Planview – Spigit v4.3

External Application Penetration Test

Prepared For:
Philip Blanchar
Planview
19 April 2019

Prepared By:
Emagined Security
2816 San Simeon Way
San Carlos, CA 94070
650-593-9829

Executive Summary

At the request of Planview (Client), Emagined Security consultants performed a penetration test of the Client's external application. The purpose of this engagement was to identify vulnerabilities attackers can leverage to compromise the environment.

Engagement Period

Start: 15 April 2019 End: 19 April 2019

Engagement Team

Philip Blanchar	Sr. Manager, Hosting Operations	pblanchar@planview.com
Lance Wright	Director of Information Security	lwright@planview.com

Testing was conducted from the following attacker's perspective:

- attacker remotely over the internet (external threat)

The results from this test apply to the Client application and its supporting infrastructure, where applicable within the written scope of the engagement. Emagined Security consultants evaluated only those assets in scope. Findings summarized below are representative of security issues found and may not list all instances of a specific issue.

The Client should bear in mind that penetration testing is a point-in-time effort, and may not be comprehensive nor reflective of the overall Client security posture. Vulnerabilities disclosed may improve, deteriorate, or remain static over time, based on mitigation activity.

In review of the vulnerabilities identified, and from discussions with the Client points of contact identified above, Emagined Security consultants noted the following with respect to the Client's external application within the confines of the testing engagement's scope, focus area, and the consultants' overall knowledge of the Client application environment:

> **Areas of Strength:** The Spigit application is configured with a strong security posture in mind that is shown by the protection from common attack vectors such as cross-site scripting, sql injection, and other user input and client-side attack vectors. Additionally, user input and file upload functionality are properly sanitized and restricted for the core functionality of the application, in that executable files are not allowed to be uploaded and certain character usage is not allowed within user input supplied areas. Furthermore, information disclosure of the application's underlying technology is securely confined within the bounds of the application and does not unnecessarily expose information that could assist would-be attackers.
>
> **Areas for Improvement:** Although the Spigit application has a strong security posture for user supplied data and information, the application could greatly benefit from adjustments to session management of its users. Users are able to maintain valid sessions for long periods of time. In this instance, sessions were still valid after being left overnight.

Emagined Security consultants offer the following caveat to the above speculative statement regarding areas of strength and improvement: Care should be taken not to place undue significance on this report, or upon any single vulnerability assessment as conducted at a given point-in-time against select Client assets as environments, systems, tests, and security are dynamic in nature. Rather focus should be placed on the Client's holistic security posture, its perimeter security controls, and the application thereof of said controls over time.

Finding Synthesis

Findings from the Spigit application penetration test are summarized in the below table.

Findings listed are categorized from a technical perspective only and do not attempt to factor nor adequately reflect all security safeguards and countermeasures present or planned for the environment in which these findings were detected. The respective target organization will want to assess risk represented by the below findings independently and in accordance with its existing risk assessment program, that includes factors planned and present security controls wholly in relation to organizational risk appetite, accepted residual risk levels, and systems, assets, and data valuation.

Unless otherwise specified in the Statement of Work, manual and automated testing did not specifically include any availability-based attack vectors such as denial of service (DoS).

How to interpret the table: Finding refers to the named technical vulnerability identified; severity pertains to the impact realized from a successful exploit of the named vulnerability; difficulty refers to the level of skill needed to perform a successful exploit against the named vulnerability; disposition pertains to the current state of remediation for the vulnerability.

Finding 1:	Concurrent Login				
Severity:	Low	Difficulty:	Easy	Disposition:	Open
Finding 2:	Insufficient Session Timeout				
Severity:	Low	Difficulty:	Easy	Disposition:	Open
Finding 3:	Wildcard Certificate in Use				
Severity:	Low	Difficulty:	Moderate	Disposition:	Open
Finding 4:	Vulnerable AngularJS				
Severity:	Low	Difficulty:	Hard	Disposition:	Open
Finding 5:	Vulnerable jQuery				
Severity:	Low	Difficulty:	Hard	Disposition:	Open

Engagement Objective

Emagined Security contracted with Planview (Client) to provide a penetration test of the Spigit application. Findings listed in the Identified Vulnerabilities and Severities section contain detailed results from the test and elaborate on those vulnerabilities directly affecting the security posture of the Client environment.

Vulnerabilities disclosed within this document represent 'point-in-time' findings at the time of testing and are indicative of security issues encountered during the test window. These vulnerabilities are weighted against industry standards, Client security policy, and the experience of Emagined Security consultants. As time progresses, this document will become less representative of the Client's environment due to changes in that environment, new vulnerability and exploit discovery and publication, and advances in technology and tools development.

Emagined Security utilizes the following criteria to provide the Client with a better understanding of the security vulnerabilities within its environment:

1. Severity rating - based on the potential damage and exposure to the application and/or network if an adversary were to launch a successful attack using a given finding

2. Difficulty rating - based on the aggregate value of current security safeguards, the position of an attacker with the organization, and the knowledge necessary to carry out the attack using a given finding

Testing Parameters

Testing environment: non-production

Attacker perspective: attacker on the internet (external threat)

Authentication method: authenticated

Roles:

PenTest Admin1	Administrator
PenTest Admin2	Administrator
PenTest Moderator1	Moderator
PenTest Moderator2	Moderator
PenTest User1	User
PenTest User1	User

The following Client URLs were tested during the engagement:

https://pentest.spigit.com