**Vulnerability Assessment and Penetration Testing**

**A Minor Project Report Submitted to**



**Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal**

**Towards Partial Fulfillment for the Award of**

**Bachelor of Technology**

**(Computer Science and Engineering)**

**Submitted By:**

**Siddharth Jain(0827CS171211)**

**Shubham Malviya(0827CS171208)**

**Siddharth Choudhary (0827CS171210)**

**CS4 III YEAR**

**Supervised By: Guided by:**

**Mr. Ritesh Khedekar Mrs. Vandana Kate**

**Ms. Nupur Agrawal**

****

**Department of Computer Science and Engineering**

**Acropolis Institute of Technology and Research, Indore**

**July - Dec 2019**

Table of Contents

[Executive Summary 2](#_bookmark0)

[Project Vision 3](#_bookmark1)

[Project Purpose 4](#_bookmark2)

[Problem / Opportunity 4](#_bookmark3)

[Project Description 4](#_bookmark4)

[Current Situation 5](#_bookmark5)

[Key Stakeholders 5](#_bookmark6)

[Project Scope 6](#_bookmark7)

[Scope 6](#_bookmark8)

[Out of Scope 7](#_bookmark9)

[Project Objectives 8](#_bookmark10)

[Terminology 9](#_bookmark11)

[Project Team 10](#_bookmark12)

[Project Stakeholders 11](#_bookmark13)

[Risk Assessment 12](#_bookmark14)

[Project Schedule 13](#_bookmark15)

[Project Facilities and Resources 14](#_bookmark16)

[Project Budget 15](#_bookmark17)

[Equipment and Facilities 15](#_bookmark18)

[Operating Costs 16](#_bookmark19)

[Promotion and Communication 17](#_bookmark20)

[Intellectual Property 18](#_bookmark21)

[Offer and Approvals 19](#_bookmark22)

[Offer 19](#_bookmark23)

[Approvals 19](#_bookmark24)

[Project Charter Signoff 19](#_bookmark25)

[References 20](#_bookmark26)

[Bibliography 20](#_bookmark27)

|  |  |
| --- | --- |
| Section  1 |  |
| Executive Summary |
|  |  |

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately. A vulnerability assessment process that is intended to identify threats and the risks they pose typically involves the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a web application firewall (WAF). Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.

# Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone. Using the Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a more detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks. Vulnerabilities can be found in applications from third-party vendors and internally made software, but most of these flaws are easily fixed once found. Using a VAPT provider enables IT security teams to focus on mitigating critical vulnerabilities while the VAPT provider continues to discover and classify vulnerabilities.

# A penetration test, or pen-test, is an attempt to evaluate the security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities may exist in operating systems, services and application flaws, improper configurations or risky end-user behavior. Such assessments are also useful in validating the efficacy of defensive mechanisms, as well as, end-user adherence to security policies. In this we will do penetration testing on website and patch their vulnerability. To make website secure.

|  |  |
| --- | --- |
| Section  2 |  |
| Project Vision |
|  |  |

This is to conclude that the project that we undertook was worked upon with a sincere effort. Most of the requirements have been fulfilled up to the mark and the requirements which have been remaining, can be completed with a short extension. This project would definitely satisfy all the requirements of the college and would be beneficial for the students and the college staff. We find the vulnerabilities in the website of successfully with the help of above tools and it is very interesting to hack into the website and make report of it.

As we update in this world of internet, new technology are introduced. So, there is large possibility of vulnerability and with the help of debugging or penetration testing. We can assist the vulnerability

and secure the future.

|  |  |
| --- | --- |
| Section  3 |  |
| Project Purpose |
|  |  |

# Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone.

# Using the Vulnerability Assessment and Penetration Testing (VAPT) approach gives an organization a more detailed view of the threats facing its applications, enabling the business to better protect its systems and data from malicious attacks.

# Vulnerabilities can be found in applications from third-party vendors and internally made software, but most of these flaws are easily fixed once found. Using a VAPT provider enables IT security teams to focus on mitigating critical vulnerabilities while the VAPT provider continues to discover and classify vulnerabilities.

# Problem / Opportunity

Now, a day we can see Cyber crime increasing day by day. So it is necessary to secure the website site from following attacks, towards user or organization:

* **Keep Software update:** When website security holes are found in software, hackers are quick to attempt to abuse them.
* **SQL injection:** SQL injection attacks are when an attacker uses a web form field or URL parameter to gain access to or manipulate your database.
* **Protect against XSS attacks:** Cross-site scripting (XSS) attacks inject malicious JavaScript into your pages.
* **Beware of error and message:** Be careful with how much information you give away in your error messages.
* **Use HTTPS:** HTTPS is a protocol used to provide security over the Internet.
* **Payment Gateway:** With the help of cookies, session, tampering payment gateway can be bypass easily.

# 

# Project Description

A vulnerability assessment is the process of defining, identifying, classifying and prioritizing vulnerabilities in computer systems, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threats to its environment and react appropriately.A vulnerability assessment process that is intended to identify threats and the risks they pose typically involves the use of automated testing tools, such as [network security scanners](https://searchsecurity.techtarget.com/definition/vulnerability-scanning), whose results are listed in a vulnerability assessment report.Organizations of any size, or even individuals who face an increased risk of cyberattacks, can benefit from some form of vulnerability assessment, but large enterprises and other types of organizations that are subject to ongoing attacks will benefit most from vulnerability analysis. Because security [vulnerabilities](https://whatis.techtarget.com/definition/vulnerability) can enable hackers to access IT systems and applications, it is essential for enterprises to identify and remediate weaknesses before they can be exploited. A comprehensive vulnerability assessment along with a management program can help companies improve the security of their systems.

# Current Situation

security [vulnerabilities](https://whatis.techtarget.com/definition/vulnerability) can enable hackers to access IT systems and applications, it is essential for enterprises to identify and remediate weaknesses before they can be exploited. A comprehensive vulnerability assessment along with a management program can help companies improve the security of their systems.

A penetration test, also known as a pen test, is a simulated cyber-attack against your computer system to check for exploitable vulnerabilities. In the context of web application security, penetration testing is commonly used to augment a [web application firewall (WAF)](https://www.imperva.com/products/web-application-firewall-waf/).Pen testing can involve the attempted breaching of any number of application systems, (e.g., application protocol interfaces (APIs), frontend/backend servers) to uncover vulnerabilities, such as unsanitized inputs that are susceptible to code injection attacks.Insights provided by the penetration test can be used to fine-tune your WAF security policies and patch detected vulnerabilities.

# Key Stakeholders

The following table outlines key stakeholders associated with this project.

|  |  |
| --- | --- |
| **Stakeholders** | **Comment** |
| Project Managers | Adam Elliott, Taylor Kinsella, Matthew Lillywhite, Christopher McNeil |
| Client | Colin Chamberlain, Jason Fischer |
| Performing Organization | Vulnerability Assessment and Penetration Testing |
| Sponsor | Colin Chamberlain, Jason Fischer |

|  |  |
| --- | --- |
| Section  4 |  |
| Project Scope |
|  |  |

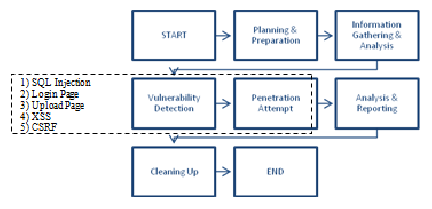
This section of the project charter specifically outlines major activities to be undertaken and their associated deliverables. It also describes the projects’ out of scope activities, which will be specifically excluded from the project’s final deliverable.

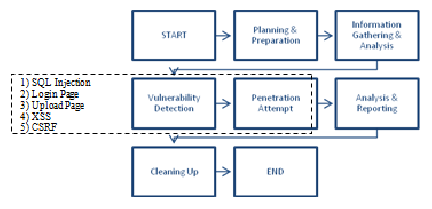
The overall target of this project is public Calgary transit clients/customers, and resolving the inaccuracy/reliability of transit scheduling services to provide a greater quality of service to Calgarians. This will be done by simulating an environment with prototype devices which could potentially be used to solve transit tracking inefficiency.

Although the main target may be public transit, there is no reason this project could not be implemented elsewhere (i.e. taxi services, delivery services, etc.). Anything can be tracked at a certain point in time using this GPS system, from small to enterprise level environments.

# Scope

The intended users can organization which hosts the website or the user both need to be secure.



****

# Out of Scope

* To perform Penetration testing it is necessary to take legal permission from the organization or website owner.
* It is necessary to have software and particular OS for the Penetration testing.
* Penetration testing requires expensive software’s and professional skills.

|  |  |
| --- | --- |
| Section  5 |  |
| Project Objectives |
|  |  |

**Assessment**The two main objectives of this phase are the planning and execution of the vulnerability assessment. Planning includes information gathering; defining activity scope, roles and responsibilities; and informing the relevant personnel of the process. Execution includes interviewing system administrators, reviewing IT security policies, and scanning of security vulnerabilities.

**Identify Exposures**This phase include a variety of tasks that is performed to the specifications and needs of your organisation. Generally, it includes the review of results from the previous phase and identification of remedy actions for the vulnerabilities.

**Address Exposures**An investigation needs to be carried out to determine if the vulnerable services are required. If the affected services are not essential, they should be disabled. Required services with security weakness must be patched or rectified, and the management needs to be informed of un-patched vulnerabilities and residual risks.

**Planning & Preparation**Before commencing the penetration test, there is a need to set clear objectives and scope. A penetration test plan with details on time, duration and potential impact to business operations needs to be defined and communicated to all stakeholders and affected staff. A formal and approved test plan also serves to absolve the penetration testers of legal liabilities, as most tests are likely to be against the law.

**Information Gathering and Analysis**The next step is to determine the reachable systems in the IT infrastructure, which would form the list of investigation targets in the vulnerability assessment. This could be done through a network survey to determine domain names, server names, Internet service provider information, IP addresses of hosts and a network map. A useful tool to conduct network survey would be Nmap (http://www.nmap.org), which would provide a comprehensive network analysis of the IT infrastructure.

**Vulnerability Detection**To begin with the penetration attempts, penetration testers need to have a collection of exploits and vulnerabilities. Automated tools such as Nessus may be used to detect the presence of vulnerabilities.

**Penetration Attempt**After determining a collection of vulnerabilities that exist within the system, penetration testers would identify suitable targets to begin an intrusive attack to test the system’s defences. The time and effort to conduct the penetration tests on the system should be estimated. Comprehensive penetration testing would involve tests such as password cracking, network exploitation, social engineering and even physical security testing.

**Reporting and Clean Up**Finally, a report summarising the penetration testing process, analysis and commentary of vulnerabilities identified would be submitted. Critical vulnerabilities identified should be addressed immediately to the overseeing management. The last step is to clean up the systems, to remove traces of data such as user accounts that was created during the penetration testing. This should be verified by organisation’s staff to ensure that it has been done successfully. The cleaning up of compromised hosts must also be done securely such that the organisation’s normal operations are not affected.

|  |  |
| --- | --- |
| Section  6 |  |
| Terminology |
|  |  |

The following terminology is used within this document and may require additional explanation:

* **Keep Software update:** When website security holes are found in software, hackers are quick to attempt to abuse them.
* **SQL injection:** SQL injection attacks are when an attacker uses a web form field or URL parameter to gain access to or manipulate your database.
* **Protect against XSS attacks:** Cross-site scripting (XSS) attacks inject malicious JavaScript into your pages.
* **Beware of error and message:** Be careful with how much information you give away in your error messages.
* **Use HTTPS:** HTTPS is a protocol used to provide security over the Internet.
* **Payment Gateway:** With the help of cookies, session, tampering payment gateway can be bypass easily.
* **BurpSuit :** Burp or Burp Suite is a graphical tool for testing Web application security. The tool is written in Java and developed by PortSwigger Web Security.
* **Doss: D**enial-of-service attack (DoS attack) is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.
* **CSRF:** Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. CSRF attacks specifically target state-changing requests, not theft of data, since the attacker has no way to see the response to the forged request.

|  |  |
| --- | --- |
| Section  7 |  |
| Project Team |
|  |  |

This project is comprised of four successful SAIT Polytechnic students, all undergoing the ‘IT Computer Systems’ course. Project team members and corresponding roles are as follows:

|  |  |
| --- | --- |
| **Member** | **Role** |
| Siddharth jain | working on applications and coding |
| Shubham malviya | working on applications and coding |
| Siddharth choudhary | working on applications and coding |

|  |  |
| --- | --- |
| Section  8 |  |
| Project Stakeholders |
|  |  |

The following table describes other project stakeholders which were not identified as key stakeholders in the Project Purpose section of this document:

|  |  |
| --- | --- |
| **Stakeholder** | **Role or Influence** |
| Sanjay sing jhala | Responsible for improving Vulnerability assessment |
| Shubham Malviya | Potentially a target for implementing this project upon completion. |
| Siddarth choudhary | Will be an end user of the product. |
| Siddarth jain | Provides the project team with a facility to carry out work needed for bug purposes. |
| Telecom/Internet Service Provider | Provides us with a network to transmit data from the hardware module to the server. |

|  |  |
| --- | --- |
| Section  9 |  |
| Risk Assessment |
|  |  |

As with any project, there are numerous risks involved which must be identified and given a strategy for mitigating their possibility of occurrence.

The following table outlines possible risks involved with the undertaking of this project, along with their associated impact/severity levels (Low/Medium/High):

|  |  |  |  |
| --- | --- | --- | --- |
| **Project Risk Assessment** | **Probability** | **Impact** | **Severity** |
| Risk 1 – Scope Creep | 4 | 5 | 20 |
| Mitigation Strategy | *As a group, we planned an outline specifying objectives and their associated deliverables involved in the project scope to be followed carefully. In addition, we have provided a list of out of scope activities*  *which will specifically not be touched upon during the course of this project.* | | |
| Risk 2 – Team Absences | 4 | 3 | 12 |
| Mitigation Strategy | *All project documents are accessible by all members via a shared network drive. By communication through e-mail, phone, video conferencing, even if a team member is absent they will be able to stay in contact. It is near impossible to make it to every meeting and*  *we understand this.* | | |
| Risk 3 – Faulty Hardware | 3 | 5 | 15 |
| Mitigation Strategy | *There is always the possibility that our hardware will be received in poor condition/not working. The simplest solution is to order more*  *than one similar model at a time. If all fail, we will order again from a different provider.* | | |
| Risk 4 – Conflicting Project Goals | 2 | 4 | 8 |
| Mitigation Strategy | *Project goals are laid out in this charter which will be agreed to and signed by each member of the team before the undertaking of the project. Group members held meetings prior to the final design of the project to discuss individual goals and find common ground at the*  *beginning of the project.* | | |
| Risk 5 – Lack of Resources | 2 | 5 | 10 |
| Mitigation Strategy | *We plan to order and maintain two copies of the hardware module for*  *redundancy in case one fails. Any resources needed for the servers will be provided by sclc and available as needed.* | | |

|  |  |
| --- | --- |
| Section  10 |  |
| Project Facilities and Resources |
|  |  |

Offensive Security is an international company working in Information security, penetration testing and digital forensics. Operating from around 2007 the company created open source projects, advanced security courses, ExploitDB (Vulnerability database) and the Kali Linux distribution. The company was started by Mati Aharoni, and employs security professionals with experience in security penetration testing and system security evaluation. The company has provided security counseling and training to the many technology companies.

In this project JNCT college help us to penetration testing the in college website. In this section we will see a real-life example of penetration testing that involved the civilian government agency FBI. The example is taken from an article in Computerworld that speaks about the penetration tester Chris Goggans that has been working as a penetration tester since 1991. One of his latest exploit was against the FBI. It only took him six hours to break into a crime database without permission. This is how he acted: he discovered a series of unpatched vulnerabilities in the civilian government agency's Web server, used a hole in the Web Server to pull down usernames and passwords that were reused on a host of enterprise systems,

therefore he got Windows domain administrator privileges gaining full access to almost all Windowsbased system in the enterprise, including workstations used by police officers. Finally, remotely controlling them he found programs on their desktops that

automatically connected the workstations to the FBI’s crime database. This vulnerability could have been eliminated through a clear separation of domains such as between the police network and the enterprise network.

|  |  |
| --- | --- |
| Section  11 |  |
| Project Budget |
|  |  |

This section outlines hardware, software and operational costs associated with the Holistic Vehicle Tracking System project budget. Project budget costs are separated based on materials needed (such as hardware and software), and man hours it will physically take our project team to complete all major activities and produce a final deliverable.

A final, cumulative budget of $95656.06 and 816.5 man hours will be required to ensure the success of this project.

# Equipment and Facilities

Software testability is the degree to which a software artifact (i.e. a software system, software module, requirements- or design document) supports testing in a given test context. If the testability of the software artifact is high, then finding faults in the system (if it has any) by means of testing is easier.A testable product ensures complete execution of the test scripts. Assuming that good test coverage is applied, most of the defects will be uncovered and fixed before the product is released. This insures customers will report a minimum number of defects. A lot of money is spent on supporting and maintaining a product after its development. Testable products are easy and less costly to maintain. The chances of achieving customer satisfaction with such products is are much higher. Hence testability is an important attribute to the maintainability of any software product.

|  |  |
| --- | --- |
| Tools | Totals |
| Burpsuit | $5000 |
| Hoxx VPN | $200 |
| MetaSploit | $400 |
| Dirsearch | $1000 |
| Internet | $10 |
| SQl injection | $100 |
| XSS | $150 |
| Total | $6860 |

|  |  |
| --- | --- |
| Section  12 |  |
| Promotion and Communication |
|  |  |

Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Application security encompasses measures taken to improve the security of an application often by finding, fixing and preventing security vulnerabilities.

Application security can be enhanced by rigorously defining enterprise assets, identifying what each application does (or will do) with respect to these assets, creating a security profile for each application, identifying and prioritizing potential threats and documenting adverse events and the actions taken in each case. This process is known as [threat modeling](https://searchsecurity.techtarget.com/definition/threat-modeling). In this context, a threat is any potential or actual adverse event that can compromise the assets of an enterprise, including both malicious events, such as a denial-of-service ([DoS](https://searchsecurity.techtarget.com/definition/DOS)) attack, and unplanned events, such as the failure of a storage device.

Once an afterthought in software design, security is becoming an increasingly important concern during development as applications become more frequently accessible over networks and are, as a result, vulnerable to a wide variety of threats. Security measures built into applications and a sound application security routine minimize the likelihood that unauthorized code will be able to manipulate applications to access, steal, modify, or delete sensitive data.

|  |  |
| --- | --- |
| Section  13 |  |
| Intellectual Property |
|  |  |

Software testability is the degree to which a software artifact (i.e. a software system, software module, requirements- or design document) supports testing in a given test context. If the testability of the software artifact is high, then finding faults in the system (if it has any) by means of testing is easier.A testable product ensures complete execution of the test scripts. Assuming that good test coverage is applied, most of the defects will be uncovered and fixed before the product is released. This insures customers will report a minimum number of defects. A lot of money is spent on supporting and maintaining a product after its development. Testable products are easy and less costly to maintain. The chances of achieving customer satisfaction with such products is are much higher. Hence testability is an important attribute to the maintainability of any software product.

Therefore, testability is often thought of as an extrinsic property which results from interdependency of the software to be tested and the test goals, test methods used, and test resources (i.e., the test context). Even though testability cannot be measured directly (such as software size) it should be considered an intrinsic property of a software artifact because it is highly correlated with other key software qualities such as encapsulation, coupling, cohesion, and redundancy. Being able to test software, a piece of code or functionality, depends on what the user can see and control, known as observability and controllability.

Observability enables a tester or user to see the external and internal of the software. When a user receives the correct expected output, but the internal or the background processes are not quite what was specified in the requirements, defects are often found elsewhere. This is more important in the case of unit and integration testing rather than a simple black box testing.

|  |  |
| --- | --- |
| Section  14 |  |
| Offer and Approvals |
|  |  |

# Offer

This is to offer that the project that we undertook was worked upon with a sincere effort. Most of the requirements have been fulfilled up to the mark and the requirements which have been remaining, can be completed with a short extension. This project would definitely satisfy all the requirements of the college and would be beneficial for the students and the college staff. We find the vulnerabilities in the website of successfully with the help of above tools and it is very interesting to hack into the website and make report of it.

# Approvals

From our project sponsor we will need:

* + Lab space to setup in and use for project work.
  + Kali linux, Offensive security help to built the project.
  + BurpSuit provide professional work space to work on this project.

And finally we need instructor approval for the initiation of our project.

# Project Charter Signoff

|  |  |  |
| --- | --- | --- |
| **Offering** | Signature | Date |
| Adam Elliott |  |  |
| Taylor M Kinsella |  |  |
| Matthew Lillywhite |  |  |
| Christopher McNeil |  |  |
| **Approval** |  |  |
| Colin Chamberlain |  |  |
| Jason Fischer |  |  |

|  |  |
| --- | --- |
| Section  15 |  |
| References |
|  |  |

# Bibliography

|  |  |
| --- | --- |
| [1] | J. Sukumaran, "The Tiny World of Electrons," 29 April 2010. [Online]. Available: http://web.archive.org/web/20121001153754/<http://jayeshprojects.blogspot.ca/2010/04/real-> time-mobile-gps-tracker-with.html. [Accessed 1 October 2012]. |
| [2] | Transit, City of Calgary - Transportation Department - Calgary, "City of Calgary - About Calgary Transit," December 2012. [Online]. Available: [http://www.calgarytransit.com/html/fleet\_information.html.](http://www.calgarytransit.com/html/fleet_information.html) [Accessed 24 November 2013]. |
| [3] | N. Dunker, "Real-time GPS tracker with mobile phone uplink," Hack a Day, 14 April 2011. [Online]. Available: [http://hackaday.com/2011/04/14/real-time-gps-tracker/.](http://hackaday.com/2011/04/14/real-time-gps-tracker/) [Accessed 15 February 2012]. |
| [4] | NextBus, "NextBus," NextBus Inc, 24 November 2013. [Online]. Available: [http://www.nextbus.com/predictor/agencySelector.jsp.](http://www.nextbus.com/predictor/agencySelector.jsp) [Accessed 24 November 2013]. |
| [5] | Microsoft, "MSDN - The Microsoft Developer Network," Microsoft, 2013. [Online]. Available: [http://msdn.microsoft.com/en-ca/.](http://msdn.microsoft.com/en-ca/) [Accessed 24 November 2013]. |
| [6] | GitHub Inc, "GitHub," 2013. [Online]. Available: https://github.com/. [Accessed 24 November 2013]. |
| [7] | J. V. Gonsalves, "Instructables," Autodesk Inc, 2013. [Online]. Available:<http://www.instructables.com/id/Athena-The-Global-Car-Tracking-> System/step1/Programming-the-Arduino/. [Accessed 17 November 2013]. |
| [8] | City of Calgary, "Open Data Catalogue," 2013. [Online]. Available: https://data.calgary.ca/OpenData/Pages/DatasetListingAlphabetical.aspx. [Accessed 17  November 2013]. |
| [9] | Microsoft, "Microsoft Azure," 2013. [Online]. Available: <http://technet.microsoft.com/en-> us/library/gg605186.aspx. [Accessed 24 November 2013]. |
| [10] | M. Hart, "Arduiniana," 7 September 2013. [Online]. Available: [http://arduiniana.org/2013/09/tinygps-a-new-view-of-global-positioning/.](http://arduiniana.org/2013/09/tinygps-a-new-view-of-global-positioning/) [Accessed 17 November 2013]. |