PENETRATION TEST

REPORT TEMPLATE

By Hoek from 0ut3r.space

**SCOPE**

Web application <APP\_NAME>

**DATE**

<START\_DATE> – <END\_DATE>

**RETEST DATE**

<RETEST\_DATE>

**AUDITORS**

<AUDITOR\_NAME>

**DOCUMENT VERSION**

<DOCUMENT\_VERSION>

# CONTENTS

[CONTENTS 2](#_Toc125807414)

[CHANGE HISTORY 3](#_Toc125807415)

[CONFIDENTIALITY NOTICE 4](#_Toc125807416)

[EXECUTIVE SUMMARY 5](#_Toc125807417)

[Scope and assumptions 5](#_Toc125807418)

[Vulnerabilities’ risk classification 6](#_Toc125807419)

[Statical overview of vulnerabilities in web application 6](#_Toc125807420)

[Most sever vulnerabilities identified 7](#_Toc125807421)

[WEB APPLICATION VULNERABILITIES 8](#_Toc125807422)

[[CRITICAL] <CRITICAL\_TITLE\_VULNERABILITY> 8](#_Toc125807423)

[[HIGH] <HIGH\_TITLE\_VULNERABILITY> 9](#_Toc125807424)

[[MEDIUM] <MEDIUM\_TITLE\_VULNERABILITY> 10](#_Toc125807425)

[[LOW] <LOW\_TITLE\_ VULNERABILITY > 11](#_Toc125807426)

[[INFO] <INFO\_TITLE\_RECOMMENDATION> 12](#_Toc125807427)

# CHANGE HISTORY

|  |  |  |
| --- | --- | --- |
| Version | Document Date | Change description |
| 0.1 | <HISTORY\_DATE> | The initial version (draft). |
| 0.2 | <HISTORY\_DATE> | Vulnerabilities added |
| 1.0 | <HISTORY\_DATE> | Updated and reviewed version. |

# 

# CONFIDENTIALITY NOTICE

This report contains sensitive, privileged, and confidential information. Precautions should be taken to protect the confidentiality of the information in this document. Publication of this report may cause reputational damage or facilitate attacks against to the company. Auditors team shall not be held liable for special, incidental, collateral or consequential damages arising out of the use of this information.

# 

# EXECUTIVE SUMMARY

This document is a summary of work conducted by 0ut3r.space auditors. The subject of the test was a web application: <WEB\_APP\_NAME>

Report is the results of audit carried out in the best-effort method within <BUSINESS\_DAYS> business days. The carried-out internal audit does not guarantee or constitute a security certificate of system safety which is the results of the scope and mode of conducted works.

The tests of the application were carried out with the following privilege levels: <PRIVILEGES>

During the tests, particular emphasis was placed on vulnerabilities that might affect confidentiality, integrity, or availability of processed data in a negative way.

The security tests were carried out in accordance with generally accepted methodologies, including: OWASP, NIST and PTES as well as internal good practices of conducting security tests developed by 0ut3r.space auditors.

As a part of the testing, an approach based on manual tests (using the above-mentioned methodologies) was used, supported by a number of automatic tools, i.a. Burp Suite Professional, DirBuster, Nikto, ffuf, wfuzz wafw00f, wapiti, SkipFish etc.

The vulnerabilities are described in detail in further parts of the report.

## Scope and assumptions

The test was executed with the following assumptions in mind:

* The amount of work is fixed to maximum <MAND\_DAYS>MD (Man Days),
* Test is executed <TIMEFRAMES\_DUIRING\_DAY>,
* The main focus of the test is to <MAIN\_GOLAS>,
* The test type is <TEST\_TYPE>,
* The test focuses on <RISK\_CLASSIFICATION> security issues,
* Only vulnerability assessment, no exploitation,
* Dictionary attack <DICTIONARY\_ATTACK>,

Test exclusions:

* Social engineering
* Backend
* Another user role than customer

## Vulnerabilities’ risk classification

Vulnerabilities are classified on a five-point scale reflecting both the probability of exploitation and the business impact of the exploitation. A short description of each severity level is presented below.

* **CRITICAL**  – exploitation of the vulnerability allows to compromise the server or network device or allows to access (in read and/or write mode) high-value data. The exploitation is usually straightforward. Vulnerabilities marked CRITICAL must be fixed without delay, especially if they occur in a production environment.
* **HIGH**  – exploitation of the vulnerability makes it possible to access high-value data (similar to CRITICAL level), however, the prerequisites for the attack (e.g. requirement for having a user account in an internal system) makes it slightly less likely. Alternatively: vulnerability is easy to exploit but the negative effects are somehow limited.
* **MEDIUM**  – exploitation of the vulnerability might depend on external factors (e.g. convincing the user to click on a hyperlink) or other conditions that are difficult to achieve. Furthermore, exploitation of the vulnerability usually allows access only to a limited set of data or to data of a lesser degree of significance.
* **LOW**  – the exploitation of the vulnerability results in a little direct impact on the security of the application or depends on conditions that are very difficult to achieve practically (e.g. physical access to the server).
* **INFO**  – issues marked as INFO are not security vulnerabilities per se. They aim to point out best practices, whose implementation will increase the overall security level of the system. Alternatively: the issues point out some solutions in the system (e.g. from an architectural perspective) that might limit the negative effects of other vulnerabilities.

## Statical overview of vulnerabilities in web application

## Most sever vulnerabilities identified

The most severe vulnerabilities identified during the assessment were:

* <MOST\_SEVERE\_1>
* <MOST\_SEVERE\_2>

In total, <NUMBER\_OF\_ISSUES> **security issues** have been identified and additionally <NUMBER\_OF\_INFO> **informative**, as a suggestion related to best practices. The vulnerabilities are described in detail in further parts of the report.

# WEB APPLICATION VULNERABILITIES

|  |
| --- |
| [CRITICAL] <CRITICAL\_TITLE\_VULNERABILITY> |

### SUMMARY

<CRITICAL\_SUMMARY>

More information:

* <CRITICAL\_MORE\_INFO\_LINK>

### PREREQUISITES FOR THE ATTACK

Account in application/None/Other.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Request 1:

|  |
| --- |
|  |

Response 1:

|  |
| --- |
|  |

### LOCATION

<CRITICAL\_URL\_OF\_FINDING>

### RECOMMENDATION

<CRITICAL\_RECOMMENDATIONS>

|  |
| --- |
| [HIGH] <HIGH\_TITLE\_VULNERABILITY> |

### SUMMARY

<HIGH\_SUMMARY>

More information:

* <HIGH\_MORE\_INFO\_LINK>

### PREREQUISITES FOR THE ATTACK

Account in application/None/Other.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Request 1:

|  |
| --- |
|  |

Response 1:

|  |
| --- |
|  |

### LOCATION

<HIGH\_URL\_OF\_FINDING>

### RECOMMENDATION

<HIGH\_RECOMMENDATIONS>

|  |
| --- |
| [MEDIUM] <MEDIUM\_TITLE\_VULNERABILITY> |

### SUMMARY

<MEDIUM\_SUMMARY>

More information:

* <MEDIUM\_MORE\_INFO\_LINK>

### PREREQUISITES FOR THE ATTACK

Account in application/None/Other.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Request 1:

|  |
| --- |
|  |

Response 1:

|  |
| --- |
|  |

### LOCATION

<MEDIUM\_URL\_OF\_FINDING>

### RECOMMENDATION

<MEDIUM\_RECOMMENDATIONS>

|  |
| --- |
| [LOW] <LOW\_TITLE\_ VULNERABILITY > |

### SUMMARY

<LOW\_SUMMARY>

More information:

* <MORE\_INFO\_LINK>

### PREREQUISITES FOR THE ATTACK

Account in application/None/Other.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Request 1:

|  |
| --- |
|  |

Response 1:

|  |
| --- |
|  |

### LOCATION

<URL\_OF\_FINDING>

### RECOMMENDATION

<RECOMMENDATIONS>

|  |
| --- |
| [INFO] <INFO\_TITLE\_RECOMMENDATION> |

### SUMMARY

<INFO\_SUMMARY>

More information:

* <INF\_MORE\_INFO\_LINK>

### PREREQUISITES FOR THE ATTACK

Account in application/None/Other.

### TECHNICAL DETAILS (PROOF OF CONCEPT)

Request 1:

|  |
| --- |
|  |

Response 1:

|  |
| --- |
|  |

### LOCATION

<INF\_URL\_OF\_FINDING>

### RECOMMENDATION

<INFO\_RECOMMENDATIONS>