ScienceDirect

Computers & Security

Volume 121, October 2022, 102859

Practical attacks on Login CSRF in OAuth

Elham Arshad, Michele Benolli, Bruno Crispo

Show more

https://doi.org/10.1016/j.cose.2022.102859

Get rights and content

Abstract

OAuth 2.0 is an important and well studied protocol. However, despite the presence of guidelines and best practices, the current implementations are still vulnerable and error-prone. This research mainly focused on the Cross-Site Request Forgery (CSRF) attack. This attack is one of the dangerous vulnerabilities in OAuth protocol, which has been mitigated through state parameter. However, despite the presence of this parameter in the OAuth deployment, many websites are still vulnerable to the OAuth-CSRF (OCSRF) attack. We studied one of the most recurrent type of OCSRF attack through a variety range of novel attack strategies based on different possible implementation weaknesses and the state of the victim's browser at the time of the attack. In order to validate them, we designed a repeatable methodology and conducted a large-scale analysis on 395 high-ranked sites to assess the prevalence of OCSRF vulnerabilities. Our automated crawler discovered about 36% of targeted sites are still vulnerable and detected about 20% more well-hidden vulnerable sites utilizing the novel attack strategies. Based on our experiment, there was a significant rise in the number of OCSRF protection compared to the past scale analyses and yet over 25% of sites are exploitable to at least one proposed attack strategy. Despite a standard countermeasure exists to mitigate the OCSRF, our study shows that lack of awareness about implementation mistakes is an important reason for a significant number of vulnerable sites.

Introduction

OAuth 2.0 is an industry-standard protocol for authorization. It was released in 2012 as RFC 6749 and nowadays is pervasively used to manage authorization flows in web, desktop, mobile applications, and in smart devices. The protocol has been widely studied, and its theoretical and practical security has been covered extensively by the literature. OAuth was designed to enhance several aspects of the former client-server authorization model.

The OAuth 2.0 Threat Model and Security Considerations Ed.(2018) and OAuth 2.0 Security Best Current PracticeLodderstedtetal.(2020) documents are published to address the most common security issues and vulnerability scenarios discovered within concrete implementations of the protocol. However, despite the rich guidelines and the many mitigation proposed over time, several OAuth-based services are still subject to a wide range of security flaws. This because, those guidelines are not detailed enough to consider all possible settings that can lead to an attack, especially for what relates client-side parameters.

As reported by Sudhodananetal.(2017) CSRF vulnerabilities related to authentication and identity management services are extremely pervasive, even among the top-ranked domains. The paper is mainly focused on a specific vulnerability, the CSRF attack against the redirect_uri Ed.(2018), since it is one of the most popular concrete attack in OAuth implementations. The attack is well documented in the Threat Model document and it can lead to serious consequences, ranging from the disclosure of sensitive information to a malicious user Barthetal.(2008) to the complete account takeover Homakov(2012). Our work extensively covers the details of this security threat, with a systematic analysis of its root causes and practical impact. We built an automated testing framework to evaluate the presence of the aforementioned vulnerability in a large number of popular sites that implement the Facebook and Google login service. The rationale of our approach is to help developers to avoid implementation mistakes by providing the most comprehensive set of attack strategy such that developers are aware what implementation settings to avoid.

The outcome of our large-scale analysis is that more than a third of the tested sites were found vulnerable to at least one of the proposed attack strategy.

We selected only one attack because the purpose of the paper is not to find the highest number of vulnerabilities, but rather to demonstrate how to build a comprehensive set of attack strategies for an attack, considering scenarios and configurations that have been so far ignored or overlooked in the literature. This is based on the wrong assumptions that those scenarios were not significant. Our analysis proved they are indeed significant and contributed to find 20% additional vulnerabilities.

The paper makes the following contributions:

- To the best of our knowledge, we present the most comprehensive set of test cases to exploit OCSRF vulnerabilities, including novel attack strategies that stress all possible client-side status. They complement and integrate the guidelines provided by documents such as Ed.(2018); Lodderstedtetal.(2020) in helping OAuth developers to mitigate implementation mistakes.
- We designed a repeatable methodology and conducted an automated analysis on 395 high-ranked sites of two representative IdP: Facebook and Google to assess the prevalence of CSRF attack against the redirect_uri in OAuth implementations.
- The analysis discovered that about 36% of targeted sites are still vulnerable and detected about 20% more well-hidden vulnerable sites utilizing the novel attack strategies.

- We analyzed other CSRF mitigation for all the implemented attack scenarios and tested the impact of the attacks on mitigation, showing how inconsistent they are in different situations.

Section snippets

Background

This work focuses on a specific vulnerability, that can lead to a cross-site request forgery attack. For a thorough understanding of the risks and consequences related to this vulnerability, this sectionprovides a brief background on OpenID Connect, that is, an authentication protocol and OAuth, that is, an authorization protocol and their implementations as Single Sign-on(SSO) in the wild. Threat model for CSRF attack and its impact are described as well. …

OAuth Cross Site Request Forgery

In the context of OAuth 2.0, a successful cross-site request forgery can allow an attacker to obtain authorization to resources protected by the protocol, without the consent of the user. A recurrent type of login OCSRF is the OCSRF attack against redirect_uriEd.(2018), where the victim is logged into an account controlled by the attacker. As a direct consequence, all the operations performed by the victim are unconsciously accomplished inside the attacker's session and the result of these …

Related Work

The security of OAuth 2.0 has been widely examined in the literature. Several theoretical studies (e.g. Bansaletal.(2014); Fettetal.(2016); Paietal.(2011); Rahatetal.(2021); Wangetal.(2013)) use abstract models to evaluate the security of the OAuth protocol. A downside of theoretical approach is that it does not allow to discover the vulnerabilities resulting from implementation errors. Empirical studies try to fill this gap by looking for vulnerabilities in the wild.

Many …

Methodology

We designed a repeatable methodology to discover and validate OCSRF vulnerabilities in targeted sites. As depicted in Fig.2, our methodology has three phases: 1. target selection, 2. measurement setup 3. OCSRF detection. We developed a tool based on Python-Selenium to automatically select targets and test different OCSRF scenarios. …

Analysis

In this section, we present the results of the empirical analysis and discuss them in detail. We conducted a large scale analysis implementing all above attack scenarios to test OCSRF attacks in the

wild. In this study we discuss the measurement results of each attack strategy with different victim browser status. We managed to answer the following research questions:

(Q1) What is the popularity of OCSRF vulnerabilities on high profile and popular sites? …

(Q2) Can OCSRF vulnerabilities be exploited in …

…

Mitigation

The OAuth 2.0 standard clearly states that developers must implement CSRF protection, by using a value that binds the authorization request to the browser session. For this purpose, the use of the state parameter is strongly recommended. The empirical evidence gathered in our work suggests that still today many OAuth implementations are vulnerable due to the absence of the state value (13% for Facebook and 21% for Google). Even when the parameter is correctly included inside the authorization …

Conclusions

Our work is mainly focused on the analysis of the CSRF attack against redirect_uri, a well-known and documented OAuth 2.0 vulnerability. Our security assessment revealed that many actual implementations of SSO services are vulnerable to the considered attack. The reason behind the prevalence of this class of vulnerabilities is related to the complexity of implementing effective mitigations and to the absence of tools to reliably detect the threats. As a future work, we plan to test similar …

CRediT authorship contribution statement

Elham Arshad: Conceptualization, Methodology, Validation, Investigation, Writing – review & editing. **Michele Benolli:** Software, Data curation, Writing – original draft. **Bruno Crispo:** Project administration, Supervision. …

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. …

Elham Arshad is currently a PhD student at the University of Trento,Italy, where previously worked as a scientific researcher in computer science department. She received her masters degree from Sharif University of Technology, Iran, in computer science, 2016. She has over 5 years job experience as a senior developer and security specialist in high-tech companies. Her major research interests lie in web application Security and privacy and mainly focused on large-scale security measurement, …

…

...

Recommended articles

References (37)

G. Bai *et al.*
Authscan: Automatic extraction of web authentication protocols from implementations
NDSS(2013)

C. Bansal *et al.*
Discovering concrete attacks on website authorization by formal analysis 1
Journal of Computer Security (2014)

A. Barth *et al.*
Robust defenses for cross-site request forgery
Proceedings of the 15th ACM conference on Computer and communications security(2008)

S. Calzavara *et al.*
{WPSE}: Fortifying web protocols via browser-side security monitoring
27th {USENIX} Security Symposium ({USENIX} Security 18)(2018)

T.L. Ed.
OAuth 2.0 Threat Model and Security Considerations
RFC(2018)

S. Farooqi *et al.*
Measuring and mitigating oauth access token abuse by collusion networks
Proceedings of the 2017 Internet Measurement Conference(2017)

D. Fett *et al.*
Spresso: A secure, privacy-respecting single sign-on system for the web
Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (2015)

D. Fett *et al.*
A comprehensive formal security analysis of OAuth 2.0
Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (2016)

HackerOne. Hackerone bug bounty platform. 2020....

D. Hardt
The OAuth 2.0 Authorization Framework
RFC(2012)

View more references

Cited by (8)

Single Sign-On Security and Privacy: A Systematic Literature Review

2025, Computers Materials and Continua

Show abstract

Formal Modelling and Analysis of Authorization Code Model in OAuth 2.0 Protocol Based on ASLan++

2025, Computer Engineering and Applications

Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities

2025, IEEE Communications Surveys and Tutorials

CSRFing the SSO Waves: Security Testing of SSO-Based Account Linking Process

2024, Proceedings 9th IEEE European Symposium on Security and Privacy Euro S and P 2024

Unified singular protocol flow for OAuth ecosystem

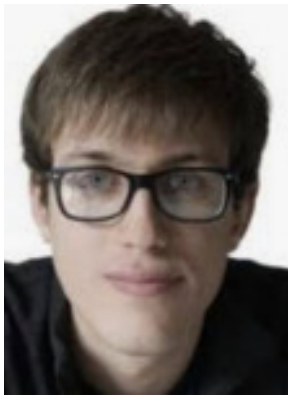
2024, International Journal of Information and Computer Security

When Push Comes to Shove: Empirical Analysis of Web Push Implementations in the Wild

2023, ACM International Conference Proceeding Series

View all citing articles on Scopus

Elham Arshad is currently a PhD student at the University of Trento,Italy, where previously worked as a scientific researcher in computer science department. She received her masters degree from Sharif University of Technology, Iran, in computer science, 2016. She has over 5 years job experience as a senior developer and security specialist in high-tech companies. Her major research interests lie in web application Security and privacy and mainly focused on large-scale security measurement, using browser instrumentation and distributed crawling.



Michele Benolli received the Bachelor and Master degree (cum laude) in Computer Science from the University of Trento, Italy, in 2015 and 2020, respectively. His academic interests are mainly related to the field of web security. During his Master's, he collaborated with the DISI Security Research Group for realizing large-scale analysis of web-based attacks and automated vulnerability detection.

Bruno Crispo is Professor at the Department of Computer Science at theUniversity of Trento in Italy. His main research interest lies in the area of systemand network security and access control. In particular, he is currently workingon smartphone and mobile app security, security and privacy on the Internet of Things and behavioral biometrics.He has published more than 140 papers in scientific journalsand international conferences. He is an Associate Editor of the ACMTransactions on Privacy and Security. He is a Senior Member of IEEE.

View full text