

# Nessus ? OWASP ZAP

В KUMA можно импортировать сведения об активах из отчетов о результатах сканирования устройств с помощью Nessus, OWASPZAP, системы контроля защищенности и соответствия стандартам. Импорт происходит через API с помощью утилиты `import_asset_Nessus_OWASP.py` (скрипт находится в Community-Pack в папке Assets [ссылка доступна из [Дисклеймера](#)]). Импортированные активы отображаются в веб-интерфейсе KUMA в разделе Активы. При необходимости вы можете редактировать параметры активов.

## ???????????????????? ???? ? KUMA

Создайте пользователя с ролью **главный администратор** со следующими **правами доступа для API**:

- GET /tenants
- GET /users/whoami
- POST /assets/import

## Пользователь

### Права доступа через API

Выключен

\*Имя  
asset-api

\*Логин  
asset-api

\*Адрес электронной почты  
asset-api@lo.cal

Получать уведомления по п

Скрывать ресурсы из обще

Может взаимодействовать

Получать уведомления о со

Группа главных администра

Доступ к объектам КИИ

**Взаимодействие с KUMA чере**

Сгенерировать токен

Изменить пароль

GET /activeLists	<input type="checkbox"/>
GET /alerts	<input type="checkbox"/>
GET /assets	<input type="checkbox"/>
GET /dictionaries	<input type="checkbox"/>
GET /events/clusters	<input type="checkbox"/>
GET /resources	<input type="checkbox"/>
GET /resources/download/id	<input type="checkbox"/>
GET /services	<input type="checkbox"/>
GET /settings/id/id	<input type="checkbox"/>
GET /system/backup	<input type="checkbox"/>
GET /tenants	<input checked="" type="checkbox"/>
GET /users/whoami	<input checked="" type="checkbox"/>
POST /activeLists/import	<input type="checkbox"/>
POST /alerts/close	<input type="checkbox"/>
POST /assets/delete	<input type="checkbox"/>
POST /assets/import	<input checked="" type="checkbox"/>
POST /dictionaries/update	<input type="checkbox"/>
POST /events	<input type="checkbox"/>
POST /resources/export	<input type="checkbox"/>
POST /resources/import	<input type="checkbox"/>
POST /resources/toc	<input type="checkbox"/>
POST /resources/upload	<input type="checkbox"/>
POST /system/restore	<input type="checkbox"/>

Сохранить

Сохраните настройки, **сгенерируйте токен** и отдельно сохраните его, например, в каком-либо текстовом редакторе. Нажмите **Сохранить**.

Добавьте **дополнительно поле** с названием «Description» в разделе **Параметры - Активы - Пользовательские атрибуты**.

# АКТИВЫ

Подробнее о пользовательских полях активов см. [в онлайн-справке](#).

При удалении настраиваемых полей также удаляются содержащиеся в них данные.

## Пользовательские атрибуты

Название

Маска (регулярное выражение, RE2)

Значение по умолчанию



Description



**Сохраните** изменения.

# ?????? ???? ?? Nessus

Пример отчета от Nessus в формате CSV:

```
Plugin ID,CVE,CVSS v2.0 Base
Score,Risk,Host,Protocol,Port,Name,Synopsis,Description,Solution,See Also,Plugin Output,STIG
Severity,CVSS v3.0 Base Score,CVSS v2.0 Temporal Score,CVSS v3.0 Temporal Score,VPR Score,Risk
Factor,BID,XREF,MSKB,Plugin Publication Date,Plugin Modification Date,Metasploit,Core
Impact,CANVAS
"70658","CVE-2008-5161","2.6","Low","1.2.3.9","tcp","22","SSH Server CBC Mode Ciphers
Enabled","The SSH server is configured to use Cipher Block Chaining.","The SSH server is
configured to support Cipher Block Chaining (CBC)encryption. This may allow an attacker to
recover the plaintext messagefrom the ciphertext.Note that this plugin only checks for the
options of the SSH server anddoes not check for vulnerable software versions.","Contact the
vendor or consult product documentation to disable CBC modecipher encryption, and enable CTR
or GCM cipher mode encryption.",,"The following client-to-server Cipher Block Chaining (CBC)
algorithmsare supported:3des-cbcaes128-cbcaes192-cbcaes256-cbcblowfish-cbcast128-cbcThe
following server-to-client Cipher Block Chaining (CBC) algorithmsare supported:3des-cbcaes128-
cbcaes192-cbcaes256-cbcblowfish-cbcast128-
cbc",,"","1.9",,"","2.5","Low","32319","CERT:958563;CWE:200",,"","2013/10/28","2018/07/30",,"
",,""
```

Далее необходимо хапустить скрипт `import_asset_Nessus_OWASP.py` по этому отчету указав необходимые параметры для его корректного запуска. Возможные опции скрипта:

```
# python import_asset.py --help
usage: import_asset.py [-h] --kuma KUMA --token TOKEN --tenant TENANT --vendor
{Nessus,OWASPZAP} --filepath FILEPATH
```

options:

-h, --help	show this help message and exit
--kuma KUMA	IP адрес сервера KUMA
--token TOKEN	Токен API
--tenant TENANT	Имя Тенанта
--vendor {Nessus,OWASPZAP}	Наименование вендора
--filepath FILEPATH	Путь до отчета

Пример запуска по отчету Nessus:

```
python3 import_asset_Nessus_OWASP.py --kuma 10.68.85.126 --token
98417b064c2a5cdfdf6bd011126c6453 --tenant Main --vendor Nessus --filepath
C:\Users\ose\Downloads\nessus.csv
```

В KUMA актив будет выглядеть следующим образом:

The screenshot displays the KUMA interface. On the left, a list of assets is shown with columns for checkboxes, names, and IP addresses. The asset with IP 12.3.9 is selected. On the right, a modal window titled 'Информация об активе' (Asset Information) is open, showing details for the selected asset. The modal includes buttons for 'Удалить' (Delete), 'Изменить' (Edit), and 'Регистрирование KEDR' (KEDR Registration). The asset details include: Name (12.3.9), Tenant (Main), Source (Created manually), Identifier (53dc3630-a855-4308-a5e8-92eed8faf0dc), Created (12.12.2023 18:04:45), Last update (12.12.2023 18:18:09), IP address (12.3.9), Owner (asset-api), and Category (Informational resource is not an object of KII). There are also expandable sections for 'Настраиваемые поля' (Custom fields) and 'Другие уязвимости' (Other vulnerabilities), with the latter showing 'SSH Server CBC Mode Ciphers Enabled' and 'CVE 1 : CVE-2008-5161'.

# ?????? ???? ?? OWASP ZAP

Пример отчета от Nessus в формате CSV:

```
{
  "@programName": "OWASP ZAP",
  "@version": "2.13.0",
  "@generated": "Mon, 25 Sep 2023 11:43:20",
  "site": [
    {
      "@name": "https://demo.lab",
      "@host": "demo.lab",
      "@port": "443",
      "@ssl": "true",
      "alerts": [
        {
          "pluginid": "10035",
          "alertRef": "10035",
          "alert": "Strict-Transport-Security Header Not Set",
          "name": "Strict-Transport-Security Header Not Set",
          "riskcode": "1",
          "confidence": "3",
          "riskdesc": "Low (High)",
          "reference": "https://ya.ru",
          "desc": "<p>HTTP Strict Transport Security (HSTS)"
        }
      ]
    }
  ]
}
```

Далее необходимо хапустить скрипт `import_asset_Nessus_OWASP.py` по этому отчету указав необходимые параметры для его корректного запуска. Возможные опции скрипта:

```
# python import_asset.py --help
usage: import_asset.py [-h] --kuma KUMA --token TOKEN --tenant TENANT --vendor
{Nessus,OWASPZAP} --filepath FILEPATH

options:
  -h, --help                show this help message and exit
```

--kuma KUMA	IP адрес сервера KUMA
--token TOKEN	Токен API
--tenant TENANT	Имя Тенанта
--vendor {Nessus,OWASPZAP}	Наименование вендора
--filepath FILEPATH	Путь до отчета

Пример запуска по отчету OWASP ZAP:

```
python3 import_asset_Nessus_OWASP.py --kuma 10.68.85.126 --token
98417b064c2a5cdfdf6bd011126c6453 --tenant Main --vendor OWASPZAP --filepath
C:\Users\ose\Downloads\owasp.json
```

В KUMA актив будет выглядеть следующим образом:

The screenshot displays the KUMA interface. On the left, there is a search bar and a list of assets. The 'demo.lab' asset is selected and highlighted. On the right, a detailed view of the 'demo.lab' asset is shown, including its name, tenant, source, identifier, creation date, last update, owner, and full domain name. A category of 'Informational resource is not an object of KII' is also visible. A section titled 'Configurable fields' shows a description: 'Created on the basis of the OWASP ZAP report system'. A category of 'Categories' is expanded, showing a vulnerability: '10035 в Strict-Transport-Security Header Not Set' with a severity of 'High'.

Revision #5

Created 2023-12-13 10:15:06 UTC by Boris RZR

Updated 2025-12-10 10:42:41 UTC by Boris RZR