* Make a good faith effort to avoid privacy violations, destruction of data, and interruption or degradation of our service. Only interact with accounts you own or with the explicit permission of the account holder.

Prohibited actions when conducting RCE attempts:
+ Altering or uploading files on the web server. (In case of file-upload functionality upload of webshells is prohibited, try uploading echo, info or any variable/info-based invocation code)
+ Altering file permissions
+ Reading sensitive files on the system (e.g /etc/shadow) and/or snooping through the file/folder structure (Same applies to XXE, LFI and Path Traversal, or any other vulnerability which allows you to read underlying file/folder structure)
+ Altering/Modifying/Deleting any files on the system.
+ Copying any files from the system and disclosing them to any third party
+ Interacting with underlying OS-level data and/or databases.
+ Interacting with other services running on the OS-level and/or any remote hosts residing on the network.
+ Interrupting the normal operation of the server.
+ Any type of establishment for persistent connection mechanisms (netcat, ssh reverse tunnel, etc) are prohibited.

Allowed actions when conducting RCE attempts - Unix:
+ Executing 'ifconfig', 'hostname', 'whoami', 'uptime', 'top' or any metrics commands
+ Reading content of the '/etc/passwd' file
+ Using 'echo' to pipe characters into a file located in the "/tmp/", reading the file and then removing it right after confirmation.

Allowed actions when conducting RCE attempts - Windows:
+ Executing 'ipconfig', 'hostname', 'whoami' or any metrics commands
+ Reading content of the 'drive:/boot.ini', 'drive:/install.ini' or 'drive:/Windows/System32/drivers/etc/networks'
+ Using 'echo' to pipe characters into a file located in the drive:/temp, reading the file (type) and then removing it right after confirmation.

SQL Injection (SQLi) Policy

Vulnerabilities which allow injection of attacker controlled parts of the SQL query should be run in accordance to this policy.
Prohibited actions when conducting SQLi attempts:
+ Reading sensitive files on the system (e.g /etc/shadow) and/or snooping through the file/folder structure (SELECT LOAD_FILE)
+ Reading specific sensitive database records

+ Creating/Altering/Modifying/Deleting any files/records on the system/database. This includes use of INTO OUTFILE
+ Command Execution (xp_cmdshell, uploading .so or any action that leads to command execution)
+ Creating/Deleting Users
+ Reading/Altering Username and Password information (includes password hashes)
+ Interrupting the normal operation of the server and the database.

Allowed actions when conducting SQLi attempts:
+ Executing SELECT queries such as "@@version", "user();" "system_user();", "database();", "@@hostname"
+ Listing Databases names from schema, listing Columns, Table names
+ Executing Mathematical, conversion or logical queries, such as:

1. ASCII Value -> Char (SELECT char(65); # returns A)
2. Char -> ASCII Value (SELECT ascii('A'); # returns 65)
3. String Concatenation (SELECT CONCAT('A','B','C'); # returns ABC)
4. Case Statement (SELECT CASE WHEN (1=1) THEN 'A' ELSE 'B' END; # returns A) 5. SELECT 0×414243; # returns ABC
6. Time Delay (SELECT BENCHMARK(1000000,MD5('A')); SELECT SLEEP(5);)

+ Using Logic and time in Server Responses
+ Using output responses

File-Upload Policy

Vulnerabilities which allow upload of files through any means (f.g PUT HTTP Method, File-upload functionality/module., etc.) are subjected to these rules

Prohibited actions when conducting File-upload attempts:

+ Altering/Modifying/Deleting/Replacing any files on the system. (f.g. defacement) + Uploading files to the account of a user which is not owned by you and you are not authorized by (does not apply to system users or web users like www-data f.g)
+ Uploading files which deliberately introduce additional exploitation vectors (f.g html code with cross-site scripting code on it etc.)
+ Uploading files which can cause Denial of Service (f.g. over-sized files or unlimited amount of files resulting in running out of Disk Quota)

Allowed actions when conducting File-upload attempts:

+ Chained exploitation vectors allowing you to jump out from the upload folder using f.g. path

traversal or path manipulation that do not violate prohibited actions mentioned in File-Upload Policy.
+Uploadofafile(anyextension)withnocontent, simplestring, integeroraspecial character.