

|                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>შემოთავაზებული გადაწყვეტილება უნდა წარმოადგენდეს ერთ მწარმოებელს.</li> <li>მიმწოდებელმა უნდა უზრუნველყოს შემოთავაზებული პროდუქტის სრულყოფილი გამართვა</li> </ul> |                                                                                                                                                                                                                                                                          |
| მოთხოვნები კომპიუტერული სისტემების სკანირების მიმართ                                                                                                                                                    |                                                                                                                                                                                                                                                                          |
| სამართავი პანელი                                                                                                                                                                                        | იყენებდეს დაშიფრულ არხს (HTTPS).                                                                                                                                                                                                                                         |
| მოწყვლადობის მენეჯმენტი                                                                                                                                                                                 | გადაწყვეტილებას უნდა შეეძლოს აღმოჩენილი სისუსტეების გამოკვლევა.                                                                                                                                                                                                          |
|                                                                                                                                                                                                         | გადაწყვეტილებამ უნდა უზრუნველყოს ქსელის სისუსტეების სკანირება, აგენტების დაინსტალირების გარეშე.                                                                                                                                                                          |
|                                                                                                                                                                                                         | გადაწყვეტილებას უნდა შეეძლოს, სკანირების დროს არხის გადატვირთვის თავიდან აცილება.                                                                                                                                                                                        |
|                                                                                                                                                                                                         | გადაწყვეტილებამ უნდა შეძლოს ავტომატურად შექმნას კონფიგურაციების სარეზერვო ასლი და საჭიროების შემთხვევაში სარეზერვო ასლიდან აღადგინოს იგი.                                                                                                                                |
|                                                                                                                                                                                                         | გადაწყვეტილებამ უნდა ჩაიწეროს ისეთი მოვლენები, როგორიცაა მომხმარებლის შესვლის დრო, ინფრასტრუქტურის კომპონენტის სკანირების დაწყება და შეწყვეტის მონაცემები.                                                                                                               |
| აგენტი                                                                                                                                                                                                  | აგენტების დაყენება შესაძლებელი უნდა იყოს Windows, Linux და Mac ოპერაციულ სისტემებზე.                                                                                                                                                                                     |
|                                                                                                                                                                                                         | ინფორმაციის შეგროვება უნდა მოხდეს მხოლოდ იმ წერტილიდან, რომელზეც დაინსტალირებულია აგენტი.                                                                                                                                                                                |
|                                                                                                                                                                                                         | შესაძლებელი უნდა იყოს აგენტების ინსტალაცია ერთი პაკეტის გამოყენებით, როგორიცაა Microsoft Group Policy ან SCCM.                                                                                                                                                           |
|                                                                                                                                                                                                         | უნდა ჰქონდეს შეგროვების დროის ინტერვალი არანაკლებ 6 საათი.                                                                                                                                                                                                               |
|                                                                                                                                                                                                         | შესაძლებელი უნდა იყოს აჩქრების ფუნქცია, ასევე რეგულირებადი უნდა იყოს აგენტების ერთდროული განახლების დასაშვები სიჩქარე. ყველა აგენტმა უნდა მიიღოს განახლებები სხვადასხვა დროს. აგენტების განახლების რაოდენობა და გამტარუნარიანობა არ უნდა აღემატებოდეს დაშვებულ ლიმიტებს. |
|                                                                                                                                                                                                         | შესაძლებელი უნდა იყოს აგენტი განთავსდეს შეზღუდული წვდომის ქსელში და სისტემებზე.                                                                                                                                                                                          |
|                                                                                                                                                                                                         | მხარს უნდა უჭერდეს 2817 (RFC) სტანდარტს                                                                                                                                                                                                                                  |
|                                                                                                                                                                                                         | ნაჩვენები უნდა იყოს სტატისტიკური მონაცემები, რომლებიც ასახავს განლაგებული აგენტების საერთო რაოდენობას მათი სტატუსით.                                                                                                                                                     |
| სკანირების პოლიტიკა                                                                                                                                                                                     | გადაწყვეტილებას უნდა გააჩნდეს სკანირების პოლიტიკების შედგენა საჭიროების მიხედვით.                                                                                                                                                                                        |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| სკანირება                   | გადაწყვეტილებას უნდა შეეძლოს 400 (ოთხასი) სამუშაო სადგურის (MS Windows, Linux, MacOS და ქსელური მოწყობილობები) ერთდროულად სკანირება.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| მონაცემთა ბაზების სკანირება | <p>გადაწყვეტილებას უნდა გააჩნდეს მოწყვლად კომპონენტებზე სკანირების საშუალება შემდეგ მონაცემთა ბაზებზე:</p> <ul style="list-style-type: none"> <li>• MS SQL Server;</li> <li>• Oracle;</li> <li>• MySQL;</li> <li>• PostgreSQL;</li> <li>• Sybase Adaptive Server Enterprise (ASE);</li> <li>• DB2.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| სკანირების შედეგი           | <p>• უნდა აჩვენოს შესაბამისობის საერთო დონე;</p> <p>• უნდა წარმოადგინოს დეტალური ტექნიკური ინფორმაცია აქტივის შესახებ და შეიცავდეს შემდეგ ინფორმაციას:</p> <ul style="list-style-type: none"> <li>• IP მისამართი;</li> <li>• Mac მისამართი;</li> <li>• პლატფორმის ტიპი;</li> <li>• ოპერაციული სისტემა;</li> <li>• დომენი;</li> <li>• მომხმარებელთა ჯგუფი;</li> <li>• მომხმარებლები;</li> <li>• ღია პორტები;</li> <li>• მიმდინარე სერვისი პორტზე</li> <li>• მონაცემთა ბაზა;</li> <li>• მავნე პროგრამა;</li> <li>• სამუშაო სადგურზე დატვირთვა დინამიკაში;</li> </ul> <p>უნდა შეეძლოს მზა შაბლონების გამოყენება აქტივების შემოწმების მიზნით წინასწარ განსაზღვრული პრაქტიკების შესაბამისად:</p> <ul style="list-style-type: none"> <li>• CIS</li> <li>• HIPAA</li> <li>• Benchmarks</li> <li>• GLBA</li> <li>• OWASP best practices</li> <li>• PHI / PII content</li> <li>• Microsoft best practice</li> </ul> <p>უნდა აჩვენოს სამუშაო სადგურზე მოწყვლადობის ჩამონათვალი: მათ შორის ID, აღწერა, CVS, CVSS და CVSSv3 ქულა, გამოქვეყნების თარიღი / მოდიფიკაცია, კატეგორია, დრო და დაუცველობის დადასტურება;</p> <p>უნდა უზრუნველყოს ეტაპობრივად მოწყვლადობის აღმოფხვრის გეგმა, დეტალური აღწერით;</p> |

|                           |                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | უნდა წარმოადგინოს ე.წ. ქსპლოიტების სია, რომლებიც, თეორიულად, შეიძლება გამოყენებულ იქნას სამუშაო სადგურზე შეტევის, მოწყვლადობის სიის შესაბამისად;                                                                                                                                                                                                                   |
|                           | უნდა დაადგინოს სამუშაო სადგურზე დაინსტალირებული პროგრამები;                                                                                                                                                                                                                                                                                                        |
|                           | უნდა წარმოადგინოს სისტემის სერვისების ჩამონათვალი, ადგილობრივი ანგარიშები, ადგილობრივი ჯგუფები, ხელმისაწვდომი რესურსები, ლოგიკური დისკი და ლიცენზიის გასაღებები, ასევე ინფორმაცია მათი აქტივაციის ვადის ამოწურვის შესახებ.                                                                                                                                         |
|                           | უნდა შეეძლოს ავტორიზებული აქტივების სკანირება საჯარო SSH გასაღების გამოყენებით.                                                                                                                                                                                                                                                                                    |
|                           | უნდა გამოვიყენოს DSA გასაღებები კონსოლთან კომუნიკაციისთვის, არანაკლებ 1024 ბიტის.                                                                                                                                                                                                                                                                                  |
|                           | შესაძლებელი უნდა იყოს მოდულების მართვის ინტერფეისში კონსოლთან კომუნიკაციის სტატუსის ნახვა.                                                                                                                                                                                                                                                                         |
| ინტეგრაცია                | Active Directory დომენის კონტროლერების სკანირებისას მომხმარებლის ჩამოთვლის პოტენციური შესრულების გავლენის შესამცირებლად, მოდულებში უნდა ჩამოთვალოთ მხოლოდ 2000 ინდივიდუალური მომხმარებლის ანგარიში და 2000 მომხმარებლის ჯგუფი თითოეული რესურსისთვის.                                                                                                               |
|                           | გადაწყვეტილებას უნდა შეეძლოს სამუშაო სადგურზე გამოვლენილი მოწყვლადი კომპონენტების შესამოწმებლად და შედეგების ვიზუალიზაციისთვის შეღწევადობის ტესტირების სისტემასთან ორმხრივი ინტეგრაცია.                                                                                                                                                                            |
|                           | გადაწყვეტილებას უნდა შეეძლოს მოთხოვნების სარეგისტრაციო სისტემებთან (ე.წ. ticketing system) ინტეგრაცია                                                                                                                                                                                                                                                              |
| სერვისების იდენტიფიცირება | გადაწყვეტილებას უნდა გააჩნდეს სერვისების იდენტიფიცირების საშუალება TCP პორტების სრულდიაპაზონზე 1-65535 და კავშირის დასამყარებლად იყენებდეს შემდეგ ტიპებს: <ul style="list-style-type: none"><li>• Stealth scan (SYN);</li><li>• Stealth scan (SYN+RST);</li><li>• Stealth scan (SYN+FIN);</li><li>• Stealth scan (SYN+ECE);</li><li>• Full connect scan.</li></ul> |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ავტომატიზირებული ქმედებები                   | <p>გადაწყვეტილებას უნდა გააჩნდეს ქმედებების ავტომატიზაციის შესაძლებლობა შემდეგ მოვლენებზე:</p> <ul style="list-style-type: none"> <li>• განახლების მიღება: <ul style="list-style-type: none"> <li>- განახლებისას მიღებულ მოწყვლად კომპონენტებზე წინასწარ განსაზღვრული სამუშაო სადგურების სკანირება.</li> </ul> </li> <li>• ახალი სამუშაო სადგურების გამოვლენა: <ul style="list-style-type: none"> <li>- აღმოჩენილი სამუშაო სადგურის დამატება არსებულ სკანირების გეგმაში და მისი სკანირება.</li> </ul> </li> </ul>                                                                                                                                                                                                                                      |
| სამუშაო სადგურების ავტომატიზირებული აღმოჩენა | <p>გადაწყვეტილებას უნდა გააჩნდეს სამუშაო სადგურების აღმოჩენის ფუნქცია შემდეგ სისტემებთან ინტეგრაციის მეშვეობით:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory;</li> <li>• Microsoft DHCP server;</li> <li>• Microsoft Exchange Server;</li> <li>• VMware ESX(i);</li> <li>• VMware VSphere.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ვებ რესურსებზე ავტორიზაცია                   | <p>გადაწყვეტილებას უნდა გააჩნდეს ვებ რესურსებზე ავტორიზაციის შემდეგი მეთოდების მხარდაჭერა:</p> <ul style="list-style-type: none"> <li>• Web Forms;</li> <li>• Header;</li> <li>• Plain Authentication.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| ვიზუალიზაცია                                 | <p>გადაწყვეტილებას უნდა გააჩნდეს სამუშაო სადგურების დაჯგუფების საშუალება დინამიურ ჯგუფებში, შემდეგი კრიტერიუმების და მათი კომბინაციის მიხედვით:</p> <ul style="list-style-type: none"> <li>• asset name</li> <li>• CVE ID</li> <li>• host type</li> <li>• IP address range</li> <li>• IP address type</li> <li>• last scan date</li> <li>• operating system name</li> <li>• PCI compliance status</li> <li>• service name</li> <li>• open port numbers</li> <li>• operating system name</li> <li>• software name</li> <li>• presence of validated vulnerabilities</li> <li>• user-added criticality level</li> <li>• user-added custom tag</li> <li>• user-added tag (location)</li> <li>• user-added tag (owner)</li> <li>• vAsset cluster</li> </ul> |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | <ul style="list-style-type: none"> <li>• vAsset datacenter</li> <li>• vAsset host</li> <li>• vAsset power state</li> <li>• vAsset resource pool path</li> <li>• CVSS risk vectors</li> <li>• vulnerability category</li> <li>• vulnerability CVSS score</li> <li>• vulnerability exposures</li> <li>• vulnerability risk scores</li> <li>• vulnerability title</li> <li>• Scan group name</li> <li>• Vulnerability CVSSv3 score</li> </ul> |
| SQL მოთხოვნები          | გადაწყვეტილებას უნდა გააჩნდეს სკანირების შედეგების დასამუშავებლად SQL მოთხოვნების გაშვების შესაძლებლობა მონაცემთა ბაზაში ვებ ინტერფეისიდან და მოთხოვნის შედეგების ექსპორტი CSV ფაილის სახით.                                                                                                                                                                                                                                               |
| რეპორტირება - გენერაცია | გადაწყვეტილებას უნდა გააჩნდეს რეპორტების გენერაციის საშუალება ახალი შაბლონის საშუალებით, არსებული შაბლონის ბაზაზე.                                                                                                                                                                                                                                                                                                                         |
| რეპორტირება             | გადაწყვეტილებას უნდა გააჩნდეს რეპორტების ექსპორტირების საშუალება შემდეგ ფორმატებში: <ul style="list-style-type: none"> <li>• PDF;</li> <li>• RTF;</li> <li>• HTML;</li> <li>• XML;</li> <li>• CSV;</li> <li>• TXT.</li> </ul>                                                                                                                                                                                                              |
|                         | მონაცემთა შემდგომში დამუშავების მიზნით, გადაწყვეტილებას უნდა გააჩნდეს სკანირების შედეგების ექსპორტირების საშუალება გარემონაცემთა ბაზებთან: <ul style="list-style-type: none"> <li>• MS SQL Server;</li> <li>• Oracle;</li> <li>• MySQL;</li> <li>• PostgreSQL.</li> </ul>                                                                                                                                                                  |
|                         | გადაწყვეტილებამ უნდა უზრუნველყოს ანგარიშების გენერირების შესაძლებლობა, დამატებითი პროგრამული უზრუნველყოფის ინსტალაციისა და გამოყენების გარეშე.                                                                                                                                                                                                                                                                                             |
|                         | გადაწყვეტილებამ უნდა უზრუნველყოს ანგარიშების შექმნის შესაძლებლობა გარკვეული მახასიათებლების საფუძველზე, მაგალითად: TOP 20 ყველაზე კრიტიკული სისუსტე.                                                                                                                                                                                                                                                                                       |
| აუდიტი                  | გადაწყვეტილებამ უნდა შეეძლოს კონფიგურაციების და პატჩების შემოწმება Windows და Linux / Ubuntu სისტემებზე.                                                                                                                                                                                                                                                                                                                                   |

|                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | გადაწყვეტილებას არ უნდა ჰქონდეს შეზღუდვა, მომხმარებლის ერთდროულად წვდომის რაოდენობაზე.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|                                               | გადაწყვეტილებას უნდა შეეძლოს მოთხოვნების შესაბამისობაზე შემოწმება, როგორცაა PCI, FDCC, FISHMA და შექმნას შესაბამისი ანგარიშები.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| მოთხოვნები ვებ აპლიკაციების სკანირების მიმართ |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| სამართავი პანელი                              | გადაწყვეტილების სამართავი პანალი წარმოდგენილი უნდა იყოს ღრუბლოვანი გარემოში, უნდა იყოს ბაზირებული ვებ ტექნოლოგიაზე და იყენებდეს დამიფრულ არხს (HTTPS).                                                                                                                                                                                                                                                                                                                                                                                               |
| სკანერის ძრავი                                | გადაწყვეტილების სკანერის ძრავის გამოყენება უნდა შეიძლებოდეს როგორც ღრუბლოვანი გარემოდან, ასევე ლოკალურად.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ლიცენზირება                                   | გადაწყვეტილებას უნდა შეეძლოს 15 ვებ აპლიკაციის (ე.წ. Fully Qualified Domain Name) პარალელური სკანირება. ლიცენზია არ უნდა ზღუდავდეს მართვის პანელში პარალელურად მომუშავე მომხმარებლების რაოდენობას და არ უნდა იყოს მიბმული ე.წ. MAC მისამართზე.                                                                                                                                                                                                                                                                                                       |
| ტესტირების მეთოდი                             | გადაწყვეტილება უნდა წარმოადგენდეს ვებ აპლიკაციების დინამიური ტესტირების ხელსაწყოს (ე.წ. Dynamic Application Security Testing – DAST)                                                                                                                                                                                                                                                                                                                                                                                                                 |
| სკანირების პოლიტიკა                           | <p>გადაწყვეტილების სკანირების კონფიგურაცია უნდა შედგებოდეს შემდეგი პარამეტრებისაგან:</p> <ul style="list-style-type: none"> <li>• Attack Policy;</li> <li>• Proxy;</li> <li>• Authentication;</li> <li>• Crawler Restrictions;</li> <li>• Attack Restrictions;</li> <li>• HTTP Headers;</li> <li>• Performance;</li> <li>• Reporting;</li> <li>• Web Service;</li> <li>• Recorded Traffic;</li> <li>• Browser Macro;</li> <li>• Selenium Recordings;</li> <li>• Parameters Training;</li> <li>• Custom URLs;</li> <li>• Advanced Options.</li> </ul> |
| სკანირება                                     | <p>გადაწყვეტილებას უნდა გააჩნდეს მოცემული ვებ ტექნოლოგიების სკანირების შესაძლებლობა:</p> <ul style="list-style-type: none"> <li>• REST;</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                   |

|                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                        | <ul style="list-style-type: none"><li>• WSDL;</li><li>• JSON;</li><li>• GWT;</li><li>• JavaScript;</li><li>• Mobile;</li><li>• AJAX;</li><li>• HTML4;</li><li>• HTML5;</li><li>• Single Page Applications (SPAs);</li><li>• SOAP;</li><li>• .NET;</li><li>• Flash Remoting (AMF);</li><li>• Silverlight;</li><li>• Living in the DOM;</li><li>• Complex Sequences;</li><li>• CSRF / XSRF Token Tracking.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| მოწყვლადი კომპონენტები | <p>გადაწყვეტილებას უნდა გააჩნდეს მოცემულ მოწყვლად კომპონენტებზე სკანირების შესაძლებლობა:</p> <ul style="list-style-type: none"><li>• Apache Struts 2 Framework Checks;</li><li>• Apache Struts Detection;</li><li>• Arbitrary File Upload;</li><li>• ASP.NET Misconfiguration;</li><li>• Autocomplete attribute;</li><li>• Browser Cache directive (web application performance);</li><li>• Browser Cache directive (leaking sensitive information);</li><li>• Brute Force (HTTP Auth);</li><li>• Brute Force (Form Auth);</li><li>• Blind SQL;</li><li>• Clients Cross-Domain Policy Files;</li><li>• Information Disclosure in comments;</li><li>• Cookie attributes;</li><li>• Cross Origin Resources Sharing (CORS);</li><li>• Credentials over an insecure channel;</li><li>• Cross-Site Request Forgery (CSRF);</li><li>• Directory Indexing;</li><li>• Email Disclosure;</li><li>• Expression Language Injection;</li><li>• Forced Browsing;</li><li>• Sensitive Data Exposure;</li><li>• Form Session Strength;</li><li>• FrontPage Checks;</li><li>• Heartbleed Check;</li><li>• HTTP Strict Transport Security;</li><li>• HTTP Authentication over insecure channel;</li><li>• HTTPS Downgrade;</li></ul> |

- HTTP Headers;
- HTTP Response Splitting;
- Information Disclosure in response;
- Information Leakage in responses;
- Java Grinder;
- LDAP Injection;
- Local Storage Usage;
- Business logic abuse attacks;
- Nginx NULL code;
- OS Commanding;
- Parameter Fuzzing;
- Credentials stored in clear text in a cookie.;
- Collecting Sensitive Personal Information;
- PHP Code Execution;
- Privacy Disclosure;
- Privilege Escalation;
- Profanity;
- Reflection;
- File Inclusion;
- HTTP Verb Tampering;
- Predictable Resource Location;
- Reverse Clickjacking;
- Reverse Proxy;
- Information Disclosure in scripts;
- Secure and non-secure content mix;
- Sensitive data over an insecure channel;
- Server Configuration;
- Server Side Include (SSI) Injection;
- Session Fixation;
- Session Strength;
- Source Code Disclosure;
- SQL Information Leakage;
- SQL Injection;
- SQL injection Auth Bypass;
- SQL Parameter Check;
- SSL Strength;
- Unvalidated Redirect;
- URL rewriting;
- ASP.NET ViewState security;
- Web Beacon;
- Cross-site tracing (XST);
- X-Content-Type-Options;
- X-Frame-Options;
- X-XSS-Protection;
- XML External Entity Attack;
- XPath Injection;
- X-Powered-By;
- DOM Cross-site scripting (XSS);
- Persistent Cross-site scripting (XSS);



|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                       | <ul style="list-style-type: none"> <li>Reflected Cross-site scripting (XSS).</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| აუტენტიფიკაცია                        | <p>გადაწყვეტილებას უნდა გააჩნდეს მოცემული აუტენტიფიკაციის მეთოდების მხარდაჭერა:</p> <ul style="list-style-type: none"> <li>Simple Form Auth;</li> <li>SSO;</li> <li>Macro;</li> <li>HTTP Auth (Basic, Digest, NTLM);</li> <li>Multi-Factor;</li> <li>CAPTCHA;</li> <li>Selenium;</li> <li>Proxy Log;</li> <li>Session Hijacking;</li> <li>HMAC;</li> <li>OAuth;</li> <li>SSL Client Certificates (Including Smart Cards /CAC Cards).</li> </ul> |
| ინტეგრაცია - WAF/IPS                  | <p>გადაწყვეტილებას უნდა შეეძლოს სკანირების შედეგების საფუძველზე ვებ აპლიკაციების ბრენდაუერებისთვის და ქსელური ანომალიების აღმოჩენის სისტემებისთვის წესების (ე.წ. Virtual Patching) და კონფიგურაციის მომზადება.</p>                                                                                                                                                                                                                              |
|                                       | <p>გადაწყვეტილებას უნდა გააჩნდეს მოცემულ სისტემებთან (ვებ აპლიკაციების ბრენდმაუერები, ქსელური ანომალიების აღმოჩენის სისტემები) ინტეგრაცია:</p> <ul style="list-style-type: none"> <li>Sourcefire;</li> <li>ModSecurity;</li> <li>Barracuda;</li> <li>Trustwave;</li> <li>NitroSecurity;</li> <li>Citrix;</li> <li>DenyAll;</li> <li>Imperva;</li> <li>F5.</li> </ul>                                                                            |
| ინტეგრაცია - ავტომატიზაციის სისტემები | <p>გადაწყვეტილებას უნდა გააჩნდეს მოცემულავტომატიზაციისა და ტესტირების სისტემებთან ინტეგრაცია:</p> <ul style="list-style-type: none"> <li>Jenkins;</li> <li>Bamboo;</li> <li>JIRA;</li> <li>HP Quality Center;</li> <li>Selenium;</li> <li>Archer;</li> <li>Burp;</li> <li>Fiddler;</li> </ul>                                                                                                                                                   |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | <ul style="list-style-type: none"> <li>• Paros;</li> <li>• WebScarab;</li> <li>• Coverity &amp; Checkmarx;</li> <li>• SOAP (WSDLs) and RESTful APIs (Swagger).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| ინტეგრაცია - DevOps        | გადაწყვეტილებას უნდა გააჩნდეს DevOps და ხარისხის მაკონტროლებელ ხელსაწყოებთან ინტეგრაციის საშუალება სკანირების ავტომატიზაციისთვის.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| რეპორტირება - ექსპორტი     | <p>გადაწყვეტილებას უნდა გააჩნდეს რეპორტების ექსპორტირების საშუალება შემდეგ ფორმატებში:</p> <ul style="list-style-type: none"> <li>• PDF;</li> <li>• HTML;</li> <li>• XML.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| რეპორტირება - ინტერაქტიული | <p>გადაწყვეტილებას უნდა გააჩნდეს ინტერაქტიული რეპორტების გენერაციის საშუალება HTML ფორმატში, რომელიც შეიცავს მოცემულ ინფორმაციას და ფუნქციონალს:</p> <ul style="list-style-type: none"> <li>• მოწყვლადი კომპონენტის მდებარეობა (გვერდი და პარამეტრი)</li> <li>• დეტალური აღწერა, რეკომენდაციები და ნორმატიულ-ტექნიკური დოკუმენტაციის ლინკები</li> <li>• მოთხოვნა/მიწოდების ჩანაწერი, როგორც პირვანდელ ტრაფიკზე, ასევე შეტევის ტრაფიკზე</li> <li>• გამოკვეთილი მოწყვლადი კომპონენტები, შეტევის ტიპი, პირვანდელი მნიშვნელობა, შეტევის მნიშვნელობა;</li> <li>• შეტევის გადათამაშების შესაძლებლობა რეპორტიდანვე;</li> <li>• შეტევის განმეორებით ნახვა;</li> <li>• საწარმოო აპლიკაციასთან ურთიერთქმედების შესაძლებლობა, ახალი მოთხოვნების გაგზავნის და შედარების შესაძლებლობა.</li> </ul> |
| კომპონენტების განახლება    | გადაწყვეტილებას უნდა გააჩნდეს პროგრამული კომპონენტების განახლებებზე შეტყობინებების გაგზავნის (კონფიგურირებადი), მათი ავტომატური განახლების და ქრონოლოგიური აღწერის შესაძლებლობა.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ზოგადი მოთხოვნები          | გადაწყვეტილებას უნდა გააჩნდეს მულტიფუნქციური გარემო, რაც დაცული იქნება როლზე დაფუძნებული მართვის პრინციპით (ე.წ. Role-based Access Control).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|  |                                                                                                                                                                                 |
|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | გადაწყვეტილებას უნდა გააჩნდეს პროგრამირების ინტერფეისი – REST API                                                                                                               |
|  | გადაწყვეტილებას უნდა გააჩნდეს ბრძანებათა გადაცემის ინტერფეისი (ე.წ. command-line interface – CLI)                                                                               |
|  | გადაწყვეტილებას უნდა გააჩნდეს სკანირების ორი მიდგომა: ჩვეულებრივი სკანირება და სიმულაციური სკანირება, რაც უნდა ეფუძნებოდეს წინასწარ განსაზღვრულ შეტევებს - არანაკლებ 80 შეტევა. |
|  | გადაწყვეტილებას უნდა შეეძლოს კომპლექსური სამუშაო პროცესის აგება, რომელიც შეიცავს აპლიკაციის თანმიმდევრულ და რამოდენიმე ნაბიჯიან დამუშავებას.                                    |
|  | გადაწყვეტილებას უნდა შეეძლოს სამუშაო პროცესის ჩაწერა ქმედებების თანმიმდევრულობის ასაგებად.                                                                                      |
|  | გადაწყვეტილებას უნდა შეეძლოს ინდივიდუალური შეტევების (ე.წ. Custom Attack) შექმნის შესაძლებლობა.                                                                                 |
|  | გადაწყვეტილებას უნდა გააჩნდეს გარემო საიდანაც შესაძლებელი იქნება შეტევების ახალი მოდულის დამატება.                                                                              |
|  | გადაწყვეტილებას უნდა გააჩნდეს უსაფრთხო სკანირების რეჟიმი საწარმოო გარემოს ტესტირებისთვის.                                                                                       |
|  | გადაწყვეტილებას უნდა შეეძლოს ვებ აპლიკაციების ცვლილებების იდენტიფიცირება.                                                                                                       |
|  | გადაწყვეტილებას უნდა შეეძლოს ვებ აპლიკაციების მონიტორინგი რეალურ დროში და განახლებების იდენტიფიცირება.                                                                          |
|  | გადაწყვეტილებას უნდა შეეძლოს განახლებული პროგრამული კოდის შემოწმება, მთლიანი ვებ აპლიკაციის შემოწმების გარეშე.                                                                  |
|  | გადაწყვეტილებას უნდა შეეძლოს შეტევის სიმძიმის კონფიგურაცია.                                                                                                                     |
|  | გადაწყვეტილებას უნდა შეეძლოს ნებისმიერ მოწყვლად კომპონენტზე რეიტინგის, პრიორიტეტის და სიმძიმის განსაზღვრა.                                                                      |
|  | გადაწყვეტილებას უნდა შეეძლოს WSDL ფაილების ავტომატური აღმოჩენა და გარჩევა.                                                                                                      |
|  | გადაწყვეტილებას უნდა შეეძლოს კომპლექსური SOAP შეტევების განხორციელება.                                                                                                          |
|  | გადაწყვეტილებას უნდა შეეძლოს მოწყვლადი კომპონენტების აღმოჩენის პროცესის ჩაწერა შემდგომში სანახავად.                                                                             |
|  | გადაწყვეტილებას უნდა გააჩნდეს სპეციალური ტექნიკები ცრუ შეტყობინებების შესამცირებლად.                                                                                            |