Security Assessment Report
Vidyano

TSF | THE SECURITY FACTORY

Table of Contents

Document Properties

Version History

Current version: **2.00**

Version	Date	Status	Author
0.01	25/02/14	Creation	Anton Delaruelle
0.02	27/02/14	Update	Anton Delaruelle
0.90	28/02/14	Review by QA	Nico Cooman
1.00	03/03/14	Final Draft	Nico Cooman
1.90	10/03/14	Retest of implemented solutions	Anton Delaruelle
2.00	13/03/14	Final Version	Nico Cooman

Executive Summary

Background

The Security Factory was tasked with performing a vulnerability assessment on the Vidyano. Framework. The purpose of this assessment was to verify the effectiveness of the security controls put in place by Vidyano to secure business-critical information, and the extent to which an attacker can compromise applications and data should these controls fail.

This report represents the findings from the assessment and the associated remediation recommendations to help Vidyano strengthen its security posture. The evaluation represent a point in time and certain vulnerabilities can become obsolete over time.

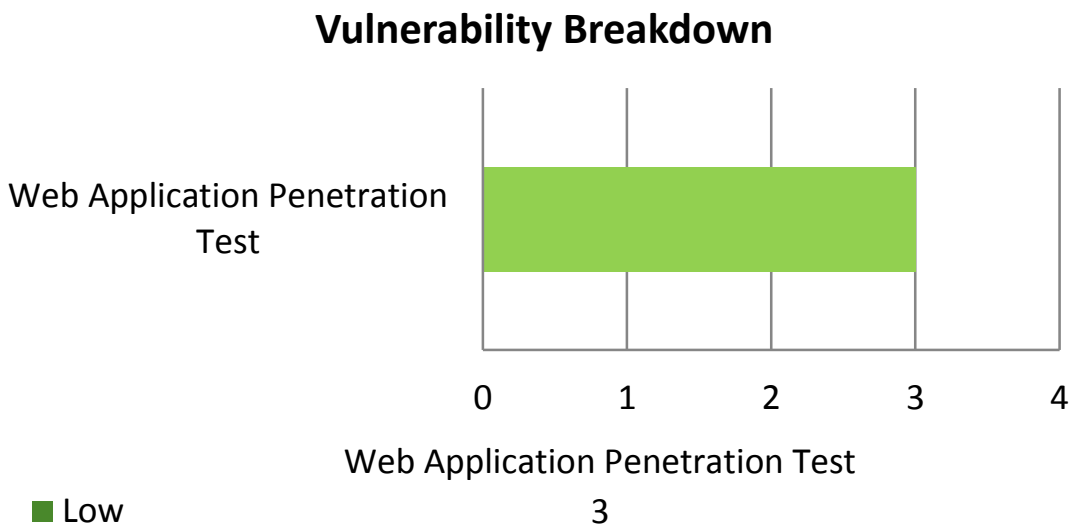
This report represent the retest after solutions were implemented by 2sky mitigating the risks defined in version 1.00 of the document.

The findings described in this document were discovered testing Vidyano **5.0.10705.3129**.

General Findings

This test was performed in two stages. Details of the original findings can be retrieved from version **1.00** of this document.

2Sky implemented solutions in their framework Vidyano. Note that 2 out of the 3 low rated vulnerabilities are out of control of 2sky to implement the proper remediation.



Positive Observations	Issues
• authToken dependant of outgoing IP address • Server-side access controls on data • Strong protection against injection attacks	• Vulnerable to coordinated brute force attacks

Strategic Overview

Comparing the security posture of the application tested at Vidyano with our experience in the market, we rate this application having a **strong** security posture.

Following table represents the most important categories evaluated and the scoring of Vidyano compared to our experience at other customers:

Category	Scoring Vidyano	Scoring Market
Misconfiguration	Strong	Medium
Incorrect use	Strong	Strong
Design flaw	Strong	Strong
Lack of (input) validation	Strong	Weak
Authentication mechanism issues	Strong	Strong
Sensitive data leakage	Strong	Medium
Other	Strong	Medium

Vulnerability Summary

Vidyano.azurewebsites.net

Risk Level	Finding	Category
Low	No brute force detection	Vulnerable software
Low	Cookies without httponly flag	Misconfiguration
Low	Cookies without secure flag	Misconfiguration

Remediation Roadmap

Immediately

- Not applicable

1 to 3 months

- Not applicable

3 to 12 months

- Security self assessment
- Implement a Web Application Firewall (WAF) to practice defense in depth

12+ months

- 3rd Party security re-assessment

Risk Levels Overview

Critical	Remotely exploitable vulnerabilities that can compromise the system. Interaction is not normally required for this exploit to be successful. Exploits are available and are reportedly being used in the wild.
High	Remotely exploitable Denial of Service (DOS) vulnerabilities that can compromise The system but do require user interaction. Vulnerabilities that may allow anonymous users to access sensitive information or take administrative actions. Interaction (such as an administrator viewing a particular page) may be required for this exploit to be successful, or in cases where interaction is not required (such as CSRF) the exploit causes only minor damage or impacts less critical systems.
Medium	Remotely exploitable vulnerabilities that can compromise the system. Interaction (such as an administrator viewing a particular page) is required for this exploit to be successful. The exploit requires the user to have some level of system access or non-default permission.
Low	A slight misconfiguration that may reduce the overall security level, but in itself does not cause serious concern.
Information	Issues which are either out of scope or have no security impact, but which were deemed interesting enough to put in the report.

Vulnerabilities

Following vulnerabilities were discovered during the time of retesting after 2sky implemented their solutions:

No brute force detection

Classification

Risk Level	**Low**

Finding

We found that there was no protection in place against brute force attacks.
Although countermeasures were taken to prevent this attack, we found that they don't provide adequate prevention. A (failed) login attempt will cause a delay of 1 second. If we launch multiple requests, all responses return at the same point in time.

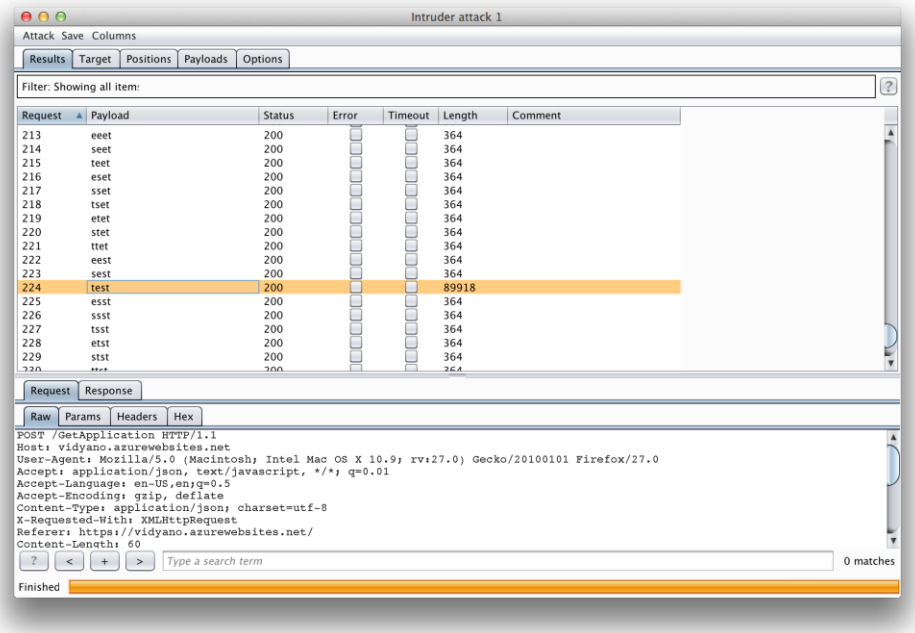
Consequences

A (distributed) brute force attack can be launched against Vidyano to gain access to valid credentials.

Remediation Advice

Restrict the number of login attempts per user and client IP. Lockout or delay attempts after a number of failed requests, preferably with an exponential delay time for each failed attempt.

Screenshots / Evidence



Cookies without httponly flag

Classification

Risk Level	**Low**
URL(s)	https://vidyano.azurewebsites.net

Finding

Cookies without the httponly flag were found.

Consequences

When the httponly flag is not set, cookies can be accessed by scripting laguages like Javascript. In the event of a cross-site-scripting attack, this could lead to leaking of the information in the cookie.

Remediation Advice

These cookies are controlled by Windows Azure, so no remediation can be implemented.

Screenshots / Evidence

Request:

```
GET / HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:27.0) Gecko/20100101 Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 9575
Content-Type: text/html; charset=utf-8
Expires: -1
ETag: "YQo4dgWZ6ZV/F27p3UtUO1NxAAcjIn98QaqCu8khcL0="
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Set-Cookie: ARRAffinity=978ef81357394441518d31c5d825ae8c5811698d7e2d3f8ffcffe0b32b08b4fb;Path=/;Domain=vidyano.azurewebsites.net
Date: Fri, 14 Mar 2014 15:39:27 GMT

<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>My CRM</title>
...........content.............
```

Cookies without secure flag

Classification

Risk Level	**Low**
URL(s)	https://vidyano.azurewebsites.net

Finding

Cookies without the secure flag were found.

Consequences

Without the secure flag, a cookie can be accessed through an unencrypted connection.

Remediation Advice

These cookies are controlled by Windows Azure, so no remediation can be implemented.

Screenshots / Evidence

Request:

```
GET / HTTP/1.1
Host: vidyano.azurewebsites.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:27.0) Gecko/20100101 Firefox/27.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 9575
Content-Type: text/html; charset=utf-8
Expires: -1
ETag: "YQo4dgWZ6ZV/F27p3UtUO1NxAAcjIn98QaqCu8khcL0="
Strict-Transport-Security: max-age=31536000
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Set-Cookie: ARRAffinity=978ef81357394441518d31c5d825ae8c5811698d7e2d3f8ffcffe0b32b08b4fb;Path=/;Domain=vidyano.azurewebsites.net
Date: Fri, 14 Mar 2014 15:39:27 GMT


<!DOCTYPE html>
<html>
<head>
    <meta charset="utf-8">
    <meta http-equiv="X-UA-Compatible" content="ie=edge">
    <title>My CRM</title>
..........content.............
```