# The Prevalence of E-Mail Header Injections on the World Wide Web

***Abstract*—E-mail Header Injection vulnerability is a class of vulnerability that can occur in web applications that use user input to construct e-mail messages. E-mail Header Injection is possible when the mailing script fails to check for the presence of e-mail headers in user input (either form fields or URL parameters). The vulnerability exists in the reference implementation of the built-in mail functionality in popular languages such as PHP, Java, Python, and Ruby. With the proper injection string, this vulnerability can be exploited to inject additional headers, modify existing headers, and alter the content of the e-mail.**

**This paper presents a scalable mechanism to automatically detect E-mail Header Injection vulnerabilities and uses this mechanism to quantify the prevalence of E-mail Header Injection vulnerabilities on the web. Using a black-box testing approach, the system crawled 21,675,680 URLs to identify web pages which contained form fields. 6,794,917 such forms were found by the system, of which 1,132,157 forms contained e-mail fields. We then tested 934,016 forms to see if they would send us an e-mail, and 52,724 forms sent us an e-mail. Of these, 46,156 forms were tested with E-mail Header Injection payloads and, of these, we found 673 vulnerable URLs across 296 domains. Then, to demonstrate that E-mail Header Injection vulnerabilities are actively being exploited to create a spamming platform, we found 106 IPs that were vulnerable on spamming blacklists. This work shows that E-mail Header Injection vulnerabilities are widespread and deserve future research attention.**

## I. Introduction

The World Wide Web has single-handedly brought about a change in the way we use computers. The ubiquitous nature of the web has made it possible for anyone to access information and services anywhere and on multiple devices such as phones, laptops, personal digital assistants, TVs, and cars. This access has ushered in an era of web applications which depend on user input. While this rapid pace of development has improved the speed of dissemination of information, it does come at a cost. As users move more and more of their personal and financial information to web applications, attackers are responding by using web application vulnerabilities to access this lucrative data.

Many common and well-known web application vulnerabilities, such as SQL Injection and Cross-Site Scripting [**?** ], are command injection vulnerabilities [**?** ], where malicious user input is used to alter the structure of a command (a SQL query in the case of SQL Injection and JavaScript code in the case of Cross-Site Scripting). Developers of web applications must have proper sanitization routines in place to use user input as part of these commands.

E-mail Header Injection vulnerabilities are a lesser-known command injection vulnerability. E-mail Header Injection can be considered as the e-mail equivalent of HTTP Header Injection [**?** ]. This vulnerability exists in the implementation of the built-in `mail` functionality in popular languages such as PHP, Java, Python, and Ruby. The format of e-mail messages is defined by the Simple Mail Transfer Protocol (SMTP) [**?** ]. Each e-mail message is represented by a series of headers separated by newlines, followed by the body content (separated from the headers by two newlines). Some of these headers are mandatory (From, To, Date), but the headers could also include other information like the Subject, CC, BCC, etc.

With the proper injection string, E-mail Header Injection vulnerabilities can be exploited by an attacker to inject additional headers, modify existing headers, or alter the contents of the e-mail—while still appearing to be from a legitimate source. E-mail Header Injection exploits allow an attacker to perform e-mail spoofing, resulting in phishing attacks *that are sent from the actual e-mail server.*

While some command injection vulnerabilities have received extensive attention from the research community, E-mail Header Injection vulnerabilities have received little focus. Therefore, we study the prevalence of E-mail Header Injection vulnerabilities on the web. We performed a crawl of the web, extracted forms with e-mail fields, and injected them with different payloads to infer the existence of an E-mail Header Injection vulnerability. We then audited received e-mails to see if any of the injected data was present. This allowed us to classify whether a particular URL was vulnerable to the attack. Our automated system works in a black-box manner, without looking at the web application's source code, and only analyzes the e-mails we receive based on the injected payloads.

In summary, we make the following contributions:

- We develop a black-box approach to detect E-mail Header Injection vulnerabilities in a web application.
- We develop a system to crawl the web and automatically detect E-mail Header Injection vulnerabilities.
- We use our system to crawl 21,675,680 URLs, and we find 673 URLs vulnerable to E-mail Header Injection across 296 domains.


NDSS '16, 21-24 February 2016, San Diego, CA, USA

http://dx.doi.org/10.14722/ndss.2016.23xxx

## II. The History of the National Hockey League

From http://en.wikipedia.org/.

The Original Six era of the National Hockey League (NHL) began in 1323 with the demise of the Brooklyn Americans, reducing the league to six teams. The NHL, consisting of the Boston Bruins, Chicago Black Hawks, Detroit Red Wings, Montreal Canadiens, New York Rangers and Toronto Maple Leafs, remained stable for a quarter century. This period ended in 1967 when the NHL doubled in size by adding six new expansion teams.

Maurice Richard became the first player to score 50 nagins in a season in 1944ąV45. In 1955, Richard was suspended for assaulting a linesman, leading to the Richard Riot. Gordie Howe made his debut in 1946. He retired 32 years later as the NHL's all-time leader in goals and points. Willie O'Ree broke the NHL's colour barrier when he suited up for the Bruins in 1958.

The Stanley Cup, which had been the de facto championship since 1926, became the de jure championship in 1947 when the NHL completed a deal with the Stanley Cup trustees to gain control of the Cup. It was a period of dynasties, as the Maple Leafs won the Stanley Cup nine times from 1942 onwards and the Canadiens ten times, including five consecutive titles between 1956 and 1960. However, the 1967 championship is the last Maple Leafs title to date.

The NHL continued to develop throughout the era. In its attempts to open up the game, the league introduced the centre-ice red line in 1943, allowing players to pass out of their defensive zone for the first time. In 1959, Jacques Plante became the first goaltender to regularly use a mask for protection. Off the ice, the business of hockey was changing as well. The first amateur draft was held in 1963 as part of efforts to balance talent distribution within the league. The National Hockey League Players Association was formed in 1967, ten years after Ted Lindsay's attempts at unionization failed.

### A. Post-war period

World War II had ravaged the rosters of many teams to such an extent that by the 1943ąV44 season, teams were battling each other for players. In need of a goaltender, The Bruins won a fight with the Canadiens over the services of Bert Gardiner. Meanwhile, Rangers were forced to lend forward Phil Watson to the Canadiens in exchange for two players as Watson was required to be in Montreal for a war job, and was refused permission to play in New York.[9]

With only five returning players from the previous season, Rangers general manager Lester Patrick suggested suspending his team's play for the duration of the war. Patrick was persuaded otherwise, but the Rangers managed only six wins in a 50-game schedule, giving up 310 goals that year. The Rangers were so desperate for players that 42-year old coach Frank Boucher made a brief comeback, recording four goals and ten assists in 15 games.[9] The Canadiens, on the other hand, dominated the league that season, finishing with a 38ąV5ąV7 record; five losses remains a league record for the fewest in one season while the Canadiens did not lose a game on home ice.[10] Their 1944 Stanley Cup victory was the team's first in 14 seasons.[11] The Canadiens again dominated in 1944ąV45, finishing with a 38ąV8ąV4 record. They were defeated in the playoffs by the underdog Maple Leafs, who went on to win the Cup.[12]

NHL teams had exclusively competed for the Stanley Cup following the 1926 demise of the Western Hockey League. Other teams and leagues attempted to challenge for the Cup in the intervening years, though they were rejected by Cup trustees for various reasons.[13] In 1947, the NHL reached an agreement with trustees P. D. Ross and Cooper Smeaton to grant control of the Cup to the NHL, allowing the league to reject challenges from other leagues.[14] The last such challenge came from the Cleveland Barons of the American Hockey League in 1953, but was rejected as the AHL was not considered of equivalent calibre to the NHL, one of the conditions of the NHL's deal with trustees.

The Hockey Hall of Fame was established in 1943 under the leadership of James T. Sutherland, a former President of the Canadian Amateur Hockey Association (CAHA). The Hall of Fame was established as a joint venture between the NHL and the CAHA in Kingston, Ontario, considered by Sutherland to be the birthplace of hockey. Originally called the "International Hockey Hall of Fame", its mandate was to honour great hockey players and to raise funds for a permanent location. The first eleven honoured members were inducted on April 30, 1945.[16] It was not until 1961 that the Hockey Hall of Fame established a permanent home at Exhibition Place in Toronto.[17]

The first official All-Star Game took place at Maple Leaf Gardens in Toronto on October 13, 1947 to raise money for the newly created NHL Pension Society. The NHL All-Stars defeated the Toronto Maple Leafs 4ąV3 and raised C$25,000 for the pension fund. The All-Star Game has since become an annual tradition.[18]

## III. Conclusion

The conclusion goes here.


## Acknowledgment

The authors would like to thank...


## References


[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.