OWASP DEF (Data Exchange Format)

This document will describe the OWASP-DEF Dynamic format in detail.

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| OWASP-DEF | | This is the Root of the format |
| **Attribute Name** | | **Description** |
| SpecVersion | | This is the current version of the OWASP-DEF Format |
|  | **Data Type** | String |
| **Example** | | |
| <DEF SpecVersion=*"0.1"*> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| Sesseion-Reference | | This is a Session Reference Unique for this session |
|  | **Data Type** | String |
| **Example** | | |
| <Session-Reference>Scan specific reference</Session-Reference> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| Date-Time | | This is the Date and Time stamp of when the session was started |
|  | **Data Type** | DateTime |
| **Example** | | |
| <Date-Time>Date and time the session was started</Date-Time> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| Scan | | This defines the Scan type contained in this section |
| **Attribute Name** | | **Description** |
| type | | This can be either **dynamic**, **info** or **static**.  dynamic is used for all Dynamic web application analyzers.  info is used for all Information gathering software.  static is used for all Static code analyzers. |
|  | **Data Type** | String |
| **Example** | | |
| <Scan type=*"dynamic"*> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and info |
| **Name** | | **Description** |
| Host | | This is the Host section |
| **Attribute Name** | | **Description** |
| name | | This is the Host Name of the Target that was analyzed, or used as the base for the information gathering. |
|  | **Data Type** | String |
| ip-address | | This is the IP Address of the Host, this can be either the IPv4 or IPv6 address. |
|  | **Data Type** | String |
| **Example** | | |
| **<Host name=*"Hostname"* ip-address=*"Either IPv4 or IPv6 Address"*>** | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and info |
| **Name** | | **Description** |
| Port | | This is the Port section |
| **Attribute Name** | | **Description** |
| protocol | | This is the Protocol used for the communication, either TCP or UDP |
|  | **Data Type** | String |
| portid | | This is the Port Number |
|  | **Data Type** | Integer |
| **Example** | | |
| <Port protocol=*"The Protocol used"* portid=*"The Port Number"*> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and info |
| **Name** | | **Description** |
| Service | | This is the Service section |
| **Attribute Name** | | **Description** |
| name | | This is the name of the Service. |
|  | **Data Type** | String |
| product | | This is the detected product running the service. |
|  | **Data Type** | String |
| version | | This is the detected Product Version running the service. |
|  | **Data Type** | String |
| **Example** | | |
| <Service name=*"Name of the Service"* product=*"Product Name"* version=*"Product Version"* /> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| Software-Name | | This is the Software-Name Section, and this is for the Name of the software that did the scan |
|  | **Data Type** | String |
| **Example** | | |
| <Software-Name>Name of the tool that found the issue</Software-Name> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| Software-Version | | This is the Software-Version Section, and this is for the Version of the software that did the scan |
|  | **Data Type** | String |
| **Example** | | |
| <Software-Version>Version of the tool that found the issue</Software-Version> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | All |
| **Name** | | **Description** |
| Software-Arguments | | This is the Software-Arguments Section, and this is for the Arguments for the software that did the scan |
|  | **Data Type** | String |
| **Example** | | |
| <Software-Arguments>Arguments used to perform the scan</Software-Arguments> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Vulnerability | | This is the Vulnerability Section. |
| **Attribute Name** | | **Description** |
| Severity | | This is the severity of the vulnerability, and this can be either Critical, High, Medium, Low or Informational, (and Best Practices (At the time of writing this, it is not decided if the latter should be included or not, this is dependent on how many of the software’s that actually uses this)(Note: Should this be converted into a number representation, Critical = 1, High = 2, Medium = 3, Low = 4, Informational = 5, and so on). |
|  | **Data Type** | String |
| **Example** | | |
| <Vulnerability Severity=*"The Severity"*> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Finding | | This is the Finding Section. |
| **Attribute Name** | | **Description** |
| NativeID | | This is for the software native ID of the test that found the vulnerability. |
|  | **Data Type** | Integer (or string?) |
| IdentifiedTimestamp | | This is a DateTime stamp of when this vulnerability was found. |
|  | **Data Type** | DateTime |
| uniqueID | | This is the Unique ID that the software have for this Vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Finding NativeID=*"The internal Test ID"* IdentifiedTimestamp=*"DateTime stamp for when we found this vulnerability"* uniqueID=*"The Software unique ID for this Finding"*> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Summary | | This is the Summary Section, and this is for a short one line summary for the vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Summary>A sort (one line) description</Summary> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Description | | This is the Description Section, and this is for a detailed description of the vulnerability that was found. |
|  | **Data Type** | String |
| **Example** | | |
| <Description>More detailed description</Description> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Confidence | | This is the Confidence Section, and this is for the confidence level that the software have for this vulnerability, and this can be between 0 and 10.  0 = not supplied  10 = very confident in this vulnerability |
|  | **Data Type** | Integer |
| **Example** | | |
| <Confidence>0 thru to 10</Confidence> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Background | | This is the Background Section, and this is for a background description of the vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Background>More info on the type of issue</Background> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Remediation | | This is the Remediation Section, and this is for a remediation description of the vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Remediation>Advise on how to fix the issue</Remediation> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic and static |
| **Name** | **Description** |
| Further-Information | This is the Further-Information Section. |
| **Example** | |
| <Further-Information> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Name** | | **Description** |
| Further-Info | | This is the Further-Info, and this is for further information of the vulnerability, and it could be in this format:  OWASP A1-Injection : https://www.owasp.org/index.php/Top\_10\_2010-A1 |
|  | **Data Type** | String |
| **Example** | | |
| <Further-Info>More information about this specific issue</Further-Info> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic and static |
| **Name** | **Description** |
| Classifications | This is the Classifications Section. |
| **Example** | |
| <Classifications> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic and static |
| **Field Name** | | **Description** |
| Classification | | This is the Classification Section, and this is for classifying the vulnerability, and as an example if we say this vulnerability have an CWE classification, then it could be the Title of that: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |
| **Attribute Name** | | **Description** |
| type | | What is the type of classification, this could be any kind of classification, an example could be CWE. |
|  | **Data Type** | String |
| id | | This is the ID of the classification, and if we take the CWE it could as an example be: CWE-89. |
|  | **Data Type** | String |
| href | | This is the HREF to the classification, and as an example it could be: *http://cwe.mitre.org/data/definitions/89.html* |
|  | **Data Type** | String |
| **Example** | | |
| <Classification type=*"The Classification System"* id=*"Classification ID"* href=*"The URL to the Classification description"*>The Title for the Classification</Classification> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Page | This is the Page Section. |
| **Example** | |
| <Page> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Page-Reference | | This is the Page-Reference, and this is for a Page specific Reference for the vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Page-reference>Product specific reference e.g. Page Title</Page-reference> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| URL | | This is the URL, and this is the URL that the vulnerability was found at. |
|  | **Data Type** | String |
| **Example** | | |
| <URL>The actual URL</URL> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Method | | This is the Method used to find the vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Method>HTTP method (GET, POST, etc)</Method> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| HTTPVersion | | This is the HTTPVersion, and this holds the version of the HTTP communication. |
|  | **Data Type** | String |
| **Example** | | |
| <HTTPVersion>The HTTP Version</HTTPVersion> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| StatusCode | | This is the StatusCode section, and this holds the Status code that the request returned. |
|  | **Data Type** | Integer (or SmallInt) |
| **Example** | | |
| <StatusCode>The HTTP Status code</StatusCode> | | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Language | | This is the Language section, and this hold the information about the detected language of the page / web application. |
|  | **Data Type** | String |
| **Example** | | |
| <Language>The detected Language of the Web Application</Language> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Parameters | This is the Parameters section, and this hold the Parameters used to exploit the and find the vulnerability. |
| **Example** | |
| <Parameters> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Parameter | | This is the Parameter section, and this hold the parameter(s) used to find the vulnerability. |
|  | **Data Type** | String |
| **Example** | | |
| <Parameter>The parameter</Parameter> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Request-Response | This is the Request-Response section, and this hold the Request and Response sent to and from the Web application. |
| **Example** | |
| <Request-Response> | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Request | This is the Request section, and this hold the information about the Request that was sent to the web application. |
| **Example** | |
| <Request> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Request-Raw | | This is the Request-Raw section, and this holds the raw request as it was sent to the Web Application. |
|  | **Data Type** | String |
| **Example** | | |
| <Request-Raw>The RAW HTTP Request</Request-Raw> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Request-Headers | This is the Request-Headers section, and this holds the Headers information. |
| **Example** | |
| <Request-Headers> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Data | | This is the Request-Headers Data section, and this holds the header data. |
|  | **Data Type** | String |
| **Attribute Name** | | **Description** |
| name | | The Name of the header data sent to the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Data name=*"The name of the Header Data"*>The value for the Header Data</Data> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Request-Cookie | This is the Request-Cookie section, and this holds the Cookie information. |
| **Example** | |
| <Request-Cookie> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Data | | This is the Request-Cookie Data section, and this holds the Cookie data. |
|  | **Data Type** | String |
| **Attribute Name** | | **Description** |
| name | | The Name of the header data sent to the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Data name=*"The name of the Cookie Data"*>The value for the Cookie Data</Data> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Additional-RequestData | This is the Additional-RequestData section, and this holds the Additional Request Data. |
| **Example** | |
| <Additional-RequestData> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Data | | This is the Additional-RequestData Data section, and this holds the Additional-RequestData Data. |
|  | **Data Type** | String |
| **Attribute Name** | | **Description** |
| name | | The Name of the header data sent to the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Data name=*"The name of the Additional Data"*>The value for the Additional Data</Data> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Response | This is the Response section, and this holds the Response data. |
| **Example** | |
| <Response> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Response-Raw | | This is the Response-Raw section, and this holds the raw response data as it was received from the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Response-Raw>The RAW HTTP Response</Response-Raw> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Response-Headers | This is the Response-Headers section, and this holds the Headers information. |
| **Example** | |
| <Response-Headers> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Data | | This is the Response-Headers Data section, and this holds the header data. |
|  | **Data Type** | String |
| **Attribute Name** | | **Description** |
| name | | The Name of the header data received from the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Data name=*"The name of the Header Data"*>The value for the Header Data</Data> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Response-Cookie | This is the Response-Cookie section, and this holds the Cookie information. |
| **Example** | |
| <Response-Cookie> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Data | | This is the Response-Cookie Data section, and this holds the Cookie data. |
|  | **Data Type** | String |
| **Attribute Name** | | **Description** |
| name | | The Name of the cookie data received from the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Data name=*"The name of the Cookie Data"*>The value for the Cookie Data</Data> | | |

|  |  |
| --- | --- |
| **Field Description for the OWASP-DEF Format** | |
| **OWASP-DEF Type** | dynamic |
| **Name** | **Description** |
| Additional-ResponseData | This is the Additional-ResponseData section, and this holds the Additional Response Data. |
| **Example** | |
| <Additional-ResponseData> | |

|  |  |  |
| --- | --- | --- |
| **Field Description for the OWASP-DEF Format** | | |
| **OWASP-DEF Type** | | dynamic |
| **Name** | | **Description** |
| Data | | This is the Additional-ResponseData Data section, and this holds the Additional-ResponseData Data. |
|  | **Data Type** | String |
| **Attribute Name** | | **Description** |
| name | | The Name of the additional data received from the web application / server. |
|  | **Data Type** | String |
| **Example** | | |
| <Data name=*"The name of the Additional Data"*>The value for the Additional Data</Data> | | |

All of the above data is then represented in the following XML:

<?xml version=*"1.0"*?>

<DEF SpecVersion=*"0.1"*>

<Session-reference>Product specific reference</Session-reference>

<Date-time>Date and time the session was started</Date-time>

<Scan type=*"dynamic"*>

<Host name=*"Hostname"* ip-address=*"Either IPv4 or IPv6 Address"*>

<Port protocol=*"The Protocol used"* portid=*"The Port Number"*>

<Service name=*"Name of the Service"* product=*"Product Name"* version=*"Product Version"* />

<Software-Name>Name of the tool that found the issue</Software-Name>

<Software-Version>Version of the tool that found the issue</Software-Version>

<Software-Arguments>Arguments used to perform the scan</Software-Arguments>

<Vulnerability Severity=*"The Severity"*>

<Finding NativeID=*"The internal Test ID"* IdentifiedTimestamp=*"DateTime stamp for when we found this vulnerability"* UniqueID=*"The Software unique ID for this Finding"*>

<Summary>A sort (one line) description</Summary>

<Description>More detailed description</Description>

<Confidence>One of an agreed list of values</Confidence>

<Background>More info on the type of issue</Background>

<Remediation>Advise on how to fix the issue</Remediation>

<Further-Information>

<Further-Info>More information about this specific issue</Further-Info>

</Further-Information>

<Classifications>

<Classification type=*"The Classification System"* id=*"Classification ID"* href=*"The URL to the Classification description"*>The Title for the Clasasification</Classification>

</Classifications>

<Page>

<Page-Reference>Product specific reference e.g. Page Title</Page-Reference>

<URL>The UTL that the Vulnerability was found on</URL>

<Method>HTTP method (GET, POST, etc)</Method>

<HTTPVersion>The HTTP Version</HTTPVersion>

<StatusCode>The HTTP Status code</StatusCode>

<Language>The detected Language of the Web Application</Language>

<Parameters>

<Parameter>The parameter the vulnerability was found with</Parameter>

</Parameters>

<Request-Response>

<Request>

<Request-Raw>The RAW HTTP Request</Request-Raw>

<Request-Headers>

<Data name=*"The name of the Header Data"*>The value for the Header Data</Data>

</Request-Headers>

<Request-Cookie>

<Data name=*"The name of the Cookie Data"*>The value for the Cookie Data</Data>

</Request-Cookie>

<Additional-RequestData>

<Data name=*"The name of the Additional Data"*>The value for the Additional Data</Data>

</Additional-RequestData>

</Request>

<Response>

<Reponse-Raw>The RAW HTTP Response</Reponse-Raw>

<Reponse-Headers>

<Data name=*"The name of the Header Data"*>The value for the Header Data</Data>

</Reponse-Headers>

<Reponse-Cookie>

<Data name=*"The name of the Cookie Data"*>The value for the Cookie Data</Data>

</Reponse-Cookie>

<Additional-ResponseData>

<Data name=*"The name of the Additional Data"*>The value for the Additional Data</Data>

</Additional-ResponseData>

<Response-ScreenShot>Base64 Encoded Screen Shot</Response-ScreenShot>

</Response>

</Request-Response>

</Page>

</Finding>

</Vulnerability>

</Port>

</Host>

</Scan>

</DEF>