

Kampai v1.0

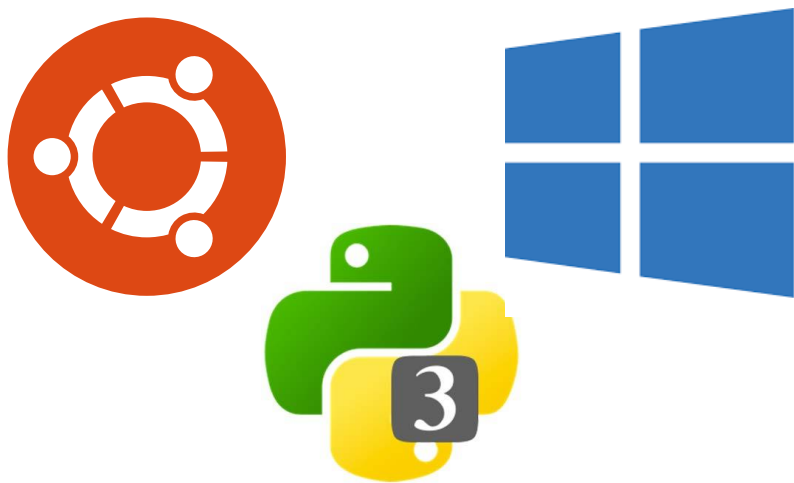
Custom Kenna Connector Utility for Single or Bulk Imports

March 2019



Kampai Development Background

- Kampai was developed with Python3 on a 32bit Ubuntu system
- Current build has been ported Windows for standalone *.exe compatibility



- Kampai.exe v1.0 is 5.7Mb

Key Requirements

- CLI utility that connects to Kenna API with read/write capabilities
- Ability to import a single vulnerability record
- Ability to import multiple vulnerability records from a XLS file
- Handle multiple asset types (IP, Host, URL)

Kampai Syntax and Help on Execution

```
c:\temp>kampai
usage: kampai [-h] [-ip IPADDRESS] [-url URL] [-host HOSTNAME] [-p PORT]
              [-id VULNID] [-fix REMEDIATION] [-s SEVERITY] [-iX EXCEL]
              [-iC CSV] [-createxls] [-d DELETE]

Kampai: Custom Kenna Connector for single or bulk import.

EXAMPLE: kampai.py -id CVE-1999-5656 -ip 10.21.21.21 -p 8080 -s 5 -fix "Upgrade to the latest version"

optional arguments:
  -h, --help            show this help message and exit
  -ip IPADDRESS, --ipaddress IPADDRESS
                        IPADDRESS
  -url URL, --url URL    URL
  -host HOSTNAME, --hostname HOSTNAME
                        HOSTNAME
  -p PORT, --port PORT   PORT
  -id VULNID, --vulnid VULNID
                        Vulnerability identifier. e.g. CVE or CWE
  -fix REMEDIATION, --remediation REMEDIATION
                        Enter context and remediation guidance.
  -s SEVERITY, --severity SEVERITY
                        Integer value. e.g. 6
  -iX EXCEL, --excel EXCEL
                        Specify a filename for bulk import. e.g. kampai_test.xlsx
  -iC CSV, --csv CSV     Specify a CSV filename for bulk import. e.g. records.csv
  -createxls            Create a sample XLSX template for population.
  -d DELETE, --delete DELETE
                        Delete vulnerability record by ID

c:\temp>
```

Kampai CLI Usage (Kampai.exe shown)

- GUI's are for asking, CLI's are for telling
- Easy to distribute (currently 5.7Mb)
- No "installation required"
- Promotes automation and operationalization

Kampai - Single Record Import

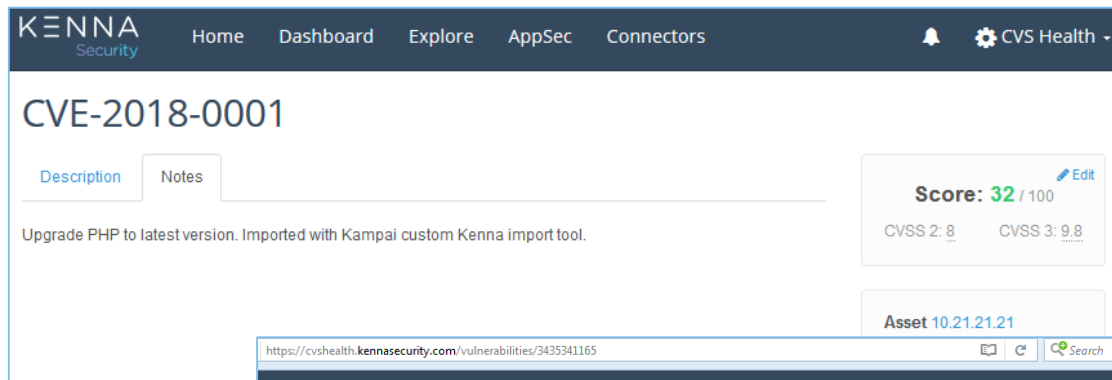
Kampai CLI Syntax for Single Record Imports

```
c:\> kumpai.exe -id CVE-2018-0001 -ip 10.21.21.21 -p 443 -s 9 -fix "Upgrade to the latest version."
```

```
c:\temp>kumpai -id CVE-2018-0001 -ip 10.21.21.21 -p 443 -s 9 -fix "Upgrade PHP to latest version."
{'vulnerability': {'cve_id': 'CVE-2018-0001',
                  'ip_address': '10.21.21.21',
                  'notes': 'Upgrade PHP to latest version. Imported with '
                          'Kumpai custom Kenna import tool.',
                  'port': '443',
                  'primary_locator': 'ip_address',
                  'severity': '9'}}
Import this record into Kenna? Y/n Y
{
  "location": "https://api.kennasecurity.com/vulnerabilities/3435341165",
  "vulnerability": {
    "asset_id": 18375640,
    "client_id": 18461,
    "closed_at": null,
    "closed_by_human": false,
    "created_at": "2019-03-26T23:57:50.000Z",
    "due_date": null,
    "id": 3435341165,
    "notes": "Upgrade PHP to latest version. Imported with Kumpai custom Kenna import tool.",
```

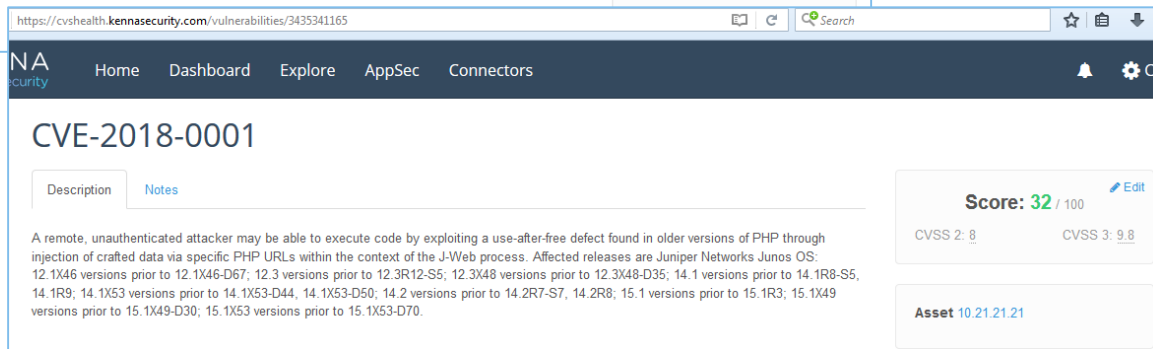
Kampai - Single Record Import

Kampai Web Interface Results



Kenna automatically populates records based on the CVE or CWE provided.

Records are found via their location ID:
<http://cvshealth.kennasecurity.com/vulnerabilities/3435341165>



Kampai - Bulk Record Import

Kampai CLI Syntax for Bulk Record Imports

	A	B	C	D	E
1	VulnID	IP Address	Port	Remediation	Severity
2	CWE-253	10.21.21.21	80	Upgrade to the latest release.	7
3	CVE-2001-1473	10.21.21.21	443	Turn off control that contains the vulnerability.	6
4	CVE-2001-0400	10.21.21.21	1044	Install patch x95950	5
5	CWE-105	10.21.21.21	443	Ensure that you validate all form fields. If a field is unused, it is still important to constrain it so that it is empty or undefined.	5
6	CVE-2017-1000382	10.21.21.21	0	Store swap files in /tmp by default	9
7	CVE-2017-5753	10.21.21.21		Ensure physical security is enforced for the system.	2
8	CWE-327	10.21.21.21	8090	Design the software so that one cryptographic algorithm can be replaced with another.	2

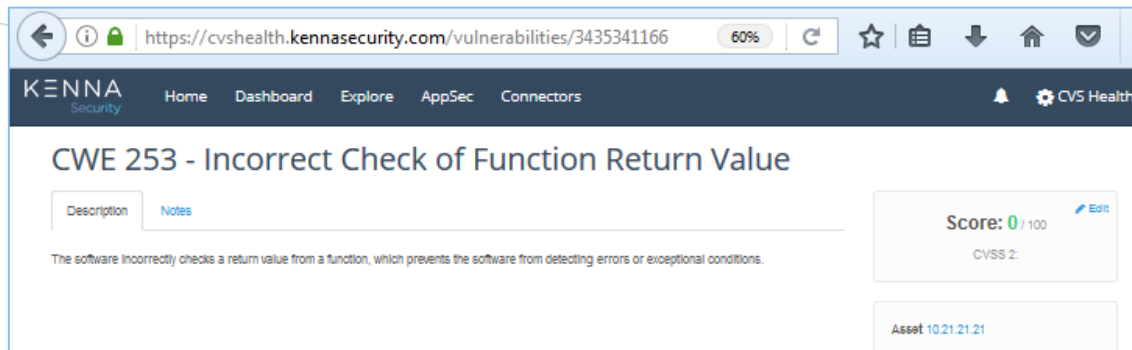
- Resource File: **kampai_xls.xls**

```
c:\> kampai.exe -iX kampai_xls.xls
```

```
Import all records into Kenna? Y/n Y
https://api.kennasecurity.com/vulnerabilities/3435341166
https://api.kennasecurity.com/vulnerabilities/3435341167
https://api.kennasecurity.com/vulnerabilities/3435341168
https://api.kennasecurity.com/vulnerabilities/3435341169
https://api.kennasecurity.com/vulnerabilities/3435341170
https://api.kennasecurity.com/vulnerabilities/3435341171
https://api.kennasecurity.com/vulnerabilities/3435341172
c:\temp>
```

Kampai - Bulk Record Import

Kampai Web Interface Results for Bulk Imports (showing 2/7)

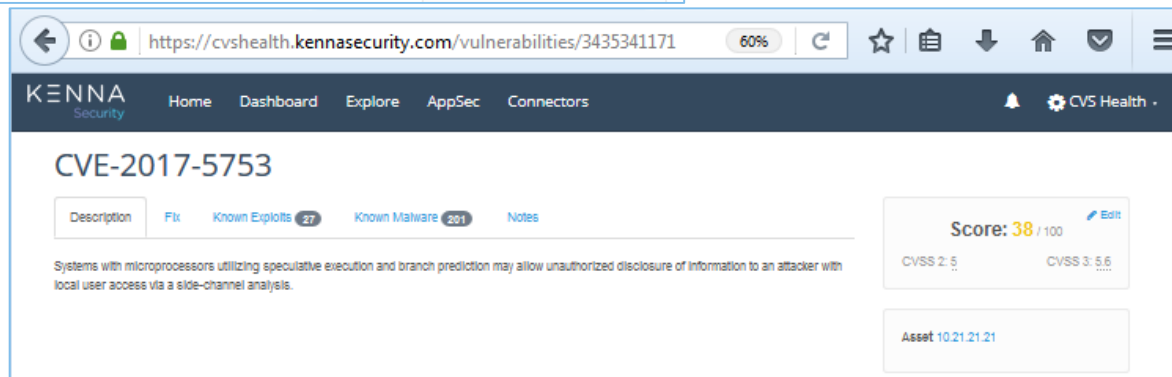


Kenna automatically populates records based on the CVE or CWE provided.

Records are found via their location ID:

<https://cvshealth.kennasecurity.com/vulnerabilities/3435341166>

<https://cvshealth.kennasecurity.com/vulnerabilities/3435341171>



Kampai – Additional Features

Kampai Generate XLS Template for Bulk Importing

```
c:\> kumpai.exe -createxls
```

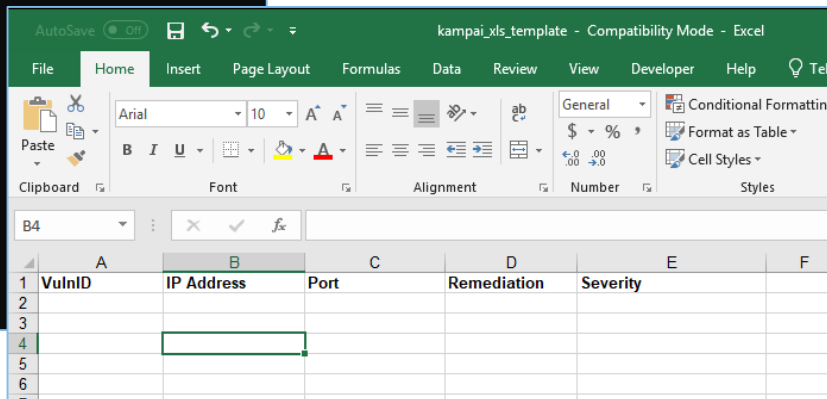
```
c:\temp>kumpai -createxls
Kumpai Template File kumpai_xls_template.xls created.

c:\temp>dir
Volume in drive C is Windows
Volume Serial Number is 4AE6-EB12

Directory of c:\temp

03/26/2019  05:43 PM    <DIR>          .
03/26/2019  05:43 PM    <DIR>          ..
03/26/2019  04:12 PM             5,847,324  kumpai.exe
03/26/2019  05:29 PM             25,600    kumpai_xls.xls
03/26/2019  05:43 PM              5,632  kumpai_xls_template.xls
               3 File(s)      5,878,556 bytes
               2 Dir(s)  1,783,781,928,960 bytes free

c:\temp>
```




The screenshot shows the Microsoft Excel interface with the file 'kumpai_xls_template - Compatibility Mode - Excel'. The ribbon includes File, Home, Insert, Page Layout, Formulas, Data, Review, View, Developer, Help, and Tell. The Home ribbon is active, showing options for Clipboard, Font, Alignment, Number, and Styles. The spreadsheet grid shows columns A through F. The first row (row 1) contains the following headers: A1: VulnID, B1: IP Address, C1: Port, D1: Remediation, E1: Severity, F1: (empty). The second row (row 2) is empty. The third row (row 3) is empty. The fourth row (row 4) is empty. The fifth row (row 5) is empty. The sixth row (row 6) is empty. The seventh row (row 7) is empty.

	A	B	C	D	E	F
1	VulnID	IP Address	Port	Remediation	Severity	
2						
3						
4						
5						
6						
7						

Kampai – Looking Forward

Kampai v2.0's Upcoming Features

- 
- Vulnerability lookup by IP, Hostname, URL
 - Delete vulnerability record by location ID
 - Import/Status/Session HTML Report
 - Various bug-fixes and aesthetic changes

As well as implementing feature requests from you.

Kampai – Demo

Questions?