List of threats used in the confirming experiment (GitHub Scenario)

Each threat has a unique ID alongside a description, the corresponding STRIDE threat (i.e., Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege), and assumptions used to validate the existence of the threat. The last column, whether the threat is valid or not, was not shown to the participants.

Unique ID	Description	STRIDE threat	Assumption	Affected Components	Real
1	The attacker uses the malicious code to gain root access to the server.	EoP	1. The attacker can submit code to a remote repository 2. The server has been pulled and running the code submitted by the attacker; 3. Code run as root on the server.	Victim's Server	Yes
2	Not only can the attacker use these third-party services, but the attacker can also push code to the remote code repository where the yml file is located.	ID (Information Disclosure)	1. An attacker can browse the project's yml file; 2. The developer has left the keys to the third-party services they need to use in the yml file that configures GitHub Actions.	Third-party services, the remote code repository	No
3	An attacker submit malicious code to the project on GitHub and get a shell of the server running the code.	EoP	1. The attacker can submit code to remote repo; 2. The server has pulled and been running the malicious code submitted by the attacker.	Victim's server	Yes
4	An attacker submit malicious code can crash the server running the code, causing a Denial of Service (DoS).	DoS	1. The attacker submits malicious code that can cause Denial of Service (DoS) to remote repo; 2. The server has pulled and been running the code submitted by the attacker.	Victim's server	Yes

5	The attacker can launch a push request to a repository on GitHub and can delete the repository.	EoP	The attacker has gained push access to the code repository on GitHub.	The remote code repository	No
6	An unauthenticated and nonprivileged attacker can still submit custom code into the remote repo to prepare the first step of another attack, e.g. turning off logging service or causing a Denial of Service.	EoP, Tampering	The attacker can reach the remote repo (e.g. through internet).	The remote code repository	No
7	If an attacker compromises a http protocol on GitHub, the attacker can steal other users' identities by using HTTP by running a man in the middle attack.	Spoofing	1. GitHub uses the HTTPS protocol; 2. The attacker has compromised the HTTP protocol on GitHub.	GitHub engine	No
8	An attacker uses leaked (e.g. on Github) configuration file to interact with the remote repo, potentially jeopardize running code and submitting malicious code.	Information Disclosure	1. The attacker finds the leaked information; 2. The attacker can (remotely) interact with the remote repo.	Victim's server	Yes
9	The attacker submits the same fake push request to other remote code repositories, causing a Denial of Service attack.	DoS	1. Permission management is properly implemented in the remote (GitHub) provided repository hosting service to differentiate user access to the code repository;	Other remote code repositories	No

			2. An attacker has the right to submit a bogus push request to a remote repository.		
10	Spoofing a remote repo admin by stealing the authentication credentials via a social engineering attack.	Spoofing	1. The attacker carries out a successful social engineering attack (attackers communicate legitimately with others, manipulating and exploiting human qualities to achieve their attack) and gets authentication credentials; 2. The credentials are valid.	The remote code repository	Yes