***Test***

nextolive

10/02/2021

test

# Contents

[Contents 2](#_Toc63844650)

[Non-Disclosure Statement and Legal Notice 4](#_Toc63844651)

[Non-Disclosure Statement 4](#_Toc63844652)

[Legal Notice 4](#_Toc63844653)

[How to use this report 5](#_Toc63844654)

[Executive Summary 5](#_Toc63844655)

[Scope of testing 5](#_Toc63844656)

[Restrictions on testing 5](#_Toc63844657)

[Summary of findings 5](#_Toc63844658)

[Test Results 5](#_Toc63844659)

[CVSS Scoring System 5](#_Toc63844660)

[Test Details 6](#_Toc63844661)

[Document Control 6](#_Toc63844662)

[1 Executive Summary 7](#_Toc63844663)

[1.1 Introduction 7](#_Toc63844664)

[1.2 Issues Identified 8](#_Toc63844665)

[1.2.1 Infrastructure Test(s) 8](#_Toc63844666)

[1.2.2 Application Test(s) 8](#_Toc63844667)

[1.2.3 Others Test(s) 9](#_Toc63844668)

[1.3 Recommended Actions 10](#_Toc63844669)

[1.3.1 Immediate Actions 10](#_Toc63844670)

[1.3.2 Medium Term Actions 10](#_Toc63844671)

[1.3.3 Long Term Actions 10](#_Toc63844672)

[2 Scope of testing 11](#_Toc63844673)

[3 Restrictions on testing 12](#_Toc63844674)

[3.1 Network Infrastructure 12](#_Toc63844675)

[3.2 Application 12](#_Toc63844676)

[4 Summary of findings 13](#_Toc63844677)

[4.1   Infrastructure 13](#_Toc63844678)

[4.1.1   Environment information disclosure 13](#_Toc63844679)

[4.1.2   Microsoft ASP.NET 'ValidateRequest' filters bypass 13](#_Toc63844680)

[4.1.3   Outdated PHP Scripting layer 13](#_Toc63844681)

[4.1.4   SSL Certificate Signed using Weak Hashing Algorithm 14](#_Toc63844682)

[4.1.5   TLS/SSL Related Vulnerabilities 14](#_Toc63844683)

[4.2   Application 14](#_Toc63844684)

[4.2.1   CGI Generic Cross-Site Request Forgery Detection (potential) 14](#_Toc63844685)

[4.2.2   Cookies Set Without the 'HttpOnly' Flag 14](#_Toc63844686)

[4.2.3   Cookies Set Without The 'Secure' Flag 14](#_Toc63844687)

[4.2.4   Missing HTTP Response Headers 15](#_Toc63844688)

[4.2.5   Script Src Integrity Check 15](#_Toc63844689)

[4.2.6   Sensitive File Disclosure 15](#_Toc63844690)

[4.3   Others 15](#_Toc63844691)

[4.3.1   Git Repository Served by Web Server 15](#_Toc63844692)

[5 Test Results 16](#_Toc63844693)

[5.1 Infrastructure 16](#_Toc63844694)

[5.2 Application 25](#_Toc63844695)

[5.3 Others 39](#_Toc63844696)

[Appendix A- Severity Scale 41](#_Toc63844697)

[Appendix B Port Scans 42](#_Toc63844698)

[B.1    178.250.102.166 42](#_Toc63844699)

[B.1    185.160.253.20 42](#_Toc63844700)

[B.1    www.hss.com 42](#_Toc63844701)

[B.1    www.hsstraining.com 42](#_Toc63844702)

[Appendix C - Supplementary Information 43](#_Toc63844703)

# Non-Disclosure Statement and Legal Notice

## Non-Disclosure Statement

This report has been made for nextolive. All information obtained during a ProCheckUp assessment about our customer's systems and assets including, but not limited to, its procedures and systems, is deemed privileged information and not for public dissemination.  ProCheckUp Ltd pledge their commitment that this information will remain strictly confidential.  This information will not be disclosed or discussed to any third party without the written consent of the customer.   ProCheckUp Ltd is fully committed to maintaining the highest level of ethical standards in its business practice.

## Legal Notice

It is impossible to test an internal network for 100% security within normal timeframes. This report does not constitute and should not be construed as a guarantee of the target's security.

# How to use this report

## Executive Summary

This section provides an overview of the test background and details and gives an indication to the security posture of the overall environment.

## Scope of testing

This section details the scope agreed with nextolive before ProCheckUp testing was conducted.

## Restrictions on testing

This section details any problems that occurred which disrupted or prevented with testing

## Summary of findings

This section gives a high-level summary of the main findings

## Test Results

This section details the results obtained whilst testing the targets and presents the LOW to HIGH severity vulnerabilities discovered. Each vulnerability includes an indication of its level of impact, a description, results and how it can be resolved. Whenever possible, an exploit for the identified vulnerability will be supplied.

## CVSS Scoring System

ProCheckUp currently uses version 2 of the Common Vulnerability Scoring System (CVSS) when rating vulnerabilities discovered during security testing. CVSS is an open industry framework used to assess the severity of security vulnerabilities based on three distinct metrics:

* Base Metrics are associated with intrinsic characteristics of a vulnerability
* Temporal Metrics are associated with evolving characteristics of a vulnerability
* Environmental Metrics are associated with vulnerabilities that are dependent on environmental factors.

The outcome of these metrics is a score indicating the severity of the vulnerability and provides an accurate input to an enterprises prioritised approach to remediation. The CVSS scheme scores are grouped as follows:

* CVSS scored 7.0-10 would be considered HIGH severity
* CVSS scored 4.0-6.9 would be considered Medium severity
* CVSS scored 0-3.9 would be considered as LOW severity

ProCheckUp use base metrics to build a traffic light system in their vulnerability reporting tables in the 'Test Results' section of this report. CVSS v3 is due to be released imminently and will be rolled out to all of our clients shortly afterwards.

More information on the system we use to rate vulnerabilities can be found in Appendix A.

# Test Details

|  |  |
| --- | --- |
| **Date of Test** | **10/02/2021** |
| Test Location | ProcheckUp Ltd [Address] [Country] [Zip] |
| Customer Contact | NextOlive |
| Telephone | [Telephone] |
| Email | [Email] |
| Tester | next olive |

# Document Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Action** | **Version** | **Author** |
| 10/02/2021 | Initial Draft | 0.1 | next-olive |
| 10/02/2021 | Draft Report sent | 0.3 |  |
| 10/02/2021 | General QA | 0.2 |  |
| 10/02/2021 | Technical QA | 0.4 |  |
| 10/02/2021 | Technical QA | 0.5 |  |
| 10/02/2021 | Final report | 1.0 | next-olive |

# 1 Executive Summary

## 1.1 Introduction

On 10/02/2021, ProCheckUp was commissioned to perform an internal penetration test on a environment. .

Overall the security of the environment was found to be Choose an item..

ProCheckUp identified a significant number of missing patches during this test.  This could be an indication of a weak patch management process and could be a warnig that software updates are not being deployed in a timely manner.

It can be seen that the issues discovered during this engagement highlight serious flaws in the security posture of which, if not remediated immediately, could lead to complete compromise of the environment under test.

## 1.2 Issues Identified

This section identifies the issues discovered on each of the networks tested during this engagement. A summary of the most serious issues can be found in Section 4 (Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5 (Test Results).

### 1.2.1 Infrastructure Test(s)

This section identifies the issues discovered on each of the infrastructure tested during this engagement. A summary of the most serious issues can be found in Section 4(Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5(Test Results).

|  |  |  |
| --- | --- | --- |
| **Issue ID** | **Issue** | **Issue Rating** |
| INF-1 | Outdated PHP Scripting layer | **lllll**  **HIGH** |
| INF-2 | SSL Certificate Signed using Weak Hashing Algorithm | **lllll**  **MEDIUM** |
| INF-3 | TLS/SSL Related Vulnerabilities | **lllll**  **MEDIUM** |
| INF-4 | Microsoft ASP.NET 'ValidateRequest' filters bypass | **lllll**  **MEDIUM** |
| INF-5 | Environment information disclosure | **lllll**  **LOW** |
| INF-6 | Environment Information Disclosure | **lllll**  **LOW** |
| INF-7 | TCP Timestamp Option Enabled | **lllll**  **LOW** |

### 1.2.2 Application Test(s)

This section identifies the issues discovered on each of the application tested during this engagement. A summary of the most serious issues can be found in Section 4(Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5(Test Results).

|  |  |  |
| --- | --- | --- |
| **Issue ID** | **Issue** | **Issue Rating** |
| APP-1 | Script Src Integrity Check | **lllll**  **HIGH** |
| APP-2 | CGI Generic Cross-Site Request Forgery Detection (potential) | **lllll**  **MEDIUM** |
| APP-3 | Sensitive File Disclosure | **lllll**  **MEDIUM** |
| APP-4 | Cookies Set Without the 'HttpOnly' Flag | **lllll**  **MEDIUM** |
| APP-5 | Cookies Set Without The 'Secure' Flag | **lllll**  **MEDIUM** |
| APP-6 | Missing HTTP Response Headers | **lllll**  **MEDIUM** |
| APP-7 | Firewall Detected | **lllll**  **INFO** |

### 1.2.3 Others Test(s)

This section identifies the issues tested during this engagement. A summary of the most serious issues can be found in Section 4(Summary of Findings) and full details of the issues, together with detailed remediation advice, can be found in Section 5(Test Results).

|  |  |  |
| --- | --- | --- |
| **Issue ID** | **Issue** | **Issue Rating** |
| 1 | Git Repository Served by Web Server | **lllll**  **MEDIUM** |
| 2 | Web Server Allows Password Auto-Completion | **lllll**  **INFO** |

## 1.3 Recommended Actions

ProCheckUp recommends that the high, medium and low risk issues identified during this engagement should be subject to urgent remedial work to ensure an increase in the security posture of the environment to project it from immediate attack.  The following prioritised approach is recommended:

### 1.3.1 Immediate Actions

* The password policy should be assessed and amended to fall in line with current best
* The session management of the application should be upgraded to ensure that a session expires when the user logs out.
* All missing CRITICAL and HIGH risk patches should be applied across the environment in accordance with the corporate patching policy.

### 1.3.2 Medium Term Actions

* should implement an enterprise wide patching policy that ensures any new patches are applied in a timely manner.
* should consider having a gold build for all like devices which should be security tested following operational testing.

### 1.3.3 Long Term Actions

* should consider adopting a regular scheduled testing framework. ProCheckUp security testing is a snapshot of security posture at a point in time. New vulnerabilities are identified every day resulting in a significant window of exposure during the 12 months between tests. ProCheckUp can assist in designing a bespoke testing programme to ensure that serious vulnerabilities are identified and remediated as soon as possible.

# 2 Scope of testing

The scope for this engagement was agreed on 10/02/2021 following between from   and from ProCheckUp.

The aim of the test was to highlight vulnerabilities and attack avenues that could be utilised by an attacker to subvert the environment or gain access to sensitive information on the Verve environment.  
The following targests were in scope for this test:

|  |  |
| --- | --- |
| **Network(s)/IPs/Host Names** | **Test Type** |
| 178.250.102.166 | Unauthenticated |
| 185.160.253.20 | Unauthenticated |
| www.hss.com | Unauthenticated |
| www.hsstraining.com | Unauthenticated |

# 3 Restrictions on testing

## 3.1 Network Infrastructure

The environment under test was a pre-production environment with a limited number of users, devices and accounts and, as such, was not a true reflection of the realtime environment. It should be considered that having an expanded user set cause additional  vulnerabilities to occur.

## 3.2 Application

No test data was available for the environement under test and databases were therefore empty. This may not have identified some issues which may exist in the live database.

# 4 Summary of findings

Multiple HIGH, MEDIUM and LOW risk vulnerabilities were identified during the infrastructure and application API tests conducted during this engagement. The most significant of these vulnerabilities are discussed below and detailed along with the lower-risk issues in Section 5(Test Results).

### 4.1   Infrastructure

### 4.1.1   Environment information disclosure

The target discloses environment information which may help attackers perform more focused attacks.

### 4.1.2   Microsoft ASP.NET 'ValidateRequest' filters bypass

According to the HTTP headers received from the remote host, the web server is configured to use the ASP.NET framework.

This framework includes the 'ValidateRequest' feature, which is used by ASP.NET web applications to filter user input in an attempt to prevent cross-site scripting attacks. However, this set of filters can be bypassed if it is the sole mechanism used for protection by a web application.

ProCheckUp was unable to remotely gather enough information within the timeframe of this assessment to determine if the 'ValidateRequest' feature is used in an unsafe manner.

See Also:  
http://www.procheckup.com/procheckup-labs/posts/2008/august/pr08-20/  
http://msdn.microsoft.com/en-us/library/bb355989.aspx

### 4.1.3   Outdated PHP Scripting layer

PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML. The PHP scripting language in use was found to be outdated and vulnerable to the following vulnerabilities:-

**PHP Foreign Function Interface Arbitrary DLL Loading safe\_mode Restriction Bypass -** According to its banner, the version of PHP installed on the remote host is affected by a security bypass vulnerability. The Foreign Function Interface (ffi) extension does not follow safe\_mode restrictions, which allows context-dependent attackers to execute arbitrary code by loading an arbitrary DLL and calling a function.

**PHP ip2long Function String Validation Weakness -** According to its banner, the 'ip2long()' function in the version of PHP installed on the remote host may incorrectly validate an arbitrary string and return a valid network IP address.

**PHP mb\_send\_mail() Function Parameter Security Bypass -** According to its banner, the version of PHP installed on the remote host is affected by a flaw that allows an attacker to gain unauthorized privileges. When used with sendmail and when accepting remote input for the additional\_parameters argument to the mb\_send\_mail function, it is possible for context-dependent attackers to read and create arbitrary files.

**PHP Symlink Function Race Condition open\_basedir Bypass -** According to its banner, the version of PHP installed on the remote host is affected by a security bypass vulnerability. A race condition exists in the symlink function that allows local users to bypass the open\_basedir restriction by using a combination of symlink, mkdir, and unlink functions.

### 4.1.4   SSL Certificate Signed using Weak Hashing Algorithm

The target site uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks.

### 4.1.5   TLS/SSL Related Vulnerabilities

TLS (Transport Layer Security) is a protocol used for establishing an encrypted connection between a server and a client - typically a web server (website) and a browser. If implemented correctly, TLS allows sensitive information such as credit card details and login credentials to be transmitted securely. For TLS to be relied upon as a secure transmission protocol, it is essential that only strong ciphers, secure encryption algorithms, and cipher suites be supported.

**SSL Certificate Signed using Weak Hashing Algorithm -** The target site uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks.

**SSL/TLS Use Of Weak RC4 cipher -** Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features. SSL/TLS protocols use ciphers such as AES, DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers have discovered that there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical. The described attack is to inject a malicious JavaScript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker with a large set of ciphertext samples that can be used for statistical analysis. If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered.  
This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For example, HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.

### 4.2   Application

### 4.2.1   CGI Generic Cross-Site Request Forgery Detection (potential)

ProCheckUp has found HTML forms on the remote web server. Some CGI scripts do not appear to be protected by random tokens, a common anti-cross-site request forgery (XSRF) protection. The web application might be vulnerable to XSRF attacks. Note that : - ProCheckup did not exploit the flaw. - ProCheckUp cannot identify sensitive actions; for example, on an online bank, consulting an account is less sensitive than transferring money. You will need to audit the source of the CGI scripts and check if they are actually affected.

### 4.2.2   Cookies Set Without the 'HttpOnly' Flag

Cookies are set without using the 'HttpOnly' flag. The HttpOnly flag prevents scripting code such as JavaScript from accessing the cookie. This helps prevent cookie theft through cross-site scripting attacks in which the 'document.cookie' object is used to redirect cookies to third-party web servers under the control of the attacker.

### 4.2.3   Cookies Set Without The 'Secure' Flag

Cookies are set without using the 'Secure' flag. This flag is recommended as it prevents web browsers from submitting cookies over clear text (only HTTPS is allowed).

### 4.2.4   Missing HTTP Response Headers

The web server does not return several protective security headers on its HTTP response:

* Strict Transport Security - The HTTP Strict Transport Security policy defines a timeframe where a browser must connect to the web server via HTTPS.
* Content Sniffing - The lack of this header causes certain browsers to try and determine the content type and encoding of the response even when these properties are defined correctly. This can make the web application vulnerable against Cross-Site Scripting (XSS) attacks.
* X-XSS-Protection - This tells a supported browser to filter any possible XSS injection
* X-Frame-Options - This header prevents the application from being framed within a separate website.
* Cache-Control - Prevents sensitive web pages from being cached on the local disk.

These headers could further improve the security posture of the web application without necessarily impacting its functionality or user experience.

**Clickjacking - X-Frame-Options Header Is Not Set -** X-Frame-Options header is not set, and that may lead to a possible framing of the page.  
An attacker can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.

**Strict Transport Header Setting Missing -** There was no "Strict-Transport-Security" header in the server response. The HTTP Strict Transport Security policy defines a timeframe where a browser must connect to the web server via HTTPS. Without a Strict Transport Security policy, the web application may be vulnerable against several attacks:  
 If the web application mixes usage of HTTP and HTTPS, an attacker can manipulate pages in the unsecured area of the application or change redirection targets (either in a manner that the switch to the secured page is not performed or where the attacker remains between client and server).  
 If there is no HTTP server, an attacker in the same network could simulate a HTTP server and motivate the user to click on a prepared URL by a social engineering attack.  
The protection is effective only for the given amount of time. Multiple occurrences of this header could cause undefined behaviour in browsers and should be avoided.

### 4.2.5   Script Src Integrity Check

The remote host may be vulnerable to payment entry data exfiltration due to javascript included from potentially untrusted and unverified third parties script src. If the host is controlled by a 3rd party, ensure that the 3rd party is PCI DSS compliant.

### 4.2.6   Sensitive File Disclosure

The remote web application hosts documents or office files that may contain sensitive information.

### 4.3   Others

### 4.3.1   Git Repository Served by Web Server

The web server on the remote host allows read access to a Git repository. This potential flaw can be used to download content from the Web server that might otherwise be private.

# 5 Test Results

### 5.1 Infrastructure

| **lllll** | **Outdated PHP Scripting layer (CVSS: 7.0)** |
| --- | --- |
| **INF-1** | PHP is a general purpose scripting language that is suited for web development and can be embedded in HTML. The PHP scripting language in use was found to be outdated and vulnerable to the following vulnerabilities:-    **PHP Symlink Function Race Condition open\_basedir Bypass (CVSS: 6.2)**  According to its banner, the version of PHP installed on the remote host is affected by a security bypass vulnerability. A race condition exists in the symlink function that allows local users to bypass the open\_basedir restriction by using a combination of symlink, mkdir, and unlink functions.    **PHP ip2long Function String Validation Weakness (CVSS: 5.0)**  According to its banner, the 'ip2long()' function in the version of PHP installed on the remote host may incorrectly validate an arbitrary string and return a valid network IP address.    **PHP mb\_send\_mail() Function Parameter Security Bypass (CVSS: 5.0)**  According to its banner, the version of PHP installed on the remote host is affected by a flaw that allows an attacker to gain unauthorized privileges. When used with sendmail and when accepting remote input for the additional\_parameters argument to the mb\_send\_mail function, it is possible for context-dependent attackers to read and create arbitrary files.    **PHP Foreign Function Interface Arbitrary DLL Loading safe\_mode Restriction Bypass (CVSS: 4.3)**  According to its banner, the version of PHP installed on the remote host is affected by a security bypass vulnerability. The Foreign Function Interface (ffi) extension does not follow safe\_mode restrictions, which allows context-dependent attackers to execute arbitrary code by loading an arbitrary DLL and calling a function.    **Results:**    **PHP Symlink Function Race Condition open\_basedir Bypass (CVSS: 6.2)**  **The following results related to target www.hss.com (443/TCP):**  Version source : X-Powered-By: PHP/7.3.10  Installed version : 7.3.10    **PHP ip2long Function String Validation Weakness (CVSS: 5.0)**  **The following results related to target www.hss.com (443/TCP):**  Version source : X-Powered-By: PHP/7.3.10  Installed version : 7.3.10    **PHP mb\_send\_mail() Function Parameter Security Bypass (CVSS: 5.0)**  **The following results related to target www.hss.com (443/TCP):**  Version source : X-Powered-By: PHP/7.3.10  Installed version : 7.3.10    **PHP Foreign Function Interface Arbitrary DLL Loading safe\_mode Restriction Bypass (CVSS: 4.3)**  **The following results related to target www.hss.com (443/TCP):**  Version source : X-Powered-By: PHP/7.3.10  Installed version : 7.3.10  **Affected Hosts:**  **PHP Symlink Function Race Condition open\_basedir Bypass (CVSS: 6.2)**   |  | | --- | | www.hss.com |   **PHP ip2long Function String Validation Weakness (CVSS: 5.0)**   |  | | --- | | www.hss.com |   **PHP mb\_send\_mail() Function Parameter Security Bypass (CVSS: 5.0)**   |  | | --- | | www.hss.com |   **PHP Foreign Function Interface Arbitrary DLL Loading safe\_mode Restriction Bypass (CVSS: 4.3)**   |  | | --- | | www.hss.com |   **Recommendations**  **Users are advised to upgrade to the latest version of PHP available. For more details about PHP releases and patches please visit PHP Homepage (http://www.php.net/).**  **Patch: Following are links for downloading patches to fix the vulnerabilities: PHP (http://php.net/downloads.php)** |

| **lllll** | **SSL Certificate Signed using Weak Hashing Algorithm (CVSS: 5.0)** |
| --- | --- |
| **INF-2** | The target site uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks.  **Results**  **The following results related to target 178.250.102.166 (443/TCP):**  The following known CA certificates were part of the certificate  chain sent by the remote host, but contain hashes that are considered  to be weak.  |-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA  |-Signature Algorithm : SHA-1 With RSA Encryption  |-Valid From : Nov 10 00:00:00 2006 GMT  |-Valid To : Nov 10 00:00:00 2031 GMT  **The following results related to target www.hss.com (443/TCP):**  The following known CA certificates were part of the certificate  chain sent by the remote host, but contain hashes that are considered  to be weak.  |-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA  |-Signature Algorithm : SHA-1 With RSA Encryption  |-Valid From : Nov 10 00:00:00 2006 GMT  |-Valid To : Nov 10 00:00:00 2031 GMT   |  | | --- | | **Affected Hosts** | | 178.250.102.166 | | www.hss.com |   **Recommendations**  **Upgrade or replace the hashing algorithm**  **More information can be found at the following URL(s)**   * **https://tools.ietf.org/html/rfc3279** * **https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2008/961509** |

| **lllll** | **TLS/SSL Related Vulnerabilities (CVSS: 5.0)** |
| --- | --- |
| **INF-3** | TLS (Transport Layer Security) and SSL (Secure Sockets Layer), its predecessor, are protocols used for establishing an encrypted connection between a server and a client-typically a web server (website) and a browser. If implemented correctly, TLS allows sensitive information such as credit card details and login credentials to be transmitted securely. For SSL to be relied upon as a secure transmission protocol, it is essential that only strong ciphers and secure encryption algorithms and cipher suites are supported.    **SSL Certificate Signed using Weak Hashing Algorithm (CVSS: 5.0)**  The target site uses an SSL certificate that has been signed using a cryptographically weak hashing algorithm - MD2, MD4, or MD5. These signature algorithms are known to be vulnerable to collision attacks.    **SSL/TLS Use Of Weak RC4 cipher (CVSS: 4.3)**  Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS) protocols provide integrity, confidentiality and authenticity services to other protocols that lack these features.  SSL/TLS protocols use ciphers such as AES, DES, 3DES and RC4 to encrypt the content of the higher layer protocols and thus provide the confidentiality service. Normally the output of an encryption process is a sequence of random looking bytes. It was known that RC4 output has some bias in the output. Recently a group of researchers have discovered that there is a stronger bias in RC4, which make statistical analysis of ciphertext more practical.  The described attack is to inject a malicious JavaScript into the victim's browser that would ensure that there are multiple connections being established with a target website and the same HTTP cookie is sent multiple times to the website in encrypted form. This provides the attacker with a large set of ciphertext samples that can be used for statistical analysis.  If this attack is carried out and an HTTP cookie is recovered, then the attacker can use the cookie to impersonate the user whose cookie was recovered. This attack is not very practical as it requires the attacker to have access to millions of samples of ciphertext, but there are certain assumptions that an attacker can make to improve the chances of recovering the cleartext from cihpertext. For example, HTTP cookies are either base64 encoded or hex digits. This information can help the attacker in their efforts to recover the cookie.    **SSL RC4 Cipher Suites Supported (Bar Mitzvah) (CVSS: 2.6)**  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.    **Results:**    **SSL Certificate Signed using Weak Hashing Algorithm (CVSS: 5.0)**  **The following results related to target 178.250.102.166 (443/TCP):**  The following known CA certificates were part of the certificate  chain sent by the remote host, but contain hashes that are considered  to be weak.  |-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA  |-Signature Algorithm : SHA-1 With RSA Encryption  |-Valid From : Nov 10 00:00:00 2006 GMT  |-Valid To : Nov 10 00:00:00 2031 GMT  **The following results related to target www.hss.com (443/TCP):**  The following known CA certificates were part of the certificate  chain sent by the remote host, but contain hashes that are considered  to be weak.  |-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA  |-Signature Algorithm : SHA-1 With RSA Encryption  |-Valid From : Nov 10 00:00:00 2006 GMT  |-Valid To : Nov 10 00:00:00 2031 GMT    **SSL/TLS Use Of Weak RC4 cipher (CVSS: 4.3)**  **The following results related to target 185.160.253.20 (443/TCP):**  The SSL/TLS service on port 443 supports the following RC4 ciphers :  High Strength Ciphers (>= 112-bit key)  RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5  RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1  The fields above are :  {OpenSSL ciphername}  Kx={key exchange}  Au={authentication}  Enc={symmetric encryption method}  Mac={message authentication code}  {export flag}  **The following results related to target www.hsstraining.com (443/TCP):**  The SSL/TLS service on port 443 supports the following RC4 ciphers :  High Strength Ciphers (>= 112-bit key)  RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5  RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1  The fields above are :  {OpenSSL ciphername}  Kx={key exchange}  Au={authentication}  Enc={symmetric encryption method}  Mac={message authentication code}  {export flag}    **SSL RC4 Cipher Suites Supported (Bar Mitzvah) (CVSS: 2.6)**  **The following results related to target 185.160.253.20 (443/TCP):**  List of RC4 cipher suites supported by the remote server :  High Strength Ciphers (>= 112-bit key)  RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5  RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1  The fields above are :  {OpenSSL ciphername}  Kx={key exchange}  Au={authentication}  Enc={symmetric encryption method}  Mac={message authentication code}  {export flag}  **The following results related to target www.hsstraining.com (443/TCP):**  List of RC4 cipher suites supported by the remote server :  High Strength Ciphers (>= 112-bit key)  RC4-MD5 Kx=RSA Au=RSA Enc=RC4(128) Mac=MD5  RC4-SHA Kx=RSA Au=RSA Enc=RC4(128) Mac=SHA1  The fields above are :  {OpenSSL ciphername}  Kx={key exchange}  Au={authentication}  Enc={symmetric encryption method}  Mac={message authentication code}  {export flag}  **Affected Hosts:**  **SSL Certificate Signed using Weak Hashing Algorithm (CVSS: 5.0)**   |  | | --- | | 178.250.102.166 | | www.hss.com |   **SSL/TLS Use Of Weak RC4 cipher (CVSS: 4.3)**   |  | | --- | | 185.160.253.20 | | www.hsstraining.com |   **SSL RC4 Cipher Suites Supported (Bar Mitzvah) (CVSS: 2.6)**   |  | | --- | | 185.160.253.20 | | www.hsstraining.com |   **Recommendations**  **Disable support for TLS 1.0 and weak ciphers such as RC4 and 64-bit block ciphers. Use only TLS 1.1 or later.**  **For general SSL/TLS Deployment Best Practices, please see: https://www.ssllabs.com/projects/best-practices/** |

| **lllll** | **Microsoft ASP.NET 'ValidateRequest' filters bypass (CVSS: 4.3)** |
| --- | --- |
| **INF-4** | According to the HTTP headers received from the remote host, the web server is configured to use the ASP.NET framework.  This framework includes the 'ValidateRequest' feature, which is used by ASP.NET web applications to filter user input in an attempt to prevent cross-site scripting attacks. However, this set of filters can be bypassed if it is the sole mechanism used for protection by a web application.  ProCheckUp was unable to remotely gather enough information within the timeframe of this assessment to determine if the 'ValidateRequest' feature is used in an unsafe manner.  See Also: http://www.procheckup.com/procheckup-labs/posts/2008/august/pr08-20/ http://msdn.microsoft.com/en-us/library/bb355989.aspx  **Results**  **The following results related to target 185.160.253.20 (80/TCP):**  The following HTTP response header was received after requesting the  following URL :  URL : http://185.160.253.20.srvlist.ukfast.net/  X-Powered-By : ASP.NET  It is not possible to determine the version from the header, so this  finding may be a false positive.  **The following results related to target 185.160.253.20 (443/TCP):**  The following HTTP response header was received after requesting the  following URL :  URL : https://185.160.253.20.srvlist.ukfast.net/  X-Powered-By : ASP.NET  It is not possible to determine the version from the header, so this  finding may be a false positive.   |  | | --- | | **Affected Hosts** | | 185.160.253.20 |   **Recommendations**  **Determine if any ASP.NET web applications solely rely on the 'ValidateRequest' feature, and use additional protections if necessary.**  **More information can be found at the following URL(s)**   * **http://www.nessus.org/u?e41a641e** * **http://msdn.microsoft.com/en-us/library/bb355989.aspx** * **http://www.nessus.org/u?553a368a** |

| **lllll** | **Environment information disclosure (CVSS: 2.6)** |
| --- | --- |
| **INF-5** | The target discloses environment information which may help attackers perform more focused attacks.    **Wordpress CMS Detection (CVSS: 2.0)**  Wordpress CMS was detected on the remote host.    **Web Server - Unconfigured - Default Install Page Present (CVSS: 1.0)**  The default IIS page is displayed.    **Firewall Detected (CVSS: 0.0)**  A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control.    **Results:**    **Wordpress CMS Detection (CVSS: 2.0)**  **The following results related to target www.hss.com (443/TCP):**  URL : https://www.hss.com/blog  Version : 5.2.4    **Web Server - Unconfigured - Default Install Page Present (CVSS: 1.0)**  **The following results related to target 185.160.253.20 (80/TCP):**  The default welcome page is from IIS.  The IIS server listening on port 80 uses the  default index page:  http://185.160.253.20.srvlist.ukfast.net/  **The following results related to target 185.160.253.20 (443/TCP):**  The default welcome page is from IIS.  The IIS server listening on port 443 uses the  default index page:  https://185.160.253.20.srvlist.ukfast.net/  **Affected Hosts:**  **Wordpress CMS Detection (CVSS: 2.0)**   |  | | --- | | www.hss.com |   **Web Server - Unconfigured - Default Install Page Present (CVSS: 1.0)**   |  | | --- | | 185.160.253.20 |   **Firewall Detected (CVSS: 0.0)**   |  | | --- | | 178.250.102.166 | | 185.160.253.20 | | www.hss.com | | www.hsstraining.com |   **Recommendations**  **In general, avoid disclosing environment information, such as version numbers, error pages and internal IP addresses.** |

| **lllll** | **Environment Information Disclosure (CVSS: 2.6)** |
| --- | --- |
| **INF-6** | The target discloses environment information which may help attackers perform more focused attacks.  **Results**  **The following results related to target 178.250.102.166:**  + 2 web servers are vulnerable to insecure http methods enabled  **The following results related to target 178.250.102.166 (80/TCP):**  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target 178.250.102.166 (443/TCP):**  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target 185.160.253.20:**  + 2 web servers are vulnerable to default web server files  + 2 web servers are vulnerable to insecure http methods enabled  **The following results related to target 185.160.253.20 (80/TCP):**  Server type : Microsoft IIS  Server version : 8.5  Source : Microsoft-IIS/8.5  Additional data : X-Powered-By: ASP.NET  The remote web server is vulnerable to default web server files  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target 185.160.253.20 (443/TCP):**  Server type : Microsoft IIS  Server version : 8.5  Source : Microsoft-IIS/8.5  Additional data : X-Powered-By: ASP.NET  The remote web server is vulnerable to default web server files  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target www.hss.com:**  + 2 web servers are vulnerable to insecure http methods enabled  **The following results related to target www.hss.com (80/TCP):**  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target www.hss.com (443/TCP):**  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target www.hsstraining.com:**  + 2 web servers are vulnerable to insecure http methods enabled  **The following results related to target www.hsstraining.com (80/TCP):**  Server type : Microsoft IIS  Server version : 8.5  Source : Microsoft-IIS/8.5  The remote web server is vulnerable to insecure http methods enabled  **The following results related to target www.hsstraining.com (443/TCP):**  The remote web server is vulnerable to insecure http methods enabled   |  | | --- | | **Affected Hosts** | | 178.250.102.166 | | 185.160.253.20 | | www.hss.com | | www.hsstraining.com |   **Recommendations**  **In general, avoid disclosing environment information, such as version numbers, error pages and internal IP addresses.** |

| **lllll** | **TCP Timestamp Option Enabled (CVSS: 2.6)** |
| --- | --- |
| **INF-7** | Typically, the timestamp used is the host's uptime (since last reboot) in various units (e.g., one hundredth of second, one tenth of a second, etc.). Based on this, we can obtain the host's uptime. After determining the uptime of the system it could be possible for an attacker to deduce which patches have been applied to the system. Some critical patches require system reboots, thus, if a system has been up for a long time, this might indicate that the recent patch has not been applied to the host.   |  | | --- | | **Affected Hosts** | | 178.250.102.166 | | 185.160.253.20 | | www.hss.com | | www.hsstraining.com |   **Recommendations**  **The TCP timestamp option on the host should be disabled. Alternatively, this could be filtered at the router or firewall.**    **More information can be found at the following URL(s): http://www.ietf.org/rfc/rfc1323.txt https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524**  **More information can be found at the following URL(s)**   * **http://www.ietf.org/rfc/rfc1323.txt** |

### 5.2 Application

| **lllll** | **Script Src Integrity Check (CVSS: 7.8)** |
| --- | --- |
| **APP-1** | The remote host may be vulnerable to payment entry data exfiltration due to javascript included from potentially untrusted and unverified third parties script src. If the host is controlled by a 3rd party, ensure that the 3rd party is PCI DSS compliant.  **Results**  **The following results related to target www.hss.com (443/TCP):**  Path : https://payments.worldpay.com/resources/hpp/integrations/embedded/js/hpp-embedded-integration-library.js  Attributes :  - src : https://payments.worldpay.com/resources/hpp/integrations/embedded/js/hpp-embedded-integration-library.js  Path : https://d3c3cq33003psk.cloudfront.net/opentag-49710-1351226.js  Attributes :  - defer : defer  - src : //d3c3cq33003psk.cloudfront.net/opentag-49710-1351226.js  Path : https://d2oh4tlt9mrke9.cloudfront.net/Record/js/sessioncam.js?ver=1.2  Attributes :  - type : text/javascript  - src : https://d2oh4tlt9mrke9.cloudfront.net/Record/js/sessioncam.js?ver=1.2  Path : https://s7.addthis.com/js/300/addthis\_widget.js#pubid=ra-5819cd5529156266  Attributes :  - type : text/javascript  - src : //s7.addthis.com/js/300/addthis\_widget.js#pubid=ra-5819cd5529156266  Path : https://pool.admedo.com/pixel?id=140750&t=js  Attributes :  - type : text/javascript  - src : //pool.admedo.com/pixel?id=140750&t=js  Path : https://maps.googleapis.com/maps/api/js?v=3.25&key=AIzaSyC8KLMV5KzQiFbANxbcrAUfaVm8I9-0OIs&libraries=places  Attributes :  - type : text/javascript  - src : https://maps.googleapis.com/maps/api/js?v=3.25&key=AIzaSyC8KLMV5KzQiFbANxbcrAUfaVm8I9-0OIs&libraries=places  Path : https://services.postcodeanywhere.co.uk/js/captureplus-2.30.min.js?key=rt74-xw14-gw36-rm79  Attributes :  - type : text/javascript  - src : https://services.postcodeanywhere.co.uk/js/captureplus-2.30.min.js?key=rt74-xw14-gw36-rm79  Path : https://services.postcodeanywhere.co.uk/js/captureplus-2.20.min.js?key=uf35-kf59-jd73-gg49  Attributes :  - type : text/javascript  - src : https://services.postcodeanywhere.co.uk/js/captureplus-2.20.min.js?key=uf35-kf59-jd73-gg49  **The following results related to target www.hsstraining.com (443/TCP):**  Path : https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js  Attributes :  - src : https://ajax.googleapis.com/ajax/libs/jquery/3.1.1/jquery.min.js  Path : https://cdn.jsdelivr.net/bxslider/4.2.12/jquery.bxslider.min.js  Attributes :  - src : https://cdn.jsdelivr.net/bxslider/4.2.12/jquery.bxslider.min.js  Path : https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js  Attributes :  - src : https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/js/bootstrap.min.js  Path : https://ajax.googleapis.com/ajax/libs/angularjs/1.4.8/angular.js  Attributes :  - src : https://ajax.googleapis.com/ajax/libs/angularjs/1.4.8/angular.js  Path : https://ajax.googleapis.com/ajax/libs/angularjs/1.4.8/angular-route.js  Attributes :  - src : https://ajax.googleapis.com/ajax/libs/angularjs/1.4.8/angular-route.js  Path : https://cdnjs.cloudflare.com/ajax/libs/angular-sanitize/1.4.8/angular-sanitize.min.js  Attributes :  - src : https://cdnjs.cloudflare.com/ajax/libs/angular-sanitize/1.4.8/angular-sanitize.min.js  Path : https://code.jquery.com/ui/1.12.1/jquery-ui.js  Attributes :  - src : https://code.jquery.com/ui/1.12.1/jquery-ui.js  Path : https://payments.worldpay.com/resources/hpp/integrations/embedded/js/hpp-embedded-integration-library.js  Attributes :  - src : https://payments.worldpay.com/resources/hpp/integrations/embedded/js/hpp-embedded-integration-library.js  Path : https://maps.googleapis.com/maps/api/js?key=AIzaSyC8KLMV5KzQiFbANxbcrAUfaVm8I9-0OIs&libraries=places  Attributes :  - src : https://maps.googleapis.com/maps/api/js?key=AIzaSyC8KLMV5KzQiFbANxbcrAUfaVm8I9-0OIs&libraries=places   |  | | --- | | **Affected Hosts** | | www.hss.com | | www.hsstraining.com |   **Recommendations**  **Set script integrity checking on target script or remove target script.**  **More information can be found at the following URL(s)**   * **http://www.nessus.org/u?c9e76c4f** * **https://www.w3.org/TR/SRI/** * **http://www.nessus.org/u?f39144f8** |

| **lllll** | **CGI Generic Cross-Site Request Forgery Detection (potential) (CVSS: 6.4)** |
| --- | --- |
| **APP-2** | ProCheckUp has found HTML forms on the remote web server. Some CGI scripts do not appear to be protected by random tokens, a common anti-cross-site request forgery (XSRF) protection. The web application might be vulnerable to XSRF attacks. Note that : - ProCheckup did not exploit the flaw. - ProCheckUp cannot identify sensitive actions; for example, on an online bank, consulting an account is less sensitive than transferring money. You will need to audit the source of the CGI scripts and check if they are actually affected.  **Results**  **The following results related to target www.hss.com (443/TCP):**  The following CGIs are not protected by a random token :  /easy-as-hss  /hire/p/floor-and-edge-sander-hire-pack  /hire/c/sanding-and-fixing/  /blog/tips-and-advice/gardening-and-landscaping/october-gardening-activity/  /blog/tips-and-advice/concreting-and-preparation/finding-the-right-breaker-for-the-job/  /blog  /blog/  /abird-apex/search  /abird-apex/search/  /blog/wp-comments-post.php  /hire/find-a-branch  /onecall/search/  /onecall/search  /all-seasons-hire/search/  /all-seasons-hire/search  /blog/winter-preparation/heating/hss-guide-heating/  /blog/how-to-guides/flooring/are-you-thinking-of-sanding-your-floor/  /hire/p/carpet-cleaner-small  /hire/c/heating/  /hire/search/  /hire/search   |  | | --- | | **Affected Hosts** | | www.hss.com |   **Recommendations**  **Restrict access to the vulnerable application. Contact the vendor for a patch or upgrade.**  **More information can be found at the following URL(s)**   * **https://en.wikipedia.org/wiki/Cross-site\_request\_forgery** |

| **lllll** | **Sensitive File Disclosure (CVSS: 5.0)** |
| --- | --- |
| **APP-3** | The remote web application hosts documents or office files that may contain sensitive information.  **Results**  **The following results related to target www.hss.com (80/TCP):**  The following URLs are potentially sensitive documents :  /medias/sys\_master/root/8877307887646.pdf  /medias/sys\_master/docs/docs/8796175826974.pdf  /medias/sys\_master/root/8871998455838.pdf  /medias/sys\_master/root/8941022314526.pdf  /medias/sys\_master/docs/docs/8803097280542.pdf  /medias/sys\_master/docs/docs/8803096985630.pdf  /medias/sys\_master/docs/docs/8803096592414.pdf  /medias/sys\_master/docs/docs/8803096887326.pdf  /medias/sys\_master/docs/docs/8840124563486.pdf  /medias/sys\_master/docs/docs/8838347292702.pdf  /medias/sys\_master/docs/docs/8796155019294.pdf  /medias/sys\_master/docs/docs/8796154396702.pdf  /medias/sys\_master/docs/docs/8984508596254.pdf  /medias/sys\_master/docs/docs/8796154920990.pdf  /medias/sys\_master/docs/docs/8837599035422.pdf  /medias/sys\_master/docs/docs/8837599100958.pdf  /medias/sys\_master/docs/docs/8836963631134.pdf  /medias/sys\_master/docs/docs/8837602803742.pdf  /medias/sys\_master/docs/docs/8796144369694.pdf  /medias/sys\_master/docs/docs/8986574716958.pdf  /medias/sys\_master/docs/docs/8836979130398.pdf  /medias/sys\_master/docs/docs/8837600411678.pdf  /medias/sys\_master/docs/docs/8837595267102.pdf  /medias/sys\_master/docs/docs/8796156133406.pdf  /medias/sys\_master/docs/docs/8836630151198.pdf  /medias/sys\_master/docs/docs/8837596676126.pdf  /medias/sys\_master/images/images/8837609783326.pdf  /medias/sys\_master/docs/docs/8837609914398.pdf  /medias/sys\_master/docs/docs/8837601591326.pdf  /medias/sys\_master/docs/docs/8837606998046.pdf  /medias/sys\_master/docs/docs/8837604999198.pdf  /medias/sys\_master/docs/docs/8837605064734.pdf  /medias/sys\_master/docs/docs/8837608964126.pdf  /medias/sys\_master/docs/docs/8837619089438.pdf  /medias/sys\_master/docs/docs/8837621153822.pdf  /medias/sys\_master/docs/docs/8835184033822.pdf  /medias/sys\_master/docs/docs/8796147154974.pdf  **The following results related to target www.hss.com (443/TCP):**  The following URLs are potentially sensitive documents :  /medias/sys\_master/root/8877307887646.pdf  /medias/sys\_master/docs/docs/8796175826974.pdf  /medias/sys\_master/root/8871998455838.pdf  /medias/sys\_master/root/8941022314526.pdf  /medias/sys\_master/docs/docs/8803097280542.pdf  /medias/sys\_master/docs/docs/8803096985630.pdf  /medias/sys\_master/docs/docs/8803096592414.pdf  /medias/sys\_master/docs/docs/8803096887326.pdf  /medias/sys\_master/docs/docs/8840124563486.pdf  /medias/sys\_master/docs/docs/8838347292702.pdf  /medias/sys\_master/docs/docs/8796155019294.pdf  /medias/sys\_master/docs/docs/8796154396702.pdf  /medias/sys\_master/docs/docs/8984508596254.pdf  /medias/sys\_master/docs/docs/8796154920990.pdf  /medias/sys\_master/docs/docs/8837599035422.pdf  /medias/sys\_master/docs/docs/8837599100958.pdf  /medias/sys\_master/docs/docs/8836963631134.pdf  /medias/sys\_master/docs/docs/8837602803742.pdf  /medias/sys\_master/docs/docs/8796144369694.pdf  /medias/sys\_master/docs/docs/8986574716958.pdf  /medias/sys\_master/docs/docs/8836979130398.pdf  /medias/sys\_master/docs/docs/8837600411678.pdf  /medias/sys\_master/docs/docs/8837595267102.pdf  /medias/sys\_master/docs/docs/8796156133406.pdf  /medias/sys\_master/docs/docs/8836630151198.pdf  /medias/sys\_master/docs/docs/8837596676126.pdf  /medias/sys\_master/images/images/8837609783326.pdf  /medias/sys\_master/docs/docs/8837609914398.pdf  /medias/sys\_master/docs/docs/8837601591326.pdf  /medias/sys\_master/docs/docs/8837606998046.pdf  /medias/sys\_master/docs/docs/8837604999198.pdf  /medias/sys\_master/docs/docs/8837605064734.pdf  /medias/sys\_master/docs/docs/8837608964126.pdf  /medias/sys\_master/docs/docs/8837619089438.pdf  /medias/sys\_master/docs/docs/8837621153822.pdf  /medias/sys\_master/docs/docs/8835184033822.pdf  /medias/sys\_master/docs/docs/8796147154974.pdf   |  | | --- | | **Affected Hosts** | | www.hss.com |   **Recommendations**  **Static files that are not necessary should be removed from the web root. If documents are required to be in the web root, and are sensitive in nature, they should require authentication.** |

| **lllll** | **Cookies Set Without the 'HttpOnly' Flag (CVSS: 4.3)** |
| --- | --- |
| **APP-4** | Cookies are set without using the 'HttpOnly' flag. The HttpOnly flag prevents scripting code such as JavaScript from accessing the cookie. This helps prevent cookie theft through cross-site scripting attacks in which the 'document.cookie' object is used to redirect cookies to third-party web servers under the control of the attacker.  **Results**  **The following results related to target www.hss.com (80/TCP):**  The following cookies do not set the HttpOnly cookie flag :  Name : recentlyViewed  Path : /  Value : vt1-eco-lighting-tower|plasterers-light|smithlight|led-self-righting-work-lights|commercial-infra-red-heaters|lpg-ducted-heate  Domain :  Version : 1  Expires : Thu, 14-Nov-2019 04:59:01 GMT  Comment :  Secure : 0  Httponly : 0  Port :  Name : hssstorefrontRememberMe  Path : /  Value : ""  Domain :  Version : 1  Expires : Thu, 01-Jan-1970 00:00:10 GMT  Comment :  Secure : 0  Httponly : 0  Port :  **The following results related to target www.hss.com (443/TCP):**  The following cookies do not set the HttpOnly cookie flag :  Name : recentlyViewed  Path : /  Value : vt1-eco-lighting-tower|plasterers-light|smithlight|led-self-righting-work-lights|commercial-infra-red-heaters|lpg-ducted-heate  Domain :  Version : 1  Expires : Thu, 14-Nov-2019 04:59:01 GMT  Comment :  Secure : 0  Httponly : 0  Port :  Name : hssstorefrontRememberMe  Path : /  Value : ""  Domain :  Version : 1  Expires : Thu, 01-Jan-1970 00:00:10 GMT  Comment :  Secure : 0  Httponly : 0  Port :   |  | | --- | | **Affected Hosts** | | www.hss.com |   **Recommendations**  **Issue cookies using the 'HttpOnly' flags.**  **More information can be found at the following URL(s)**   * **https://www.owasp.org/index.php/HttpOnly** |

| **lllll** | **Cookies Set Without The 'Secure' Flag (CVSS: 4.3)** |
| --- | --- |
| **APP-5** | Cookies are set without using the 'Secure' flag. This flag is recommended as it prevents web browsers from submitting cookies over clear text (only HTTPS is allowed).  **Results**  **The following results related to target www.hss.com (80/TCP):**  The following cookies do not set the secure cookie flag :  Name : recentlyViewed  Path : /  Value : vt1-eco-lighting-tower|plasterers-light|smithlight|led-self-righting-work-lights|commercial-infra-red-heaters|lpg-ducted-heate  Domain :  Version : 1  Expires : Thu, 14-Nov-2019 04:59:01 GMT  Comment :  Secure : 0  Httponly : 0  Port :  Name : hss-uk-cart  Path : ""  Value : f2a62153a2c4bdbf9db1491bbe99cd0bd53b5642  Domain :  Version : 1  Expires : Fri, 13-Dec-2019 04:59:02 GMT  Comment :  Secure : 0  Httponly : 1  Port :  Name : hssstorefrontRememberMe  Path : /  Value : ""  Domain :  Version : 1  Expires : Thu, 01-Jan-1970 00:00:10 GMT  Comment :  Secure : 0  Httponly : 0  Port :  **The following results related to target www.hss.com (443/TCP):**  The following cookies do not set the secure cookie flag :  Name : recentlyViewed  Path : /  Value : vt1-eco-lighting-tower|plasterers-light|smithlight|led-self-righting-work-lights|commercial-infra-red-heaters|lpg-ducted-heate  Domain :  Version : 1  Expires : Thu, 14-Nov-2019 04:59:01 GMT  Comment :  Secure : 0  Httponly : 0  Port :  Name : hss-uk-cart  Path : ""  Value : f2a62153a2c4bdbf9db1491bbe99cd0bd53b5642  Domain :  Version : 1  Expires : Fri, 13-Dec-2019 04:59:02 GMT  Comment :  Secure : 0  Httponly : 1  Port :  Name : hssstorefrontRememberMe  Path : /  Value : ""  Domain :  Version : 1  Expires : Thu, 01-Jan-1970 00:00:10 GMT  Comment :  Secure : 0  Httponly : 0  Port :   |  | | --- | | **Affected Hosts** | | www.hss.com |   **Recommendations**  **Issue cookies using the 'Secure' flags. It may not always be feasible to implement the 'Secure' flag on every cookie, as some non-session critical cookies will be passed between HTTP and HTTPS. See** [**https://www.owasp.org/index.php/SecureFlag**](%20https://www.owasp.org/index.php/SecureFlag)  **More information can be found at the following URL(s)**   * **https://www.owasp.org/index.php/SecureFlag** |

| **lllll** | **Missing HTTP Response Headers (CVSS: 4.3)** |
| --- | --- |
| **APP-6** | A number of HTTP response headers are recommended to improve security. Not all the recommended headers were found in responses from the application. Specifically, the following were found to be missing:    **Clickjacking - X-Frame-Options Header Is Not Set (CVSS: 4.3)**  X-Frame-Options header is not set, and that may lead to a possible framing of the page. An attacker can trick the user into clicking on the link by framing the original page and showing a layer on top of it with dummy buttons.    **Strict Transport Header Setting Missing (CVSS: 4.3)**  There was no "Strict-Transport-Security" header in the server response.  The HTTP Strict Transport Security policy defines a timeframe where a browser must connect to the web server via HTTPS. Without a Strict Transport Security policy, the web application may be vulnerable against several attacks: If the web application mixes usage of HTTP and HTTPS, an attacker can manipulate pages in the unsecured area of the application or change redirection targets (either in a manner that the switch to the secured page is not performed or where the attacker remains between client and server). If there is no HTTP server, an attacker in the same network could simulate a HTTP server and motivate the user to click on a prepared URL by a social engineering attack. The protection is effective only for the given amount of time. Multiple occurrences of this header could cause undefined behaviour in browsers and should be avoided.    **Results:**    **Clickjacking - X-Frame-Options Header Is Not Set (CVSS: 4.3)**  **The following results related to target 185.160.253.20 (80/TCP):**  The following pages do not set a X-Frame-Options response header or set a permissive policy:  - http://185.160.253.20.srvlist.ukfast.net/  **The following results related to target 185.160.253.20 (443/TCP):**  The following pages do not set a X-Frame-Options response header or set a permissive policy:  - https://185.160.253.20.srvlist.ukfast.net/  **The following results related to target www.hss.com (443/TCP):**  The following pages do not set a X-Frame-Options response header or set a permissive policy:  - https://www.hss.com/abird-apex/  - https://www.hss.com/abird-apex/c/abird-apex-generators/  - https://www.hss.com/abird-apex/c/abird-apex/  - https://www.hss.com/abird-apex/c/lighting-tower/  - https://www.hss.com/abird-apex/contact-us  - https://www.hss.com/abird-apex/find-a-branch/all-branches  - https://www.hss.com/abird-apex/fuel-savings  - https://www.hss.com/abird-apex/harvest-energy  - https://www.hss.com/abird-apex/login  - https://www.hss.com/abird-apex/p/1250kva-silenced-generator  - https://www.hss.com/abird-apex/p/1260kva-whisper-box-generator  - https://www.hss.com/abird-apex/p/180kva-silenced-generator  - https://www.hss.com/abird-apex/p/40kva-silenced-generator  - https://www.hss.com/abird-apex/p/60kva-silenced-generator  - https://www.hss.com/abird-apex/p/8kva-lighting-tower  - https://www.hss.com/abird-apex/power-your-events  - https://www.hss.com/abird-apex/pre-register  - https://www.hss.com/abird-apex/remote-fleet-management  - https://www.hss.com/abird-apex/search  - https://www.hss.com/abird-apex/search/  - https://www.hss.com/all-seasons-hire  - https://www.hss.com/all-seasons-hire/  - https://www.hss.com/all-seasons-hire/about-us  - https://www.hss.com/all-seasons-hire/air-conditioning-services  - https://www.hss.com/all-seasons-hire/all-seasons-hire-air-conditioning  - https://www.hss.com/all-seasons-hire/all-seasons-hire-boilers  - https://www.hss.com/all-seasons-hire/all-seasons-hire-chillers  - https://www.hss.com/all-seasons-hire/all-seasons-hire-heating  - https://www.hss.com/all-seasons-hire/boiler-hire-services  - https://www.hss.com/all-seasons-hire/c/air-conditioners-ash/  - https://www.hss.com/all-seasons-hire/c/air-handlers-ash/  - https://www.hss.com/all-seasons-hire/c/all-seasons-hire/  - https://www.hss.com/all-seasons-hire/c/boilers-and-burners-ash/  - https://www.hss.com/all-seasons-hire/c/chillers-ash/  - https://www.hss.com/all-seasons-hire/c/dehumidifiers-and-dryers-ash/  - https://www.hss.com/all-seasons-hire/c/fuel-tanks-ash/  - https://www.hss.com/all-seasons-hire/c/heaters-ash/  - https://www.hss.com/all-seasons-hire/chiller-hire-services  - https://www.hss.com/all-seasons-hire/contact-us  - https://www.hss.com/all-seasons-hire/find-a-branch/all-branches  - https://www.hss.com/all-seasons-hire/find-a-branch/current-location  - https://www.hss.com/all-seasons-hire/find-a-branch/tel%3A%2B4408000828001  - https://www.hss.com/all-seasons-hire/fuel-management  - https://www.hss.com/all-seasons-hire/heating-solutions  - https://www.hss.com/all-seasons-hire/login  - https://www.hss.com/all-seasons-hire/p/1-2mw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/1.2mw-containerised-boiler-600kw-dual-burner  - https://www.hss.com/all-seasons-hire/p/100kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/100kw-bicold-heat-pump-chiller  - https://www.hss.com/all-seasons-hire/p/100kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/100kw-fluid-chiller  - https://www.hss.com/all-seasons-hire/p/100kw-heat-pump-chiller  - https://www.hss.com/all-seasons-hire/p/100kw-packaged-boiler  - https://www.hss.com/all-seasons-hire/p/10kw-chiller  - https://www.hss.com/all-seasons-hire/p/10kw-heat-pump-chiller  - https://www.hss.com/all-seasons-hire/p/15-30kw-air-handler  - https://www.hss.com/all-seasons-hire/p/150kw-trane-heat-pump-chiller  - https://www.hss.com/all-seasons-hire/p/160kw-fluid-chiller-mta  - https://www.hss.com/all-seasons-hire/p/20-40kw-air-handler  - https://www.hss.com/all-seasons-hire/p/20-40kw-event-air-handler-black  - https://www.hss.com/all-seasons-hire/p/20-40kw-event-air-handler-white  - https://www.hss.com/all-seasons-hire/p/200kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/200kw-trane-heat-pump-chiller-  - https://www.hss.com/all-seasons-hire/p/20kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/250kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/250kw-electric-container-boiler  - https://www.hss.com/all-seasons-hire/p/30-60kw-air-handler  - https://www.hss.com/all-seasons-hire/p/300kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/300kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/30kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/320kw-fluid-chiller  - https://www.hss.com/all-seasons-hire/p/350kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/45kw-chiller  - https://www.hss.com/all-seasons-hire/p/50-100kw-air-handler  - https://www.hss.com/all-seasons-hire/p/50-100kw-air-handler-small-footprint  - https://www.hss.com/all-seasons-hire/p/500kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/500kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/50kw-chiller  - https://www.hss.com/all-seasons-hire/p/50kw-low-temperature-air-handler  - https://www.hss.com/all-seasons-hire/p/550kw-boiler-trailer  - https://www.hss.com/all-seasons-hire/p/550kw-fluid-chiller  - https://www.hss.com/all-seasons-hire/p/5kw-chiller  - https://www.hss.com/all-seasons-hire/p/600kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/620kw-containerised-boiler  - https://www.hss.com/all-seasons-hire/p/750kw-trane-chiller  - https://www.hss.com/all-seasons-hire/p/75kw-fluid-chiller  - https://www.hss.com/all-seasons-hire/p/80kw-bicold-chiller  - https://www.hss.com/all-seasons-hire/p/95kw-compact-boiler  - https://www.hss.com/all-seasons-hire/p/air-handler-100kw  - https://www.hss.com/all-seasons-hire/p/air-handler-150kw  - https://www.hss.com/all-seasons-hire/p/all-seasons-hire/p/evaporative-coolers-cool-space-glacier-tb  - https://www.hss.com/all-seasons-hire/p/arcotherm-jumbo-150s-oil  - https://www.hss.com/all-seasons-hire/p/arcotherm-jumbo-200kw-1ph  - https://www.hss.com/all-seasons-hire/p/big-brother-100kw-gas  - https://www.hss.com/all-seasons-hire/p/breezeair  - https://www.hss.com/all-seasons-hire/p/comcool-230v  - https://www.hss.com/all-seasons-hire/p/commander-3000  - https://www.hss.com/all-seasons-hire/p/cool-space-avalanche  - https://www.hss.com/all-seasons-hire/p/cool-space-blizzard  - https://www.hss.com/all-seasons-hire/p/cool-space-glacier  - https://www.hss.com/all-seasons-hire/p/cool-space-glacier-tb  - https://www.hss.com/all-seasons-hire/p/cool-space-wave  - https://www.hss.com/all-seasons-hire/p/coolair-12  - https://www.hss.com/all-seasons-hire/p/coolair-14  - https://www.hss.com/all-seasons-hire/p/coolair-15  - https://www.hss.com/all-seasons-hire/p/coolbreeze-15e  - https://www.hss.com/all-seasons-hire/p/coolbreeze-15p  - https://www.hss.com/all-seasons-hire/p/coolbreeze-20e  - https://www.hss.com/all-seasons-hire/p/coolbreeze-22p  - https://www.hss.com/all-seasons-hire/p/coolbreeze-25b  - https://www.hss.com/all-seasons-hire/p/coolbreeze-25p  - https://www.hss.com/all-seasons-hire/p/coolbreeze-27e  - https://www.hss.com/all-seasons-hire/p/coolbreeze-28e  - https://www.hss.com/all-seasons-hire/p/coolbreeze-35e  - https://www.hss.com/all-seasons-hire/p/coolbreeze-50b  - https://www.hss.com/all-seasons-hire/p/cyclone-30-230v  - https://www.hss.com/all-seasons-hire/p/cyclone-50-110v  - https://www.hss.com/all-seasons-hire/p/electric-boiler-22kw  - https://www.hss.com/all-seasons-hire/p/evaporative-coolers-cool-space-glacier-tb  - https://www.hss.com/all-seasons-hire/p/event-heater  - https://www.hss.com/all-seasons-hire/p/fire-flo-ff42-42kw  - https://www.hss.com/all-seasons-hire/p/honeywell-cl60pm  - https://www.hss.com/all-seasons-hire/p/hot-block-25-3kw  - https://www.hss.com/all-seasons-hire/p/hot-block-65-12kw  - https://www.hss.com/all-seasons-hire/p/hot-cube-25-3kw-230v  - https://www.hss.com/all-seasons-hire/p/hot-cube-65  - https://www.hss.com/all-seasons-hire/p/hot-cube-800  - https://www.hss.com/all-seasons-hire/p/hot-cube-95-3-phase  - https://www.hss.com/all-seasons-hire/p/hot-house-ace-140kw-oil  - https://www.hss.com/all-seasons-hire/p/hot-house-ace-150  - https://www.hss.com/all-seasons-hire/p/hot-house-ace-200kw-oil  - https://www.hss.com/all-seasons-hire/p/kalahari  - https://www.hss.com/all-seasons-hire/p/little-brother-60-58-4kw  - https://www.hss.com/all-seasons-hire/p/mojave-cr40  - https://www.hss.com/all-seasons-hire/p/mojave-cr70  - https://www.hss.com/all-seasons-hire/p/ordos-dv  - https://www.hss.com/all-seasons-hire/p/powerblow-carpet-dryer  - https://www.hss.com/all-seasons-hire/p/quattro-plus-gas  - https://www.hss.com/all-seasons-hire/p/radial-200-3ph-heater  - https://www.hss.com/all-seasons-hire/p/radial-65kw-230v-oil  - https://www.hss.com/all-seasons-hire/p/red-star-25kw-230v  - https://www.hss.com/all-seasons-hire/p/red-star-30kw  - https://www.hss.com/all-seasons-hire/p/red-star-85-230v  - https://www.hss.com/all-seasons-hire/p/slendertherm-2-5kw-oil-rads  - https://www.hss.com/all-seasons-hire/p/solaris-28kw  - https://www.hss.com/all-seasons-hire/p/tanami-35  - https://www.hss.com/all-seasons-hire/p/vulcan-3kw  - https://www.hss.com/all-seasons-hire/p/warm-glow-3kw-230v  - https://www.hss.com/all-seasons-hire/pre-register  - https://www.hss.com/all-seasons-hire/search  - https://www.hss.com/all-seasons-hire/search/  - https://www.hss.com/all-seasons-hire/services  - https://www.hss.com/blog/  - https://www.hss.com/blog/calculators-results/  - https://www.hss.com/blog/calculators/  - https://www.hss.com/blog/category/company-news/  - https://www.hss.com/blog/category/company-news/allseasonshire/  - https://www.hss.com/blog/category/company-news/allseasonshire/page/2/  - https://www.hss.com/blog/category/company-news/csr/  - https://www.hss.com/blog/category/company-news/page/2/  - https://www.hss.com/blog/category/company-news/pr/  - https://www.hss.com/blog/category/how-to-guides/  - https://www.hss.com/blog/ca  [Read More..](https://report.portal.procheckup.com/Customers/ResultDetail?name=Missing+HTTP+Response+Headers+&host=www.hss.com&port=443&protocol=TCP&testId=1117)  **The following results related to target www.hsstraining.com (443/TCP):**  The following pages do not set a X-Frame-Options response header or set a permissive policy:  - https://www.hsstraining.com/  - https://www.hsstraining.com/basket  - https://www.hsstraining.com/bst  - https://www.hsstraining.com/bstHist  - https://www.hsstraining.com/c  - https://www.hsstraining.com/click  - https://www.hsstraining.com/contact  - https://www.hsstraining.com/content  - https://www.hsstraining.com/content/basket  - https://www.hsstraining.com/content/bst  - https://www.hsstraining.com/content/bstHist  - https://www.hsstraining.com/content/c  - https://www.hsstraining.com/content/click  - https://www.hsstraining.com/content/content  - https://www.hsstraining.com/content/content/basket  - https://www.hsstraining.com/content/content/bst  - https://www.hsstraining.com/content/content/bstHist  - https://www.hsstraining.com/content/content/c  - https://www.hsstraining.com/content/content/click  - https://www.hsstraining.com/content/content/contact  - https://www.hsstraining.com/content/content/content  - https://www.hsstraining.com/content/content/content/basket  - https://www.hsstraining.com/content/content/content/bst  - https://www.hsstraining.com/content/content/content/bstHist  - https://www.hsstraining.com/content/content/content/c  - https://www.hsstraining.com/content/content/content/click  - https://www.hsstraining.com/content/content/content/contact  - https://www.hsstraining.com/content/content/content/content  - https://www.hsstraining.com/content/content/content/content/basket  - https://www.hsstraining.com/content/content/content/content/bst  - https://www.hsstraining.com/content/content/content/content/bstHist  - https://www.hsstraining.com/content/content/content/content/c  - https://www.hsstraining.com/content/content/content/content/click  - https://www.hsstraining.com/content/content/content/content/contact  - https://www.hsstraining.com/content/content/content/content/content  - https://www.hsstraining.com/content/content/content/content/content/basket  - https://www.hsstraining.com/content/content/content/content/content/bst  - https://www.hsstraining.com/content/content/content/content/content/bstHist  - https://www.hsstraining.com/content/content/content/content/content/c  - https://www.hsstraining.com/content/content/content/content/content/click  - https://www.hsstraining.com/content/content/content/content/content/contact  - https://www.hsstraining.com/content/content/content/content/content/content  - https://www.hsstraining.com/content/content/content/content/content/content/basket  - https://www.hsstraining.com/content/content/content/content/content/content/bst  - https://www.hsstraining.com/content/content/content/content/content/content/bstHist  - https://www.hsstraining.com/content/content/content/content/content/content/c  - https://www.hsstraining.com/content/content/content/content/content/content/click  - https://www.hsstraining.com/content/content/content/content/content/content/contact  - https://www.hsstraining.com/content/content/content/content/content/content/content  - https://www.hsstraining.com/content/content/content/content/content/content/content/basket  - https://www.hsstraining.com/content/content/content/content/content/content/content/bst  - https://www.hsstraining.com/content/content/content/content/content/content/content/bstHist  - https://www.hsstraining.com/content/content/content/content/content/content/content/c  - https://www.hsstraining.com/content/content/content/content/content/content/content/click  - https://www.hsstraining.com/content/content/content/content/content/content/content/contact  - https://www.hsstraining.com/content/content/content/content/content/content/content/credit-account-application  - https://www.hsstraining.com/content/content/content/content/content/content/content/home  - https://www.hsstraining.com/content/content/content/content/content/content/content/keypress  - https://www.hsstraining.com/content/content/content/content/content/content/content/login  - https://www.hsstraining.com/content/content/content/content/content/content/content/pre-register  - https://www.hsstraining.com/content/content/content/content/content/content/content/profile  - https://www.hsstraining.com/content/content/content/content/content/content/content/requestAnimationFrame  - https://www.hsstraining.com/content/content/content/content/content/content/content/scroll  - https://www.hsstraining.com/content/content/content/content/content/content/content/training-centre-landing  - https://www.hsstraining.com/content/content/content/content/content/content/content/webkit  - https://www.hsstraining.com/content/content/content/content/content/content/content/webkitC  - https://www.hsstraining.com/content/content/content/content/content/content/credit-account-application  - https://www.hsstraining.com/content/content/content/content/content/content/home  - https://www.hsstraining.com/content/content/content/content/content/content/keypress  - https://www.hsstraining.com/content/content/content/content/content/content/login  - https://www.hsstraining.com/content/content/content/content/content/content/pre-register  - https://www.hsstraining.com/content/content/content/content/content/content/profile  - https://www.hsstraining.com/content/content/content/content/content/content/requestAnimationFrame  - https://www.hsstraining.com/content/content/content/content/content/content/scroll  - https://www.hsstraining.com/content/content/content/content/content/content/training-centre-landing  - https://www.hsstraining.com/content/content/content/content/content/content/webkit  - https://www.hsstraining.com/content/content/content/content/content/content/webkitC  - https://www.hsstraining.com/content/content/content/content/content/credit-account-application  - https://www.hsstraining.com/content/content/content/content/content/home  - https://www.hsstraining.com/content/content/content/content/content/keypress  - https://www.hsstraining.com/content/content/content/content/content/login  - https://www.hsstraining.com/content/content/content/content/content/pre-register  - https://www.hsstraining.com/content/content/content/content/content/profile  - https://www.hsstraining.com/content/content/content/content/content/requestAnimationFrame  - https://www.hsstraining.com/content/content/content/content/content/scroll  - https://www.hsstraining.com/content/content/content/content/content/training-centre-landing  - https://www.hsstraining.com/content/content/content/content/content/webkit  - https://www.hsstraining.com/content/content/content/content/content/webkitC  - https://www.hsstraining.com/content/content/content/content/credit-account-application  - https://www.hsstraining.com/content/content/content/content/home  - https://www.hsstraining.com/content/content/content/content/keypress  - https://www.hsstraining.com/content/content/content/content/login  - https://www.hsstraining.com/content/content/content/content/pre-register  - https://www.hsstraining.com/content/content/content/content/profile  - https://www.hsstraining.com/content/content/content/content/requestAnimationFrame  - https://www.hsstraining.com/content/content/content/content/scroll  - https://www.hsstraining.com/content/content/content/content/training-centre-landing  - https://www.hsstraining.com/content/content/content/content/webkit  - https://www.hsstraining.com/content/content/content/content/webkitC  - https://www.hsstraining.com/content/content/content/credit-account-application  - https://www.hsstraining.com/content/content/content/home  - https://www.hsstraining.com/content/content/content/keypress  - https://www.hsstraining.com/content/content/content/login  - https://www.hsstraining.com/content/content/content/pre-register  - https://www.hsstraining.com/content/content/content/profile  - https://www.hsstraining.com/content/content/content/requestAnimationFrame  - https://www.hsstraining.com/content/content/content/scroll  - https://www.hsstraining.com/content/content/content/training-centre-landing  - https://www.hsstraining.com/content/content/content/webkit  - https://www.hsstraining.com/content/content/content/webkitC  - https://www.hsstraining.com/content/content/credit-account-application  - https://www.hsstraining.com/content/content/home  - https://www.hsstraining.com/content/content/keypress  - https://www.hsstraining.com/content/content/login  - https://www.hsstraining.com/content/content/pre-register  - https://www.hsstraining.com/content/content/profile  - https://www.hsstraining.com/content/content/requestAnimationFrame  - https://www.hsstraining.com/content/content/scroll  - https://www.hsstraining.com/content/content/training-centre-landing  - https://www.hsstraining.com/content/content/webkit  - https://www.hsstraining.com/content/content/webkitC  - https://www.hsstraining.com/content/credit-account-application  - https://www.hsstraining.com/content/home  - https://www.hsstraining.com/content/keypress  - https://www.hsstraining.com/content/pre-register  - https://www.hsstraining.com/content/profile  - https://www.hsstraining.com/content/requestAnimationFrame  - https://www.hsstraining.com/content/scroll  - https://www.hsstraining.com/content/training-centre-landing  - https://www.hsstraining.com/content/webkit  - https://www.hsstraining.com/content/webkitC  - https://www.hsstraining.com/credit-account-application  - https://www.hsstraining.com/css  - https://www.hsstraining.com/home  - https://www.hsstraining.com/keypress  - https://www.hsstraining.com/login  - https://www.hsstraining.com/manager  - https://www.hsstraining.com/manager/basket  - https://www.hsstraining.com/manager/bst  - https://www.hsstraining.com/manager/bstHist  - https://www.hsstraining.com/manager/c  - https://www.hsstraining.com/manager/click  [Read More..](https://report.portal.procheckup.com/Customers/ResultDetail?name=Missing+HTTP+Response+Headers+&host=www.hsstraining.com&port=443&protocol=TCP&testId=1117)    **Strict Transport Header Setting Missing (CVSS: 4.3)**  **The following results related to target 178.250.102.166 (443/TCP):**  The remote HTTPS server does not send the HTTP  "Strict-Transport-Security" header.  **The following results related to target 185.160.253.20 (443/TCP):**  The remote HTTPS server does not send the HTTP  "Strict-Transport-Security" header.  **The following results related to target www.hss.com (443/TCP):**  The remote HTTPS server does not send the HTTP  "Strict-Transport-Security" header.  **The following results related to target www.hsstraining.com (443/TCP):**  The remote HTTPS server does not send the HTTP  "Strict-Transport-Security" header.  **Affected Hosts:**  **Clickjacking - X-Frame-Options Header Is Not Set (CVSS: 4.3)**   |  | | --- | | 185.160.253.20 | | www.hss.com | | www.hsstraining.com |   **Strict Transport Header Setting Missing (CVSS: 4.3)**   |  | | --- | | 178.250.102.166 | | 185.160.253.20 | | www.hss.com | | www.hsstraining.com |   **Recommendations**  **Content Sniffing Response Header The following response header should be set: X-Content-Type-Options: nosniff**  **A Strict-Transport-Security HTTP header should be sent with each HTTPS response. The syntax is as follows: Strict-Transport-Security: max-age=<seconds>[; includeSubDomains]**  **The parameter max-age gives the time frame for requirement of HTTPS in seconds and should be chosen quite high, e.g. several months. A value below 7776000 is considered as too low by this scanner check. The flag includeSubDomains defines that the policy applies also for sub domains of the sender of the response.**  **XSS Protection Header The following header should be set: X-XSS-Protection: 1; mode=block** |

| **lllll** | **Firewall Detected (CVSS: 0.0)** |
| --- | --- |
| **APP-7** | A packet filtering device protecting this IP was detected. This is likely to be a firewall or a router using access control.   |  | | --- | | **Affected Hosts** | | 178.250.102.166 | | 185.160.253.20 | | www.hss.com | | www.hsstraining.com |   **Recommendations**  **N/A** |

### 5.3 Others

| **lllll** | **Git Repository Served by Web Server (CVSS: 5.0)** |
| --- | --- |
|  | The web server on the remote host allows read access to a Git repository. This potential flaw can be used to download content from the Web server that might otherwise be private.  **Results**  **The following results related to target www.hss.com (443/TCP):**  The following repositories were found on the remote web server :  Repository : https://www.hss.com/blog/.git  Type : Non-Bare  Transport : Plain HTTP   |  | | --- | | **Affected Hosts** | | www.hss.com |   **Recommendations**  **Verify that the listed Git repositories are served intentionally.**  **More information can be found at the following URL(s)**   * **https://blog.skullsecurity.org/2012/using-git-clone-to-get-pwn3d** * **http://www.nessus.org/u?b573eafc** |

# Appendix A- Severity Scale

Vulnerabilities are supplied with corresponding ratings indicating their severity, and these are rated on a scale of one to five using the icons below.

A rating of five means that the vulnerability could enable an attacker to compromise the device, and a rating of one is of low severity.

A more detailed description of the rating system, including examples, can be found in the table below:

|  |  |
| --- | --- |
| **Severity** | **Description** |
| **lllll**  **INFO**  **(CVSS 0)** | Level 1 issues are raised purely for **informational** purposes and do not pose any risks to security.  The reason for their inclusion is to make the customer aware of their presence in case their status was to change.  For example, sensitive entries in a robots.txt file may not be accessible at the time of testing, but may become accessible in the future. |
| **lllll**  **LOW**  **(CVSS 0.1-3.9)** | Level 2 vulnerabilities pose a **low** threat to security. Low threat issues include for example: Leakage of information (such as software versions) which an attacker may find useful; exposure of unnecessary content/functionality; configurations that do not meet best security practice. |
| **lllll**  **MEDIUM**  **(CVSS 4-6.9)** | Level 3 vulnerabilities pose a **medium** threat to security. Medium-risk issues could allow an attacker to gain limited access to system commands or sensitive data.  In addition, vulnerabilities addressed as medium risk when combined with other factors could have a high impact on security if exploited. |
| **lllll**  **HIGH**  **(CVSS 7-9.9)** | Level 4 vulnerabilities pose a **high** threat to security. Issues are raised as high-threat when exploitation could result in a major security breach, such as allowing attackers to gain privileged access, escalate privileges, or to access/modify/remove sensitive information and/or functionality. |
| **lllll**  **CRITICAL**  **(CVSS 10)** | Level 5 vulnerabilities pose a **critical** threat to security. Security issues raised at this level would generally allow an attacker to gain unauthorised access to a system or sensitive data using publicly-available tools and exploits. As an example, if a host was found to be running an unsupported operating system for which exploits were publicly available, this would qualify as a level 5.  If fully exploited such vulnerabilities could have disastrous effects on the business. |

# Appendix B Port Scans

This section of the report details the results of ports scans conducted against all of the targets in scope for this testing.  Full port TCP scans and common port UDP scans were conducted during this test.  Only OPEN and CLOSED ports are shown in this section, filtered ports have been omitted.

## B.1    178.250.102.166

|  |  |  |  |
| --- | --- | --- | --- |
| **PORT** | **PROTOCOL** | **STATUS** | **SERVICE** |
| **80** | **TCP** | **OPEN** | **HTTP** |
| **443** | **TCP** | **OPEN** | **HTTPS** |

## B.1    185.160.253.20

|  |  |  |  |
| --- | --- | --- | --- |
| **PORT** | **PROTOCOL** | **STATUS** | **SERVICE** |
| **80** | **TCP** | **OPEN** | **HTTP** |
| **443** | **TCP** | **OPEN** | **HTTPS** |

## B.1    www.hss.com

|  |  |  |  |
| --- | --- | --- | --- |
| **PORT** | **PROTOCOL** | **STATUS** | **SERVICE** |
| **80** | **TCP** | **OPEN** | **HTTP** |
| **443** | **TCP** | **OPEN** | **HTTPS** |

## B.1    www.hsstraining.com

|  |  |  |  |
| --- | --- | --- | --- |
| **PORT** | **PROTOCOL** | **STATUS** | **SERVICE** |
| **80** | **TCP** | **OPEN** | **HTTP** |
| **443** | **TCP** | **OPEN** | **HTTPS** |

# Appendix C - Supplementary Information

This could contain anything which would bulk out the report unnecessarily, such as a list of missing patches per host, dirbuster output etc.