



ENGINEER THESIS

To obtain the diploma of **Engineer**
Field: **Computer Science**
Specialty: **Ingénierie des systèmes informatiques (ISI)**

Thème

HTTP Method Interchangeability: Detection, Measurement, and Security Implications

Presented by: **HANNACHI Seif Errahmane**

Submission Date: 23/06/2026

In front of the jury composed of:

BEKKOUCHE Mohammed	President
Bedjaoui Mohamed	Supervisor
Kazi Tani Mohammed Yassine	Co-Supervisor
Matteo Golinelli (University of Trento)	Co-Supervisor
Bousba Fadia Nouna	Examiner

Academic Year: 2025–2026

Abstract

The HTTP specification defines distinct semantics for safe, idempotent methods and unsafe, state-changing methods, yet a substantial fraction of modern web applications accept the same operation over more than one method on the same route. This phenomenon, denoted MI in this work, expands the attack surface of deployed applications. For CSRF, it enables cross-method delivery of payloads that token-validation defences assume are bound to POST: when the same operation is also accepted over GET, those defences can be bypassed because they are anchored to method semantics that the application layer does not enforce. Independently, it can supply the cacheable GET variant that a WCD attack requires. The prevalence of MI in production deployments has, to date, not been measured at scale.

This thesis introduces Method-Interchangeability Detection Engine (MIDE), an automated measurement methodology that crawls web applications in a browser, records the POST requests generated by page loads and user-interface interactions, converts supported POST bodies into GET candidates, and compares the replayed responses against the original POST response. To avoid counting generic or parameter-independent responses as interchangeable, MIDE also sends a no-query GET baseline to the same endpoint, and classifies each request into one of four classes by whether the converted GET and the baseline GET reproduce the POST response: *strong interchangeability* (the converted GET matches but the baseline does not), *ambiguous* (both match), *baseline collision* (only the baseline matches), and *not interchangeable* (neither matches). The approach is implemented as a reproducible capture-and-replay pipeline and is applied to the Tranco top 10k list. Of 14,244 replayed first-party POST requests, 1,228 (8.6%) were classified as strongly interchangeable; this corresponds to a method interchangeability prevalence of 14.9% of eligible sites (407 of 2,734) and 7.8% of replayed routes (646 of 8,291). A targeted CSRF token-replay check over the interchangeable candidates finds cases where an invalid token is rejected for POST but accepted for the equivalent GET, exposing a method-scoped gap in token-validation defences; and a follow-up WCD analysis observes cache-deception conditions and cacheable GET responses for interchangeable request instances. These results provide an empirical basis for discussing the security implications of MI at web scale.

Keywords: HTTP method interchangeability, web security, CSRF, web cache deception, framework parameter binding, large-scale measurement, Tranco.

Résumé

La spécification HTTP définit des sémantiques distinctes pour les méthodes sûres et idempotentes d’une part, et pour les méthodes non sûres modifiant l’état d’autre part ; pourtant, une fraction substantielle des applications web modernes acceptent une même opération via plusieurs méthodes sur la même route. Ce phénomène, désigné par MI dans ce travail, élargit la surface d’attaque des applications déployées. Pour le CSRF, elle permet l’acheminement, par une autre méthode, de charges utiles que les défenses de validation de jeton supposent liées à POST : lorsque la même opération est aussi acceptée via GET, ces défenses peuvent être contournées, car elles reposent sur des sémantiques de méthode que la couche applicative ne fait pas respecter. Indépendamment, elle peut fournir la variante GET mise en cache qu’une attaque WCD requiert. La prévalence de MI dans les déploiements en production n’a, à ce jour, pas été mesurée à grande échelle.

Cette thèse présente Method-Interchangeability Detection Engine (MIDE), une méthodologie de mesure automatisée qui parcourt les applications web dans un navigateur, enregistre les requêtes POST générées par les chargements de pages et les interactions d’interface, convertit les corps POST pris en charge en candidats GET, et compare les réponses rejouées à la réponse POST originale. Pour éviter de compter comme interchangeables des réponses génériques ou indépendantes des paramètres, MIDE envoie également une requête GET de référence sans paramètres (*no-query baseline*) vers le même point d’accès, et classe chaque requête dans l’une de quatre classes selon que le GET converti et le GET de référence reproduisent la réponse POST : *interchangeabilité forte* (le GET converti correspond, mais pas la référence), *ambiguë* (les deux correspondent), *collision de référence* (seule la référence correspond) et *non interchangeable* (aucun ne correspond). L’approche est implémentée sous la forme d’un pipeline reproductible de capture et de rejeu, appliqué au top 10k de Tranco. Sur 14,244 requêtes POST de première partie rejouées, 1,228 (8,6%) ont été classées comme fortement interchangeables ; cela correspond à une prévalence de l’interchangeabilité des méthodes de 14,9% des sites éligibles (407 sur 2,734) et de 7,8% des routes rejouées (646 sur 8,291). Une vérification ciblée de rejeu de jeton CSRF sur les candidats interchangeables relève des cas où un jeton invalide est rejeté pour POST mais accepté pour le GET équivalent, révélant une faille liée à la méthode dans les défenses de validation de jeton ; et une analyse WCD de suivi observe des conditions de tromperie de cache ainsi que des réponses GET mises en cache pour des instances de requêtes interchangeables. Ces résultats fournissent une base empirique pour discuter des implications de sécurité de MI à l’échelle du web.

Mots-clés : Interchangeabilité des méthodes HTTP, sécurité web, CSRF, web cache deception, liaison de paramètres des frameworks, mesure à grande échelle, Tranco.

ملخص

تُعرف مواصفة HTTP دلالات مختلفة للطرائق الآمنة والمتكافئة من جهة، وللطرائق غير الآمنة التي تغير الحالة من جهة أخرى؛ ومع ذلك تقبل نسبة كبيرة من تطبيقات الويب الحديثة العملية نفسها عبر أكثر من طريقة على المسار نفسه. هذه الظاهرة، التي نرسم إليها بـ MI في هذا العمل، توسع سطح الهجوم للتطبيقات المنشورة. ففي حالة CSRF، تتيح إيصال حمولات عبر طريقة أخرى تفترض دفاعات التحقق من الرمز المميز أنها مرتبطة بـ POST: فعندما تُقبل العملية نفسها أيضاً عبر GET، يمكن الالتفاف على تلك الدفاعات لأنها تستند إلى دلالات الطرائق التي لا تفرضها طبقة التطبيق. وبشكل مستقل، يمكن تسلسل MI نحو WCD: فبكشفها عن صيغة GET قابلة للتخزين المؤقت لعملية ديناميكية، توفر مكوناً ضرورياً، وإن لم يكن كافياً بذاته، لهجوم خداع التخزين المؤقت الذي ما يزال يتطلب تحقق شروط إضافية. ولم يُقس انتشار MI في عمليات النشر الإنتاجية على نطاق واسع حتى الآن.

تقدم هذه الأطروحة Method-Interchangeability Detection Engine (MIDE)، وهي منهجية قياس آلية تصفح تطبيقات الويب داخل متصفح، وتسجل طلبات POST الناتجة عن تحميل الصفحات وتفاعلات واجهة المستخدم، وتحول أجسام POST المدعومة إلى طلبات GET مرشحة، وتقارن الاستجابات المُعاد تشغيلها بالاستجابة الأصلية لـ POST. ولتجنب احتساب الاستجابات العامة أو المستقلة عن المعاملات على أنها قابلة للتبديل، يرسل MIDE أيضاً طلب GET مرجعياً بلا معاملات إلى نقطة النهاية نفسها، ويصنف كل طلب ضمن واحدة من أربع فئات بحسب ما إذا كان GET المُحول وGET المرجعي يعيدان إنتاج استجابة POST: قابلية تبديل قوية (يطابق GET المُحول بينما لا يطابق المرجعي)، وملتبسة (يطابق كلاهما)، وتصادم مرجعي (يطابق المرجعي وحده)، وغير قابلة للتبديل (لا يطابق أي منهما). نُفذت المقاربة على شكل خطّ معالجة قابل لإعادة الإنتاج للالتقاط وإعادة التشغيل، وطُبقت على أعلى 10k موقعاً من قائمة Tranco. ومن بين 14,244 من طلبات POST من الطرف الأول المُعاد تشغيلها، صُنّف 1,228 (6.8%) على أنها قابلة للتبديل بقوة، ويقابل ذلك انتشاراً لقابلية تبديل الطرائق بنسبة 9.14% من المواقع المؤهلة (407 من 2,734) و8.7% من المسارات المُعاد تشغيلها (646 من 8,291). وتكشف عملية تحقق موجهة لإعادة تشغيل رمز CSRF المميز على المرشحات القابلة للتبديل حالات يُرفض فيها الرمز غير الصالح عند وصوله عبر POST بينما يُقبل عند وصوله عبر GET المكافئ، ما يُظهر ثغرة مرتبطة بالطريقة في دفاعات التحقق من الرمز المميز؛ كما يرصد تحليل WCD لاحق شروط خداع التخزين المؤقت واستجابات GET القابلة للتخزين المؤقت لدى نماذج الطلبات القابلة للتبديل. توفر هذه النتائج أساساً تجريبياً لمناقشة الانعكاسات الأمنية لـ MI على نطاق الويب.

المعاملات ربط للويب، المؤقت التخزين خداع، CSRF الويب، أمن، HTTP طرائق تبديل قابلية: الكلمات المفتاحية Tranco. واسع، نطاق على القياس العمل، أطر في