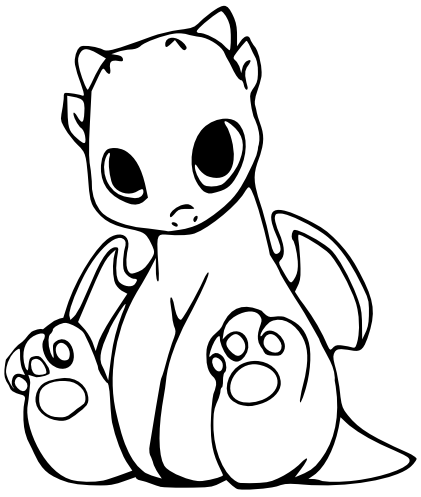
Dragon_DFD

Owner:
Reviewer:
Contributors:
Date Generated: Thu Oct 10 2024



OWASP Threat Dragon

Executive Summary

High level system description

Not provided

Summary

Total Threats	14
Total Mitigated	0
Not Mitigated	14
Open / High Priority	13
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

Syuzhetna indi-hra na movi prohramuvannia Python

Syuzhetna indi-hra na movi prohramuvannia Python

User (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Computer Application (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Managment (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Processing (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data entry based on options (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
1	Spoofing the Computer Application Process	Tampering	High	Open		Computer Application may be spoofed by an attacker and this may lead to information disclosure by Human User. Consider using a standard authentication mechanism to identify the destination process.	Provide remediation for this threat or a reason if status is N/A
1	Spoofing the Human User External Entity	Information disclosure	High	NotApplicable		Human User may be spoofed by an attacker and this may lead to unauthorized access to Computer Application. Consider using a standard authentication mechanism to identify the external entity.	Provide remediation for this threat or a reason if status is N/A

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Potential Lack of Input Validation for Computer Application	Tampering	High	Open		Data flowing across Data entry based on options may be tampered with by an attacker. This may lead to a denial of service attack against Computer Application or an elevation of privilege attack against Computer Application or an information disclosure by Computer Application. Failure to verify that input is as expected is a root cause of a very large number of exploitable issues. Consider all paths and the way they handle data. Verify that all input is verified for correctness using an approved list input validation approach.	
6	Data Flow Data entry based on options Is Potentially Interrupted	Denial of service	High	Open		An external agent interrupts data flowing across a trust boundary in either direction.	Provide remediation for this threat or a reason if status is N/A
6	Elevation Using Impersonation	Information disclosure	High	Open		Computer Application may be able to impersonate the context of Human User in order to gain additional privilege.	Provide remediation for this threat or a reason if status is N/A
8	Computer Application May be Subject to Elevation of Privilege Using Remote Code Execution	Information disclosure	High	Open		Human User may be able to remotely execute code for Computer Application.	Provide remediation for this threat or a reason if status is N/A

Displaying options (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Authenticated Data Flow Compromised	Tampering	High	Open		An attacker can read or modify data transmitted over an authenticated dataflow.	Provide remediation for this threat or a reason if status is N/A

Updating data components (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Elevation Using Impersonation	Information disclosure	High	Open		An attacker can read or modify data transmitted over an authenticated dataflow.	Provide remediation for this threat or a reason if status is N/A

Downloading the original data (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Elevation Using Impersonation	Information disclosure	High	Open		Data Management may be able to impersonate the context of Data Processing in order to gain additional privilege.	Provide remediation for this threat or a reason if status is N/A

Saving serialised data to local storage (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Potential Excessive Resource Consumption for Data Processing or Data Storage	Tampering	High	Open		Does Data Processing or Data Storage take explicit steps to control resource consumption? Resource consumption attacks can be hard to deal with, and there are times that it makes sense to let the OS do the job. Be careful that your resource requests don't deadlock, and that they do timeout.	Provide remediation for this threat or a reason if status is N/A

Data transfer for serialisation or deserialisation (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Elevation Using Impersonation	Information disclosure	High	Open		Data Processing may be able to impersonate the context of Data Management in order to gain additional privilege.	Provide remediation for this threat or a reason if status is N/A

Transmission of component setting data (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Weak Access Control for a Resource	Information disclosure	High	Open		Improper data protection of Data Storage can allow an attacker to read information not intended for disclosure. Review authorization settings.	Provide remediation for this threat or a reason if status is N/A
6	Spoofing of Source Data Store Data Storage	Tampering	High	Open		Data Storage may be spoofed by an attacker and this may lead to incorrect data delivered to Data Processing. Consider using a standard authentication mechanism to identify the source data store.	Provide remediation for this threat or a reason if status is N/A

Downloading saved data (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Elevation Using Impersonation	Information disclosure	High	Open		Data Management may be able to impersonate the context of Computer Application in order to gain additional privilege.	Provide remediation for this threat or a reason if status is N/A

Data Storage (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations