**Vulnerability Assessment Report**

**For**



**USUI**

**Date March 03 2022**

**Document Security Level:** Confidential

**Document Version:** 1.0

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Edit Report** | **Editor** |
| 1.0 | March 03 2022 | Creation | INET Managed Services |

|  |  |  |  |
| --- | --- | --- | --- |
| USUI | | INET Managed Services CO., LTD. | |
| Name |  | **Name** |  |
| Position |  | **Position** |  |
| Tel |  | **Tel** |  |
| Signature |  | **Signature** |  |

**Table of Contents**

[1. Restrictions on disclosure and use of information 4](#_Toc97201647)

[2. Operation Method 5](#_Toc97201648)

[3. Project Scope 6](#_Toc97201649)

[3.1 Infrastructure Vulnerability Assessment 6](#_Toc97201650)

[3.2 Web Application Vulnerability Assessment 6](#_Toc97201651)

[4. Testing Tools 7](#_Toc97201652)

[5. Infrastructure Vulnerability Assessment 7](#_Toc97201653)

[5.1 Target Information 8](#_Toc97201654)

[5.2 Executive summary 9](#_Toc97201655)

[5.2.1 Summary Vulnerability by Severity 9](#_Toc97201656)

[5.2.2 Vulnerability by Target 9](#_Toc97201657)

[5.3 Infrastructure Vulnerability Detail 11](#_Toc97201658)

[6. Web Application Vulnerability Assessment 12](#_Toc97201659)

[6.1 Target Information 13](#_Toc97201660)

[6.2 Executive summary 14](#_Toc97201661)

[6.2.1 Summary Vulnerability by Severity 14](#_Toc97201662)

[6.2.2 Vulnerability by Target 14](#_Toc97201663)

[6.3 Web Application Vulnerability Detail 15](#_Toc97201664)

[7. Port Discovery 18](#_Toc97201665)

[8. Appendix 19](#_Toc97201666)

[8.1 About Nessus 19](#_Toc97201667)

[8.1.1 Nessus vulnerabilities 19](#_Toc97201668)

[8.1.2 Nessus risk score 19](#_Toc97201669)

[8.2 About Acunetix 21](#_Toc97201670)

[8.2.1 Acunetix web vulnerabilities 21](#_Toc97201671)

[8.2.2 Acunetix risk score 22](#_Toc97201672)

# Restrictions on disclosure and use of information

Restriction on Disclosure and Use of Confidential Information. The Executive understands and agrees that the Confidential Information constitutes an asset of the Company and its affiliated entities and may not be converted to the Executive's own use. Accordingly, the Executive hereby agrees that the Executive shall not, directly, or indirectly, at any time, reveal, divulge, or disclose to any Person not expressly authorized by the Company any Confidential Information, and the Executive shall not, directly, or indirectly, use or make use of any Confidential Information in connection with any business activity other than that of the Company. The parties acknowledge and agree that this Agreement is not intended to, and does not, alter either the Company's rights or the Executive's obligations under any state or federal statutory or common law regarding trade secrets and unfair trade.

# Operation Method

* 1. Posture Review
  2. Information Gathering
  3. Enumeration
  4. Vulnerability Assessment
  5. Analyze & Evaluate Risk Value
  6. Report



Figure 1: Operation Method

# Project Scope

## **3.1 Infrastructure Vulnerability Assessment**

**Target / IP Address:**

| **No.** | **Domain / Server Name** | **Public IP Address** | **Private IP Address** | **OS/Model** | **Functions** | **Public Assessment** | **Private Assessment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | DATABASE01 | - | 172.16.69.13 | Ubuntu 18 | Database Server 01 |  | ✓ |
| 2 | WEB01 | 123.123.123.123 | 172.16.69.14 | Ubuntu 20 | Web Server |  | ✓ |
| 3 | TERM | - | 172.16.69.52 | Windows Server 2016 | Terminal Server |  | ✓ |
| 4 | SMB01 | 12.12.12.12 | 172.16.69.53 | Windows Server 2019 | SMB Server |  | ✓ |
| 5 | DATABASE02 | - | 172.16.69.54 | Ubuntu 18 | Database Server 02 |  | ✓ |

## **3.2 Web Application Vulnerability Assessment**

**Target / IP Address:**

| **No.** | **Domain / Server Name** | **Public IP Address** | **Private IP Address** | **OS/Model** | **Functions** | **Public Assessment** | **Private Assessment** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | https://example.com/ | 123.123.123.123 | 172.16.69.14 | Ubuntu 20 | เว็บไซต์ขายของ | ✓ |  |

# Testing Tools

|  |  |
| --- | --- |
| **Tool Name** | **Testing Type** |
| Nmap | Host and Service Discovery |
| Nessus | Infrastructure Vulnerability Assessment |
| Acunetix | Web Application Vulnerability Assessment |

# Infrastructure Vulnerability Assessment

**Vulnerability Assessment from Public Access (for public target)**

**Testing date:** March 30, 2021

**Tester IP Address:** 203.150.110.29

Diagram

Description automatically generated

Figure 2: Vulnerability Assessment from Public Access

**Vulnerability Assessment from Private Access (for private or restricted access target)**

**Testing date:** March 30, 2021

**Tester IP Address:** Private IP from VPN access

A picture containing diagram

Description automatically generated

Figure 3: Vulnerability Assessment from Private Access

## **5.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 |  | 192.168.5.203 |  | TCP : 80, 1745, 3389, 8080 |
| 2 |  | 192.168.100.102 |  | TCP : 25, 80, 135, 139, 143, 443, 445, 593, 691, 993, 1047, 1052, 1053, 1058, 1117, 1126, 1127, 1150, 1179, 1183, 3389, 6001, 6002, 6004 UDP : 1118, 1128, 1180, 1184 |
| 3 |  | 192.168.100.103 |  | TCP : 135, 139, 445, 3389, 5800, 5900, 5985, 49664, 49665, 49669, 49672, 49673, 49706, 49718, 49735, 49780 |
| 4 |  | 192.168.100.106 |  | TCP : 21, 80, 81, 82, 135, 139, 443, 445, 990, 1801, 2103, 2105, 2107, 3306, 3389, 5985, 8443, 49664, 49665, 49669, 49670, 49677, 49699, 49707, 49736, 49751 |
| 5 |  | 203.154.244.93 |  | TCP : 4443, 4444, 8443 UDP : 500 |

## **5.2 Executive summary**

The purpose of this activity is to find the vulnerability on the target infrastructure.

### **5.2.1 Summary Vulnerability by Severity**

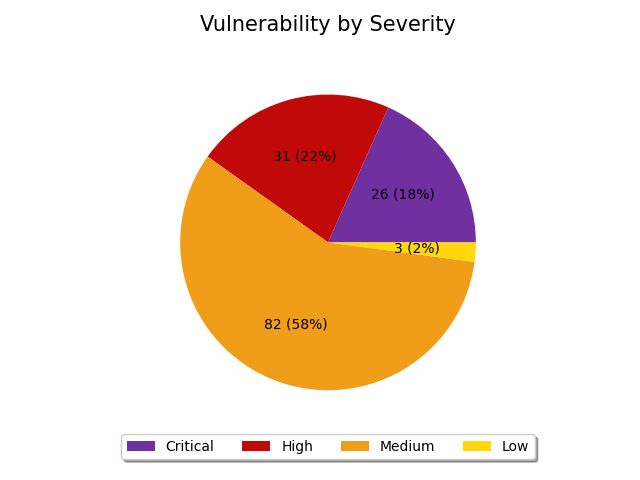


Figure 4: Summary by Severity of Infrastructure Vulnerability Assessment

### **5.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | - | 192.168.5.203 | 0 | 0 | 0 | 0 | 0 |
| 2 | - | 192.168.100.102 | 8 | 4 | 16 | 3 | 31 |
| 3 | - | 192.168.100.103 | 0 | 1 | 5 | 0 | 6 |
| 4 | - | 192.168.100.106 | 18 | 26 | 57 | 0 | 101 |
| 5 | - | 203.154.244.93 | 0 | 0 | 4 | 0 | 4 |
| **Total** | | | 26 | 31 | 82 | 3 | 142 |

## **5.3 Infrastructure Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Unsupported Web Server Detection |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.102(80, 443), 192.168.100.106(80, 443) | | |
| **Detail** | According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities. | | |
| **Solution** | Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (uncredentialed check) |
| **Severity** | Critical | **Port** | TCP: 445 |
| **Target** | 192.168.100.102(445) | | |
| **Detail** | The remote Windows host is affected by a remote code execution vulnerability in the 'Server' service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with 'System' privileges. ECLIPSEDWING is one of multiple Equation Group vulnerabilities and exploits disclosed on 2017/04/14 by a group known as the Shadow Brokers. | | |
| **Solution** | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008. | | |
| **Remark** | https://www.nessus.org/u?adf86aac | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution (958687) (uncredentialed check) |
| **Severity** | Critical | **Port** | TCP: 445 |
| **Target** | 192.168.100.102(445) | | |
| **Detail** | The remote host is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the remote host. | | |
| **Solution** | Microsoft has released a set of patches for Windows 2000, XP, 2003, Vista and 2008. | | |
| **Remark** | http://www.microsoft.com/technet/security/bulletin/ms09-001.mspx | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 4 | **Finding** | Microsoft Windows Server 2003 Unsupported Installation Detection |
| **Severity** | Critical | **Port** | TCP: 0 |
| **Target** | 192.168.100.102(0) | | |
| **Detail** | The remote host is running Microsoft Windows Server 2003. Support for this operating system by Microsoft ended July 14th, 2015. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities. | | |
| **Solution** | Upgrade to a version of Windows that is currently supported. | | |
| **Remark** | http://www.nessus.org/u?76f71a39 http://www.nessus.org/u?321523eb https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/ http://www.nessus.org/u?8dcab5e4 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 5 | **Finding** | Microsoft IIS 6.0 Unsupported Version Detection |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.102(80, 443) | | |
| **Detail** | According to its self-reported version number, the installation of Microsoft Internet Information Services (IIS) 6.0 on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of Microsoft IIS that is currently supported. | | |
| **Remark** | http://www.nessus.org/u?d99a8431 https://www.microsoft.com/en-us/cloud-platform/windows-server-2003 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 6 | **Finding** | Unsupported Windows OS (remote) |
| **Severity** | Critical | **Port** | TCP: 0 |
| **Target** | 192.168.100.102(0) | | |
| **Detail** | The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a supported service pack or operating system | | |
| **Remark** | https://support.microsoft.com/en-us/lifecycle | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 7 | **Finding** | Apache 2.2.x 2.2.15 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.15. It is, therefore, potentially affected by multiple vulnerabilities :  - A TLS renegotiation prefix injection attack is possible.   (CVE-2009-3555)  - The 'mod\_proxy\_ajp' module returns the wrong status code  if it encounters an error which causes the back-end   server to be put into an error state. (CVE-2010-0408)  - The 'mod\_isapi' attempts to unload the 'ISAPI.dll' when  it encounters various error states which could leave  call-backs in an undefined state. (CVE-2010-0425)  - A flaw in the core sub-request process code can lead to  sensitive information from a request being handled by   the wrong thread if a multi-threaded environment is  used. (CVE-2010-0434)  - Added 'mod\_reqtimeout' module to mitigate Slowloris  attacks. (CVE-2007-6750) | | |
| **Solution** | Upgrade to Apache version 2.2.15 or later. | | |
| **Remark** | http://httpd.apache.org/security/vulnerabilities\_22.html https://bz.apache.org/bugzilla/show\_bug.cgi?id=48359 https://archive.apache.org/dist/httpd/CHANGES\_2.2.15 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 8 | **Finding** | Apache 2.2.x 2.2.13 APR apr\_palloc Heap Overflow |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its self-reported banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.13. As such, it includes a bundled version of the Apache Portable Runtime (APR) library that contains a flaw in 'apr\_palloc()' that could cause a heap overflow.  Note that the Apache HTTP server itself does not pass unsanitized, user-provided sizes to this function so it could only be triggered through some other application that uses it in a vulnerable way. | | |
| **Solution** | Upgrade to Apache 2.2.13 or later. | | |
| **Remark** | http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 9 | **Finding** | PHP Unsupported Version Detection |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its version, the installation of PHP on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of PHP that is currently supported. | | |
| **Remark** | http://php.net/eol.php https://wiki.php.net/rfc/releaseprocess | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 10 | **Finding** | OpenSSL Unsupported |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the remote web server is running a version of OpenSSL that is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. | | |
| **Solution** | Upgrade to a version of OpenSSL that is currently supported. | | |
| **Remark** | https://www.openssl.org/policies/releasestrat.html http://www.nessus.org/u?4d55548d | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 11 | **Finding** | OpenSSL 1.0.1 1.0.1u Multiple Vulnerabilities (SWEET32) |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the remote host is running a version of OpenSSL 1.0.1 prior to 1.0.1u. It is, therefore, affected by the following vulnerabilities :   - Multiple integer overflow conditions exist in s3\_srvr.c,  ssl\_sess.c, and t1\_lib.c due to improper use of pointer  arithmetic for heap-buffer boundary checks. An  unauthenticated, remote attacker can exploit this to  cause a denial of service. (CVE-2016-2177)   - An information disclosure vulnerability exists in the  dsa\_sign\_setup() function in dsa\_ossl.c due to a failure  to properly ensure the use of constant-time operations.  An unauthenticated, remote attacker can exploit this,  via a timing side-channel attack, to disclose DSA key  information. (CVE-2016-2178)   - A denial of service vulnerability exists in the DTLS  implementation due to a failure to properly restrict the  lifetime of queue entries associated with unused  out-of-order messages. An unauthenticated, remote  attacker can exploit this, by maintaining multiple  crafted DTLS sessions simultaneously, to exhaust memory.  (CVE-2016-2179)   - An out-of-bounds read error exists in the X.509 Public  Key Infrastructure Time-Stamp Protocol (TSP)  implementation. An unauthenticated, remote attacker can  exploit this, via a crafted time-stamp file that is  mishandled by the 'openssl ts' command, to cause   denial of service or to disclose sensitive information.  (CVE-2016-2180)   - A denial of service vulnerability exists in the  Anti-Replay feature in the DTLS implementation due to  improper handling of epoch sequence numbers in records.  An unauthenticated, remote attacker can exploit this,  via spoofed DTLS records, to cause legitimate packets to  be dropped. (CVE-2016-2181)   - An overflow condition exists in the BN\_bn2dec() function  in bn\_print.c due to improper validation of  user-supplied input when handling BIGNUM values. An  unauthenticated, remote attacker can exploit this to  crash the process. (CVE-2016-2182)   - A vulnerability exists, known as SWEET32, in the 3DES  and Blowfish algorithms due to the use of weak 64-bit  block ciphers by default. A man-in-the-middle attacker  who has sufficient resources can exploit this  vulnerability, via a 'birthday' attack, to detect a  collision that leaks the XOR between the fixed secret  and a known plaintext, allowing the disclosure of the  secret text, such as secure HTTPS cookies, and possibly  resulting in the hijacking of an authenticated session.  (CVE-2016-2183)   - A flaw exists in the tls\_decrypt\_ticket() function in  t1\_lib.c due to improper handling of ticket HMAC  digests. An unauthenticated, remote attacker can exploit  this, via a ticket that is too short, to crash the  process, resulting in a denial of service.  (CVE-2016-6302)   - An integer overflow condition exists in the   MDC2\_Update() function in mdc2dgst.c due to improper  validation of user-supplied input. An unauthenticated,  remote attacker can exploit this to cause a heap-based  buffer overflow, resulting in a denial of service  condition or possibly the execution of arbitrary code.  (CVE-2016-6303)   - A flaw exists in the ssl\_parse\_clienthello\_tlsext()  function in t1\_lib.c due to improper handling of overly  large OCSP Status Request extensions from clients. An  unauthenticated, remote attacker can exploit this, via  large OCSP Status Request extensions, to exhaust memory  resources, resulting in a denial of service condition.  (CVE-2016-6304)   - An out-of-bounds read error exists in the certificate  parser that allows an unauthenticated, remote attacker  to cause a denial of service via crafted certificate  operations. (CVE-2016-6306)   - A flaw exists in the GOST ciphersuites due to the use of  long-term keys to establish an encrypted connection. A  man-in-the-middle attacker can exploit this, via a Key  Compromise Impersonation (KCI) attack, to impersonate  the server. | | |
| **Solution** | Upgrade to OpenSSL version 1.0.1u or later.  Note that the GOST ciphersuites vulnerability is not yet fixed by the vendor in an official release; however, a patch for the issue has been committed to the OpenSSL github repository. | | |
| **Remark** | https://www.openssl.org/news/secadv/20160922.txt http://www.nessus.org/u?09b29b30 https://sweet32.info/ https://www.openssl.org/blog/blog/2016/08/24/sweet32/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 12 | **Finding** | Apache 2.2.x 2.2.33-dev / 2.4.x 2.4.26 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.33-dev or 2.4.x prior to 2.4.26. It is, therefore, affected by the following vulnerabilities :   - An authentication bypass vulnerability exists due to  third-party modules using the ap\_get\_basic\_auth\_pw()  function outside of the authentication phase. An  unauthenticated, remote attacker can exploit this to  bypass authentication requirements. (CVE-2017-3167)   - A NULL pointer dereference flaw exists due to  third-party module calls to the mod\_ssl  ap\_hook\_process\_connection() function during an HTTP  request to an HTTPS port. An unauthenticated, remote  attacker can exploit this to cause a denial of service  condition. (CVE-2017-3169)   - A NULL pointer dereference flaw exists in mod\_http2 that  is triggered when handling a specially crafted HTTP/2  request. An unauthenticated, remote attacker can exploit  this to cause a denial of service condition. Note that  this vulnerability does not affect 2.2.x.  (CVE-2017-7659)   - An out-of-bounds read error exists in the  ap\_find\_token() function due to improper handling of  header sequences. An unauthenticated, remote attacker  can exploit this, via a specially crafted header  sequence, to cause a denial of service condition.  (CVE-2017-7668)   - An out-of-bounds read error exists in mod\_mime due to  improper handling of Content-Type response headers. An  unauthenticated, remote attacker can exploit this, via a  specially crafted Content-Type response header, to cause  a denial of service condition or the disclosure of  sensitive information. (CVE-2017-7679)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.2.33-dev / 2.4.26 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.32 https://archive.apache.org/dist/httpd/CHANGES\_2.4.26 https://httpd.apache.org/security/vulnerabilities\_22.html https://httpd.apache.org/security/vulnerabilities\_24.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 13 | **Finding** | Apache 2.2.x 2.2.34 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache running on the remote host is 2.2.x prior to 2.2.34. It is, therefore, affected by the following vulnerabilities :   - An authentication bypass vulnerability exists in httpd  due to third-party modules using the  ap\_get\_basic\_auth\_pw() function outside of the  authentication phase. An unauthenticated, remote  attacker can exploit this to bypass authentication  requirements. (CVE-2017-3167)   - A denial of service vulnerability exists in httpd due to  a NULL pointer dereference flaw that is triggered when a  third-party module calls the mod\_ssl  ap\_hook\_process\_connection() function during an HTTP  request to an HTTPS port. An unauthenticated, remote  attacker can exploit this to cause a denial of service  condition. (CVE-2017-3169)   - A denial of service vulnerability exists in httpd due to  an out-of-bounds read error in the ap\_find\_token()  function that is triggered when handling a specially  crafted request header sequence. An unauthenticated,  remote attacker can exploit this to crash the  service or force ap\_find\_token() to return an incorrect  value. (CVE-2017-7668)   - A denial of service vulnerability exists in httpd due to  an out-of-bounds read error in the mod\_mime that is  triggered when handling a specially crafted Content-Type  response header. An unauthenticated, remote attacker can  exploit this to disclose sensitive information or cause  a denial of service condition. (CVE-2017-7679)   - A denial of service vulnerability exists in httpd due to  a failure to initialize or reset the value placeholder  in [Proxy-]Authorization headers of type 'Digest' before  or between successive key=value assignments by  mod\_auth\_digest. An unauthenticated, remote attacker can  exploit this, by providing an initial key with no '='  assignment, to disclose sensitive information or cause a  denial of service condition. (CVE-2017-9788)  Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.2.34 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.34 https://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 14 | **Finding** | Apache 2.4.49 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.   - A crafted request uri-path can cause mod\_proxy to forward the request to an origin server choosen by the  remote user. (CVE-2021-40438)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.4.49 or later. | | |
| **Remark** | https://downloads.apache.org/httpd/CHANGES\_2.4 https://httpd.apache.org/security/vulnerabilities\_24.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 15 | **Finding** | Apache 2.4.49 Multiple Vulnerabilities |
| **Severity** | Critical | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.49 changelog.   - ap\_escape\_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass  untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)   - Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798)  Note that Nessus has not tested for this issue but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.4.49 or later. | | |
| **Remark** | https://downloads.apache.org/httpd/CHANGES\_2.4 https://httpd.apache.org/security/vulnerabilities\_24.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 16 | **Finding** | SSL Version 2 and 3 Protocol Detection |
| **Severity** | High | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:  - An insecure padding scheme with CBC ciphers.  - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'. | | |
| **Solution** | Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead. | | |
| **Remark** | https://www.schneier.com/academic/paperfiles/paper-ssl.pdf http://www.nessus.org/u?b06c7e95 http://www.nessus.org/u?247c4540 https://www.openssl.org/~bodo/ssl-poodle.pdf http://www.nessus.org/u?5d15ba70 https://www.imperialviolet.org/2014/10/14/poodle.html https://tools.ietf.org/html/rfc7507 https://tools.ietf.org/html/rfc7568 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 17 | **Finding** | Microsoft Windows SMB NULL Session Authentication |
| **Severity** | High | **Port** | TCP: 445 |
| **Target** | 192.168.100.102(445) | | |
| **Detail** | The remote host is running Microsoft Windows. It is possible to   log into it using a NULL session (i.e., with no login or password).  Depending on the configuration, it may be possible for an unauthenticated, remote attacker to leverage this issue to   get information about the remote host. | | |
| **Solution** | Apply the following registry changes per the referenced Technet advisories :    Set :   - HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1  - HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1  Reboot once the registry changes are complete. | | |
| **Remark** | http://www.nessus.org/u?e32d594f http://www.nessus.org/u?9182e66b http://www.nessus.org/u?a33fe205 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 18 | **Finding** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | High | **Port** | TCP: 443, 3389, 8443 |
| **Target** | 192.168.100.102(443), 192.168.100.103(3389), 192.168.100.106(3389, 8443) | | |
| **Detail** | The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or  else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network. | | |
| **Solution** | Reconfigure the affected application if possible to avoid use of medium strength ciphers. | | |
| **Remark** | https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 19 | **Finding** | MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387) (uncredentialed check) |
| **Severity** | High | **Port** | TCP: 3389 |
| **Target** | 192.168.100.102(3389) | | |
| **Detail** | An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the remote Windows host. The vulnerability is due to the way that RDP accesses an object in memory that has been improperly initialized or has been deleted.  If RDP has been enabled on the affected system, an unauthenticated, remote attacker could leverage this vulnerability to cause the system to execute arbitrary code by sending a sequence of specially crafted RDP packets to it.  This plugin also checks for a denial of service vulnerability in Microsoft Terminal Server.  Note that this script does not detect the vulnerability if the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting is enabled or the security layer is set to 'SSL (TLS 1.0)' on the remote host. | | |
| **Solution** | Microsoft has released a set of patches for Windows XP, 2003, Vista, 2008, 7, and 2008 R2. Note that an extended support contract with Microsoft is required to obtain the patch for this vulnerability for Windows 2000. | | |
| **Remark** | https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2012/ms12-020 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 20 | **Finding** | PHP 5 5.2.7 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is prior to 5.2.7. It is, therefore, affected by multiple vulnerabilities :  - There is a buffer overflow flaw in the bundled PCRE  library that allows a denial of service attack.  (CVE-2008-2371)  - Multiple directory traversal vulnerabilities exist in  functions such as 'posix\_access', 'chdir', and 'ftok'  that allow a remote attacker to bypass 'safe\_mode'  restrictions. (CVE-2008-2665 and CVE-2008-2666).  - A buffer overflow flaw in 'php\_imap.c' may be triggered  when processing long message headers due to the use of  obsolete API calls. This can be exploited to cause a  denial of service or to execute arbitrary code.  (CVE-2008-2829)  - A buffer overflow in the 'imageloadfont' function in  'ext/gd/gd.c' can be triggered when a specially crafted  font is given. This can be exploited to cause a denial  of service or to execute arbitrary code. (CVE-2008-3658)  - A buffer overflow flaw exists in PHP's internal function  'memnstr' which can be exploited by an attacker using  the delimiter argument to the 'explode' function. This  can be used to cause a denial of service or to execute  arbitrary code. (CVE-2008-3659)  - When PHP is used as a FastCGI module, an attacker by  requesting a file whose file name extension is preceded  by multiple dots can cause a denial of service.  (CVE-2008-3660)  - A heap-based buffer overflow flaw in the mbstring  extension can be triggered via a specially crafted  string containing an HTML entity that is not handled  during Unicode conversion. This can be exploited to  execute arbitrary code.(CVE-2008-5557)  - Improper initialization of global variables 'page\_uid'  and 'page\_gid' when PHP is used as an Apache module  allows the bypassing of security restriction due to  SAPI 'php\_getuid' function overloading. (CVE-2008-5624)  - PHP does not enforce the correct restrictions when  'safe\_mode' is enabled through a 'php\_admin\_flag'  setting in 'httpd.conf'. This allows an attacker, by  placing a specially crafted 'php\_value' entry in  '.htaccess', to able to write to arbitrary files.  (CVE-2008-5625)  - The 'ZipArchive::extractTo' function in the ZipArchive  extension fails to filter directory traversal sequences  from file names. An attacker can exploit this to write  to arbitrary files. (CVE-2008-5658)  - Under limited circumstances, an attacker can cause a  file truncation to occur when calling the 'dba\_replace'  function with an invalid argument. (CVE-2008-7068)  - A buffer overflow error exists in the function  'date\_from\_ISO8601' function within file 'xmlrpc.c'  because user-supplied input is improperly validated.  This can be exploited by a remote attacker to cause a  denial of service or to execute arbitrary code.  (CVE-2014-8626) | | |
| **Solution** | Upgrade to PHP version 5.2.8 or later. Note that version 5.2.7 has been removed from distribution because of a regression in that version that results in the 'magic\_quotes\_gpc' setting remaining off even if it was set to on. | | |
| **Remark** | http://cxsecurity.com/issue/WLB-2008110041 http://cxsecurity.com/issue/WLB-2008110058 http://cxsecurity.com/issue/WLB-2008120011 https://seclists.org/fulldisclosure/2008/Jun/237 https://seclists.org/fulldisclosure/2008/Jun/238 https://www.openwall.com/lists/oss-security/2008/08/08/2 https://www.openwall.com/lists/oss-security/2008/08/13/8 https://seclists.org/fulldisclosure/2008/Nov/674 https://seclists.org/fulldisclosure/2008/Dec/90 https://bugs.php.net/bug.php?id=42862 https://bugs.php.net/bug.php?id=45151 https://bugs.php.net/bug.php?id=45722 http://www.php.net/releases/5\_2\_7.php http://www.php.net/ChangeLog-5.php#5.2.7 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 21 | **Finding** | PHP 5.2.8 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is earlier than 5.2.8. As such, it is potentially affected by the following vulnerabilities :  - PHP fails to properly sanitize error messages of  arbitrary HTML or script code, would code allow for   cross-site scripting attacks if PHP's 'display\_errors'   setting is enabled. (CVE-2008-5814)  - Version 5.2.7 introduced a regression with regard to  'magic\_quotes' functionality due to an incorrect fix to   the filter extension. As a result, the   'magic\_quotes\_gpc' setting remains off even if it is set   to on. (CVE-2008-5844) | | |
| **Solution** | Upgrade to PHP version 5.2.8 or later. | | |
| **Remark** | https://bugs.php.net/bug.php?id=42718 http://www.php.net/releases/5\_2\_8.php | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 22 | **Finding** | Apache 2.2.x 2.2.12 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x. running on the remote host is prior to 2.2.12. It is, therefore, affected by the following vulnerabilities :  - A heap-based buffer underwrite flaw exists in the  function 'apr\_strmatch\_precompile()' in the bundled copy  of the APR-util library, which could be triggered when  parsing configuration data to crash the daemon.  (CVE-2009-0023)  - A flaw in the mod\_proxy\_ajp module in version 2.2.11  only may allow a remote attacker to obtain sensitive  response data intended for a client that sent an  earlier POST request with no request body.  (CVE-2009-1191)  - The server does not limit the use of directives in a  .htaccess file as expected based on directives such  as 'AllowOverride' and 'Options' in the configuration  file, which could enable a local user to bypass  security restrictions. (CVE-2009-1195)  - Failure to properly handle an amount of streamed data  that exceeds the Content-Length value allows a remote  attacker to force a proxy process to consume CPU time  indefinitely when mod\_proxy is used in a reverse proxy  configuration. (CVE-2009-1890)  - Failure of mod\_deflate to stop compressing a file when  the associated network connection is closed may allow a  remote attacker to consume large amounts of CPU if  there is a large (>10 MB) file available that has  mod\_deflate enabled. (CVE-2009-1891)  - Using a specially crafted XML document with a large  number of nested entities, a remote attacker may be  able to consume an excessive amount of memory due to  a flaw in the bundled expat XML parser used by the  mod\_dav and mod\_dav\_svn modules. (CVE-2009-1955)  - There is an off-by-one overflow in the function  'apr\_brigade\_vprintf()' in the bundled copy of the  APR-util library in the way it handles a variable list  of arguments, which could be leveraged on big-endian  platforms to perform information disclosure or denial  of service attacks. (CVE-2009-1956) Note that Nessus has relied solely on the version in the Server response header and did not try to check for the issues themselves or even whether the affected modules are in use. | | |
| **Solution** | Upgrade to Apache version 2.2.12 or later. Alternatively, ensure that the affected modules / directives are not in use. | | |
| **Remark** | http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 23 | **Finding** | PHP 5.2.11 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is older than 5.2.11. Such versions may be affected by several security issues :  - An unspecified error occurs in certificate validation  inside 'php\_openssl\_apply\_verification\_policy'.  - An unspecified input validation vulnerability affects  the color index in 'imagecolortransparent()'.  - An unspecified input validation vulnerability affects  exif processing.  - Calling 'popen()' with an invalid mode can cause a  crash under Windows. (Bug #44683)  - An integer overflow in 'xml\_utf8\_decode()' can make it  easier to bypass cross-site scripting and SQL injection   protection mechanisms using a specially crafted string   with a long UTF-8 encoding. (Bug #49687)  - 'proc\_open()' can bypass 'safe\_mode\_protected\_env\_vars'.  (Bug #49026) | | |
| **Solution** | Upgrade to PHP version 5.2.11 or later. | | |
| **Remark** | http://www.php.net/ChangeLog-5.php#5.2.11 http://www.php.net/releases/5\_2\_11.php http://news.php.net/php.internals/45597 http://www.php.net/ChangeLog-5.php#5.2.11 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 24 | **Finding** | Apache 2.2.x 2.2.14 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the  remote host is prior to 2.2.14. It is, therefore, potentially affected by multiple vulnerabilities :  - Faulty error handling in the Solaris pollset support   could lead to a denial of service. (CVE-2009-2699)  - The 'mod\_proxy\_ftp' module allows remote attackers to   bypass intended access restrictions. (CVE-2009-3095)  - The 'ap\_proxy\_ftp\_handler' function in   'modules/proxy/proxy\_ftp.c' in the 'mod\_proxy\_ftp'   module allows remote FTP servers to cause a   denial of service. (CVE-2009-3094) Note that the remote web server may not actually be affected by these vulnerabilities as Nessus did not try to determine whether the affected modules are in use or check for the issues themselves. | | |
| **Solution** | Upgrade to Apache version 2.2.14 or later. Alternatively, ensure that the affected modules are not in use. | | |
| **Remark** | http://www.securityfocus.com/advisories/17947 http://www.securityfocus.com/advisories/17959 http://www.nessus.org/u?e470f137 https://bz.apache.org/bugzilla/show\_bug.cgi?id=47645 http://www.nessus.org/u?c34c4eda | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 25 | **Finding** | PHP 5.2 5.2.14 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.14. Such versions may be affected by several security issues :  - An error exists when processing invalid XML-RPC   requests that can lead to a NULL pointer  dereference. (bug #51288) (CVE-2010-0397)  - An error exists in the function 'fnmatch' that can lead  to stack exhaustion.  - An error exists in the sqlite extension that could   allow arbitrary memory access.  - A memory corruption error exists in the function  'substr\_replace'.  - The following functions are not properly protected  against function interruptions :  addcslashes, chunk\_split, html\_entity\_decode,   iconv\_mime\_decode, iconv\_substr, iconv\_mime\_encode,  htmlentities, htmlspecialchars, str\_getcsv,  http\_build\_query, strpbrk, strstr, str\_pad,  str\_word\_count, wordwrap, strtok, setcookie,   strip\_tags, trim, ltrim, rtrim, parse\_str, pack, unpack,   uasort, preg\_match, strrchr, strchr, substr, str\_repeat  (CVE-2010-1860, CVE-2010-1862, CVE-2010-1864,  CVE-2010-2097, CVE-2010-2100, CVE-2010-2101,  CVE-2010-2190, CVE-2010-2191, CVE-2010-2484)  - The following opcodes are not properly protected   against function interruptions :  ZEND\_CONCAT, ZEND\_ASSIGN\_CONCAT, ZEND\_FETCH\_RW  (CVE-2010-2191)  - The default session serializer contains an error  that can be exploited when assigning session  variables having user defined names. Arbitrary  serialized values can be injected into sessions by  including the PS\_UNDEF\_MARKER, '!', character in  variable names.  - A use-after-free error exists in the function  'spl\_object\_storage\_attach'. (CVE-2010-2225)  - An information disclosure vulnerability exists in the  function 'var\_export' when handling certain error   conditions. (CVE-2010-2531) | | |
| **Solution** | Upgrade to PHP version 5.2.14 or later. | | |
| **Remark** | http://www.php.net/releases/5\_2\_14.php http://www.php.net/ChangeLog-5.php#5.2.14 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 26 | **Finding** | PHP 5.3.9 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is older than 5.3.9. As such, it may be affected by the following security issues :  - The 'is\_a()' function in PHP 5.3.7 and 5.3.8 triggers a   call to '\_\_autoload()'. (CVE-2011-3379)  - It is possible to create a denial of service condition   by sending multiple, specially crafted requests   containing parameter values that cause hash collisions   when computing the hash values for storage in a hash   table. (CVE-2011-4885)    - An integer overflow exists in the exif\_process\_IFD\_TAG   function in exif.c that can allow a remote attacker to   read arbitrary memory locations or cause a denial of   service condition. This vulnerability only affects PHP   5.4.0beta2 on 32-bit platforms. (CVE-2011-4566)  - Calls to libxslt are not restricted via  xsltSetSecurityPrefs(), which could allow an attacker  to create or overwrite files, resulting in arbitrary  code execution. (CVE-2012-0057)  - An error exists in the function 'tidy\_diagnose' that  can allow an attacker to cause the application to   dereference a NULL pointer. This causes the application  to crash. (CVE-2012-0781)  - The 'PDORow' implementation contains an error that can  cause application crashes when interacting with the   session feature. (CVE-2012-0788)  - An error exists in the timezone handling such that  repeated calls to the function 'strtotime' can allow  a denial of service attack via memory consumption.  (CVE-2012-0789) | | |
| **Solution** | Upgrade to PHP version 5.3.9 or later. | | |
| **Remark** | https://www.tenable.com/security/research/tra-2012-01 http://xhe.myxwiki.org/xwiki/bin/view/XSLT/Application\_PHP5 http://www.php.net/archive/2012.php#id2012-01-11-1 https://seclists.org/bugtraq/2012/Jan/91 https://bugs.php.net/bug.php?id=55475 https://bugs.php.net/bug.php?id=55776 https://bugs.php.net/bug.php?id=53502 http://www.php.net/ChangeLog-5.php#5.3.9 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 27 | **Finding** | PHP 5.3.12 / 5.4.2 CGI Query String Code Execution |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is earlier than 5.3.12 / 5.4.2, and as such is potentially affected by a remote code execution and information disclosure vulnerability.  An error in the file 'sapi/cgi/cgi\_main.c' can allow a remote attacker to obtain PHP source code from the web server or to potentially execute arbitrary code. In vulnerable configurations, PHP treats certain query string parameters as command line arguments including switches such as '-s', '-d', and '-c'.  Note that this vulnerability is exploitable only when PHP is used in CGI-based configurations. Apache with 'mod\_php' is not an exploitable configuration. | | |
| **Solution** | Upgrade to PHP version 5.3.12 / 5.4.2 or later. A 'mod\_rewrite' workaround is available as well. | | |
| **Remark** | http://eindbazen.net/2012/05/php-cgi-advisory-cve-2012-1823/ https://bugs.php.net/bug.php?id=61910 http://www.php.net/archive/2012.php#id2012-05-03-1 http://www.php.net/ChangeLog-5.php#5.3.12 http://www.php.net/ChangeLog-5.php#5.4.2 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 28 | **Finding** | Apache 2.2.x 2.2.23 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.23. It is, therefore, potentially affected by the following vulnerabilities :  - The utility 'apachectl' can receive a zero-length  directory name in the LD\_LIBRARY\_PATH via the 'envvars'  file. A local attacker with access to that utility  could exploit this to load a malicious Dynamic Shared  Object (DSO), leading to arbitrary code execution.  (CVE-2012-0883)  - An input validation error exists related to  'mod\_negotiation', 'Multiviews' and untrusted uploads  that can allow cross-site scripting attacks.  (CVE-2012-2687) Note that Nessus has not tested for these flaws but has instead relied on the version in the server's banner. | | |
| **Solution** | Upgrade to Apache version 2.2.23 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.23 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 29 | **Finding** | Apache 2.2.x 2.2.28 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.28. It is, therefore, affected by the following vulnerabilities :  - A flaw exists within the 'mod\_headers' module which  allows a remote attacker to inject arbitrary headers.  This is done by placing a header in the trailer portion  of data being sent using chunked transfer encoding.  (CVE-2013-5704)  - A flaw exists within the 'mod\_deflate' module when  handling highly compressed bodies. Using a specially  crafted request, a remote attacker can exploit this to  cause a denial of service by exhausting memory and CPU  resources. (CVE-2014-0118)  - The 'mod\_status' module contains a race condition that  can be triggered when handling the scoreboard. A remote  attacker can exploit this to cause a denial of service,  execute arbitrary code, or obtain sensitive credential  information. (CVE-2014-0226)  - The 'mod\_cgid' module lacks a time out mechanism. Using  a specially crafted request, a remote attacker can use  this flaw to cause a denial of service by causing child  processes to linger indefinitely, eventually filling up  the scoreboard. (CVE-2014-0231) Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number. | | |
| **Solution** | Upgrade to Apache version 2.2.29 or later. Note that version 2.2.28 was never officially released. | | |
| **Remark** | https://www.zerodayinitiative.com/advisories/ZDI-14-236/ https://archive.apache.org/dist/httpd/CHANGES\_2.2.29 http://httpd.apache.org/security/vulnerabilities\_22.html http://swende.se/blog/HTTPChunked.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 30 | **Finding** | OpenSSL 1.0.2i Default Weak 64-bit Block Cipher (SWEET32) |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of OpenSSL running on the remote host is prior to 1.0.2i. It is, therefore, affected by a vulnerability, known as SWEET32, in the 3DES and Blowfish algorithms due to the use of weak 64-bit block ciphers by default. A man-in-the-middle attacker who has sufficient resources can exploit this vulnerability, via a 'birthday' attack, to detect a collision that leaks the XOR between the fixed secret and a known plaintext, allowing the disclosure of the secret text, such as secure HTTPS cookies, and possibly resulting in the hijacking of an authenticated session. | | |
| **Solution** | Upgrade to OpenSSL version 1.0.2i or later. | | |
| **Remark** | https://www.openssl.org/blog/blog/2016/08/24/sweet32/ https://sweet32.info/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 31 | **Finding** | PHP 7.3.24 Multiple Vulnerabilities |
| **Severity** | High | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.24. It is, therefore affected by multiple vulnerabilities | | |
| **Solution** | Upgrade to PHP version 7.3.24 or later. | | |
| **Remark** | https://www.php.net/ChangeLog-7.php#7.3.24 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 32 | **Finding** | SSL Certificate Expiry |
| **Severity** | Medium | **Port** | TCP: 21, 443, 990 |
| **Target** | 192.168.100.102(443), 192.168.100.106(21, 990) | | |
| **Detail** | This plugin checks expiry dates of certificates associated with SSL- enabled services on the target and reports whether any have already expired. | | |
| **Solution** | Purchase or generate a new SSL certificate to replace the existing one. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 33 | **Finding** | Microsoft Outlook Web Access (OWA) owalogon.asp Redirection Account Enumeration |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote host is running Microsoft Outlook Web Access (OWA) 2003.  Due to a lack of sanitization of the user input, the remote version of this software is vulnerable to URL injection that can be exploited to redirect a user to a different, unauthorized web server after authenticating to OWA. This unauthorized site could be used to capture sensitive information by appearing to be part of the web application. | | |
| **Solution** | Upgrade to Microsoft Exchange Server 2007 as that reportedly addresses the issue.  Alternatively, edit the 'logon.asp' script used by OWA and hardcode a value for 'redirectPath' in line 54. | | |
| **Remark** | https://seclists.org/fulldisclosure/2005/Feb/101 https://seclists.org/fulldisclosure/2005/Jul/483 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 34 | **Finding** | Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 192.168.100.102(3389) | | |
| **Detail** | The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP  client makes no effort to validate the identity of the server when  setting up encryption. An attacker with the ability to intercept  traffic from the RDP server can establish encryption with the client  and server without being detected. A MiTM attack of this nature would  allow the attacker to obtain any sensitive information transmitted,  including authentication credentials. This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack. | | |
| **Solution** | - Force the use of SSL as a transport layer for this service if supported, or/and - Select the 'Allow connections only from computers running Remote  Desktop with Network Level Authentication' setting if it is available. | | |
| **Remark** | http://www.nessus.org/u?8033da0d http://technet.microsoft.com/en-us/library/cc782610.aspx | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 35 | **Finding** | SSL Weak Cipher Suites Supported |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote host supports the use of SSL ciphers that offer weak encryption. Note: This is considerably easier to exploit if the attacker is on the same physical network. | | |
| **Solution** | Reconfigure the affected application, if possible to avoid the use of weak ciphers. | | |
| **Remark** | http://www.nessus.org/u?6527892d | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 36 | **Finding** | MS10-024: Vulnerabilities in Microsoft Exchange and Windows SMTP Service Could Allow Denial of Service (981832) (uncredentialed check) |
| **Severity** | Medium | **Port** | TCP: 25 |
| **Target** | 192.168.100.102(25) | | |
| **Detail** | The installed version of Microsoft Exchange / Windows SMTP Service is affected by at least one vulnerability :  - Incorrect parsing of DNS Mail Exchanger (MX) resource  records could cause the Windows Simple Mail Transfer  Protocol (SMTP) component to stop responding until   the service is restarted. (CVE-2010-0024)  - Improper allocation of memory for interpreting SMTP  command responses may allow an attacker to read random   email message fragments stored on the affected server.  (CVE-2010-0025) | | |
| **Solution** | Microsoft has released a set of patches for Windows 2000, XP, 2003, and 2008 as well as Exchange Server 2000, 2003, 2007, and 2010. | | |
| **Remark** | https://www.nessus.org/u?261981ca | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 37 | **Finding** | SSL Certificate Cannot Be Trusted |
| **Severity** | Medium | **Port** | TCP: 21, 443, 990, 3389, 4443, 4444 |
| **Target** | 192.168.100.102(443), 192.168.100.103(3389), 192.168.100.106(21, 990, 3389), 203.154.244.93(4443, 4444) | | |
| **Detail** | The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :  - First, the top of the certificate chain sent by the  server might not be descended from a known public  certificate authority. This can occur either when the  top of the chain is an unrecognized, self-signed  certificate, or when intermediate certificates are  missing that would connect the top of the certificate  chain to a known public certificate authority.  - Second, the certificate chain may contain a certificate  that is not valid at the time of the scan. This can  occur either when the scan occurs before one of the  certificate's 'notBefore' dates, or after one of the  certificate's 'notAfter' dates.  - Third, the certificate chain may contain a signature  that either didn't match the certificate's information  or could not be verified. Bad signatures can be fixed by  getting the certificate with the bad signature to be  re-signed by its issuer. Signatures that could not be  verified are the result of the certificate's issuer  using a signing algorithm that Nessus either does not  support or does not recognize. If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and  identity of the web server. This could make it easier to carry out  man-in-the-middle attacks against the remote host. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 38 | **Finding** | SMB Signing not required |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 192.168.100.102(445), 192.168.100.103(445), 192.168.100.106(445) | | |
| **Detail** | Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server. | | |
| **Solution** | Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details. | | |
| **Remark** | http://www.nessus.org/u?df39b8b3 http://technet.microsoft.com/en-us/library/cc731957.aspx http://www.nessus.org/u?74b80723 https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html http://www.nessus.org/u?a3cac4ea | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 39 | **Finding** | Terminal Services Encryption Level is Medium or Low |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 192.168.100.102(3389) | | |
| **Detail** | The remote Terminal Services service is not configured to use strong cryptography.  Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes. | | |
| **Solution** | Change RDP encryption level to one of :  3. High  4. FIPS Compliant | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 40 | **Finding** | SSL RC4 Cipher Suites Supported (Bar Mitzvah) |
| **Severity** | Medium | **Port** | TCP: 443, 3389, 8443 |
| **Target** | 192.168.100.102(443), 192.168.100.103(3389), 192.168.100.106(3389, 8443) | | |
| **Detail** | The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced into the stream, decreasing its randomness. If plaintext is repeatedly encrypted (e.g., HTTP cookies), and an attacker is able to obtain many (i.e., tens of millions) ciphertexts, the attacker may be able to derive the plaintext. | | |
| **Solution** | Reconfigure the affected application, if possible, to avoid use of RC4 ciphers. Consider using TLS 1.2 with AES-GCM suites subject to browser and web server support. | | |
| **Remark** | https://www.rc4nomore.com/ http://www.nessus.org/u?ac7327a0 http://cr.yp.to/talks/2013.03.12/slides.pdf http://www.isg.rhul.ac.uk/tls/ https://www.imperva.com/docs/HII\_Attacking\_SSL\_when\_using\_RC4.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 41 | **Finding** | SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote host is affected by a man-in-the-middle (MitM) information disclosure vulnerability known as POODLE. The vulnerability is due to the way SSL 3.0 handles padding bytes when decrypting messages encrypted using block ciphers in cipher block chaining (CBC) mode. MitM attackers can decrypt a selected byte of a cipher text in as few as 256 tries if they are able to force a victim application to repeatedly send the same data over newly created SSL 3.0 connections. As long as a client and service both support SSLv3, a connection can be 'rolled back' to SSLv3, even if TLSv1 or newer is supported by the client and service. The TLS Fallback SCSV mechanism prevents 'version rollback' attacks without impacting legacy clients; however, it can only protect connections when the client and service support the mechanism. Sites that cannot disable SSLv3 immediately should enable this mechanism. This is a vulnerability in the SSLv3 specification, not in any particular SSL implementation. Disabling SSLv3 is the only way to completely mitigate the vulnerability. | | |
| **Solution** | Disable SSLv3. Services that must support SSLv3 should enable the TLS Fallback SCSV mechanism until SSLv3 can be disabled. | | |
| **Remark** | https://www.imperialviolet.org/2014/10/14/poodle.html https://www.openssl.org/~bodo/ssl-poodle.pdf https://tools.ietf.org/html/draft-ietf-tls-downgrade-scsv-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 42 | **Finding** | SSL/TLS EXPORT\_RSA = 512-bit Cipher Suites Supported (FREAK) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote host supports EXPORT\_RSA cipher suites with keys less than or equal to 512 bits. An attacker can factor a 512-bit RSA modulus in a short amount of time. A man-in-the middle attacker may be able to downgrade the session to use EXPORT\_RSA cipher suites (e.g. CVE-2015-0204). Thus, it is recommended to remove support for weak cipher suites. | | |
| **Solution** | Reconfigure the service to remove support for EXPORT\_RSA cipher suites. | | |
| **Remark** | https://www.smacktls.com/#freak https://www.openssl.org/news/secadv/20150108.txt http://www.nessus.org/u?b78da2c4 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 43 | **Finding** | SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote host supports SSLv2 and therefore may be affected by a vulnerability that allows a cross-protocol Bleichenbacher padding oracle attack known as DROWN (Decrypting RSA with Obsolete and Weakened eNcryption). This vulnerability exists due to a flaw in the Secure Sockets Layer Version 2 (SSLv2) implementation, and it allows captured TLS traffic to be decrypted. A man-in-the-middle attacker can exploit this to decrypt the TLS connection by utilizing previously captured traffic and weak cryptography along with a series of specially crafted connections to an SSLv2 server that uses the same private key. | | |
| **Solution** | Disable SSLv2 and export grade cryptography cipher suites. Ensure that private keys are not used anywhere with server software that supports SSLv2 connections. | | |
| **Remark** | https://drownattack.com/ https://drownattack.com/drown-attack-paper.pdf | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 44 | **Finding** | MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) |
| **Severity** | Medium | **Port** | TCP: 1126 |
| **Target** | 192.168.100.102(1126) | | |
| **Detail** | The remote Windows host is affected by an elevation of privilege vulnerability in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker able to intercept communications between a client and a server hosting a SAM database can exploit this to force the authentication level to downgrade, allowing the attacker to impersonate an authenticated user and access the SAM database. | | |
| **Solution** | Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, and 10. | | |
| **Remark** | http://www.nessus.org/u?52ade1e9 http://badlock.org/ | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 45 | **Finding** | TLS Version 1.0 Protocol Detection |
| **Severity** | Medium | **Port** | TCP: 21, 443, 990, 3389, 8443 |
| **Target** | 192.168.100.102(443), 192.168.100.103(3389), 192.168.100.106(21, 443, 990, 3389, 8443) | | |
| **Detail** | The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.  As of March 31, 2020, Endpoints that aren’t enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.  PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits. | | |
| **Solution** | Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0. | | |
| **Remark** | https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 46 | **Finding** | HSTS Missing From HTTPS Server (RFC 6797) |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | The remote web server is not enforcing HSTS, as defined by RFC 6797.  HSTS is an optional response header that can be configured on the server to instruct  the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. | | |
| **Solution** | Configure the remote web server to use HSTS. | | |
| **Remark** | https://tools.ietf.org/html/rfc6797 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 47 | **Finding** | Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote) |
| **Severity** | Medium | **Port** | TCP: 445 |
| **Target** | 192.168.100.102(445) | | |
| **Detail** | The remote host is affected by an NTLM reflection elevation of privilege vulnerability known as 'PetitPotam'. An unauthenticated, remote attacker can exploit this, by sending a specially-crafted EFSRPC request, to cause the affected host to connect to a malicious server. An attacker can then utilize an NTLM relay to impersonate the target host and authenticate against remote services. One attack scenario, described within KB5005413, uses this exploit to initiate an NTLM session as a domain controller's machine account. This session is then relayed to an Active Directory Certificate Services (AD CS) host to obtain a certificate. This certificate could be then used to move laterally within the domain environment. | | |
| **Solution** | Apply the updates supplied by the vendor. Optionally, refer to Microsoft's KB5005413 for mitigation guidance. RPC filters may also be implemented to block remote access to the interface UUIDs necessary for this exploit. | | |
| **Remark** | https://github.com/topotam/PetitPotam https://kb.cert.org/vuls/id/405600 https://msrc.microsoft.com/update-guide/vulnerability/ADV210003 http://www.nessus.org/u?d0ab9e93 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 48 | **Finding** | SSL Self-Signed Certificate |
| **Severity** | Medium | **Port** | TCP: 21, 990, 3389, 4443, 4444 |
| **Target** | 192.168.100.103(3389), 192.168.100.106(21, 990, 3389), 203.154.244.93(4443, 4444) | | |
| **Detail** | The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.  Note that this plugin does not check for certificate chains that end in a certificate that is not self-signed, but is signed by an unrecognized certificate authority. | | |
| **Solution** | Purchase or generate a proper SSL certificate for this service. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 49 | **Finding** | HTTP TRACE / TRACK Methods Allowed |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections. | | |
| **Solution** | Disable these HTTP methods. Refer to the plugin output for more information. | | |
| **Remark** | https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper\_XST\_ebook.pdf http://www.apacheweek.com/issues/03-01-24 https://download.oracle.com/sunalerts/1000718.1.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 50 | **Finding** | Apache 2.2.x 2.2.9 Multiple Vulnerabilities (DoS, XSS) |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.9. It is, therefore, affected by multiple vulnerabilities :  - Improper handling of excessive forwarded interim   responses may cause denial of service conditions in   mod\_proxy\_http. (CVE-2008-2364)  - A cross-site request forgery vulnerability in the   balancer-manager interface of mod\_proxy\_balancer.  (CVE-2007-6420) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves. | | |
| **Solution** | Upgrade to Apache version 2.2.9 or later. Alternatively, ensure that the affected modules are not in use. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 51 | **Finding** | PHP 5.2.9 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is older than 5.2.9. Such versions may be affected by several security issues :  - Background color is not correctly validated with a non true  color image in function 'imagerotate()'. (CVE-2008-5498)  - A denial of service condition can be triggered by trying to   extract zip files that contain files with relative paths   in file or directory names.  - Function 'explode()' is affected by an unspecified   vulnerability.  - It may be possible to trigger a segfault by passing a   specially crafted string to function 'json\_decode()'.  - Function 'xml\_error\_string()' is affected by a flaw  which results in messages being off by one. | | |
| **Solution** | Upgrade to PHP version 5.2.9 or later. | | |
| **Remark** | http://news.php.net/php.internals/42762 http://www.php.net/releases/5\_2\_9.php http://www.php.net/ChangeLog-5.php#5.2.9 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 52 | **Finding** | PHP 5.2.10 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is older than 5.2.10. Such versions are reportedly affected by multiple vulnerabilities :  - Sufficient checks are not performed on fields reserved   for offsets in function 'exif\_read\_data()'. Successful   exploitation of this issue could result in a denial of   service condition. (bug 48378)  - Provided 'safe\_mode\_exec\_dir' is not set (not set by  default), it may be possible to bypass 'safe\_mode'   restrictions by preceding a backslash in functions   such as 'exec()', 'system()', 'shell\_exec()',   'passthru()' and 'popen()' on a system running PHP   on Windows. (bug 45997) | | |
| **Solution** | Upgrade to PHP version 5.2.10 or later. | | |
| **Remark** | https://bugs.php.net/bug.php?id=45997 https://bugs.php.net/bug.php?id=48378 http://www.php.net/releases/5\_2\_10.php http://www.php.net/ChangeLog-5.php#5.2.10 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 53 | **Finding** | PHP 5.2.12 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is older than 5.2.12. Such versions may be affected by several security issues :  - It is possible to bypass the 'safe\_mode' configuration  setting using 'tempnam()'. (CVE-2009-3557)  - It is possible to bypass the 'open\_basedir'   configuration setting using 'posix\_mkfifo()'.   (CVE-2009-3558)  - Provided file uploading is enabled (it is by default),  an attacker can upload files using a POST request with  'multipart/form-data' content even if the target script  doesn't actually support file uploads per se. By   supplying a large number (15,000+) of files, an attacker  could cause the web server to stop responding while it  processes the file list. (CVE-2009-4017)  - Missing protection for '$\_SESSION' from interrupt  corruption and improved 'session.save\_path' check.  (CVE-2009-4143)  - Insufficient input string validation in the   'htmlspecialchars()' function. (CVE-2009-4142) | | |
| **Solution** | Upgrade to PHP version 5.2.12 or later. | | |
| **Remark** | http://www.nessus.org/u?57f2d08f http://www.php.net/releases/5\_2\_12.php http://www.php.net/ChangeLog-5.php#5.2.12 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 54 | **Finding** | PHP 5.3.2 / 5.2.13 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is older than 5.3.2 / 5.2.13. Such versions may be affected by several security issues :  - Directory paths not ending with '/' may not be  correctly validated inside 'tempnam()' in   'safe\_mode' configuration.  - It may be possible to bypass the 'open\_basedir'/   'safe\_mode' configuration restrictions due to an  error in session extensions.  - An unspecified vulnerability affects the LCG entropy. | | |
| **Solution** | Upgrade to PHP version 5.3.2 / 5.2.13 or later. | | |
| **Remark** | http://securityreason.com/achievement\_securityalert/82 http://securityreason.com/securityalert/7008 https://seclists.org/fulldisclosure/2010/Feb/208 http://www.php.net/releases/5\_3\_2.php http://www.php.net/ChangeLog-5.php#5.3.2 http://www.php.net/releases/5\_2\_13.php http://www.php.net/ChangeLog-5.php#5.2.13 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 55 | **Finding** | Apache 2.2.x 2.2.16 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.16. It is, therefore, potentially affected by multiple vulnerabilities :  - A denial of service vulnerability in mod\_cache and   mod\_dav. (CVE-2010-1452)    - An information disclosure vulnerability in mod\_proxy\_ajp,  mod\_reqtimeout, and mod\_proxy\_http relating to timeout   conditions. Note that this issue only affects Apache on   Windows, Netware, and OS/2. (CVE-2010-2068) Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves. | | |
| **Solution** | Upgrade to Apache version 2.2.16 or later. | | |
| **Remark** | http://httpd.apache.org/security/vulnerabilities\_22.html https://issues.apache.org/bugzilla/show\_bug.cgi?id=49246 https://bz.apache.org/bugzilla/show\_bug.cgi?id=49417 http://www.nessus.org/u?ce8ac446 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 56 | **Finding** | Apache 2.2.x 2.2.17 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.17. It is, therefore, affected by the following vulnerabilities :  - Errors exist in the bundled expat library that may allow  an attacker to crash the server when a buffer is over-  read when parsing an XML document. (CVE-2009-3720 and  CVE-2009-3560)  - An error exists in the 'apr\_brigade\_split\_line'   function in the bundled APR-util library. Carefully  timed bytes in requests result in gradual memory  increases leading to a denial of service.   (CVE-2010-1623)   Note that the remote web server may not actually be affected by these vulnerabilities. Nessus did not try to determine whether the affected modules are in use or to check for the issues themselves. | | |
| **Solution** | Upgrade to Apache version 2.2.17 or later. Alternatively, ensure that the affected modules are not in use. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.17 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 57 | **Finding** | PHP 5.2 5.2.15 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP 5.2 installed on the remote host is older than 5.2.15. Such versions may be affected by several security issues :    - A crash in the zip extract method.  - A possible double free exists in the imap extension.  (CVE-2010-4150)  - An unspecified flaw exists in 'open\_basedir'.   (CVE-2010-3436)  - A possible crash could occur in 'mssql\_fetch\_batch()'.    - A NULL pointer dereference exists in   'ZipArchive::getArchiveComment'. (CVE-2010-3709)  - A crash exists if anti-aliasing steps are invalid.  (Bug #53492)  - A crash exists in pdo\_firebird getAttribute(). (Bug   #53323)  - A user-after-free vulnerability in the Zend engine when  a '\_\_set()', '\_\_get()', '\_\_isset()' or '\_\_unset()'   method is called can allow for a denial of service   attack. (Bug #52879 / CVE-2010-4697)  - A stack-based buffer overflow exists in the   'imagepstext()' function in the GD extension. (Bug   #53492 / CVE-2010-4698)    - The extract function does not prevent use of the  EXTR\_OVERWRITE parameter to overwrite the GLOBALS  superglobal array and the 'this' variable, which  allows attackers to bypass intended access restrictions.  (CVE-2011-0752) | | |
| **Solution** | Upgrade to PHP version 5.2.15 or later. | | |
| **Remark** | http://www.php.net/releases/5\_2\_15.php http://www.php.net/ChangeLog-5.php#5.2.15 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 58 | **Finding** | PHP 5.2 5.2.17 / 5.3 5.3.5 String To Double Conversion DoS |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.17 or 5.3.5.  Such versions may experience a crash while performing string to double conversion for certain numeric values. Only x86 32-bit PHP processes are known to be affected by this issue regardless of whether the system running PHP is 32-bit or 64-bit. | | |
| **Solution** | Upgrade to PHP 5.2.17/5.3.5 or later. | | |
| **Remark** | https://bugs.php.net/bug.php?id=53632 http://www.php.net/distributions/test\_bug53632.txt http://www.php.net/releases/5\_2\_17.php http://www.php.net/releases/5\_3\_5.php | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 59 | **Finding** | Apache 2.2.x 2.2.18 APR apr\_fnmatch DoS |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.18. It is, therefore, affected by a denial of service vulnerability due to an error in the apr\_fnmatch() function of the bundled APR library.  If mod\_autoindex is enabled and has indexed a directory containing files whose filenames are long, an attacker can cause high CPU usage with a specially crafted request.  Note that the remote web server may not actually be affected by this vulnerability. Nessus did not try to determine whether the affected module is in use or to check for the issue itself. | | |
| **Solution** | Upgrade to Apache version 2.2.18 or later. Alternatively, ensure that the 'IndexOptions' configuration option is set to 'IgnoreClient'. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.18 http://httpd.apache.org/security/vulnerabilities\_22.html#2.2.18 http://securityreason.com/achievement\_securityalert/98 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 60 | **Finding** | Apache 2.2.x 2.2.21 mod\_proxy\_ajp DoS |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.21. It is, therefore, potentially affected by a denial of service vulnerability. An error exists in the 'mod\_proxy\_ajp' module that can allow specially crafted HTTP requests to cause a backend server to temporarily enter an error state. This vulnerability only occurs when 'mod\_proxy\_ajp' is used along with 'mod\_proxy\_balancer'. Note that Nessus did not actually test for the flaws but instead has relied on the version in the server's banner. | | |
| **Solution** | Upgrade to Apache version 2.2.21 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.21 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 61 | **Finding** | Apache 2.2.x 2.2.22 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x installed on the remote host is prior to 2.2.22. It is, therefore, potentially affected by the following vulnerabilities :  - When configured as a reverse proxy, improper use of the  RewriteRule and ProxyPassMatch directives could cause  the web server to proxy requests to arbitrary hosts.  This could allow a remote attacker to indirectly send  requests to intranet servers.  (CVE-2011-3368, CVE-2011-4317)  - A heap-based buffer overflow exists when mod\_setenvif  module is enabled and both a maliciously crafted   'SetEnvIf' directive and a maliciously crafted HTTP   request header are used. (CVE-2011-3607)  - A format string handling error can allow the server to  be crashed via maliciously crafted cookies.  (CVE-2012-0021)  - An error exists in 'scoreboard.c' that can allow local  attackers to crash the server during shutdown.  (CVE-2012-0031)  - An error exists in 'protocol.c' that can allow   'HTTPOnly' cookies to be exposed to attackers through  the malicious use of either long or malformed HTTP  headers. (CVE-2012-0053)  - An error in the mod\_proxy\_ajp module when used to   connect to a backend server that takes an overly long   time to respond could lead to a temporary denial of   service. (CVE-2012-4557) Note that Nessus did not actually test for these flaws, but instead  has relied on the version in the server's banner. | | |
| **Solution** | Upgrade to Apache version 2.2.22 or later. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.22 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 62 | **Finding** | Terminal Services Doesn't Use Network Level Authentication (NLA) Only |
| **Severity** | Medium | **Port** | TCP: 3389 |
| **Target** | 192.168.100.106(3389) | | |
| **Detail** | The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication,  NLA also helps protect the remote computer from malicious users and  software by completing user authentication before a full RDP  connection is established. | | |
| **Solution** | Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the 'Remote' tab of the 'System' settings on Windows. | | |
| **Remark** | https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11) http://www.nessus.org/u?e2628096 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 63 | **Finding** | PHP 5.3.11 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP installed on the remote host is earlier than 5.3.11, and as such is potentially affected by multiple vulnerabilities :  - During the import of environment variables, temporary  changes to the 'magic\_quotes\_gpc' directive are not  handled properly. This can lower the difficulty for  SQL injection attacks. (CVE-2012-0831)  - The '$\_FILES' variable can be corrupted because the  names of uploaded files are not properly validated.  (CVE-2012-1172)  - The 'open\_basedir' directive is not properly handled by  the functions 'readline\_write\_history' and  'readline\_read\_history'.  - The 'header()' function does not detect multi-line  headers with a CR. (Bug #60227 / CVE-2011-1398) | | |
| **Solution** | Upgrade to PHP version 5.3.11 or later. | | |
| **Remark** | http://www.nessus.org/u?e81d4026 https://bugs.php.net/bug.php?id=61043 https://bugs.php.net/bug.php?id=54374 https://bugs.php.net/bug.php?id=60227 https://marc.info/?l=oss-security=134626481806571=2 http://www.php.net/archive/2012.php#id2012-04-26-1 http://www.php.net/ChangeLog-5.php#5.3.11 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 64 | **Finding** | Apache 2.2.x 2.2.24 Multiple XSS Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.24. It is, therefore, potentially affected by the following cross-site scripting vulnerabilities :  - Errors exist related to the modules mod\_info,  mod\_status, mod\_imagemap, mod\_ldap, and mod\_proxy\_ftp  and unescaped hostnames and URIs that could allow cross-  site scripting attacks. (CVE-2012-3499)  - An error exists related to the mod\_proxy\_balancer  module's manager interface that could allow cross-site  scripting attacks. (CVE-2012-4558) Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner. | | |
| **Solution** | Upgrade to Apache version 2.2.24 or later. Alternatively, ensure that the affected modules are not in use. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.24 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 65 | **Finding** | Apache 2.2.x 2.2.25 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is prior to 2.2.25. It is, therefore, potentially affected by the following vulnerabilities :  - A flaw exists in the 'RewriteLog' function where it  fails to sanitize escape sequences from being written  to log files, making it potentially vulnerable to  arbitrary command execution. (CVE-2013-1862)  - A denial of service vulnerability exists relating to  the 'mod\_dav' module as it relates to MERGE requests.  (CVE-2013-1896) Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner. | | |
| **Solution** | Upgrade to Apache version 2.2.25 or later. Alternatively, ensure that the affected modules are not in use. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.25 http://httpd.apache.org/security/vulnerabilities\_22.html http://www.nessus.org/u?f050c342 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 66 | **Finding** | PHP PHP\_RSHUTDOWN\_FUNCTION Security Bypass |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of PHP 5.x installed on the remote host is 5.x prior to 5.3.11 or 5.4.x prior to 5.4.1 and thus, is potentially affected by a security bypass vulnerability. An error exists related to the function 'PHP\_RSHUTDOWN\_FUNCTION' in the libxml extension and the 'stream\_close' method that could allow a remote attacker to bypass 'open\_basedir' protections and obtain sensitive information. Note that this plugin has not attempted to exploit this issue, but has instead relied only on PHP's self-reported version number. | | |
| **Solution** | Upgrade to PHP version 5.3.11 / 5.4.1 or later. | | |
| **Remark** | http://www.nessus.org/u?bcc428c2 https://bugs.php.net/bug.php?id=61367 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 67 | **Finding** | Apache 2.2.x 2.2.27 Multiple Vulnerabilities |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its banner, the version of Apache 2.2.x running on the remote host is a version prior to 2.2.27. It is, therefore, potentially affected by the following vulnerabilities :  - A flaw exists with the 'mod\_dav' module that is caused  when tracking the length of CDATA that has leading white  space. A remote attacker with a specially crafted DAV  WRITE request can cause the service to stop responding.  (CVE-2013-6438)  - A flaw exists in 'mod\_log\_config' module that is caused  when logging a cookie that has an unassigned value. A  remote attacker with a specially crafted request can  cause the service to crash. (CVE-2014-0098) Note that Nessus did not actually test for these issues, but instead has relied on the version in the server's banner. | | |
| **Solution** | Upgrade to Apache version 2.2.27 or later. Alternatively, ensure that the affected modules are not in use. | | |
| **Remark** | https://archive.apache.org/dist/httpd/CHANGES\_2.2.27 http://httpd.apache.org/security/vulnerabilities\_22.html | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 68 | **Finding** | Apache Server ETag Header Information Disclosure |
| **Severity** | Medium | **Port** | TCP: 80 |
| **Target** | 192.168.100.106(80) | | |
| **Detail** | The remote web server is affected by an information disclosure vulnerability due to the ETag header providing sensitive information that could aid an attacker, such as the inode number of requested files. | | |
| **Solution** | Modify the HTTP ETag header of the web server to not include file inodes in the ETag header calculation. Refer to the linked Apache documentation for more information. | | |
| **Remark** | http://httpd.apache.org/docs/2.2/mod/core.html#FileETag | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 69 | **Finding** | JQuery 1.2 3.5.0 Multiple XSS |
| **Severity** | Medium | **Port** | TCP: 443 |
| **Target** | 192.168.100.106(443) | | |
| **Detail** | According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.  Note, the vulnerabilities referenced in this plugin have no security impact on PAN-OS, and/or the scenarios  required for successful exploitation do not exist on devices running a PAN-OS release. | | |
| **Solution** | Upgrade to JQuery version 3.5.0 or later. | | |
| **Remark** | https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/ https://security.paloaltonetworks.com/PAN-SA-2020-0007 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 70 | **Finding** | PHP 7.3.28 Email Header Injection |
| **Severity** | Medium | **Port** | TCP: 80, 443 |
| **Target** | 192.168.100.106(80, 443) | | |
| **Detail** | According to its self-reported version number, the version of PHP running on the remote web server is prior to 7.3.28. It is, therefore affected by an email header injection vulnerability, due to a failure to properly handle CR-LF sequences in header fields. An unauthenticated, remote attacker can exploit this, by inserting line feed characters into email headers, to gain full control of email header content. | | |
| **Solution** | Upgrade to PHP version 7.3.28 or later. | | |
| **Remark** | https://www.php.net/ChangeLog-7.php#7.3.28 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 71 | **Finding** | Terminal Services Encryption Level is not FIPS-140 Compliant |
| **Severity** | Low | **Port** | TCP: 3389 |
| **Target** | 192.168.100.102(3389) | | |
| **Detail** | The encryption setting used by the remote Terminal Services service is not FIPS-140 compliant. | | |
| **Solution** | Change RDP encryption level to :  4. FIPS Compliant | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 72 | **Finding** | SMTP Service Cleartext Login Permitted |
| **Severity** | Low | **Port** | TCP: 25 |
| **Target** | 192.168.100.102(25) | | |
| **Detail** | The remote host is running an SMTP server that advertises that it allows cleartext logins over unencrypted connections. An attacker may be able to uncover user names and passwords by sniffing traffic to the server if a less secure authentication mechanism (i.e. LOGIN or PLAIN) is used. | | |
| **Solution** | Configure the service to support less secure authentication mechanisms only over an encrypted channel. | | |
| **Remark** | https://tools.ietf.org/html/rfc4422 https://tools.ietf.org/html/rfc4954 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 73 | **Finding** | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits |
| **Severity** | Low | **Port** | TCP: 443 |
| **Target** | 192.168.100.102(443) | | |
| **Detail** | At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014. Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt. | | |
| **Solution** | Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate. | | |
| **Remark** | https://www.cabforum.org/wp-content/uploads/Baseline\_Requirements\_V1.pdf | | |



# Web Application Vulnerability Assessment

**Vulnerability Assessment from Public Access (for public target)**

**Testing date:** March 30, 2021

**Tester IP Address:** 203.150.79.252

Diagram

Description automatically generated

Figure 5: Vulnerability Assessment from Public Access

## **6.1 Target Information**

| **No.** | **Domain / Server Name** | **IP Address** | **OS/Model** | **Port** |
| --- | --- | --- | --- | --- |
| 1 | https://example.com | 123.123.123.123 | Ubuntu 20 | TCP 22, 53, 80, 113, 123, 443, 2000, 4118, 4119, 4120, 4121, 4122, 4444, 5000, 5060, 8008, 8082 |

## **6.2 Executive summary**

The purpose of this activity is to find the vulnerability on the target web application.

### **6.2.1 Summary Vulnerability by Severity**

Figure 6: Summary by Severity of Web Application Vulnerability Assessment

### **6.2.2 Vulnerability by Target**

| **No.** | **Domain/Server Name** | **IP Address** | **Critical** | **High** | **Medium** | **Low** | **Total** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | https://example.com | 123.123.123.123 | 0 | 0 | 1 | 3 | 4 |
| **Total** | | | **0** | **0** | **1** | **3** | **4** |

## **6.3 Web Application Vulnerability Detail**

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 1 | **Finding** | Clickjacking: X-Frame-Options header |
| **Severity** | **Low** | **Port** | TCP 443 |
| **Target** | https://example.com/  https://example.com/sitemap.xml  https://example.com/sitemap.xml.gz  https://example.com/login  https://example.com/backend/  https://example.com/backend/api/v1/  https://example.com/backend/api/  https://example.com/backend.bak  https://example.com/backend.7z  https://example.com/backend.cfg  https://example.com/backend.csv  https://example.com/backend.dump  https://example.com/backend.ini  https://example.com/backend.jar  https://example.com/backend.old  https://example.com/backend.ost  https://example.com/backend.pst  https://example.com/backend.sh  https://example.com/backend.sln  https://example.com/backend.tar  https://example.com/backend.war | | |
| **Detail** | Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information, or taking control of their computer while clicking on seemingly innocuous web pages.  The server did not return an X-Frame-Options header with the value DENY or SAMEORIGIN, which means that this website could be at risk of a clickjacking attack. The X-Frame-Options HTTP response header can be used to indicate whether a browser should be allowed to render a page inside a frame or iframe. Sites can use this to avoid clickjacking attacks, by ensuring that their content is not embedded into untrusted sites. | | |
| **Impact** | The impact depends on the affected web application. | | |
| **Solution** | Configure your web server to include an X-Frame-Options header and a CSP header with frame-ancestors directive. Consult Web references for more information about the possible values for this header. | | |
| **Remark** | - | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 2 | **Finding** | HTTP Strict Transport Security (HSTS) not implemented |
| **Severity** | **Low** | **Port** | TCP 443 |
| **Target** | https://example.com/  https://example.com/sitemap.xml  https://example.com/sitemap.xml.gz  https://example.com/login  https://example.com/backend/  https://example.com/backend/api/v1/  https://example.com/backend/api/  https://example.com/backend.bak  https://example.com/backend.7z  https://example.com/backend.cfg  https://example.com/backend.csv  https://example.com/backend.dump  https://example.com/backend.ini  https://example.com/backend.jar  https://example.com/backend.old  https://example.com/backend.ost  https://example.com/backend.pst  https://example.com/backend.sh  https://example.com/backend.sln  https://example.com/backend.tar  https://example.com/backend.war | | |
| **Detail** | HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response. | | |
| **Impact** | HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks | | |
| **Solution** | It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information | | |
| **Remark** | |  | | --- | | https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **ID.** | 3 | **Finding** | Sensitive pages could be cached |
| **Severity** | **Low** | **Port** | TCP 443 |
| **Target** | https://example.com/?password=g00dPa$$w0rDusername=pHqghUme | | |
| **Detail** | One or more pages contain possible sensitive information (e.g., a password parameter) and could be potentially cached. Even in secure SSL channels sensitive data could be stored by intermediary proxies and SSL terminators. To prevent this, a Cache-Control header should be specified. | | |
| **Impact** | Possible sensitive information disclosure. | | |
| **Solution** | Prevent caching by adding "Cache Control: No-store" and "Pragma: no-cache" to the HTTP response header. | | |
| **Remark** | - | | |

# Port Discovery

| **Port** | **Protocol** | **Service** |
| --- | --- | --- |
| 22 | TCP | ssh |
| 80 | TCP | http |
| 110 | TCP | pop3 |
| 143 | TCP | imap-proxy |
| 443 | TCP | https |
| 465 | TCP | ssl/smtp |
| 587 | TCP | smtp |
| 993 | TCP | ssl/imap-proxy |
| 995 | TCP | ssl/pop3 |
| 8443 | TCP | https-alt? |
| 9071 | TCP | ssl/http |

# Appendix

## **8.1 About Nessus**

Nessus is a proprietary vulnerability scanner developed by Tenable, Inc. Nessus is trusted by more than 30,000 organizations worldwide as one of the most widely deployed security technologies on the planet - and the gold standard for vulnerability assessment.

Reference: https://www.tenable.com/products/nessus

### **8.1.1 Nessus vulnerabilities**

As information about new vulnerabilities are discovered and released into the public domain, Tenable, Inc. research staff designs programs to enable Nessus to detect them. These programs are named plugins, and are written in the Nessus proprietary scripting language, called Nessus Attack Scripting Language (NASL). Plugins contain vulnerability information, a generic set of remediation actions, and the algorithm to test for the presence of the security issue.

Reference: https://www.tenable.com/plugins

### **8.1.2 Nessus risk score**

There are four risk levels in this document: Critical, High, Medium, and Low. There are methods for determining the risk level. Based on the Common Vulnerability Scoring System (CVSS), a standard for assessing the severity of vulnerabilities in computer systems. Regarded by the NIAC (National Infrastructure Advisory Council), expert assessments are measured in a range of 0 – 10

| **Severity** | **Description** | **Score** |
| --- | --- | --- |
| Critical | Vulnerabilities that score in the critical range usually have most of the following characteristics:   * Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. * Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions.   For critical vulnerabilities, is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place. For example, a mitigating factor could be if your installation is not accessible from the Internet. | 9.0 – 10.0 |
| High | Vulnerabilities that score in the high range usually have some of the following characteristics:   * The vulnerability is difficult to exploit. * Exploitation could result in elevated privileges. * Exploitation could result in a significant data loss or downtime. | 7.0 – 8.9 |
| Medium | Vulnerabilities that score in the medium range usually have some of the following characteristics:   * Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. * Denial of service vulnerabilities that are difficult to set up. * Exploits that require an attacker to reside on the same local network as the victim. * Vulnerabilities where exploitation provides only very limited access. * Vulnerabilities that require user privileges for successful exploitation. | 4.0 – 6.9 |
| Low | Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access. | 0.1 – 3.9 |

## **8.2 About Acunetix**

Acunetix by Invicti Security is an application security testing tool built to help small mid-size organizations around the world take control of their web security. Acunetix is built to evolve and stay ahead of cybersecurity changes. Acunetix industry-leading dynamic and interactive application security testing (DAST and IAST) technology automates vulnerability management and empowers security teams to uncover more vulnerabilities, reduce false positives, increase productivity, and simplify remediation efforts.

Reference: https://www.acunetix.com/product/, https://www.acunetix.com/about/

### **8.2.1 Acunetix web vulnerabilities**

The following reference link is a list of known web application vulnerabilities that can be automatically detected by Acunetix.

Reference: https://www.acunetix.com/vulnerabilities/web/

### **8.2.2 Acunetix risk score**

Severity is a metric for classifying the level of risk which a security vulnerability poses. The severity level of a vulnerability is assigned based on the security risk posed to an organization should the vulnerability be exploited, as well as the degree of difficulty involved in exploiting it. The result of a successful attack by exploiting a vulnerability could vary from denial of service and information disclosure to a complete compromise of applications or systems. The following provides a description of what the results in this analysis consider to be the impact of each vulnerability severity level.

| **Severity** | **Description** |
| --- | --- |
| High | An attacker can **fully** compromise the confidentiality, integrity, or availability, of a target system without specialized access, user interaction or circumstances that are beyond the attacker’s control. Very likely to allow lateral movement and escalation of attack to other systems on the internal network of the vulnerable application. |
| Medium | An attacker can **partially** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control may be required for an attack to succeed. Very likely to be used in conjunction with other vulnerabilities to escalate an attack. |
| Low | An attacker can **limitedly** compromise the confidentiality, integrity, or availability, of a target system. Specialized access, user interaction, or circumstances that are beyond the attacker’s control is required for an attack to succeed. Needs to be used in conjunction with other vulnerabilities to escalate an attack. |