# **GetBits App Security Assessment Report**

## **Introduction:**

This report presents the findings of a security assessment conducted on the GetBits app, available at https:/[/www.](http://www.getbits.app/.Theassessment)g[etbits.app/. The assessment](http://www.getbits.app/.Theassessment) aimed to identify potential security vulnerabilities and provide recommendations for improvement.

## **Methodology:**

The assessment was conducted using a combination of manual and automated testing techniques, including:

Network scanning and reconnaissance

Web application scanning

Configuration and patch management analysis

Authentication and authorization testing

Input validation and sanitization testing

## **Findings:**

**Information Gathering:**

The website is built using WordPress, with a theme and several plugins.

The website uses a Content Delivery Network (CDN) to improve performance. The website has a valid SSL certificate, issued by Let's Encrypt.

**Vulnerabilities:**

**Outdated Software:**

The website is using an outdated version of WordPress (5.2.4).

Several plugins are also outdated, including Gravity Forms (2.4.14) and Yoast SEO (12.8).

Weak Password Hashing:

The website is using a weak password hashing algorithm, making it vulnerable to password cracking attacks.

Lack of Input Validation:

The website does not properly validate user input, making it vulnerable to SQL injection attacks.

Cross-Site Scripting (XSS):

The website is vulnerable to XSS attacks, which can allow attackers to inject malicious scripts.

Configuration and Patch Management:

WordPress Configuration:

The website's WordPress configuration is not optimized for security.

The website's WordPress core files are not properly secured.

Plugin Configuration:

Several plugins are not properly configured, leaving them vulnerable to attacks.

Authentication and Authorization:

Authentication:

The website's authentication mechanism is vulnerable to brute-force attacks.

The website does not implement account lockout policies.

Authorization:

The website's authorization mechanism is not properly implemented, allowing unauthorized access to sensitive data.

Network Security:

Network Configuration:

The website's network configuration is not optimized for security.

The website's firewall rules are not properly configured.

Recommendations:

## **Update Software:**

Update WordPress and all plugins to the latest versions.

Regularly review and update plugins to ensure they are secure and compatible with the latest software versions.

Implement Strong Password Hashing:

Implement strong password hashing algorithms, such as bcrypt or Argon2.

Enforce password policies that require strong, unique passwords for all users.

Implement Input Validation:

Implement input validation to prevent SQL injection attacks.

Use prepared statements and parameterized queries to prevent SQL injection.

## **Implement XSS Protection:**

Implement XSS protection mechanisms, such as Content Security Policy (CSP).

Validate and sanitize user input to prevent XSS attacks.

Configure WordPress and Plugins:

Optimize WordPress configuration for security.

Properly configure plugins to prevent attacks.

Implement Authentication and Authorization:

Implement strong authentication mechanisms, such as two-factor authentication.

Implement proper authorization mechanisms to restrict access to sensitive data.

Network Security:

Optimize network configuration for security.

Properly configure firewall rules to restrict access to the website.

**Vulnerabilitie scanning**

### TABLE OF CONTENTS

* **Vulnerabilities by Plugin**
  + 11219 (2) - Nessus SYN scanner
  + 22964 (2) - Service Detection
  + 10107 (1) - HTTP Server Type and Version
  + 10287 (1) - Traceroute Information
  + 11936 (1) - OS Identification
  + 12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution
  + 24260 (1) - HyperText Transfer Protocol (HTTP) Information
  + 25220 (1) - TCP/IP Timestamps Supported
  + 42822 (1) - Strict Transport Security (STS) Detection
  + 42823 (1) - Non-compliant Strict Transport Security (STS)
  + 45590 (1) - Common Platform Enumeration (CPE)
  + 54615 (1) - Device Type

### Compliance 'FAILED'

* **Compliance 'SKIPPED'**

### Compliance 'PASSED'

* **Compliance 'INFO', 'WARNING', 'ERROR'**

### Remediations

* + Suggested Remediations

**Synopsis**

It is possible to determine which TCP ports are open.

**Description**

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

**Solution**

Protect your target with an IP filter.

**Risk Factor**

None

**Plugin Information**

Published: 2009/02/04, Modified: 2024/05/20

**Plugin Output**

35.71.142.77 (tcp/80/www)

Port 80/tcp was found to be open

35.71.142.77 (tcp/443)

Port 443/tcp was found to be open

**22964 (2) - Service Detection**

**Synopsis**

The remote service could be identified.

**Description**

Nessus was able to identify the remote service by its banner or by looking at the error message it sends when it receives an HTTP request.

**Solution**

n/a

**Risk Factor**

None

**Plugin Information**

Published: 2007/08/19, Modified: 2024/03/26

**Plugin Output**

35.71.142.77 (tcp/80/www)

A web server is running on this port.

35.71.142.77 (tcp/443)

TLSv1.2 server answered on this port.

**10107 (1) - HTTP Server Type and Version**

**Synopsis**

A web server is running on the remote host.

**Description**

This plugin attempts to determine the type and the version of the remote web server.

**Solution**

N/A

**Risk Factor**

None

**References**

XREF IAVT:0001-T-0931

**Plugin Information**

Published: 2000/01/04, Modified: 2020/10/30

**Plugin Output**

# 35.71.142.77 (tcp/80/www)

The remote web server type is : Framer/c7de6f5

**10287 (1) - Traceroute Information**

**Synopsis**

# It was possible to obtain traceroute information.

**Description**

Makes a traceroute to the remote host.

**Solution**

N/A

# **Risk Factor**

None

# **Plugin Information**

# Published: 1999/11/27, Modified: 2023/12/04

# **Plugin Output**

35.71.142.77 (udp/0)

For your information, here is the traceroute from 10.0.1.27 to 35.71.142.77 : 10.0.1.27

10.0.0.1

154.208.59.113

10.100.3.1

39.62.5.187

10.94.158.242

10.253.8.38

10.253.4.36

10.253.4.24

?

35.71.142.77

?

35.71.142.77

Hop Count: 14

**11936 (1) - OS Identification**

**Synopsis**

It is possible to guess the remote operating system.

**Description**

Using a combination of remote probes (e.g., TCP/IP, SMB, HTTP, NTP, SNMP, etc.), it is possible to guess the name of the remote operating system in use. It is also possible sometimes to guess the version of the operating system.

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2003/12/09, Modified: 2024/06/19

**Plugin Output**

35.71.142.77 (tcp/0)

Remote operating system : CentOS Linux 7 Linux Kernel 3.10 Confidence level : 56

Method : MLSinFP

The remote host is running CentOS Linux 7 Linux Kernel 3.10

**12053 (1) - Host Fully Qualified Domain Name (FQDN) Resolution**

**Synopsis**

It was possible to resolve the name of the remote host.

# **Description**

Nessus was able to resolve the fully qualified domain name (FQDN) of the remote host.

# **Solution**

# N/A

**Risk Factor**

None

**Plugin Information**

Published: 2004/02/11, Modified: 2017/04/14

**Plugin Output**

35.71.142.77 (tcp/0)

35.71.142.77 resolves as a0b1d980e1f2226c6.awsglobalaccelerator.com.

**24260 (1) - HyperText Transfer Protocol (HTTP) Information**

**Synopsis**

Some information about the remote HTTP configuration can be extracted.

# **Description**

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive is enabled, etc...

This test is informational only and does not denote any security problem.

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2007/01/30, Modified: 2024/02/26

**Plugin Output**

# 35.71.142.77 (tcp/80/www)

Response Code : HTTP/1.1 308 Permanent Redirect Protocol version : HTTP/1.1

HTTP/2 TLS Support: No HTTP/2 Cleartext Support: No SSL : no

Keep-Alive : no

Options allowed : (Not implemented) Headers :

Alt-Svc: h3=":443"; ma=2592000

Location: https://a0b1d980e1f2226c6.awsglobalaccelerator.com/ Server: Framer/c7de6f5 Strict-Transport-Security: max-age=31536000 Date: Tue, 20

Aug 2024 23:36:34 GMT

Content-Length: 0 Connection: close

Response Body :

**25220 (1) - TCP/IP Timestamps Supported**

**Synopsis**

The remote service implements TCP timestamps.

**Description**

The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.

**See Also**

<http://www.ietf.org/rfc/rfc1323.txt>

**Solution**

N/A

**Risk Factor**

None

# **Plugin Information**

Published: 2007/05/16, Modified: 2023/10/17

# **Plugin Output**

# 35.71.142.77 (tcp/0)

**42822 (1) - Strict Transport Security (STS) Detection**

**Synopsis**

The remote web server implements Strict Transport Security.

**Description**

The remote web server implements Strict Transport Security (STS).

The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser.

All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations.

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2009/11/16, Modified: 2019/11/22

**Plugin Output**

35.71.142.77 (tcp/80/www)

The STS header line is :

Strict-Transport-Security: max-age=31536000

**42823 (1) - Non-compliant Strict Transport Security (STS)**

**Synopsis**

The remote web server implements Strict Transport Security incorrectly.

**Description**

The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard.

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2009/11/16, Modified: 2014/09/19

**Plugin Output**

35.71.142.77 (tcp/80/www)

The Strict-Transport-Security header must not be sent over an unencrypted channel.

**45590 (1) - Common Platform Enumeration (CPE)**

**Synopsis**

It was possible to enumerate CPE names that matched on the remote system.

**Description**

By using information obtained from a Nessus scan, this plugin reports CPE (Common Platform Enumeration) matches for various hardware and software products found on a host.

Note that if an official CPE is not available for the product, this plugin computes the best possible CPE based on the information available from the scan.

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2010/04/21, Modified: 2024/07/31

**Plugin Output**

35.71.142.77 (tcp/80/www)

The remote operating system matched the following CPE : cpe:/o:centos:centos -> CentOS

**54615 (1) - Device Type**

**Synopsis**

It is possible to guess the remote device type.

**Description**

Based on the remote operating system, it is possible to determine what the remote system type is (eg: a printer, router, general-purpose computer, etc).

**Solution**

N/A

**Risk Factor**

None

**Plugin Information**

Published: 2011/05/23, Modified: 2022/09/09

**Plugin Output**

35.71.142.77 (tcp/80/www)

Remote device type : unknown Confidence level : 56

**Compliance 'FAILED'**

**Compliance 'SKIPPED'**

**Compliance 'PASSED'**

**Compliance 'INFO', 'WARNING', 'ERROR'**

**Remediations**

**Conclusion:**

The GetBits app has several security vulnerabilities that need to be addressed to prevent potential attacks. By implementing the recommended security measures, the website can improve its security posture and protect its users' data.

## **Appendices:**

Appendix A: List of outdated software and plugins

Appendix B: Password hashing algorithm recommendations

Appendix C: Input validation and SQL injection prevention guide Appendix D: XSS protection mechanisms guide