CVE Compatibility Questionnaire

ORGANIZATION NAME:
Bluedon Information Security Technologies Co., Ltd.

WEBSITE:
https://www.bluedon.com/

Product/Service Basic Information Questions

PRODUCT/SERVICE NAME:
Bluedon Vulnerability Scanning System

PRODUCT/SERVICE VERSION NUMBER:
V2.0

PRODUCT/SERVICE RELEASE DATE:
2009/12/12

PRODUCT/SERVICE TYPE:
Vulnerability Scanning Tool/Hardware

PRODUCT/SERVICE HOME PAGE:
https://www.bluedon.com/security_detail-01-7.html

General Capability Questions

PRODUCT ACCESSIBILITY <CR_2.4>
Provide a short description of how and where your capability is made available to your customers and the public (required):
Our customers and the public can log into the repository of Vulnerability Scanning System to search for vulnerability and related CVE content. Please refer to Figures 1,2,3.

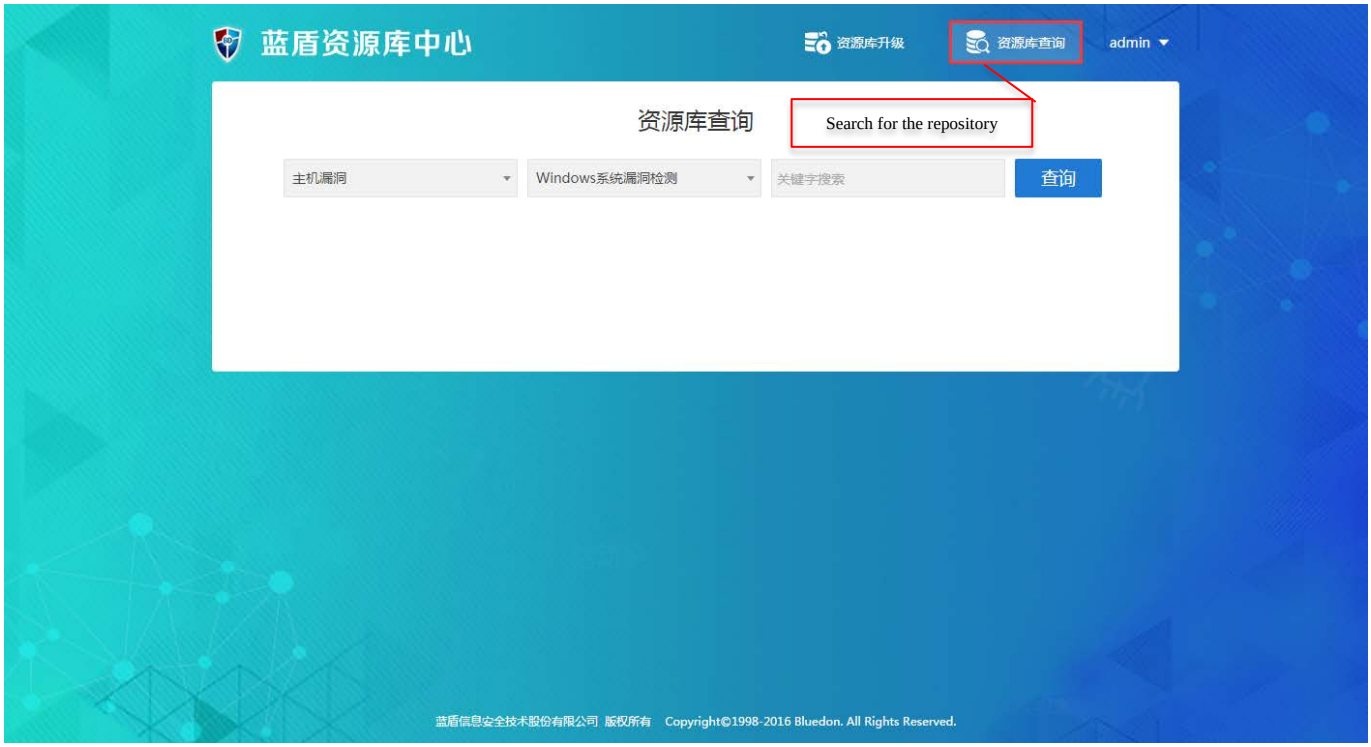


Figure 1

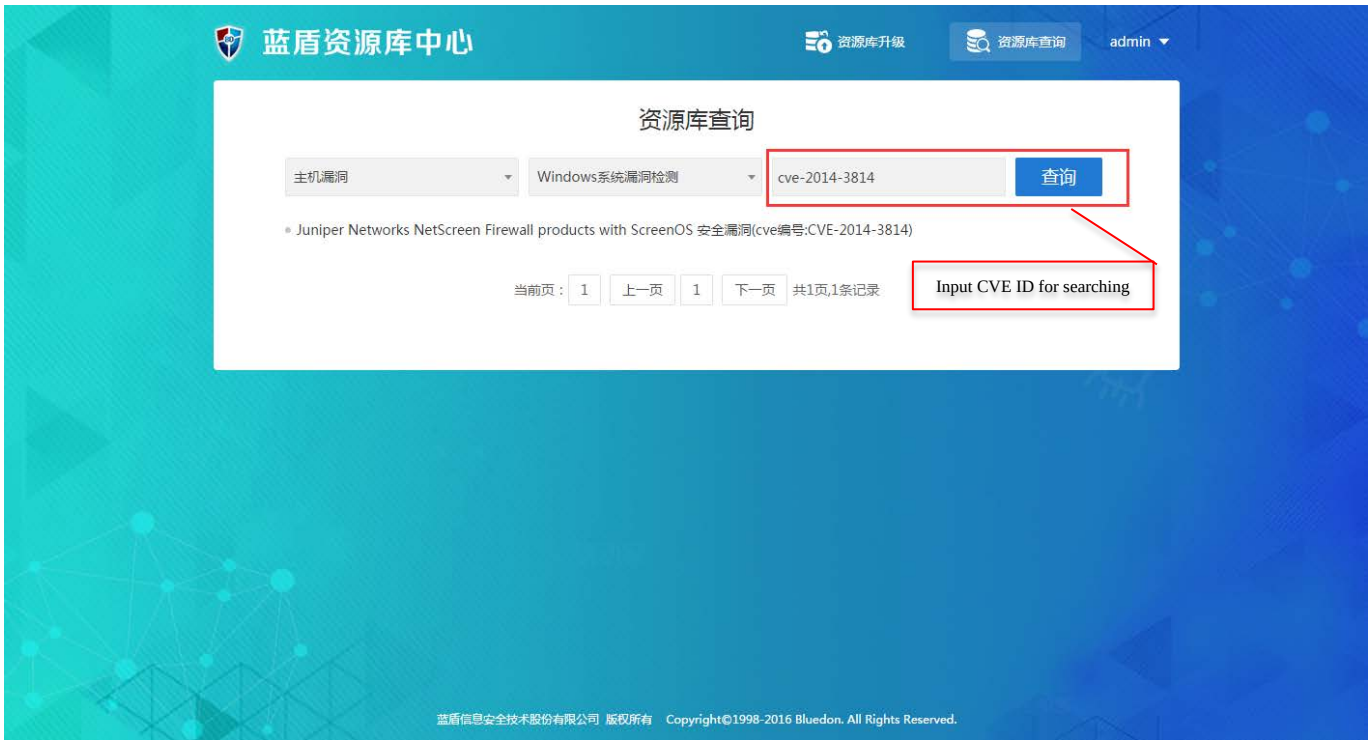


Figure 2

Figure 3

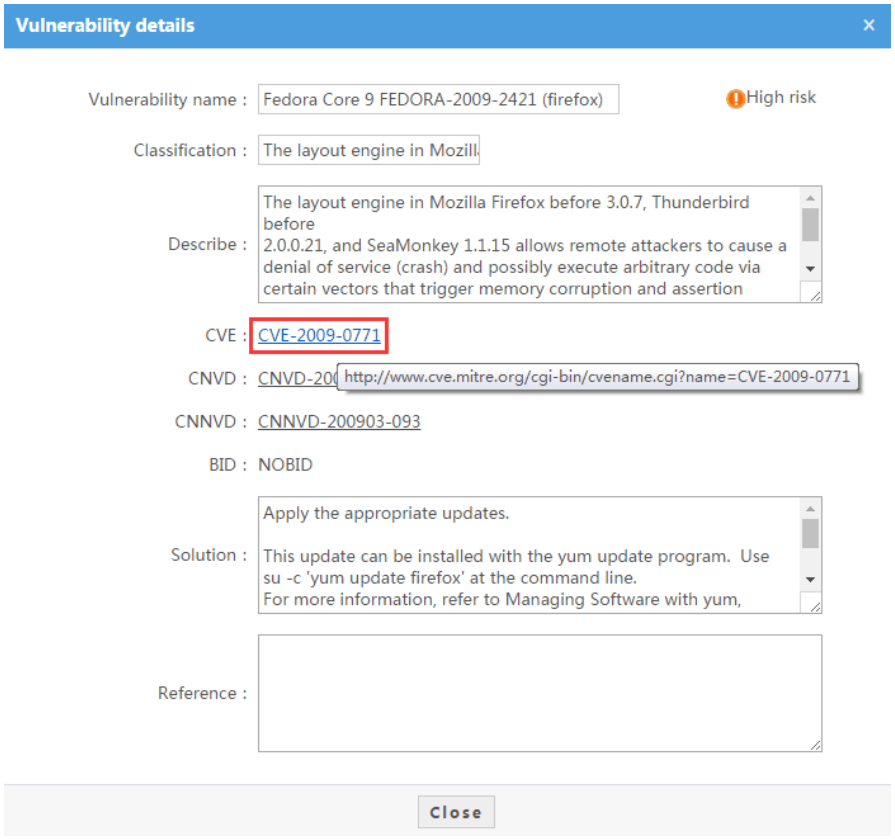
Mapping Questions

MAP CURRENCY INDICATION <CR_5.1>

Describe how and where your capability indicates the most recent CVE content used to create or update its mappings (required):

We have a vulnerability template, in which CVE IDs can be found with description of related vulnerability. Users can also see the newly specific CVE-description on the CVE website by clicking the hyperlink of CVE IDs. Our developer team will update vulnerability database each two weeks. If we find out new vulnerability, we will update the database as soon as possible.

See figure below.



MAP CURRENCY UPDATE APPROACH <CR_5.2>

Indicate how often you plan on updating the mappings to reflect the current CVE content and describe your approach to keeping reasonably current with the CVE content when mapping them to your repository (required):

Our team will update the mappings every two weeks to reflect the current CVE content. For users, they can use the website address http://172.16.10.106/site/list to enter the repository center, and then click “update repository(资源库升级)” to find and download the Update Package. After installing the Update Package, our vulnerability scanning system can be updated. In this way, users can obtain the latest CVE content in our system.

MAP CURRENCY UPDATE TIME <CR_5.3>

Describe how and where you explain to your customers the timeframe they should expect an update of your capability's mappings to reflect newly available CVE content (required):

On the main page of repository center, when users click the “update repository(资源库升级)”, they can find the timeframe that notifies them to download the newly available CVE content.

MAP CONTENT SELECTION CRITERIA <CR_5.4>

Describe the criteria used for determining the relevance of a given CVE Identifier to your Capability (required):

In our Vulnerability Scanning System, the CVE identifiers are determined to map relevant vulnerabilities by our team based on the detection policies and scripts. When a new vulnerability occurs, our team will follow the CVE website and get new CVE ID for our product’s mapping.

MAP CURRENCY UPDATE MECHANISM <CR_5.4>

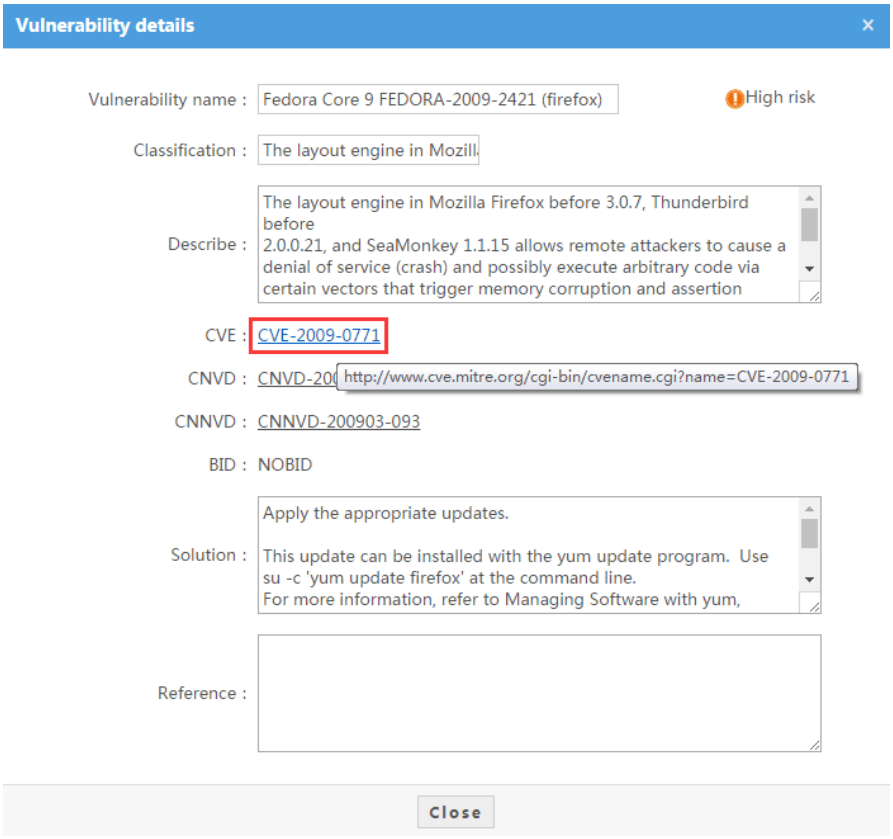
Describe the mechanism used for reviewing CVE for content changes (required):

Our team will follow the updates on the CVE website, and check the official website every week in order to find whether the CVE content has been updated. If there are new CVE updates, we will follow that and update our repository.

MAP CONTENT SOURCE <CR_5.5>

Describe the source of your CVE content (required):

The source of the CVE content for our vulnerability base comes from the CVE website. We get the CVE content from the website. Users can also see the original CVE content through the hyperlink of CVE ID which is shown in the vulnerability details.

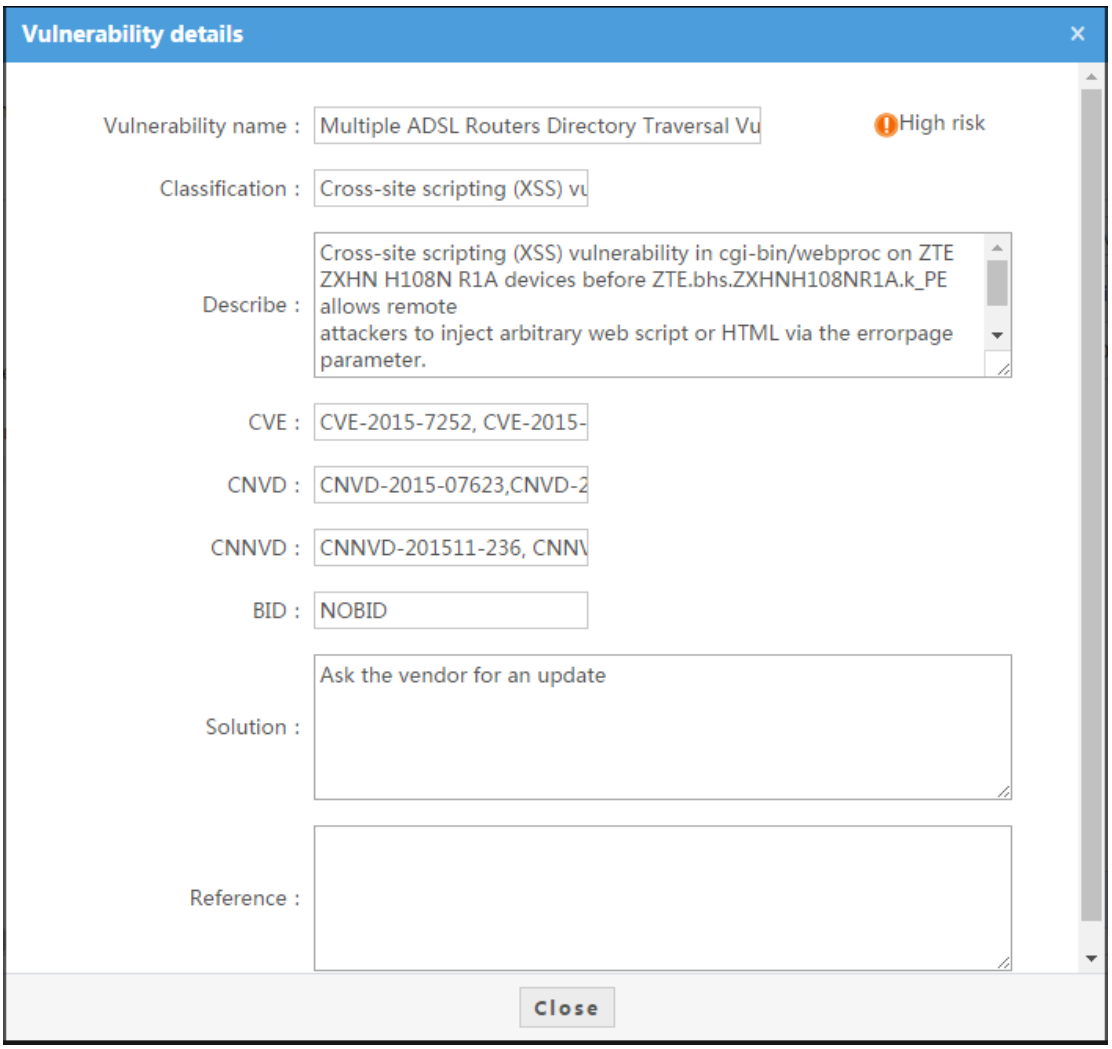


Documentation Questions

CVE AND COMPATIBILITY DOCUMENTATION <CR_4.1>

Provide a copy, or directions to its location, of where your documentation describes CVE and CVE compatibility for your customers (required):

We show our customers the CVE compatibility of our product in the User Manual. CVE description and CVE compatibility can be also shown on a page of vulnerability details.



DOCUMENTATION OF FINDING ELEMENTS USING CVE IDS <CR_4.2>

Provide a copy, or directions to its location, of where your documentation describes the specific details of how your customers can use CVE IDs to find the individual security elements within your capability's repository (required):

The method for users to find elements by using CVE IDs is included in the User Guide:

1. Choose the module “Host” in the drop-down list of “Policies”. Please refer to Figure 1.
2. Click the green button “Add”.
3. Input CVE ID in the searching box in the upper right corner of the pop-up page, relevant security elements that associated with CVE IDs can be found. Please refer to Figure 2.

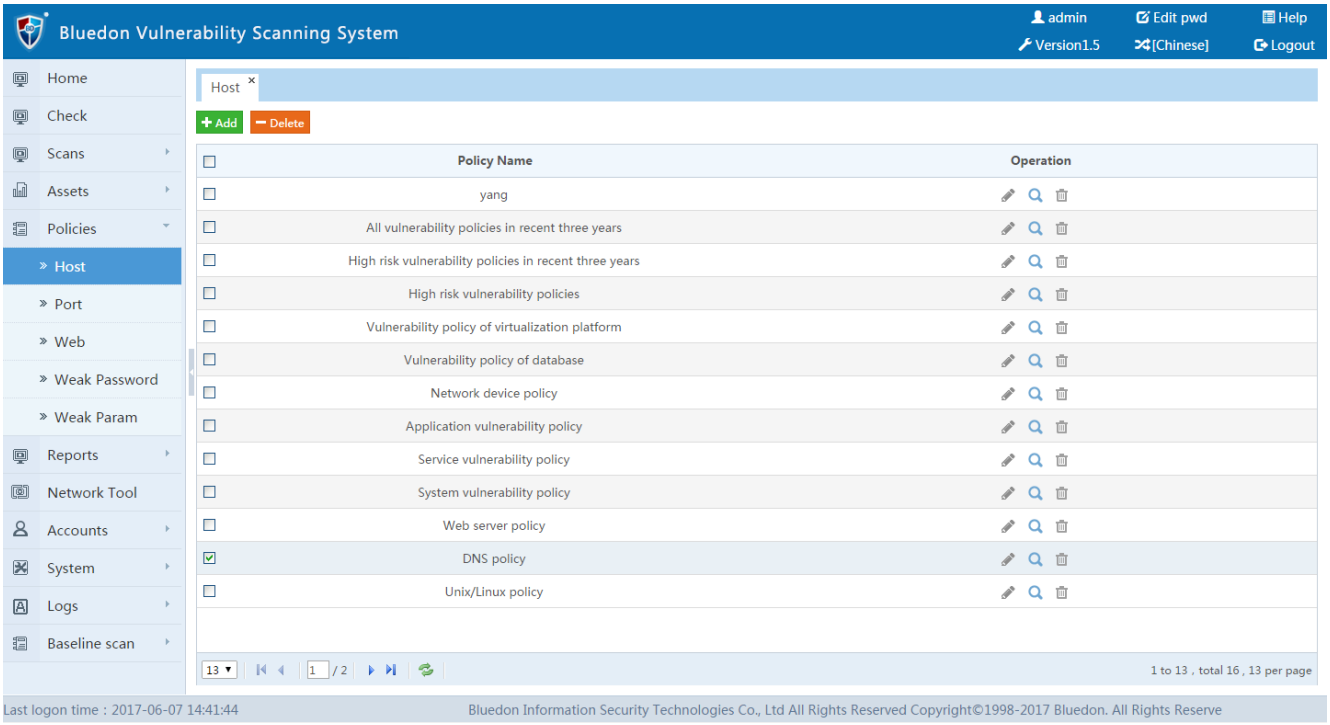


Figure 1

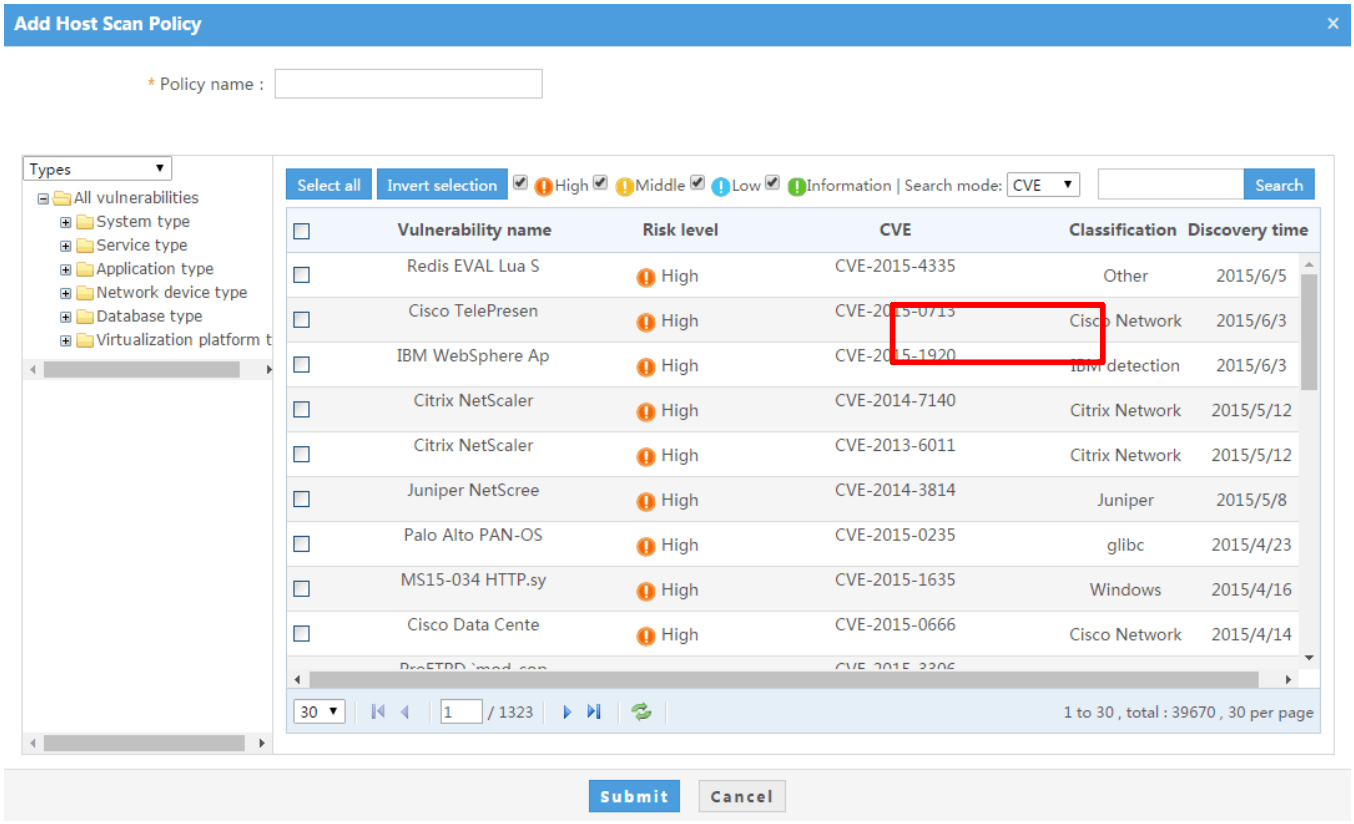


Figure 2

DOCUMENTATION OF FINDING CVE IDS USING ELEMENTS <CR_4.3>

Provide a copy, or directions to its location, of where your documentation describes the process a user would follow to find the CVE IDs associated with individual security elements within your capability's repository (required):

The method for users to find the CVE IDs associated with individual security elements is included in the User Guide.

1. Click “Check” on the left list to find the scanning reports. And then click the icon to show the pop-up page. Please refer to Figure 1.
2. Choose a report of vulnerability to find CVE IDs or users can directly input CVE ID to find the information they want. Besides, users can find related information about the CVE content by clicking the hyperlink of CVE ID. Please refer to Figure 2 and 3.

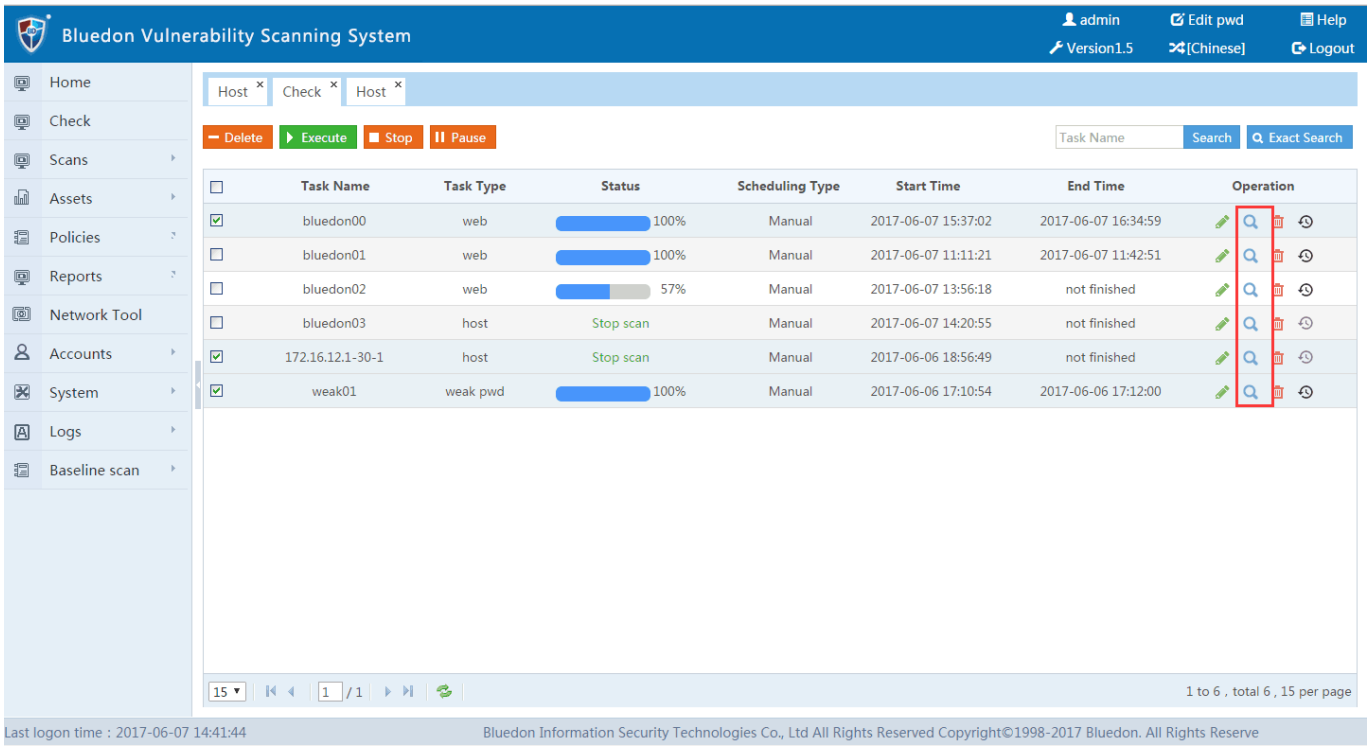


Figure 1

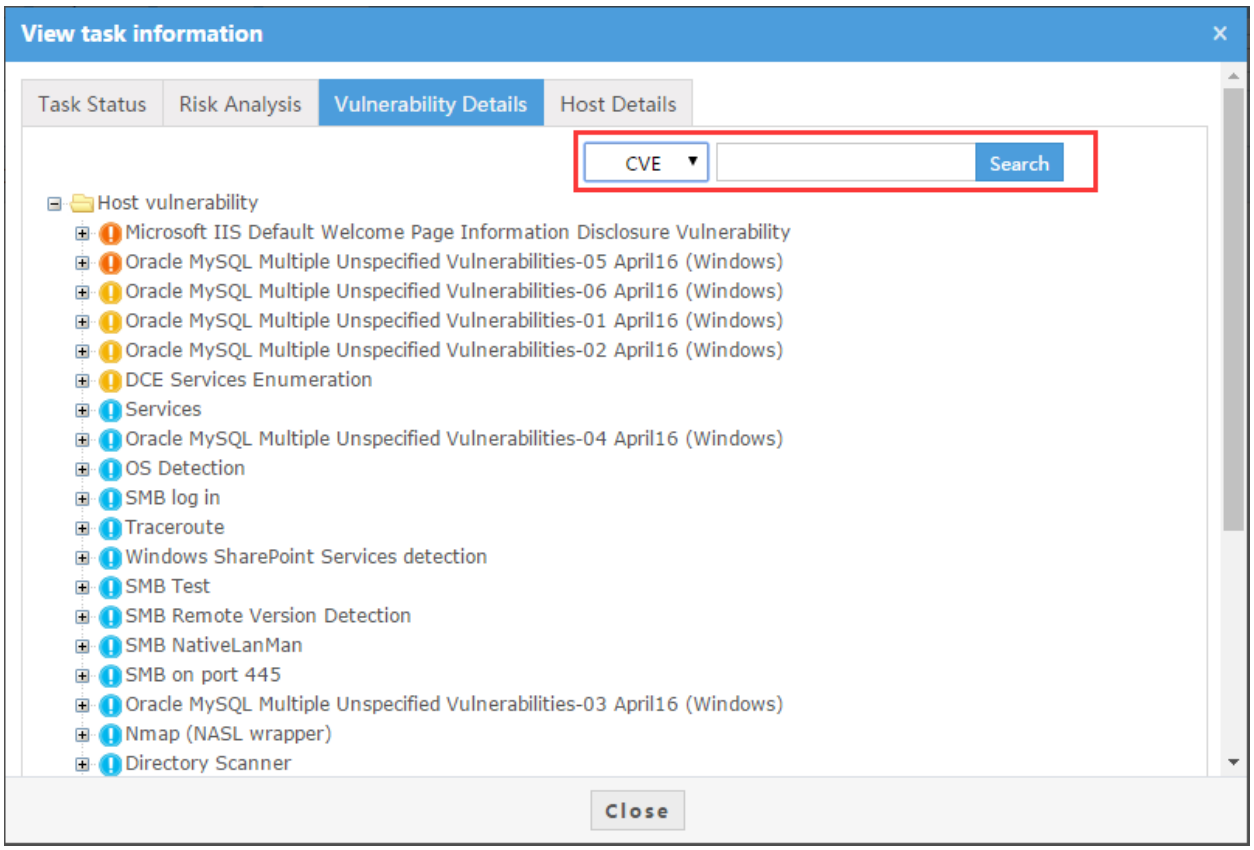


Figure 2

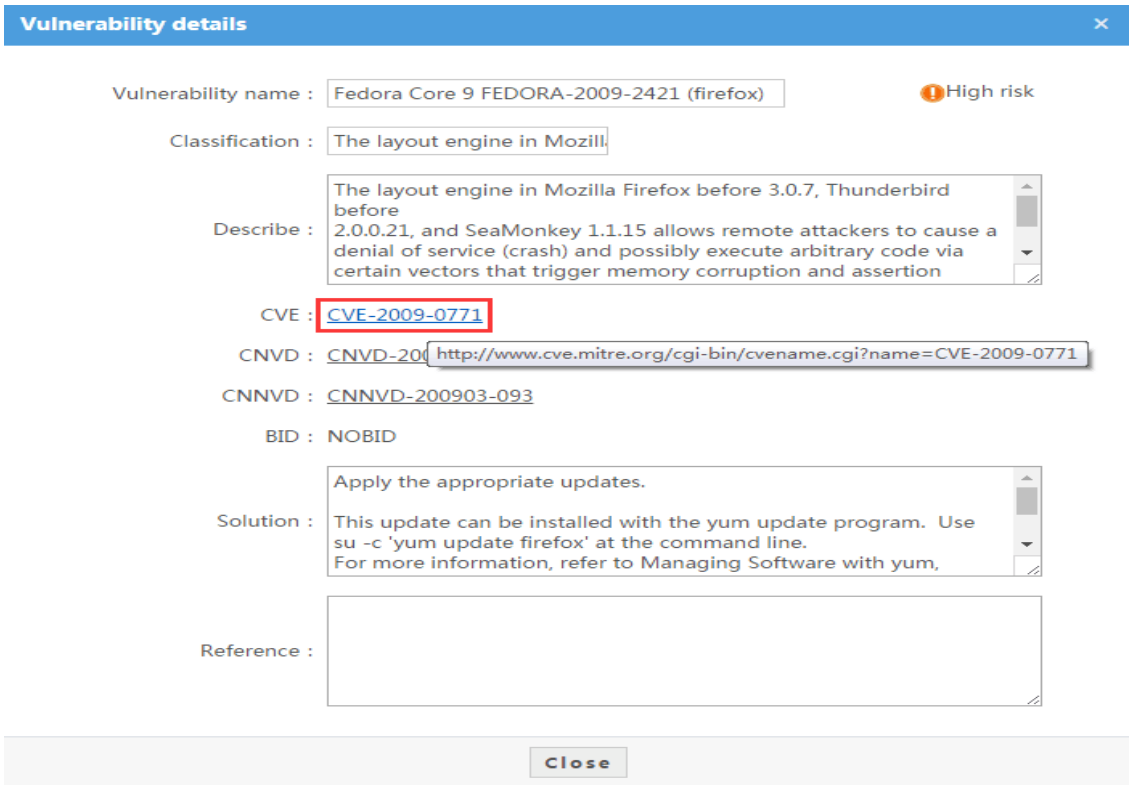


Figure 3

12) DOCUMENTATION INDEXING OF CVE-RELATED MATERIAL <CR_4.4>
If your documentation includes an index, provide a copy of the items and resources that you have listed under "CVE" in your index. Alternately, provide directions to where these "CVE" items are posted on your web site (recommended):

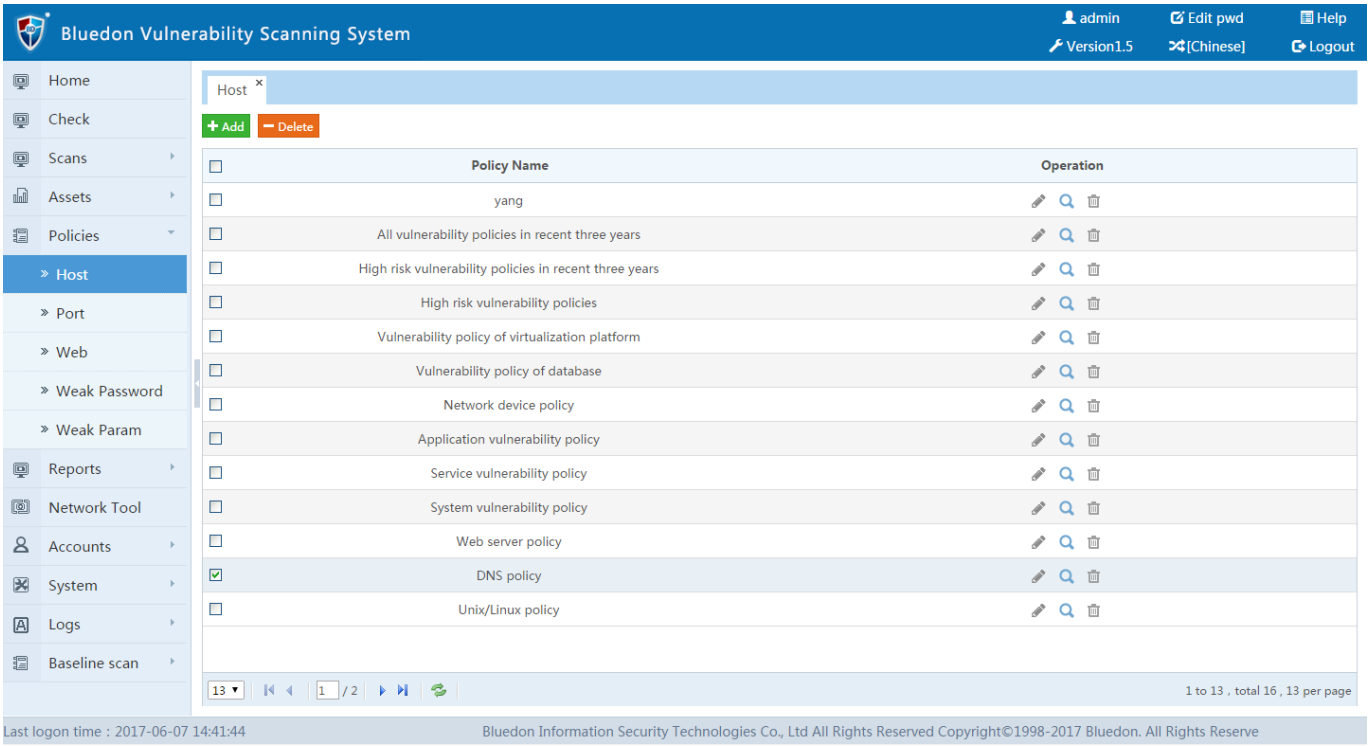
N/A

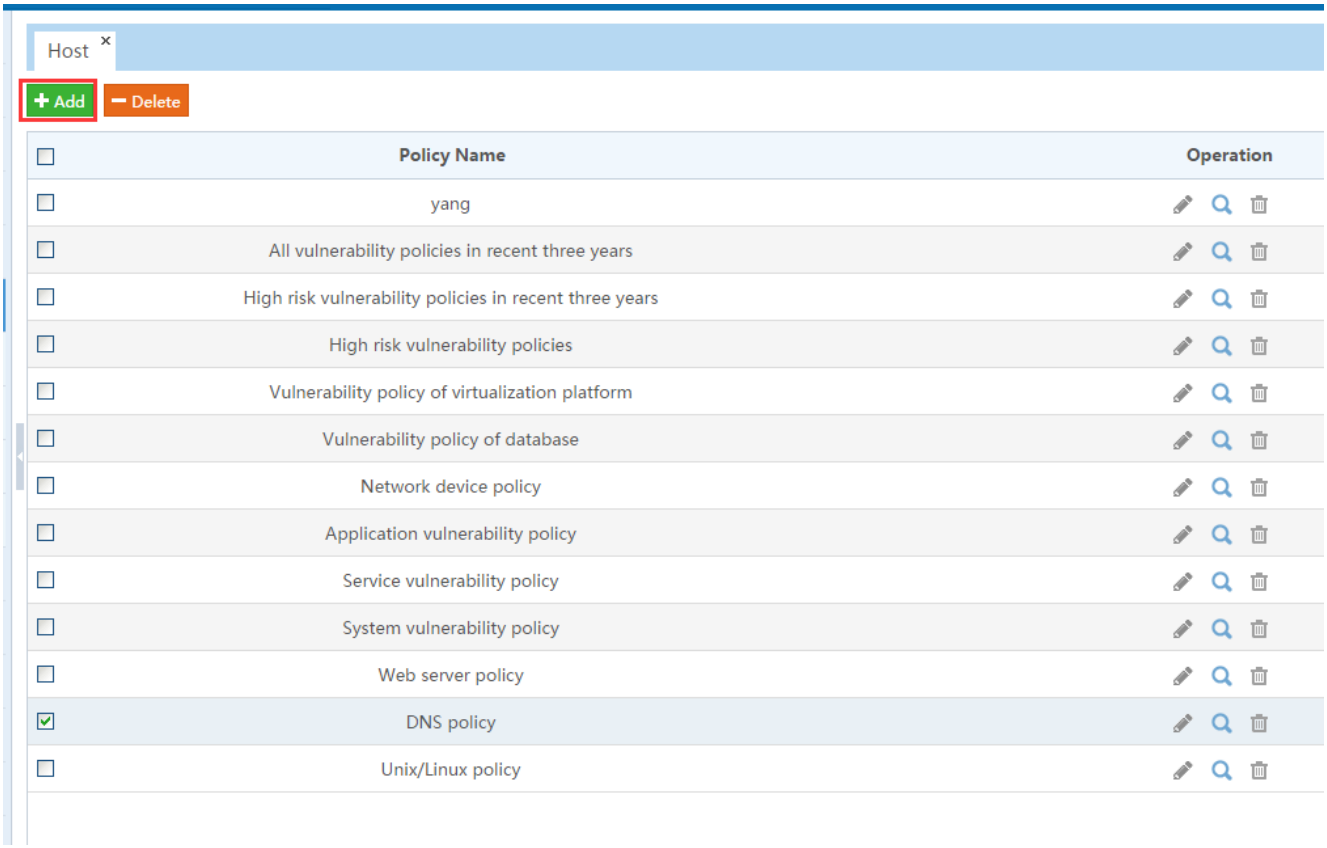
Type-Specific Capability Questions

Tool Questions

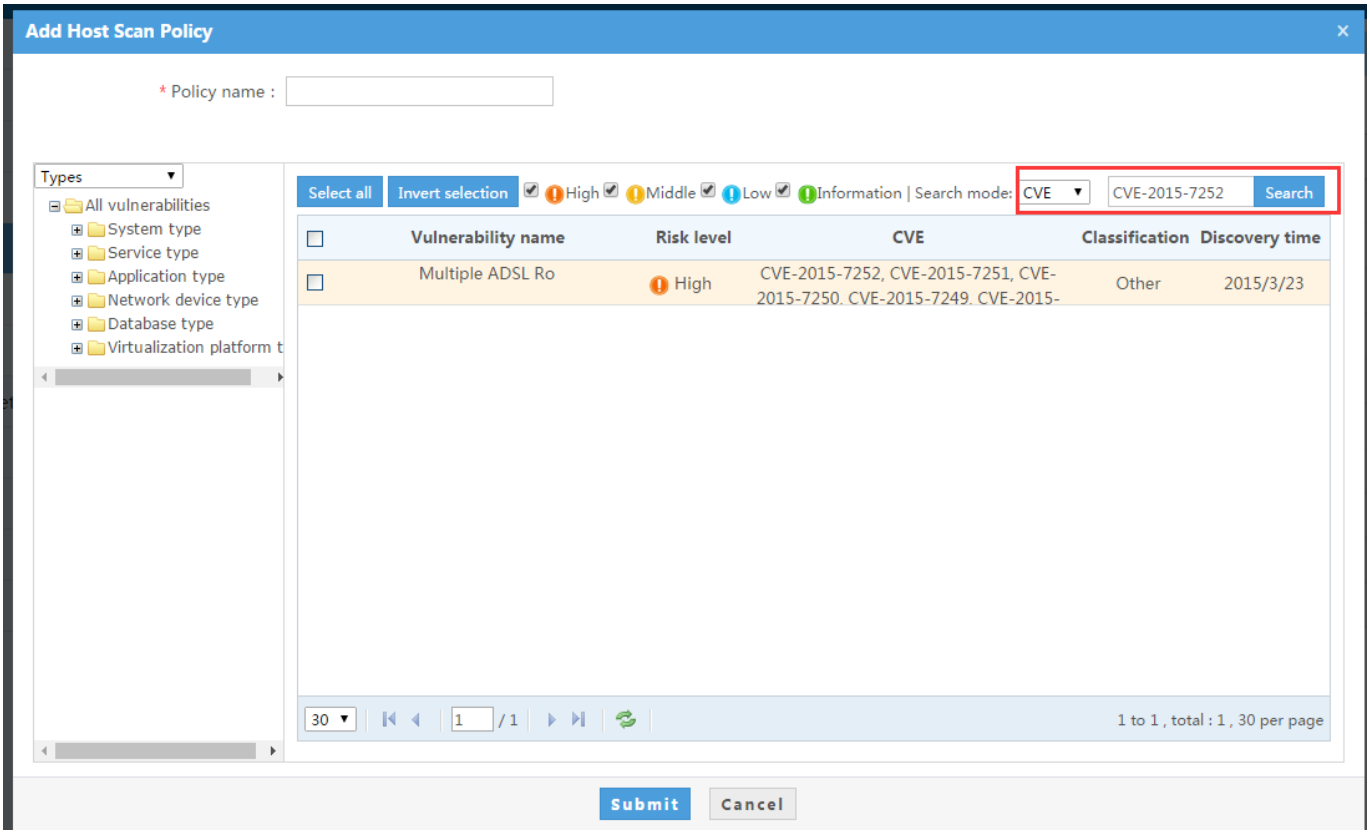
FINDING TASKS USING CVE IDS <CR_A.2.1>
Give detailed examples and explanations of how a user can locate tasks in the tool by looking for their associated CVE ID (required):
Users can find tasks by using CVE IDs which is shown as follows:

1. Click the tab “Policies” on the left list. And then click “Host” to find the green button “Add”. Click and then open the page of vulnerability template.





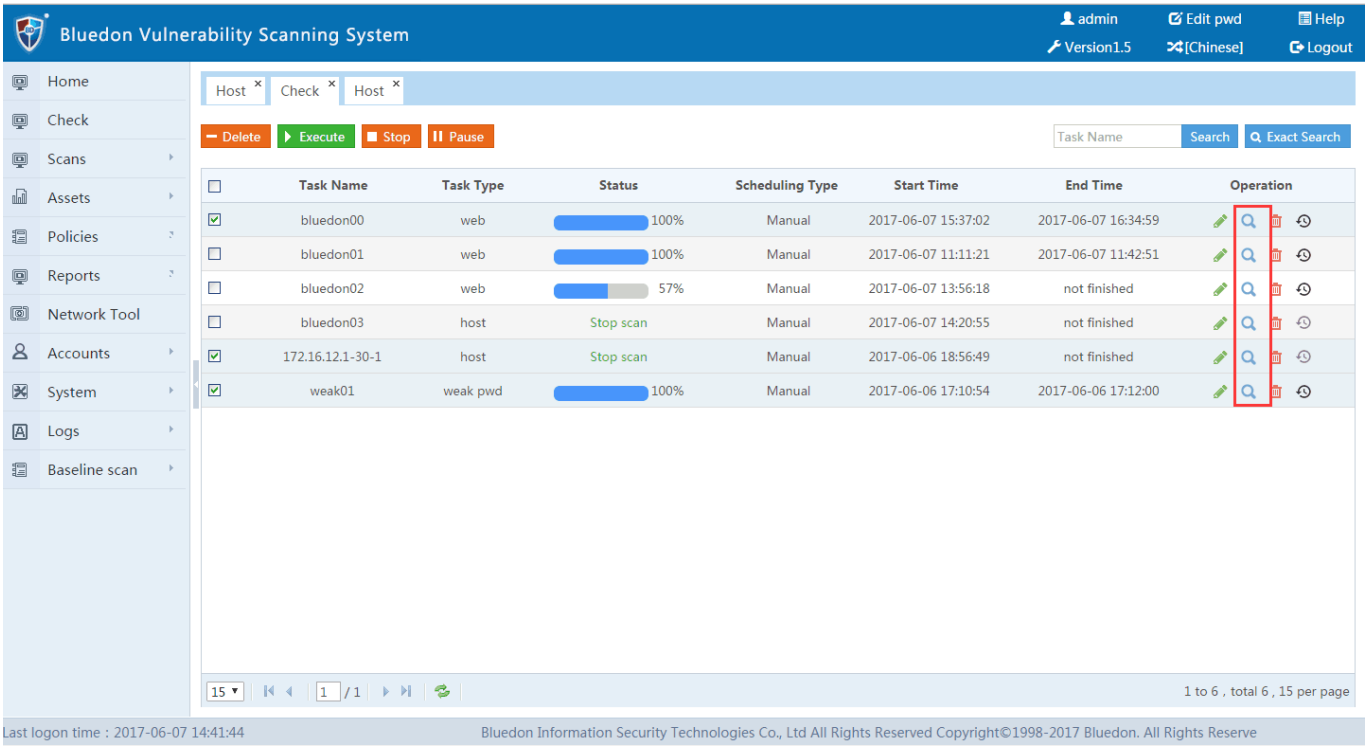
2. Users can see the searching box in the upper right corner. Input CVE ID and then click “Search” in order to find security elements.



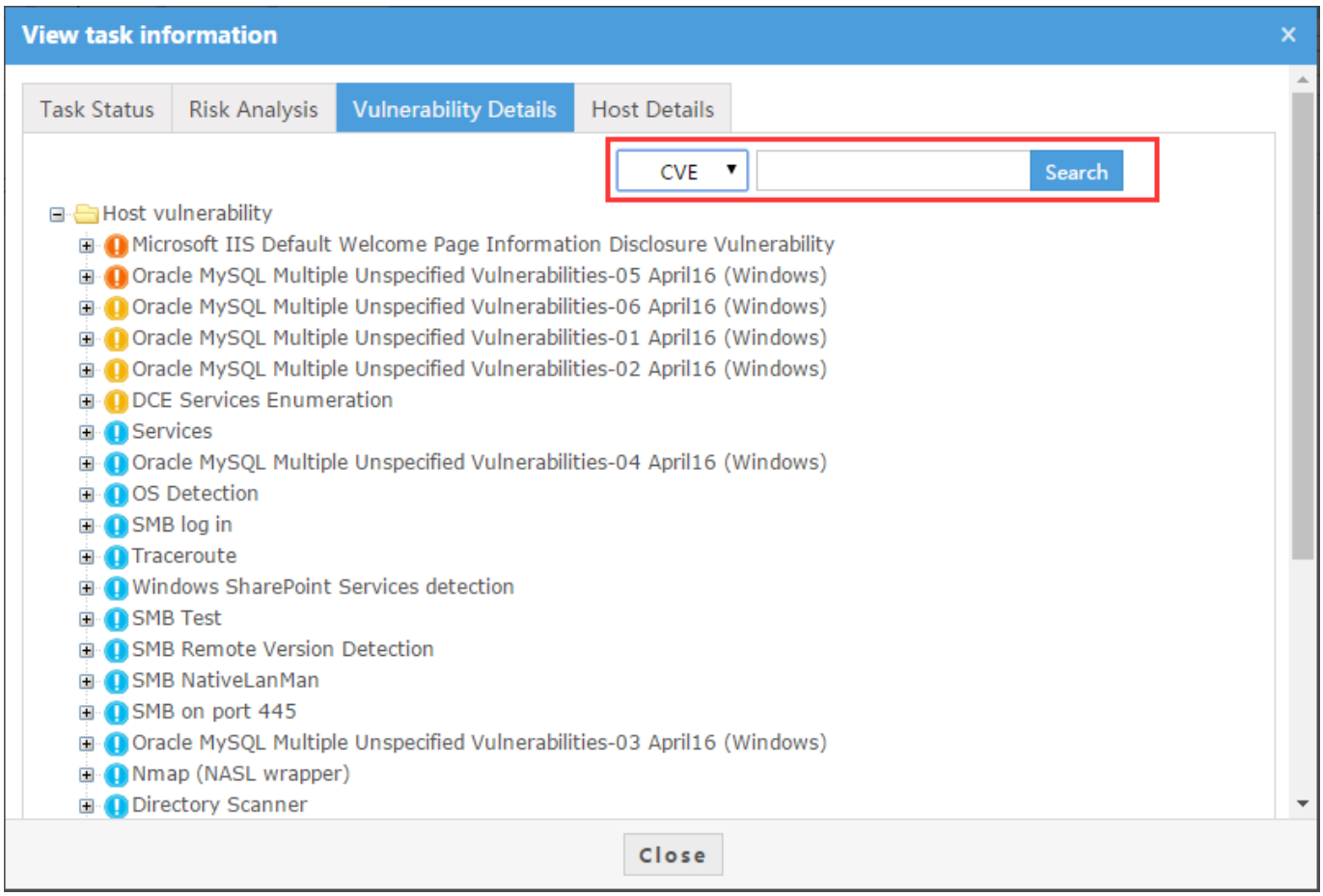
FINDING CVE IDS USING ELEMENTS IN REPORTS <CR_A.2.2>

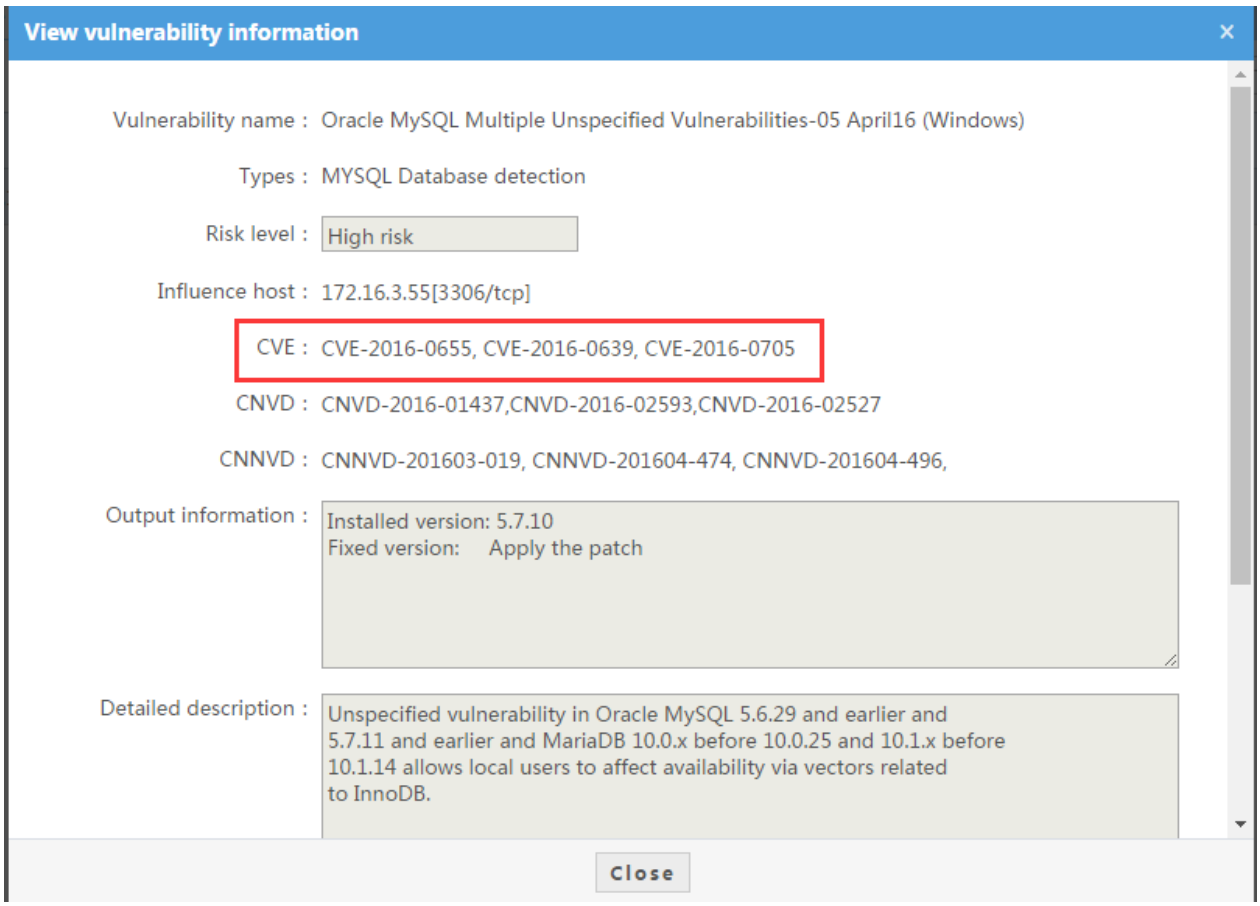
Give detailed examples and explanations of how, for reports that identify individual security elements, the tool allows the user to determine the associated CVE IDs for the individual security elements in the report (required):

1. Users can open the tab of “Check” and see reports on the page, then they can search the reports by clicking the icon.



2. Users can find CVE IDs related to vulnerabilities by inputting the CVE ID, or open the reports in the list to see the CVE IDs and other details.


View task information
Task Status
Risk Analysis
Vulnerability Details
Host Details
CVE
Search
Host vulnerability
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability
Oracle MySQL Multiple Unspecified Vulnerabilities-05 April16 (Windows)
Oracle MySQL Multiple Unspecified Vulnerabilities-06 April16 (Windows)
Oracle MySQL Multiple Unspecified Vulnerabilities-01 April16 (Windows)
Oracle MySQL Multiple Unspecified Vulnerabilities-02 April16 (Windows)
DCE Services Enumeration
Services
Oracle MySQL Multiple Unspecified Vulnerabilities-04 April16 (Windows)
OS Detection
SMB log in
Traceroute
Windows SharePoint Services detection
SMB Test
SMB Remote Version Detection
SMB NativeLanMan
SMB on port 445
Oracle MySQL Multiple Unspecified Vulnerabilities-03 April16 (Windows)
Nmap (NASL wrapper)
Directory Scanner
Close



GETTING A LIST OF CVE IDS ASSOCIATED WITH TASKS <CR_A.2.4>
Give detailed examples and explanations of how a user can obtain a listing of all of the CVE IDs that are associated with the tool's tasks (recommended):
N/A

SELECTING TASKS WITH A LIST OF CVE IDS <CR_A.2.5>
Describe the steps and format that a user would use to select a set of tasks by providing a file with a list of CVE IDs (recommended):
N/A

SELECTING TASKS USING INDIVIDUAL CVE IDS <CR_A.2.6>
Describe the steps that a user would follow to browse, select, and deselect a set of tasks for the tool by using individual CVE IDs (recommended):
N/A

NON-SUPPORT NOTIFICATION FOR A REQUESTED CVE ID <CR_A.2.7>
Provide a description of how the tool notifies the user that task associated to a selected CVE ID cannot be performed (recommended):
N/A

Service Questions

SERVICE COVERAGE DETERMINATION USING CVE IDS <CR_A.3.1>
Give detailed examples and explanations of the different ways that a user can use CVE IDs to find out which security elements are tested or detected by the service (i.e. by asking, by providing a list, by examining a coverage map, or by some other mechanism) (required):
N/A

FINDING CVE IDS IN SERVICE REPORTS USING ELEMENTS <CR_A.3.2>
Give detailed examples and explanations of how, for reports that identify individual security elements, the user can determine the associated CVE IDs for the individual security elements in the report (required):
N/A

SERVICE'S PRODUCT UTILIZATION DETAILS <CR_A.3.4>
Please provide the name and version number of any product that the service allows users to have direct access to if that product identifies security elements (recommended):
N/A

Online Capability Questions

FINDING ONLINE CAPABILITY TASKS USING CVE IDS <CR_A.4.1>
Give detailed examples and explanations of how a "find" or "search" function is available to the user to locate tasks in the online capability by looking for their associated CVE ID or through an online mapping that links each element of the capability with its associated CVE ID(s) (required):
N/A

ONLINE CAPABILITY INTERFACE TEMPLATE USAGE <CR_A.4.1.1>
Provide a detailed description of how someone can use your "URL template" (examples: http://www.example.com/cgi-bin/db-search.cgi?cvename=CVE-YYYY-NNNN and http://www.example.com/cve/CVE-YYYY-NNNN.html) to interface to your capability's search function (recommended):
N/A

ONLINE CAPABILITY CGI GET METHOD SUPPORT <CR_A.4.1.2>
If the URL template is for a CGI program, does it support the HTTP "GET" method — N/A, YES, or NO? (recommended):
N/A

FINDING CVE IDS USING ONLINE CAPABILITY ELEMENTS <CR_A.4.2>
Give detailed examples and explanations of how, for reports that identify individual security elements, the online capability allows the user to determine the associated CVE IDs for the individual security elements in the report (required):
N/A

ONLINE CAPABILITY ELEMENT TO CVE ID MAPPING <CR_A.4.3>
If details for individual security elements are not provided, give examples and explanations of how a user can obtain a mapping that links each element with its associated CVE ID(s), otherwise enter N/A (required):
N/A

Aggregation Capability Questions

FINDING ELEMENTS USING CVE IDS <CR_A.5.1>
Give detailed examples and explanations of how a user can associated elements in the capability by looking for their associated CVE ID (required):
N/A

28) FINDING CVE IDS USING ELEMENTS IN REPORTS <CR_A.5.2>
Give detailed examples and explanations of how, for reports that identify individual security elements, the capability allows the user to determine the associated CVE IDs for the individual security elements in the report (required):
N/A

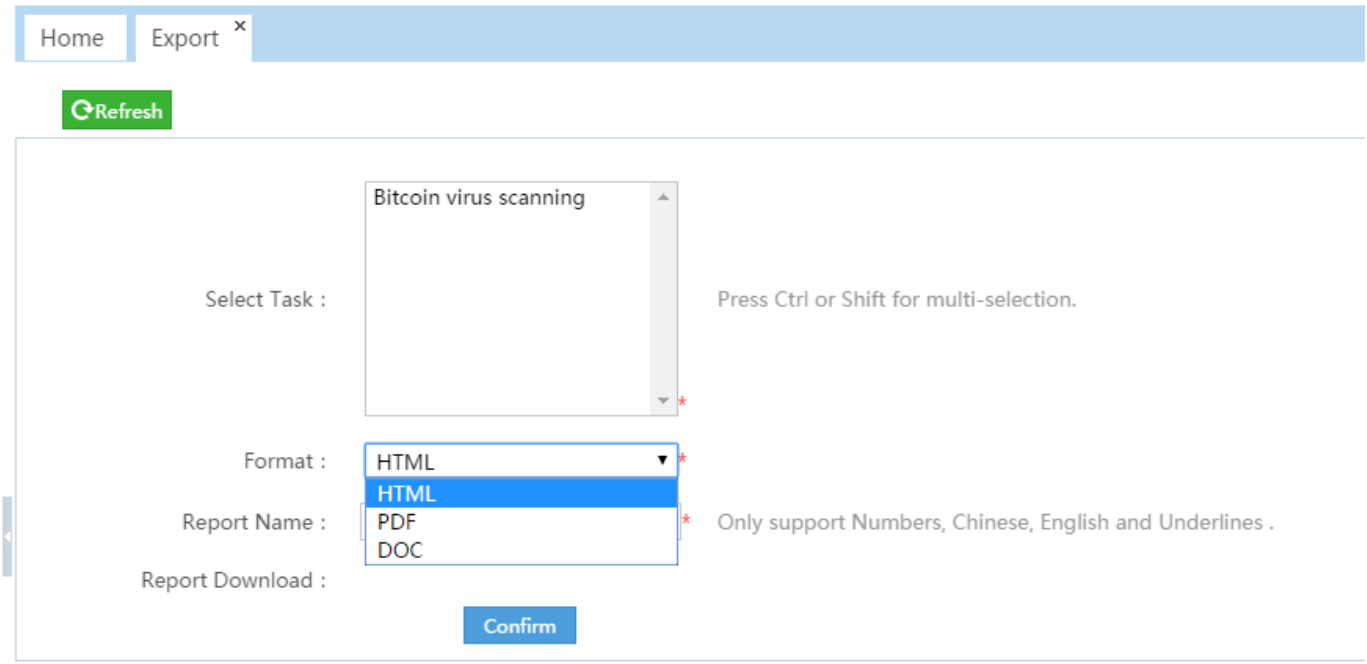
GETTING A LIST OF CVE IDS ASSOCIATED WITH TASKS <CR_A.5.4>
Give detailed examples and explanations of how a user can obtain a listing of all of the CVE IDs that are associated with the capability's tasks (recommended):
N/A

30) SELECTING TASKS WITH A LIST OF CVE IDS <CR_A.5.5>
Describe the steps and format that a user would use to select a set of tasks by providing a file with a list of CVE IDs (recommended):
N/A

SELECTING TASKS USING INDIVIDUAL CVE IDS <CR_A.5.6>
Describe the steps that a user would follow to browse, select, and deselect a set of tasks for the capability by using individual CVE IDs (recommended):
N/A

Media Questions

ELECTRONIC DOCUMENT FORMAT INFO <CR_B.3.1>
Provide details about the different electronic document formats that you provide and describe how they can be searched for specific CVE-related text (required):
We provide users with various electronic document formats including HTML, PDF and DOC. In the module of "Reports", users can see tab of "Exports" and then click it to see the page of exporting reports. They can choose one report format to download the report which contains CVE compatibility, description and remediation methods.

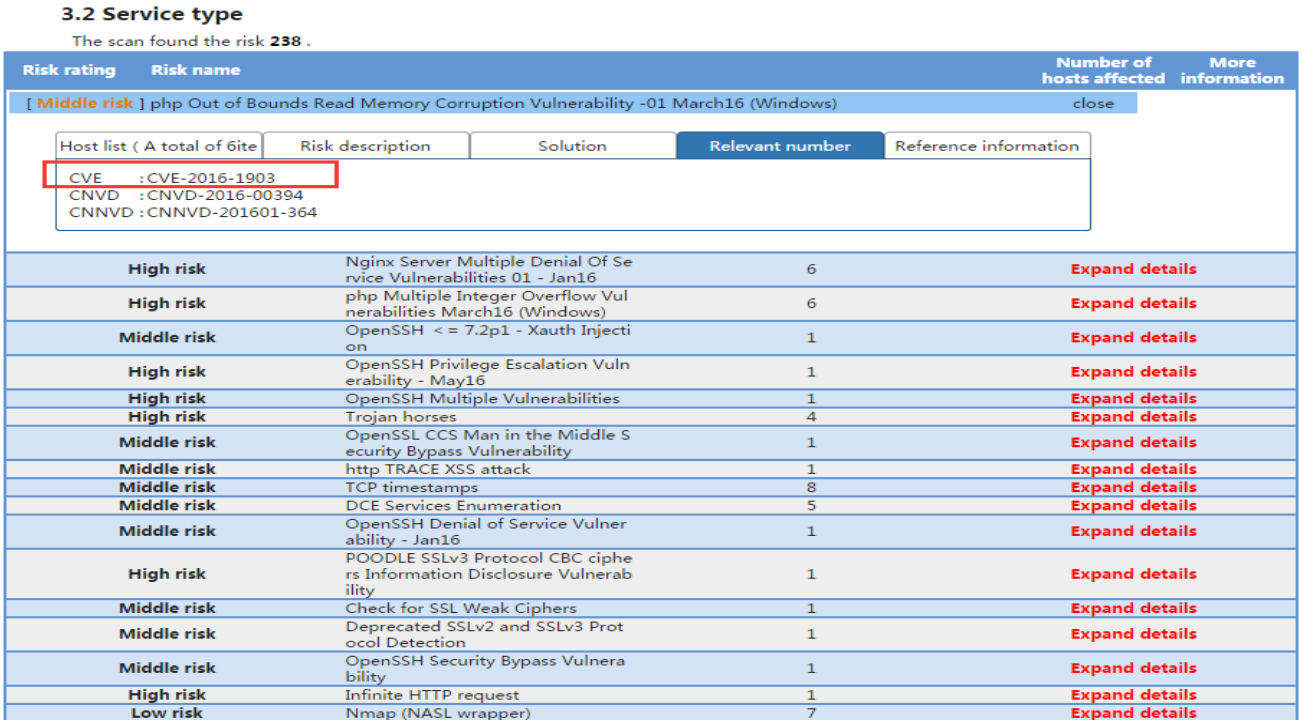


ELECTRONIC DOCUMENT LISTING OF CVE IDS <CR_B.3.2>

If one of the capability's standard electronic documents only lists security elements by their short names or titles provide example documents that demonstrate how the associated CVE IDs are listed for each individual security element (required):

Our standard electronic reports will list each CVE IDs that are associated with a related vulnerability. In the reports of vulnerabilities, users can search the reports and find the associated CVE IDs for each vulnerability.

Vulnerability name	Risk level	CVE	Classification	Discovery time
Redis EVAL Lua S	High	CVE-2015-4335	Other	2015/6/5
Cisco TelePresen	High	CVE-2015-0713	Cisco Network	2015/6/3
IBM WebSphere Ap	High	CVE-2015-1920	IBM detection	2015/6/3
Citrix NetScaler	High	CVE-2014-7140	Citrix Network	2015/5/12
Citrix NetScaler	High	CVE-2013-6011	Citrix Network	2015/5/12
Juniper NetScree	High	CVE-2014-3814	Juniper	2015/5/8
Palo Alto PAN-OS	High	CVE-2015-0235	glibc	2015/4/23
MS15-034 HTTP.sy	High	CVE-2015-1635	Windows	2015/4/16
Cisco Data Cente	High	CVE-2015-0666	Cisco Network	2015/4/14



3.2 Service type

The scan found the risk **238** .

Risk rating	Risk name	Number of hosts affected	More information
[Middle risk] php Out of Bounds Read Memory Corruption Vulnerability -01 March16 (Windows)		close	
Host list (A total of 6ite	Risk description	Solution	Relevant number	Reference information
CVE :CVE-2016-1903 CNVD :CNVD-2016-00394 CNNVD :CNNVD-201601-364				
High risk	Nginx Server Multiple Denial Of Service Vulnerabilities 01 - Jan16	6	Expand details	
High risk	php Multiple Integer Overflow Vulnerabilities March16 (Windows)	6	Expand details	
Middle risk	OpenSSH < = 7.2p1 - Xauth Injection	1	Expand details	
High risk	OpenSSH Privilege Escalation Vulnerability - May16	1	Expand details	
High risk	OpenSSH Multiple Vulnerabilities	1	Expand details	
High risk	Trojan horses	4	Expand details	
Middle risk	OpenSSL CCS Man in the Middle Security Bypass Vulnerability	1	Expand details	
Middle risk	http TRACE XSS attack	1	Expand details	
Middle risk	TCP timestamps	8	Expand details	
Middle risk	DCE Services Enumeration	5	Expand details	
Middle risk	OpenSSH Denial of Service Vulnerability - Jan16	1	Expand details	
High risk	POODLE SSLv3 Protocol CBC ciphers Information Disclosure Vulnerability	1	Expand details	
Middle risk	Check for SSL Weak Ciphers	1	Expand details	
Middle risk	Deprecated SSLv2 and SSLv3 Protocol Detection	1	Expand details	
Middle risk	OpenSSH Security Bypass Vulnerability	1	Expand details	
High risk	Infinite HTTP request	1	Expand details	
Low risk	Nmap (NASL wrapper)	7	Expand details	

ELECTRONIC DOCUMENT ELEMENT TO CVE ID MAPPING <CR_B.3.3>

Provide example documents that demonstrate the mapping from the capability's individual elements to the respective CVE ID(s) (recommended):

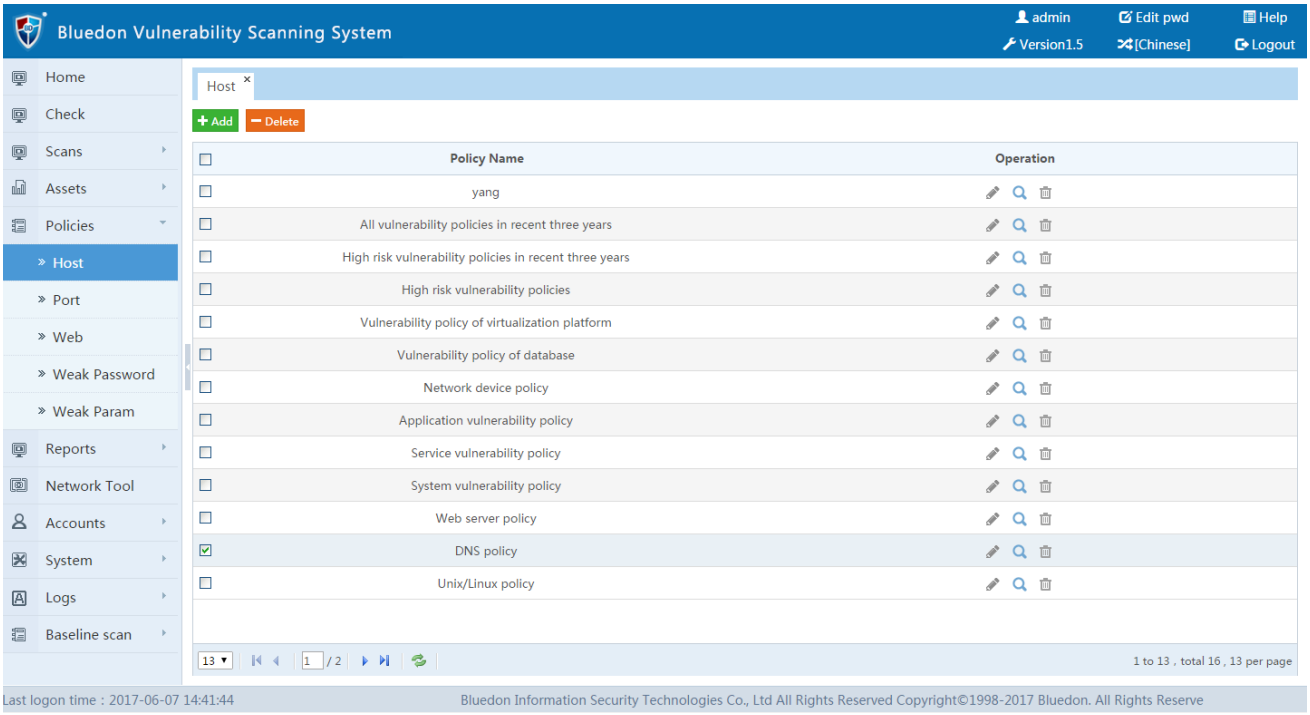
N/A

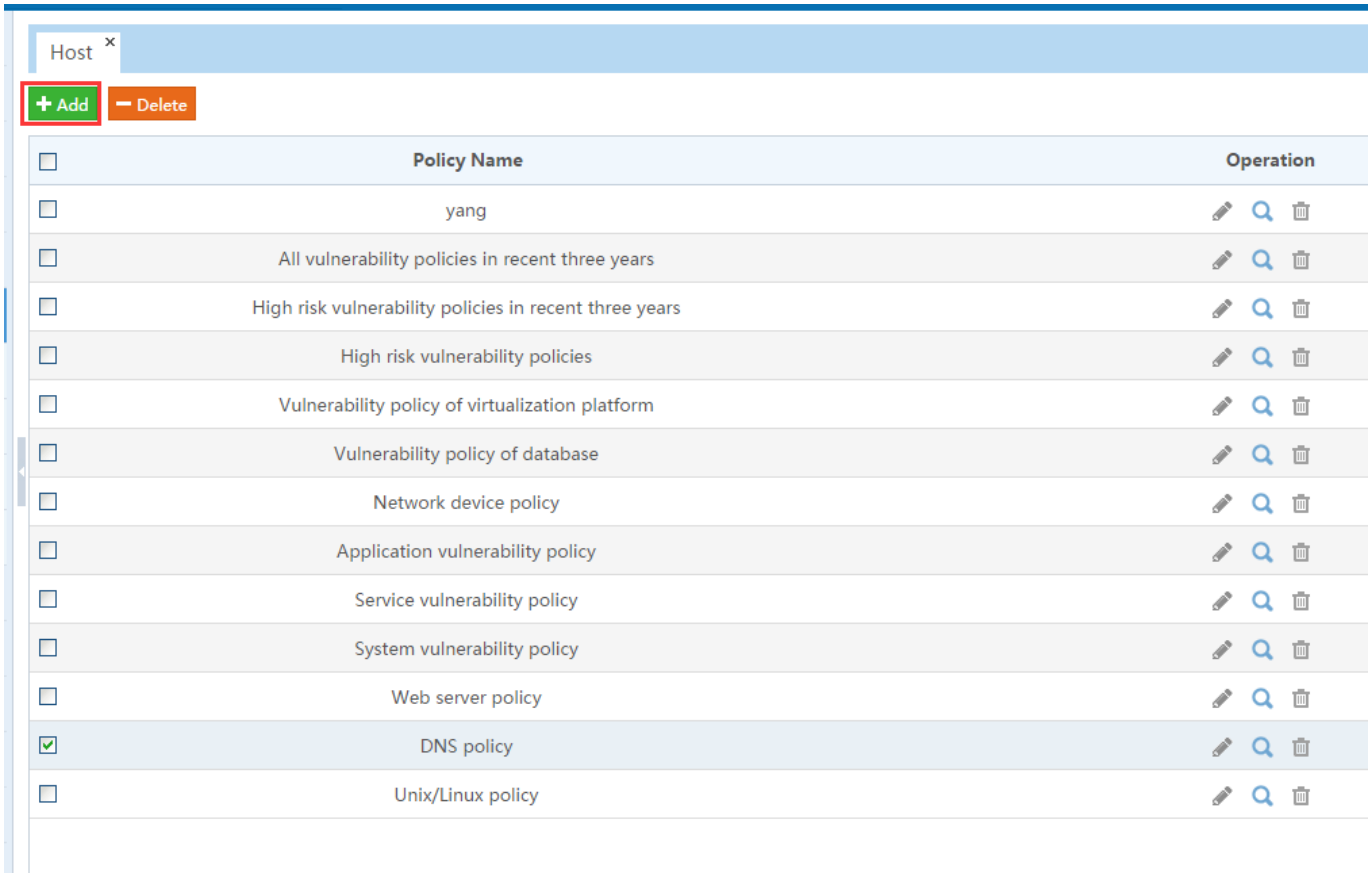
Graphical User Interface (GUI)

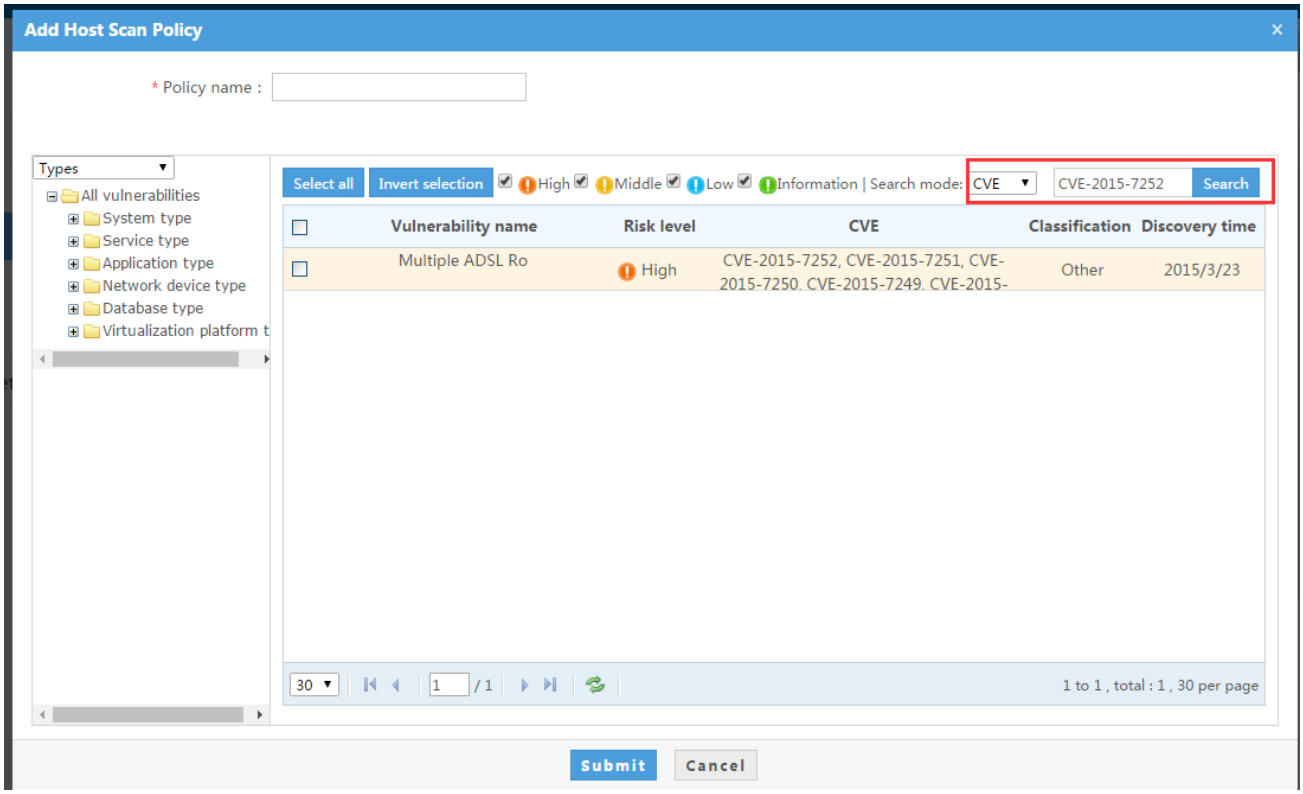
FINDING ELEMENTS USING CVE IDS THROUGH THE GUI <CR_B.4.1>

Give detailed examples and explanations of how the GUI provides a "find" or "search" function for the user to identify your capability's elements by looking for their associated CVE ID(s) (required):

The “search” function for the users to identify our products’ elements can be found in the “Host” module of “Policies”. Thereby they can look for associated CVE ID(s). This can be referred to <CR_4.2> and <CR_4.3>.


Bluedon Vulnerability Scanning System
admin
Edit pwd
Help
Version1.5
[Chinese]
Logout
Home
Check
Scans
Assets
Policies
Host
Port
Web
Weak Password
Weak Param
Reports
Network Tool
Accounts
System
Logs
Baseline scan
Host
Add
Delete
Policy Name
Operation
yang
All vulnerability policies in recent three years
High risk vulnerability policies in recent three years
High risk vulnerability policies
Vulnerability policy of virtualization platform
Vulnerability policy of database
Network device policy
Application vulnerability policy
Service vulnerability policy
System vulnerability policy
Web server policy
DNS policy
Unix/Linux policy
1 to 13 , total 16 , 13 per page
Last logon time : 2017-06-07 14:41:44
Bluedon Information Security Technologies Co., Ltd All Rights Reserved Copyright©1998-2017 Bluedon. All Rights Reserve

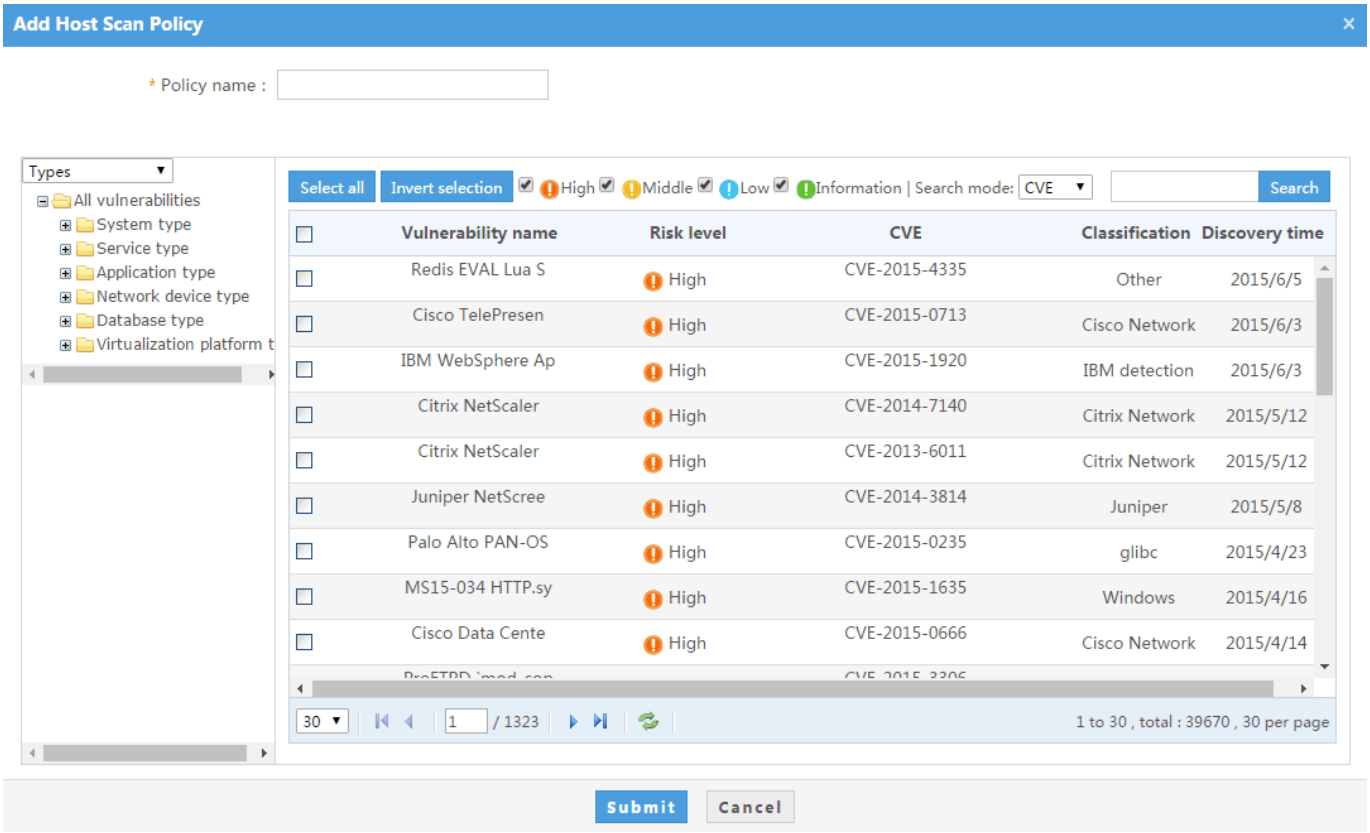

Host
Add
Delete
Policy Name
Operation
yang
All vulnerability policies in recent three years
High risk vulnerability policies in recent three years
High risk vulnerability policies
Vulnerability policy of virtualization platform
Vulnerability policy of database
Network device policy
Application vulnerability policy
Service vulnerability policy
System vulnerability policy
Web server policy
DNS policy
Unix/Linux policy



36) GUI ELEMENT TO CVE ID MAPPING <CR_B.4.2>

Briefly describe how the associated CVE IDs are listed for the individual security elements or discuss how the user can use the mapping between CVE entries and the capability's elements, also describe the format of the mapping (required):

CVE IDs are listed in the vulnerabilities template. Users can use the mapping between CVE entries and the elements to get the information about description of vulnerabilities, CVE IDs, etc. Please refer to <CR_4.2>.



GUI EXPORT ELECTRONIC DOCUMENT FORMAT INFO <CR_B.4.3>
Provide details about the different electronic document formats that you provide for exporting or accessing CVE-related data and describe how they can be searched for specific CVE-related text (recommended):
N/A

Questions for Signature

STATEMENT OF COMPATIBILITY <CR_2.7>
Have an authorized individual sign and date the following Compatibility Statement (required):

> **"As an authorized representative of my organization I agree that we will abide by all of the mandatory CVE Compatibility Requirements as well as all of the additional mandatory CVE Compatibility Requirements that are appropriate for our specific type of capability."**

Name: Chunchun Liu
Title: Certificate Manager

STATEMENT OF ACCURACY <CR_3.4>
Have an authorized individual sign and date the following accuracy Statement (recommended):

> **"As an authorized representative of my organization and to the best of my knowledge, there are no errors in the mapping between our capability's Repository and the CVE entries our capability identifies."**

Name: Chunchun Liu

Title: Certificate Manager

STATEMENT ON FALSE-POSITIVES AND FALSE-NEGATIVES <CR_A.2.8 and/or CR_A.3.5>
FOR TOOLS AND SERVICES ONLY - Have an authorized individual sign and date the following statement about your tools efficiency in identification of security elements (required):

> **"As an authorized representative of my organization and to the best of my knowledge, normally when our capability reports a specific security element, it is generally correct and normally when an event occurs that is related to a specific security element our capability generally reports it."**

Name: Chunchun Liu
Title: Certificate Manager