

# Information Security Audit Report

---



May 9, 2022

GABRIELLE DECKER | MICHAEL PHAM

**Information Security Audit Report**

**Prepared for**



## Table of Contents

<b>Table of Contents</b> .....	<b>2</b>
<b>1 Executive Summary</b> .....	<b>3</b>
<b>2 Introduction</b> .....	<b>3</b>
2.1 Background .....	3
2.2 Objective .....	3
2.3 Scope .....	4
2.4 Disclaimer .....	4
<b>3 Methodology</b> .....	<b>5</b>
3.1 Identification and Analysis .....	5
3.2 Vulnerability Detection .....	5
3.3 Reporting .....	6
3.4 Standards .....	6
<b>4 Findings</b> .....	<b>7</b>
4.1 Physical .....	7
4.2 Logical .....	9
4.3 Application .....	10
<b>5 Appendix</b> .....	<b>15</b>
5.1 Evidence for ID 9 .....	15
5.2 Evidence for ID 10 .....	16
5.3 Evidence for ID 13 .....	16
5.4 Evidence for ID 14 .....	17
5.5 Evidence for ID 15 .....	17
5.6 FGDS Script .....	17
5.7 FGDS Results .....	18
5.8 WindowsManagerConfiguration.xml .....	18

## 1 Executive Summary

Gabrielle Decker and Michael Pham ("we" or "us") were invited to conduct a cyber security audit and review on the [REDACTED] on May 6, 2022. The objective of this audit was to obtain practical experience in discovering and identifying exploitable vulnerabilities within an organization.

In Section 4, we provide explanations and recommendations of our findings. The recommendations can be classified as Physical (P), Logical (L), and Application (A).

The results of the assessment suggest that [REDACTED] overall security posture fulfills federal criteria and that basic security mechanisms are in place to deter potential attacks. However, [REDACTED] has vulnerabilities that leave it open to attacks with expensive consequences.

We conclude, within our limitations, that while [REDACTED] physical security meets standards, web security was lacking many essential safeguards for modern deterrence of malicious actors. While not overtly obvious, this poses as much a threat to operational security as incidents [REDACTED].

## 2 Introduction

As described in the "Scope," we conducted a security audit of the [REDACTED]. This document details the assessment's findings. The security evaluation began and ended on May 6 of 2022 and was due for completion by May 13, 2022. The objective of the assessment was to find security risks and propose recommendations for their remediation.

Basic observation, group discussion, and suggestions from our course professor were used to identify issues. Although the observed issues were evaluated, formal severity categorization is beyond the scope of the assignment and will not be provided in this paper. In this security report, corrective measures to mitigate the risks associated with discovered security issues are presented.

### 2.1 Background

We are Information Technology ("IT") students at the assessed organization, and the audit was assigned by Dr. John McHenry, professor of Principles of Information Security.

### 2.2 Objective

The assessment's aim is to provide a reliable opinion on [REDACTED] security posture to the best of our ability and within the boundaries of the assignment. The assessment identifies and quantifies weaknesses and vulnerabilities so they can be managed and addressed, thereby helping to:

- Prevent malfunction and/or financial loss due to fraud or unreliable infrastructure
- Provide due diligence to management and stakeholders

- Protect [REDACTED] against reputation loss.

### 2.3 Scope

Dr. McHenry led our physical security audit of [REDACTED] as part of the course. We investigated potential attack vectors and other threats to organizational information assets and documented our observations. Typical areas that are restricted, locked, or otherwise off-limits to students were not assessed, but any observations made were recorded. Observed areas include:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

A cyber security examination was conducted in two stages.

The first was conducted in a conference room delegated by Dr. McHenry immediately after the physical assessment. Systems were examined for vulnerabilities using the computers in the conference room. We were instructed to look for potential attack vectors but forbidden from attempting to breach any resistance if we were denied access.

After the group discussion, the second audit was conducted utilizing public open-source tools and simple searches on [REDACTED] internet-facing website. We followed all the rules and restrictions indicated in the conference room in our second evaluation as well.

The tools and their findings are included in the Appendix.

### 2.4 Disclaimer

The audit disclosed is not a legal audit and should not be regarded as such. Our recommendations, on the other hand, are legitimate and are based on the knowledge we received while attending [REDACTED]. We do not claim to be experts, and any recommendations would require review from official [REDACTED] staff.

Because time and resources are limited in any authorized audit or assessment, the existence of vulnerabilities and weaknesses can be verified, but the absence of vulnerabilities cannot be guaranteed.

In this context, while we made every effort to audit and assess the systems using our best abilities, knowledge, and beliefs, this report does not guarantee the establishment of an impenetrable system, nor can we guarantee with professional certainty that the risks listed in this

document pose a current and valid threat. We are not licensed as of the audit date, and any guarantees would be a gross irresponsibility that could jeopardize our prospective professions. Furthermore, the audit was not a comprehensive examination, and any identified risks were not investigated in relation to their context within the system as a whole.

### 3 Methodology

The following steps were conducted to deliver a comprehensive opinion regarding effectiveness and adequacy of the security controls of organizational systems:

- Threat Identification: Identification of threats and potential attack surface
- Vulnerability Detection: Evaluation of current security posture
- Reporting: Determination and reporting of appropriate measures to eliminate or minimize risk



Figure 3

#### 3.1 Identification and Analysis

The first phase of the audit focused on acquiring, analyzing, and organizing information about the items in scope, primarily using passive analysis techniques. In addition, relevant information on the target area was retrieved from public sources such as websites and search engines. This was done to identify the environment's attack surface and gather information for the subsequent testing phases. To adopt and direct the manual testing techniques, potential risks were identified and classified by type.

#### 3.2 Vulnerability Detection

To identify potential vulnerabilities, we integrated automated and manual testing methods. Using scripts accelerates and improves the discovery of known security issues.

The external tools utilized for this assessment are publicly accessible and have been approved by credible information security groups and specialists. The tools used include:

- Browser-based website toolset from <https://geekflare.com/>
- Browser-based vulnerability scanners from <https://observatory.mozilla.org/>
- The OSINT script "Fast Google Dorks Scan" by Ivan Glinkin, one of the top ten on the Global World Ethical Hacking Leaderboard. The tool's URL can be found on his personal website, <https://www.ivanglinkin.com/>. The source code can be found at <https://github.com/IvanGlinkin/Fast-Google-Dorks-Scan>.

In terms of search parameters, the public URL of the [REDACTED] website, [REDACTED] was all that was used. There was no additional research nor investigation, and the OSINT script only returns Google results. The results of these tests should be carefully evaluated. A quick search revealed the information provided, making it an easy step in the footprinting process for possible attackers.

### 3.3 Reporting

The assessment results are documented and provided in the form of an audit report. The report includes an executive summary detailing the environment's overall security posture, in addition to key findings, a review of the environment in scope, a description of the assessment methodology and work performed, and a complete list of findings and recommendations.

### 3.4 Standards

Within our constraints, we conducted assurance work in line with the Information Technology Assurance Framework ("ITAF"), a recognized standard for conducting IT assurance issued by the Information Systems Audit and Control Association ("ISACA"). From a technological standpoint, we adhere to industry security requirements for information systems in accordance with the National Institute of Standards and Technology ("NIST") Cybersecurity Framework ("CSF"). Other frameworks exist, each with its own set of advantages and disadvantages for educational institution use cases.

Furthermore, the purpose of this assessment is to provide practical and actionable measures that [REDACTED] leaders can take to decrease the cybersecurity risks they face. It is not intended to be a replacement for any other compliance testing and reporting that [REDACTED] may be familiar with. Rather, it should be viewed as additive, with any recommendations considering [REDACTED] specific context, requirements, resources, and ambitions.

## 4 Findings

### 4.1 Physical

ID 1	
<b>Title</b>	Surveillance
<b>Description</b>	There were no cameras in the entry annex of the main building. There were no security guards or police officers present during the audit, raising the question of whether cameras, if existent, were being watched.
<b>Recommendation</b>	██████████ should assess their surveillance strategy and determine if monitoring needs to be reconfigured. We feel that special care should be taken in regions that are not easily seen from main areas, such as remote corners and around corners, because these are ideal places for a crime to go unnoticed. Also, if there is a staff deficit, we propose that ██████████ management conduct thorough searches for qualified candidates to fill open positions through job postings, adverts, or career fairs.

ID 2	
<b>Title</b>	Hardware
<b>Description</b>	There were no locks nor intrusion detection systems discovered on kiosk PCs, allowing an attacker entry to the system's internal components. Furthermore, the kiosks had open USB ports, though we were unable to determine whether these were disabled. Many of the workstations in the financial aid hallway had their back panels facing public areas, making them easily accessible. There were numerous open ethernet/RJ-45 ports. Many exposed wires were found in a ceiling panel above the maintenance closet in the main building's automotive division, posing both a physical and security issue.
<b>Recommendation</b>	All public kiosks/computers should have intrusion detection systems installed on their chassis. If these machines' USB ports haven't already been disabled, they should be disabled immediately. All RJ-45 ports that are not in use should be disabled or locked to prevent unauthorized network access. All wiring in the ceiling panel of the automotive section should be inspected, and the ceiling tile should be replaced.

ID 3	
<b>Title</b>	Employee Awareness
<b>Description</b>	We discovered numerous unattended workstations with insufficient surveillance. Furthermore, most of them had post-it notes and open



<p><b>Recommendation</b></p>	<p>software in their work areas, which makes it simple for a malicious actor to steal information. This might be a [REDACTED] violation.                  The call center was extremely secure, and staff awareness was high.                  We propose tougher workspace policies and management follow-through. If [REDACTED] stakeholders do not want to risk losing federal funding due to [REDACTED] violations, this should be strictly enforced. In addition to standard security awareness training, all staff should receive instruction on impersonation tactics and tailgating.</p>
------------------------------	--

ID	4
<p><b>Title</b></p> <p><b>Description</b></p>	<p>Public Exposure                  Personal phone numbers and addresses were posted on public bulletin boards. Most of them had no [REDACTED] approval. The [REDACTED] had cluttered desks and boxes, providing an information and fire danger. The [REDACTED] offered a plethora of information but no barriers to prevent shoulder surfing. Classroom 1N2 had nobody inside, but the computer was still projecting to a large screen. Additionally, it was still logged in and no screensaver was set. Although the room was locked, any passer-by could see what was on the screen. If an email notification popped up, it just became public information. We spotted [REDACTED] that had stained glass windows in the door to prevent anyone from peering inside. Good!</p>
<p><b>Recommendation</b></p>	<p>Reminders should be sent out to [REDACTED] reminding them of Policy No. [REDACTED] and Policy No. [REDACTED]. Management should review Policy No. [REDACTED] and determine risk appetite for fire hazards and, as per the policy, adhere to provision [REDACTED].</p>

ID	5
<p><b>Title</b></p> <p><b>Description</b></p>	<p>Appliances                  Many unprotected thermostats were discovered throughout the [REDACTED]. This exposes them to tampering, which could result in extreme price fluctuations and safety issues. There were no locks or securing mechanisms found on TVs and similar electronics, significantly increasing the potential of theft. Due to the wireless adapters installed, vending machines with credit card capabilities may pose a risk with card readers.</p>

<b>Recommendation</b>	Maintenance should be performed on a regular basis to ensure that all unsecured thermostats are dummies. It would be preferable to either remove them entirely or confine them within a cage. Cable locks should be fitted on all televisions and vendors must ensure that any software updates or hardware fixes are completed as soon as is feasible.
-----------------------	---

## 4.2 Logical

<b>ID</b>	<b>6</b>
<b>Title</b>	System Configuration
<b>Description</b>	The Windows Defender Firewall was turned off. In both private and public networks, inbound connections that do not match a rule are not blocked. Basic [REDACTED] accounts can alter their DNS server addresses. The bandwidth can be changed. SSL Cipher Suites are modifiable. Services that are currently running can be viewed and modified. New user accounts can be created locally.
<b>Recommendation</b>	Access control policies must be examined, and user permissions be updated to restrict access to certain instances. We are aware that when computers are logged out, all settings are reset. However, this does not eliminate the risks. There are numerous exploits that can achieve privilege escalation to make changes permanent and system wide. This is especially true when paired with the USB vulnerabilities discussed in ID 2 (P) of section 5.1. The principle of least privilege should also apply to what is visible to users.

<b>ID</b>	<b>7</b>
<b>Title</b>	System Administration
<b>Description</b>	The password policy cannot be changed. Good! Guest networks do not have a user agreement page that must be accepted before a user may connect to the network. We are aware of policy No. [REDACTED], but the guest network is open, and the policy is not as accessible. This increases the risk of liability in the event of a lawsuit.
<b>Recommendation</b>	[REDACTED] should implement a guest wireless Terms of Use page to reduce the risk of [REDACTED] being held responsible in the event someone uses the network for illicit purposes.

### 4.3 Application

ID	8
<b>Title</b>	Nginx Server
<b>Description</b>	Vulnerability scanners did not detect cPanel or Webmail, which is good. Because no further testing could be completed, we offer general recommendations for Nginx servers. On April 9, 2020, hackers publicly disclosed a vulnerability in NGINX LDAP reference implementations. Input is not sanitized by the Python daemon. As a result, an attacker can utilize a specially constructed request header to circumvent the group membership (memberOf) check, allowing them to authenticate even if they are not members of the required groups.
<b>Recommendation</b>	Leave the location = /auth-proxy block of the NGINX configuration empty. Additionally, make sure all optional options are empty. Remove special characters from the username field. It must remove the opening and closing parenthesis () and the equal symbol =, which are uniquely important for LDAP servers.

ID	9
<b>Title</b>	Security Headers
<b>Description</b>	<p>The public-facing website ██████████ was missing many security headers. This makes it highly vulnerable to attacks, which could result in legal ramifications if any information is exposed, loss of federal funds, and reputation damage if ██████████ or vendors no longer feel comfortable on ██████████ or online.</p> <p>The X-Powered-By header, however, gives information about the server's specific technology. This information could be used by an attacker to launch targeted attacks against the detected software type and version. The Appendix contains evidence.</p>
<b>Recommendation</b>	<p>The following headers should be added to the nginx.conf file:</p> <pre>Strict-Transport-Security: max-age=&lt;seconds&gt;[; includeSubDomains] Content-Security-Policy: upgrade-insecure-requests; add_header X-Frame-Options "SAMEORIGIN" always; X-XSS-Protection: 1; mode=block; X-Content-Type-Options: nosniff; add_header Referrer-Policy "strict-origin-when-cross-origin";</pre> <p>Information that allows the identification of software platform, technology, server, and operating system: HTTP server headers, HTML meta information, etc. should be removed or hidden.</p>

ID	10
<b>Title</b>	Admin Console

<b>URL</b>	https://[REDACTED]edu/wp-login
<b>Description</b>	The WordPress admin console is exposed and easily detected by vulnerability scanners. By exposing the admin console, hackers may attempt to log in as the administrator via brute force. The Appendix contains evidence.
<b>Recommendation</b>	[REDACTED] should change the default admin console URL to prevent brute force attacks.

ID 11	
<b>Title</b>	XML-RPC
<b>URL</b>	https://[REDACTED]/xmlrpc.php
<b>Description</b>	A web browser is not required to use the XML-RPC API. Attackers use this channel to remotely access and modify WordPress sites. If XML-RPC is not disabled, hackers can repeatedly attempt to log in until they succeed.
<b>Recommendation</b>	The [REDACTED] should either remove the xml-rpc.php file from the root of the WP folder or disable XML-RPC for all IPs except known valid IPs. Basic syntax is shown below. <pre>&lt;FilesMatch "xmlrpc\.php\$"&gt;   order deny,allow   deny from all   allow from 1.2.3.4 &lt;/FilesMatch&gt;</pre>

ID 12	
<b>Title</b>	WP-Cron
<b>URL</b>	https://[REDACTED]/wp-cron.php
<b>Description</b>	On a medium or larger site, WP-Cron doubles the current traffic on the website and creates a simple DDoS attack against itself. This is because the cron uses HTTP to execute several times each minute. The HTTP request adds overhead by generating, negotiating, and establishing a network socket. It also affects the web server's effective capacity.
<b>Recommendation</b>	It should not be the default behavior because it can easily be misused or converted into an attack vector on a server. The only alternative is to set up a regular system cronjob to run the wp-cron.php script every minute to ensure that scheduled tasks are done on time. To prevent overloading the web server's capacity or adding to the network layer's memory overhead, it should be done via PHP rather than HTTP. To do so, [REDACTED] should add the following to the wp-cronfig.php file: <pre>define('DISABLE_WP_CRON', true);</pre> This new setting should be inserted in the file just after the DB_COLLATE database line which looks like the following <pre>define('DB_COLLATE', '');</pre>

To learn how to set up a system cron job, read the cPanel documentation here: <https://documentation.cpanel.net/display/70Docs/Cron+Jobs>.

ID	13
<b>Title</b>	Subresource Integrity
<b>Description</b>	JavaScript scripts and stylesheets stored on content delivery networks (CDNs) are protected by SRI. SRI is not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via <code>src="/..."</code>
<b>Recommendation</b>	Evidence is given in the Appendix. All external JavaScript resources loaded from non-Mozilla systems must use subresource integrity. Set the Access-Control-Allow-Origin header to enable SRI.

ID	14
<b>Title</b>	Windows Manager Configuration
<b>Description</b>	In the results, the FGDS produced the WindowsManagerConfiguration.xml file. We were able to download the file, which contained the following information. Only a portion of the results are displayed due to the length of the results. The whole file is included in the Appendix, along with a screen capture of a section of the FGDS scan and its full file.

```

1 <!--*****Confidential and Proprietary*****
2 * File Name: WindowsManagerConfiguration.xml
3 *****Copyright (c) Hyland Software, Inc. 1991-2015*****
4 <WindowEvent TYPE="DocumentQuery">
5 |   <Setting TYPE="target">frmViewer</Setting>
6 |   <Setting TYPE="action">DocSelectPage.aspx</Setting>
7 </WindowEvent>
8 ...
9 <WindowEvent TYPE="UserAdministration">
10 | <Setting TYPE="target">frmViewer</Setting>
11 | <Setting TYPE="action">Admin/UserAdministration.aspx</Setting>
12 </WindowEvent>
13 <WindowEvent TYPE="DisplayDistributionRecipients">
14 | <Setting TYPE="target">frmViewer</Setting>
15 | <Setting TYPE="action">Admin/DistributionRecipients.aspx</Setting>
16 </WindowEvent>
17 <WindowEvent TYPE="EditDistributionRecipients">
18 | <Setting TYPE="target">_blank</Setting>
19 | <Setting TYPE="action">Admin/EditRecipient.aspx</Setting>
20 </WindowEvent>
21 <WindowEvent TYPE="ExecuteCustomQuery">
22 | <Setting TYPE="target">frmViewer</Setting>
23 | <Setting TYPE="action">DocSelectPage.aspx</Setting>
24 </WindowEvent>
25 <WindowEvent TYPE="ExecuteEFormCustomQuery">
26 | <Setting TYPE="target">_blank</Setting>
27 | <Setting TYPE="action">DocSelectPage.aspx</Setting>
28 </WindowEvent>
29 ...
30 <WindowEvent TYPE="DatamineRedirect">
31 | <Setting TYPE="target">dataMineRedir</Setting>
32 | <Setting TYPE="action">DataMineRedirect.aspx</Setting>
33 </WindowEvent>
34 <WindowEvent TYPE="OpenDigitalSignatures">
35 | <Setting TYPE="target">_blank</Setting>
36 | <Setting TYPE="action">applets/DigitalSignaturesHost.aspx</Setting>
37 </WindowEvent>
38 ...
39 <WindowEvent TYPE="ConfigurePortalNewLayout">
40 | <Setting TYPE="target">frmViewer</Setting>
41 | <Setting TYPE="action">Portal/Portal.aspx</Setting>
42 </WindowEvent>
43 ...
44 <WindowEvent TYPE="LockAdministration">
45 | <Setting TYPE="target">frmViewer</Setting>
46 | <Setting TYPE="action">LockGrid.aspx</Setting>
47 </WindowEvent>

```

**Recommendation**





















We were unable to confirm whether this document was still relevant due to scope constraints. However, even if this configuration file was obsolete and no longer in use, it could provide insight into what system configurations are present, and an attacker could use basic pattern guessing to deduce the current configuration. We believe this file was available on Google due to incorrect server header configuration.

Correctly implementing server headers as indicated in ID 9 (A) may reduce this danger, but all security settings should be examined to ensure that no data that [REDACTED] did not intend to disclose is being released.

<b>ID</b>	<b>15</b>
<b>Title</b>	Website Application Firewall
<b>Description</b>	No WAF was detected on the website. Because they can only allow or deny traffic, traditional firewalls are ineffective at managing web traffic. There is no security against suspicious web traffic if online traffic is allowed to pass over the firewall, which is required to visit the website. Evidence is listed in the Appendix.
<b>Recommendation</b>	A WAF is recommended because it targets HTTP traffic.

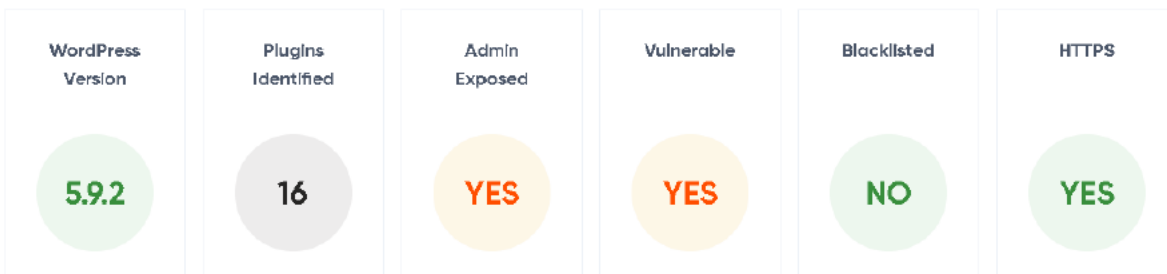
## 5 Appendix

### 5.1 Evidence for ID 9

Software / Version	Category
php -PHP	Programming languages
 WordPress	CMS, Blogs
 Elementor 3.6.4	Page builders
 MySQL	Databases
 Swiper Slider	Miscellaneous
 YouTube	Video players
 Nginx	Web servers, Reverse proxies
 Smash Balloon Instagram Feed	WordPress plugins
 MonsterInsights 8.5.0	WordPress plugins, Analytics
 Yeast SEO 18.6	SEO, WordPress plugins
 GTranslate	WordPress plugins, Translation
 Slick	JavaScript libraries
 Google Font API	Font scripts
 Facebook	Widgets
 Twitter Emoji (Twemoji)	Font scripts
 jQuery UI 1.12.1	JavaScript libraries
 jQuery Migrate 3.3.2	JavaScript libraries
 jQuery 3.6.0	JavaScript libraries
 Google Tag Manager	Tag managers
 Google Remarketing Tag	Retargeting
 Google Analytics	Analytics



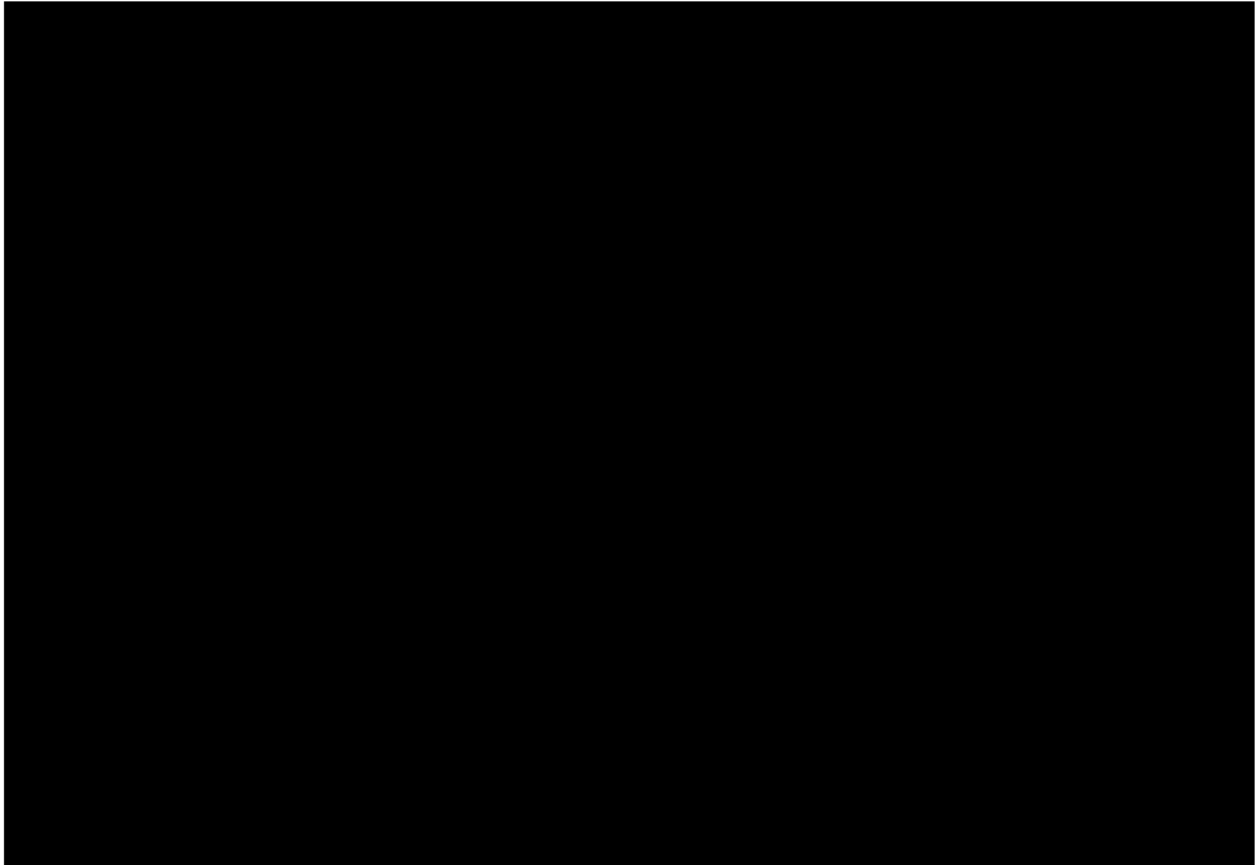
## 5.2 Evidence for ID 10



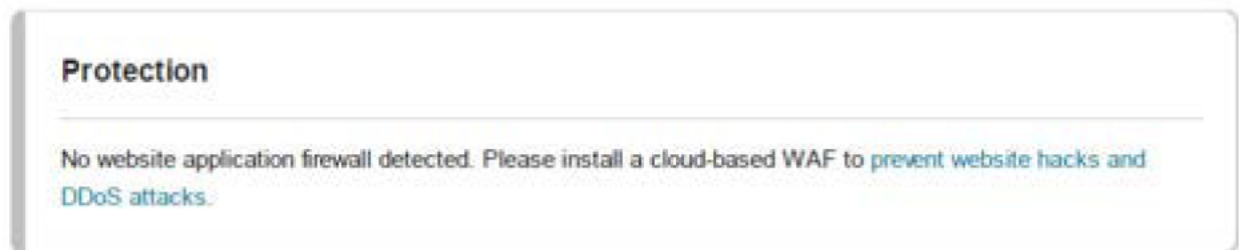
## 5.3 Evidence for ID 13

Test	Pass	S
<a href="#">Content Security Policy</a>	✗	
<a href="#">Cookies</a>	—	
<a href="#">Cross-origin Resource Sharing</a>	✓	
<a href="#">HTTP Public Key Pinning</a>	—	
<a href="#">HTTP Strict Transport Security</a>	✗	
<a href="#">Redirection</a>	✓	
<a href="#">Referrer Policy</a>	—	
<a href="#">Subresource Integrity</a>	✗	
<a href="#">X-Content-Type-Options</a>	✗	
<a href="#">X-Frame-Options</a>	✗	
<a href="#">X-XSS-Protection</a>	✗	

#### 5.4 Evidence for ID 14



#### 5.5 Evidence for ID 15



#### 5.6 FGDS Script



## 5.7 FGDS Results



## 5.8 WindowsManagerConfiguration.xml

