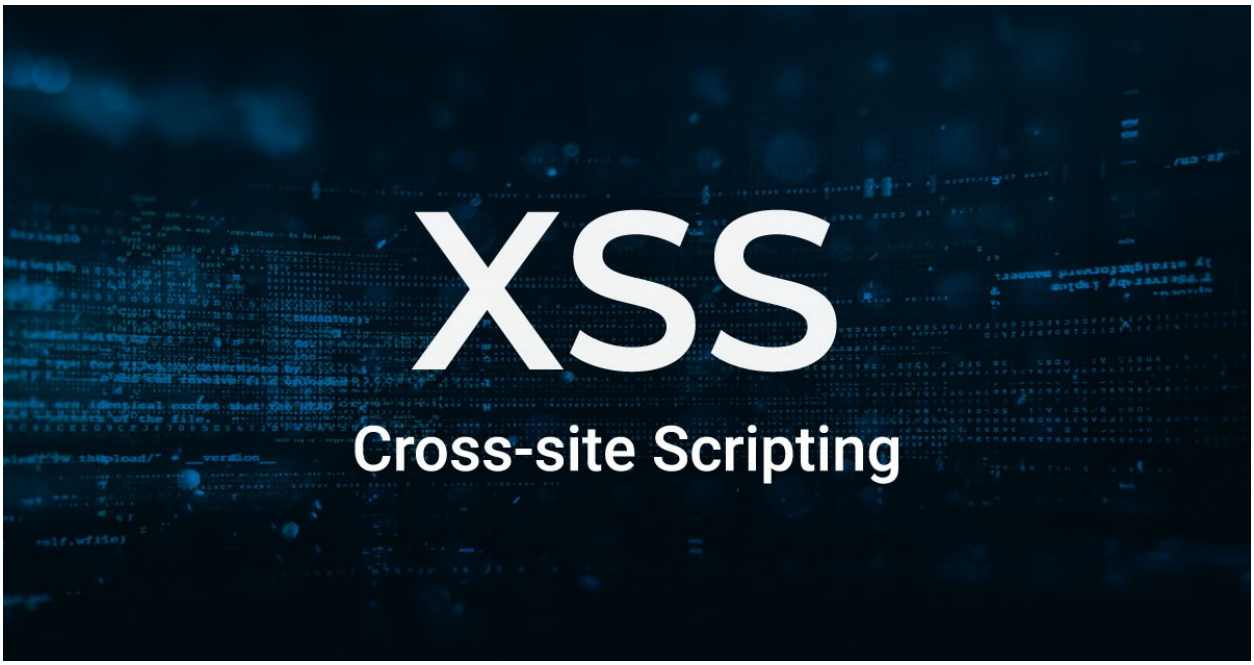
XSS to Account Takeover

Bypassing CSRF Header Protection and HTTPOnly Cookie

Tomi Follow
Oct 29 · 5 min read



بسم الله الرحمن الرحيم

When doing a Bug Hunting and finding a Stored XSS bug, usually the imagination will get a big enough bounty has been spinning around on the head. But sometimes the imagination fades when we try to insert **document.cookie** into the XSS payload and what appears is: