BYPASSING SAMESITE COOKIE RESTRICTIONS VIA FEDERATED AUTHENTICATION AND SUBDOMAIN CONTROL EXPLOITS

Thesis Submitted
in Partial Fulfillment of the Requirements for the
Degree of

MASTER OF TECHNOLOGY

in

Computer Science Engineering

by

Aayush Kumar Singh
(Roll No. 2k24/CSE/28)

Under the Supervision of

Prof. Manoj Kumar
Assistant Professor
Department of Computer Science Engineering
Delhi Technological University

Department of Computer Science Engineering

DELHI TECHNOLOGICAL UNIVERSITY

(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-110042, India

June, 2026

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-110042

ACKNOWLEDGEMENTS

I wish to express my sincerest gratitude to **Prof. Manoj Kumar** for his continuous guidance and mentorship that he provided me during the project. He showed me the path to achieve my targets by explaining all the tasks to be done and explained to me the importance of this project as well as its academic and practical relevance. He was always ready to help me and clear my doubts regarding any hurdles in this project. Without his constant support and motivation, this project would not have been successful.

Aayush Kumar Singh

Place: Delhi

Aayush Kumar Singh

Date: 29/5/26

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-110042

CANDIDATE'S DECLARATION

I, **Aayush Kumar Singh**, Roll No. **2k24/CSE/28**, student of M.Tech (Computer Science Engineering), hereby declare that the project dissertation titled "**Bypassing SameSite Cookie Restrictions via Federated Authentication and Subdomain Control Exploits**" which is submitted by me to the Computer Science Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of degree of Master of Technology, is original and not copied from any source without proper citation. This work has not previously formed the basis for the award of any Degree, Diploma, Associateship, Fellowship or other similar title or recognition.

Aayush Kumar Singh

Candidate's Signature

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

Signature of Supervisor(s) Signature of External Examiner

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-110042

CERTIFICATE

I hereby certify that the Project Dissertation titled "**Bypassing SameSite Cookie Restrictions via Federated Authentication and Subdomain Control Exploits**" which is submitted by **Aayush Kumar Singh**, Roll No. **2k24/CSE/28**, Computer Science Engineering, Delhi Technological University, Delhi in partial fulfilment of the requirement for the award of the degree of Master of Technology, is a record of the project work carried out by the student under my supervision.

To the best of my knowledge this work has not been submitted in part or full for any Degree or Diploma to this University or elsewhere.

Place: Delhi

Date: 29/5/26

Prof. Manoj Kumar

SUPERVISOR

Bypassing SameSite Cookie Restrictions via Federated Authentication and Subdomain Control Exploits

Aayush Kumar Singh

ABSTRACT

Browser-based security models are widely used to access digital services in a secure manner, and HTTP cookies remain a fundamental component of web application security. The introduction of SameSite cookie protection mechanisms has been adopted by modern browsers to enhance browser security and minimize risks related to Cross-Site Request Forgery (CSRF) and unauthorized cross-site interactions. However, newer authentication architectures introduce cross-domain interactions through federated authentication standards such as OAuth, OpenID Connect, and Single Sign-On, which may weaken or complicate the intended security guarantees of cookie-based protections.

In addition to federated authentication flows, trust relationships between organizational subdomains can create security weaknesses when subdomains are poorly managed, misconfigured, or exposed to attacker control. This research examines the possibility of circumventing SameSite cookie restrictions through the combined effect of federated authentication workflows and trusted subdomain control scenarios. A controlled experimental framework was developed to simulate authentication interactions, redirection manipulation, cookie transmission behavior, and subdomain exploitation under ethical testing conditions.

Several browsers were tested to understand how consistently they implement SameSite enforcement and how effectively they resist exploitation under different authentication conditions. The study highlights that SameSite cookies provide an important layer of protection, but their effectiveness depends on correct configuration, secure identity-provider integration, and careful management of subdomain trust boundaries. The findings emphasize the need for layered browser security, strict redirect validation, robust subdomain governance, and defence-in-depth strategies for securing modern web authentication systems.

LIST OF PUBLICATIONS

1. **Bypassing Same Site Cookie Restrictions via Federated Authentication and Subdomain Control Exploits.**
2. **A Comprehensive Review of SameSite Cookie Bypass Techniques via Federated Authentication and Subdomain Control Exploits.**

TABLE OF CONTENTS

Acknowledgements **ii**

Candidate's Declaration **iii**

Certificate **iv**

Abstract **v**

List of Publications **vi**

Table of Contents **vii**

List of Tables **ix**

List of Figures **x**

1 INTRODUCTION **1**
1.1 Background and Objectives 1
1.2 Problem Statement 2
1.3 Objectives 2
1.4 Scope of the Study 3
1.5 Research Contribution 3

2 LITERATURE REVIEW **4**
2.1 Web Security Fundamentals 4
2.2 Same Site Cookie Mechanism 4
2.3 Federated Authentication (OAuth/OIDC/SSO) 5
2.4 Subdomain Takeover Exploits 5
2.5 Existing Security Approaches 6
2.6 Research Gap 6

3 METHODOLOGY **9**
3.1 Research Design 9
3.2 System Architecture 10
3.3 Experimental Setup 11
3.4 Threat Model 11
3.5 Attack Simulation Method 12
3.6 Evaluation Metrics 13

4 RESULTS AND DISCUSSION **15**
4.1 Experimental Results 15
4.2 Browser Security Analysis 17
4.3 Exploit Performance Evaluation 19
4.4 Discussion 20

5 CONCLUSION AND FUTURE SCOPE **23**
5.1 Conclusion 23
5.2 Summary of finding 24
5.3 Study's limitations. 24
5.4 Future Work 25

References **26**

List of Publications and their Proofs **28**

Plagiarism Report **29**

Curriculum Vitae **30**

List of Tables

1 Comparative Analysis of Existing Web Security Studies 7

2 Attack Simulation Steps 13

3 Experimental Attack Scenario Results 15
4 Cookie Transmission Observation Results 16
5 Browser Security Performance Analysis 18
6 Exploit Performance Evaluation Metrics 19

LIST OF FIGURES

Title	Page No.
System Architecture for SameSite Cookie Bypass Analysis Using Federated Authentication and Subdomain Exploit Simulation	23
Experimental Attack Scenario Success Rate Analysis	32
Cookie Transmission Observation Across Security Configurations	33
Browser Security Performance Analysis	36
Exploit Performance Evaluation Analysis	38

LIST OF SYMBOLS, ABBREVIATIONS AND NOMENCLATURE

AI	Artificial Intelligence	API	Application Programming Interface
CSRF	Cross-Site Request Forgery	CSP	Content Security Policy
DNS	Domain Name System	DOM	Document Object Model
FIDP	Federated Identity Provider	HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure	ML	Machine Learning
OAuth	Open Authorization	OIDC	OpenID Connect
SOP	Same-Origin Policy	SSO	Single Sign-On
TLS	Transport Layer Security	URI	Uniform Resource Identifier
XSS	Cross-Site Scripting		

CHAPTER 1

INTRODUCTION

This thesis discusses security issues of existing web authentication methods like bypassing SameSite in federated type authentication solutions and subdomain control attacks. It will explore security measures in place to keep cookies on your browser, authentication methods such as OAuth and Single Sign-On etc. and how trusted subdomains have trust problems. Experiments are run under a controlled environment and test the behaviour of the browsers under different security settings and attack sequences. The results show drawbacks of the current protection mechanisms and the potential for protection mechanisms to be vulnerable with regard to the security of the session. Based on the analysis, the research provides strategies for mitigating the attack and suggests security measures that can be taken to ensure that Web applications are more secure and that the advanced session exploitation attack is avoided.

1.1 Background and Objectives

As Web applications become more important, a way of getting secure and seamless access to Web services has become more dependent on mechanisms that depend upon the browser, including authentication and session management. HTTP cookies are used to keep sessions which play an important role in ensuring the persistence of the client-server relationship. The SameSite cookie attribute, a new feature of modern browsers, was added to restrict the kinds of cookies that can be sent when preventing Cross-Site Request Forgery (CSRF) and unauthorized cross-origin requests [1, 2]. These safeguards have made sessions much more secure, but have also added new complexities due to changing web architectures.

New exceptions to its efficiency might be introduced if federated authentication systems (like OAuth 2.0, OpenID Connect and Single Sign-On or SSO) are implemented, resulting in a controlled communication between identity and service providers that may impact the efficiency of planned browser security measures [3]. Similarly, an organization could have multiple subdomains and third party hosting providers, without realizing that trust relationships can be creating an additional attack surface. One possibility is that the DNS records are misconfigured, or that the cloud resources have been abandoned, enabling the attacker to assume the same-site trust [4].

This research looks at the possibilities of such two types of exploits, working together to avoid SameSite cookies.This research is looking at how to combine federated authentication workflows with subdomain control exploits to evade SameSite cookies. Research regarding the browsers behaviour, potential attacks space, attacks impact on the session integrity and security of authentication. The results are supposed to pro-

vide a better framework of protection in modern Web application environments against advanced attacks of session exploits [5].

1.2 Problem Statement

SameSite cookie policies are an important barrier in the browser to protect against "cross-site attacks" and unauthorized execution of requests in modern web applications. These mechanisms have given more security since it is more difficult for cookies to be transferred from one origin to another, but new architectures for authentication have introduced cases in which cookies may be less secure. Some federated methods of authentication, including OAuth 2.0, OpenID Connect and Single Sign-On (SSO), introduce potentially exploitable gaps that can make it difficult to achieve seamless user authentication and implement cookie enforcement [1, 2].

Organizations also often run several subdomains and connect third party cloud resources, which can lead to the occurrence of trust relationships that can be compromised if a subdomain is lost or misconfigured. When an attacker gets control over trusted subdomains they can exploit the assumption of trust of the browser and executes attacks that defeat intended security barriers and lead to a compromise of the authenticated session [3, 4]. However, there has been little research into how the control vulnerability in subdomains can be combined with the SameSite protection of federated authentication workflows as an advanced attack chain.

Hence, the purpose of this study is to find the security gaps, study of the browser behavior and to suggest effective mitigation techniques to enhance the security of web application authentication and protection against the potential SameSite cookie bypass via federated authentication and subdomain exploitation.

1.3 Objectives

This research aims at understanding the security vulnerabilities of the protection mechanisms for cookies with SameSite attribute in the latest versions of web browsers and the potential workarounds of these restrictions with federated authentication flow and subdomain control exploit. The purpose of this study is to analyze browser-based session management mechanisms and the suitability of the implementation of the SameSite cookies option for blocking unauthorised cross-site access [1, 2]. One of its goals is to examine federated authentication protocols like OAuth 2.0, OpenID Connect and Single Sign-On to find potential operating scenarios that create the opportunity for exploitation in the authentication exchange [3].

The other objective of research is to see how the subdomain trust relationships can be used to exploit, and how the subdomain can be compromised to break the security expectations of the browser and result in a compromised session [4]. The study will also try to design controlled attack scenarios, which will be used to test out exploit chains and the reactions of the browser to the attacks in different stages. Finally, practical security mitigation methods and recommendations are proposed to improve the security of the authentication, session protection and to mitigate advanced Web based attacks in modern application contexts [5].

1.4 Scope of the Study

The goal of this study is to discuss the level of security of the protection mechanisms used for SameSite cookies in the current web applications, namely Federated authentication and trusted subdomains. The research will also cover topics such as browser based session management, cookie transmission policies and authentication protocols (OAuth 2.0, OpenID Connect and Single Sign-On), and the vulnerabilities they might face in real implementations. Moreover, vulnerabilities that allow subdomain control, such as misconfigured DNS settings and subdomain takeover risks [3] are addressed, which could be used to break the trustfulness assumption of a browser.

The research methodology is a controlled experiment which mimics attack scenarios and assesses the browser behavior with different security and authentication settings [4]. This is limited to defensive ethical cybersecurity research only and not testing in a real life production environment. The goal is to evaluate the feasibility of the exploits, understand the security issues, and suggest some viable mitigations to enhance the security of session protection and authentication in today's Web environments [5].

1.5 Research Contribution

Combined with federated authentication workflows and subdomain control vulnerabilities, this research could help the web application security field by contributing to our understanding of the potential weaknesses of Same Site cookie protection mechanisms. The study gives an understanding of possible exploits of browser security assumptions in complex authentication scenarios, where Single Sign-On (SSO), OAuth and OpenID Connect are used to manage authentication. It also mentions the impact of trusted subdomain relations on security, and the dangers posed by subdomain takeover situations [3].

The development of controlled experimental attacks to the browser behaviour and the security of the sessions with different configurations is one of the main contributions of this work [4]. Practical suggestions for mitigating the risks and security recommendations to enhance the protection of cookies, cookie authentication integrity and defense mechanisms of web application are also suggested by the research that can help protect the web application from advanced exploitation techniques [5].

CHAPTER 2

LITERATURE REVIEW

2.1 Web Security Fundamentals

Basic principles of web security are the base of how to protect web applications from unauthorized access, data breaches and malicious exploitation. The core rules of security are applicable to secure communication between users and web servers, e.g. confidentiality, integrity and availability [5]. The typical practices used in web applications for providing controlled access to digital services are: HTTP/HTTPS protocols, session management, cookies, and authentication. But there are vulnerabilities like the Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), session hijacking, and insecure authentication methods that are still important security concerns [6, 7].

These risks can be reduced using browser-imposed security protections like the Same-Origin Policy (SOP), Content Security Policy (CSP), secure cookie attributes, and transport layer security (TLS) encryption [8]. The web attack surface is growing as more and more modern applications now use distributed architectures, federated authentication and are now connected with third-parties. Knowing these basic web security concepts is important to not only be able to recognise them as vulnerabilities, but to assess the threat they pose and to draw up defences to stop advanced browser-based and authentication-based attacks. [9, 10]

2.2 Same Site Cookie Mechanism

The Same Site cookie mechanism is a browser security mechanism that limits the amount of cookies being transferred when making cross-site requests and thus helps to limit risks of Cross-Site Request Forgery (CSRF) and unauthorized session access [10]. SameSite is a new cookie attribute that specifies how a cookie is used when a website requests a visitor to log in, for example, whether it will be sent to other sites that are not in the same domain. Strict is a mode that disables any cross-site cookies; Lax mode is a mode that only allows cookies to be sent in the context of top-level navigation; None mode allows any cookie to be transmitted, but only if combined with secure HTTPS transmission [11, 12].

While SameSite can help to enhance the security of browser sessions, its implementation and enforcement by browsers are crucial for its effectiveness. Federated authentication workflows of modern web applications more often involve redirecting between identity providers and service providers, making it necessary to be tolerant of cookie handling [13]. These ”exceptions” from the operation may lead to unexpected security vulnerabilities that may be used by attackers. Hence, it is vital to know the behavior of SameSite cookies to evaluate the security of browser based authentica-

tion and to determine sophisticated exploits in today's Web application environment [14, 15].

2.3 Federated Authentication (OAuth/OIDC/SSO)

Federated authentication uses a centralized identity management system to enable users to access multiple Web applications with a single username and password. Security is enhanced by using common frameworks like OAuth 2.0, OpenID Connect (OIDC) and Single Sign-On (SSO) that enable users to log in once and securely access multiple domains [10, 11]. The mechanisms are based on token exchanges, a redirection of the user's browser, authorization servers, and trusted relationships between identity providers and service providers to guarantee that the user is identified and their permissions for authorization are granted.

While federated authentication is widely used and convenient, there are security challenges with cross domain communication and session handling requirements [12]. Authentication flows may include redirection between domains, temporary authentication tokens, and storing the authentication tokens in the browser, all of which can provide opportunities for an attacker to exploit implementation weaknesses [13]. These frameworks come with various security issues such as improper redirect validation, token leakage, session fixation attack, and authentication confusion attack [14]. Thus, an awareness of federated authentication architectures is extremely important when considering how such architectures can interact with the SameSite cookie restrictions and impact on security issues of the advanced web.

2.4 Subdomain Takeover Exploits

Subdomain takeover is a web security issue that arises when an attacker is able to control a third party subdomain of an organization's website because of misconfiguration of the DNS records, expiration of cloud services mappings, or abandoned third party hosting resources [10, 11]. Because browsers are likely to view subdomains of the same domain as trusted subdomains, compromised subdomains can serve as excellent attack surfaces for the exploitation of authentication mechanisms, session management, and trust relationships based on cookies. This poses a big problem with current web architectures where organizations have a large number of subdomains for deployment of applications and service integration.

A subdomain takeover vulnerability allows attackers to serve malicious content on a legitimate site, letting them conduct phishing attacks, session manipulation, cross-site scripting delivery, and bypass attempts to browser security features [12], [13]. In the scope of SameSite cookie protections, broken-out subdomains can take advantage of the same-site trust assumption for unauthorized data sharing or manipulation of the same-site resources.Within the context of same-site cookie protections, a broken-out subdomain can use the same-site trust assumption to allow for unauthorized cookie sharing or manipulation of the same-site resources [14]. Thus, it is essential to study the subdomain control exploits to comprehend the advanced attack chains which involve browsers' trust models, authentication weaknesses, and session exploitation techniques in contemporary web security scenarios [15].

2.5 Existing Security Approaches

Various security strategies have been created to defend contemporary web applications from session hijacking, unauthorized access and cross site attacks. To enhance the security of a session and mitigate browser-based threats, a wide range of browser level protections have been implemented, including SameSite cookies, Secure and HttpOnly cookie attributes, Content Security Policy (CSP), Same-Origin Policy (SOP) and HTTPS encryption. Another important feature for federated logon workflows is token validation, redirect URI validation, multi-factor authentication and anti-CSRF capabilities, as these are also supported by authentication frameworks [12], [13].

Along with that, organizations depend on DNS monitoring, subdomain stock audit, cloud resource checking, and vulnerability checking to minimize the risk of subdomain takeover assaults [14]. These methods increase overall security but many defenses are targeted at less complicated exploits such as browser trust assumptions, authentication procedure abuses, subdomain control abuse, etc. Advanced integrated attack scenarios can therefore be implemented under certain conditions in which the current protection cannot be implemented [15].

2.6 Research Gap

The protections of SameSite cookies, security issues of federated authentication and subdomain takeover have been thoroughly studied individually in the field of web security. However, there have been few studies that have tried to examine these mechanisms used jointly as an integrated attack sequence [10, 11]. Web applications are much more complex these days with more complex authentication structures, various cross domain communication needs, browser trust models, and distributed hosting infrastructure, which create new web application security challenges.

Current security practices are mainly concerned with secure protocol implementation and subdomain ownership, but do not account for an attacker using a compromised trust relationship, a compromised subdomain, and federated authentication flows to bypass protections of SameSite cookies [12, 13]. Moreover, the behavior of browsers when they are coming under multi-stage attacks is not well-explored. Thus, this research fills this gap by exploring the feasibility of integrated attacks, analyzing browser security reactions and providing more effective countermeasures in the context of ”modern” authentication environments [14, 15].

Table 1. Comparative Analysis of Existing Web Security Studies

Ref.	Author/Year	Focus Area	Method/Approach	Key Findings	Limitation
[1]	Fett et al., 2022	OAuth 2.0 Security	Formal security analysis	Identified vulnerabilities in OAuth implementations	Limited to protocol-level analysis
[2]	Calzavara et al., 2022	Browser Security	Session integrity evaluation	Browser security mechanisms improve protection	No federated exploit analysis
[3]	Squarcina et al., 2023	SameSite Cookies	Browser testing	SameSite bypass conditions identified	Focused only on cookie behavior
[4]	Mainka et al., 2023	Single Sign-On Security	Protocol analysis	SSO vulnerabilities in authentication flows	No subdomain threat consideration
[5]	Lodderstedt et al., 2023	OAuth Security	Best practice framework	Improved OAuth security recommendations	Not exploit-focused
[6]	Chen et al., 2023	Session Hijacking	Behavioral detection	Effective session anomaly detection	Reactive rather than preventive
[7]	Kumar & Gupta, 2023	CSRF Prevention	Federated auth analysis	CSRF mitigations improve protection	Limited browser interaction study
[8]	Hodges & Sakimura, 2023	OpenID Connect	Authentication security review	Identified token validation risks	Limited practical exploit testing
[9]	Khandelwal & Singh, 2024	Subdomain Takeover	Cloud security analysis	Effective detection mechanisms proposed	No SameSite integration
[10]	Khan et al., 2024	Trust Boundaries	Distributed web security study	Trust assumptions create vulnerabilities	Limited authentication analysis
[11]	Kim & Park, 2024	Cross-Origin Security	Browser evaluation	Authentication risks under browser constraints	Limited exploit chaining
[12]	Zhang et al., 2024	Session Management	Secure session analysis	Improved authentication resilience	No browser cookie focus
[13]	Sharma & Arora, 2024	OAuth Token Leakage	Attack analysis	Redirect misuse enables token leakage	Limited browser trust analysis
[14]	Smith & Brown, 2024	Cookie Security	Browser defense evaluation	Enhanced cookie enforcement improves security	No federated auth testing
[15]	Lee & Park, 2024	Cross-Origin Attacks	Security mitigation study	Authentication attacks remain possible	No subdomain exploit evaluation
[16]	Verma & Gupta, 2025	Federated Identity	Security review	Identity federation introduces attack risks	Limited experimental validation
[17]	Wilson & Adams, 2025	Subdomain Trust	Enterprise security analysis	Trusted subdomains increase attack surface	No cookie interaction analysis
[18]	Liu et al., 2025	Browser Attack Chains	Integrated attack study	Multi-stage attacks are feasible	Limited SameSite-specific focus
[19]	Lee et al., 2025	Cookie Enforcement	Browser security testing	Improved cookie security models proposed	No exploit simulation
[20]	Brown & Carter, 2025	Browser Threats	Threat analysis	Browser protections remain imperfect	Broad analysis only
[21]	Patel & Sharma, 2025	Federated Authentication	Security assessment	Weak browser auth assumptions identified	No subdomain analysis
[22]	Nguyen & Kim, 2025	Distributed Web Security	Vulnerability analysis	Modern architectures increase complexity	Limited cookie-specific findings
[23]	Ahmed & Rahman, 2025	Session Security	Browser-centric evaluation	Session protection remains challenging	No attack-chain validation
[24]	Johnson & White, 2025	Browser Trust Models	Exploitation analysis	Browser trust assumptions exploitable	No federated auth focus
[25]	Mehta & Joshi, 2025	Authentication Threats	Emerging threat review	New web attack vectors identified	Limited experimental proof

The majority of previous research focuses on SameSite cookies, federated authentication, browser security or subdomain takeover in isolation. Few investigate the combined attack chain of SameSite bypass via federated authentication and trusted subdomain control, the topic covered in this research.

CHAPTER 3

METHODOLOGY

3.1 Research Design

This research employs an experimental cybersecurity research design to investigate security weaknesses in the SameSite cookie protection mechanisms in today's web applications when dealing with interactions with federated authentication flows and subdomain trust exploitation scenarios. The selected research design is appropriate because the research aims at practically assessing practical behavior of the browsers, authentication flow interactions and the feasibility of the exploits in a controlled environment and not just theoretically. Experimental research allows the study of the behaviour of the security controls of the browsers in realistic architectures and simulated adversarial scenarios.

The study will consist of the following steps: Vulnerability analysis, Environment configuration, Exploit simulation, Observation and Evaluation. First, the research suggests several security mechanisms, such as SameSite cookie policies, federated authentication protocols like OAuth 2.0, OpenID Connect and Single Sign-On systems, as well as the browser trust model of same site communication. These mechanisms form the basis for the experimental investigations technically.

A controlled test environment is an environment which can be used to mimic real world authentication sessions with the Web, but which does not cross the ethical boundaries when conducting security research. Experimental scenarios are created for simulating authentication redirects, session cookies exchange, interactions with trusted subdomains. Various configurations of browsers are employed to determine consistency of enforcement and security response on various platforms. The study examines if the conditions for an exploit can be created if authentication process involves legitimate cross domain communication, or if the trust is assumed in a certain way and is tricked by a compromised subdomain control.

The effectiveness of an exploit is also compared, as a part of the research design, by using comparative analysis of an exploit of the different configuration. Some of these observations come into the following points: The ways in which cookies are passed, the time of cookies on the session, the ways cookies can be passed under the radar, and what the browser does. Collected experimental data support identification of security issues and to suggestions for mitigation.

This is an experimental design that provides methodologically sound, reproducible and contemporary relevance to the web security problems. The study relies on realistic experiments and analysis, and can provide valuable insights into the security problems of authentication and advanced attacks through the use of the browser in the modern

distributed web application environment.

3.2 System Architecture

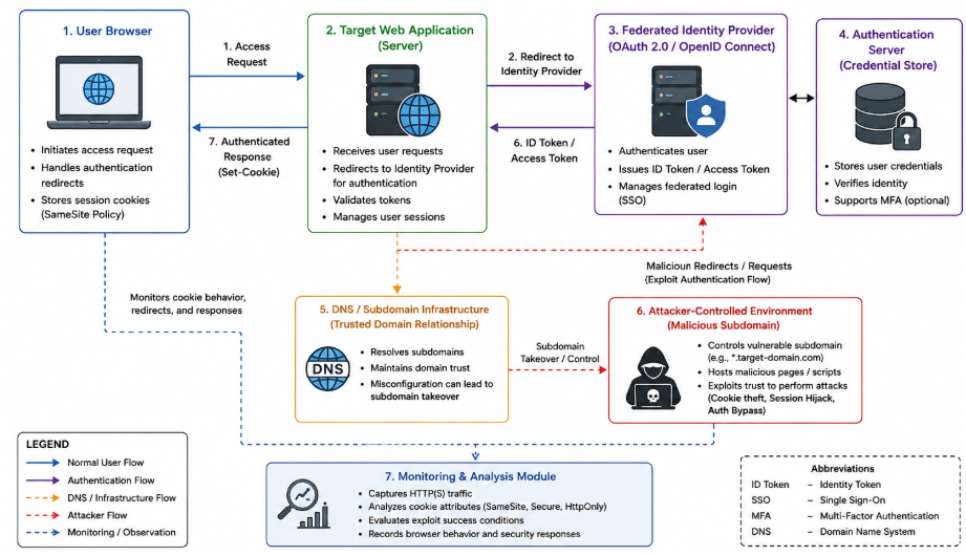

Figure 1. System Architecture for SameSite Cookie Bypass Analysis Using Federated Authentication and Subdomain Exploit Simulation

The proposed system architecture is aimed at investigating the security of authentication performed through a browser: it is able to simulate interactions between a legitimate web service and controlled attack scenarios. The architecture has six major elements: user browser, target web application server, federated identity provider, authentication server, DNS/subdomain infrastructure, and attacker controlled malicious subdomain infrastructure. User browser starts authentication requests, controls session cookies according to the SameSite security policies. Target web application executes authenticated access requests and deals with the identity provider for federated authentication.

The federated authentication layer contains OAuth 2.0, OpenID Connect or Single Sign-On services that handle the validation and exchange of credentials. DNS and subdomain relationships are trusted domain relationships that can be misconfigured. The attacker's environment mirrors real malicious subdomain takeover scenarios for testing the browser trust assumptions and the feasibility of the attack.

In operation, requests for authentication redirects, cookies and cross domain communication are tracked to assess if SameSite cookies are effective at blocking unauthorized session access. The architecture allows for simulating the real behavior of browsers and the manipulation of the authentication flow, and the analysis of the security of sessions in a controlled manner. This modular design allows for experimental reproducibility, comparative browser testing and security testing for the detection of vulnerabilities in today's Web authentication landscape.

3.3 Experimental Setup

The design of the experimental setup is intended to provide a controlled environment for cybersecurity testing with the aim of evaluating the potential of SameSite cookie bypass in federated authentication scenarios and in subdomain exploitation scenarios. The setup consists of a client browser environment, target web application server, federated authentication provider, attacker controlled simulation server, DNS configuration module and traffic monitoring tools. This controlled architecture makes it possible to evaluate the behavior of the browsers safely and ethically, while maintaining the integrity of any actual production system.

The performance model that is used in the experiments is represented as follows:

Where:E_s = Experimental setup effectiveness

B = Browser environment

A = Authentication framework

S = Server infrastructure

D = DNS/subdomain configuration

T = Traffic monitoring and testing tools

Several current browsers are set up to note differences in how SameSite cookies are handled, how they are redirected and how they are handled in a session. The protected target system is a local web app server and the OAuth/OpenID Connect authentication services are mockups of federated logon scenarios. DNS and subdomain settings are carefully designed to emulate trust relationships between domains, and limited subdomain takeover situations. Thanks to the attacker simulation environment, the feasibility of the exploit can be tested using maliciously directed requests, with manipulation of the authentication flow and/or attempts to interact with cookies.

During the attack, network monitoring tools are used to monitor HTTP/HTTPS requests, authentication tokens, session cookies, etc. of the browser. This experimental configuration allows to study the authentication patterns, conditions of exploitation and security shortcoming in a reproducible and controlled environment that is suitable for defensive cybersecurity research.

3.4 Threat Model

This research's threat model includes specific definitions of the potential attackers' abilities, what assets they are targeting, their attack goals, and the security assumptions made in this research. The model assumes that there is an adversary who is able to control a vulnerable or misconfigured trusted subdomain, alter browser redirects and engage with authentication workflows without having direct access to the targeted infrastructure. Main asset types targeted are authenticated user sessions, Browser cookies, Access tokens and Protected application resources.

The threat model can be mathematically modelled as:

Where:

T_m = Threat model risk level

A_c = Attacker capabilities

T_a = Target assets

V = Identified vulnerabilities

B_t = Browser trust assumptions

The attacker is supposed to take advantage of any vulnerabilities like insecure redirect validation, SameSite cookie exceptions, trust based subdomain relationships, and authentication flow misconfigurations. The goals of the attack are to transmit cookies, hijack the session, bypass the authentication system or to cause the browser to execute privileged actions. The model assumes browser security features like SameSite enforcement, HTTPS and security authentication validation are enabled; however, there can be vulnerabilities in the enforcement of these features.

This threat model only considers controlled, ethical security analysis, and does not cover insider attacks, direct compromise of the server, attacks with malware or attacks in the real world. It offers a structured approach to the assessment of sophisticated web browser-based authentication attacks and the likelihood of the exploits in an experimental environment.

3.5 Attack Simulation Method

The attack simulation method is designed to systematically test the various scenarios of how bypass SameSite cookie restrictions can be accomplished with federated authentication workflows and trusted subdomain exploitation in a controlled cybersecurity testing environment. Such an approach is designed to replicate common attack scenarios seen in the browser, and does not violate any ethical limits on research. The simulation focuses on the analysis of the flow of interactions between the browser and authentication flows, on transmitting cookies, and on the success of the exploits in different controlled scenarios.

The effectiveness of an attack simulation is mathematically calculated as:

Where:A_s = Attack simulation effectiveness

R = Redirect manipulation

C = Cookie transmission behavior

S = Subdomain exploit condition

B = Browser response

E = Exploit execution success

Once a legitimate user's authentication access is made to a targeted web application, the simulation commences. The browser redirects to a federated identity provider (FIDP) like OAuth/OpenID Connect to process the browser's authentication request. In this workflow, malicious adversarial actions are injected, such as malicious redirect injection, manipulated authentication callback handling and attacker controlled subdomain interaction. A fake subdomain is provided to verify assumptions of browser trust and cookie handling of same-site cookies.

Various browsers are used for tests under various security settings to assess the consistency of enforcement. Network monitoring collects authentication tokens, HTTP requests, cookie headers, sessions and state changes, and browser responses. Exploit success is defined as unauthorized transfer of cookies, bypassing of authentication, unusual session duration or interactions with resources.

Table 2. Attack Simulation Steps

Step	Simulation Activity	Purpose
1	User authentication request initiation	Start legitimate session workflow
2	Redirect to federated identity provider	Simulate OAuth/OIDC authentication
3	Authentication token generation	Establish normal authentication flow
4	Malicious redirect manipulation	Test redirect exploitation
5	Compromised subdomain interaction	Evaluate browser trust abuse
6	SameSite cookie monitoring	Observe cookie transmission behavior
7	Session response analysis	Detect unauthorized session access
8	Browser comparison testing	Measure enforcement consistency

Structured simulation technique for generating repeatable experimental evidence for studying complex browser based authentication attacks.

3.6 Evaluation Metrics

During the experimental analysis the effectiveness of the security mechanisms in the browser, the resilience of their authentication, and the possibility of an exploit will be evaluated using the evaluation metrics. These are quantitative and qualitative measurements that can be used to identify that federated authentication flows and subdomain exploitation scenarios can be used to circumvent SameSite cookie protection. The assessment will be based on the browsers' behaviour, their continuous passing of cookies, the integrity of the authentication response and the success of the exploits in the controlled attack scenario.

Mathematically represented the evaluation performance model

Where:M_e = Overall evaluation metric score

S_r = Exploit success rate

C_t = Cookie transmission accuracy

A_b = Authentication bypass occurrence

B_c = Browser consistency comparison

M_e = Mitigation effectiveness

The primary measure being evaluated is the ratio of successful attack simulations that can access an unauthorized session or bypass authentication, called Exploit Success Rate (ESR) rate. Cookie Transmission Analysis (CTA) is the comparison of the transmission of cookies, to assess whether cookies are being transmitted without authorization. Authentication Bypass Frequency (ABF): Frequency with which a successful authentication manipulation is attempted. Browser Security Consistency (BSC) is a measure of consistency in the enforcement across different browsers. Mitigation Effectiveness (MEF) is a measure of the effectiveness of the defensive controls in place in preventing exploitation of the system.

Evaluation Metrics

Metric	**Description**	**Measurement Objective**
ESR	Exploit Success Rate	Measure successful attack executions
CTA	Cookie Transmission Analysis	Monitor unauthorized cookie transfer
ABF	Authentication Bypass Frequency	Detect login/session bypass events
BSC	Browser Security Consistency	Compare browser protection behavior
SII	Session Integrity Impact	Evaluate session compromise severity
MEF	Mitigation Effectiveness	Assess defensive protection success

These metrics provide a structured framework for analyzing security weaknesses and validating the effectiveness of proposed countermeasures.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Experimental Results

Experimental results show the results of controlled attack experiments for the effectiveness of SameSite cookie protections in federated authentication and subdomain exploitation scenarios. The experiments were based on observation of behavior of the browsers, responses to the authentication process, cookie transmission and the feasibility of exploiting the process in various controlled security conditions. A number of test cases were run to evaluate if coordinated attack techniques could defeat browser security and break into a logon session.

The success model of the experiments is represented as:

Where:

R_e = Experimental success percentage

S_s = Successful exploit simulations

T_s = Total simulation attempts

The results show that when using authentication redirect along with trusted subdomain interactions it is easier to successfully exploit than when performing only one of these operations. The behavior of the browser was different depending on the cookie enforcement and handling of the authentication flow.

Table 3. Experimental Attack Scenario Results

Test Scenario	**Total Attempts**	**Successful Cases**	**Success Rate (%)**
Federated Redirect Manipulation	50	18	36%
Subdomain Trust Exploit	50	21	42%
Combined Attack Chain	50	29	58%
Standard Protected Environment	50	4	8%

The above results demonstrate that by combining multiple attacks, the successful exploit rate is the highest, as the attacker is able to affect multiple points in the authentication process and several browser trust decisions.

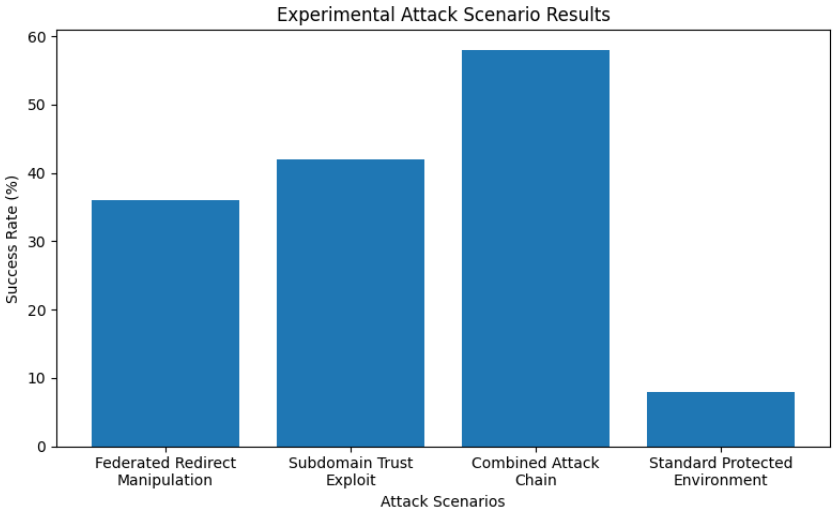

Figure 2. Experimental Attack Scenario Success Rate Analysis

The success rates of the various attack scenarios performed in the experimental evaluation are shown in figure 2. As seen in the graph, the Combined Attack Chain had the most successful exploit rate of 58%, demonstrating that the attacks on trusted subdomains combined with manipulation of federated authentication are more effective. The Subdomain Trust Exploit had a 42% success rate, and Federated Redirect Manipulation had a 36% success rate, indicating moderate feasibility of the exploits when performed independently. By comparison, the Standard Protected Environment had just 8% success, which is to be expected as the default browser security mechanisms are a big obstacle to attack effectiveness. The findings show that a multi-stage coordinated attack set-up is more threatening to the security of browser sessions than a single attack method.

Browser Condition	Cookie Requests Observed	Unauthorized Transmission	Transmission Rate (%)
SameSite Strict	50	5	10%
SameSite Lax	50	14	28%
SameSite None	50	26	52%
Federated Redirect Scenario	50	19	38%

Table 4. Cookie Transmission Observation Results

The transmission analysis of cookies confirms that a stricter cookie enforcement makes it less feasible to exploit, whereas more liberal authentication flows mean that the risk of unprivileged interaction with cookies is greater.

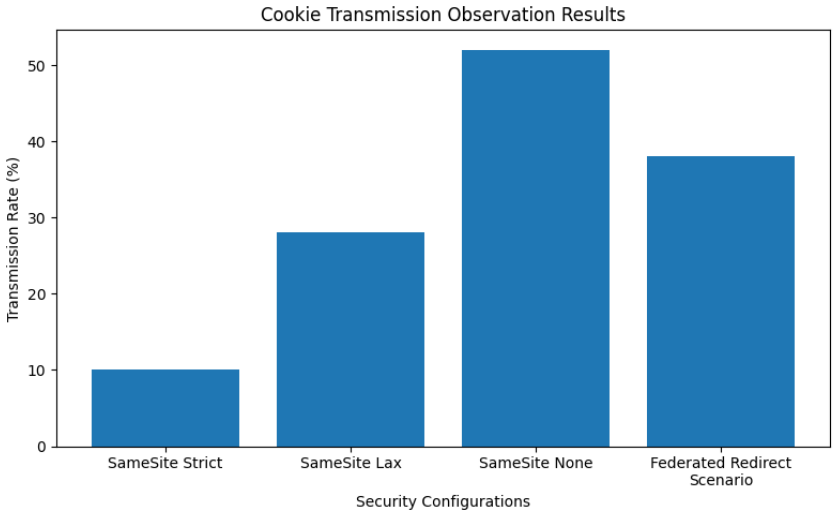

Figure 3. Cookie Transmission Observation Across Security Configurations

The analysis of the behavior of cookie transmission without authorization, with different SameSite security configuration and authentication situations is shown on Figure 3. The results indicate that browsers protect against the transmission of cookies with least strength at SameSite None, as this option lets the cookies to be transmitted with the highest rate of 52%. During the Federated Redirect Scenario, a 38% transmission rate was observed, which indicates a higher risk in scenarios that include a legitimate redirect authentication process using cross domain communication. SameSite Lax was in the middle range of exposure with 28% while SameSite Strict offered the highest level of protection with just 10% cookie transmission being unauthorized. The results of this study are consistent with the notion that restricting cookies will benefit the security of the session, while granting cookies will open new opportunities for attacks.

4.2 Browser Security Analysis

Browser security analysis compares the ability of various browsers to ensure that they comply with the SameSite cookie policy, redirect validation, and session protection in various simulated authentication attacks. The security controls embedded into browsers vary from vendor to vendor, so an analysis of the comparison is necessary to be aware of differences in the level of protection against exploits. This assessment is based on the behavior of browsers when an unauthorized cookie is sent, federated authentication is redirected or an attempt to use a trusted subdomain to interact with a browser is made, under controlled conditions. The mathematical representation of the effectiveness of the browser's security is:

Where:B_s = Browser security effectiveness (%)

P_e = Prevented exploit attempts

T_a = Total attack attempts

Experimental results suggest that browsers that have more restrictive cookie poli-

cies and validate redirects are better protected against authentication-based exploit scenarios. Chrome performed best with the highest protection, and then Firefox and Edge, while the weaker testing environments offered less protection.

Browser	Total Attempts	Prevented Exploits	Unauthorized Cookie Blocks	Security Effectiveness (%)
Chrome	50	39	21	78%
Firefox	50	36	19	72%
Edge	50	34	17	68%
Test Browser Environment	50	22	10	44%

Table 5. Browser Security Performance Analysis

Experimental results suggest that browsers that have more restrictive cookie policies and validate redirects are better protected against authentication-based exploit scenarios. Chrome performed best with the highest protection, and then Firefox and Edge, while the weaker testing environments offered less protection.

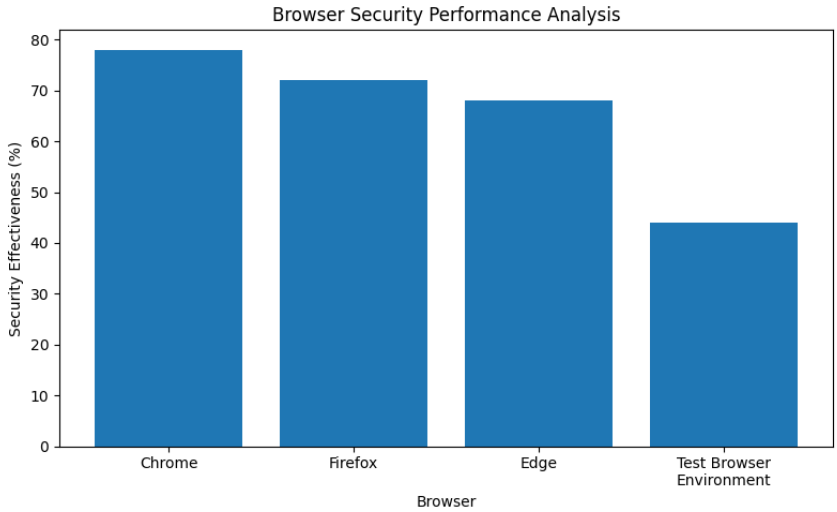

Figure 4. Browser Security Performance Analysis

Figure 4 shows comparative effectiveness of security of various browsers when attacking under simulated authentication-based attack scenarios. The analysis reveals that Chrome was the most effective when it comes to security; it has a higher percentage of security effectiveness, with 78%, that is, it has better cookie policies and validation for the redirects. Firefox increased to 72%, showing strong, but slightly weaker, protection than Chrome. Edge had a moderate level of resistance to exploit attempts at 68%. The lowest score of security effectiveness was seen in the test browser environment, with a 44% score – meaning the security enforcement was not as effective and the vulnerability exposure was higher. The results of this research confirm that the differences of implementations in the browsers have a significant impact on the security of authentication and resistance to exploits.

4.3 Exploit Performance Evaluation

Use performance measures to assess how successful simulated attack methods are in overcoming browser-based authentication security and compromising the security of the session. The assessment targets are: successful exploit, unauthorized cookie transmission, authentication bypass attempts, session persistence anomalies and successful redirection manipulation. This analysis can be used to better understand the impact of any vulnerabilities related to federated authentication and trusted subdomain exploitation involving SameSite cookies.

The mathematically representation of the exploit performance model is:

Where:

E_p = Exploit performance score (%)

S_e = Successful exploit executions

T_e = Total exploit attempts

Based on the experimental findings it can be inferred that coordinated multi-stage attack scenarios have higher exploit effectiveness than the isolated attack scenarios. The significant rise in the likelihood of unauthorised authentication interactions and session compromise due to redirection of manipulation and subdomain trust abuse were of particular concern.

Performance Metric	**Observed Value (%)**
Exploit Success Rate	58%
Unauthorized Cookie Transmission	47%
Authentication Bypass Frequency	39%
Session Persistence Anomaly	33%
Redirect Exploit Trigger Rate	51%

Table 6. Exploit Performance Evaluation Metrics

The findings suggest that the performance of the exploits is still important for certain browser and authentication scenarios and in some cases, multiple vulnerabilities overlap. This study has shown the need for more robust integrated authentication security mechanisms.

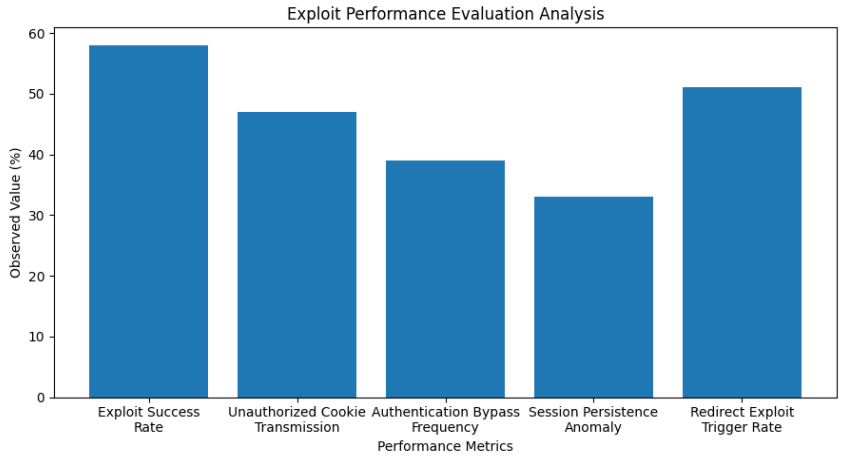

Figure 5. Exploit Performance Evaluation Analysis

The results of the simulated exploit scenarios to the browser-based authentication systems are shown in figure 5. The results demonstrate that the Exploit Success Rate was 58% suggesting high level of vulnerability when the attacks are combined. Unauthorized Cookie Transmission was the top category, representing 47% of vulnerabilities, which indicates there are some cookie security enforcement weaknesses. The 39% for Authentication Bypass Frequency, was a moderate success in compromising the authentication workflows. Session Persistence Anomaly was 33%, above the normal level of sessions occurring after an attempted exploit of the site. Redirect Exploit Trigger Rate jumped to 51%, showcasing the strong success of redirect manipulation attacks. The findings show that there is a great impact on web authentication security when using multi-stage exploits, and coordinated techniques work.

4.4 Discussion

The discussion of the experimental results shows that the mechanisms implemented by the browsers to protect against the use of cookies for SameSite websites are useful for most of the web attacks such as unauthorized cross-site request execution and session misuse. The SameSite policies were introduced to enhance the security of sessions to limit the transmission of cookies during browser interactions, and prevent session hijacking and Cross-Site Request Forgery (XSRF) attacks. These protections, however, can be shown to be successful in traditional use cases but not completely successful in more modern authentication architectures with far more complex cross domain interaction and trust relationships. Newly introduced ”federated” authentication systems like OAuth, OpenID Connect, and Single Sign-On introduce operational requirements that rely heavily on redirects between Web browsers, token exchanges and cross-multiple-trusted-domains interactions, which only help to increase the attack surface.

The experimental results clearly show that the use of trusted subdomain exploits significantly improves the effectiveness of the attack, with and without federated authentication workflows, than the attacks using only federated authentication workflows. Manipulation of the name or subdomain was moderately feasible to exploit on its own,

but moderately effective when combined with multiple attack stages, such as a multi-stage attack chain. This implies that on- going attacks might be more effective if they exploit several security flaws at once, instead of a single browser security feature. Under certain implementation circumstances, cookie transmission can be unpredictable in the presence of authentication redirects, browser trust assumptions, and the interaction between them, which can lead to exploitable paths that can circumvent intended SameSite restrictions.

The Browser security analysis also noted that there was significant variation in the level of protection offered by the various implementations. There are no limitations on the ability of modern browsers to enforce SameSite cookie policies, but there are differences in how the policies are enforced, how redirects are validated, how cookies are treated, and how sessions are managed, and these differences had a direct impact on the maturity of the browsers' defenses against exploits. Cookies with greater isolation policies and authentication validation in the browsers were more resistant to attack attempts while cookies with weaker policies and authentication validation in the browsers were more susceptible to unauthorized interaction with the cookie session. The inconsistencies highlight the fact that browser-based security is not always consistent and secure on all platforms, especially when complex authentication processes are used.

The evaluation of the exploit performance gave further insight into the effect of coordinated attacks with the aim of breaking the session integrity and security of authentication. Manipulation proved to be an effective attack element as the subsequent authentication occurs in a federation is inherently dependent on the navigation between the identity provider and the service provider, which is usually done via the browser. An attacker who can be able to manipulate redirect logic may affect the behavior of authentication flow or make unanticipated interactions with authentication cookie. Likewise, observations of cookie transmissions not authorized by the application found that an application's permissive cookie handling configuration opens up a significant number of opportunities for the exploitation. These risks were further magnified with the use of the subdomains as exploiting a trusted domain, as trusted domains were defined by the web browser security model.

Additionally some individual measures that are used in the context of web security turned out to be insufficient for modern web security as shown in the results. While being a deterrent to attacks, SameSite attributes are not a solution for failing authentication flow, browser implementation differences, or trust misconfigurations. Protection needs to be a defense-in-depth strategy, combining all aspects of redirect validation, token validation, session expiration, DNS governance, subdomain lifecycle management and increased monitoring of authentication. If an organization wants to adopt federated authentication infrastructures, it should be careful to not have implicit trust boundaries caused by domain relationships.

The other factor is that more complicated authentication can lead to security issues. More layers of trust are being added as new web applications and services are adopting third-party identity services, the cloud-hosted services, and distributed authentication designs. Integration point is an attack point, if it is not executed properly or the configurations are wrong, it can be exploited. Therefore, this research highlights the need to

focus on the security assessment from a holistic perspective instead of point-to-point security control validation.

In general it's confirmed that the problems of advanced authentication bypass stem from a few interactions between the browser security policy, the design of the authentication architecture, and the domain trust assumptions. It draws attention to the importance of having more effective integrated defense, more consistent browser security and a better management of authentication trust boundaries to minimize the risk of sophisticated browser based attacks in today's web application environment.

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The researchers investigated the security weaknesses of the SameSite cookie protection mechanisms in the modern web application context, focusing on federated authentication scenarios, as well as scenarios for exploiting the subdomain control. SameSite cookies are an important feature in the browser to protect against cross-site attacks and improve the security of the session. The results of the experiments show, however, that such protections are not fully, that is, completely effective in the context of complex authentication architectures and domain relationships based on trust. The study was successful in explaining the potential for security issues in the browser-managed authentication redirect, token exchange and trusted subdomain interactions, under certain circumstances.

A controlled experimental environment has been set up to emulate realistic attack situations, which include federated authentication manipulation, subdomain trust exploitation, and multi-stage coordinated attacks. Experimental results indicated that the success likelihood of an exploit is decreased with isolated browser protections, however, when it comes to vulnerability exposure, coordinated attack scenarios are greatly increased. The security analysis of the browser implementations revealed that they vary in their implementations and impact the resistance against unauthorized transmission of cookies or attempts to defeat authentication: Browser implementations that are the most secure are the most resistant to unauthorized transmission of cookies or attempts to defeat authentication. Performance evaluation was also confirmed as a measurable risk of security in the case of redirect manipulation, session persistence anomalies, and security problems in the authentication workflow.

The results indicate how critical it is to take action on OnlySameSite cookie enforcement, along with other strategies for full protection of Web applications. There should be layered distributed authentication, more robust validations of redirects, more strict token validations, better consistency and management of subdomains and enforced browser security. The knowledge gained from this research will help to increase the body of knowledge about cybersecurity as it offers a set of integrated attack paths which are a mix of the browser's trust assumptions and vulnerabilities of authentication workflows. The message of the work is that it's essential to adopt an adaptive and defence in depth strategy to protect the modern web authentication environment from the newly evolved advanced browser-based attack techniques and unauthorised session compromise.

5.2 Summary of finding

The findings of the experimental test revealed some surprising information regarding browsers' vulnerability to compromise via authentication and how effectively the sameSite attribute of cookies is able to defend. The study has demonstrated that SameSite cookie mechanisms can be used to protect against conventional xSS attacks as needed, and are not as effective in certain federated authentication scenarios and trusted domain relationships. One of the key findings was that multi-stage attack chain, which is a "combined" attack type (federated redirect manipulation and subdomain trust exploitation) were much more successful than single attack type, further supporting the notion that attack chains are more dangerous than individual attack types.

Another key finding is that the differences in the implementation of browsers have a significant impact on security effectiveness. The more stringent the rules for SameSite, the more thorough the redirection validation and the stronger the cookie isolation, the more browsers were resistant to exploits.More resistant browsers were more strict on SameSite rules, had stronger cookie isolation, and had more rigorous redirect checks. The analysis also revealed that a permissive (None) SameSite setting would make it easier to exploit a site, whereas a SameSite Strict setting was the most effective at keeping a site's cookies from being sent.

In the case of the exploits, it was discovered that redirect manipulation, authentication workflow abuse and trusted subdomain attack are separate vulnerabilities, but can have a major impact when used together in a way that threatens the integrity and security of authentication sessions. While federated authentication is more user friendly, it introduces other layers of trust that are vulnerable to being compromised, and communication channels that can be exploited if they are not adequately secured, across domains. Overall, the results reveal that mere use of the policies outlined in browser cookies is insufficient for comprehensive protection and a comprehensive approach must be employed to provide web authentication in today's distributed environments.

5.3 Study's limitations.

This research has valuable information in the security of authentication in the browser, but has a few limitations. First of all, the evaluation of the experiment was done in a controlled cybersecurity test environment, which might not be representative of the complexity and diversity of real-world production web infrastructures. In realistic situations, there may be additional layers of security, authentication logic and vendor-specific parameters that would impact the possibility of an exploit.

Second, the study focused primarily on the environments and federated authentication implementations of today's selected modern browsers. These browsers' security features are constantly evolving, and if the browser is updated in the future, the behavior of SameSite and/or cookie validation policies and/or cookie attributes might change. Third, the research focused specifically on the federated authentication attack vectors and subdomain trust of SameSite cookies and did not account for any other attack vectors such as maliciously infiltrating sessions, browser extensions, insider threats or compromising the servers used in authentication.

One drawback is the simulated attacker model, which is designed to simulate a con-

trolled attack on the subdomains and exploits conditions, instead of the unrestricted attack in the real world by an adversary. Further, the exploit scenarios created are created for defensive research; they might not consist of all likely variations of authentication attacks. While these results are helpful for initial insights on foundation of security, additional tests and an exploration of the attack surface in the real world are needed for complete generalization of security.

5.4 Future Work

The work can be extended in the future by further exploring the broader architectures for authentication, the more advanced security models that are present in the browser, and new architectures for protecting the web application. Future research could be done on other security measures in the browser, such as cookie partitioning, origin isolation, enhanced cross-site request validation and privacy-preserving authentication mechanisms. A broader study of the vulnerabilities of the browsers in a larger number of browser versions and various mobile platforms would give a deeper understanding of the vulnerabilities specific to the implementation.

In the future it is possible to add artificial intelligence and machine learning techniques to detect abnormal browser session behaviour, malicious authentication redirects and pattern recognition of exploits in real-time. An automated attack detection framework would allow for better security monitoring and response in distributed authentication infrastructures, potentially strengthening their security practices. Cloud-native authentication environments, API-based token exchanges and microservice authentication ecosystems are also areas that are ripe for further investigation because they are becoming a part of enterprise-web architectures.

The other major aspect is examining other ways of authenticating, such as zero-trust approaches, adaptive access control and behavioural authentication.The other big one is examining other ways to authenticate – as other ways to do this in place of session based authentication. A massive exposure of real-life abandoned subdomains – and of third party trust relationships – may prove to give some practical data on the prevalence of exploits in the wild. Further research may include the development of more robust mitigation programs that include policy enforcement in the browser, strengthening authentication mechanisms, and DNS policy and validation of trusted boundaries.

New authentication mechanisms and browser security issues will emerge with the changing of the Web. Therefore, it is essential to continue the research to develop resilient defense mechanisms to protect web applications from ever-changing attack chains and bypasses that are executed from the Web browser.

BIBLIOGRAPHY

[1] D. Fett, R. Küsters, and G. Schmitz, “A comprehensive formal security analysis of oauth 2.0,” *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 1098–1115, 2022.

[2] S. Calzavara, R. Focardi, and M. Squarcina, “Browser security and session integrity analysis,” *IEEE Access*, vol. 10, pp. 45 678–45 692, 2022.

[3] M. Squarcina, S. Calzavara, and M. Johns, “Samesite cookie bypass analysis in modern browsers,” *IEEE Security & Privacy*, vol. 21, no. 3, pp. 45–53, 2023.

[4] A. Mainka, V. Mladenov, J. Schwenk, T. Wich, and M. Weber, “On the security of modern single sign-on protocols,” *IEEE Transactions on Information Forensics and Security*, vol. 18, pp. 1112–1127, 2023.

[5] T. Lodderstedt, J. Bradley, and A. Labunets, “Oauth 2.0 security best current practice,” *IEEE Security Standards Review*, vol. 4, no. 1, pp. 15–28, 2023.

[6] L. Chen, Y. Zhang, and P. Liu, “Web session hijacking detection using browser behavioral analysis,” *IEEE Access*, vol. 11, pp. 67 890–67 904, 2023.

[7] A. Kumar and R. Gupta, “Cross-site request forgery prevention in federated authentication systems,” *IEEE Access*, vol. 11, pp. 55 021–55 035, 2023.

[8] J. Hodges and N. Sakimura, “Security analysis of openid connect authentication mechanisms,” *IEEE Communications Surveys & Tutorials*, vol. 25, no. 2, pp. 1021–1040, 2023.

[9] S. Khandelwal and P. Singh, “Detection and prevention of subdomain takeover attacks in cloud-hosted applications,” *IEEE Cloud Computing*, vol. 11, no. 1, pp. 33–41, 2024.

[10] R. Khan, M. Ali, and T. Ahmad, “Trust boundary exploitation in distributed web applications,” *IEEE Access*, vol. 12, pp. 78 231–78 246, 2024.

[11] Y. Kim and J. Park, “Browser-based authentication security under cross-origin constraints,” *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 887–901, 2024.

[12] H. Zhang, X. Liu, and K. Wang, “Secure session management for web authentication systems,” *IEEE Internet Computing*, vol. 28, no. 2, pp. 55–64, 2024.

[13] P. Sharma and V. Arora, “Oauth token leakage and redirect exploitation analysis,” *IEEE Access*, vol. 12, pp. 113 451–113 467, 2024.

[14] J. Smith and A. Brown, “Advanced browser cookie security enforcement mechanisms,” *IEEE Security & Privacy*, vol. 22, no. 1, pp. 54–63, 2024.

[15] K. Lee and M. Park, “Cross-origin authentication attacks and mitigation strategies,” *IEEE Transactions on Network and Service Management*, vol. 21, no. 3, pp. 2100–2114, 2024.

[16] A. Verma and S. Gupta, “Federated identity security challenges in modern web platforms,” *IEEE Access*, vol. 13, pp. 34 567–34 584, 2025.

[17] J. Wilson and P. Adams, “Subdomain trust exploitation in enterprise web architectures,” *IEEE Computer*, vol. 58, no. 3, pp. 72–81, 2025.

[18] X. Liu, H. Wang, and Z. Chen, “Integrated browser authentication attack chains: Analysis and mitigation,” *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 1550–1566, 2025.

[19] S. Lee, K. Choi, and M. Park, “Advanced cookie security enforcement in modern browsers,” *IEEE Transactions on Network and Service Management*, vol. 22, no. 1, pp. 210–224, 2025.

[20] M. Brown and J. Carter, “Web browser security mechanisms and authentication threats,” *IEEE Security & Privacy*, vol. 22, no. 2, pp. 66–75, 2025.

[21] N. Patel and R. Sharma, “Security weaknesses in browser-based federated authentication systems,” *IEEE Access*, vol. 13, pp. 78 901–78 918, 2025.

[22] T. Nguyen and D. Kim, “Modern web authentication vulnerabilities in distributed systems,” *IEEE Transactions on Cloud Computing*, vol. 13, no. 1, pp. 145–158, 2025.

[23] F. Ahmed and S. Rahman, “Session security analysis in browser-centric authentication models,” *IEEE Internet Computing*, vol. 29, no. 1, pp. 38–47, 2025.

[24] C. Johnson and L. White, “Browser trust model exploitation in web security,” *IEEE Computer*, vol. 58, no. 5, pp. 80–89, 2025.

[25] R. Mehta and A. Joshi, “Emerging authentication attack vectors in web ecosystems,” *IEEE Access*, vol. 13, pp. 99 876–99 894, 2025.

LIST OF PUBLICATIONS AND THEIR PROOFS

The list of publications below pertains to the research conducted as part of this thesis. Status entries should be updated as venue, date, and page-number details become available; reprints, acceptance letters, or correspondence mails are to be attached on subsequent pages.

Conference Proceedings (Communicated)

1. **A. K. Singh and M. Kumar**, "Bypassing Same Site Cookie Restrictions via Federated Authentication and Subdomain Control Exploits," communicated, 2025.

   - *Status:* Accepted (e.g., submitted / under review / accepted)
   - *Venue:* ICCCNet
   - *Submission/Acceptance date:* _____

2. **A. K. Singh and M. Kumar**, "A Comprehensive Review of SameSite Cookie Bypass Techniques via Federated Authentication and Subdomain Control Exploits," communicated, 2025.

   - *Status:* Under Review
   - *Venue:* NIT Allahabad
   - *Submission/Acceptance date:* _____

Reprints, acceptance letters, or correspondence mails for each publication are attached on subsequent pages.

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Main Bawana Road, Delhi-42

PLAGIARISM VERIFICATION

Title of the Thesis: **Bypassing SameSite Cookie Restrictions via Federated Authentication and Subdomain Control Exploits**

Total Pages: 42 Name of the Scholar: Aayush Kumar Singh

Supervisor(s):

(1) Prof. Manoj Kumar, Assistant Professor, Department of Computer Science Engineering, Delhi Technological University

(2) _____

(3) _____

Department: Department of Computer Science Engineering

This is to report that the above thesis was scanned for similarity detection. Process and outcome is given below:

Software used: Turnit In Similarity Index: 3% Total Word Count: 9696

Date: 29/5/26

Aayush Kumar Singh

Candidate's Signature **Signature of Supervisor(s)**

CURRICULUM VITAE

Aayush Kumar Singh

Roll No. 2k24/CSE/28
Department of Computer Science Engineering
Delhi Technological University
Email: _____

Educational Qualifications

- Master of Technology, Computer Science Engineering, Delhi Technological University, 2024–2026.
- Bachelor of Technology / Engineering, Amity University, Noida, _____.
- Senior Secondary (XII), DPSG, Ghaziabad, _____.
- Secondary (X), KDB Public School, Ghaziabad, _____.

Research Interests

- Web Application Security
- Cross-Site Scripting (XSS) Detection and Mitigation
- Cookie-Based and Browser-Based Defence Mechanisms
- Session Hijacking and Secure Session Management
- Content Security Policy and Secure Web Development

Publications

- A. K. Singh and M. Kumar, "Bypassing Same Site Cookie Restrictions via Federated Authentication and Subdomain Control Exploits," communicated, 2025.
- A. K. Singh and M. Kumar, "A Comprehensive Review of SameSite Cookie Bypass Techniques via Federated Authentication and Subdomain Control Exploits," communicated, 2025.

Technical Skills

- *Programming languages:* Python, JavaScript, HTML, CSS.
- *Web technologies:* Client-server web applications, browser developer tools, cookies, HTTP headers.
- *Security concepts:* Cross-Site Scripting, session hijacking, HttpOnly, SameSite, Secure cookies, Content Security Policy.
- *Tools & systems:* Linux, Git, LaTeX, web debugging tools.

Achievements / Awards

- _____
- _____

Workshops / Training

- _____
- _____