test1

Date 03/29/2016

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Customer Information | | | | | |
| Company Name: |  | | | | |
| City: |  | State: |  | Zip Code: |  |
| URL: |  |  |  |  |  |

|  |  |
| --- | --- |
| Customer Contact Information | |
| Contact Name: |  |
| Title: |  |
| Telephone: |  |
| E-mail: |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Consultant Information | | | | | |
| Company Name: | Serpico Template Report, LLC | | | | |
| Contact Name: | hadhemi | | | | |
| Title: | intern | | | | |
| Telephone: |  | | | | |
| E-mail: |  | | | | |
| Business Address: | 123 Paper St | | | | |
| City | TestCity | State: | MA | Zip Code: | 11111 |
| URL: | <http://www.serpicoreport.com> | | | | |

# Executive Summary

Serpico Template Company (STC) was contracted to perform a penetration test for . This report discusses the results from the assessment. Really, if you are reading this you should update the template to match your executive summary. The symbols throughout this report are used to display the data. Please see the README to understand how they work.

Overall, STC was able to achieve the goals of the assessment and exfiltrate the targeted data. There were a number of critical findings during the assessment including the following:

|  |  |
| --- | --- |
| Finding Name | DREAD Score |

MOAR STUFF

# Attack Narrative

The following discusses the details of the assessment.

# Findings

## Findings Table

The following were the results from the assessment:

|  |  |  |
| --- | --- | --- |
| Finding Name | DREAD Score | Remediation Effort |
| **High Risk Findings (36-50)** |  |  |
|  |  |  |
| **Moderate Risk Findings (20-35)** |  |  |
|  |  |  |
| **Low Risk Findings (1-19)** |  |  |
| User credentials are sent in clear text | 1 | Quick |
| Retrieved x-powered-by header: ASP.NET | 1 |  |
| Retrieved x-aspnet-version header: 2.0.50727 | 1 |  |
| robots.txt contains 1 entry which should be manually viewed. | 1 |  |
| Clickjacking: X-Frame-Options header missing | 1 |  |
| Slow HTTP Denial of Service Attack | 1 |  |
| Cookie without Secure flag set | 1 |  |
| Cookie without HttpOnly flag set | 1 |  |
| Login page password-guessing attack | 1 |  |
| Email address found | 1 |  |
| JSF ViewState client side storage | 1 |  |
| Possible username or password disclosure | 1 |  |
|  |  |  |