Columbia Gorge Community College

External Network Tier Two Penetration Test Report

2018 CGCC Pen Test Tier - 2 Test

Test Completed: June 4, 2018
Report Generated: June 4, 2018

1 Executive Summary

As part of an enrollment in Trustwave's Managed Security Testing services, Columbia Gorge Community College engaged Trustwave SpiderLabs to perform an External Network Opportunistic Threat Penetration Test. The primary objective of this security test was to evaluate the resiliency of CGCC's target systems and networks to various attacks launched from the Internet.

Trustwave conducted the test between the dates of May 10 - 31, 2018. Over these dates during the predetermined testing times, a Trustwave consultant analyzed and tested the attack surface of CGCC's target perimeter network by simulating the tactics of a skilled but opportunistic attacker.

The scope was consisted of 254 IPv4 targets. Trustwave was able to identify 11 out of the 254 hosts with open ports which were accepting inbound connections. TCP ports 80, 443 and 22 were found open among the majority of the live hosts. These machines were mainly acting as web servers running on various versions of Unix and Microsoft Windows Operating Systems.

While no vulnerabilities were discovered that led to significant compromise, some security best-practices are not being fully followed. Addressing these issues will further protect the network from attack.

The risk was significantly affected by the exposure of two WebCTRL admin interfaces over the Internet. An adversary can brute force the interface to gain unauthorized access. It should be noted those two hosts did not enforce any transport encryption as a result the login credentials are transmitted in clear text every time a user logs in. An attacker in close proximity or with access to the victim's traffic will be able to easily steal the credentials and compromise the victim's account.

Trustwave also discovered a Cross-site Scripting vulnerability in the web application at https://support.cgcc.edu/Login.aspx. This vulnerability allows attacker code to run within the context of the vulnerable application when accessed by legitimate users through an attacker controlled link. This code could capture the session information, credentials or submitted data of individuals using the application, and allow attackers to impersonate any legitimate actions permitted by those users.

It should be noted that MST Penetration Test reports do not include findings of vulnerabilities that have little likelihood of playing a role in the compromise of target systems or data. Such vulnerabilities receive coverage in MST Maintenance Tests. MST Penetration Tests focus on vulnerabilities actually exploited, or those that could be exploited under a realistic attack scenario that falls outside the scope of testing. Raw vulnerability scan results are included in the Documents section.

New attack techniques are developed on a regular basis, potentially affecting the security of all systems and networks. Similarly, new flaws may be discovered in infrastructure components leading to vulnerabilities in the network through no fault of CGCC. Continuing their current program of regular security testing will help CGCC to avoid these problems.

1.1 Scope

Trustwave used information provided by Columbia Gorge Community College staff to set limits on the scope of the test. Trustwave performed the testing as an external, unauthenticated user with minimal knowledge of the environment (i.e., blackbox testing methods). The rules of engagement followed for all testing included the use of techniques commonly used to exploit vulnerabilities and gain access to systems, but not techniques that intentionally destroy data or harm the ability of devices to function, such as denial of service attacks.

Before the test began, Columbia Gorge Community College provided the Trustwave team with the following information:

Targets

Type	Target
IP Address Range	198.236.191.1 - 198.236.191.254

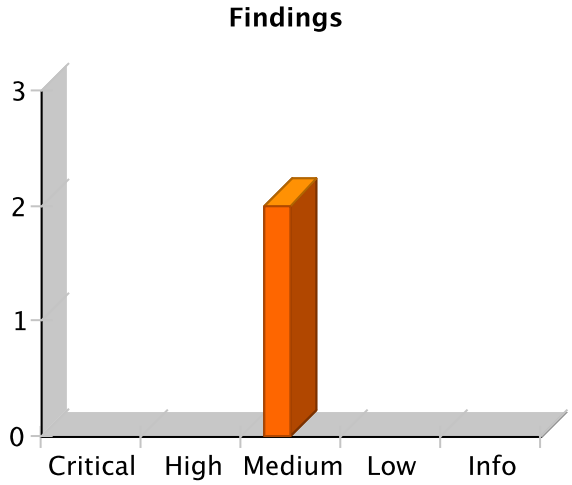
Scope

Scope Limitations	This test was limited in ways that would differentiate the test performed from an actual attack against CGCC by a malicious third-party: only a subset of systems on the perimeter network were tested; certain attack vectors, such as denial of service and social engineering attacks were not utilized; and the test was limited to a very specific time window. An attacker would have no such limitations.

This test was constrained in ways that would differentiate the test performed from an actual attack against Columbia Gorge Community College from an external attacker. These constraints vary by test type, and are described in the Methodology section.

1.2 Results

For the purpose of this test, Trustwave defines a compromise as the ability to either gain unauthorized access to a target system or extract sensitive data from it. Events including, but not limited to, login bypass, ability to run commands on a target system, the extraction of data from an application database, a successful session hijack, successful credential theft, and successful escalation of privileges are considered compromises. A summary of any system or application compromised by Trustwave during testing can be found below. Also documented are significant vulnerabilities discovered that may require an additional attack vector beyond the scope of this engagement in order to leverage a compromise.



Identified Vulnerabilities

ID	Risk Level	Name	Status
PTM-F618372	Medium	Publicly Exposed Administrative Interface	Open
PTM-F617922	Medium	Cross-Site Scripting (XSS), Reflected	Open

1.3 Summary Recommendations

Columbia Gorge Community College's efforts, as evidenced by this test, show a basis for a comprehensive information security program, but weaknesses remain. CGCC should continue a multi-year program of periodic assessments and reviews addressing both technical and policy issues as part of an ongoing information security program.

Trustwave has documented tactical recommendations for the remediation of specific vulnerabilities in later sections of this report. However, based on our cumulative years of experience, industry best practices, and observations documented during testing, we suggest the following strategic actions that CGCC can take to further improve their overall security posture:

- This black-box test did not use any application credentials, and as a result only part of the attack surface of the target web application was exposed. Based on the findings, it is possible there are additional vulnerabilities that lie within the authenticated areas. Trustwave highly recommends a full credentialed application test to find other areas of concern within the vulnerable application.

- Consider implementing a Web Application Firewall (WAF) to provide real-time, continuous application security. These systems can help notify and in many cases protect against common attack vectors such as cross-site scripting plus the data loss that can occur as a result of those attacks.

- Consider external network penetration testing that includes client-side attacks, such as through a targeted phishing exercise, to determine CGCC's resistance to this common attack scenario.

Trustwave is available to help you with any of these issues.

2 Testing Methodology

Trustwave SpiderLabs delivers thousands of safe, actionable, high quality managed validated vulnerability scans and penetration tests each year for clients of all sizes all over the world. Using our proprietary methods and tools to simulate real-world attackers, Trustwave demonstrates actual exploitable vulnerabilities within systems and applications and provides tactical and strategic recommendations for fixing the problem.

Vulnerability scanning is an automated process that provides a broad view of potential weaknesses in target systems. We supplement our vulnerability scanning with the experience and knowledge of our SpiderLabs penetration testers to remove false positives and prioritize each discovered vulnerability by assigning it a realistic risk level.

During our penetration tests, our Trustwave SpiderLabs testers manually analyze targets and then exploit systems in an effort to access target data. Penetration testing focuses on depth over breadth using actual, demonstrable vulnerabilities. Our Attack Sequences show how an attacker can chain together several low-risk weaknesses in the target environment to compromise our clients' systems. Our reports provide actionable guidance on the remediation of findings.

Due to the nature of penetration testing, Trustwave may not locate all vulnerabilities present in the target environment. The aim of testing is to discover and evaluate those vulnerabilities in target systems that are visible to an unauthenticated, remote attacker and most likely to be leveraged for system exploitation. With this concentrated attack simulation, our clients gain insight into the effectiveness of their current controls and how those controls might be circumvented during an actual attack.

Trustwave MST includes maintenance testing consisting of managed vulnerability scans and four tiers of network penetration testing to model four common adversaries in order of increasing sophistication: basic, opportunistic, targeted, and advanced threats.

Maintenance Test

Maintenance testing consists of SpiderLabs experts conducting vulnerability scanning using our proprietary Trustwave Vulnerability Management product. Trustwave's dedicated vulnerability research team writes tests and plug-ins for the Trustwave Vulnerability Management scanning engine to provide coverage for the latest vulnerabilities and help clients assess their exposure to emerging threats. The Trustwave Vulnerability Management scan engine uses OS, protocol and application fingerprinting and other gathered knowledge to provide accurate vulnerability detection.

Trustwave SpiderLabs penetration testing experts then interpret and validate the vulnerability scan results to report on particular findings that an attacker could chain together in order to compromise a system. Unlike a generic vulnerability scan with false positives removed, an MST maintenance test will report only actionable, prioritized findings based on what SpiderLabs penetration testing experts believe pose a real-world threat to the client.

Basic Penetration Test

This is the elementary Trustwave SpiderLabs penetration test, the foundation on which all other testing is built. The Basic test simulates the level of sophistication and tactics of an attacker with minimal skills. These attackers typically use freely available automated attack tools and are sometimes referred to as script kiddies.

Trustwave models the basic threat by using highly tuned, proprietary and open source tools to validate findings through the demonstration of exploitation. As a part of this test, Trustwave SpiderLabs will demonstrate the exploitation of confirmed vulnerabilities that can play a role in the compromise of a target or document a proof-of-concept attack for vulnerabilities that did not lead to a compromise but could contribute to a realistic attack scenario that falls outside the scope of testing. Findings consist of written descriptions and screen shots. All findings include enough detail to allow a technical reader to reproduce the results.

Opportunistic Threat Penetration Test

This test simulates the level of sophistication and tactics of an opportunistic attacker. Opportunistic attackers are a class of cybercriminal motivated by profit, and they will move on quickly if an organization's defenses take significant effort to bypass.

Trustwave models the opportunistic threat by extending the basic test methodology to include additional attack vectors and deeper exploitation. Trustwave will manually investigate the entire attack surface to identify the most likely means of exploitation. If a system can be compromised as a part of the test, Trustwave SpiderLabs will attempt to use the leverage provided by the compromised system to attack other target systems. Findings consist of written descriptions, screen shots, and in some cases video evidence. All findings include enough detail to allow a technical reader to reproduce the results.

Targeted Threat Penetration Test

This test simulates the level of sophistication and tactics of a targeted attacker - a class of cybercriminal that's well funded, sophisticated, somewhat patient and targets specific organizations for large-scale data theft. Targeted attackers are profit-driven and once they choose a target, they'll expend significant effort trying to compromise it.

This test is comprehensive in that any system found adjacent to target systems that Trustwave SpiderLabs can leverage for strategic advantage will be leveraged. This test will also include defined goals such that the scope of the test will include attempting to access specific systems that handle business-critical or high value data

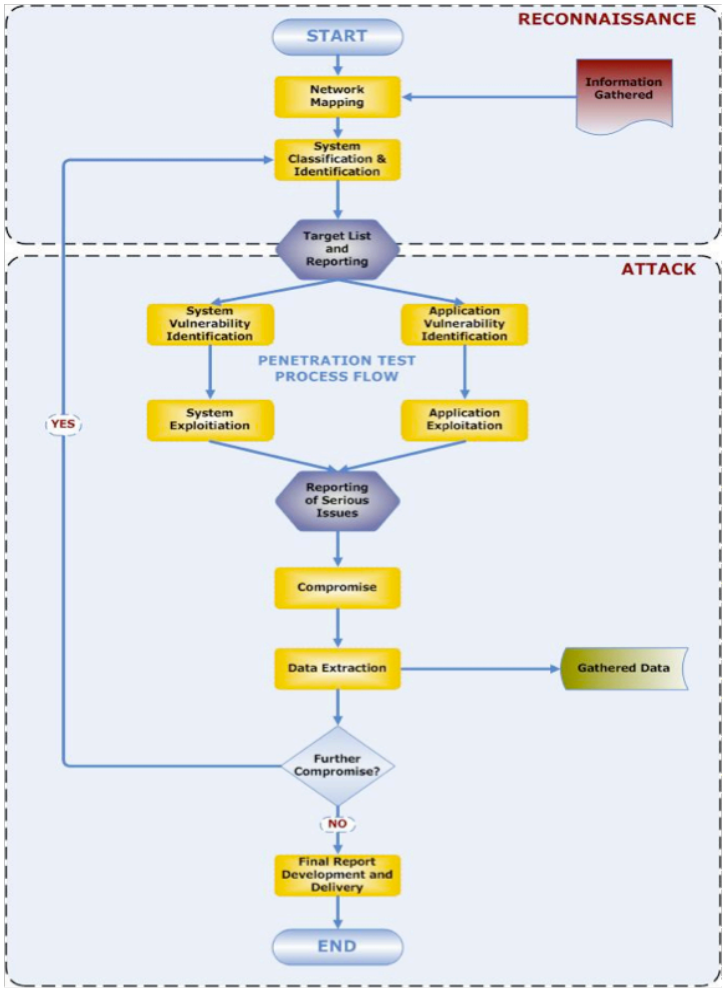
In addition, targeted threat tests introduce social engineering attacks where a SpiderLabs will launch a limited phishing exercise against a defined list of target email addresses. Findings consist of written descriptions, screen shots, and in some cases video evidence. All findings include enough detail to allow a technical reader to reproduce the results.

Advanced Threat Penetration Test

This test simulates a real-world attack by a highly motivated, well-funded and extremely sophisticated attacker who will exhaust all options for compromise before relenting. This test is the most exhaustive and all-encompassing of Trustwave SpiderLabs penetration testing.

This test builds on the targeted threat test, expanding the social engineering vector to include client-side attacks such as malicious updates and browser exploits against a greater sample of users. Where necessary this test will also include attacks against uncommon protocols, and the discovery / exploitation of previously undocumented vulnerabilities.

The advanced threat will not stop at the perimeter and will use all compromised systems and information to attempt to gain access to the internal network. Findings consist of written descriptions, screen shots, and in some cases video evidence. All findings include enough detail to allow a technical reader to reproduce the results.



3 Test Details

3.1 Recon Results

The following table details the results of Trustwave's reconnaissance efforts using the aforementioned techniques. The test team conducted reconnaissance against the addresses listed in Section 1.1's Table of Targets as well as additional hosts discovered and agreed upon in the course of testing.

IP Address	Fully Qualified Domain Name (FQDN)	Operating System Guess	Listening (Open) Ports	Recon Notes / Application URL's
198.236.191.16	ws016.cgcc.cc.or.us	Microsoft Windows Server 2008	1009/tcp, 10176/tcp, 12162/tcp, 12687/tcp, 13519/tcp, 15378/tcp, 16279/tcp, 19081/tcp, 22711/tcp, 26065/tcp, 26477/tcp, 27846/tcp, 28106/tcp, 28177/tcp, 28221/tcp, 28393/tcp, 30917/tcp, 31163/tcp, 31190/tcp, 31390/tcp, 32177/tcp, 32212/tcp, 33142/tcp, 33617/tcp, 33724/tcp, 34334/tcp, 34429/tcp, 35577/tcp, 35959/tcp, 36012/tcp, 36613/tcp, 37131/tcp, 38669/tcp, 39382/tcp, 39458/tcp, 39515/tcp, 40176/tcp, 40649/tcp, 41889/tcp, 42580/tcp, 42622/tcp, 42714/tcp, 47847/tcp, 49324/tcp, 49427/tcp, 50064/tcp, 5115/tcp, 51309/tcp, 51431/tcp, 52012/tcp, 53332/tcp, 54036/tcp, 54458/tcp, 54485/tcp, 54972/tcp, 55341/tcp, 55642/tcp, 56191/tcp, 5704/tcp, 57736/tcp,	- Running a CJServer/ 1.1 on port 80/tcp. - WebCTRL web interface

IP Address	Fully Qualified Domain Name (FQDN)	Operating System Guess	Listening (Open) Ports	Recon Notes / Application URL's
			59084/tcp, 59281/tcp, 60608/tcp, 60610/tcp, 61294/tcp, 62193/tcp, 62956/tcp, 64526/tcp, 64953/tcp, 80/tcp, 8070/tcp, 8705/tcp, 9764/tcp	
198.236.191.81	ws081.cgcc.cc.or.us	Unix	155/tcp, 158/tcp, 162/tcp, 163/tcp, 165/tcp, 166/tcp, 168/tcp, 169/tcp, 170/tcp, 171/tcp, 172/tcp, 173/tcp, 174/tcp, 175/tcp, 176/tcp, 177/tcp, 178/tcp, 179/tcp, 180/tcp, 181/tcp, 182/tcp, 183/tcp, 184/tcp, 185/tcp, 186/tcp, 187/tcp, 188/tcp, 443/tcp, 80/tcp	- Running on Apache Tomcat/7.0.42 - WebCTRL web interface
198.236.191.84	support.cgcc.edu	Microsoft Windows Server 2008 R2	443/tcp, 80/tcp	
198.236.191.92	web2.cgcc.cc.or.us	Unix	80/tcp	
198.236.191.177	web3.cgcc.cc.or.us	Microsoft Windows Server	443/tcp, 80/tcp	Microsoft-IIS
198.236.191.178	web3.cgcc.cc.or.us/	Microsoft Windows Server	443/tcp, 80/tcp	Microsoft-IIS

IP Address	Fully Qualified Domain Name (FQDN)	Operating System Guess	Listening (Open) Ports	Recon Notes / Application URL's
198.236.191.179	ws179.cgcc.cc.or.us	Microsoft Windows Server	114/tcp, 115/tcp, 137/tcp, 138/tcp, 139/tcp, 140/tcp, 141/tcp, 142/tcp, 145/tcp, 146/tcp, 147/tcp, 148/tcp, 149/tcp, 150/tcp, 151/tcp, 152/tcp, 153/tcp, 154/tcp, 155/tcp, 156/tcp, 157/tcp, 158/tcp, 159/tcp, 160/tcp, 161/tcp, 162/tcp, 163/tcp, 164/tcp, 165/tcp, 166/tcp, 167/tcp, 168/tcp, 169/tcp, 170/tcp, 171/tcp, 172/tcp, 173/tcp, 174/tcp, 175/tcp, 176/tcp, 177/tcp, 178/tcp, 179/tcp, 180/tcp, 181/tcp, 182/tcp, 183/tcp, 184/tcp, 185/tcp, 186/tcp, 187/tcp, 443/tcp, 80/tcp	Running Microsoft-IIS/8.5 on port 443/tcp
198.236.191.214	ws214.cgcc.cc.or.us	Unix	22/tcp	
198.236.191.216	ws216.cgcc.cc.or.us	Microsoft Windows Server	121/tcp, 122/tcp, 123/tcp, 124/tcp, 125/tcp, 126/tcp, 127/tcp, 128/tcp, 129/tcp, 175/tcp, 177/tcp, 178/tcp, 179/tcp, 181/tcp, 183/tcp, 184/tcp, 185/tcp, 186/tcp, 188/tcp, 189/tcp, 190/tcp, 191/tcp, 192/tcp, 193/tcp, 194/tcp, 22/tcp, 443/tcp, 80/tcp	

IP Address	Fully Qualified Domain Name (FQDN)	Operating System Guess	Listening (Open) Ports	Recon Notes / Application URL's
198.236.191.234	xenapp.cgcc.cc.or.us	Citrix	158/tcp, 161/tcp, 162/tcp, 165/tcp, 166/tcp, 167/tcp, 168/tcp, 169/tcp, 170/tcp, 171/tcp, 172/tcp, 173/tcp, 174/tcp, 175/tcp, 176/tcp, 177/tcp, 178/tcp, 179/tcp, 180/tcp, 181/tcp, 182/tcp, 183/tcp, 184/tcp, 185/tcp, 186/tcp, 187/tcp, 188/tcp, 443/tcp, 80/tcp	Citrix NetScaler
198.236.191.253	live-cgccedu.pantheonsite.io, www.cgcc.cc.or.us	Microsoft Windows Server 2003	161/tcp, 162/tcp, 163/tcp, 166/tcp, 167/tcp, 168/tcp, 169/tcp, 170/tcp, 171/tcp, 172/tcp, 173/tcp, 174/tcp, 175/tcp, 176/tcp, 177/tcp, 178/tcp, 179/tcp, 180/tcp, 181/tcp, 182/tcp, 183/tcp, 184/tcp, 185/tcp, 186/tcp, 187/tcp, 188/tcp, 21/tcp, 80/tcp	

3.2 Narrative

There is no narrative for this test.

4 System Exploitation and Vulnerability Report

4.1 Risk Assessment

The following table categorizes the risk level of issues presented in this report:

Risk Level	Definition
Critical	• The attack scenario tested in this exercise succeeded and resulted in a systems compromise. • Exploitation impacts production systems without requiring valid authentication. • Exploitation is trivial. • Successful exploitation results in a large-scale loss of customer or cardholder information. • No controls to prevent the exploit are present, or controls to prevent the vulnerability from being exploited are ineffective. • A strong need for immediate corrective measures exists.

High	• The attack scenario tested in this exercise succeeded, and resulted in a systems compromise.
	• Technical vulnerability details and/or exploit code are publicly available.
	• Exploitation is trivial.
	• An additional attack vector may be needed to craft a successful attack using this exploit, but that vector is also trivial.
	• No controls to prevent the exploit are present or controls to prevent the vulnerability from being exploited are ineffective.
	• Exploitation of the vulnerability:
	  • may result in the highly costly loss of major tangible assets or resources,
	  • may significantly violate, harm, or impede the organization's mission, reputation, or interests.
	• A strong need for corrective measures exists.

Medium	• Exploitation requires a skilled attacker.
	• Exploitation does not result in elevated privileges.
	• Controls are in place that may impede successful exploitation of the vulnerability.
	• To craft a successful attack using this exploit/vulnerability an additional vector is needed (such as phishing or social engineering).
	• Exploitation of the vulnerability:
	  • may result in the costly loss of tangible assets or resources,
	  • may violate, harm, or impede the organization's mission, reputation, or interests.
	• Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.

Low	• Exploitation is extremely difficult. • Controls are in place to prevent, or at least significantly impede, the vulnerability from being exploited. • The attack scenario under which this vulnerability can be exploited is possible, but extremely unlikely. • The system's accrediting authority must determine whether corrective actions are required or decide to accept the risk.
Informational	• Information disclosed may be of interest to an attacker • The information disclosed will be useful to an attacker should a higher risk issue be found that allows for a system exploit • Information is disclosed that is necessary to carry out an attack • The vulnerability could not be exploited during the engagement, but could present a more significant risk given other techniques or attack vectors. • The vulnerability could not be exploited during the engagement, but could present a more significant risk given other techniques or attack vectors.

4.2 Findings

This section provides details regarding noteworthy vulnerabilities that were identified during testing.

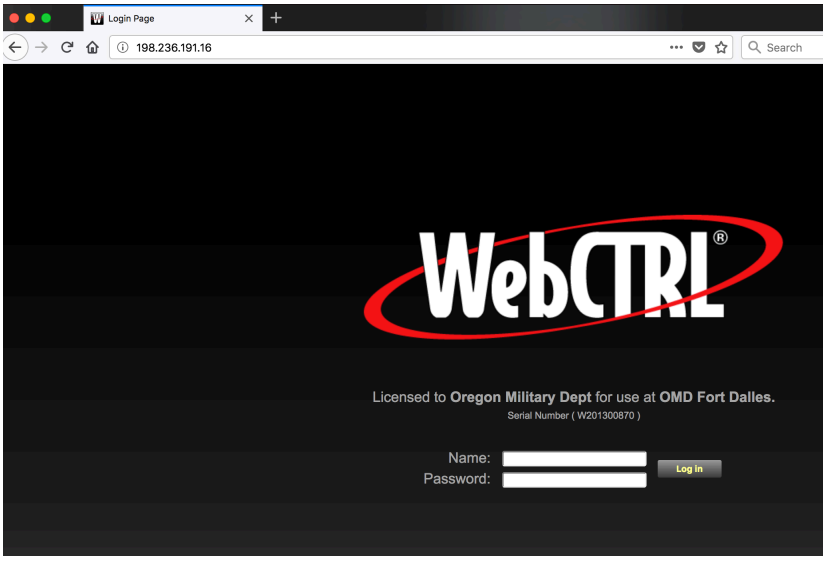
ID	PTM-F618372		
Name	Publicly Exposed Administrative Interface		
Risk Level	Medium	**Status**	Open
Opened Date	6/4/2018	**Closed Date**	
Impact	Privilege Escalation		
Data Exposure			
Location	http://198.236.191.81, http://198.236.191.16		
CVSS Overall Score			
CVSS Vector			

Description:

- Trustwave discovered WebCTRL administrative interfaces at the URLs listed above.
- Generally speaking, administrative interfaces should not be exposed publicly; this significantly increases the attack surface of the application.
- Flaws in a private administrative interface with a relatively minor impact could become a major risk when exposed to the entire Internet.
- These services are also prone to brute force password guessing attacks if not configured to use 2 factor authentication. Attempts to guess valid credentials were unsuccessful during the limited timeframe of this engagement, but could present a future risk to the organisation.
- Equally, if credentials are captured via other means, these interfaces can exacerbate the severity of the situation by providing a means to use them to gain access into the internal network.
- In particular the risk was increased to Medium since the WebCTRL is a web based building automation system which manages sensitive infrastructure.

Evidence:

WebCtrl server is accessible over the internet. An adversary bypassing the authentication controls will be able to control and discrupt senstive electronic components (LGR routers, Controllers) which are managed by the software.



Recommendation:

- It is a best-practice to keep all administrative interfaces on private networks.
- If an administrative interface must be on an Internet-facing website, consider limiting access to specific IP addresses or utilizing two-factor authentication.
- Perform credentialed penetration tests of all publicly-exposed administrative interfaces.

References:

OWASP	https://www.owasp.org/index.php/Category:Access_Control
Top 10 2014-I6 Insecure Cloud Interface	https://www.owasp.org/index.php/Top_10_2014-I6_Insecure_Cloud_Interface

ID	PTM-F617922		
Name	Cross-Site Scripting (XSS), Reflected		
Risk Level	Medium	**Status**	Open
Opened Date	6/4/2018	**Closed Date**	
Impact	Integrity Violation		
Data Exposure			
Location	See Description		
CVSS Overall Score			
CVSS Vector			

Description:

- The application is vulnerable to Cross-Site Scripting (XSS) attacks. This occurs when web applications do not properly validate user-supplied inputs before including them in dynamic web pages.
- By modifying the user-supplied data described below, Trustwave was able to inject arbitrary HTML in the application.
- Exploiting this issue allows an attacker to define arbitrary client-side code (typically JavaScript) that will ultimately be rendered and executed by the end user's web browser.
- This type of attack may be used to steal sensitive information such as usernames and passwords, perform session hijacking, remotely control or monitor the user's browser, or impersonate a web page used to gather order information, including credit card numbers.

Location 1: https://support.cgcc.edu/Login.aspx
HTTP Method: GET
Authentication: Not Required
Vulnerable Parameter(s): brand
Sample Payload: " onload="alert(2018)" "
Example Attack: https://support.cgcc.edu/Login.aspx?form=&brand=**%22%20onload=%22alert(2018)%22%20%22**&updatesplash=

Evidence:

The following evidence includes a sample request and response pair. The injected Proof of Concept (PoC) JavaScript was returned in the server's resposne.

Request:

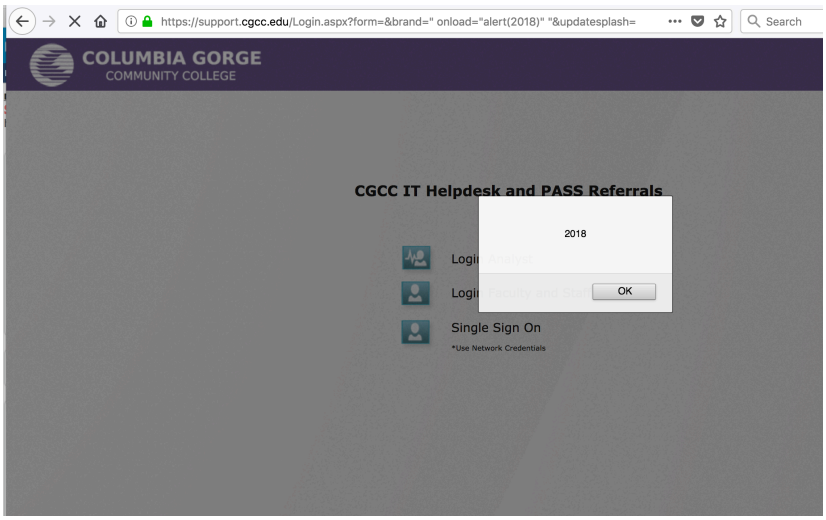
```
GET /Login.aspx?form=&brand=%22%20onload=%22alert(2018)%22%20%22&updatesplash= HTTP/1.1
Host: support.cgcc.edu
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.12; rv:58.0) Gecko/20100101 Firefox/58.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: ASP.NET_SessionId=t1axw2jsldz4pj4bc1et0p4r
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1
```

Response:

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache,no-cache
Content-Type: text/html; charset=utf-8
Expires: -1
Vary: Accept-Encoding
Server: Microsoft-IIS/7.5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Fri, 01 Jun 2018 09:02:49 GMT
Connection: close
Content-Length: 846

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head id="Head1" profile="http://www.w3.org/2005/10/profile"><title>
CGCC HelpDesk
</title><link rel="shortcut icon" type="image/x-icon" href="Application_Images/Login/favicon.ico" /><link rel="Bookmark" type="image/x-icon" href="Application_Images/Login/favicon.ico" /></head>
<frameset rows="65,*" frameborder="0" framespacing="0">
<frame name="banner" noResize scrolling="no" src="Banner.aspx?brand=" onload="alert(2018)" "&login="">
<frame name="main" src="LoginList.aspx?form=&brand=" onload="alert(2018)" "">
<noframes><p align="center"><font face="Arial">Minimum Requirement: Internet Explorer 5.0 Or Later</font></p></noframes>
</frameset>
</html>
```

A screenshot showing the generated PoC XSS.



Recommendation:

- Mark cookies as "Secure" and "HTTP-Only" where appropriate to minimize the impact of cross-site scripting attacks.
- Before using any user-supplied data, validate its format and reject any characters that are not explicitly allowed (i.e. a white-list). This list should be as restrictive as possible.
- Before using any data (stored or user-supplied) to generate web page content, escape all non alpha-numeric characters (i. e. output-validation). This is particularly important when the original source of data is beyond the control of the application. Even if the source of the data isn't performing input-validation, output-validation will still prevent XSS. This can be done by converting characters to “&#nn;” (ignore the quotes), where “nn” is the hexadecimal ASCII character number.

References:

OWASP	http://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

5 Contacts

5.1 Columbia Gorge Community College Contacts

Role	First Name	Last Name	Email	Phone
Project Manager	Rich	Jepson	rjepson@cgcc.edu	541 506 6096

5.2 Trustwave Consultants

First Name	Last Name	Email	Phone
Andreas	Georgiou	AGeorgiou@trustwave.com	+44 2070 705985

6 About Trustwave and SpiderLabs

6.1 About Trustwave

Trustwave helps businesses fight cybercrime, protect data and reduce security risks. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs while safely embracing business imperatives including big data, BYOD and social media. More than 2.5 million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective data protection, risk management and threat intelligence. Trustwave is a privately held company, headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit www.trustwave.com.

6.2 About SpiderLabs

SpiderLabs® is the advanced security team at Trustwave focused on incident response, network penetration testing, physical security, application security, and security research. SpiderLabs provides thought leadership to the entire Trustwave organization and our clients. SpiderLabs has responded to thousands of security incidents, performed thousands of penetration tests and tested the security of thousands of business applications for organizations ranging from the largest companies in the world to nimble start-ups. Members of the SpiderLabs teams are frequently asked to speak at global security conferences such as Black Hat, OWASP, SANS, and DEFCON. For more information, visit https://www.trustwave.com/spiderlabs.

6.3 SpiderLabs Qualifications

Businesses worldwide depend on the global SpiderLabs team at Trustwave to keep them ahead of the latest security threats. Our security breach investigations, malware reverse-engineering projects, millions of scans, thousands of penetration tests, leadership of open-source security projects and contributions to the security community have established Trustwave SpiderLabs as world-renowned experts on the past, present and future of security.

Our SpiderLabs experts have an average of 12 years of experience in the industry, possess numerous industry-recognized certifications, are distributed across ten countries and include penetration testers, incident responders, forensic investigators, malware reverse-engineers, security researchers, published authors and sought-after speakers. We recruit and hire top members of the community who speak regularly at industry events such as Black Hat, DEF CON, RSA, Shmoocon, Toorcon, SOURCE, SecTor, SANS and more.

The SpiderLabs team also makes pivotal contributions to the information security community through the annual Trustwave Global Security Report, security tools maintained at the SpiderLabs GitHub page, serving as officers for a number of security organizations (like OWASP, Infragard, B-Sides and others), and the SpiderLabs blog, which features original research, attack techniques, and trend analysis. Our findings are also regularly featured in major media outlets such as CNN, MSNBC, CNBC, The Wall Street Journal, Fox News Channel, and CBS Evening News among others.