



# Web Application Defender

---

K. V. Prashant & Mohammed Imran

# Who We are.....

- K.V.Prashant(kvbbhai)
  - Security Consultant, working for IT services company
  - CISSP & CEH, member of null open security and hacking community
- Mohammed Imran(Imran Bhai)
  - Security Researcher, working for IT services major
  - CEH, SCJP, Member of OWASP, Matriux and null community





## What are you going to tolerate for next 30 mins...

---

**Web Application Defender:** A tool currently in development

**What it does:-**

we are trying to propose a mechanism for whitelisting based request filtering. Basically know and allowing inputs what you think is valid.

**How is it different from Web Application Firewall:**

Convention Firewalls work on the concept of blacklist. WAF block request what they feel is incorrect.

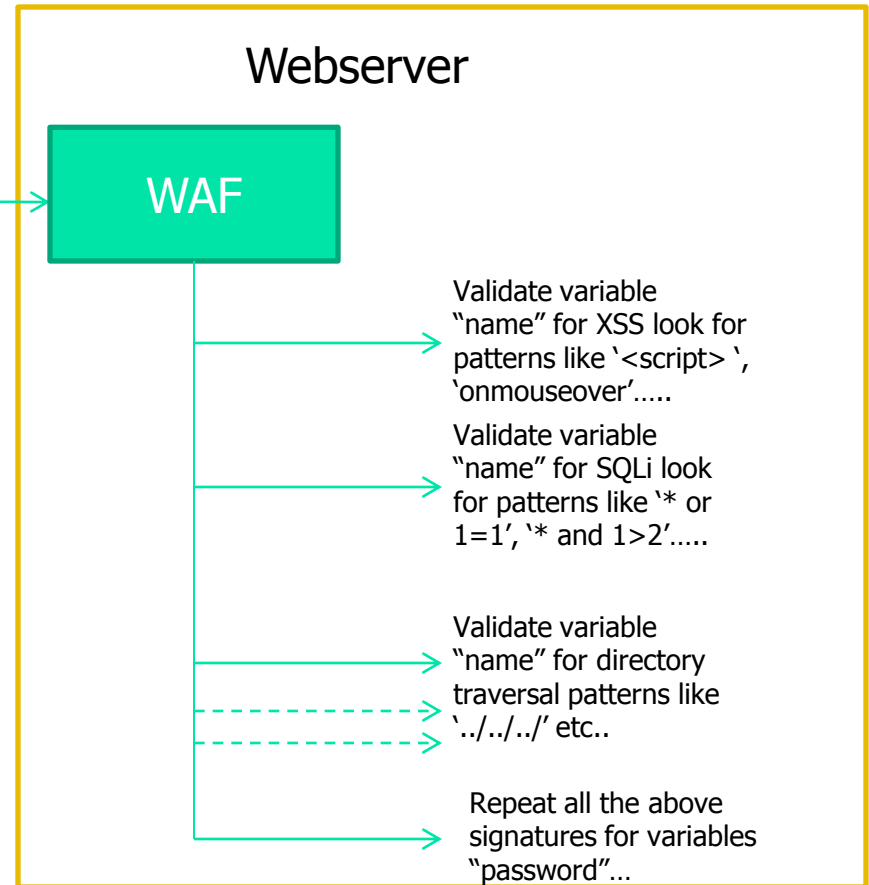
**Advantage:**

A properly configured WAD will be faster, tightly coupled with application

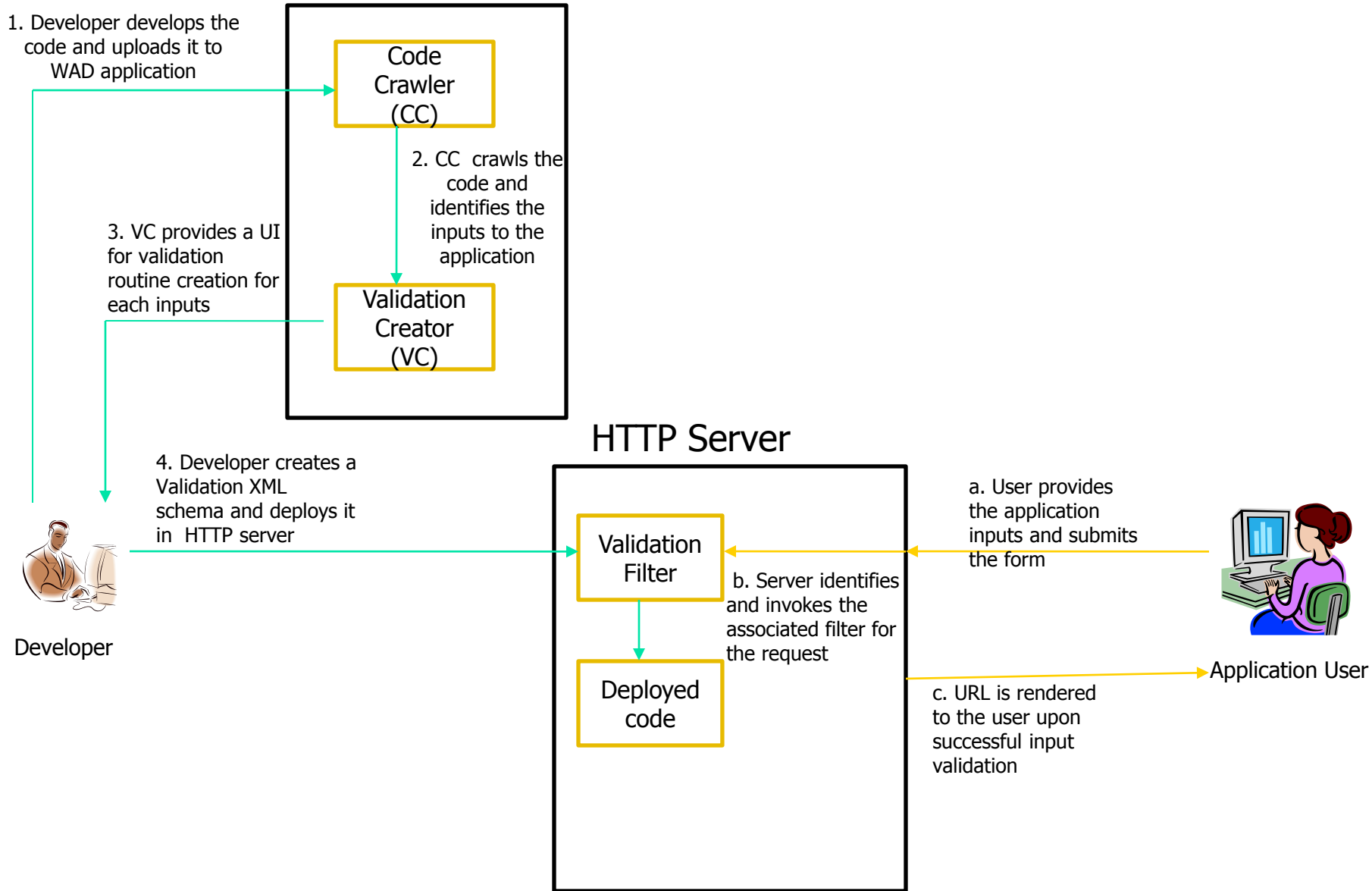
# Working of a typical WAF



Site.com/Login.jsp?username  
=name&password=password



# Web Application Defender (WAD)





# Components used

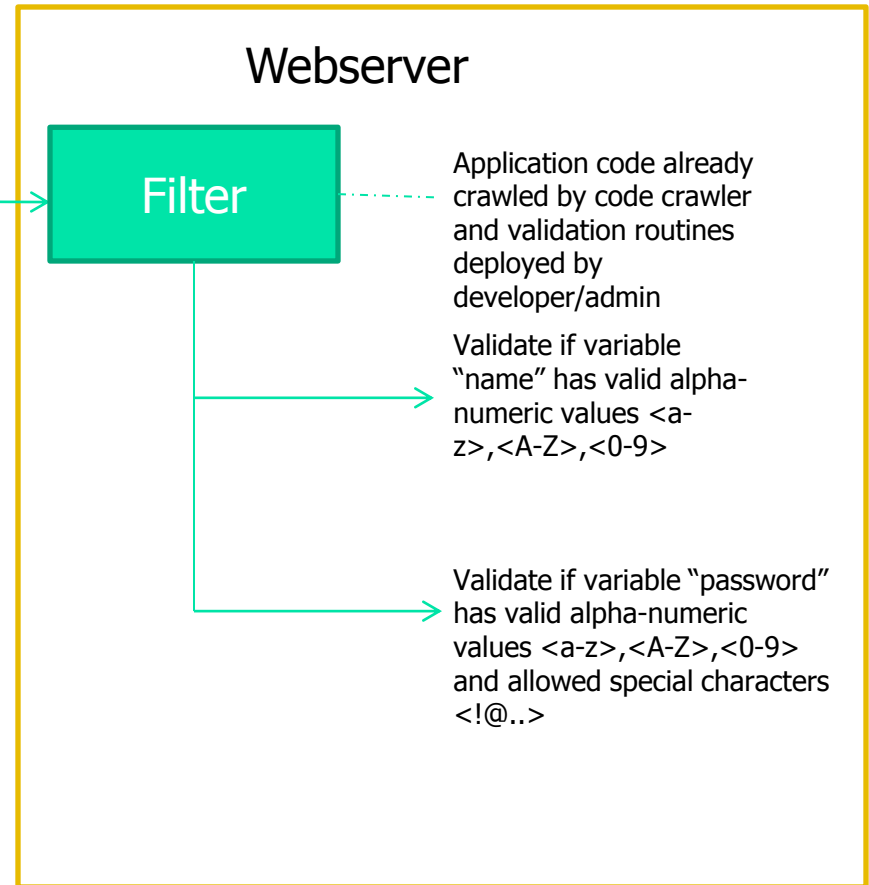
---

- **OWASP Code Crawler** : To be used for code crawling and input identification. Wrappers to be written to identify input keywords. Plan to develop it as a full fledge manual code review tool.
- **Validation Creator(VC)**: Custom UI component , To help tool user to create input validation schema.
- **OWASP Stinger Tool**: To use the validations developed by VC module.

# Working of a WAD



Site.com/Login.jsp?username  
=name&password=password





# Some Disadvantages

---

- Essentially not plug and play
- Requires manual intervention
- Technology stack dependent & tightly coupled with application and web server





# Road Ahead.....

---

- Adding more capabilities to tool to handle/validate:
  - CSRF
  - HTTP Method validation
  - Add wrappers to develop code crawler as a manual code review tool

..... Eliminate evil 😊.....



Thanks for tolerating us

---

Special thanks to Securitybyte Team