

Initial Access with sqlmap



Casey Dunham

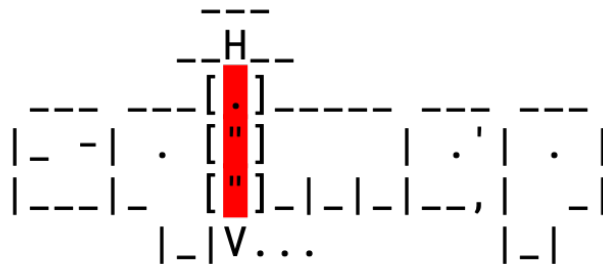
APPLICATION SECURITY CONSULTANT

@CaseyDunham www.caseydunham.com



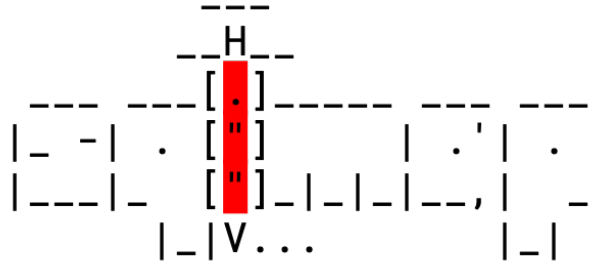
			H						
			[.]				
			["]				
			["]				
			V	.	.	.			





Creators: Bernardo Damele A. G.
and Miroslav Stampar



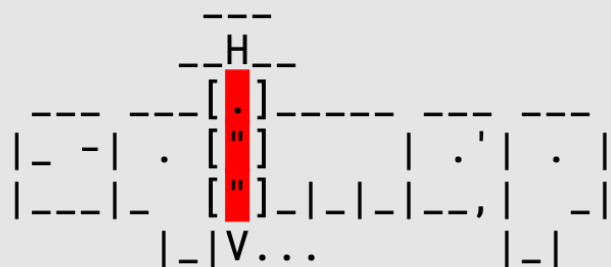


Creators: Bernardo Damele A. G.
and Miroslav Stampar



Used to automate the process of detecting and exploiting SQL injection flaws. Powerful detection engine for database fingerprinting, data exfiltration, and underlying operating system access.





Available for download at

<http://sqlmap.org/>

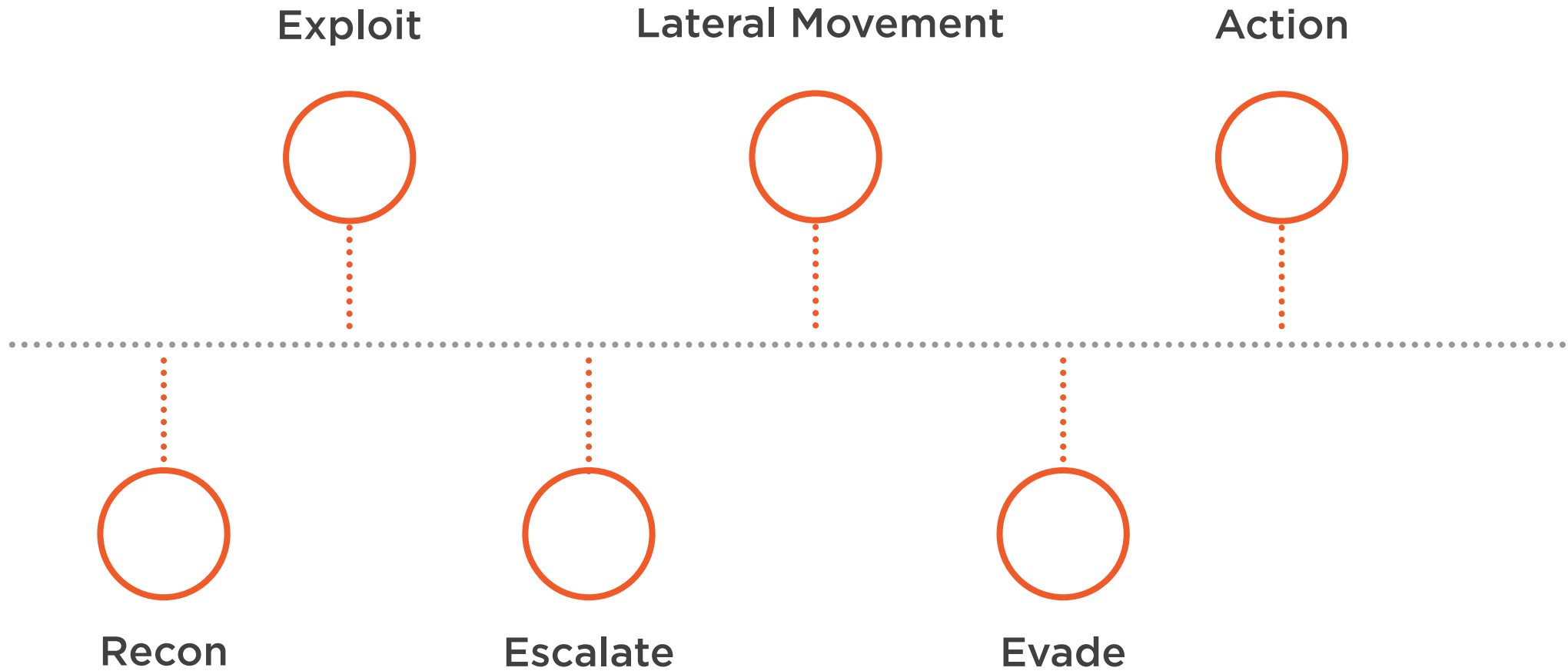
github.com/sqlmapproject/sqlmap

Works out of the box on any platform
that runs Python 2.6, 2.7, or 3.x

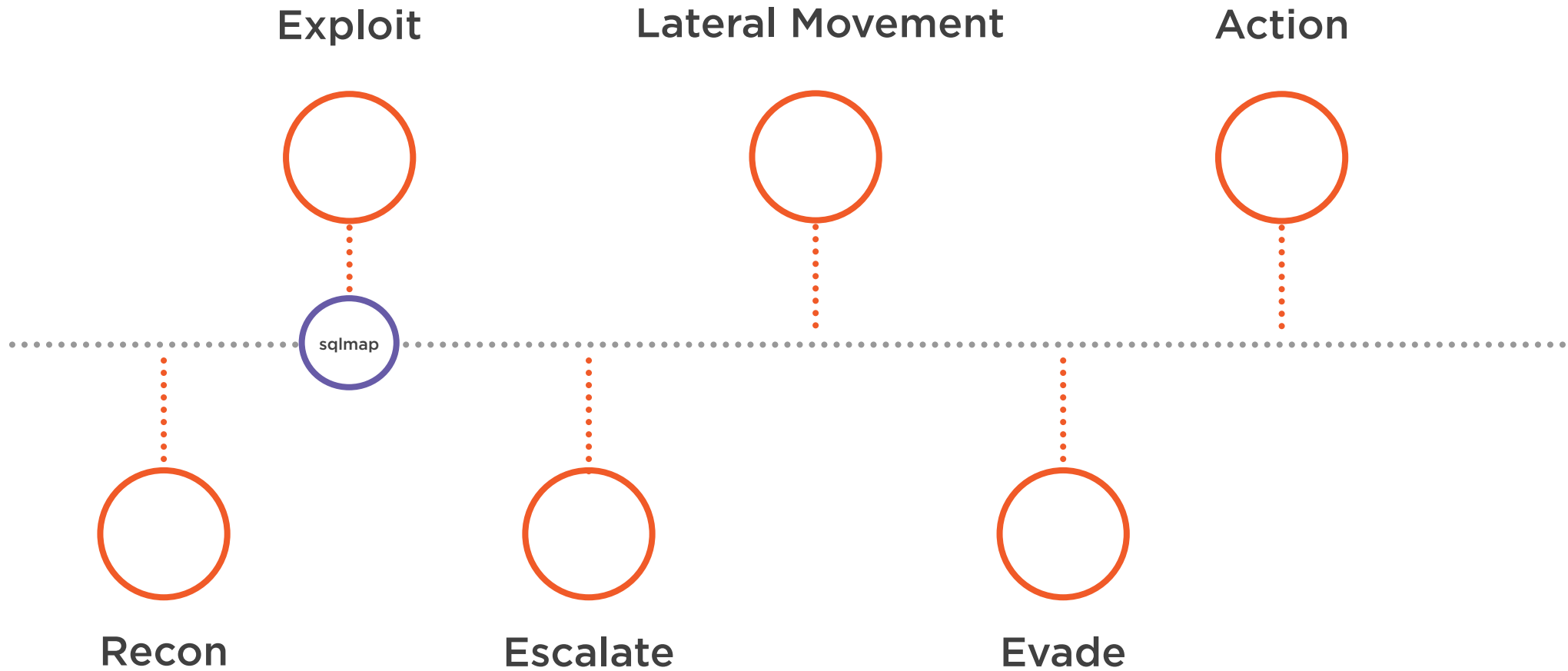
Pre-installed on Kali Linux 2020.2



Kill Chain



Kill Chain



MITRE ATT&CK



MITRE ATT&CK

Tactics



MITRE ATT&CK

Tactics

- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command & Control
- Exfiltration
- Impact



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact



MITRE ATT&CK

Tactics

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command & Control

Exfiltration

Impact

T1190:

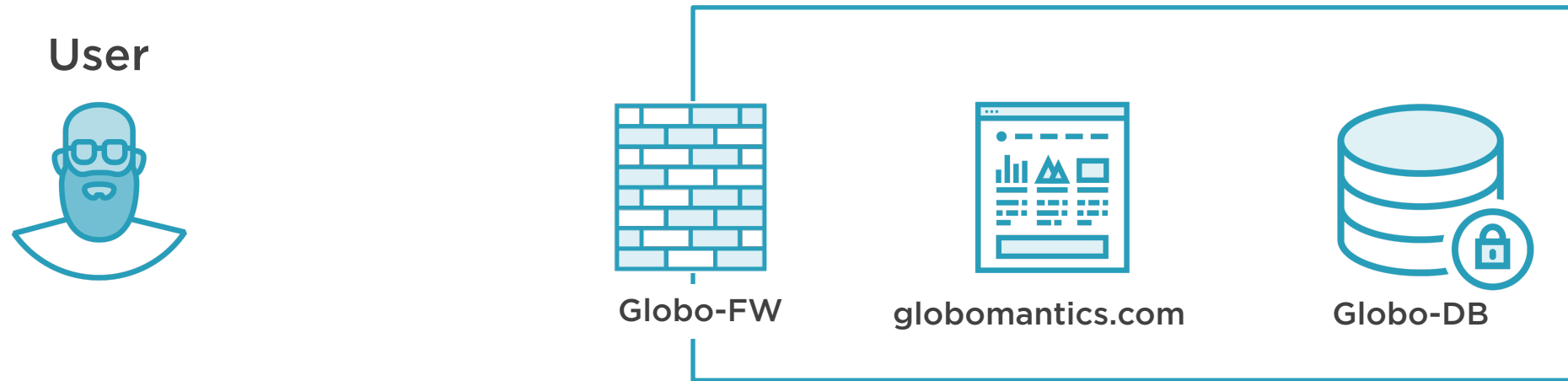
Exploit Public Facing Application



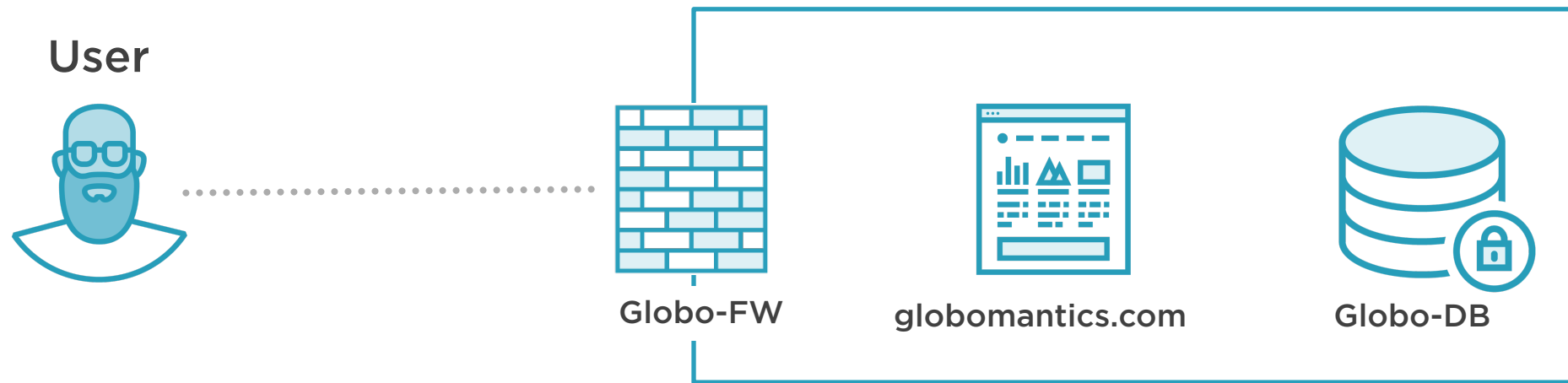
Anatomy of a Typical SQL Injection Attack from the User Perspective



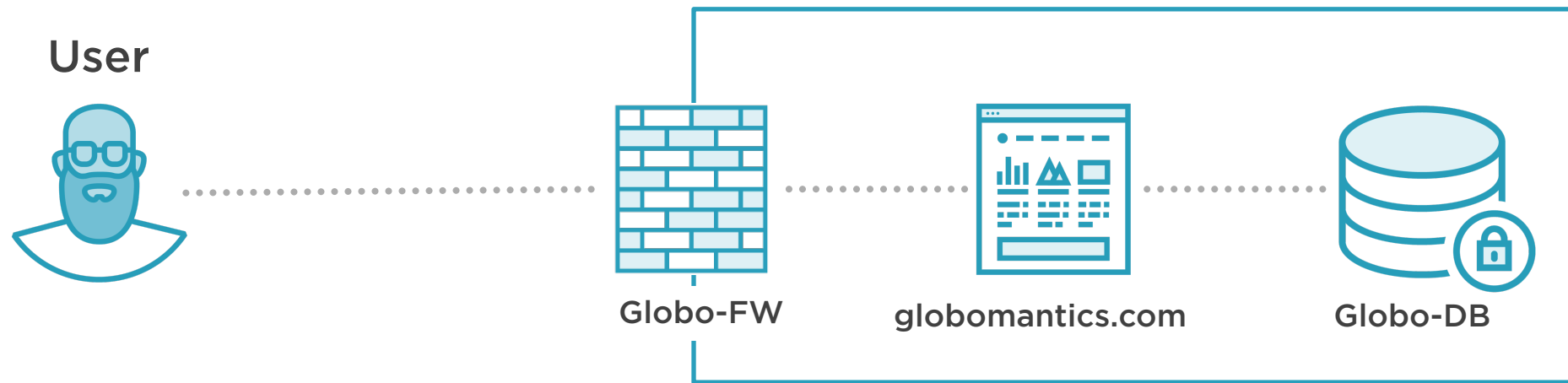
Anatomy of a Typical SQL Injection Attack from the User Perspective



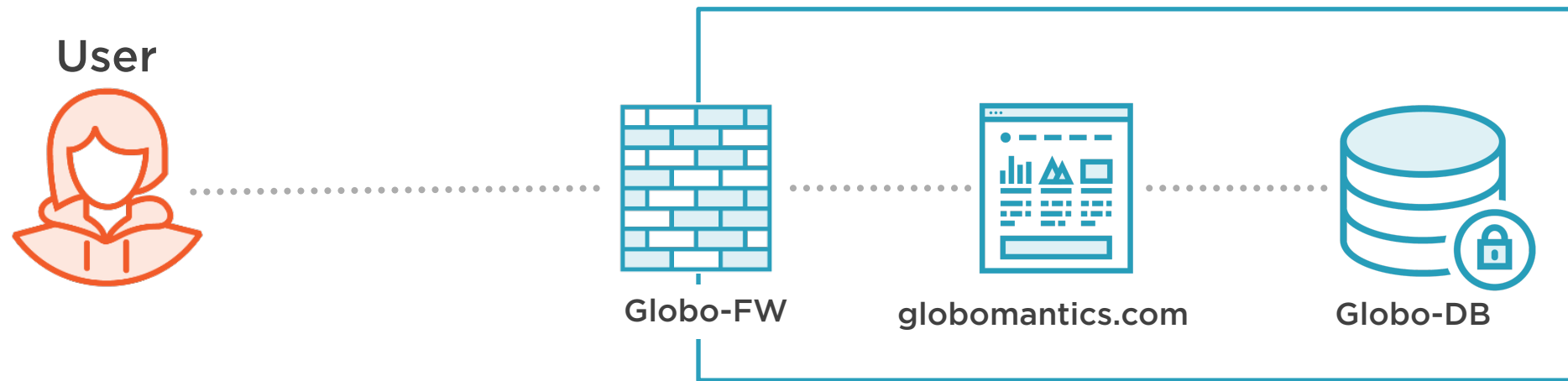
Anatomy of a Typical SQL Injection Attack from the User Perspective



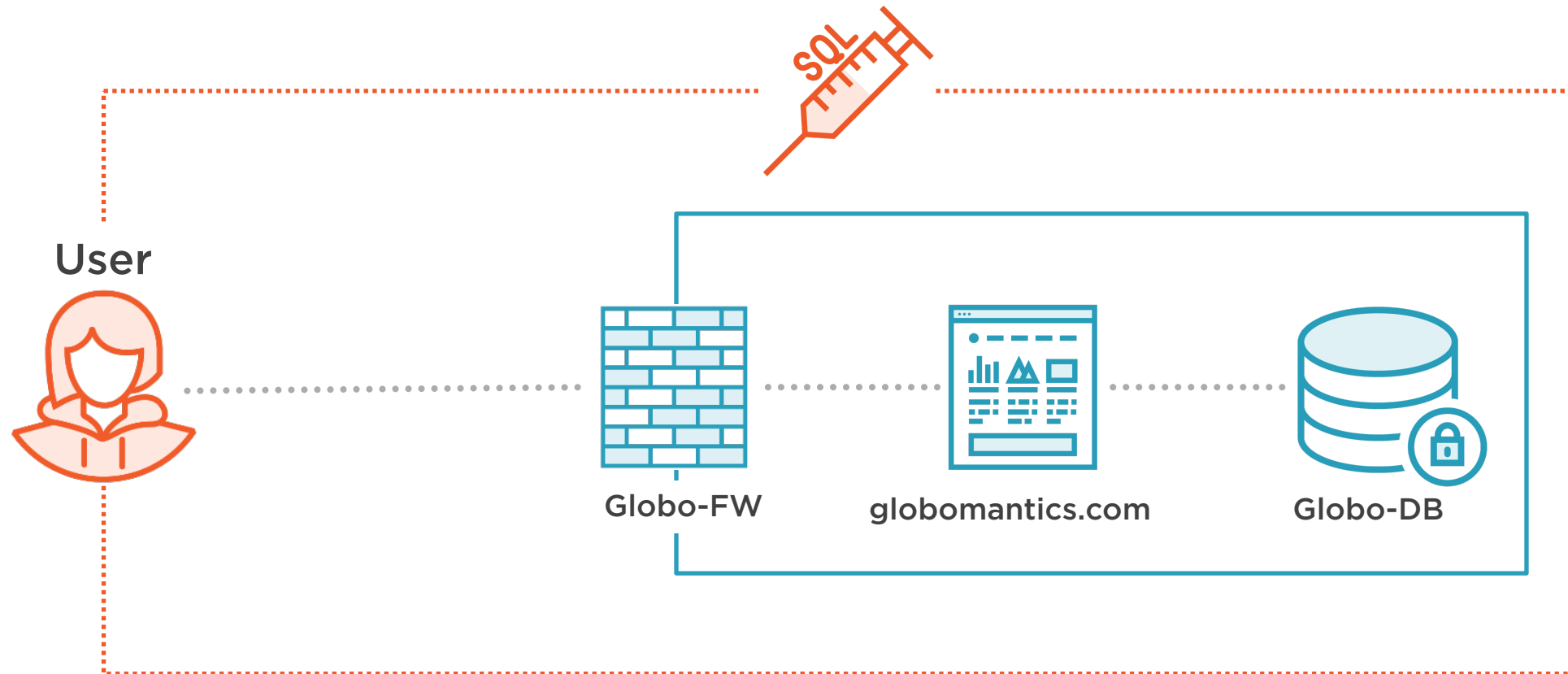
Anatomy of a Typical SQL Injection Attack from the User Perspective



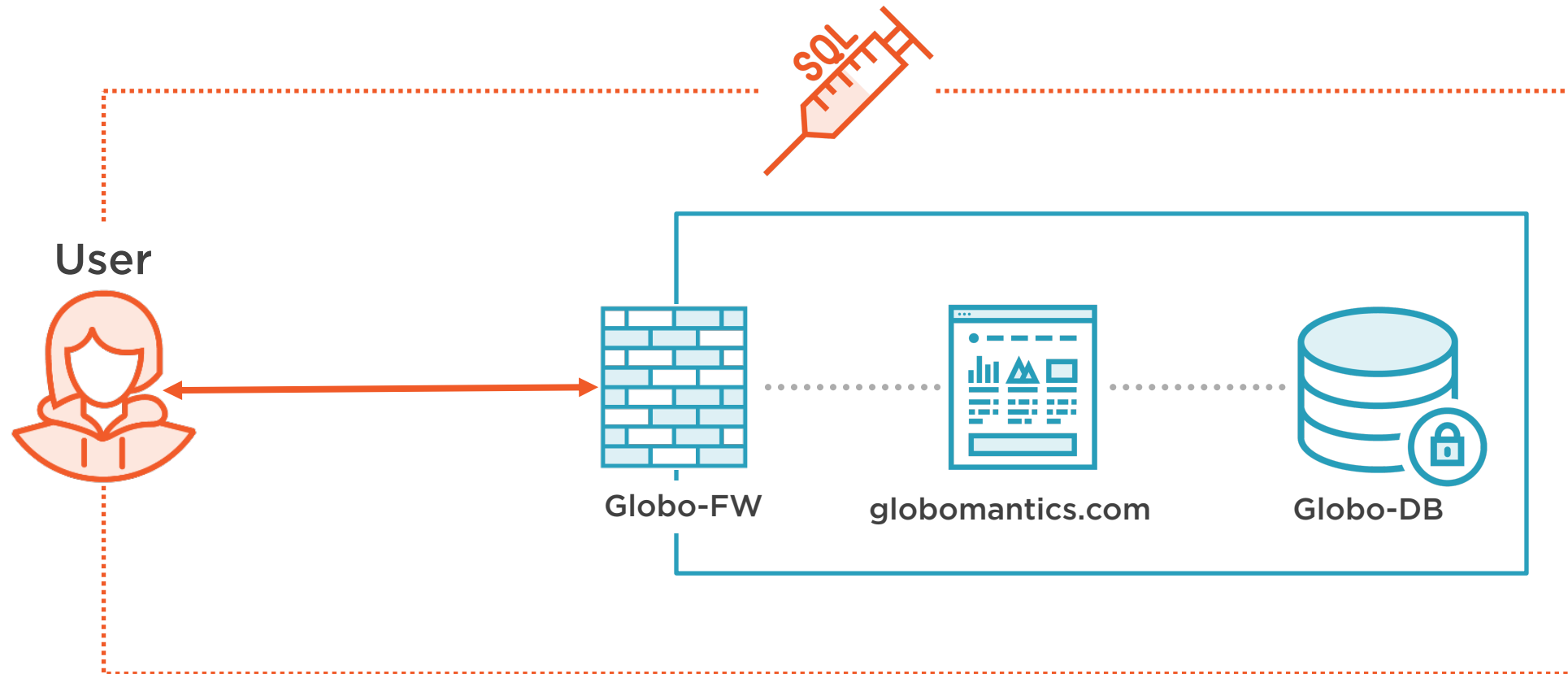
Anatomy of a Typical SQL Injection Attack from the User Perspective



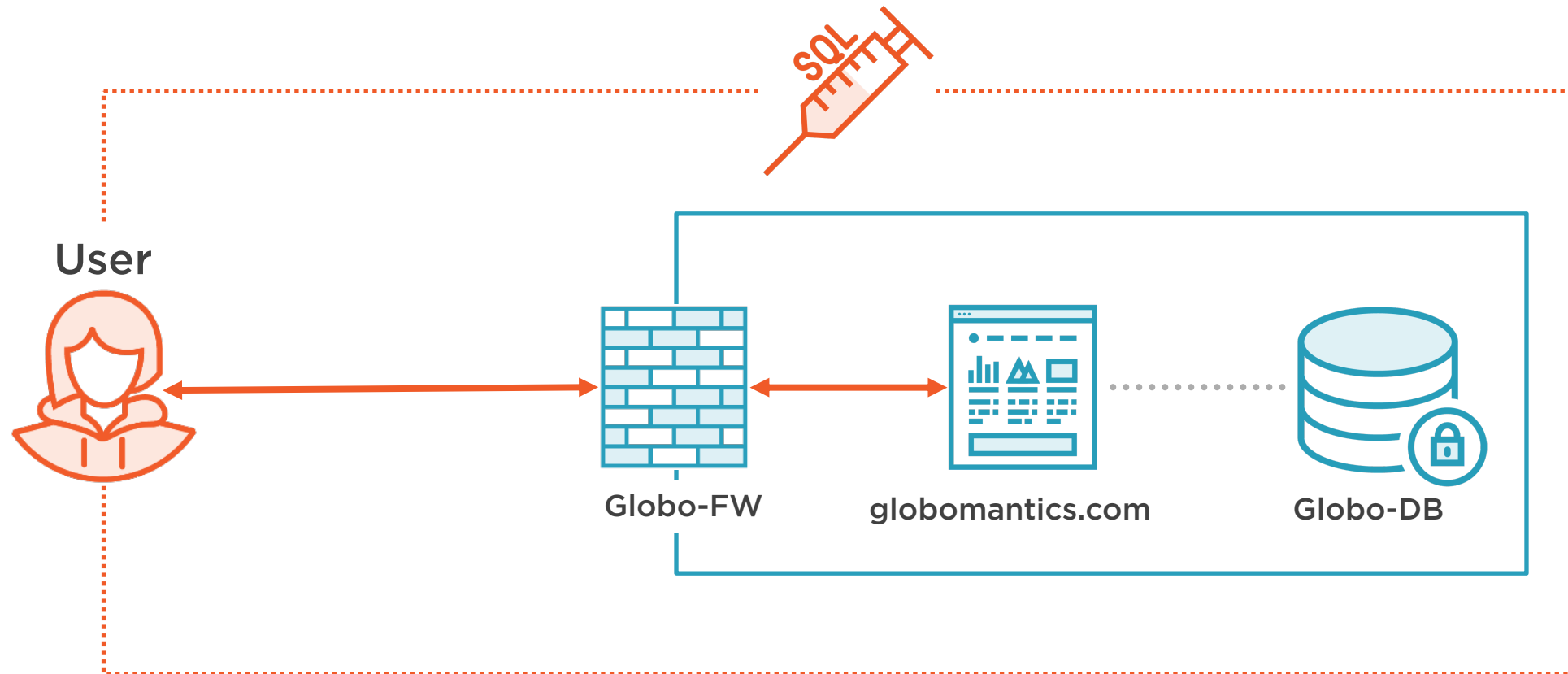
Anatomy of a Typical SQL Injection Attack from the User Perspective



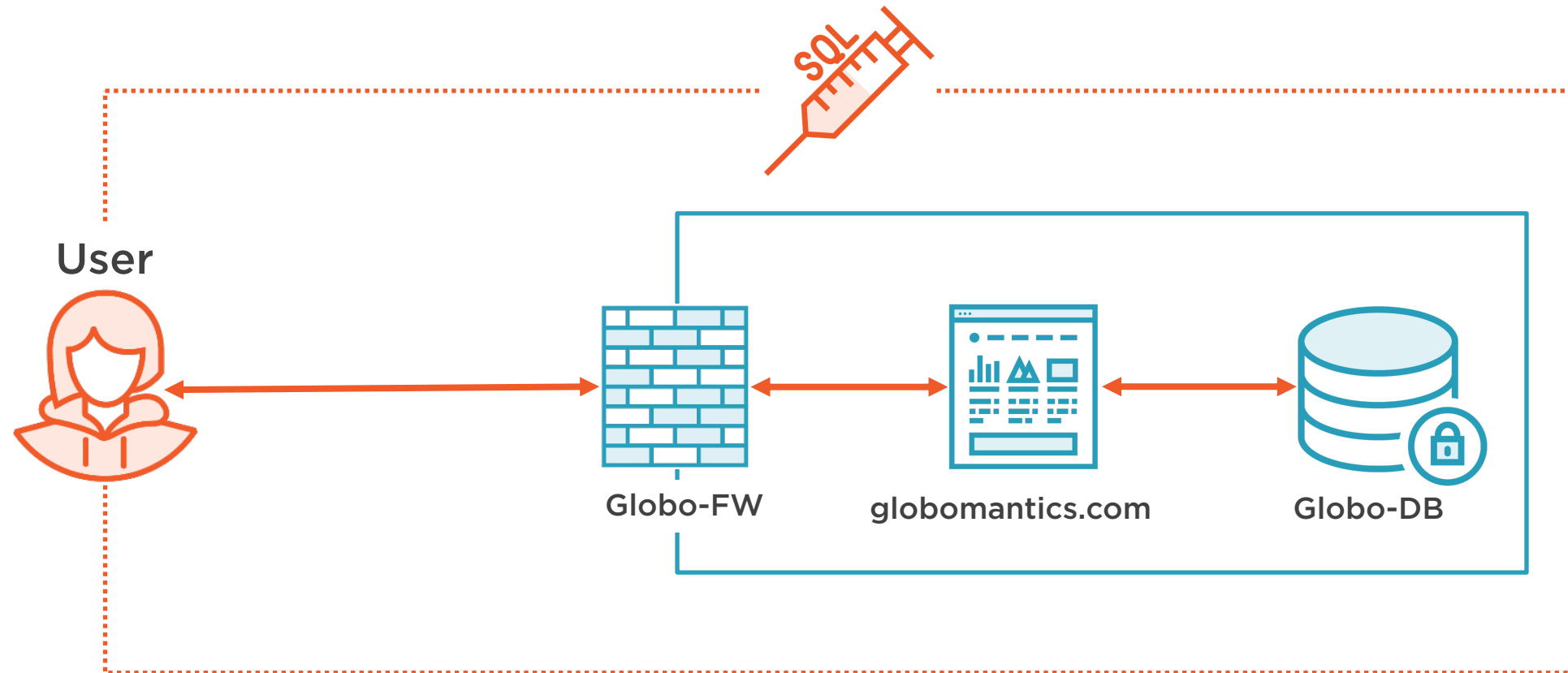
Anatomy of a Typical SQL Injection Attack from the User Perspective



Anatomy of a Typical SQL Injection Attack from the User Perspective



Anatomy of a Typical SQL Injection Attack from the User Perspective



Demo



Scan a website to identify SQL Injection vulnerabilities

Exploit an identified vulnerability to enumerate data

Use the level and risk parameters for tuning scans

Gain remote server access using sqlmap

