



Penetration Test Report Holert GmbH

v1.2

confidential

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

Author:
Gabriel Terhorst

Date:
31st January, 2022

Contents

i	List of changes	2
1	Contact persons	3
1.1	Contact person Holert GmbH	3
1.2	Contact person binsec GmbH	3
1.3	About binsec GmbH	3
2	Project overview	4
2.1	Introduction	4
2.2	Project scope	4
2.3	Classification	5
2.4	Period of execution	5
3	Management overview	6
3.1	Summary	6
3.2	List of vulnerabilities	6
4	Technical report	7
4.1	Cross-Site-Scripting	7
4.2	Missing rate limiting	8
4.3	Missing attributes in HTTP headers	9
5	Appendix A	10
5.1	General approach	10
5.2	Procedure for web applications and APIs	11
5.3	Risk assessment	13
6	Legal Notice	15

i List of changes

Version	Description	Author	Date
1.0	Report generation	Gabriel Terhorst	19 th January, 2022
1.1	Quality assurance	QA team	20 th January, 2022
1.2	Review of vulnerabilities	Gabriel Terhorst	31 st January, 2022

1 Contact persons

1.1 Contact person Holert GmbH

Renke Holert
Consulting - Development

Holert GmbH
Luise-Ullrich-Str. 20
80636 Munich

Phone +49 89599974700
E-mail: renke@holert.com

1.2 Contact person binsec GmbH

Gabriel Terhorst, M.Sc.
Senior Penetration Tester

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main

Phone: +49 69 2475607-14
E-mail: gt@binsec.com

1.3 About binsec GmbH

We are a consulting firm specializing in IT and information security located in Frankfurt am Main, Germany. We primarily focus on comprehensive security consulting and the implementation of technical security analyses. We assist our customers from the implementation of technical security measures through to company-wide security management. As an owner-managed company, the long-term satisfaction of our customers is of great importance to us. The certifications of our employees, the lecturing activities at universities and our practical experience speak for themselves.

2 Project overview

2.1 Introduction

The company Holert GmbH implemented a tool to display project data and export that data to Excel, PDF and Outlook. The data in question is imported to the webapp via a REST-API from a MS Project plugin. The authentication is done through Azure AD. The following webapp was tested during the penetration test:

- <https://webapp.cloud.allocatus.com>

2.2 Project scope

Test accounts had been created for testing the web application, which are listed below:

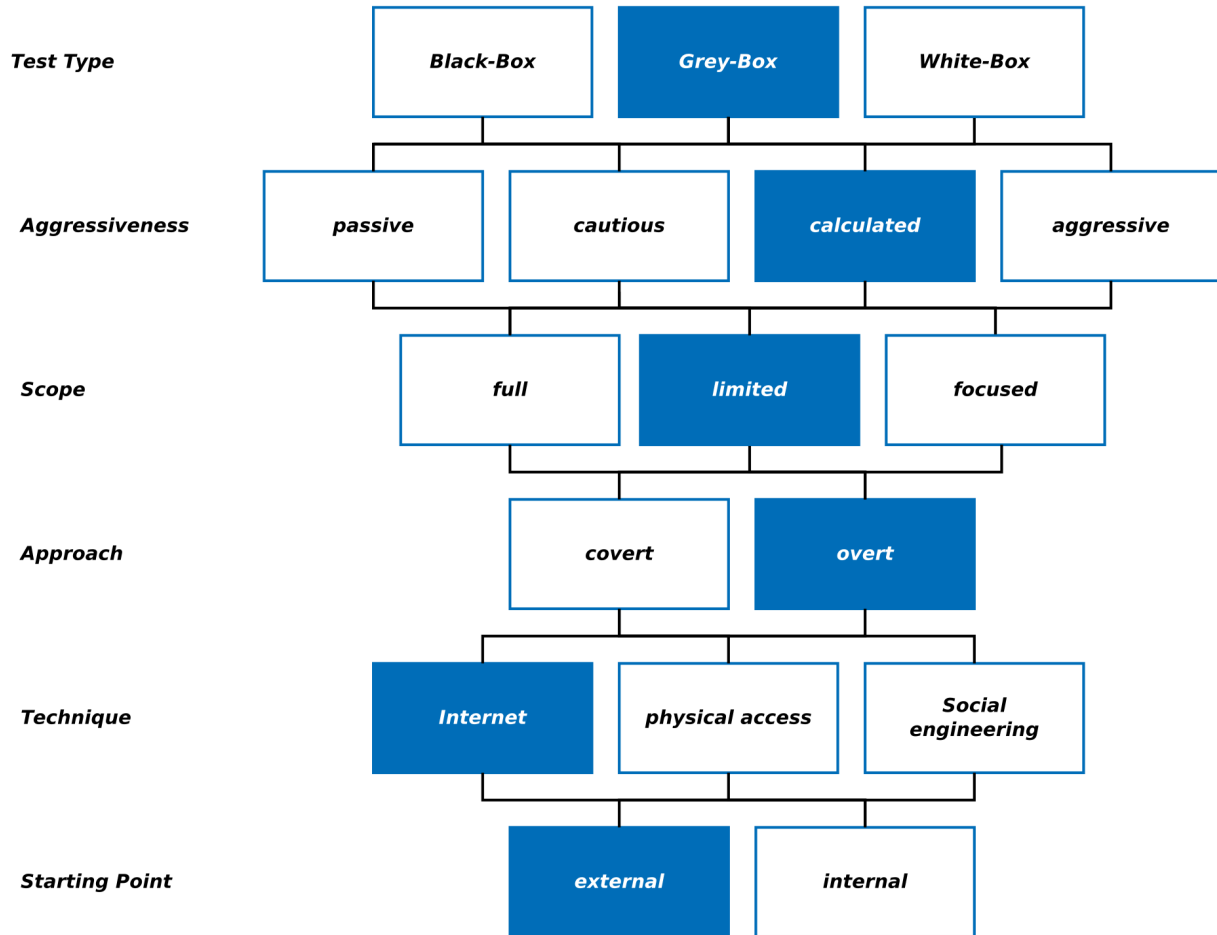
Webapplication	User account	Comment
https://webapp.cloud.allocatus.com	admin@ierot345.onmicrosoft.com, gabriel.terhorst@ierot345.onmicrosoft.com	-

Recommendation

All user accounts which have been created for the penetration test should be deleted after the agreed execution period, or at least be deactivated.

2.3 Classification

In cooperation with Holert GmbH, the following classification variant was agreed as the approach: The penetration test was performed as an external grey box test, without using aggressive attacking techniques such as DDoS attacks. The exact procedure is described in chapter 5.2.



2.4 Period of execution

The penetration test was conducted on the 17th and 18th January 2022 from the IPv4 address 185.156.252.230 and 217.111.127.122.




3 Management overview

3.1 Summary

Date	Description	Vulnerabilities	critical
17.01.2022- 18.01.2022	Initial Pentest	3	1
31.01.2022	Review	2	fixed

During the initial penetration test 3 vulnerabilities could be identified in total, one of those was a critical one. The critical vulnerability allowed for any authenticated user to inject Javascript into the webapp. The other two listed vulnerabilities elevate the security level of the webapp in general. The critical vulnerability has been fixed.

3.2 List of vulnerabilities

No.	Risk Assessment	Description
1	 immediate action required	Missing input validation for a parameter enables cross-site scripting. Fixed YES
2	 note	The number of requests sent to the API is not limited. Fixed NO
3	 note	Security-relevant attributes in the HTTP header are missing. Fixed NO

4 Technical report

4.1 Cross-Site-Scripting



high occurrence probability, medium extent of damage

OWASP Top 10: A3 - Injection

In case of Cross-Site-Scripting (XSS), any script code can be injected into the web application that is executed by the victim's browser. The Project Overview is prone to stored XSS, as JavaScript can be injected via the column names.

As an example, the string `` is set as the DisplayName of the column ProjectOwnerName:

ColumnName	DisplayName	CustomField	Width	Position	Sortable	Visible
ProjectOwnerName	<code></code>	false	200	1	false	true
Start	Start	false	200	3	false	true
Title	Project Name	false	200	2	false	true
LastPublished	LastPublished	false	200	5	false	true
End	Finish	false	200	4	false	true

Project Name	Start	Finish
Renke Holert	Schulze Hausbau	
Renke Holert	Schmidt Hausbau	
Renke Holert	Müller Hausbau	
Renke Holert	Meyer Hausbau	
gt	holert-test	01/17/2022
	Holert Hausbau	01/17/2022
		01/18/2022
		01/09/2023

Recommendation

To prevent XSS all html parameters should be escaped. More information on XSS prevention can be found on the following OWASP website: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

4.3 Missing attributes in HTTP headers



high occurrence probability, warning

OWASP Top 10: A5 - Security Misconfiguration

The protocol header of HTTP offers security related attributes, that are not set for the web application `https://webapp.cloud.allocatus.com`. Following HTTP header fields are affected:

- X-XSS-Protection enables the Cross-Site-Scripting (XSS) filter on newer browsers. With XSS, arbitrary script code can be injected into the web application, which is then executed by the victim's browser.
- Content-Security-Policy (CSP) prevents XSS by prohibiting the use of scripts in the source code of the page, the so-called inline-scripts. Instead, the scripts must be outsourced to separate files.
- X-Frame-Options prevents Clickjacking-Attacks, in which the contents of the application are overlaid by another surface. The contents of the application can no longer be integrated in an IFrame on another page.

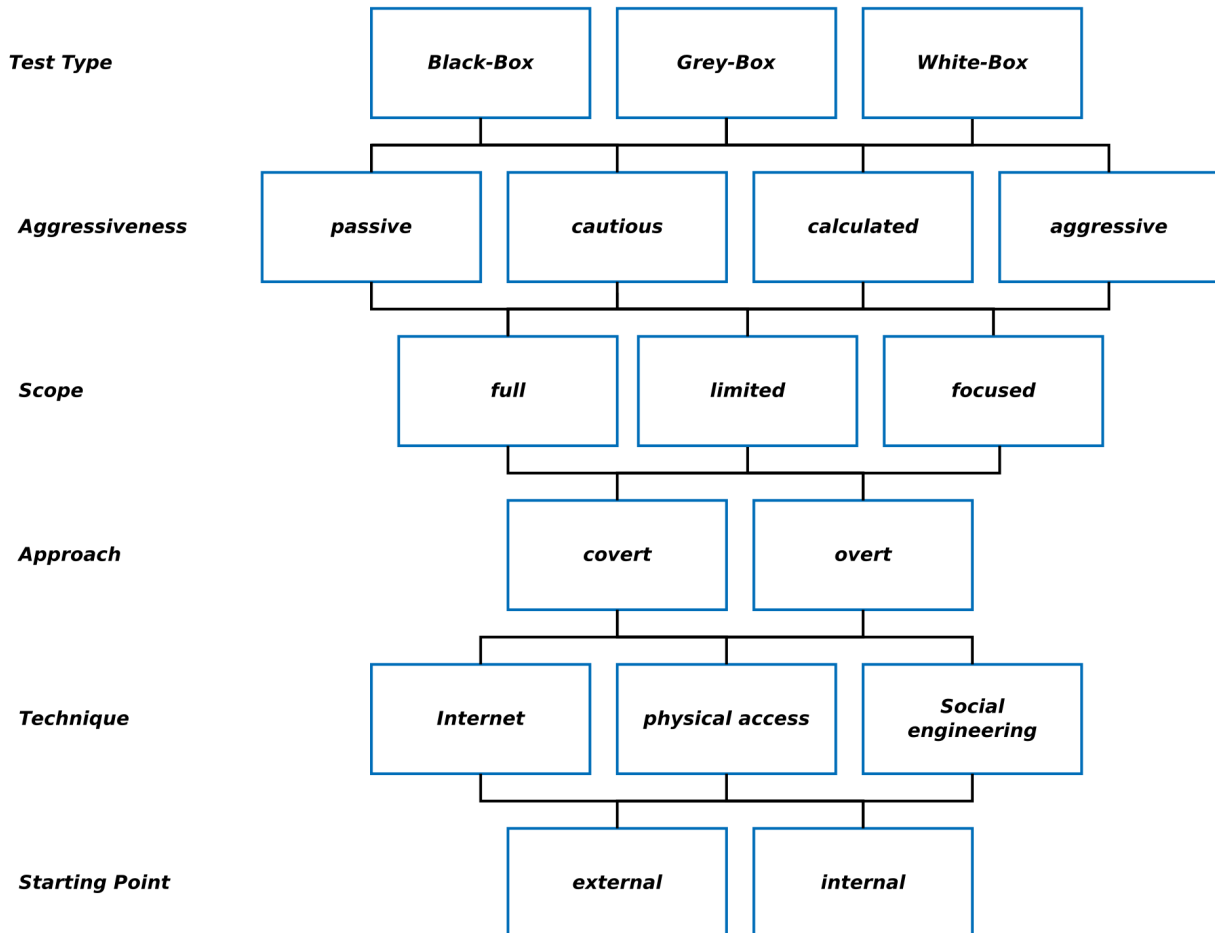
Recommendation

The missing attributes should be added to the HTTP header. The proper operation of the applications should be verified.

5 Appendix A

5.1 General approach

Pursuant to the study “Implementation Concept for Penetration Tests“ by the German Federal Office for Information Security (BSI), binsec GmbH uses the following formula to classify penetration tests:



There are different approaches and attack methods for penetration tests (pentests). While no information about the target is available in the case of a black box pen test, the penetration tester is provided all relevant information in the case of a white box pentest. The informative value and the implications of the pentest depend on various factors, such as the underlying information available or the starting point. To strike a balance between effort and informative value, we generally recommend using a limited and weighted grey box test that is not implemented covertly. However, the ultimate selection, technique used and the starting point always depend upon the requirements and expectations of the client.

5.2 Procedure for web applications and APIs

The test method used by binsec GmbH for web applications is based on the OWASP Testing Guide and the OWASP TOP 10. The Open Web Application Security Project (OWASP) is currently the world's largest non-profit organisation, the objective of which is to increase the security of applications.

Penetration tests for credit card processing companies also comply with the requirements of the Payment Card Industry Security Standards (PCI DSS). While this standard also references OWASP publications, it additionally defines special requirements regarding credit card data.

OWASP TOP 10

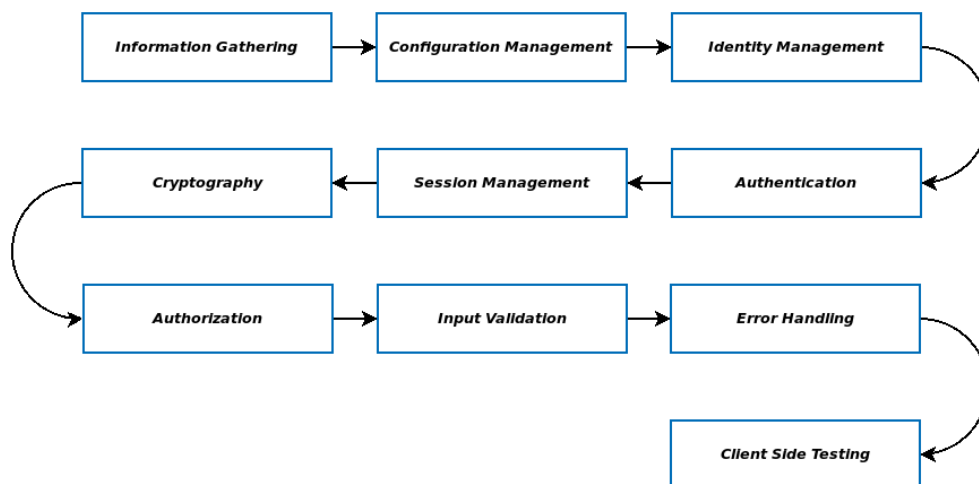
The OWASP Top 10 includes the ten most critical vulnerabilities in web applications. In the current publication from 2021, the following points are listed:

- A1 Broken Access Control
- A2 Cryptographic Failures
- A3 Injection
- A4 Insecure Design
- A5 Security Misconfiguration
- A6 Vulnerable and Outdated Components
- A7 Identification and Authentication Failures
- A8 Software and Data Integrity Failures
- A9 Security Logging and Monitoring Failures
- A10 Server-Side Request Forgery (SSRF)

Most web application vulnerabilities are due to missing or incorrect authorization management.

Methods of approach

The methodical test approach of binsec GmbH is roughly divided into the following 10 test phases:



Within the test phases, the web application is examined for the aforementioned vulnerabilities of the OWASP TOP 10. Various analysis tools are used during the pentest, as well as intensive manual testing. The exact course of the penetration test depends heavily on the characteristics of the respective application and is based on the approach a real attacker would take. If Application Programming Interfaces (APIs) are part of the object of investigation, the OWASP API Security Top 10 are also taken into account during the penetration test.

OWASP API Security Top 10

The OWASP API Security Top 10 includes the ten most common vulnerabilities in Application Programming Interfaces. In the first and current publication from 2019, the following points are listed:

- API1 Broken Object Level Authorization
- API2 Broken User Authentication
- API3 Excessive Data Exposure
- API4 Lack of Resources & Rate Limiting
- API5 Broken Function Level Authorization
- API6 Mass Assignment
- API7 Security Misconfiguration
- API8 Injection
- API9 Improper Assets Management
- API10 Insufficient Logging & Monitoring

5.3 Risk assessment

Binsec GmbH considers the term “risk“ to mean a combination of the probability of occurrence of a vulnerability (or the likelihood of its exploitation) and the possible extent of damage. The probability of occurrence or the probability of exploitation of a security gap in IT systems essentially depends on these factors:

- How easily can the vulnerability be identified? (Visibility)
- Are there any exploits for this vulnerability available, or is the attacker required to have a certain level of knowledge to exploit them? (Exploitability)
- Does the exploitation require special rights? (Privilege Escalation)
- Is a combination with other security holes required? (Vulnerability Chaining)
- Is human interaction necessary for the vulnerability? (Social Engineering)

The following classifications are decisive for the possible extent of damage:

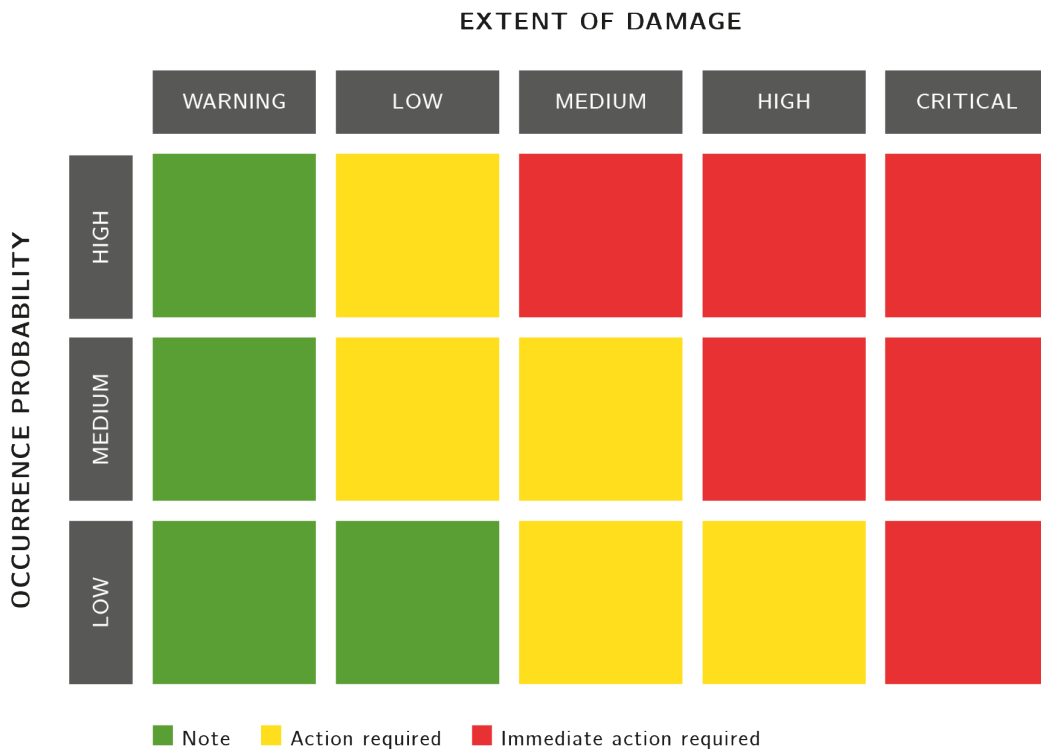
1. Financial damage
2. Complete compromising of the system
3. Violation of security objectives related to data or user accounts:
 - (a) Confidentiality
 - (b) Availability
 - (c) Integrity
4. Bypassing of security measures
5. Information disclosure

Taking into account both the probability of occurrence and the potential extent of damage, the penetration tester makes a subjective assessment of the risk for each vulnerability found. We recommend taking an own assessment of the vulnerabilities.

The assessment is subject to the following classification:

Occurrence probability	High	The vulnerability is obvious or exploits are freely available.	Extent of damage	High Critical	Complete compromising of the system.
	Medium	The vulnerability can be identified in a reasonable amount of time; exploits may need to be adapted.		Medium	Violation of security objectives concerning information or IT systems.
	Low	The vulnerability is difficult to find and may require permissions or the exploitation of other vulnerabilities.		Low Warning	Preparation for exploitation of other vulnerabilities as part of a sustained attack. Information disclosure.

The risk classification entails a priority for action.



6 Legal Notice

binsec GmbH
Solmsstraße 41
60486 Frankfurt am Main
Germany

E-Mail: info@binsec.com
Telephone: +49 69 2475607-0
Fax: +49 69 2475607-20

Managing Director: Patrick Sauer
Authorised Officer: Florian Zavatzki

Commercial Register: Frankfurt a.M. HRB 97277
VAT ID no.: DE290966808