CST 620 Prevention of Cyber Attack Methodologies
Project 3 – Web Application Security Controls

Security Control Implementation Report

Prepared By: *Abbrin Hoagland*

Version 1.0

Contents

1. Introduction

In response to the critical imperative for bolstering web application security at FICBANK, this Security Control Implementation Report encapsulates a comprehensive strategy aimed at fortifying the online banking infrastructure. Recognizing the increasing reliance on online banking services, FICBANK, despite its status as a small credit union, acknowledges the necessity of a proactive and robust cybersecurity approach tailored to its unique operational context. The objective of this initiative is to harness the expertise of our cybersecurity professionals in identifying, configuring, and testing best-practice security controls for FICBANK's web application stack.

The primary focus of this endeavor is the implementation of a robust security framework, encompassing crucial controls such as SSL, application protocols, and the meticulous inspection of incoming web traffic. Faced with a lack of in-house expertise, FICBANK has entrusted our cybersecurity professionals with the responsibility of determining the most effective tools, techniques, and practices to fortify the security posture of its web application.

As part of the preliminary steps, our cybersecurity professionals executed a comprehensive security strategy, including the secure installation and configuration of the WAMP web server on the Windows VM hosted in the MARS environment. This strategic approach ensures not only the installation of WAMP but also the enabling of secure communications through the meticulous implementation of SSL. Throughout this process, specific attention was given to the capture of IP addresses and passwords for these virtual machines, aligning with the realistic constraints and requirements of a banking institution.

The installation of WAMP was executed with precision, following step-by-step instructions reflective of real-world scenarios. The cybersecurity professionals downloaded the latest version of WAMP from the official website, configured installation settings, and rigorously verified the functionality of the server. Additionally, the implementation of security controls included essential steps such as permitting connections to the server from authorized users, aligning with best practices to restrict access appropriately within the Apache server configuration.

To further enhance the security posture, our professionals delved into the meticulous implementation of SSL for the WAMP server. This encompassed the installation of OpenSSL, the generation of a certificate for secure communication, and the configuration of SSL settings within the Apache server. The strategic approach extended to modifying firewall rules to ensure secure connections on port 443, aligning with the stringent security requirements expected of a financial institution.

This report serves as a comprehensive documentation of the security strategy undertaken, laying the foundation for subsequent phases of the contract outlined by FICBANK. It not only equips FICBANK with practical insights into implementing robust web application security controls but also validates the effectiveness of these controls in a simulated yet realistic banking environment. The subsequent sections of this report will delve into the identified best practices, the precise configuration of security controls, and the rigorous testing and evaluation procedures undertaken to fortify FICBANK's web application against potential cyber threats.

2. Web Application Security Best Practices

In the dynamic landscape of modern cybersecurity, robust web application security is essential to protect against evolving threats. FICBANK, recognizing the criticality of safeguarding its online banking services, adopts a comprehensive approach outlined in the following best practices:

1. Implement HTTPS Encryption:

- Ensure secure data transmission by deploying HTTPS, safeguarding against eavesdropping and unauthorized access. (NIST Security 2020)

2. SSL/TLS Certificates:
   - Authenticate the website owner's identity with SSL/TLS certificates, ensuring data integrity and preventing unauthorized access.

3. Enforce Strong Password Policies:
   - Mitigate the risk of unauthorized access by enforcing strong password policies for user accounts.

4. Input Validation:
   - Guard against injection attacks like SQL injection and XSS by validating and sanitizing user inputs.

5. Secure Session Management:
   - Enhance security through secure session practices, including timeout mechanisms and secure cookie attributes.

6. Content Security Policy (CSP):
   - Mitigate cross-site scripting risks with CSP headers, specifying allowable sources of content on web pages. (NIST Security 2020)

7. Implement Security Headers:
   - Bolster browser security with headers like HSTS, X-Content-Type-Options, and X-Frame-Options.

8. Deploy Web Application Firewalls (WAFs):
   - Filter and monitor incoming traffic with WAFs to detect and block malicious requests and common vulnerabilities. (Palo)

9. Conduct Regular Security Audits:
   - Identify and address potential weaknesses through routine security audits and vulnerability assessments.

10. Multi-Factor Authentication (MFA):
    - Strengthen access controls with MFA, providing an additional layer of security beyond passwords. (Snyk 2023)

11. Customize Error Handling:
    - Limit information exposure by customizing error messages, preventing attackers from exploiting vulnerabilities.

12. File Upload Security:
    - Apply stringent controls on file uploads, verifying types, sizes, and handling to prevent malicious uploads.

13. Database Security Measures:
- Follow the principle of least privilege for database accounts, encrypt sensitive data, and keep databases updated. (NIST Cybersecurity 2020)

14. Regular Security Patching:
- Maintain up-to-date software components to address known vulnerabilities and reduce exploitation risks.

15. Logging and Monitoring:
- Establish robust logging mechanisms and continuous monitoring to detect and respond promptly to security incidents.

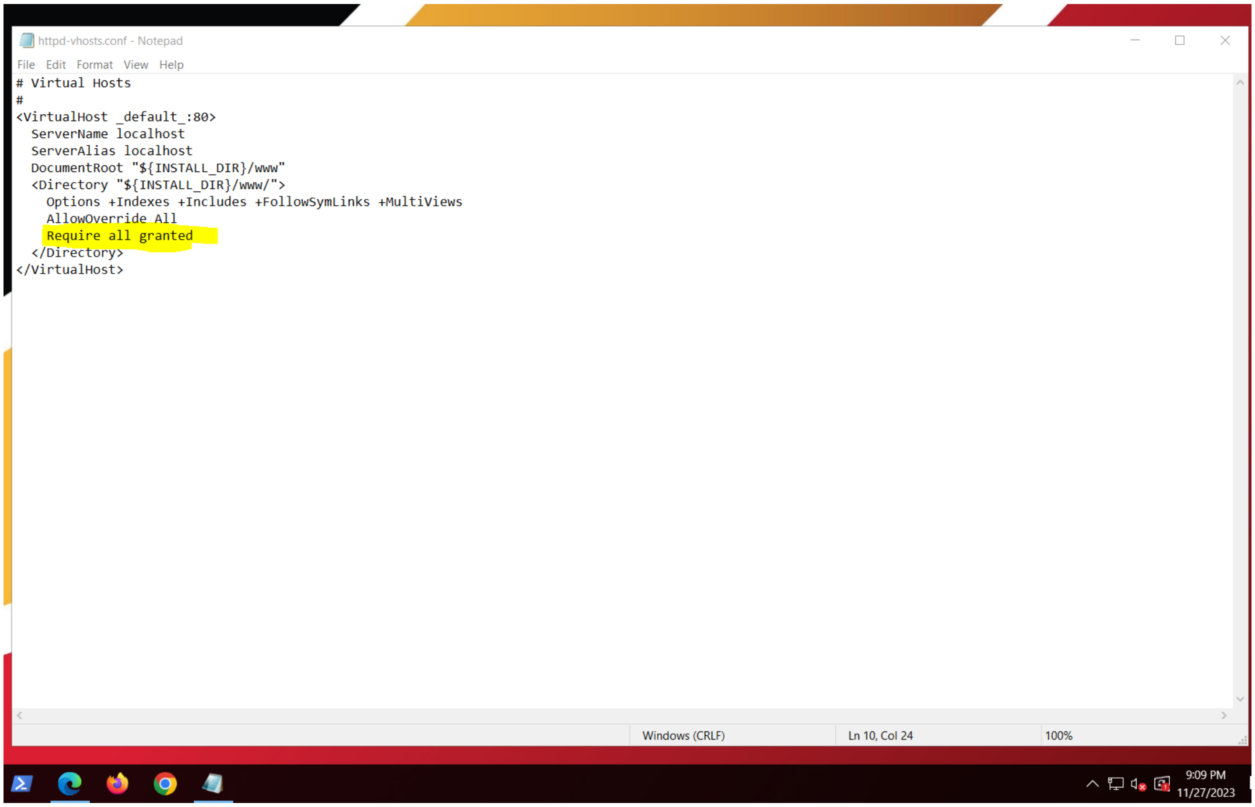
16. Security Education and Training:
- Foster a security-conscious culture by providing ongoing education and training for developers, administrators, and users. (NIST Cybersecurity 2020)

These best practices collectively form a comprehensive defense strategy, ensuring FICBANK's web applications remain resilient against diverse cyber threats. By incorporating these measures, FICBANK fortifies its commitment to maintaining a secure online banking environment for its clientele.

3. Web Application Security Control Implementation and Testing

In this pivotal phase of our cybersecurity initiative for FICBANK, our dedicated team executed a meticulously planned series of actions to implement and test web application security control best practices. The hands-on exercise began with the installation and configuration of the WAMP web server, a critical component in fortifying the online banking infrastructure. Our professionals, well-versed in industry best practices, downloaded the latest version of WAMP from the official website and embarked on a seamless installation process. This involved configuring essential components such as Apache, PHP, MySQL, and MariaDB, laying a robust foundation for subsequent security measures.

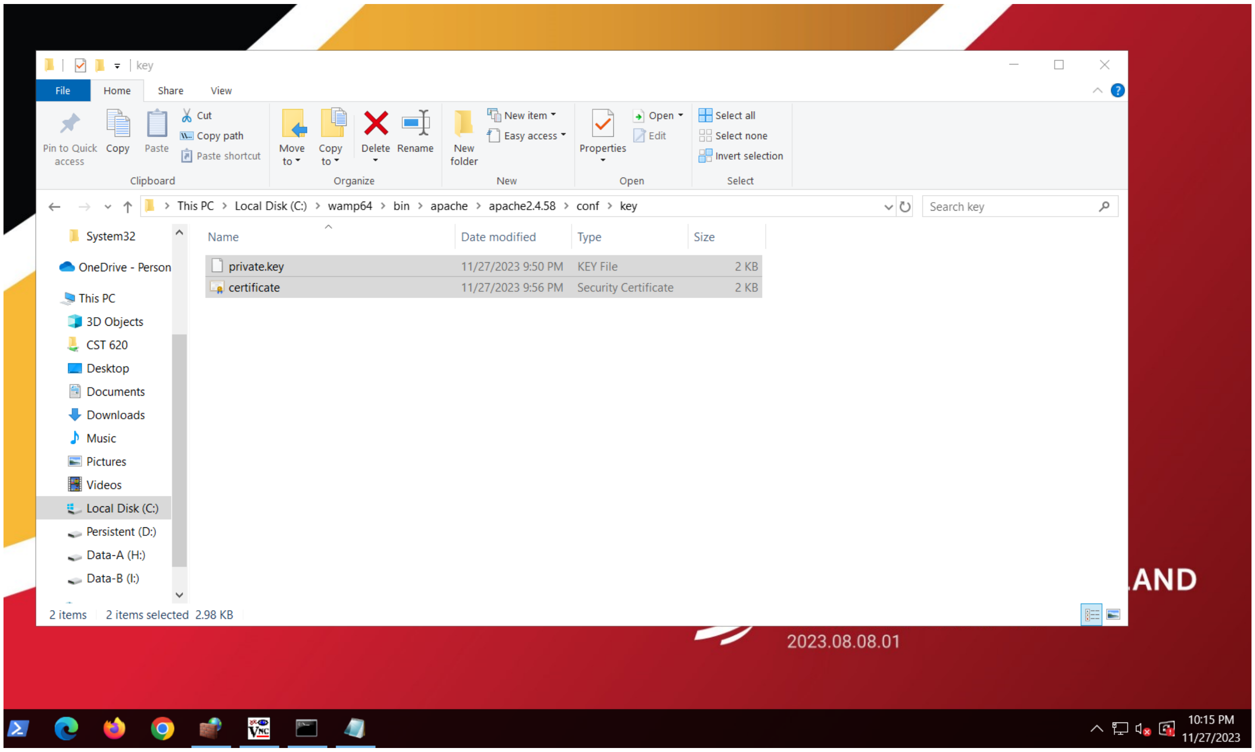
A key facet of our implementation strategy was the meticulous adjustment of permissions within the Apache server's configuration files, particularly the https-vhosts.conf file. This deliberate step ensured precise control over user access, aligning with the principle of least privilege and bolstering the overall security posture. As part of the process, our cybersecurity professionals focused on defining specific users allowed to access the server securely, a critical measure to prevent unauthorized intrusion into the web application.



```
# Virtual Hosts
#
<VirtualHost _default_:80>
  ServerName localhost
  ServerAlias localhost
  DocumentRoot "${INSTALL_DIR}/www"
  <Directory "${INSTALL_DIR}/www/">
    Options +Indexes +Includes +FollowSymLinks +MultiViews
    AllowOverride All
    Require all granted
  </Directory>
</VirtualHost>
```

Simultaneously, our team delved into the implementation of Secure Sockets Layer (SSL), a fundamental security protocol. The installation of OpenSSL, a cryptographic tool, marked the beginning of this phase. Our professionals adeptly generated a secure certificate for encrypted communication, ensuring the confidentiality and integrity of data transmitted between web servers and users' browsers. Configuration adjustments within the Apache server, encapsulated in the httpd.conf and httpd-ssl.conf files, were meticulously undertaken to seamlessly integrate

SSL, thereby enhancing the security of web communications.

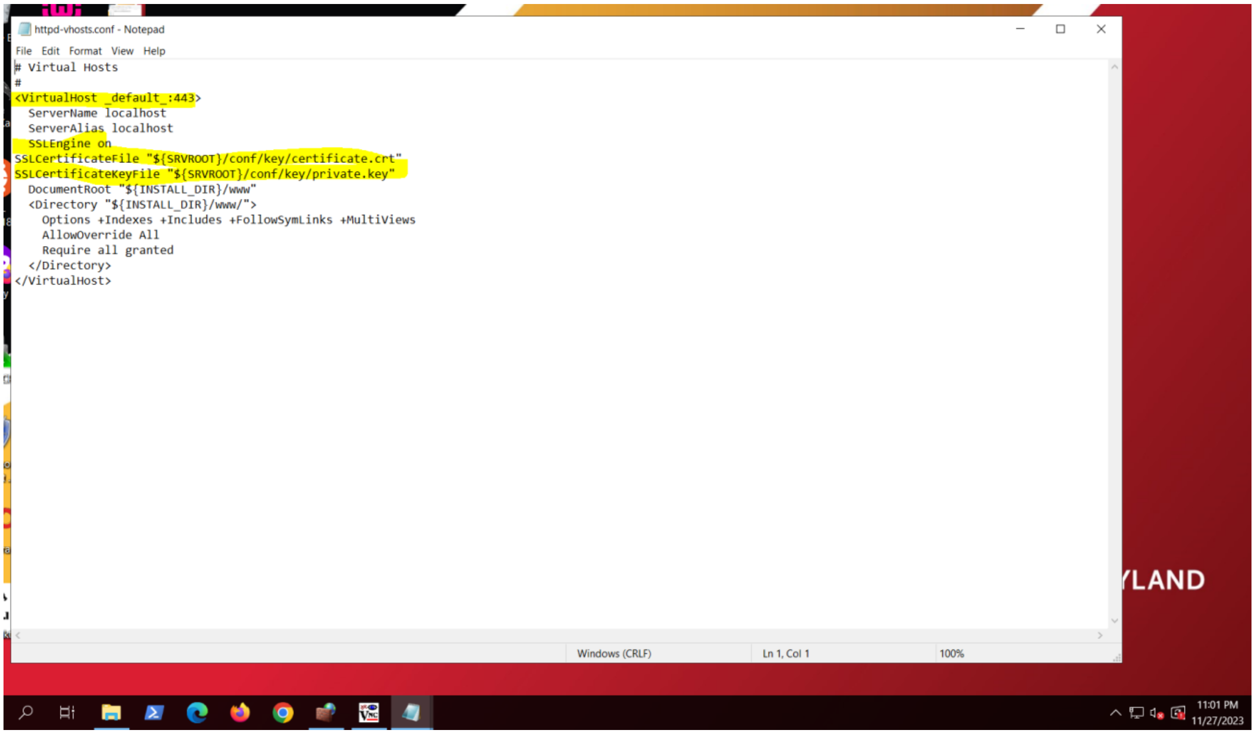


This PC > Local Disk (C:) > wamp64 > bin > apache > apache2.4.58 > conf > key

Name	Date modified	Type	Size
private.key	11/27/2023 9:50 PM	KEY File	2 KB
certificate	11/27/2023 9:56 PM	Security Certificate	2 KB

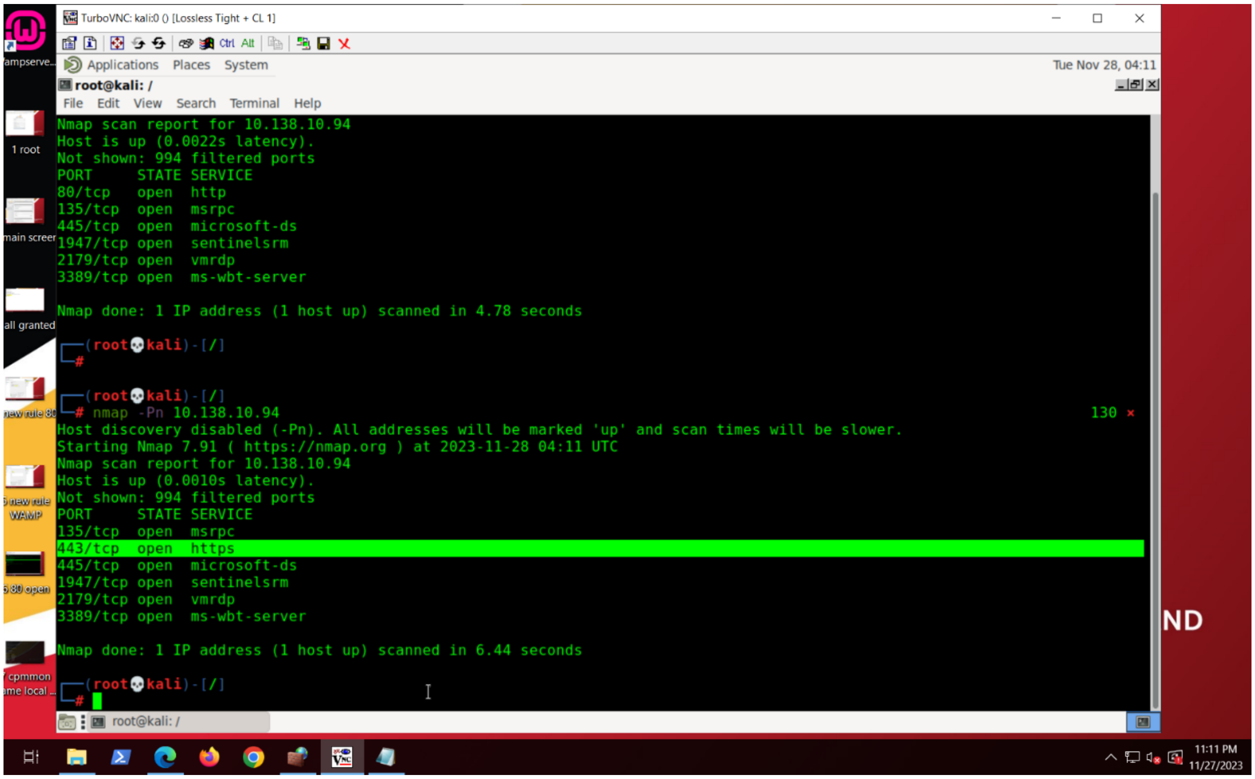
2 items   2 items selected 2.98 KB

With the WAMP server and SSL in place, our cybersecurity professionals turned their attention to firewall configurations, an integral component of a robust defense strategy. Adjustments to permissions within the Apache server's https-vhosts.conf file were executed to control incoming traffic effectively. For version 3.3.0, the team replaced "Require local" with "Require all granted," aligning with the need for precise control over server access.



```
# Virtual Hosts
#
<VirtualHost _default_:443>
  ServerName localhost
  ServerAlias localhost
  SSLEngine on
SSLCertificateFile "${SRVROOT}/conf/key/certificate.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/key/private.key"
  DocumentRoot "${INSTALL_DIR}/www"
  <Directory "${INSTALL_DIR}/www/">
    Options +Indexes +Includes +FollowSymLinks +MultiViews
    AllowOverride All
    Require all granted
  </Directory>
</VirtualHost>
```

The next crucial step involved configuring Windows Defender Firewall settings to control and permit secure connections. A new inbound rule was meticulously created to allow traffic on port 443, securing communication channels while explicitly disallowing insecure HTTP traffic. This dual-layered approach to firewall configurations was instrumental in fortifying FICBANK's web application against potential cyber threats.


TurboVNC: kali:0 () [Lossless Tight + CL 1]
Applications Places System
Tue Nov 28, 04:11
root@kali: /
File Edit View Search Terminal Help
11:11 PM
11/27/2023

```
Nmap scan report for 10.138.10.94
Host is up (0.0022s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
445/tcp  open  microsoft-ds
1947/tcp open  sentinelsrm
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 4.78 seconds

┌──(root💀kali)-[/]
└─#

┌──(root💀kali)-[/]
└─# nmap -Pn 10.138.10.94                                                  130 ×
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2023-11-28 04:11 UTC
Nmap scan report for 10.138.10.94
Host is up (0.0010s latency).
Not shown: 994 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
443/tcp  open  https
445/tcp  open  microsoft-ds
1947/tcp open  sentinelsrm
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 6.44 seconds

┌──(root💀kali)-[/]
└─#
```

Following the meticulous implementation of security controls, our team entered the crucial phase of vulnerability assessment and testing. Leveraging tools like Nmap from the Kali VM, our cybersecurity professionals conducted comprehensive scans to identify open ports and validate the efficacy of implemented security measures. The meticulous testing process served as a litmus test, ensuring that the robust security controls put in place were not only effective but resilient to potential cyber threats.

In documenting these steps, our team employed a combination of written descriptions and screenshots. These tangible artifacts not only serve as documentation but also provide FICBANK with a visual representation of the implemented security measures, further reinforcing the efficacy of our cybersecurity initiative. The culmination of these efforts represents a comprehensive and tailored approach to web application security control implementation, aligning with industry best practices and tailored to the specific needs of FICBANK's online banking infrastructure.

4. Conclusion

In conclusion, the Security Control Implementation Report represents a pivotal step in fortifying FICBANK's web application security. The comprehensive approach, ranging from the strategic installation of the WAMP web server to the meticulous implementation of SSL and firewall configurations, underscores our commitment to addressing FICBANK's cybersecurity needs. By adhering to industry best practices and tailoring our actions to the unique context of online banking, our cybersecurity professionals have laid a robust foundation for a secure web application stack.

The integration of web application security best practices, as outlined in the report, positions FICBANK to navigate the evolving landscape of cyber threats effectively. From HTTPS encryption to multi-factor authentication and regular security audits, the adopted measures collectively contribute to a resilient defense strategy. The hands-on implementation and testing phase, documented with precision and accompanied by screenshots, not only ensures the practicality of the security controls but also equips FICBANK with valuable insights into the robustness of its cybersecurity posture.

As FICBANK moves forward, this report serves not only as a documentation artifact but as a testament to our commitment to enhancing cybersecurity resilience. The collaboration between FICBANK and our cybersecurity professionals exemplifies a proactive and tailored approach to safeguarding online banking services. This comprehensive initiative reflects our dedication to maintaining the confidentiality, integrity, and availability of sensitive financial data, fostering trust among FICBANK's clientele.

5. References

- National Institute of Standards and Technology (NIST). (2020). Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5, Includes updates as of January 2023. https://doi.org/10.6028/NIST.SP.800-53r5

- National Institute of Standards and Technology (NIST). (2020). Cybersecurity Framework Version 1.1. https://www.nist.gov/cyberframework

- Snyk (2023). *Application Security Controls Explained.* Snyk.io. https://snyk.io/learn/application-security/application-security-controls/

- *What is a WAF?* (n.d.). Palo Alto Networks. Retrieved November 20, 2023, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-web-application-firewall