通过尽早检测 CRLF 注入，最大限度地减少 Web 应用程序漏洞

MD AsibulHasan计算机科学与工程系 东南大学asifhasan12355@gmail.com

Md.Mijanur Rahman计算机科学与工程系 东南大学
mijanur.rahman@seu.edu.bd

arXiv:2303.02567v1 [cs.CR] 5 Mar 2023

摘要——**回车（CR）和换行（LF）也称为 CRLF 注入，是一种漏洞，允许黑客向 Web 应用中输入特殊字符，从而改变其运行方式或使管理员困惑。日志投毒和 HTTP响应拆分是这种技术的两种主要危害。此外，攻击者还可以利用 CRLF 注入来攻击其他漏洞，例如跨站脚本攻击（XSS）。电子邮件注入（也称为电子邮件头注入）是另一种可用于改变电子邮件行为的方式。开放式Web应用程序安全项目（OWASP）是一个研究漏洞并根据风险等级对其进行排名的组织。根据 OWASP 的说法，CRLF 漏洞位列十大漏洞之中，属于一种注入攻击。然而，CRLF 漏洞也可能导致发现其他高风险漏洞；在早期阶段采取更好的方法来缓解 CRLF 漏洞，有助于保护应用程序免受已知漏洞的影响。尽管针对其他类型的注入攻击（例如结构化查询语言注入（SQL 注入））已有大量研究，但针对 CRLF 漏洞及如何通过自动化测试检测这类漏洞的研究较少。该主题仍有进一步研究的空间，以便为相关问题提出创新解决方案。通过检查每个请求的头部响应，也有助于减少误报告警。安全系统发出的自动化警报能够更快、更准确地识别潜在漏洞，并有助于减少误报告警。尽管针对 Web 应用程序中各种漏洞的研究十分广泛，但 CRLF 漏洞直到最近才被纳入研究范围。将自动化测试作为一项定期任务，有助于企业持续了解其系统的最新情况并提升安全性。**

关键词——网络安全、***OWASP*** 漏洞、安全检测、***CRLF***注入、注入攻击

I. 引言

网络安全主要关注保护所有连接到互联网的事物，包括应用程序/软件、网络、设备等。应用程序中存在多种漏洞，例如 SQL 注入、跨站脚本攻击（XSS）和本地文件包含（LFI）；网络漏洞则可能包括拒绝服务（DoS）攻击、嗅探和欺骗[3] [4]。为确保网络安全，工程师必须优先保障机密性、完整性和可用性，这三者构成了 CIA 三元组。本研究旨在识别一种特定的应用程序漏洞。网络安全行业规模庞大，主要由两类团队组成：一类为公司工作，另一类则与公司对抗，通常是入侵者。在软件开发生命周期（SDLC）中，每个人都必须遵循这一流程，但由于缺乏理解或高度重视程度不足，一些组织会跳过安全测试。然而，安全测试能够检查软件是否容易受到网络攻击，评估恶意活动的影响，并确定软件的长期成功与否。

大多数研究人员研究了不同类型的漏洞，这些漏洞对 Web 应用程序及其他软件同样具有危害性。然而，针对 CRLF 注入漏洞的研究较少，而它近年来已成为最危险的漏洞之一。由于这一漏洞是最近才被发现的，因此目前尚无关于它的详细研究，这也意味着 CRLF 检测仍有改进空间。研究人员只调查了其他类型的漏洞，这些漏洞的攻击主要基于 HTTP 攻击[1]。本研究仅涉及 Web 应用程序漏洞，这是开发安全应用程序[5]时面临的一个重大问题。CRLF漏洞不像跨站脚本攻击或 SQL 注入 [5][6] 那样常见，但它可能导致其他漏洞，并使系统中的关键信息暴露。如果某个漏洞泄露了公司的内部信息，或暴露了用户／客户的信息，将会给公司造成巨大损失。Web 应用程序中最普遍的缺陷是注入，其中包括 SQL、HTML、CRLF 及其他类型的注入。其他缺陷包括 XSS、访问控制失效、安全配置错误、敏感数据暴露、攻击防护不足、使用存在已知漏洞的组件、使用未受保护的 API、本地文件包含，以及身份验证和会话管理失效 [1][7]。为了解决这一问题，许多研究人员尝试了多种方法，但针对 CRLF 漏洞检测或发现的研究仍然较少，而这一漏洞至今仍是最严重的漏洞之一。它可能暴露系统信息，攻击者也可能从应用程序中窃取机密数据。CRLF 不仅是一种单独的漏洞，还可能导致其他漏洞，尤其是注入类漏洞。

大多数关注自身安全的组织都会聘请安全专家来防止安全漏洞，

请在此处填写适用的资助机构。如果没有，请删除此内容。

并聘请安全工程师手动检查漏洞，但这一过程耗时很长，会降低工作效率。随着网络威胁不断演变，安全工程师越来越多地承担起威胁建模、渗透测试和自动化工作，以主动确定漏洞的严重程度。本文聚焦于一种关键的注入漏洞：CRLF。CRLF 指回车和换行。这是一种注入攻击，可能导致跨站脚本攻击；攻击者借此可以窃取用户会话，在某些情况下还可以提升权限[8][9]。XSS攻击是一种注入方式，攻击者会将恶意脚本注入原本无害且可信的网站。当攻击者利用 Web应用，通过此类在线应用向其他终端用户发送恶意代码（通常是浏览器端脚本）时，就会发生 XSS攻击。Web浏览器的代码通常采用 JavaScript 片段的形式，但也可以是 HTML、Flash 或浏览器能够执行的任何其他类型的代码。[10][11]。XSS漏洞通常允许攻击者伪装成受害用户，执行该用户能够执行的任何操作，并访问该用户的所有数据[6]。已有大量研究围绕 Web应用程序漏洞、网络漏洞及其威胁展开。其中大多数都是危险攻击，能够控制整个系统。然而，尽管 CRLF漏洞是一种尚未得到研究人员充分探索的新型漏洞，尤其是其特定类型的漏洞，仍有一些软件能够完美处理 CRLF漏洞，但这些软件都是付费应用。为了解决 CRLF漏洞问题，本研究将为希望在这一领域开展工作的人提供见解和合乎逻辑的方法。本研究第一部分介绍摘要，第二部分介绍研究背景，第三部分阐述文献综述，随后介绍研究方法，最后给出研究结论。

II. 文献综述

根据我们的研究，已有相当数量的研究关注漏洞管理。其中一些研究聚焦于基于注入的攻击，包括 SQL 注入、HTML注入和代码注入。一项针对孟加拉国教育网站和金融网站上三种主要 SQL注入技术的研究，对 Web 应用程序进行了分析，以确定其安全状况 [1]。但该研究没有提及任何 CRLF漏洞。另有一些案例研究探讨了孟加拉国若干网站中不同类型的漏洞。此外，一些论文还研究了多个领域中的自动化渗透测试和手动渗透测试。一项案例研究使用名为 Tunestore 的在线应用开展安全测试，并以此展示借助工具和人工辅助的 Web应用安全测试。该研究使用 Paros、WebScarab、JBroFuzz、Fortify 和 Acunetix 对 Tunestore 进行了测试。 [5]。

本文旨在消除 Web 应用程序中的 CRLF漏洞，并帮助安全测试人员在产品发布前检测出该漏洞。解决此漏洞还将保护应用程序免受 XSS攻击，因为 CRLF 也可能导致跨站脚本攻击。这些是 OWASP 认定的重大漏洞。

III. 方法论

Web 应用程序中的 CRLF漏洞是一个重大的安全问题，可能造成严重后果。该漏洞允许攻击者将恶意代码插入网页或应用程序中，随后由 Web浏览器或程序执行。这可能导致敏感信息泄露、任意代码执行或拒绝服务攻击。

CRLF 漏洞常通过 CRLF 注入攻击加以利用，即将恶意代码注入网页或应用程序中。为防止 CRLF 注入攻击，必须对所有输入进行适当的验证和清理。任何将用于结构化查询语言（SQL）的用户输入都应经过适当编码，并检查是否包含不正确的字符。此外，及时将所有 Web服务器和应用程序更新至最新版本并安装安全修复也至关重要。

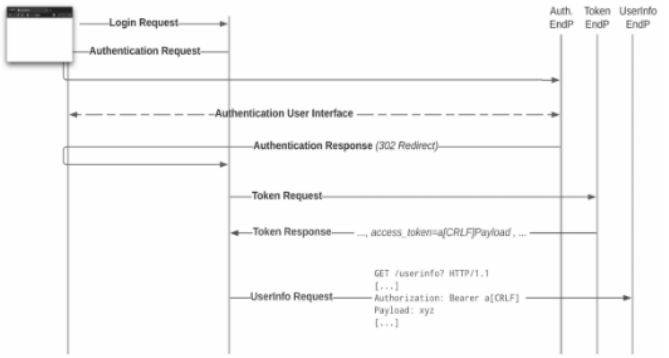

图 01：CRLF 攻击的发生过程

这种 CRLF 攻击会引发更多危害性攻击，包括 XSS、页面注入、Web缓存投毒等。日志投毒和 HTTP响应拆分是这类攻击的常见形式。攻击者通过添加行结束符和额外的行来伪造日志文件条目，从而欺骗系统管理员或掩盖其他攻击 [10]。LF、CR、# 和 ! 是用于发动服务器端攻击的常见 ASCII字符。将这些字符纳入特征集后，即可检测出此类攻击。[2]

利用 CRLF 漏洞的一种方式是向 Web应用注入 CRLF 字符，以利用缓冲区溢出漏洞。另一种利用 CRLF 漏洞的方式是向 Web应用注入 CRLF 字符，以利用 XSS 漏洞。用于发现 CRLF 漏洞的所提框架：

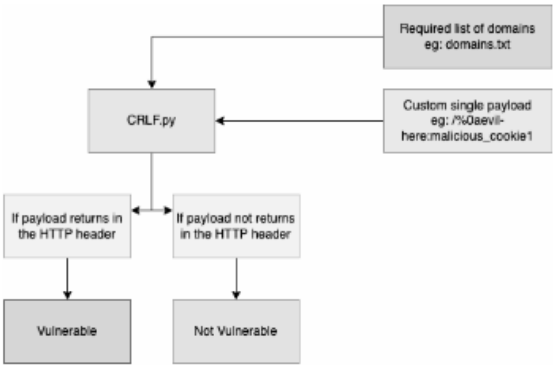

图 02：所提框架

在此图中，用户运行 CRLF 时会输入一组网站链接或单个链接。之后，应用会检查头部响应中是否存在 CR 或 LF 标记，并据此确认应用是否存在漏洞。与其他应用相比，该框架产生的误报告警更少。完整 HTTP GET 请求的摘录如下：[1]

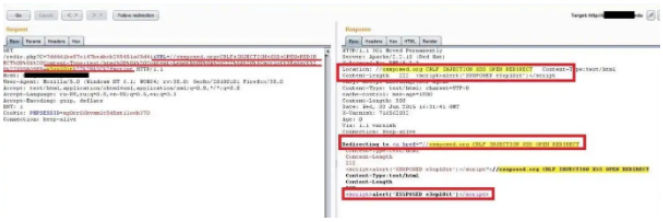

图 03：标头中的 CRLF

在此图中，这是一个标头请求，其中可以找到 CRLF，即 CR 和 LF 标签。

CR 和 LF 是特殊字符（分别为 ASCII 13 和 10，也称为 \r 和 \n），用于表示行尾（EOL）。它们用于标记一行的终止，但在当今流行的操作系统中，其处理方式有所不同。

IV. 结果与讨论

我们的研究重点是确定现实环境中 CRLF 漏洞的存在及其后果，同时探讨潜在的补救措施，以及预防和解决这些问题的最有效方法。研究表明，大量网站和在线应用都受到 CRLF 漏洞的影响，这类漏洞在 Web 应用程序中相当普遍。这些缺陷可能造成严重后果，例如使黑客能够将恶意代码插入网站或应用程序，进而导致数据泄露、身份盗窃及其他安全漏洞。为减轻这些问题，我们建议采用多项质量标准，例如对用户输入进行输入验证、清理和编码，同时定期测试和监控 Web 应用程序，以发现并修复任何漏洞。总之，我们的研究强调，以积极主动的方式处理在线安全至关重要，其中包括定期识别并修补 CRLF 问题等潜在漏洞。通过这样做，企业可以抵御安全漏洞，保障用户的安全，并保护其网站和应用程序。

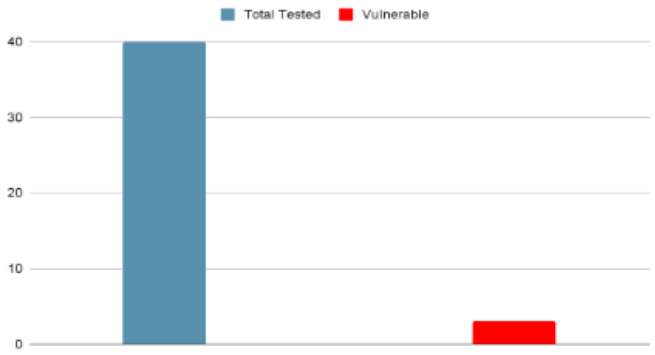

图 04：漏洞图表

这项调查的结果表明，研究人员使用所提出的用于定位 CRLF 漏洞的框架，对共计 40 个网站进行了检查，如图 4 所示。根据数据图表，这 40 个网站中有 3 个被判定容易受到 CRLF 注入攻击。由于某些法律问题，我们无法披露目标网站的名称或网址。

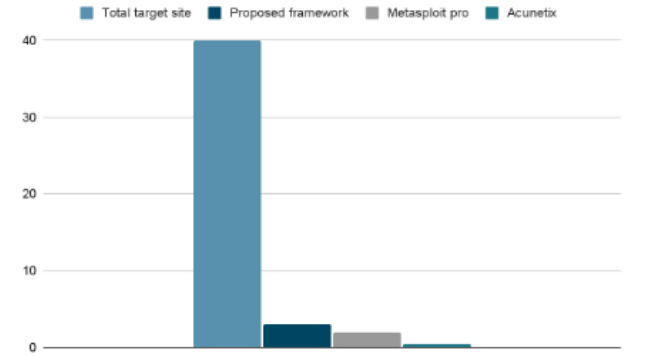

图 05：比较图表

研究结果显示，研究人员使用图 5 所示的三种不同框架，对 40 个网站进行了 CRLF 漏洞检测。根据图中的统计数据，所提出的框架发现的易受攻击网站数量超过了 Acunetix 和 Metasploit Pro 的总和。

V. 结论

本研究旨在增进我们对 Web 应用程序中 CRLF 漏洞的了解。本研究考察了 CRLF 漏洞的特征及其潜在影响，并探讨了发现和降低这些风险的技术。所提出的框架比现有工具更有效，且误报更少。我们的研究表明，在软件开发生命周期中考虑 CRLF 漏洞至关重要，并凸显了此类漏洞对在线应用程序安全性的影响。通过提供实用知识，

这些知识或可帮助个人和组织抵御数字世界中不断变化的威胁，本研究也为网络安全这一更广泛的领域作出了贡献。

参考文献

[1] Hassan, M.M., Bhuyian, T., Sohel, M.K., Sharif, M.H. 和 Biswas, S., 2018. SAISAN：一种自动化本地文件包含漏洞检测模型。《国际工程与技术期刊》，7(2-3)，第4页。 [2] Agarwal, V., Hubballi, N., Chitrakar, A.S. 和 Franke, K., 2019年12月。使用关联规则挖掘识别异常HTTP流量。载于《2019年IEEE高级网络与电信系统国际会议（ANTS）论文集》（第1-6页）。IEEE。 [3] Suroto, S., 2017. 慢速HTTP攻击防御综述。JOIV：《信息学可视化国际期刊》，1(4)，第127-134页。 [4] Kshirsagar, D. 和 Kumar, S., 2016年8月。使用本体检测HTTP洪水攻击。载于《信息通信技术与计算进展国际会议论文集》（第1-4页）。 [5] Dukes, L., Yuan, X. 和 Akowuah, F., 2013年4月。使用工具和手动测试进行Web应用安全测试的案例研究。载于《2013年IEEE东南地区会议论文集》（第1-6页）。IEEE。 [6] Mohammadi, M., Chu, B. 和 Lipford, H.R., 2017年7月。通过自动化单元测试检测跨站脚本漏洞。载于《2017年IEEE软件质量、可靠性与安全国际会议（QRS）论文集》（第364-373页）。IEEE。 [7] Buja, G., Abd Jalil, K.B., Ali, F.B.H.M. 和 Rahman, T.F.A., 2014年4月。SQL注入攻击检测模型：防止Web应用遭受SQL注入攻击的方法。载于《2014年IEEE计算机应用与工业电子学研讨会（ISCAIE）论文集》（第60-64页）。IEEE。 [8] Ami, P.V. 和 Malav, S.C., 2013. Web 应用程序面临的五大危险安全风险。《计算机科学新兴趋势与技术国际期刊》，2(1)，第41-43页。 [9] Al-Khurafi, O.B. 和 Al-Ahmad, M.A., 2015年12月。Web应用漏洞攻击综述。载于《2015年第四届高级计算机科学应用与技术国际会议（AC-SAT）论文集》（第154-158页）。IEEE。 [10] Gupta, S. 和 Gupta, B.B., 2015年5月。PHP-sensor：一种用于发现PHP Web应用程序中的工作流违规和XSS漏洞的原型方法。载于第12届ACM计算前沿国际会议论文集（第1-8页）。 [11] Shar, L.K. 和 Tan, H.B.K., 2012. 自动消除Web应用程序中的跨站脚本漏洞。《信息与软件技术》，54(5)，第467-478页。