

Cookie Bomb 攻撃を検知するブラウザ拡張機能 Browser extension to detect cookie bomb attack

岡澤 佳寛 * 齊藤 泰一 †
Okazawa Yoshihiro Taiichi Saito

キーワード Cookie , ブラウザ拡張機能, Cookie Bomb 攻撃

あらまし

サーバソフトウェアには、受け入れられる Cookie ヘッダのサイズに上限が設けられている. Egor Homakov[1]は、その上限を利用した Cookie Bomb Attack を提案した. Cookie Bomb Attack とは攻撃者が被害者のブラウザに巨大なサイズの Cookie を設定して、ブラウザがウェブサイトへアクセスする度に巨大なサイズの Cookie を送信させることで、ウェブサイトを利用できないようにすることである. 攻撃によって被害者のブラウザには 4xx エラーや 5xx エラーなどのエラーメッセージが表示される. 被害者にとって、エラーメッセージの内容から、ブラウザが攻撃を受けているのか、サーバ側のエラーなのか判断するのが難しい場合がある[2].

そこで本研究では、被害者側で Cookie Bomb Attack を検知するブラウザ拡張機能を作成した.

参考文献

- [1] Egor Homakov “Cookie Bomb or let's break the Internet.”[Online]
<https://homakov.blogspot.com/2014/01/cookie-bomb-or-lets-break-internet.html> (参照 : 2021/11/30)
- [2] yamory “改行コードに要注意！ HTTP ヘッダインジェクションの概要と対策” [Online]
<https://yamory.io/blog/about-http-header-injection/>
(参照 : 2021/11/30)

* 東京電機大学大学院 工学研究科 情報通信工学専攻,
〒120-8551 東京都足立区千住旭町5, Tokyo Denki University,
5, SenjuAsahi-cho, Adachi-ku, Tokyo, 120-8551, Japan

† 東京電機大学 工学部 情報通信工学科
〒120-8551 東京都足立区千住旭町5, Tokyo Denki University,
5, SenjuAsahi-cho, Adachi-ku, Tokyo, 120-8551, Japan