WMC | GLOBAL

WORLDWIDE BRAND AND CUSTOMER PROTECTION AT SCALE

URL SUBMISSION
API DOCUMENTATION

v1.0 08.06.2024

TABLE OF CONTENTS

GETTING STARTED WITH URL SUBMISSION

The URL Submission API allows customers to submit URLs to WMC Global's anti-phishing platform for analysis. The API classifies phishing and collects both victim credentials and phishing kits. With URL Submission, you can:

- Submit URLs for analysis
- Retrieve threat intelligence about phishing attacks from the Phishfeed API
- Retrieve victim information from the Compromised Credential Recovery API
- Compare phishing kits via the KITIntel API

DOCUMENT STATUS

This document supports v1.1 for the URL Submission API. The API and documentation are subject to change.

WMC Global Website

URL SUBMISSION DATA DIRECTORY

DATA DICTIONARY INPUT PARAMETERS

PARAMETER NAME	DESCRIPTION	DATA TYPE
x-api-key	User API key; a unique identifier used to authenticate a user issued by WMC Global.	string

DATA DICTIONARY BODY PARAMETERS

PARAMETER NAME	DESCRIPTION	DATA TYPE
urls	Submit up to 10,000 URLs for processing.	array of strings

DATA DICTIONARY OUTPUT PARAMETERS

PARAMETER NAME	DESCRIPTION	DATA TYPE
uuid	The unique submission ID.	integer
received_date	The date and time the submission was received.	string
urls_received	The count of URLs received in the submission.	integer

URL SUBMISSION RESPONSES

BASE URL: api.phishfeed.com/submissions/v1

SCHEME: HTTPS

API: POST /submit-url

CONTENT TYPE: application/JSON

Sample Query

JSON

```json
{
  "urls": [
    "http://www.example.com"
  ]
}
```

Responses

RESPONSE CODE	DESCRIPTION
202	success

JSON

```json
{
  "uuid": "123456",
  "received_date": "YYYY-mm-ddTHH:MM:SSZ",
  "urls_received": 987
}
```

RESPONSE CODE	DESCRIPTION
401	bad_api_key

JSON

```
{
  "errors": [
    {
      "code": 1000,
      "data": null,
      "message": "Invalid username or password"
    }
  ]
}
```

URL DETECTION: UNSUPPORTED MEDIA

Unsupported MIME types

Some URLs lead to certain content that cannot be processed for phishing due to the nature of its format. "Multipurpose Internet Mail Extensions" or MIME type is a standard that indicates the nature and format of a document, file, or assortment of bytes.

WMC Global phishing detection will process content with text/ MIME type and attempt to process unknown media types.

UNSUPPORTED MIME TYPES AND EXAMPLES

MIME TYPE (Linked to full list)	DESCRIPTION	MEDIA TYPE EXAMPLES
image/	Bitmap, vector still images, and animated image formats.	PNG, JPEG, GIF
audio/	Audio or music data.	MP3, AIFF, WAV, DSD, FLAC, MP4, WMA
video/	Video data or files.	MP4, MOV, AVI, MPEG-4
font/	Font/typeface data.	WOFF, TTF, OTF
application/	Binary data that doesn't fall explicitly into one of the other types.	APK, EXE, JSON, EPUB, ZIP, GZIP, RAR, 27
multipart	A document comprised of multiple component parts, each of which may have its own individual MIME type; or a multipart type may encapsulate multiple files being sent together in one transaction.	Email Attachments
message/	A message that encapsulates other messages.	Forwarded or replied-to message quoting
model/	Model data for a 3D object or scene.	3MF VRML

No type or unknown type	Media with no type set or with a new and unclassified type that phishing detection cannot process.	

FULL TYPE LIST

The current IANA media type list is available at www.iana.org.

ADDITIONAL RESOURCES

Learn more about MIME Types on the Mozilla Developer Network.