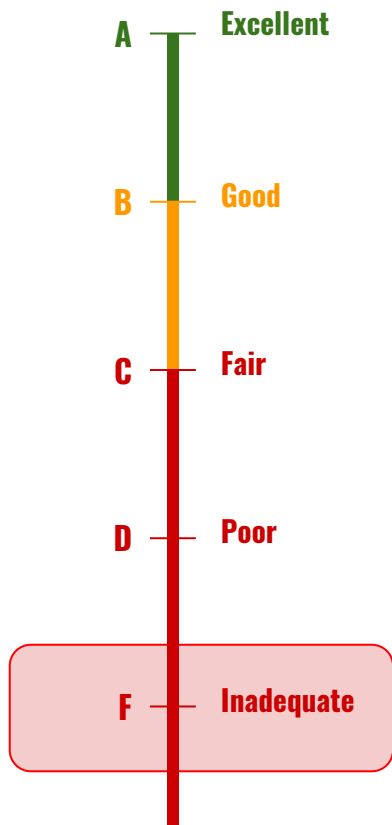
Q billing Highlight All Match Case Whole Words 1 of 1 match

# Remediation Phase

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

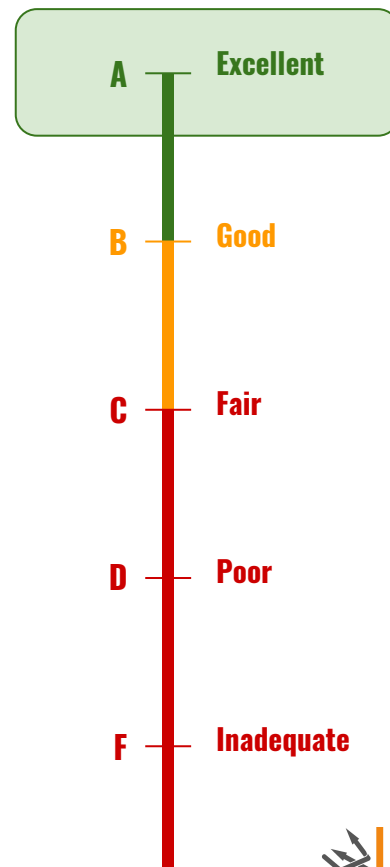


# Project Results

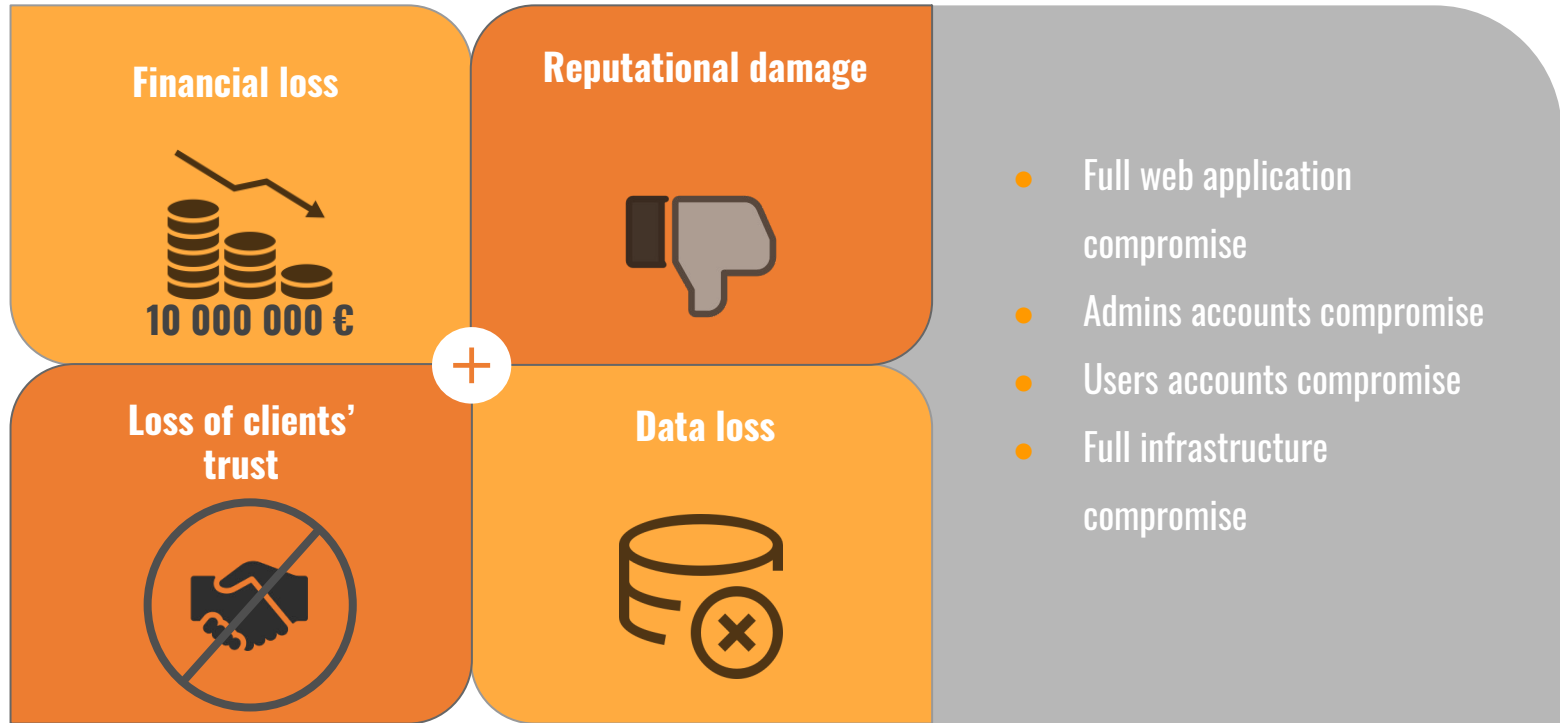


**UnderDefense** has delivered a comprehensive report covering all found vulnerabilities and providing recommendations on the best ways of mitigation

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!

Call us now at +1 929 999 5101