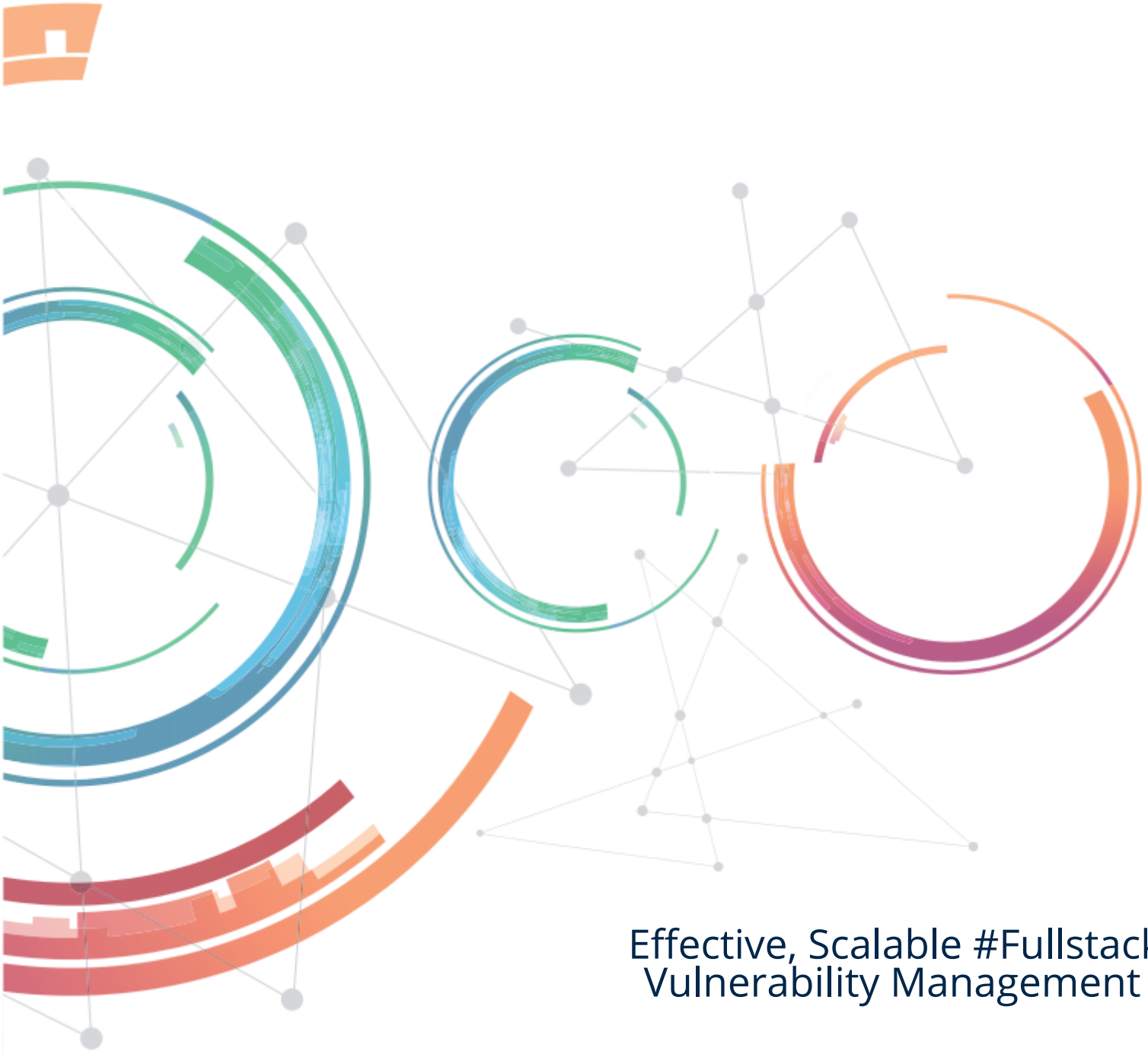
edgescan™

API Guide v1.3



Effective, Scalable #Fullstack
Vulnerability Management

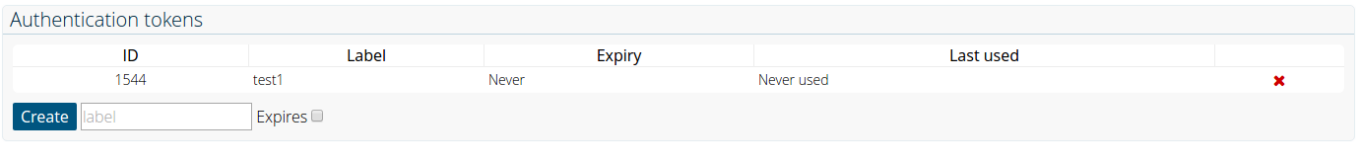
Contents

Edgescan™ API Guide

The edgescan™ API adheres to the REST model. It is available in both XML and JSON formats. The API is accessible through the root URL https://live.edgescan.com/api/.

1 Authentication

1.1 Generating an API token



Clients must authenticate using an API token they generate using the edgescan™ web application. To generate a token, open the edgescan™ user interface and navigate to Config > General.

This page contains a section titled Authentication token (pictured above), which displays a table containing the details of all API tokens previously created, including their label, expiry date and when they were last used.

To create a token, enter a descriptive label in the text box at the bottom of the table and click 'Create', a dialog box will appear showing the generated token. It is important to note that this value is not stored by edgescan™, users are solely responsible for storing the value of any tokens they generate in a secure location. Once this dialog is closed the value of the token will never be displayed again.

Each token is associated with the account of the user who generated it, and has the same permissions as that user.

It's recommended to use a clearly identifiable label for each token to unambiguously identify what it's used for, furthermore it's recommended to generate a different token for each individual service, script, etc. that will use the API.

API tokens can be set to expire on a particular date by checking the 'Expires' checkbox and entering a date. After this date the token will no longer be accepted by the API. Setting an expiry is a good security practice, particularly if the token will be stored somewhere that people other than associated user can access (in a configuration file in a server, for instance).

If a token becomes compromised (e.g. an unauthorised person gains access to it) the API token can be deleted by pressing the red 'x' to the right of the corresponding row in the table. The API will stop accepting the token Immediately after deletion.

1.2 Authenticating API calls

Once an api token has been generated it can be used to authenticate API calls in in two ways:

Using HTTP Basic Authentication, with the token as the password:

```
GET /api/v1/vulnerabilities.json?status=open HTTP/1.1
Host: live.edgescan™.com
Authorization: Basic bXlhcHA6NWQ5MGM3ZWNmNTc0ZDcyOA==
```

This is the preferred method of authentication. A username is not necessary, but it is recommended to set it to something identifiable.

In the HTTP Header: X-API-Token:

```
GET /api/v1/vulnerabilities.json?status=open HTTP/1.1
Host: live.edgescan™.com
X-API-TOKEN: 5d90c7ecf574d728|265
```

This method is not recommended as the header value may be visible in log files.

The token must be supplied with each request.

2 General Usage

The table below gives an overview of the possible actions available for an API endpoint.

Action	HTTP Method	URI	Response Code	Description	Returns
List resources	GET	/resources	200	Successful query	A representation of a list of resources, optionally filtered
			400	Client Error, (e.g. invalid params)	No content, or a description of the error if applicable/possible
			403	Unauthorized	Explanation of authorization failure
Show detailed information about a specific resource	GET	/resources/:id	200	Successful	A representation of the resource with given id
			403	Unauthorized	Explanation of authorization failure
			404	No resource matching id	No content
Create a new resource	POST	/resources	200	Successful creation of resource	A representation of the new resource
			400	Client Error, (e.g. invalid params)	A description of the error(s)
			403	Unauthorized	Explanation of authorization failure
Update an existing resource	PUT	/resources/:id	200	Successful update of resource	A representation of the new state of the resource
			400	Client Error, (e.g. invalid params)	A description of the error(s)
			403	Unauthorized	Explanation of authorization failure
			404	No resource	No content matching id
Delete an existing resource	DELETE	/resources/:id	200	Successful deletion of resource	A representation of the deleted resource
			403	Unauthorized	Explanation of authorization failure
			404	No resource	No content matching id

All api endpoints are prefixed with /api/[version]. The current version is v1, so the vulnerabilities endpoint for example would be:

```
/api/v1/vulnerabilities
```

To specify which data type is expected simply append a format parameter to the url like so:

```
/api/v1/vulnerabilities.json
/api/v1/vulnerabilities.xml
```

The examples given in the remainder of this document will use JSON as expected data type, however all examples will equally work with XML by simply changing the format parameter.

Some endpoints will have child resources. These correspond to resources that are owned by the parent resource. As an example, each vulnerability will have multiple annotation resources. The list of annotations for vulnerability with id 53 can be accessed using the following path:

```
/api/v1/vulnerabilities/53/annotations.json
```

This path can be used to list and create new annotations for that vulnerability. However, given a specific annotation, if you wish to view, edit or delete it you would use the root path as normal:

```
/api/v1/annotations/<id>.json
```

where is the numeric id of the annotation.

To specify filters on the data, append a url parameter to the request like the following:

```
/api/v1/vulnerabilities.json?c[asset_id]=53
```

This will filter the vulnerabilities by the asset_id field. Comparisons besides simple equality can be achieved by appending keywords to the field name. For example to find all vulnerabilities opened after a certain date, use the following:

```
/api/v1/vulnerabilities.json?c[date_opened_after]=25-06-13
```

Possible comparisons are:

Comparison	**Description**
is_null, never	field value is not set
is_not_null	field value is set
less_than, before	field value is less than given value.
greater_than, more_than, after	field value is greater than given value.
like	field value contains the given value as a substring

Some comparisons have multiple aliases to provide better semantics for some queries.

Filters can be chained together by adding further url parameters using the same format.

```
/api/v1/vulnerabilities.json?c[asset_id]=4&c[risk]=3
```

3 Endpoints

This section lists all of the endpoints available in the API.

Resource	Path	Fields	Actions	Subresources

assets	/api/v1/assets	`name`
		`hostname`
		`priority`
		`date_added`
			List
			Show
				vulnerabilities
				annotations
				credentials
				hosts

hosts	/api/v1/hosts	`asset_id`
		`address`
		`label`
		`hostname`
		`status`
			List
			Show
				services

services	/api/v1/services	*none*	List	

vulnerabilities	/api/v1/vulnerabilities	`asset_id`
		`name`
		`layer`
		`location`
		`label`
		`risk`
		`severity`
		`threat`
		`date_opened`
		`date_closed`
		`status`
			List
			Show
				details
				annotations

annotations	/api/v1/annotations	`user_id` `category`	List Show Create	

details	/api/v1/details	`port`
		`protocol`
		`parameter_name`
		`parameter_type`
			Show	

request_responses	/api/v1/request_responses	*none*	Show	

4 Api Examples

This section contains a number of example API calls along with sample responses.

4.1 Assets

List assets

```
GET /api/v1/assets.json
```


```
{
    "assets": [
        {
            "id": 60,
            "name": "edgebank",
            "hostname": "app.edgebank.net",
            "priority": 7,
            "type": "app",
            "authenticated": true,
            "host_count": 1,
            "created_at": "20130905T14:52:50.000Z",
            "updated_at": "20171101T15:02:24.376Z",
            "location_specifiers": [
                {
                    "id": 1,
                    "location": "app.edgebank.net",
                    "location_type": "hostname"
                }
            ],
            "tags": [
                "CriticalAsset",
                "pci"
            ]
        },
        {
            "id": 61,
            "name": "edgenet",
            "hostname": "192.168.3.0/24",
            "priority": 5,
            "type": "net",
            "authenticated": false,
            "host_count": 256,
            "created_at": "20130905T15:31:43.000Z",
            "updated_at": "20171107T15:37:52.661Z",
            "location_specifiers": [
                {
                    "id": 2,
                    "location": "192.168.3.0/24",
                    "location_type": "cidr"
                }
            ],
            "tags": [
                "CriticalAsset",
```

```
                "Internal"
            ]
        },
        {
            "id": 62,
            "name": "edgeapp",
            "hostname": "edgeapp.com",
            "priority": 4,
            "type": "app",
            "authenticated": true,
            "host_count": 1,
            "created_at": "20130905T16:48:41.000Z",
            "updated_at": "20171107T15:21:53.326Z",
            "location_specifiers": [
                {
                    "id": 3,
                    "location": "edgeapp.com",
                    "location_type": "hostname"
                }
            ],
            "tags": [
                "SOXCompliant",
                "pci",
                "Math"
            ]
        }
    ]
}
```


Filtering by exact name

```
GET /api/v1/assets.json?c[name]=edgeapp
```


```
{
    "assets": [
        {
            "id": 62,
            "name": "edgeapp",
            "hostname": "edgeapp.com",
            "priority": 4,
            "type": "app",
            "authenticated": true,
            "host_count": 1,            "created_at": "20130905T16:48:41.000Z",
            "updated_at": "20171107T15:21:53.326Z",
            "location_specifiers": [
                {
                    "id": 3,
                    "location": "edgeapp.com",
                    "location_type": "hostname"
                }
            ],
            "tags": [
                "SOXCompliant",
                "pci",
                "Math"
            ]
```

```
        }
    ]
}
```

Filtering by location specifier, fuzzy matching

```
GET /api/v1/assets.json?c[location_like]=192.168

{
    "total": 1,
    "count": 1,
    "assets": [
        {
            "id": 61,
            "name": "edgenet",
            "hostname": "192.168.3.0/24",
            "priority": 5,
            "created_at": "20130905T15:31:43.000Z",
            "updated_at": "20141209T12:33:34.000Z",
            "location_specifiers": [
              {
                "id": 2,
                "location": "192.168.3.0/24",
                "location_type": "cidr"
              }
            ],
            "tags": [
                "CriticalAsset",
                "Internal"
            ]
        }
    ]
}
```

Filtering using comparisons

```
GET /api/v1/assets.json?c[priority_greater_than]=4

{
    "total": 2,
    "count": 2,
    "assets": [
        {
            "id": 60,
            "name": "edgebank",              "hostname": "app.edgebank.net",
            "priority": 6,
            "created_at": "20130905T14:52:50.000Z",
            "updated_at": "20150121T09:48:44.000Z",
            "location_specifiers": [
                {
                    "id": 1,
                    "location": "app.edgebank.net",
                    "location_type": "hostname"
                }
```

```
            ],
            "tags": [
                "CriticalAsset",
                "pci"
            ]
        },
        {
            "id": 61,
            "name": "edgenet",
            "hostname": "192.168.3.0/24",
            "priority": 5,
            "created_at": "20130905T15:31:43.000Z",
            "updated_at": "20141209T12:33:34.000Z",
            "location_specifiers": [
              {
                "id": 2,
                "location": "192.168.3.0/24",
                "location_type": "cidr"
              }
            ],
            "tags": [
                "CriticalAsset",
                "Internal"
            ]
        }
    ]
}
```


Update priority

```
PUT /api/v1/asset.json/61.json
{
  "asset": {
    "priority": 4
  }
}
```


```
{
    "asset": {
        "id": 61,
        "name": "edgenet",
        "hostname": "54.171.25.64/27, 52.210.85.8/29, 185.58.18.16/28",
        "priority": 5,
        "type": "net",
        "authenticated": false,
        "host_count": 56,
        "created_at": "20130905T15:31:43.000Z",
        "updated_at": "20171107T15:37:52.661Z",
        "location_specifiers": [            {
                "id": 2,
                "location": "54.171.25.64/27",
                "location_type": "cidr"
            },
            {
                "id": 29,
                "location": "52.210.85.8/29",
```

```
                "location_type": "cidr"
            },
            {
                "id": 30,
                "location": "185.58.18.16/28",
                "location_type": "cidr"
            }
        ],
        "tags": [
            "CriticalAsset",
            "Internal"
        ],
        "assessments": [...],
        "schedule": [],
        "assessment_count": 11,
        "permissions": [
            "view",
            "edit"
        ]
    }
}
```


4.2 Vulnerabilities

Vulnerability index endpoint, filtered by asset_id

```
GET /api/v1/vulnerabilities.json?c[asset_id]=61
```


```
{
    "total": 25,
    "count": 25,
    "vulnerabilities": [
        {
            "id": 21620,
            "name": "Unencrypted Telnet Server",
            "definition_id": 53,
            "asset_id": 61,
            "severity": 2,
            "threat": 4,
            "risk": 2,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140605T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
            "location": "192.168.3.97",
            "label": null,
            "layer": "Network"
        },
        {            "id": 21621,
            "name": "SSH Server CBC Mode Ciphers Enabled",
            "definition_id": 25,
            "asset_id": 61,
```

```
            "severity": 1,
            "threat": 1,
            "risk": 1,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140905T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
            "location": "192.168.3.97",
            "label": null,
            "layer": "Network"
        }
    ]
}
```


Vulnerability index endpoint, multiple asset_ids

```
GET /api/v1/vulnerabilities.json?c[asset_id_in]=61 ,62
```


```
{
    "total": 25,
    "count": 25,
    "vulnerabilities": [
        {
            "id": 21620,
            "name": "Unencrypted Telnet Server",
            "definition_id": 53,
            "asset_id": 61,
            "severity": 2,
            "threat": 4,
            "risk": 2,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140605T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
            "location": "192.168.3.97",
            "label": null,
            "layer": "Network"
        },
        {
            "id": 21621,
            "name": "Crosssite Scripting (Reflected)",
            "definition_id": 25,
            "asset_id": 62,
            "severity": 4,
            "threat": 5,
            "risk": 5,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140905T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
            "location": "edgeapp.net/index.html",
            "label": null,              "layer": "Application"
        },
```

```
            ...
        ]
    }
```

Complex query, show vulnerabilities on asset id 61, opened before 7th June 2014, with name that contains 'SSL', with risk greater than 1

```
GET /api/vulnerabilities?c[asset_id]=61&c[date_opened_before]=201406
07&c[name_like]=SSL&c[risk_greater_than]=1

{
    "total": 1,
    "count": 1,
    "vulnerabilities": [
        {
            "id": 21641,
            "name": "SSL Weak Cipher Suites Supported",
            "definition_id": 8,
            "asset_id": 61,
            "severity": 2,
            "threat": 2,
            "risk": 2,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140605T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
            "location": "192.168.3.113",
            "label": null,
            "layer": "Network"
        }
    ]
}
```

Show vulnerabilities on a specific host

```
GET /api/v1/vulnerabilities.json?c[asset_id]=61&c[location]=192.168.3.114
{
    "total": 9,
    "count": 9,
    "vulnerabilities": [
        {
            "id": 21632,
            "name": "Tomcat 4.1 XSS",
            "definition_id": 56,
            "asset_id": 61,
            "severity": 3,
            "threat": 4,
            "risk": 3,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140605T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
```

```
            "location": "192.168.3.114",
            "label": null,              "layer": "Network"
        },
        {
            "id": 21633,
            "name": "Apache Tomcat servlet/JSP container default files",
            "definition_id": 18,
            "asset_id": 61,
            "severity": 2,
            "threat": 1,
            "risk": 1,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140905T15:42:03.000Z",
            "date_closed": null,
            "status": "open",
            "location": "192.168.3.114",
            "label": null,
            "layer": "Network"
        },
        ...
    ]
}
```


Limit results

```
GET /api/v1/vulnerabilities.json?c[asset_id]=62&limit=1
```

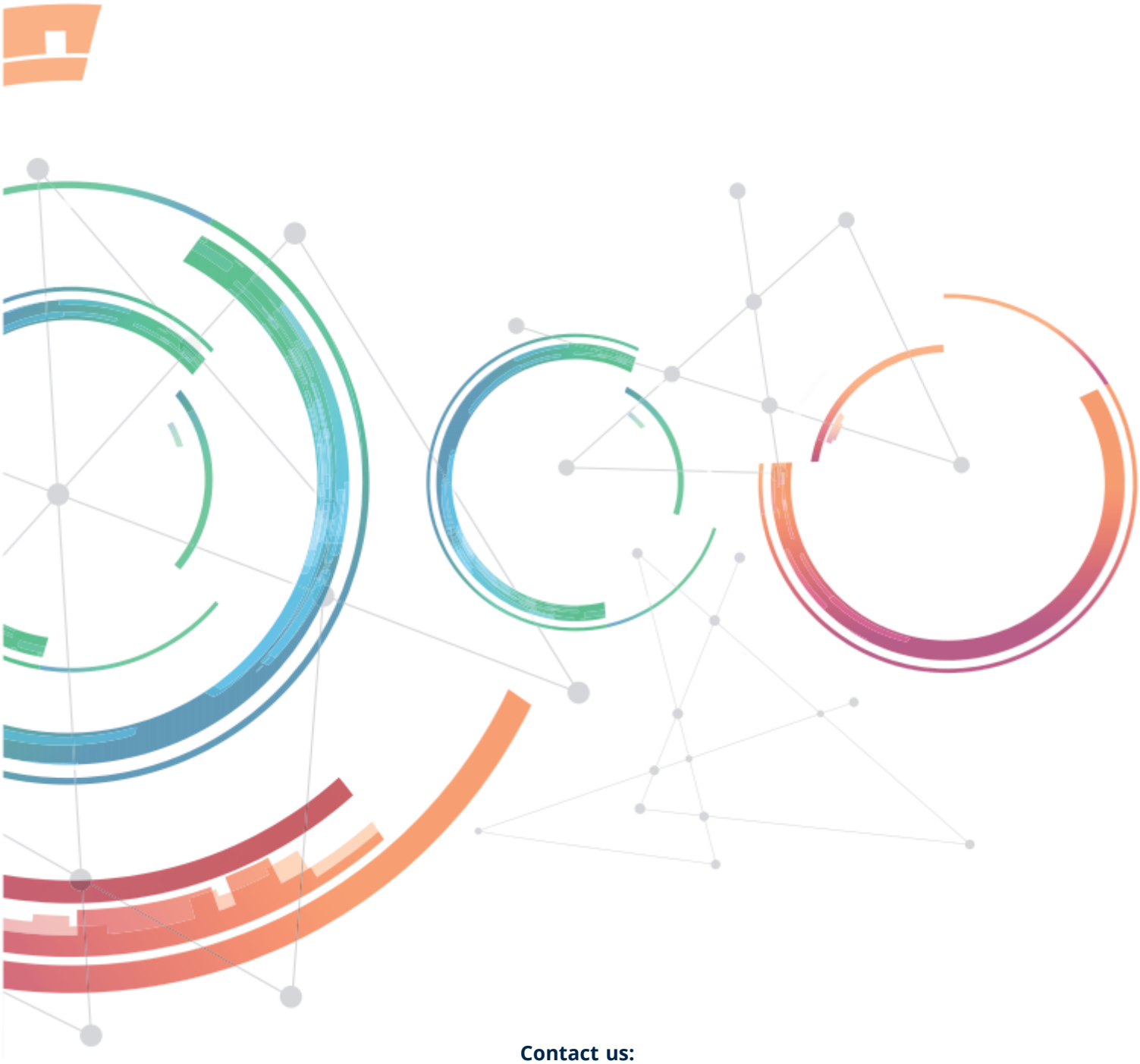

```
{
    "total": 68,
    "count": 1,
    "vulnerabilities": [
        {
            "id": 21645,
            "name": "Crosssite scripting (reflected)",
            "definition_id": 66,
            "asset_id": 62,
            "severity": 4,
            "threat": 5,
            "risk": 5,
            "cvss_score": 0,
            "cvss_vector": null,
            "date_opened": "20140805T16:50:12.000Z",
            "date_closed": null,
            "status": "open",
            "location": "http://edgeapp.com/newsnippet2",
            "label": "",
            "layer": "application"
        }
    ]
}
```


Show vulnerability detail

```
GET /api/v1/vulnerabilities/21645.json

{
  "vulnerability": {
    "id": 21645,
    "name": "Crosssite scripting (reflected)",    "definition_id": 66,
    "asset_id": 62,
    "severity": 4,
    "threat": 4,
    "risk": 4,
    "cvss_score": 6.1,
    "cvss_vector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N",
    "cvss_v2_score": 6.4,
    "cvss_v2_vector": "AV:N/AC:L/Au:N/C:P/I:P/A:N",
    "cvss_version": 3,
    "date_opened": "20140805T16:50:12.000Z",
    "date_closed": null,
    "status": "open",
    "location": "http://edgeapp.com/newsnippet2",
    "label": null,
    "layer": "application",
    "updated_at": "20180109T17:06:48.806Z",
    "created_at": "20140805T16:50:12.000Z",
    "fingerprint": "2829228661530831711",
    "details": [
      {
        "id": 12345,
        "type": "attack_vector",
        "port": null,
        "protocol": null,
        "original_detail_hash": "",
        "parameter_name": "snippet_id",
        "parameter_type": "parameter",
        "html": "<p>The value of the <strong>snippet_id</strong> request
parameter is copied into a JavaScript string which is encapsulated in double
quotation marks.",
        "src": "The value of the **snippet_id** request parameter is copied into
a JavaScript string which is encapsulated in double quotation marks."
      }
    ]
  }
}
Show vulnerability definition
GET /api/v1/vulnerabilities/21645/definition.json
{
  "definition": {
    "id": 66,
    "name": "Crosssite scripting (reflected)",
    "layer": 7,
    "risk": 4,
    "severity": 4,
    "threat": 4,
    "cvss_score": 6.1,
    "cvss_vector": "CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N",
    "cvss_v2_score": 6.4,
    "cvss_v2_vector": "AV:N/AC:L/Au:N/C:P/I:P/A:N",
```

```
    "cvss_version": 3,
    "remediation": "<p>Description of what XSS is</p>",
    "description": "<p>Use strict contextual escaping</p>"
  }
}
```



Contact us:

IRL: +353 (0) 1 6815330
UK: +44 (0) 203 769 0963
US: +1 646 630 8832

sales@edgescan.com
www.edgescan.com
www.bccriskadvisory.com

edgescan