FEEMCO TECHNOLOGIES

FROM CACHES TO CRASHES

Security Assessment & Findings Report

Created for Myself

Business Confidential

Confidentiality Statement

This document is the exclusive property of COMPANY and Feemco Technologies. This document contains proprietary and confidential information. Any duplication, redistribution, or use requires the written consent of both parties. Further restrictions for this are outlined in any agreements made between these two parties and will be upheld based on that agreement.

Disclaimer

The Cyber Defense Penetration Testing performed by Feemco Technologies, and the report prepared by the tester (Jeff Feemster), is intended to showcase identified security flaws found during testing of a point-in-time reference. While it may be impossible to denote every possible exploitation, we've prepared this document to showcase the issues we found at the time of testing with priority on things likely to be or become identified by attackers. This does not and cannot showcase things that weren't tested against, or from a time outside of the testing window.

Due to this, and an ever changing threat landscape, we highly recommend retesting after remediation has been validated, to further identify issues.

Contact Information

Sometimes when performing testing we come across issues, evidence of exploitation, or other concerns that merits immediate contact. Sometimes that may also include several contacts depending on the severity type of concern. Due to that, we have both a priority scale and a notes section filled out by the customer when agreeing to our services. Priority is ranked 1-3, under the basis of:

1. Primary point of contact for all things
2. Secondary contact, or contact for specific issues
3. One of the others hasn't responded, and the issue is urgent, get these people on the phone.

Contact Name	Number/Email	Priority	Notes
Myself	root@localhost.local	1	It's me

Assessment Overview

Feemco Technologies was engaged to perform a general security posture assessment of internal and external infrastructure compared to industry standards and best practices. The assessment took place between (6/23/2025 - 6/24/3025).

This process was acted on in phases, which can be explained by the following:

- Planning - Customer goals are gathered, scope defined, and rules of engagement confirmed prior to any other activities.
- Discovery - This can be broken down further into Reconnaissance, Scanning, and general assessment of potential vulnerabilities.
  - Reconnaissance - This process is developing general idea of items in scope's attack surface, and can be considered intelligence gathering.
  - Scanning - This is the process of performing checks to confirm, validate, or find further information not previously found.
  - Assessment - Take what's found and attempt to bring possible exploits to light.
- Exploitation - This is the phrase where we've already found possible vectors, and will attempt to validate the exploitability of those.
- Reporting - Documenting vulnerabilities and proven exploits found as well as steps taken. Attempt to provide strengths and weaknesses found within the environment.

Scope

The agreed scope of this engagement is defined by the following:

Asset	Type	Restrictions
10.10.11.74	IP address	Avoid Downtime
artificial.htb	domain name	Avoid Downtime, No dns takeovers

Executive Summary

Evaluated the HTB Artificial system's security posture through defense penetration testing (PenTesting) from (6/23/2025-6/24/2025). The following sections provide high level overview of vulnerabilities discovered, attempts made, and general recommendations.

Limitations

- No testing performed that would damage the infrastructure the host sits on
- No testing that would accidently cause others testing the system to be interfered with

Testing Summary

During testing we found a website vulnerable to remote code execution, and were able to leverage that to gain access to the system. Normally we'd put something more important here like root access, domain access, things like that but we're ending this shorter because it's only about the documentation process.

Key Observations

- Outdated libraries

- public, unverified registration
- file uploads that can contain code to be ran
- something else here

Recommendations

- upgrade tensorflow immediately
- do at minimum email validation for users
- check all incoming models for risky calls or pickling operations
- sandbox all executions

Identified Strengths

- Registration requires email field
- user separation

Identified Weaknesses

- library updates
- sanitization of inputs

Pentest Findings

CVE/CWE :	**Unsure right now**
Description:	old tensorflow version vulnerable to known exploits using the model files
System/Service:	http://artificial.htb/
Impact:	Remote code execution
References:	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-26266 https://www.oligo.security/blog/tensorflow-keras-downgrade-attack-cve-2024-3660-bypass

POC:

```
something probably
```