



May 2, 2022

Mr. Jian Zhao  
Vibe, Inc.  
2018 156th Ave NE, Office 165  
Bellevue, WA 98007  
(206) 658-8251  
[zi@vibe.us](mailto:zi@vibe.us)

Dear Mr. Zhao:

Please find enclosed a Web Application Security Audit Penetration Test Report prepared by Altius Information Technologies, Inc. (Altius IT). Our services and scope included a review and assessment of web site applications for security related vulnerabilities. Our assessment was limited to the review period April 28 2022 – May 2, 2022.

This Web Application Security Audit Penetration Test Report identifies the scope of services performed, our findings, alternatives, and Altius IT recommendations. Our review included a high-level examination of various security aspects of your Web Applications including interfaces to databases.

Our scope included the use of vulnerability assessment and penetration testing tools to search for and identify many different types of vulnerabilities that threaten web applications and databases. The Exhibits section of this report includes details on our findings and possible web application vulnerabilities. For your convenience, we have classified the vulnerabilities according to the perceived risk to your organization.

Please contact us if you have any questions regarding this Web Application Security Audit Report.

Sincerely,

Jim Kelton, CISA, CRISC, CGEIT  
Managing Principal

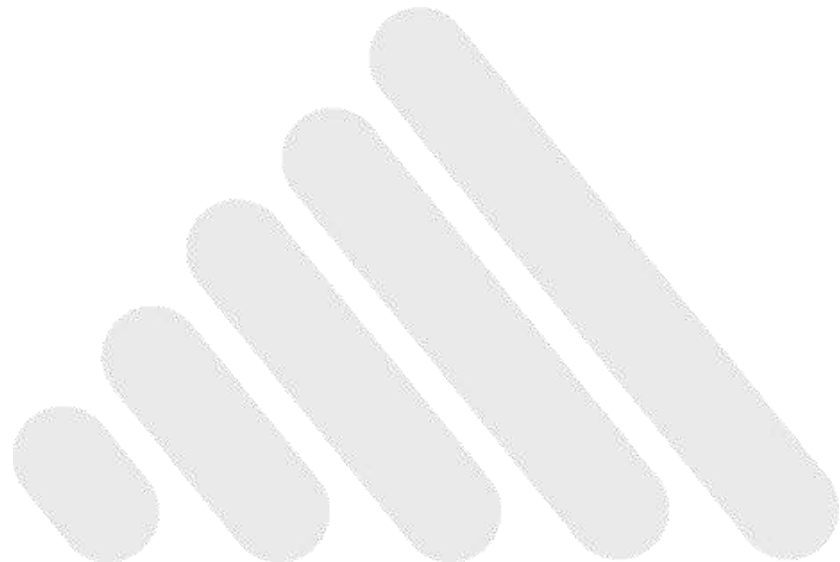


# WEB APPLICATION SECURITY AUDIT PENETRATION TEST REPORT

For

Vibe, Inc.

May 2, 2022



## Table of Contents

I. Executive Summary .....	1
A. Security Audits .....	1
B. Findings and Recommendations .....	1
C. False Positives .....	1
D. Audit Team .....	2
II. Audit Scope .....	3
A. Areas Reviewed .....	3
B. Database Terminology .....	3
C. Security Protection .....	3
D. Audit Process .....	3
E. Areas Excluded .....	4
F. Disclaimer .....	4
III. Common Types of Attacks .....	6
A. Overview of Attacks .....	6
B. SQL Injection Attacks .....	6
C. Cross Site Scripting (XSS) .....	6
D. Authentication Attacks .....	6
E. Authorization Attacks .....	6
F. Client-Side Attacks .....	7
G. Information Disclosure Attacks .....	7
H. Logical Attacks .....	7
I. JavaScript and Ajax Attacks .....	8
IV. Design and Programming Risks .....	9
A. Responsibilities and Practices .....	9
B. User Interaction .....	9
C. Password Management .....	10
D. Software Quality .....	10
E. Auditing and Logging .....	10
F. Sensitive Data Protection .....	11
G. Ensure coding practices .....	12
Exhibits .....	13
Exhibit A – Assessor’s Qualifications and Certifications .....	14
Exhibit B – Potential Web Application Vulnerabilities .....	17

# I. Executive Summary

## **A. SECURITY AUDITS**

Leading organizations use security audits and penetration tests to protect their “information assets”. Altius IT’s process evaluated your security by simulating an attack by an unwanted intruder, malicious employee, partner, or customer. The process involved an active analysis to identify weaknesses, technical flaws, security vulnerabilities, configuration, and compliance issues.

Our service provides insight into various methods of attack against a system or target. Altius IT’s methodology provided a practical demonstration of security by attempting to circumvent those features intended to protect your systems.

## **B. FINDINGS AND RECOMMENDATIONS**

The first part of this report describes the purpose of the evaluation and provides some information on our qualifications and experience. Exhibit B – Potential Security Vulnerabilities provides a prioritized list of findings and recommendations.

Altius IT uses a combination of manual and automated vulnerability assessment and penetration testing tools to identify potential issues. Vulnerabilities and recommendations are grouped into the following major categories according to the risk and impact on your organization:

- High Priority (Red)
- Medium Priority (Orange)
- Low Priority (Yellow)
- Informational (Gray)

For each vulnerability/finding Altius IT’s report provides:

- Description – brief description of the vulnerability
- Vulnerability – information about the issue and how systems might be impacted
- Solution – recommended steps to address the vulnerability/finding
- Details – technical details and additional supporting information

Not all information reviewed by Altius IT is included in the Exhibits and only the information we determined to be relevant is included in the Exhibits.

## **C. FALSE POSITIVES**

Altius IT’s evaluation was performed using a combination of manual and automated tools that look for specific weaknesses, technical flaws and other vulnerabilities.

The speed and cost effectiveness of our services must be balanced against “false positive” results (vulnerabilities that do not exist). Examples of false positives include:

- *Versions* - Where it is not possible to confirm a potential vulnerability without risking a disruption of services (exploiting a flaw that can shut down a system),

vulnerabilities may be flagged on the basis of a software version number rather than the actual error condition. This can lead to false positive results.

- *Configurations* - Altius IT continually improves our tools to eliminate as many false positive issues as possible. However, we also configure our utilities to error on the safe side, by identifying issues that may pose risks to an organization. This process may identify issues that may not be true vulnerabilities or weaknesses. When the assessment is configured stringently enough to be effective, there is a fairly high chance of getting false positives.
- *Knowledge* – In most instances, our services are provided with limited information about your firewalls, routers, server configurations, etc. As a result, we may lack specific knowledge and details about your unique environment. In this case, our findings may result in false positives.

Our findings may include both false positives and false negatives (our service may have missed some vulnerabilities). Use our service as a part of a larger plan to identify and protect systems.

#### **D. AUDIT TEAM**

Altius IT is a California Corporation providing IT security audit and security consulting services. Altius IT helps organizations develop and implement strategies that reduce risks and meet information security and compliance requirements.

Our audit team certifications include Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Controls (CRISC), Certified in the Governance of Enterprise IT (CGEIT), and other related certifications and advanced degrees. For more information on the audit team, please see Exhibit A – Assessor’s Qualifications and Certifications.

## II. Audit Scope

### **A. AREAS REVIEWED**

For many organizations, Web applications are the most vulnerable element of an organization's IT infrastructure. As organizations use the Internet for customer, supplier, employee, and vendor interactions, Web technologies become more complex. If organizations do not secure their web applications, then security risks will only increase.

Altius IT's services included a review of the domain(s) at the time periods listed in our cover letter to this report.

### **B. DATABASE TERMINOLOGY**

A database is a collection of records, or pieces of knowledge. The model in most common use today is the relational model, in which information exists in tables, each consisting of rows and columns (the true definition uses mathematical terminology).

SQL or Structured Query Language is a computer language that allows a programmer to inquire, modify, and delete data stored in a relational database (a collection of tables which organize and store data). SQL is a web application that allows users to interact with the database. Examples of relational databases include Oracle, Microsoft Access, MS SQL Server, MySQL, and Filemaker Pro, all of which use SQL.

### **C. SECURITY PROTECTION**

Since web sites need to be public, security mechanisms must allow public web traffic to communicate with database servers through web applications. As a result, firewalls and similar intrusion detection mechanisms provide little defense against full-scale web attacks.

Patching servers, databases, programming languages and operating systems is critical but is not a replacement for web vulnerability and database assessments.

### **D. AUDIT PROCESS**

By following the links on the web site, and other files such as robots.txt, we inventoried the available web site pages. Our software then mapped out the web site structure and displayed detailed information about each page. We emulated a hacker attack by using vulnerability assessment and penetration testing tools to launch a series of vulnerability attacks on each web site page. Our tools analyzed each page for input data, and subsequently attempted different input combinations in an effort to identify weaknesses.

Altius IT's assessment tools scanned for SQL injection, Cross site scripting, Google hacking, and many other vulnerabilities. As we identified vulnerabilities, Altius IT inventoried and documented information about the vulnerability and recommendations

on how to correct the issue. The Exhibits include a detailed analysis of the types of vulnerabilities encountered.

#### **E. AREAS EXCLUDED**

Our scope included a review of web application security vulnerabilities. Our scope and review were limited:

- Altius IT's services were performed externally. We did not interview personnel or travel to web site data centers. In addition, we did not travel to employees' homes, the offices of third-party service providers, or other locations.
- Altius IT's review was limited in scope to the effectiveness and appropriateness of web application security safeguards related to the security, confidentiality, and integrity of information.
- Software licensing, trade mark infringement, etc. was not included in the project scope.
- Our review was limited to the review period indicated in this Report.

#### **F. DISCLAIMER**

Altius IT's web vulnerability assessment and penetration testing tools analyzed web site applications for many common types of risks associated with attacks on web sites and databases. Our tools are only one means of identifying and managing risks and your organization should augment our findings with other tools and methodologies. In addition, our tools may not have identified all of your web application and database vulnerabilities.

Altius IT did not evaluate business logic flaws such as weaknesses in business processes and code. We did not evaluate the use of negative numbers which, in a transaction, could reverse the flow of money allowing a hacker to siphon money out of an account rather than transfer it into the account.

This report is Confidential and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. If you are not the intended recipient, any use, disclosure, copying or distribution of the report is Unauthorized. If you have received this report in error, please destroy it immediately.

Altius IT's web application security services ("Services") are provided on an "As Is, As Available" basis without any warranty of any kind. By accepting this report, you understand that assessing computer security is highly complex and changeable. Altius IT makes no warranty that the "Services" will find every vulnerability in your Web Application or Web Server(s), or that the solutions suggested and advice provided in this report will be complete or error-free. Altius IT shall be held harmless and free from all liabilities for any use or application of the information provided by Altius IT in connection with using the "Services". You use the "Services" at your own risk. You are solely responsible for any damage to your devices as a result of using the "Services".

**ALTIUS IT MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR**

PURPOSE IN CONNECTION WITH THIS AGREEMENT OR YOUR USE OF ALTIUS  
IT'S SERVICES.



## III. Common Types of Attacks

### **A. OVERVIEW OF ATTACKS**

The Web Application Security Consortium (WASC) is a cooperative effort that clarifies and organizes the threats to the security of a web site. Threats are classified according to the type of risks faced. Major web application threat categories are listed below.

### **B. SQL INJECTION ATTACKS**

SQL Injection is one of the many web attack mechanisms used by hackers to steal data from organizations. It is perhaps one of the most common application layer attack techniques used today. It is the type of attack that takes advantage of improper coding of web applications that allows hacker to inject SQL commands to gain access to the data held within a database. SQL Injection vulnerabilities occur when user input fields allow SQL statements to pass through and query the database directly.

### **C. CROSS SITE SCRIPTING (XSS)**

Cross Site Scripting (also known as XSS or CSS) is generally believed to be one of the most common application layer hacking techniques. Cross site scripting (XSS) is a type of computer security vulnerability typically found in web applications which enable malicious attackers to inject client-side script into web pages viewed by other users. Cross Site Scripting allows an attacker to embed malicious JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable dynamic page to fool the user, executing the script on his machine in order to gather data. The use of CSS might compromise private information, manipulate or steal cookies, create requests that can be mistaken for those of a valid user, or execute malicious code on the end-user system. The data is usually formatted as a hyperlink containing malicious content. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls.

### **D. AUTHENTICATION ATTACKS**

Authentication attacks target a web site's method of validating the identity of a user, service or application. A Brute Force attack is an automated process of trial and error used to guess a person's username, password, credit-card number or cryptographic key. Insufficient Authentication occurs when a web site permits an attacker to access sensitive content or functionality without having to properly authenticate. Weak Password Recovery Validation occurs when a web site permits an attacker to illegally obtain, change or recover another user's password.

### **E. AUTHORIZATION ATTACKS**

Authorization attacks target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action. For example, many web sites should only allow certain users to access specific content or functionality. Other times a user's access to other resources might be restricted. Using various techniques, an attacker can fool a web site into increasing their privileges to protected areas. Credential/Session Prediction is a method of hijacking or

impersonating a web site user. Insufficient Authorization includes threats when a web site permits access to sensitive content or functionality that should require increased access control restrictions. Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorization. Session Fixation is an attack technique that forces a user's session ID to an explicit value.

#### **F. CLIENT-SIDE ATTACKS**

Client-side attacks focus on the abuse or exploitation of a web site's users. When a user visits a web site, trust is established between the two parties both technologically and psychologically. A user expects web sites they visit to deliver valid content. A user also expects the web site not to attack them during their stay. By leveraging these trust relationship expectations, an attacker may employ several techniques to exploit the user. Content Spoofing is an attack technique used to trick a user into believing that certain content appearing on a web site is legitimate and not from an external source.

#### **G. INFORMATION DISCLOSURE ATTACKS**

Information disclosure attacks acquire system specific information about a web site. System specific information includes version numbers and patch levels. Or the information may contain the location of backup files and temporary files. In most cases, divulging this information is not required to fulfill the needs of the user. Most web sites will reveal a certain amount of data, but it's best to limit the amount of data whenever possible. The more information about the web site an attacker learns, the easier the system becomes to compromise. Directory Indexing and automatic directory listing/indexing is a web server function that lists all of the files within a requested directory if the normal base file is not present. Information leakage occurs when a web site reveals sensitive data, such as developer comments or error messages, which may aid an attacker in exploiting the system. Path traversal attacks force access to files, directories, and commands that potentially reside outside the web document root directory. Predictable resource location attack techniques uncover hidden web site content and functionality.

#### **H. LOGICAL ATTACKS**

Logical attacks focus on the abuse or exploitation of a web application's logic flow. Application logic is the expected procedural flow used in order to perform a certain action. Password recovery, account registration, auction bidding, and ecommerce purchases are all examples of application logic. A web site may require a user to correctly perform a specific multi-step process to complete a particular action. An attacker may be able to circumvent or misuse these features to harm a web site and its users. Abuse of Functionality attacks use a web site's own features and functionality to consume, defraud, or circumvents access controls mechanisms. Denial of Service (DoS) attacks prevent a web site from serving normal user activity. Insufficient anti-automation attacks allow a hacker to automate a process that should only be performed manually. Insufficient process validation permits an attacker to bypass or circumvent the intended flow control of an application.

## **I. JAVASCRIPT AND AJAX ATTACKS**

Asynchronous JavaScript Technology and XML (AJAX) provide increased interactivity, speed, and usability. Increased interactivity within a web application means an increase of XML, text, and general HTML network traffic. This leads to exposing back-end applications which might have not been previously vulnerable, or, if there is insufficient server-side protection, giving unauthenticated users the opportunity to manipulate configurations. Since XML HTTP requests use the same HTTP protocol, AJAX-based web applications are vulnerable to the same hacking methodologies as 'normal' applications. As a result, there is an increase in session management vulnerabilities and a greater risk of hackers gaining access to the many hidden URLs which are necessary for AJAX requests to be processed.

## IV. Design and Programming Risks

### **A. RESPONSIBILITIES AND PRACTICES**

Vulnerabilities are classified according to the risks presented to the organization. Some risks may be introduced at the time of initial design while others are created during the programming, implementation, and maintenance phases of a system's lifecycle.

When identifying threats to your assets, your organization must evaluate your risks faced if your code is not kept up-to-date. Your risk management process should include the risks faced, likelihood of the event, and impact on your organization. A risk response action plan will help mitigate and eliminate risks.

### **B. USER INTERACTION**

Pages that accept an ID and password should have this information encrypted both in transit and while stored. The cost of a single site SSL certificate from GoDaddy is reasonably priced at approximately \$10 per year.

Users play an important part in protecting information systems and data. By allowing non-complex passwords, user passwords are easy to crack and data will be vulnerable to attack. To be effective, passwords must be complex and require special characters. In addition, sessions should timeout after a period of inactivity.

It is important to not just strip out risky characters, but also validate input areas. For example, if a dollar amount is entered, ensure that the user can't input a negative number. By allowing negative numbers, the program might actually transfer money out of an account vs. depositing money into an account. The same for quantities, no negative numbers unless it is appropriate.

During the design process certain decisions are made that later result in risks to the client, to the code, and to the software developer's image and reputation. By reviewing decisions made during your design and implementation process, you can identify other areas that create risks.

Programmers should assume that all input is malicious. Use a standard input validation mechanism to validate all input for length, type, syntax, and business rules before accepting the data to be displayed, processed, or stored. Reject any input that does not strictly conform to specifications.

The proper handling of error messages is an important part of programming best practices. When an error occurs, the code should not continue normal execution that would result in incorrect information returned to the client or database. When errors are encountered, SQL Server passes information back to the program and it is up to the program to interpret the message and take the appropriate action.

### **C. PASSWORD MANAGEMENT**

Passwords may be compromised in a number of ways. A common practice is to force users to change their passwords when they log in for the first time. In general, users should be required to change their passwords regularly, at most every 60 days, and preferably more frequently. Users should not reuse old passwords, as they may already have been compromised.

Enforce a password rule that limits the number of password changes that a user may make in any given day. It is important to ensure that users who request a password reset are reliably authenticated. In practice, this means that each user should be required to answer a unique set of questions for authentication, users should be prompted to answer truly personal questions, if possible, users should be asked to answer different, randomly-selected questions every time they must authenticate, users should be able to update their own personal question and answer profiles, and repeated failed attempts to authenticate as a user should trigger a security incident, and lock out the user's account

Programmers should ensure that authentication is performed over a secure encrypted channel such as SSL. Programmers responsible for developing new applications can and should take effective precautions, such as storing passwords using a well-known and trusted hashing algorithm.

### **D. SOFTWARE QUALITY**

In the context of software engineering, software quality measures how well software is designed (quality of design), and how well the software conforms to that design (quality of conformance).

Software testing, when done correctly, can increase overall software quality of conformance by testing that the product conforms to its requirements. Testing includes, but is not limited to, unit and system testing, functional testing, performance testing, failover testing, usability testing, etc.

### **E. AUDITING AND LOGGING**

Many industries are required by legal and regulatory requirements to be well written applications with dual-purpose logs and activity traces for audit and monitoring. The software should make it easy to track a transaction without excessive effort or access to the system. Software should be:

- Auditable. All activities that affect user state or balances are formally tracked.
- Traceable. It's possible to determine where an activity occurs in all tiers of the application
- High integrity. Logs cannot be overwritten or tampered by local or remote users

Ensure that the application has a "safe mode" to which it can return if something truly unexpected occurs. If all else fails, log the user out and close the browser window.

Logs should be written so that the log file attributes are such that only new information can be written (older records cannot be rewritten or deleted). For added security, logs should also be written to a write once / read many device such as a CD-R.

Copies of log files should be made at regular intervals depending on volume and size (daily, weekly, monthly, etc.). A common naming convention should be adopted with regards to logs, making them easier to index. Verification that logging is still actively working is overlooked surprisingly often, and can be accomplished via a simple schedule (cron) job.

## **F. SENSITIVE DATA PROTECTION**

Protection of data includes information availability, confidentiality, and data integrity. Protection must be included during the data lifecycle including data storage and transmission. Sensitive data includes not only user data, but cryptographic keys, passwords, security tokens, and other information that an application relies on for critical decisions.

Stored procedures can be used to help protect against SQL injection errors. It is possible to validate each user input file to scrub the data to protect against Injection. However, input validation can be a single point of failure and sometimes requires a complex set of logic code to determine if the input is OK or bad. Proper coding passing parameters to stored procedures can greatly reduce the threat of SQL Injection in logon screens.

A cookie is used by a web site to store client specific information on a client system. A cookie is simply a file, containing a series of variable-value pairs and linked to a domain. When a client requests a particular domain, the values in the cookie file are read and imported into the server environment, where a developer can read, modify and use them for different purposes. A cookie is a convenient way to carry forward data from one client visit to the next.

Another common approach is to use a session to store connection specific data; this session data is preserved on the server for the duration of the visit, and is destroyed on its conclusion. Sessions work by associating every session with a session ID (a unique identifier for the session) that is automatically generated by PHP. This session ID is stored in two places: on the client using a temporary cookie, and on the server in a flat file or a database. By using the session ID to put a name to every request received, a developer can identify which client initiated which request, and track and maintain client-specific information in session variables (variable-value pairs which remain alive for the duration of the session and which can store textual or numeric information).

A cookie container, "cookieJar", can be shared across multiple domains and requests and manages incoming and outgoing cookie information.

If session IDs are generated in a predictable manner, an attacker could hijack legitimate sessions by guessing the session IDs of authenticated users. In some instances,

cookies are used to track session states. Programmers can minimize risks by ensuring that the cookieJar contains at least 128 bits of random data.

### **G. ENSURE CODING PRACTICES**

Securing web applications is critical in safeguarding an organization's environment and data. Ensure secure coding practices are implemented by developers:

- Safeguard against commonly known web application vulnerabilities (Open Web Application Security Project [http://www.owasp.org/index.php/Main\\_Page](http://www.owasp.org/index.php/Main_Page) is a useful resource.)
- Conduct application source-code reviews
- Independently assess the web application security (contact Altius IT for an annual review or whenever you update your code)

Include security within each phase of the application life cycle:

- Requirements gathering phase—Includes encryption, application privileges and input validation
- Design phase—Includes access controls and auditing
- Implementation phase—Includes security testing and software development
- Installation and configuration—Includes securing custom code, libraries and applicable systems (e.g., web, application, database)
- Implement application-level firewalls to enforce security policies between the web application and the client.

Regularly test the web application

- An application source-code analyzer
- Regularly conduct web application audits to ensure that the software meets current industry standards for securing a web application (contact Altius IT for an annual review or whenever you update your code)

Exhibits

**EXHIBIT A**  
**Assessor's Qualifications and Certifications**



## **EXHIBIT A – ASSESSOR’S QUALIFICATIONS AND CERTIFICATIONS**

### **A. Altius IT**

Altius IT offers a full range of asset protection, security audit, and risk management services. Founded in 1993, Altius Information Technologies, Inc. (Altius IT) is a California Corporation providing IT security audits, security consulting, compliance, and risk management services. Over 1,000 organizations have relied on our expertise to help them develop and implement their strategies to reduce risks.



### **B. Nationally Recognized Leadership**

Elected by our peers into leadership roles, we are experienced information security auditors and have served on the Boards of Directors of international and national associations:

- International Association of Professional Security Consultants
- NetTeCH nationwide association of IT companies
- Association of Professional Consultants
- Technology Professionals Association



### **C. Expert Authority**

As a leading authority, our track record of helping organizations manage risks has been featured on national television and in over 40 publications. Please visit [www.altiusit.com/news.htm](http://www.altiusit.com/news.htm) to view televised clips and articles.



### **D. Project Team Certifications**

Altius, meaning "higher", embodies our philosophy of delivering higher performance and results to our clients. We believe we are uniquely qualified to provide assessment services to your organization. Our project team certifications include *Certified Information Systems Auditor (CISA)*, *Certified in Risk and Information Systems Controls (CRISC)*, and *Certified in the Governance of Enterprise IT (CGEIT)*.





## Mr. Jim Kelton, Managing Principal

Certified Information Systems Auditor (CISA™)  
Certified in Risk and Information Systems Controls (CRISC™)  
Certified in the Governance of Enterprise IT (CGEIT™)

Jim Kelton is a risk management and IT security consultant with 30 years of risk assessment, security management, and technical experience. He serves as Managing Principal of Altius IT, served as a board member of the International Association of Professional Security Consultants (IAPSC), and is past Chairman of the Cybersecurity Special Interest Group (SIG).

### **AREAS OF EXPERTISE**

- IT security audits and assessments
- Risk management, risk treatment, and risk reduction strategies
- Third party system audits
- Security regulations and compliance requirements
- Security best practices

### **ACHIEVEMENT HIGHLIGHTS**

- Certified Information Systems Auditor
- Certified in Risk and Information Systems Controls
- Certified in the Governance of Enterprise IT
- Compliance assessments and protection of information assets and sensitive data
- Featured on *MSNBC* and in over 40 publications including *The Wall Street Journal*, *Business Week*, *USA Today*, *Los Angeles Times*, and others
- Past Chief Information Officer (CIO) of subsidiary of Philip Morris (1979 – 1993)
- Specialist in IT security strategy to deliver sustainable and cost-effective results
- Graduated 1st in class from a Top 5 MIS University (*US News and World Report*)
- Instructor at the University of Arizona (MIS department)

### **RECENT PROFESSIONAL EXPERIENCE (1993 to Present)**

Jim Kelton is Managing Principal of Altius IT, a state-of-the-art IT security assessment and risk management consulting firm dedicated to the advancement of business and IT services. Recently Mr. Kelton has consulted with organizations on security, information asset protection, risk management, and compliance.

Mr. Kelton has created best-in-class practices that deliver sustainable results. He is a Chief Audit Executive and risk management consultant and manages client assessment engagements and educates business managers on ways to manage threats and reduce risks to acceptable levels.

### **EDUCATION**

**U.S. News and Work Report ranked the University of Arizona's MIS program first in the nation and 9<sup>th</sup> globally among all public universities.**

- M.S., University of Arizona, MIS, Graduated *First in Class*
- B.A. University of Arizona, Accounting and Finance



**EXHIBIT B**  
**Potential Web Application Vulnerabilities**

## **EXHIBIT B – POTENTIAL WEB APPLICATION VULNERABILITIES**

### **A. Approach**

Altius IT used a combination of manual and automated vulnerability assessment and penetration testing tools to identify potential web application security vulnerabilities. In some instances, the information reported below may be a “false positive”, not an actual vulnerability. Altius IT recommends that the information below be reviewed with your web site developers and related support staff to determine if the findings listed below are actual vulnerabilities. Please refer to the Assessor’s Comments section of this report for more information on false positives.

### **B. Findings and Potential Vulnerabilities**

This report identifies possible risk areas. When in doubt, Altius IT lists possible vulnerabilities so our clients can make an educated and informed decision. Some of the issues listed below may be required to support web application functionality or business processes. As you review the possible vulnerabilities listed below, you may decide to accept the risk or mitigate and reduce your risks by closing the vulnerabilities.

The following pages identify our findings and recommendations. Vulnerabilities are prioritized according to the risk and impact on your organization. Security risk ratings are based on the Common Vulnerabilities and Exposures (CVE) system which provides a reference method for publicly known information security vulnerabilities and exposures. The U.S. National Cybersecurity Federally Funded Research and Development Center (FFRDC), operated by the Mitre Corporation, maintains the system, with funding from the National Cyber Security Division of the United States Department of Homeland Security. CVE vulnerability data is taken from U.S. National Vulnerability Database (NVD) provided by U.S. National Institute of Standards and Technology (NIST):

- *High Priority* (Red) - issues that allow remote or local access or immediate execution of code or commands with unauthorized privileges. Examples are SQL injection vulnerabilities, most buffer overflows, backdoors, default or no password, and bypassing security controls.
- *Medium Priority* (Orange) - issues that have the potential of granting access or allowing code execution by means of complex or lengthy exploit procedures, or low risk issues applied to major Internet components. Examples are cross-site scripting, man-in-the-middle attacks, denial of service of major applications, and denial of service resulting in system information disclosure (such as core files).
- *Low Priority* (Low) - issues that deny service or provide non-system information that could be used to formulate structured attacks on a target, but not directly gain unauthorized access. Examples are brute force attacks, non-system information disclosure (configurations, paths, etc.), and denial of service attacks.
- *Informational* (Gray) - issues documented in this section are for informational purposes and should be reviewed for relevancy to your organization.

Altius IT’s audit services were not whitelisted. We were not allowed to bypass your Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). The purpose of whitelisting is that it allows an evaluation internal layers of security defenses should

the IDS/IPS be breached or malfunction. A whitelist is a register of those that are provided a particular privilege, service, mobility, access or recognition.

④ Informational	Possible Access Restricted
<b>Description</b>	Altius IT's services were not whitelisted (trusted). As a result, our services may have been restricted by a firewall, Intrusion Detection System (IDS), or Intrusion Prevention System (IPS).
<b>Vulnerability</b>	<p>Altius IT's analysis of your application and web server may have been restricted by one of more of the following security mechanisms:</p> <ul style="list-style-type: none"> <li>• Firewall – a network security system that controls the incoming and outgoing network traffic based on a defined set of rules. A firewall establishes a barrier between a trusted secure internal network and another network (e.g., the Internet) that is assumed not to be secure and trusted.</li> <li>• Intrusion Detection System (IDS) – a device or application that monitors network or systems for malicious activities or policy violations. Produces reports for subsequent analysis and action. Variations of IDS systems include Network based (NIDS) and host based (HIDS) intrusion detection systems. Intrusion detection systems are primarily focused on identifying possible incidents, logging, and reporting.</li> <li>• Intrusion Prevention System (IPS) – IPS systems are typically an intrusion detection and prevention systems (IDPS) that monitors network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about the activity, attempt to block or stop the activity, and report the activity.</li> </ul>
<b>Solution</b>	<p>Ensure internal layers of security protection are implemented to protect public facing applications. Internal layers of security can include:</p> <ul style="list-style-type: none"> <li>• Access control systems.</li> <li>• Formal approach to patch management.</li> <li>• Anti-malware Policy and up-to-date protection.</li> <li>• Network segmentation.</li> <li>• Logging and monitoring systems.</li> <li>• Backup Policy and Backup Plan.</li> <li>• Incident Response Policy and Incident Response Plan.</li> <li>• Role based security training.</li> </ul>
<b>Details</b>	Access to the application and web server may have been restricted

④ Informational	Risk Management – Service Providers
<b>Description</b>	Ensure risk management processes are in place to treat risks related to third-party service providers that host network and web environments.
<b>Vulnerability</b>	Formal processes are needed to identify threats, vulnerabilities, potential impact, and the likelihood of an event.
<b>Solution</b>	<p>Ensure a formal security risk management process is in place that includes third-party service provider:</p> <ul style="list-style-type: none"> <li>• Risk assessment – identify assets, specific security threats to the assets, and vulnerabilities that exist as a result of each threat.</li> <li>• Risk analysis – identify likelihood and impact of each event on the organization. Identify preventive, detective, and corrective controls that reduce risks to acceptable levels.</li> <li>• Risk treatment – document prioritized safeguards to be implemented, assigned responsibility, and dates.</li> </ul> <p>Ensure the risk management program is reviewed and updated on a regular basis per organization policy.</p>
<b>Details</b>	Ensure risk treatment identifies how each third-party service provider risk is to be addressed with preventive, detective, and corrective controls. Residual risk is the risk left over after implementing risk treatment steps that avoid the risk, transfer the risk, reduce the risk, or accept the risk.




# VIBE.US


13.32.145.42 (server-13-32-145-42.cdg50.r.cloudfront.net)

13.32.145.69 (server-13-32-145-69.cdg50.r.cloudfront.net)


13.32.145.88 (server-13-32-145-88.cdg50.r.cloudfront.net)


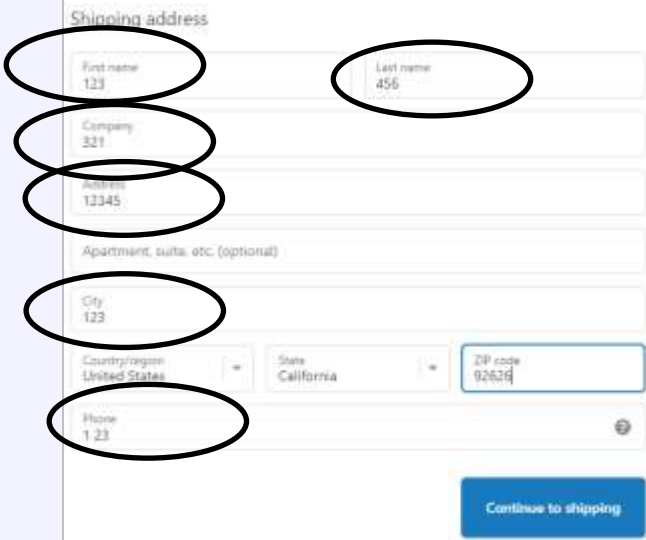
13.32.145.35 (server-13-32-145-35.cdg50.r.cloudfront.net)

	<b>Insufficient Testing</b>
<b>Description</b>	Applications and changes to applications should be properly configured and thoroughly tested before being placed in a production environment.
<b>Vulnerability</b>	Without sufficient testing, applications may not provide services that meet agreed upon requirements. Users may get frustrated and abandon the application.
<b>Solution</b>	Applications should be tested in a quality control environment on a variety of browsers and with varying inputs and assumptions.  See the Open Web Application Security Project (OWASP) Web Security Testing Guide version 4.2 for more information.
<b>Details</b>	<p>Examples are listed below. Ensure all pages are fully tested with appropriate action taken.</p> <p><a href="https://vibe.us/">https://vibe.us/</a></p> <ul style="list-style-type: none"> <li>✖ Failed to execute 'postMessage' on 'DOMWindow': The <code>www-widgetapi.js:969</code> target origin provided ('<a href="https://www.youtube.com/">https://www.youtube.com/</a>') does not match the recipient window's origin ('<a href="https://vibe.us/">https://vibe.us/</a>').</li> <li>[D]: Consent granted. <span style="float: right;">(index):1786</span></li> <li>[D]: Load google tag manager. <span style="float: right;">(index):1786</span></li> <li>[D]: Observer disconnected. <span style="float: right;">(index):1786</span></li> <li>✖ Access to XMLHttpRequest at '<a href="https://googleads.g.doubleclick.net/pagead/viewthroughconversion/962985656/...0YmXj2A&amp;label=followon_view&amp;pptype=no_rmkt&amp;random=264352104&amp;cv attributed=0">https://googleads.g.doubleclick.net/pagead/viewthroughconversion/962985656/...0YmXj2A&amp;label=followon_view&amp;pptype=no_rmkt&amp;random=264352104&amp;cv attributed=0</a>' (redirected from '<a href="https://www.youtube.com/pagead/viewthroughconversion/962985656/?backend=inn...=5dzw8og61IwH12b0YmXj2A&amp;label=followon_view&amp;pptype=no_rmkt&amp;random=264352104">https://www.youtube.com/pagead/viewthroughconversion/962985656/?backend=inn...=5dzw8og61IwH12b0YmXj2A&amp;label=followon_view&amp;pptype=no_rmkt&amp;random=264352104</a>') from origin '<a href="https://www.youtube.com/">https://www.youtube.com/</a>' has been blocked by CORS policy: No 'Access-Control-Allow-Origin' header is present on the requested resource.</li> <li>✖ Failed to load resource: <code>googleads.g.doublecl...4&amp;cv attributed=0:1</code>  <span style="float: right;">net::ERR_FAILED</span></li> <li>✖ The service worker navigation preload request was cancelled before 'preloadResponse' settled. If you intend to use 'preloadResponse', use <code>waitUntil()</code> or <code>respondWith()</code> to wait for the promise to settle.</li> <li>✖ Failed to load resource: the <code>tag.vibe.us/g/collec...&amp;ep.visible=false:1</code>  <span style="float: right;">server responded with a status of 502 ()</span></li> </ul> <p><a href="https://app.vibe.us/login">https://app.vibe.us/login</a></p> <ul style="list-style-type: none"> <li>⚠ DevTools failed to load source map: Could not load content for <code>https://app.vibe.us/static/css/main.4eb82499.chunk.css.map</code>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE</li> <li>⚠ DevTools failed to load source map: Could not load content for <code>https://app.vibe.us/static/css/1.91536f27.chunk.css.map</code>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE</li> </ul> <p><a href="https://vibe.us/customer/">https://vibe.us/customer/</a></p> <ul style="list-style-type: none"> <li>⚠ DevTools failed to load source map: Could not load content for <code>https://vibe.us/is/common/ads.min.js.map</code>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE</li> </ul>

	<b>Transport Layer Security</b>
<b>Description</b>	The device does not support connections using a newer version of Transport Layer Security (TLSv1.3) encryption.
<b>Vulnerability</b>	<p>TLS 1.3 was defined in RFC 8446 in August 2018. It is based on the earlier TLS 1.2 specification. Some functional differences between</p> <p>TLS 1.2 and TLS 1.3:</p> <ul style="list-style-type: none"> <li>• The list of supported symmetric encryption algorithms has been pruned of all algorithms that are considered legacy.</li> <li>• Static RSA and Diffie-Hellman cipher suites have been removed; all public-key based key exchange mechanisms now provide forward secrecy.</li> <li>• All handshake messages after the ServerHello are now encrypted.</li> <li>• The key derivation functions have been redesigned.</li> </ul>
<b>Solution</b>	Ensure systems and applications also support TLSV1.3.
<b>Details</b>	<p style="color: #4F81BD; font-size: 1.2em;">Protocol Support</p> <p>TLSv1.2</p>



	<b>Privacy Policy – Not Updated</b>
<b>Description</b>	Privacy Policy not reviewed and updated within the past 12 months.
<b>Vulnerability</b>	Violating regulations and laws can result in fines and penalties.
<b>Solution</b>	Ensure the Privacy Policy is reviewed and updated on an annual basis. A full review of the Privacy Policy is beyond the scope of a security audit. Contact Altius IT for information on our Privacy Audit services.
<b>Details</b>	<p>The privacy policy does not state the date of the most recent update. User adds item to Cart, clicks Checkout, user selects Privacy Policy at bottom of page  <a href="https://order.vibe.us/14495744064/checkouts/56ef641444af8958fcae7cfd7e26eef9">https://order.vibe.us/14495744064/checkouts/56ef641444af8958fcae7cfd7e26eef9</a></p> <p>No date listed for most recent update</p> <h2 style="text-align: center;">Privacy policy</h2> <hr/> <p>This Privacy Policy describes how your personal information is used when you make a purchase from order.vibe.us (the “Site”).</p> <h3>PERSONAL INFORMATION WE COLLECT</h3> <p>When you visit the Site, we automatically collect certain information about your web browser, IP address, time zone, and so on. Additionally, as you browse the Site, we collect information about the pages you view, what websites or search terms referred you to the Site. We refer to this automatically-collected information as “Usage Data.”</p>

	<b>Improper Input Validation</b>
<b>Description</b>	The application does not appear to properly validate input.
<b>Vulnerability</b>	Failure to properly validate input can result in errors during processing of the information. Failure to properly validate input can let hackers know that the application has weak validation routines. This may encourage hackers to spend additional time trying to find other weak areas in the application that can lead to higher level attacks and compromise of systems.
<b>Solution</b>	<p>Assume that all input is malicious. Ensure that all fields are properly validated according to their data type, field length, ranges, and use. Ensure appropriate error messages are produced.</p> <p>The Open Web Application Security Project (OWASP) aims to raise awareness about application security by identifying some of the most critical risks facing organizations. The most common web application security weakness is the failure to properly validate input from the client or environment. Ensure that the application is robust against all forms of input data, whether obtained from the user, infrastructure, external entities or database systems. Data from the client should never be trusted for the client has every possibility to tamper with the data.</p> <ul style="list-style-type: none"> <li>• Integrity checks: Ensure that the data has not been tampered with and is the same as before.</li> <li>• Validation: Ensure that the data is strongly typed, correct syntax, within length boundaries, contains only permitted characters, or that numbers are correctly signed and within range boundaries.</li> <li>• Business rules: Ensure that data is not only validated, but business rule correct. For example, amounts fall within permitted boundaries.</li> </ul> <p>For more information see:</p> <ul style="list-style-type: none"> <li>• <a href="https://www.owasp.org/index.php/Data_Validation">https://www.owasp.org/index.php/Data_Validation</a></li> <li>• <a href="https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html">https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html</a></li> </ul>
<b>Details</b>	<p>Below are examples of input validation needed. Altius IT did not test/evaluate every input field. Altius IT recommends that client perform quality control testing to ensure all fields have proper input validation.</p> <p><a href="https://vibe.us/order/us-sales/">https://vibe.us/order/us-sales/</a>  <a href="https://order.vibe.us/14495744064/checkouts/56ef641444af8958fcae7cfd7e26eef9">https://order.vibe.us/14495744064/checkouts/56ef641444af8958fcae7cfd7e26eef9</a></p>  <p>Invalid order accepted</p>

	Information > Shipping > Payment	
	Contact	123@123.com <a href="#">Change</a>
	Ship to	321, 12345, 123 CA 92626, United States <a href="#">Change</a>

<b>④ Informational</b>	<b>No Vulnerabilities Identified – wss://wss.vibe.us</b>
<b>Description</b>	At the time of our review Altius IT did not identify vulnerabilities on this application.
<b>Vulnerability</b>	Threats must be managed using a formal approach to protect your systems. Ad-hoc approaches to security can give you a false sense of security and leave your systems vulnerable to an attack.
<b>Solution</b>	<p>Altius IT makes the following recommendations:</p> <ul style="list-style-type: none"> <li>• Prepare and implement formal policies, procedures, and plans to identify and manage network and software vulnerabilities.</li> <li>• Monitor security alerts. Subscribe to vulnerability monitoring services that issue notifications when vulnerabilities are discovered in networks, applications, scripting languages, operating systems, etc.</li> <li>• Management. Ensure networks and applications are patched in a timely manner. Security best practices specify that high priority networks and applications be patched within 30 calendar days of notice of important security vulnerability.</li> <li>• Audit. Ensure systems are audited on an annual basis. Audits should be performed more frequently if major changes occur.</li> </ul>
<b>Details</b>	For more information, see: National Institute of Standards and Technology (NIST) Special Publication 800-40 Guide to Enterprise Patch Management Technologies.


# APP.VIBE.US











52.222.158.90 (server-52-222-158-90.cdg52.r.cloudfront.net)


52.222.158.59 (server-52-222-158-59.cdg52.r.cloudfront.net)


52.222.158.78 (server-52-222-158-78.cdg52.r.cloudfront.net)


52.222.158.3 (server-52-222-158-3.cdg52.r.cloudfront.net)

 <b>Low</b>	<b>Change Management - Lodash</b>
<b>Description</b>	The server operating system and related applications should be patched on a regular basis.
<b>Vulnerability</b>	Hackers can exploit vulnerabilities in unpatched software.
<b>Solution</b>	Ensure you are running the most current version of the operating system and applications and they are fully patched and up-to-date.  Ensure a formal patch management policy and related procedures exist.  Upgrade to version 4.17.21 issued February 20, 2021. More information is available <a href="https://en.wikipedia.org/wiki/Lodash">https://en.wikipedia.org/wiki/Lodash</a> .
<b>Details</b>	Lodash Without direct access to the device, Altius IT could not fully confirm the installed version of Lodash. The device appears to be running an older version with known vulnerabilities <b>Lodash</b> <b>4.17.20</b>  Lodash versions prior to 4.17.21 are vulnerable to Command Injection attacks.  Lodash versions prior to 4.17.21 are vulnerable to Regular Expression Denial of Service (ReDoS) via the toNumber, trim and trimEnd functions.

	<b>Insufficient Testing</b>
<b>Description</b>	Applications and changes to applications should be properly configured and thoroughly tested before being placed in a production environment.
<b>Vulnerability</b>	Without sufficient testing, applications may not provide services that meet agreed upon requirements. Users may get frustrated and abandon the application.
<b>Solution</b>	Applications should be tested in a quality control environment on a variety of browsers and with varying inputs and assumptions.  See the Open Web Application Security Project (OWASP) Web Security Testing Guide version 4.2 for more information.
<b>Details</b>	<p>Examples are listed below. Ensure all pages are fully tested with appropriate action taken.</p> <p>User signs in  <a href="https://app.vibe.us/smart.RECENT/InQAPbYYPQaYI3ihaamDbg/jquwakDrh3EdAcWCbi5iO1">https://app.vibe.us/smart.RECENT/InQAPbYYPQaYI3ihaamDbg/jquwakDrh3EdAcWCbi5iO1</a></p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/s_tatic/js/4.10fec231.chunk.js.map">https://app.vibe.us/s_tatic/js/4.10fec231.chunk.js.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/s_tatic/js/8.d555abbd.chunk.js.map">https://app.vibe.us/s_tatic/js/8.d555abbd.chunk.js.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/s_tatic/css/2.a1596f27.chunk.css.map">https://app.vibe.us/s_tatic/css/2.a1596f27.chunk.css.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/s_tatic/css/main.aeb92499.chunk.css.map">https://app.vibe.us/s_tatic/css/main.aeb92499.chunk.css.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/s_tatic/js/3.485ca611.chunk.js.map">https://app.vibe.us/s_tatic/js/3.485ca611.chunk.js.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p> <a href="https://app.vibe.us/login?board_id=BFUNCcLHNQt-c41iUyPbjB&amp;from=%2Fsmart.PRIVATE_BOARDS%2FBFUNCcLHNQt-c41iUyPbjB%2Fc2Ur4_kA_ovcxdBvvm1006">https://app.vibe.us/login?board_id=BFUNCcLHNQt-c41iUyPbjB&amp;from=%2Fsmart.PRIVATE_BOARDS%2FBFUNCcLHNQt-c41iUyPbjB%2Fc2Ur4_kA_ovcxdBvvm1006</a> (user chooses Flowchart)         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/stat_ic/css/main.aeb92499.chunk.css.map">https://app.vibe.us/stat_ic/css/main.aeb92499.chunk.css.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/stat_ic/css/2.a1596f27.chunk.css.map">https://app.vibe.us/stat_ic/css/2.a1596f27.chunk.css.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p> <a href="https://app.vibe.us/smart.RECENT/qoFyi80N7Ft-g8ugB49aS9/qIn9BVBqc-Opigibe-TBqu">https://app.vibe.us/smart.RECENT/qoFyi80N7Ft-g8ugB49aS9/qIn9BVBqc-Opigibe-TBqu</a> </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/stat_ic/css/main.aeb92499.chunk.css.map">https://app.vibe.us/stat_ic/css/main.aeb92499.chunk.css.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p> <p>  DevTools failed to load source map: Could not load content for <a href="https://app.vibe.us/stat_ic/css/2.a1596f27.chunk.css.map">https://app.vibe.us/stat_ic/css/2.a1596f27.chunk.css.map</a>: HTTP error: status code 404, net::ERR_HTTP_RESPONSE_CODE_FAILURE         </p>

	<b>Transport Layer Security</b>
<b>Description</b>	The device does not support connections using a newer version of Transport Layer Security (TLSv1.3) encryption.
<b>Vulnerability</b>	<p>TLS 1.3 was defined in RFC 8446 in August 2018. It is based on the earlier TLS 1.2 specification. Some functional differences between</p> <p>TLS 1.2 and TLS 1.3:</p> <ul style="list-style-type: none"> <li>• The list of supported symmetric encryption algorithms has been pruned of all algorithms that are considered legacy.</li> <li>• Static RSA and Diffie-Hellman cipher suites have been removed; all public-key based key exchange mechanisms now provide forward secrecy.</li> <li>• All handshake messages after the ServerHello are now encrypted.</li> <li>• The key derivation functions have been redesigned.</li> </ul>
<b>Solution</b>	Ensure systems and applications also support TLSV1.3.
<b>Details</b>	<p style="color: #4f81bd; font-size: 1.2em;">Protocol Support</p> <p>TLSv1.2</p>

	<b>Missing Security Header – X-Frame-Options</b>
<b>Description</b>	The application may be vulnerable to a Clickjacking attack.
<b>Vulnerability</b>	<p>When the X-Frame-Options header is not sent by the server, an attacker may be able to embed this website into an iframe of a third party website. By manipulating the display attributes of the iframe, the attacker could trick the user into performing mouse clicks in the application, thus performing activities without user consent (ex: delete user, subscribe to newsletter, etc). More information is available:</p> <p><a href="https://owasp.org/www-community/attacks/Clickjacking">https://owasp.org/www-community/attacks/Clickjacking</a></p>
<b>Solution</b>	Add the X-Frame-Options HTTP header with the values DENY or SAMEORIGIN to every page that you want to be protected against Clickjacking attacks.
<b>Details</b>	<p>Response headers do not include the HTTP X-Frame-Options security header.</p> <p>HTTP Security Header: X-Frame-Options  Header Role: Mitigates Clickjacking attacks  Status: Not set</p>

	<b>Missing Security Header - Content Security Policy</b>
<b>Description</b>	Web applications are vulnerable to a wide range of attacks including cross site scripting.
<b>Vulnerability</b>	The HTTP Content-Security-Policy response header allows the web page to control resources the user is allowed to load on a page. Specifying server origins and script endpoints can help guard against cross site scripting attacks (XSS).
<b>Solution</b>	Review and implement additional cross site scripting controls including Content-Security-Policy  For more information see <a href="https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy">https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy</a>
<b>Details</b>	Response headers do not include the HTTP Content-Security-Policy security header.  HTTP Security Header: Content-Security-Policy Header Role: Mitigates Cross-Site Scripting (XSS) attacks Status: Not set