Journal of Computing and Security

Research Article, 2021, Volume 8, Number 1
http://www.jcomsec.org

# تشخیص خودکار مقاومت در برابر آسیب‌پذیری CSRF در برنامه‌های تحت وب به‌صورت جعبه سیاه

سمیرا صادقی[آ]، محمدعلی هدوی[آ،*]

[آ] دانشکده مهندسی برق و کامپیوتر، دانشگاه صنعتی مالک اشتر، ایران.

**اطلاعات مقاله**

*تاریخچه مقاله:*
دریافت: 2 February 2020
اصلاح: 21 April 2021
پذیرش: 18 April 2021
انتشار آنلاین: 9 July 2021

*کلمات کلیدی:*
امنیت وب، تشخیص آسیب‌پذیری، جعل درخواست میان‌وب‌گاهی، نشانه ضد CSRF، تجزیه و تحلیل ترافیک.

**چکیده**

حمله CSRF حمله‌ای است که در آن یک وب‌گاه آلوده، مرورگر کاربر قربانی را مجبور به انجام عملی ناخواسته در وب‌گاه مورد اعتماد کاربر می‌کند. اصلی‌ترین روش مقابله با این حمله، استفاده از نشانه‌های تصادفی و غیرقابل حدس در درخواست‌هایی است که مرورگر ارسال می‌کند. از آنجاکه چنین نشانه‌هایی توسط مهاجم قابل حدس زدن و بازسازی نیستند، وی قادر به جعل درخواست‌ها نیست. نشانه‌های استفاده شده می‌توانند مختص هر درخواست، هر صفحه و یا هر نشست باشند. روش‌های موجود برای تشخیص مقاومت در برابر حمله CSRF، عمدتاً به‌صورت فعال بر شبیه‌سازی حمله با تغییر درخواست یا ایجاد درخواست‌های جعلی متکی می‌باشند. این نوع آزمون باید برای هر درخواست در یک برنامه وب تکرار شود تا مشخص شود که آیا برنامه آسیب‌پذیر است. علاوه بر این ارسال درخواست‌های جعلی، ممکن است منجر به تغییرات ناخواسته در وضعیت برنامه شود. در این مقاله روشی برای شناسایی منفعل درخواست‌های مقاوم در برابر CSRF با تجزیه و تحلیل ترافیک در وب‌سایت موردنظر ارائه‌شده است. برای این منظور، ما مجموعه‌ای از قوانین را برای تحلیل وجود احتمالی نشانه‌های ضد CSRF ارائه کرده‌ایم. تجزیه و تحلیل ترافیک بر اساس قوانین پیشنهادی، درخواست‌های مقاوم را به دلیل استفاده از نشانه‌های تصادفی ارائه می‌دهد. درنتیجه، درخواست‌های فاقد چنین نشانه‌هایی احتمالاً آسیب‌پذیر هستند. روش پیشنهادی توسط ترافیک استخراج شده از چندین وب‌سایت اجرا و ارزیابی می‌شود. نتایج تأیید می‌کنند که این روش می‌تواند نشانه‌های ضد CSRF را در درخواست‌ها شناسایی کند و هرچه بازدید وب‌سایت کامل‌تر باشد، نتایج دقیق‌تر خواهد بود.



* نویسنده مسئول.
آدرس‌های رایانامه: s.sadeghi@mut.ac.ir (س. صادقی)،
hadavi@mut.ac.ir (م. هدوی)

ISSN: 2322-4460 