[ICoICT 2021] Your paper #1570709295 ('JSON Web Token Penetration Testing on Cookie Storage with CSRF Techniques')

1 message

icoict@telkomuniversity.ac.id <icoict=telkomuniversity.ac.id@edas.info> Thu, Apr 8, 2021 at 9:52 PM
Reply-To: icoict@telkomuniversity.ac.id
To: Irfan Darmawan <irfandarmawan@telkomuniversity.ac.id>, Aditya Abdul Karim <aditya1995.jr@gmail.com>, Alam Rahmatulloh <alam@unsil.ac.id>, Rohmat Gunawan <rohmatgunawan@unsil.ac.id>
Cc: Anditya Arifianto <anditya@telkomuniversity.ac.id>, Warih Maharani <wmaharani@telkomuniversity.ac.id>, Ade Romadhony <aderomadhony@telkomuniversity.ac.id>, Vera Suryani <verasuryani@telkomuniversity.ac.id>, Dawam Dwi Jatmiko Suwawi <dawamdjs@telkomuniversity.ac.id>, Ong Thian Song <tsong@mmu.edu.my>, Ying Han Pang <yhpang@mmu.edu.my>

Dear Mr. Irfan Darmawan:

On behalf of ICoICT 2021 Program Committee, we regret to inform you that your paper titled “JSON Web Token Penetration Testing on Cookie Storage with CSRF Techniques” has not been accepted to the ICoICT 2021. The overall quality of the papers submitted to the conference is extremely high, so we have to reject a number of good and interesting papers.

Please refer to the following reviewers' comments which we hope will give helpful feedback to your work.

The program committees wish to thank you for submitting your paper and we look forward to receive your new submission in the future.

Best regards,

Dr. Warih Maharani
General Chair of ICoICT 2021

REVIEWS

======= Review 1 =======

> *** Recommendation: Recommendation to accept or reject the paper
Rejected (0)

> *** Detailed Comments: Please give your recommendation whether to accept or reject and suggest improvements in technical content or presentation min.500 chars.

This paper presents an experimental result by conducting penetration testing of the security of JSON Web Token storage on cookie storage using CSRF technique, and subsequently shows that this technique successfully sent faked requests, and that the victim's account was penetrated. While the implementation seems fine to me, I consider this implementation straightforward with little or no research value. There should be some observations derived from this study and the comparison analysis with different techniques in the literature.

Page 1-3rd paragraph has some Malay wordings “ditandatangani secara kriptografis yang dirancang untuk tidak dapat dipalsukan”, to be revised.

======= Review 2 =======

> *** Recommendation: Recommendation to accept or reject the paper
Rejected (0)

> *** Detailed Comments: Please give your recommendation whether to accept or reject and suggest

improvements in technical content or presentation min.500 chars.

The paper "JSON Web Token Penetration Testing on Cookie Storage with CSRF Techniques" presents a replication of tutorial results from OWASP WebGoat and JuiceShop to show that CSRF attacks can be mounted on JWTs in the OWASP testbed setting.

While the paper is well-written in its majority (good explanations and replicable steps in Section IV), I do not see how this is new knowledge as the experiment can be easily lifted from a tutorial site such as https://www.coursera.org/lecture/exploiting-securing-vulnerabilities-java-applications/solution-demo-exploiting-json-web-tokens-jwt-2ZbMb

Most of the literature review work cited also conduct the same experiments using tutorial settings. Maybe my requirements are high, but I think that a publication can only be considered novel and of interest to be published at an academic conference if the attack was found to work on an actual production site rather than a tutorial testbed. My opinion is that works like this manuscript should be disclosed on archival sites or final year project symposiums, not an academic conference.

Moreover, the authors did not discuss concrete steps to rectify the CSRF vulnerability on JWTs, only a single sentence in the conclusion suggesting HttpOnly cookies.

However, I am open to have the TPCs overrule my decision should they deem this conference be a suitable place for disclosure of tutorial results. To the authors receiving this decision, feel free to dispute this decision with the TPCs if tutorials results are allowed.

On some more minor issues, while most of the paper is well written, Section II seems to have been missed-out during proof reading as most of the grammatical errors are found here, e.g. the first sentence already seems off. Another jarring problem is Part 3 of Section IV, where some Bahasa Indon is used in the title. Please revise these errors before publication.