**Armchair Analysis.com Webhooks for Developers**

This section explains how the receiver of a webhook should be setup.

Each webhook is a HTTP POST request to the specified URL. The request will include two items:

- A Header which will contain a signature calculated from the secret key for the customer
- A JSON payload

There is no authentication provided by the webhook system, your endpoint must be open, but the signature can be used to verify the request. While the url isn't required to use https, it is recommended over http to be secure.

**Header**

The Header included in the request will be `x-signature`. It will contain a signature calculated from the secret key you received when you subscribed to the webhook alert.
The signature is an HMAC hex digest which is calculated using the sha1 hash algorithm and the secret key. The caller should decode the signature using the data body, as a string, and the secret key. Here is example python code using flask to use the signature to verify the request:

```
secret_token="abc123" # this was provided at the time of webhook subscription
armchair_sig = request.headers.get('x-signature').encode(encoding='UTF-8')
calculated_sig = hmac.new(key.encode(encoding='UTF-8'),
msg=json.dumps(request.get_json(force=True, silent=True)), digestmod=hashlib.sha1).hexdigest()

trusted = hmac.compare_digest(armchair_sig, calculated_sig) # will be True if this message is
trusted, False otherwise
```

This should be used to verify that the request is sent from armchairanalysis.com and not from a third party.

**Payload**

The payload of the request will be a json packet which contains the URL of the file to download. The following is an example payload:

```
{
    "url": "https://armchair-nfl-data-
files.s3.amazonaws.com/proplus/nfl_18.zip?AWSAccessKeyId=ABC&Expires=1541340613&x-amz-security-
token=XYZ"
}
```