Enhancing security measures for multi-factor authentication in web applications to counter evolving attack vectors

Philipp Liermann 20-475873-20
Supervisor: Prof. Dr. Raad Bin Tareaf

January 28, 2024

Contents

1 Problem statement

These days most websites have implemented two-factor authentication systems to prevent malicious third-party actors from using stolen login credentials to commit cyberfraud. Despite this, a new technique referred to as reverse proxy phishing still provides malicious actors the means to bypass two-factor authentication systems. This creates a critical security vulnerability, as this technique can be used to gain unauthorized access to otherwise secure systems. To resolve this issue, it is imperative to develop and implement effective measures to counteract reverse proxy phishing and other methods of bypassing two-factor authentication systems.

2 Research question

How can we protect two factor authentication secured web applications from reverse proxy phishing attacks? Based on this question the following sub questions were derived:

- What exactly are classical phishing attacks in general and how do they differ from the new attack vector?
- How big is the threat imposed by this new type of phishing attack?
- Why are many organizations still not aware of this issue?
- What can be done to help developers evade this type of security threat?

3 Objective

As credential theft and cyberfraud in general are still a growing problem in the digital age, it is important to develop and implement effective measures to counteract this threat. The objective of this thesis is to find and document different strategy's that can help organizations and developers to mitigate this new attack vector.

4 Theoretical foundations & current state of research

Cyberfraud is a form of internet-based fraud, usually involving the use of false identities and/or stolen information to illegally obtain money, property, or services. Cyberfraud is an increasingly pervasive problem that is becoming increasingly difficult to combat, as fraudsters become more sophisticated in their methods. In 2020, cyberfraud was estimated to cost the global economy over $6 trillion[1], with the financial sector suffering the most damages. The social, economic and reputational costs of cyberfraud can be incredibly damaging, and can range from the loss of money, to identity theft, to the disruption of businesses. Cyberfraud has become so pervasive that it is essential for businesses and individuals to take measures to protect themselves from it. This includes using strong passwords, using two-factor authentication, and staying up to date with the latest security protocols.

A phishing attack is a type of cyberattack in which an attacker attempts to gain confidential information, such as passwords, credit card numbers, or other sensitive information, by sending emails or other messages disguised as legitimate entities. These messages often include malicious links to faked login prompts that will steal the victims credentials upon entering them. These attacks are becoming increas-

ingly sophisticated and difficult to recognize, making it important for everyone to remain vigilant and take steps to protect against them.

A HTTP reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers. This type of proxy is sometimes referred to as a "gateway" or "tunneling" proxy because it acts as a gateway for the traffic to and from the server. A reverse proxy will typically receive a request from a client, then forward that request to an appropriate server on the same network. It then retrieves the response from the server and sends it back to the client. This type of proxy server is most often used in enterprise networks to protect against malicious traffic, to balance load between multiple servers, and to cache static content.
Reverse proxy phishing is a new technique used by attackers to intercept and steal two-factor authentication (2FA) tokens from unsuspecting users. Instead of copying HTML code from the original page that the attacker is trying to impersonate, this new attack uses a HTTP reverse proxy to just redirect the users traffic to the original page. The attacking proxy operator can view and modify all traffic that is going through it while the victim sees a one by one copy of the original login page. By doing so login credentials and 2FA tokens can be extracted easily.

Many scientific papers have been published on this topic, but there is still a lack of information on how to protect against this new attack vector. This is why it is important to find and document different strategies that can help organizations and developers to mitigate this new attack vector.

5 Research design

This thesis will be conducted in a quantitative research design. By analyzing existing literature and scientific papers on the topic, but also by running own experiments in which open source reverse proxy phishing toolkits will be used to setup attack simulations with the goal to find flaws in their attack implementation. With the gained knowledge from this experiments this paper will outline easy to follow strategies to protect web services from this threat.

6 Preliminary outline

1. Introduction
    (a) Problem statement
    (b) Research question
    (c) Objective
2. Theoretical Foundation
    (a) Phishing attacks
    (b) HTTP reverse proxy
    (c) Reverse proxy phishing
3. Research Methodology
    (a) Research design
    (b) Analysis
    (c) Experiment Setup
4. Results
    (a) Analysis results
    (b) Experiment results
5. Discussion
6. Conclusion

7 Preliminary time table

Planned starting date: 01.03.2023

- Week 1
  - Meet supervisor
  - Start writing introduction
- Week 2
  - Theoretical foundation
- Week 2
  - Research methodology
- Week 3
  - Start with research
- Week 4
  - Start with attack simulation experiment
- Week 5
  - Finish & analyze experiments
- Week 6
  - Results
- Week 7
  - Discussion & Conclusion

- Week 8
  - Buffer

8 References

[1] Cybercrime Damages $6 Trillion By 2021 https://cybersecurityventures.com/annual-cybercrime-report-2017/

[2] Catching Transparent Phish: Analyzing and Detecting MITM Phishing Toolkits https://catching-transparent-phish.github.io/catching_transparent_phish.pdf

[3] Geo-Location based QR-Code Authentication Scheme to Defeat Active Real-Time Phishing Attack https://sci-hub.hkvisa.net/10.1145/2517881.2517889

[4] Analyzing 2FA Phishing Attacks and Their Prevention Techniques https://ieeexplore.ieee.org/abstract/document/9945766

[5] Secure authentication scheme to thwart RT MITM, CR MITM and malicious browser extension based phishing attacks https://www.sciencedirect.com/science/article/abs/pii/S2214212618300140

[6] Modlishka. Reverse Proxy https://github.com/drk1wi/Modlishka

[7] EvilNginx. Reverse Proxy https://breakdev.org/evilginx-2-next-generation-of-phishing-2fa-tokens/