



Security Assessment

HandSqueeze DAPP

Verified on 10/09/2023

SUMMARY

Project

HandSqueeze DAPP

CHAIN

BSC/ETH

METHODOLOGY

Manual & Automatic Analysis

FILES

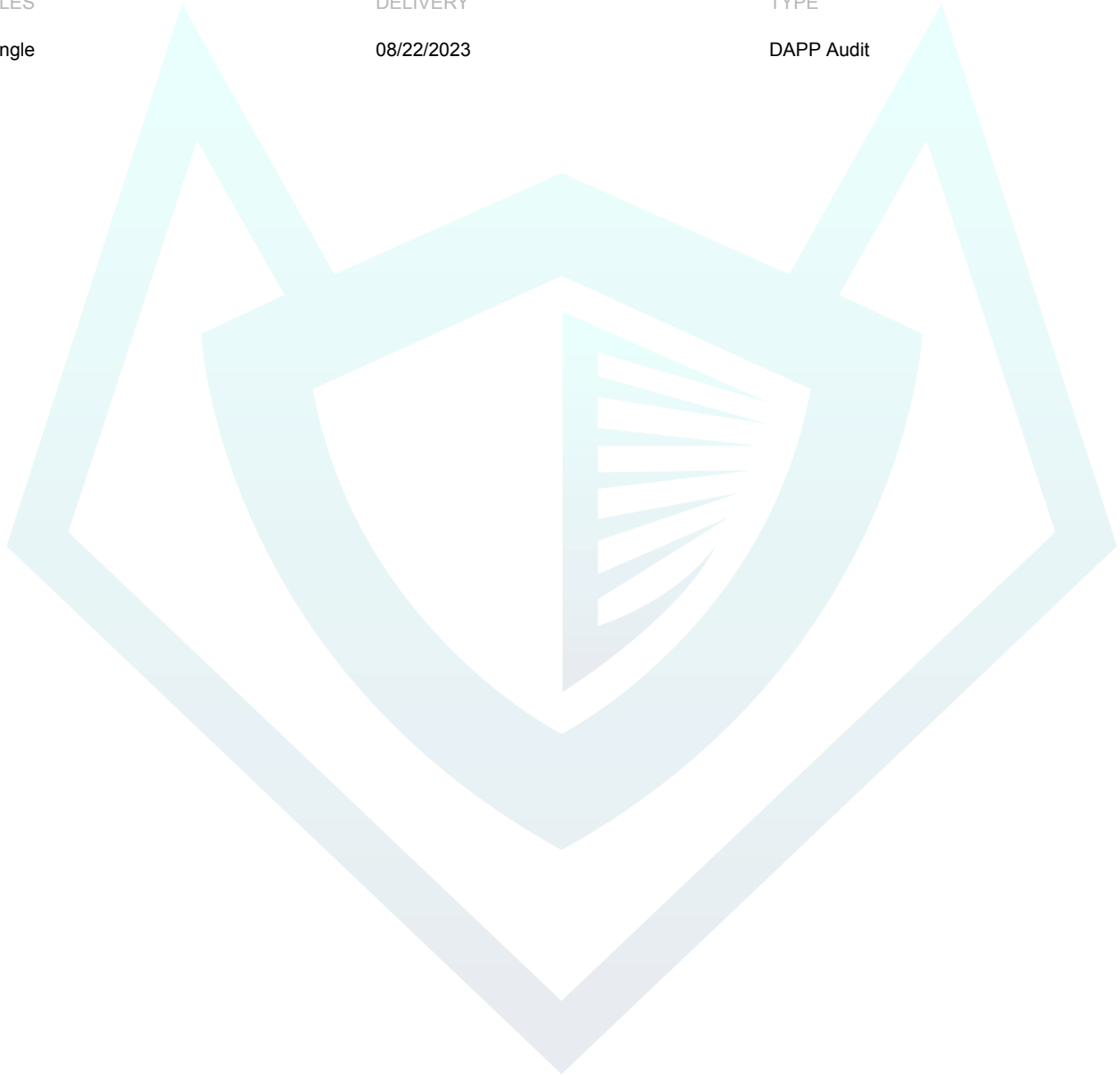
Single

DELIVERY

08/22/2023

TYPE

DAPP Audit



STATUS

✓ **AUDIT PASSED**

TABLE OF CONTENTS | HandSqueeze DAPP

| Summary

Project Summary
Findings Summary
Disclaimer
Scope of Work
Auditing Approach

| Project Information

Token/Project Details
Inheritance Graph
Call Graph

| Findings

Issues
SWC Attacks
CW Assessment
Fixes & Recommendation
Audit Comments

DISCLAIMER | HandSqueeze DAPP

ContractWolf audits and reports should not be considered as a form of project's "Advertisement" and does not cover any interaction and assessment from "Project Contract" to "External Contracts" such as PancakeSwap, UniSwap, SushiSwap or similar.

ContractWolf does not provide any warranty on its released report and should not be used as a decision to invest into audited projects.

ContractWolf provides a transparent report to all its "Clients" and to its "Clients Participants" and will not claim any guarantee of bug-free code within its **SMART CONTRACT**.

ContractWolf's presence is to analyze, audit and assess the Client's Smart Contract to find any underlying risk and to eliminate any logic and flow errors within its code.

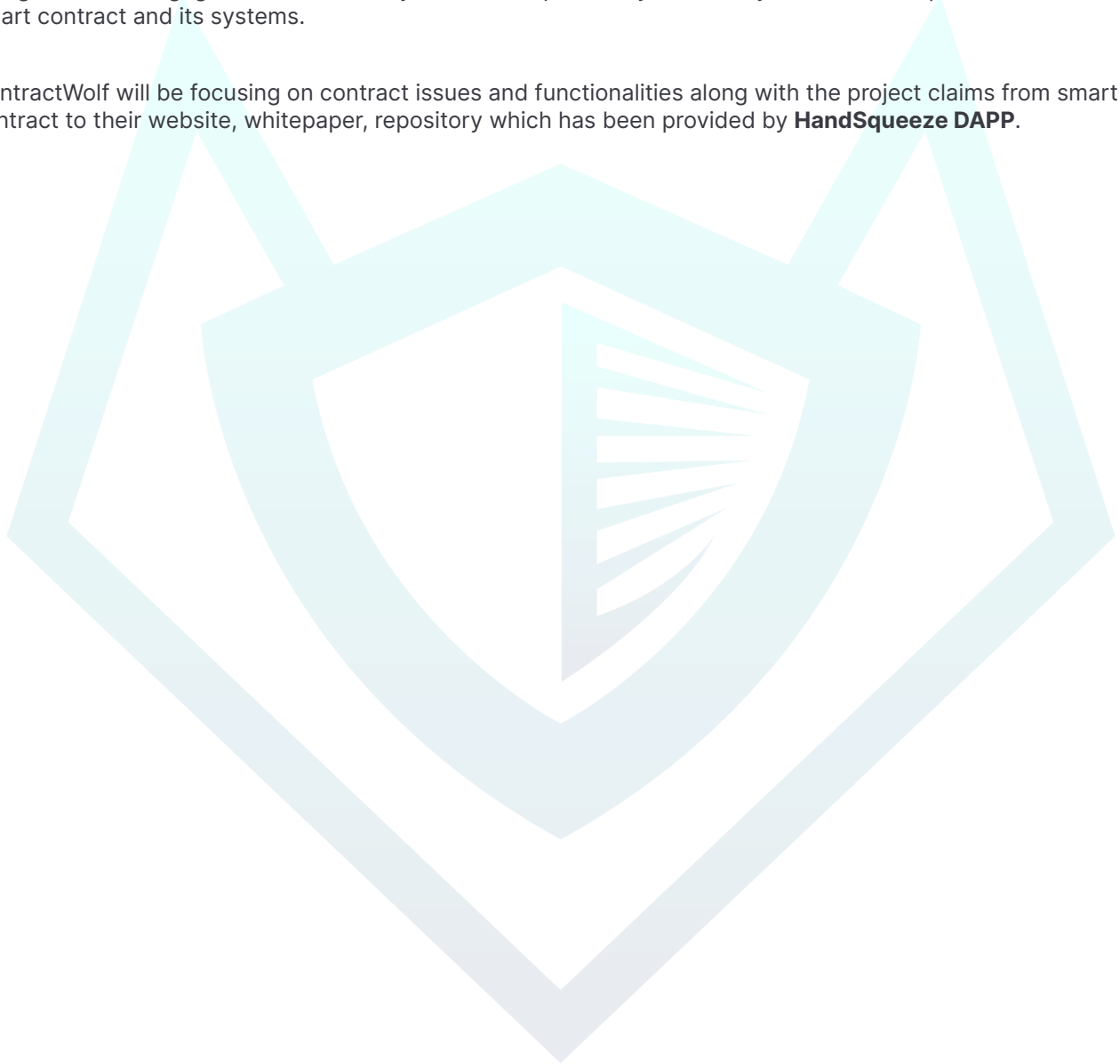
Each company or project should be liable to its security flaws and functionalities.

SCOPE OF WORK | HandSqueeze DAPP

HandSqueeze DAPP team has agreed and provided us with the files that need to be tested (*Github, BSCscan, Etherscan, Local files etc*). The scope of audit is the main contract.

The goal of this engagement is to identify if there is a possibility of security flaws in the implementation of smart contract and its systems.

ContractWolf will be focusing on contract issues and functionalities along with the project claims from smart contract to their website, whitepaper, repository which has been provided by **HandSqueeze DAPP**.



AUDITING APPROACH | HandSqueeze DAPP

Every line of code along with its functionalities will undergo manual review to check for security issues, quality of logic and contract scope of inheritance. The manual review will be done by our team that will document any issues that they discovered.

METHODOLOGY

The auditing process follows a routine series of steps :

1. Code review that includes the following :
 - Review of the specifications, sources and instructions provided to ContractWolf to make sure we understand the size, scope and functionality of the smart contract.
 - Manual review of code. Our team will have a process of reading the code line-by-line with the intention of identifying potential vulnerabilities, underlying and hidden security flaws.
2. Testing and automated analysis that includes :
 - Testing the smart contract function with common test cases and scenarios to ensure that it returns the expected results.
3. Best practices and ethical review. The team will review the contract with the aim to improve efficiency, effectiveness, clarifications, maintainability, security and control within the smart contract.
4. Recommendations to help the project take steps to eliminate or minimize threats and secure the smart contract.

TOKEN DETAILS | HandSqueeze DAPP



Token Name	Symbol	Decimal	Total Supply	Chain
-	-	-	-	BSC/ETH

SOURCE

Source <https://app.handsqueeze.io/>

FINDINGS | HandSqueeze DAPP

0 Critical

0 High Risk

2 Medium Risk

10 Low Risk

7 Informational


Security Overview

Widget Description

33 medium

Improve the Risk Score by addressing what needs to be remediated.

app HandSqueeze: 33%


**CONTRACT
WOLF**

Faces associated with your website ⓘ
Completed - No findings

Leaked Accounts Check ⓘ
Completed - No findings

Sensitive Public Information Check ⓘ
Completed - No findings

Subdomains found ⓘ
Completed - Discovered 2 findings

app.handsqueeze.io
app-staging.handsqueeze.io

Risk
An attacker could use this information to conduct attacks on vulnerable web targets.

Recommendation
We recommend you secure all publicly available subdomains and remove any that are unused.

Web Application Firewall Check ⓘ
Completed - Discovered 2 findings

☒ firewall detected

☒ https://app.handsqueeze.io/login firewall detected

Risk
WAF's mitigate DDoS attacks, filter bot activity, detect anomalies and malicious payloads.

Recommendation
We recommend you protect your application with a Web Application Firewall.

Classification
CWE-79

References
<https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/>

Missing HTTP headers found ⓘ
Completed - Discovered 9 findings

Rule	Message
Cache-Control	Value does not match security policy
Content-Security-Policy	Header not included in response
Pragma	Header not included in response
Referrer-Policy	Header not included in response
Server	Header should not be returned
Set-Cookie - XSRF-TOKEN	Must-Contain directive missed
Set-Cookie - handsqueeze_session	Must-Contain directive missed
Strict-Transport-Security	Header not included in response
X-XSS-Protection	Value does not match security policy

Risk
An attacker could identify missing headers to leverage known exploitation techniques.

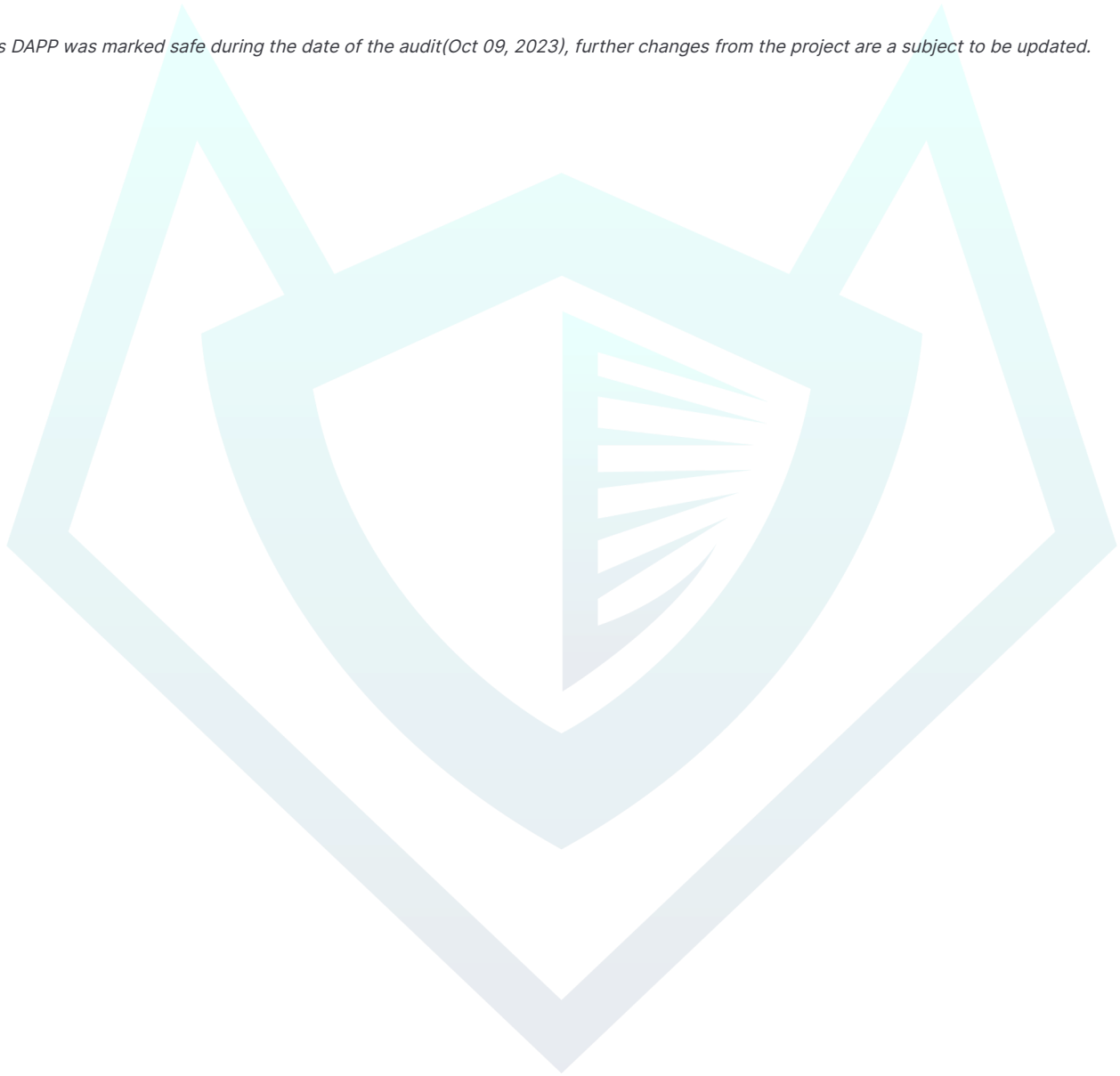
Recommendation
We recommend your HTTP headers are appropriate for the requests your application receives.

FIXES & RECOMMENDATION

Informational | Secured DAPP

ContractWolf did not find any major technical issues within the DAPP and marked the website <https://app.handsqueeze.io/> safe to interact with.

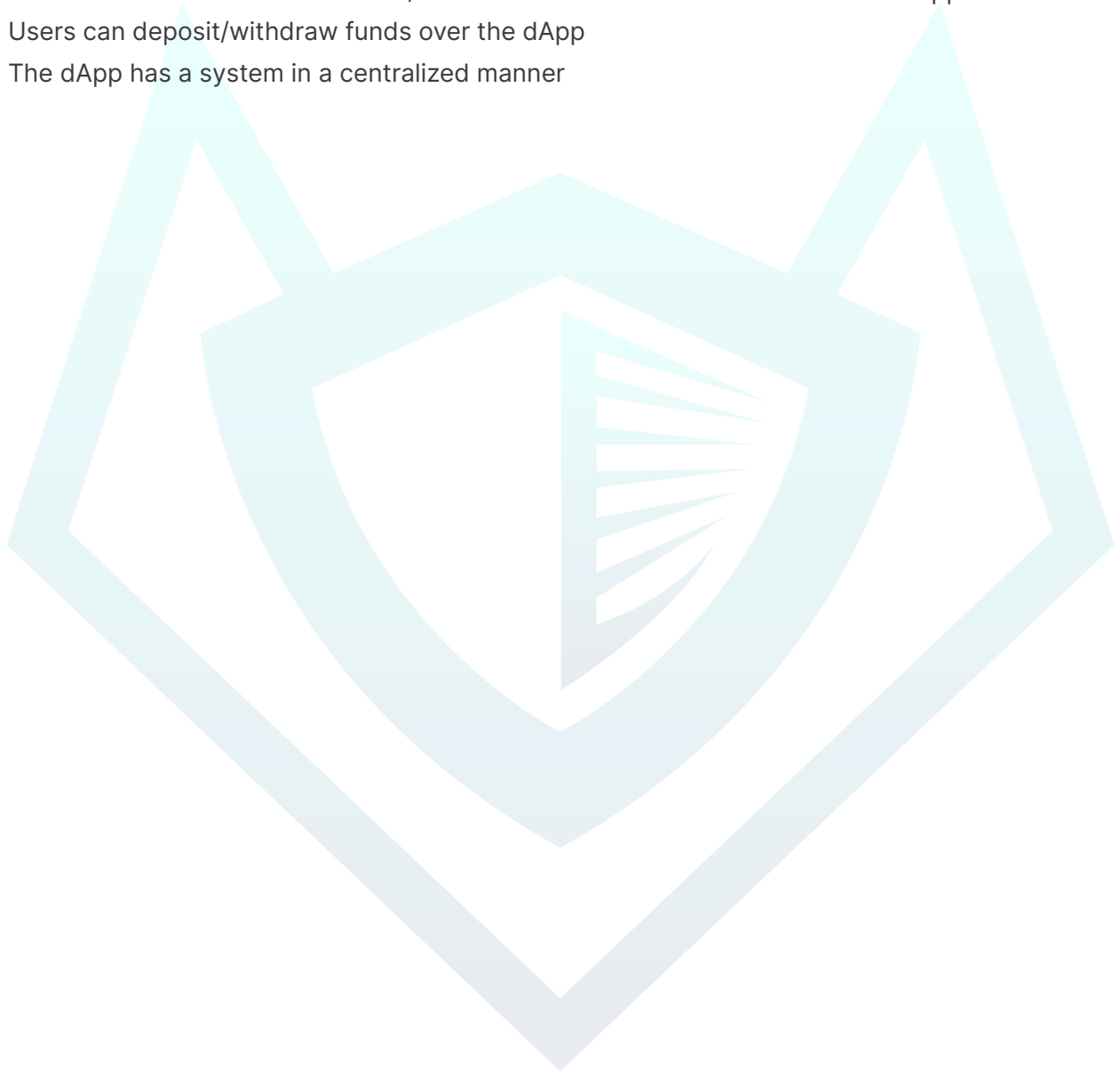
This DAPP was marked safe during the date of the audit(Oct 09, 2023), further changes from the project are a subject to be updated.



AUDIT COMMENTS | HandSqueeze DAPP

Audit comment for a non-technical perspective

- Users can safely interact with the dApp (<https://app.handsqueeze.io/>)
- The users can create account and/or wallet and make transactions over the dapp
- Users can deposit/withdraw funds over the dApp
- The dApp has a system in a centralized manner





CONTRACTWOLF

Blockchain Security - Smart Contract Audits