Pentest Report

Penetration test of **Contoso**

Consultant: John Doe

01/11/2019

Executive Sumary

Overview

Issue2Report performed a Web Application Penetration Test on Contoso applications. The scope of the testing was the following.

- a.client.com
- b.client.com
- c.client.com
- d.client.com
- e.client.com
- f.client.com

Issue2Report found that with a few minor exceptions the quality and coverage of security controls in the Contoso applications were very solid.

Resume

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Nulla vehicula volutpat urna, eget rhoncus lacus congue at. Donec sagittis erat at tortor consectetur, in dapibus massa finibus. Etiam enim est, pharetra nec faucibus interdum, pretium vel risus. Donec risus tellus, pretium a odio eu, hendrerit vestibulum odio. Vestibulum consequat viverra eros. Nunc vehicula massa consectetur, gravida nibh quis, commodo nunc. Duis malesuada egestas dui sit amet sagittis. Vestibulum cursus interdum diam sed interdum. Donec volutpat libero sit amet finibus elementum. Aenean placerat sodales mollis. In quis euismod ex. Donec pulvinar faucibus nisl at iaculis. Fusce sed consectetur nisi, eget gravida turpis. Etiam consectetur maximus nulla sed rhoncus. Nulla eu condimentum felis. Nulla lobortis et purus vitae ornare.

Cras aliquam, mi nec scelerisque tempor, odio leo aliquam elit, at tincidunt diam dolor in nisl. Phasellus nibh purus, eleifend vel enim eu, facilisis tempor turpis. Mauris viverra lacinia sodales. Suspendisse dapibus lacus ac venenatis lacinia. Phasellus quis nibh purus. In dignissim urna neque, a volutpat odio egestas vitae. Nam venenatis pharetra ligula, a suscipit ante pellentesque a. Nullam volutpat urna at nisl cursus, ut consequat massa varius. Nulla tempor ut dui non aliquam. In id velit a purus ultricies suscipit. Nulla finibus, mauris eu rhoncus consequat, justo libero accumsan libero, vel convallis neque metus vel neque. In rhoncus arcu sed turpis sodales aliquet. Praesent volutpat sem non dignissim tempor. Pellentesque consectetur rhoncus feugiat.

Ut ut mauris sed ante mattis aliquam. Cras nec vehicula nisl. In et urna vitae est tristique dignissim eu eu ipsum. Ut mattis scelerisque placerat. Integer eget efficitur velit, interdum scelerisque risus. Donec faucibus eros nunc, sed consectetur sapien viverra in. Phasellus a facilisis purus, non accumsan urna. Sed eget consequat tortor, nec malesuada nisi.

Phasellus et risus hendrerit, ultrices libero ac, blandit felis. Vestibulum tempus felis et mauris dictum laoreet. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque posuere ipsum vel magna ullamcorper imperdiet. In hac habitasse platea dictumst. Sed at pretium ex, ut efficitur ipsum. Mauris tristique erat sit amet aliquam varius. Vivamus tincidunt, mauris ut rutrum tincidunt, magna libero posuere mauris, in pretium nibh justo nec diam. Sed aliquet, sem vel vehicula varius, dui mi dignissim nisi, et porttitor tellus velit in justo. Cras id arcu id libero dignissim porttitor. Nullam nulla elit, vehicula eu eros non, euismod iaculis elit.

Duis quis lorem vel velit finibus efficitur. Integer ornare sodales erat, ut tempor dolor convallis porta. Duis egestas condimentum libero, sed blandit nulla elementum eget.

Nullam fringilla erat dictum pellentesque mollis. Sed ac bibendum ante. Maecenas ac augue nec sem ornare pellentesque. Morbi sollicitudin, lectus imperdiet feugiat lacinia, lorem felis faucibus ipsum, et tincidunt ex neque et diam.

Finding Classification

Each finding is classified as a High, Medium, or Low risk based on Issue2Report considerations of potential threats, the likelihood of attack, and the possible impact of a successful attack against Instructure’s Contoso applications. Each of these factors is assessed individually and in combination to determine the overall risk designation. These assessments are based on Issue2Report professional judgment and experience providing consulting services to enterprises across the country. This report outlines the findings Issue2Report collected from the testing, as well as Issue2Report recommendations that will assist Instructure in reducing its risks and helping remove the vulnerabilities found.

Vulnerabilities and Recomendations

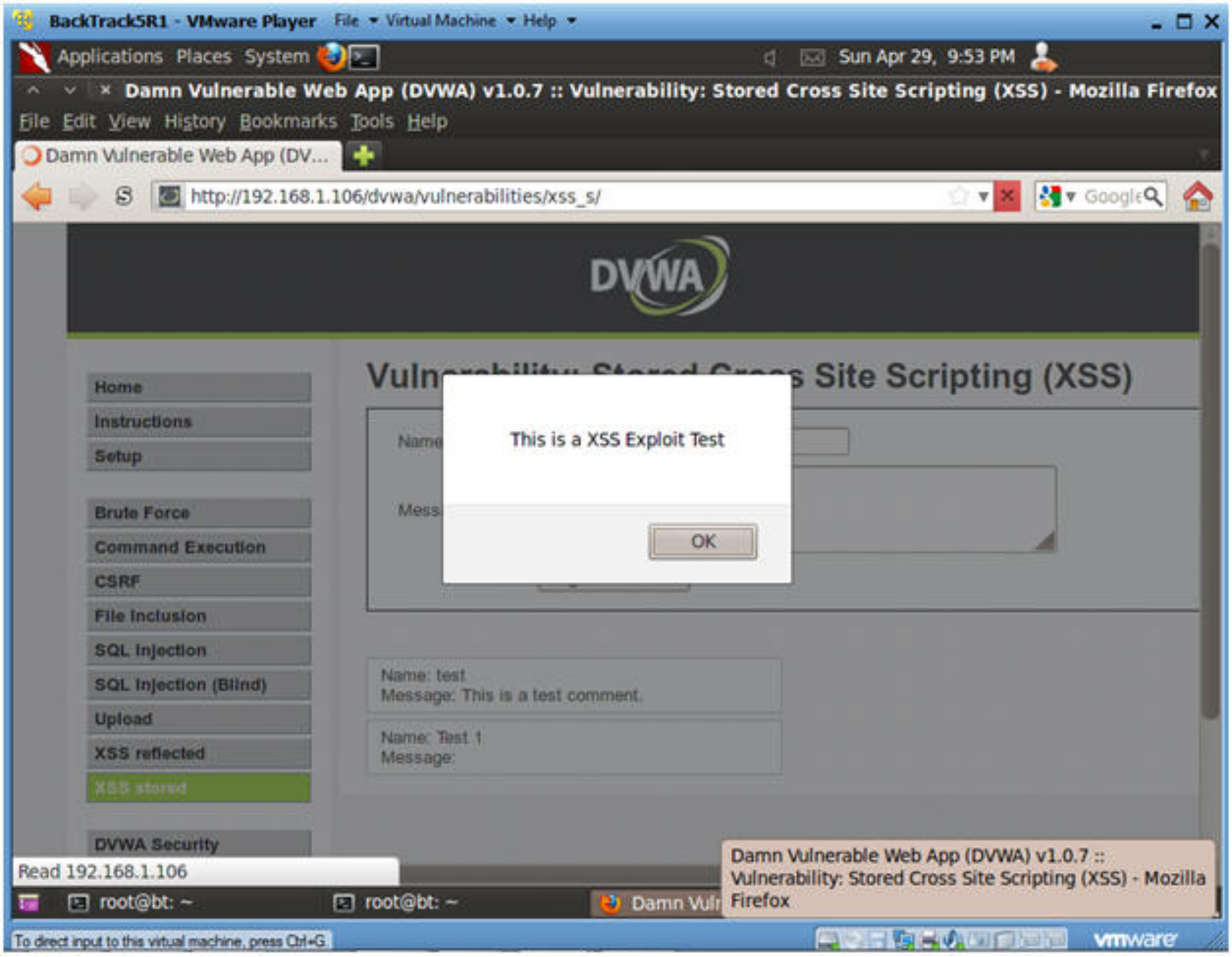
Persistent Cross-Site Scripting

high

Description

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user’s browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.



Damn Vulnerable Web App (DVWA) v1.0.7 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox

http://192.168.1.106/dvwa/vulnerabilities/xss_s/

Vulnerability: Stored Cross Site Scripting (XSS)

This is a XSS Exploit Test

OK

Name: test
Message: This is a test comment.

Name: Test 1
Message:

Read 192.168.1.106

Recomendation

The primary defenses against XSS are described in the OWASP XSS Prevention Cheat Sheet.

Also, it's crucial that you turn off HTTP TRACE support on all web servers. An attacker can steal cookie data via Javascript even when document.cookie is disabled or not supported by the client. This attack is mounted when a user posts a malicious script to a forum so when another user clicks the link, an asynchronous HTTP Trace call is triggered which collects the user's cookie information from the server, and then sends it over to another malicious server that collects the cookie information so the attacker can mount a session hijack attack. This is easily mitigated by removing support for HTTP TRACE on all web servers.

The OWASP ESAPI project has produced a set of reusable security components in several languages, including validation and escaping routines to prevent parameter tampering and the injection of XSS attacks. In addition, the OWASP WebGoat Project training application has lessons on Cross-Site Scripting and data encoding.

Conclusion

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Etiam commodo risus dui, nec porttitor sapien accumsan ac. Sed molestie, quam a blandit varius, ante justo posuere sem, id pulvinar velit orci vitae felis. Morbi rutrum mi eu interdum viverra. Integer pulvinar enim eu magna ullamcorper, vel tempus nisl convallis. Maecenas quis vestibulum nisi. Morbi non mauris in lacus blandit bibendum. Quisque at aliquet enim. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas.

Aliquam id aliquam orci, ut mattis odio. Sed sit amet purus condimentum, luctus tellus eu, vestibulum metus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Vivamus id tincidunt ante. Sed lacinia bibendum mi non eleifend. Sed malesuada lectus eget nulla tristique dapibus at sed quam. Donec tempor, ligula efficitur convallis sodales, eros dolor mattis tellus, fermentum euismod nisl arcu a ante. Proin at dui vitae ipsum dictum viverra. Vestibulum id eros dignissim, mollis orci interdum, dictum orci. Vestibulum facilisis tempus justo eu imperdiet. Integer elementum eu mi sit amet vestibulum. Nunc quis molestie velit. Quisque sed sapien interdum, facilisis sem vitae, lacinia felis. Quisque quam magna, scelerisque sed consectetur vitae, tincidunt in purus. Ut at consequat felis.

Curabitur metus felis, egestas eu arcu a, pulvinar maximus lorem. Aenean orci ex, dictum eu lectus vitae, pulvinar ultricies justo. Aenean placerat dolor vel nunc finibus molestie. Praesent tempus, diam eu aliquet viverra, lacus massa commodo ipsum, sit amet congue nulla arcu eu enim. Maecenas tortor ipsum, interdum nec facilisis ac, laoreet vitae lorem. Suspendisse nec mauris sem. Integer tincidunt feugiat lectus. Aliquam luctus est turpis, sed sodales ipsum dignissim nec. Vivamus fringilla, enim in sodales convallis, tellus lorem consectetur ligula, eu blandit metus risus quis augue.