FUSE: Finding File Upload Bugs via Penetration Testing

作者: Taekjin Lee, Seongil Wi, Suyoung Lee, Sooel Son

出处：†School of Computing, KAIST ‡The Afﬁliated Institute of ETRI

链接：

<https://www.ndss-symposium.org/ndss-program/2020-program/>

**简要**：本文主要论述UFU（Unrestricted File Upload）当中存在的漏洞，通过绕过过滤机制来测试web应用当中这些漏洞的危害性。这个团队利用FUSE方法，已发现了在33个实际web应用中有30多个未知文件上传漏洞。

**主要内容**：

1. 介绍UFU与UEFU（Unrestricted Executable File Upload）漏洞的主要形式以及相关算法。
2. 介绍FUSE方法在PHP、HTML、XHTML、JS文件中的渗透模式，同时列举除了一些威胁模型
3. 详细说明FUSE方法的渗透算法：第一步：统一总链，生成种子测试文件，并通过种子文件进行变型。第二步：变型并上传文件。第三步：确认上传成功。包括上传返回确认、摘要网页回传、文件监控。
4. 详细变型方法介绍。包括：预备学习、执行限制、设置变型向量、生成变型目标。
5. 对每一个变型向量（Mi）进行详细作用分析

**目前缺点**：

1. 测试样本不够多，覆盖面不广（30个应用、630个上传请求）
2. 浏览器会根据部分头文件信息阻止部分的上传请求导致无法测试。