**IT Assesment**

|  |  |  |  |
| --- | --- | --- | --- |
| Project Name | **IT Assesment - agrianalytica.com** | Cod Proiect | AGRA001A |
| Authors | [Laurentiu RADU](mailto:laurentiu.radu@forwardsoftware.ro?subject=AGRA001A) | Approved by |  |
| Creation Date | 14.06.2017 | Last modification date | 16.06.2017 |
| Version | 0.1 | Status | Propus |

Table of Contents

[1. Infrastructure 2](#_Toc485382566)

[1.1. Internal Server Infrastructure 2](#_Toc485382567)

[1.2. External Server Infrastructure 2](#_Toc485382568)

[1.3. Networking infrastructure 3](#_Toc485382569)

[1.4. Data Storage 3](#_Toc485382570)

[1.5. Cloud Services 3](#_Toc485382571)

[1.6. Business Services/Applications 4](#_Toc485382572)

[1.7. Disaster Recover/Business Continuity 4](#_Toc485382573)

[2. Agrianalytica Application 4](#_Toc485382574)

[2.1. Architecture diagram 4](#_Toc485382575)

[2.2. Key Performance Indicators (KPI) 5](#_Toc485382576)

[2.3. Security Checklist 5](#_Toc485382577)

[2.3.1. Information Gathering 5](#_Toc485382578)

[2.3.2. Configuration Management 6](#_Toc485382579)

[2.3.3. Secure Transmission 6](#_Toc485382580)

[2.3.4. Authentication 7](#_Toc485382581)

[2.3.5. Session Management 7](#_Toc485382582)

[2.3.6. Authorization 8](#_Toc485382583)

[2.3.7. Cryptography 8](#_Toc485382584)

[2.3.8. Data Validation 8](#_Toc485382585)

[2.3.9. Denial of Service 9](#_Toc485382586)

[2.3.10. Specific Risky Functionality 9](#_Toc485382587)

# Infrastructure

## Internal Server Infrastructure

This section’s purpose is to assess the current internal server infrastructure regarding volume, performance, capability planning, virtualization, operating systems. If more than one server involved, please duplicate the table below and fill in the details.

SSC =„Strategia & Sviluppo Consultants Ukraine”

N/A

|  |  |
| --- | --- |
| **Infrastructure server purpose** | DATABASE/APPLICATION SERVER/ESB/Other (please provide additional informations about the purpose of this server) |
| **Configuration** | |
| **CPU (physical or virtual)** | N/A |
| **RAM** | N/A |
| **Storage (include special configuration if applicable eg. RAID)** | N/A |
| **Virtualization** | N/A |
| **Operating System** | N/A |
| **Operating System version** | N/A |
| **Latest security patch installed** | N/A |
| **Additional informations**  **(eg. Bandwith, Throughput or other relevant informations)** | N/A |
| **Additional details (if applicable)** | |
| **Database Provider** | N/A |
| **Database Version** | N/A |
| **Application Server** | N/A |
| **Application Server Version** | N/A |

## External Server Infrastructure

This section’s purpose is to assess the current external server infrastructure regarding providers, servers involved, performance, capability planning, virtualization, operating systems. If more than one server involved, please duplicate the table below and fill in the details.

[TO BE COMPLETED BY SSC]

|  |  |
| --- | --- |
| **Hosting provider** | [Hosting Ukraine](https://www.ukraine.com.ua/) |
| **Infrastructure server purpose** | DATABASE/APPLICATION SERVER/ESB/Other (please provide additional informations about the purpose of this server) |
| **Configuration** | |
| **CPU (physical or virtual)** | N/A |
| **RAM** | N/A |
| **Storage (include special configuration if applicable eg. RAID)** | SSD |
| **Virtualization** |  |
| **Operating System** | Linux |
| **Operating System version** | N/A |
| **Latest security patch installed** | N/A |
| **Additional informations**  **(eg. Bandwith, Throughput or other relevant informations)** | N/A |
| **Additional details (if applicable)** | |
| **Database Provider** | [Hosting Ukraine](https://www.ukraine.com.ua/) |
| **Database Version** | 5.7.x |
| **Application Server** | N/A |
| **Application Server Version** | N/A |

## Networking infrastructure

N/A

|  |  |
| --- | --- |
| **ISP** | N/A |
| **Network switching** | N/A |
| **Wireless** | N/A |
| **Cabling and conectivity** | N/A |
| **LAN/WAN** | N/A |

## Data Storage

N/A where not applicable, type N/A, otherwise provide as many informations as you can

|  |  |
| --- | --- |
| **SAN** | N/A |
| **Vendor/Model** | N/A |
| **Storage** | N/A |
| **Permissions** | N/A |
| **Accessibility** | N/A |
| **Availability** | N/A |

## Cloud Services

[TO BE COMPLETED BY SSC] where not applicable, type N/A, otherwise provide as many informations as you can

|  |  |
| --- | --- |
| **Provider** | N/A |
| **Compliance** | N/A |
| **Availability** | N/A |
| **Accessibility** | N/A |
| **Service delivery models** | N/A |

## Business Services/Applications

N/A where not applicable, type N/A, otherwise provide as many informations as you can

|  |  |
| --- | --- |
| **Collaboration and messaging software** | N/A |
| **Financial management software** | N/A |
| **CRM** | N/A |
| **Active Directory/directory services** | N/A |
| **Business intelligence** | N/A |
| **File/print sharing** | N/A |

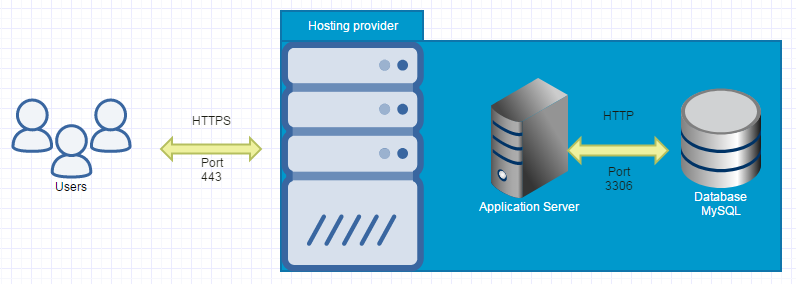
## Disaster Recover/Business Continuity

N/A where not applicable, type N/A, otherwise provide as many informations as you can

|  |  |
| --- | --- |
| **Recovery Time Objective (RTO)** | N/A |
| **Recovery Point Objective (RPO)** | N/A |
| **Disaster Recovery (DR) planning** | N/A |
| **Business and Impact analysis in case of disaster** | N/A |
| **Backups planning** | N/A |
| **Additional informations** | N/A |

# Agrianalytica Application

## Architecture diagram



## Key Performance Indicators (KPI)

\*this indicators must be completed regarding the current infrastructure regarding the Production environment of AGRA Project.

|  |  |
| --- | --- |
| **Response Times** | 0.300ms |
| **Maximum Concurrent Users** | 5000 |
| **Capacity Scaling** | N/A |
| **Implement and Verify Load Balancing** | N/A |
| **3rd Party Functions** | N/A |
| **Logging** | N/A |
| **Monitoring** | N/A |
| **Optimized for mobile** | N/A |

## Security Checklist

N/A where not applicable, type N/A, otherwise provide as many informations as you can (regarding the implementation method used in the application to counteract the threat)

### Information Gathering

|  |  |
| --- | --- |
| **Manually explore the site to find sensible files** | Successfully conducted |
| **Spider/crawl for missed or hidden content** | Successfully conducted |
| **Check the Webserver Metafiles for information leakage files that expose content, such as robots.txt, sitemap.xml, .DS\_Store** | N/A |
| **Check the caches of major search engines for publicly accessible sites** | N/A |
| **Check for differences in content based on User Agent (eg, Mobile sites, access as a Search engine Crawler)** | N/A |
| **Check The Webpage Comments and Metadata for Information Leakage** | N/A |
| **Check The Web Application Framework** | N/A |
| **Perform Web Application Fingerprinting** | N/A |
| **Identify technologies used** | N/A |
| **Identify user roles** | N/A |
| **Identify application entry points** | N/A |
| **Identify client-side code** | N/A |
| **Identify multiple versions/channels (e.g. web, mobile web, mobile app)** | N/A |
| **Identify web services** | N/A |
| **Identify co-hosted and related applications** | N/A |
| **Identify all hostnames and ports** | N/A |
| **Identify third-party hosted content** | N/A |

### Configuration Management

|  |  |
| --- | --- |
| **Check for commonly used application and administrative URLs** | Success |
| **Check for old, backup and unreferenced files** | Success |
| **Check HTTP methods supported and Cross Site Tracing (XST)** | N/A |
| **Test file extensions handling** | N/A |
| **Test RIA cross domain policy** | N/A |
| **Test for security HTTP headers (e.g. CSP, X-Frame-Options, HSTS)** | N/A |
| **Test for policies (e.g. Flash, Silverlight, robots)** | N/A |
| **Check for sensitive data in client-side code (e.g. API keys, credentials)** | N/A |

### Secure Transmission

|  |  |
| --- | --- |
| **Check SSL Version, Algorithms, Key length** | N/A not yet conducted |
| **Check for Digital Certificate Validity (Duration, Signature and CN)** | N/A not yet conducted |
| **Check credentials only delivered over HTTPS** | N/A not yet conducted |
| **Check that the login form is delivered over HTTPS** | N/A not yet conducted |
| **Check session tokens only delivered over HTTPS** | N/A not yet conducted |
| **Check if HTTP Strict Transport Security (HSTS) in use** | N/A not yet conducted |
| **Test ability to forge requests** | N/A not yet conducted |
| **Test Web Messaging (HTML5)** | N/A not yet conducted |
| **Check CORS implementation (HTML5)** | N/A not yet conducted |
| **Test for Web Service Issues** | N/A |
| **Test REST** | N/A |

### Authentication

|  |  |
| --- | --- |
| **Test password quality rules** | N/A not yet conducted |
| **Test remember me functionality** | Successfully conducted |
| **Test password reset and/or recovery** | N/A not yet conducted |
| **Test password change process** | N/A not yet conducted |
| **Test CAPTCHA** | N/A not yet conducted |
| **Test multi factor authentication** | N/A not yet conducted |
| **Test for logout functionality presence** | Successfully conducted |
| **Test for default logins** | Successfully conducted |
| **Test for out-of channel notification of account lockouts and successful password changes** | N/A not yet conducted |
| **Test for consistent authentication across applications with shared authentication schema / SSO and alternative channels** | N/A not yet conducted |
| **Test for Weak security question/answer** | N/A not yet conducted |
| **Test for user enumeration** | Successfully conducted |
| **Test for authentication bypass** | Successfully conducted |
| **Test for brute force protection** | Successfully conducted |
| **Test for Credentials Transported over an Encrypted Channel** | N/A not yet conducted |
| **Test for cache management on HTTP (eg Pragma, Expires, Max-age)** | N/A not yet conducted |
| **Test for user-accessible authentication history** | N/A not yet conducted |

### Session Management

|  |  |
| --- | --- |
| **Establish how session management is handled in the application (eg, tokens in cookies, token in URL)** | Successfully conducted |
| **Check session tokens for cookie flags (httpOnly and secure)** | Successfully conducted |
| **Check session cookie scope (path and domain)** | N/A not yet conducted |
| **Check session cookie duration (expires and max-age)** | Successfully conducted |
| **Check session termination after a maximum lifetime** | Successfully conducted |
| **Check session termination after relative timeout** | Successfully conducted |
| **Check session termination after logout** | Successfully conducted |
| **Test to see if users can have multiple simultaneous sessions** | Successfully conducted |
| **Test session cookies for randomness** | N/A not yet conducted |
| **Confirm that new session tokens are issued on login, role change and logout** | Successfully conducted |
| **Test for consistent session management across applications with shared session management** | Successfully conducted |
| **Test for session puzzling** | N/A not yet conducted |
| **Test for CSRF and clickjacking** | N/A not yet conducted |

### Authorization

|  |  |
| --- | --- |
| **Test for path traversal** | Successfully conducted |
| **Test for vertical Access control problems (a.k.a. Privilege Escalation)** | Successfully conducted |
| **Test for horizontal Access control problems (between two users at the same privilege level)** | Successfully conducted |
| **Test for missing authorisation** | Successfully conducted |
| **Test for Insecure Direct Object References** | N/A not yet conducted |

### Cryptography

|  |  |
| --- | --- |
| **Check if data which should be encrypted is not** | Successfully conducted |
| **Check for wrong algorithms usage depending on context** | Successfully conducted |
| **Check for weak algorithms usage** | Successfully conducted |
| **Check for proper use of salting** | Successfully conducted |
| **Check for randomness functions** | Successfully conducted |

### Data Validation

|  |  |
| --- | --- |
| **Test for HTML Injection** | Successfully conducted |
| **Test for SQL Injection** | Successfully conducted |
| **Test for LDAP Injection** | not used |
| **Test for ORM Injection** | not used |
| **Test for XML Injection** | not used |
| **Test for XXE Injection** | not used |
| **Test for SSI Injection** | N/A not yet conducted |
| **Test for XPath Injection** | not used |
| **Test for XQuery Injection** | N/A not yet conducted |
| **Test for IMAP/SMTP Injection** | N/A not yet conducted |
| **Test for Code Injection** | Successfully conducted |
| **Test for Expression Language Injection** | N/A not yet conducted |
| **Test for Command Injection** | not used |
| **Test for NoSQL injection** | N/A not yet conducted |
| **Test for Reflected Cross Site Scripting** | N/A not yet conducted |
| **Test for Stored Cross Site Scripting** | N/A not yet conducted |
| **Test for DOM based Cross Site Scripting** | N/A not yet conducted |
| **Test for Cross Site Flashing** | N/A not yet conducted |
| **Test for Overflow (Stack, Heap and Integer)** | N/A not yet conducted |
| **Test for Format String** | Successfully conducted |
| **Test for incubated vulnerabilities** | N/A not yet conducted |
| **Test for HTTP Splitting/Smuggling** | N/A not yet conducted |
| **Test for HTTP Verb Tampering** | N/A not yet conducted |
| **Test for Open Redirection** | N/A not yet conducted |
| **Test for Local File Inclusion** | N/A not yet conducted |
| **Test for Remote File Inclusion** | N/A not yet conducted |
| **Compare client-side and server-side validation rules** | N/A not yet conducted |
| **Test for HTTP parameter pollution** | N/A not yet conducted |
| **Test for auto-binding** | N/A not yet conducted |
| **Test for Mass Assignment** | N/A not yet conducted |
| **Test for NULL/Invalid Session Cookie** | Successfully conducted |
| **Test for integrity of data** | Successfully conducted |
| **Test for the Circumvention of Work Flows** | Successfully conducted |
| **Test Defenses Against Application Mis-use** | Successfully conducted |
| **Test That a Function or Feature Cannot Be Used Outside Of Limits** | Successfully conducted |
| **Test for Process Timing** | N/A not yet conducted |
| **Test for Web Storage SQL injection (HTML5)** | Successfully conducted |
| **Check Offline Web Application** | Successfully conducted |

### Denial of Service

|  |  |
| --- | --- |
| **Test for anti-automation** | N/A not yet conducted |
| **Test for account lockout** | N/A not yet conducted |
| **Test for HTTP protocol DoS** | N/A not yet conducted |
| **Test for SQL wildcard DoS** | N/A not yet conducted |

### Specific Risky Functionality

|  |  |
| --- | --- |
| **Test that acceptable file types are whitelisted and non-whitelisted types are rejected** | Successfully conducted |
| **Test that file size limits, upload frequency and total file counts are defined and are enforced** | Successfully conducted |
| **Test that file contents match the defined file type** | Successfully conducted |
| **Test that all file uploads have Anti-Virus scanning in-place.** | N/A not yet conducted |
| **Test upload of malicious files** | N/A not yet conducted |
| **Test that unsafe filenames are sanitized** | Successfully conducted |
| **Test that uploaded files are not directly accessible within the web root** | Successfully conducted |
| **Test that uploaded files are not served on the same hostname/port** | Successfully conducted |
| **Test that files and other media are integrated with the authentication and authorisation schemas** | Successfully conducted |
| **Test for known vulnerabilities and configuration issues on Web Server and Web Application** | N/A not yet conducted |
| **Test for default or guessable password** | N/A not yet conducted |
| **Test for Injection vulnerabilities** | Successfully conducted |
| **Test for Buffer Overflows** | N/A not yet conducted |
| **Test for Insecure Cryptographic Storage** | N/A not yet conducted |
| **Test for Insufficient Transport Layer Protection** | Successfully conducted |
| **Test for Improper Error Handling** | N/A not yet conducted |
| **Test for all vulnerabilities with a CVSS v2 score > 4.0** | N/A not yet conducted |
| **Test for Authentication and Authorization issues** | Successfully conducted |
| **Test for CSRF** | N/A not yet conducted |