**Business Requirements Document**

**1.0 Background and Problem Statement**

Smithgall Woods is a State Park in Helen, Georgia where attendees of the park can partake in recreational activities such as fishing, hiking, camping, and volunteering. Smithgall Woods obtains return volunteer hours from the state which gives an incentive for friends chapters to volunteer their time so that the park itself can get more state money. The Smithgall Woods site should have the capability for volunteers to be able to log their hours in an easy to use interface. Another large concern that the park has is security and maintenance of the site. However, no specifications of what was preferred by the park was ever distinguished. It is understood that updating the site content is complex to the administrator and that it becomes difficult to change things. Most recently, the site has been hacked with “Cialis” links dispersed throughout the site.

1. **Business Requirements**

**2.1 Requirements Breakdown**

* User manual and training documents to be utilized by the Smithgall Woods team and website admins
* Potentially switch over to Java programming language
* User friendly interface
* Website mobility usage
* Pictures: Smithgall Woods wants to connect to the state site to rent cabins, along with include pictures of cabins and highlight of volunteers
* MySQL language

**2.2 Requirement Details**

N/A for right now

**3.0 Functional Specifications**

N/A for right now—will add one as we get more detail around requirements

**4.0 Discoveries**

* **Existence of unnecessary accounts**
  + Hosting site
    - 17505820 – Dr. Huber’s account
  + Databases
    - [db357026991](https://my.1and1.com/mysql-database-details/db357026991?__lf=ftp_create_account_flow) (FSGW)
    - [db358933030](https://my.1and1.com/mysql-database-details/db358933030?__lf=ftp_create_account_flow) (FSGWData); Database for Volunteer Hours
    - [db360322876](https://my.1and1.com/mysql-database-details/db360322876?__lf=ftp_create_account_flow) (Fresh root WP install): This is the database the WordPress site pulls from and saves to for page content.
    - [db265662256](https://my.1and1.com/mysql-database-details/db265662256?__lf=ftp_create_account_flow) (login and hours database): We think this is the volunteer hours db.
    - [db268336715](https://my.1and1.com/mysql-database-details/db268336715?__lf=ftp_create_account_flow) (calendardb)
  + FTP accounts
    - [u48922589](https://my.1and1.com/ftp-account-details/54939311?__lf=ftp_create_account_flow)
    - [u48922589-drdan](https://my.1and1.com/ftp-account-details/75464305?__lf=ftp_create_account_flow) : This is the only account we can access. The passwords for the others are incorrect. We only need one account, so we propose getting rid of the remaining
    - [u48922589-students](https://my.1and1.com/ftp-account-details/76946453?__lf=ftp_create_account_flow)
    - [u48922589-Admin](https://my.1and1.com/ftp-account-details/77483152?__lf=ftp_create_account_flow)
  + WordPress accounts
    - mhuber ([mhuber@uga.edu](mailto:mhuber@uga.edu))
    - admin ([youdomaincom977@gmail.com](mailto:youdomaincom977@gmail.com)) : this is the default admin name in WP and we suggest that it should be changed via the wp\_users table in the database, assuming that nothing becomes disrupted
    - Admin1 ([webmaster@friendsofsmithgallwoods.org](mailto:webmaster@friendsofsmithgallwoods.org))
    - lcompton ([compton.pl@gmail.com](mailto:compton.pl@gmail.com)) : Web Committee Leader
* **Outdated Plugins**
  + WordPress – Running version 4.5.9🡪update to 4.8.1
  + PHP – Running version 5.2🡪update to 7.0
  + WordPress theme – No update found
  + WordPress plugins
    - Akismet – Running version 3.0🡪update to 3.3.4
    - NextGEN Gallery – Running version 1.7.4🡪update to 2.2.12
    - Page Links To – Running version 2.4🡪update to 2.9.9
    - Seo Meta Tags – Running version 1.0🡪update to 1.4
* **Hidden Link Injection:**
  + Hidden link injections in WordPress is when the attacker inserts links into the files of active WordPress themes and are typically wrapped in HTML comments. It is believed that this is what is pointing to the “Cialis” site. This is a common problem in WordPress versions 2.8x and attackers are able to get into the \wp-admin\upload.php file and insert files on the server
  + A base64\_decode on the second line of the \wp-includes\locale.php file was found and identified as part of the injected malicious code that triggers the “cialis” messages with external web links to be displayed in multiple site pages.

**5.0 Proposed Solutions to Security Vulnerability**

* Deleting the malicious html insert from the file
  + Note: Commenting the injected code out prevents the “Cialis” messages with hyperlinks from being displayed throughout the site
* Updating plugins and software to suggested versions found in **“Discoveries”** section
* Removing unnecessary accounts as suggested in **“Discoveries”** section
* Considering other programming languages that are more robust
* Use the hosting website’s security application to help prevent further issues.
  + 1&1 SiteLock - <https://help.1and1.com/hosting-c37630/sitelock-c85170/what-is-1and1-sitelock-a792625.html>
    - Basic ($.99/month)
      * Daily malware scan
      * Trust Seal
      * Search engine blacklist monitoring
      * SSL verification
      * Web app scan (on demand once a month)
      * SQL injection scan (on demand once a month)
      * XSS scan (on demand once a month)
      * Number of pages monitored – 25
    - Premium ($4.99/month)
      * Daily malware scan
      * Trust Seal
      * Search engine blacklist monitoring
      * SSL verification
      * Web app scan
      * SQL injection scan
      * XSS scan
      * File Change Monitoring
      * Number of pages monitored – 500