UNIVERSITA‘ DEGLI STUDI DI BARI —ALDO MORO

DIPARTIMENTO DI INFORMATICA

CORSO DI LAUREA IN

Informatica e Tecnologie per la Produzione del Software

TESI DI LAUREA IN PROGRAMMAZIONE WEB

METODOLOGIE E TECNICHE DI TEST PER LA SICUREZZA NELLA PROGRAMMAZIONE

RELATORE:
Ch.mo Prof. Michele Scalera

LAUREANDO:
Marco Carani

ANNO ACCADEMICO 2015/2016

Di cosa parleremo

- La sicurezza
- Cyber security
- Sicurezza lato software: il caso di studio
  - Tool utilizzati
  - SQL Injection
  - XSS Injection
  - Password cracking e algoritmo del sale
  - Clickjacking (X-Frame-Options)
  - Sicurezza dei cookie (HTTP Only e Secure flag)
  - MIME sniffing (X-Content-Type)
- Sviluppi futuri

La sicurezza

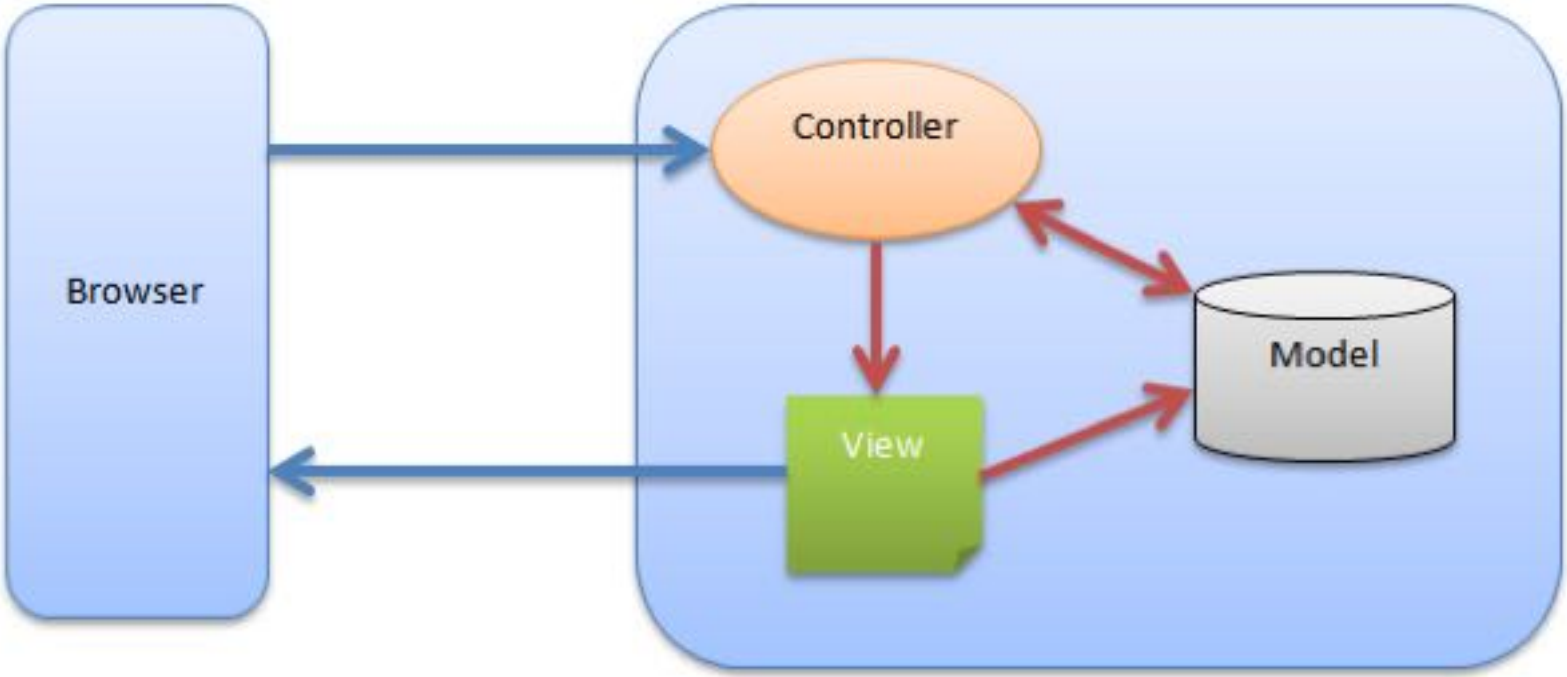
- Definizione
- Tipi di sicurezza (fisica, personale, delle informazioni, nazionale, operativa, ecc…)
- Cyber security ←→ sicurezza in ambito dipendente da tecnologia informatica

Cyber security

- Sicurezza lato hardware
  - Denial of Service (DoS o Distributed DoS)
  - Sniffing
  - Man In The Middle (MITM)
  - …
- Sicurezza lato software
  - SQL Injection
  - XSS Injection
  - Crittografia delle password
  - …

Sicurezza lato software – Caso di studio

- Architettura web application: MVC



- Test eseguiti → metodo blackbox
- Relazioni per ogni problema individuato

Tool utilizzati

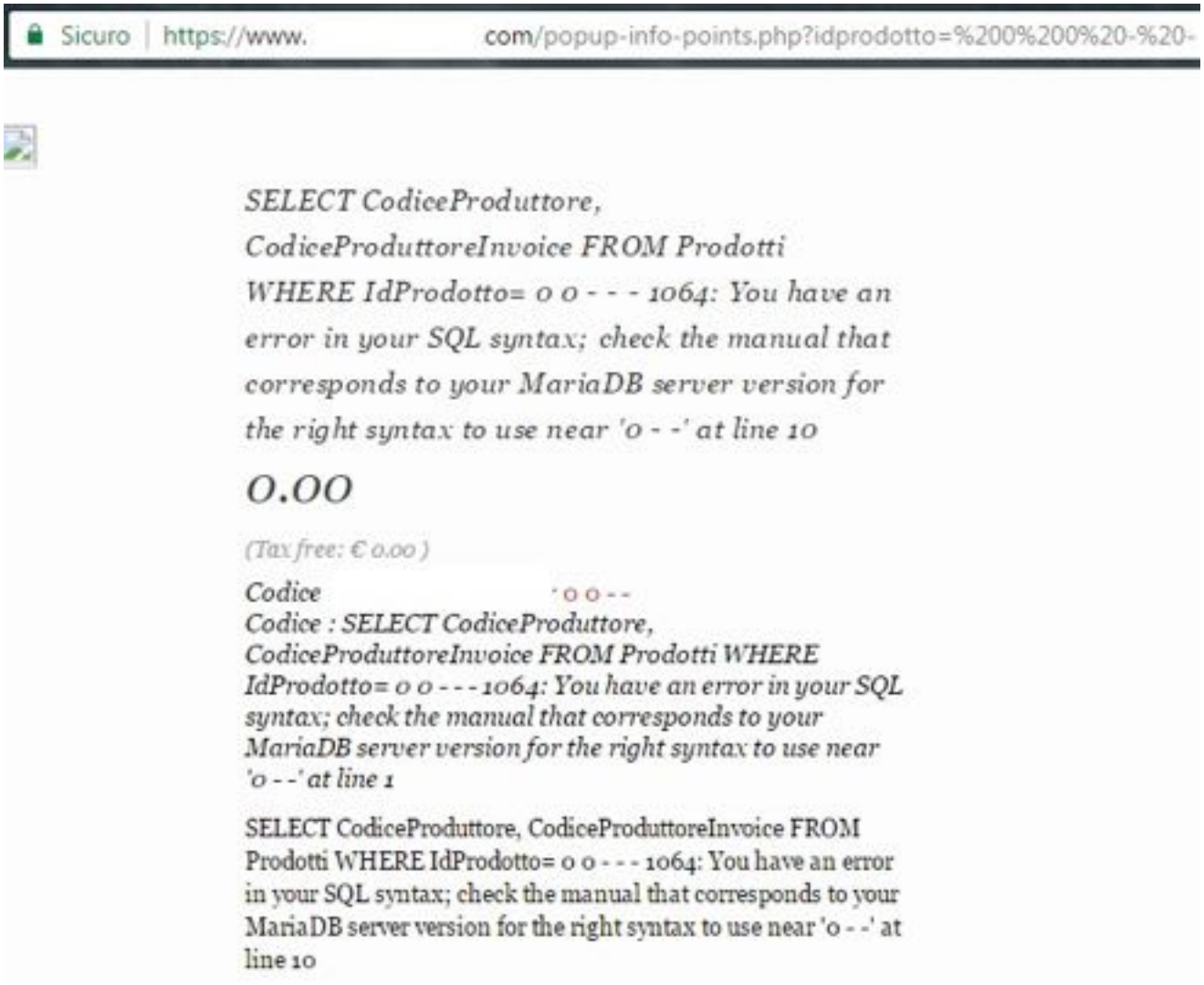
- **Vega**: è una piattaforma sviluppata dalla Subgraph dotata di una GUI scritta in JAVA per testare la sicurezza di una web application. È disponibile sia per Linux, OS X e Windows;
- **OWASP ZAP** (Zed Attack Proxy Project): altro tool freeware utile per la scansione di una web application con relativo report sulle vulnerabilità;
- **Console Network di Google Chrome** utile per controllare i cookie e gli header di risposta;
- **SQLMap** software contenuto in **Kali Linux** una distribuzione basata su Debian GNU/Linux utilizzato per il testing di SQL injection;
- **OWASP Xenotix Xss Exploit Framework 6.2**, un framework utilizzato per testare vulnerabilità di script injection.

SQL Injection

- Definizione
- Diverse tipologie di SQL injection
  - Illegal/Logically Incorrect queries;
  - Union query.
- Soluzioni proposte:
  - Display_errors=off in php.ini

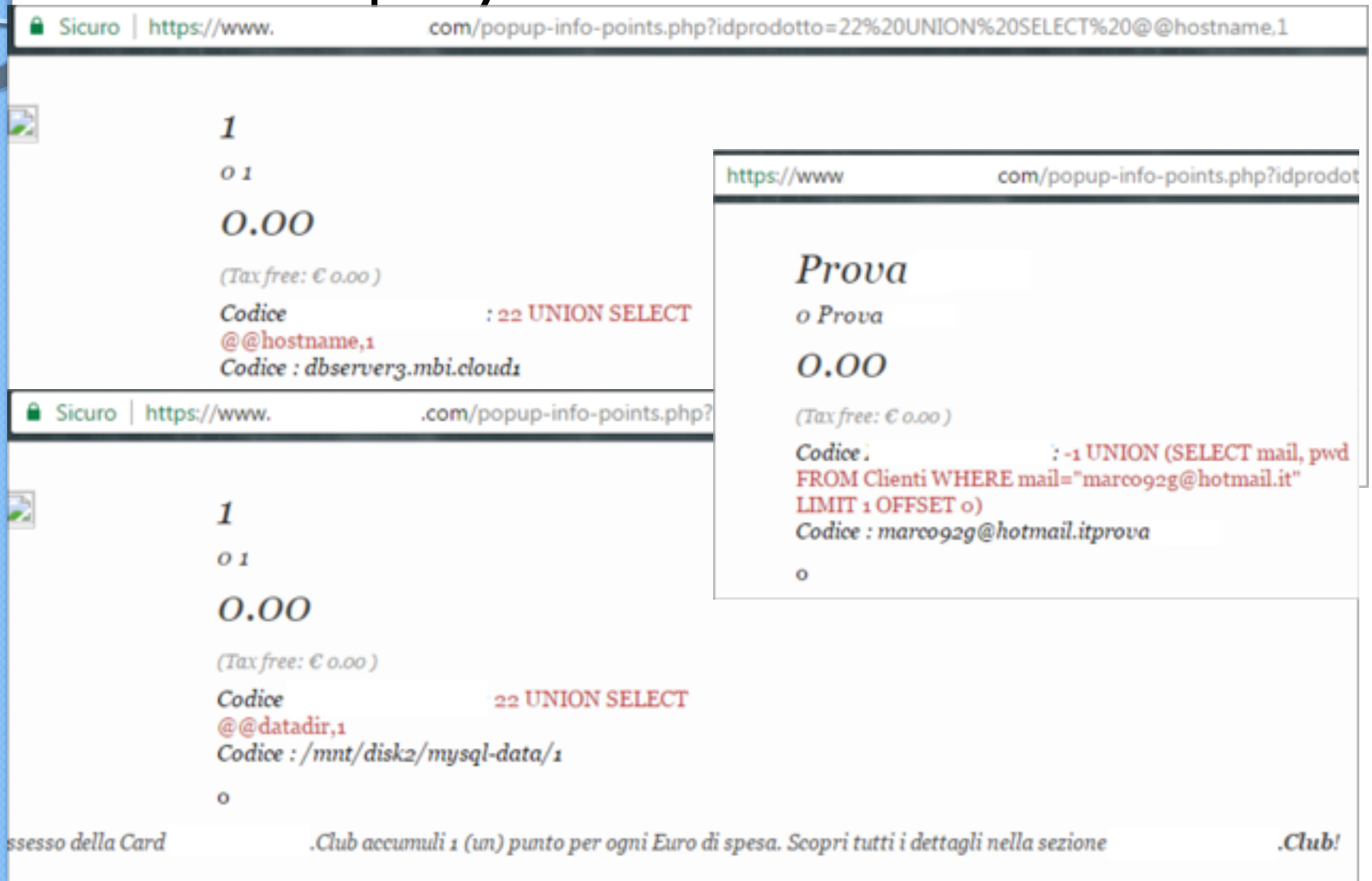
SQL Injection

- Illegal/Logically Incorrect queries

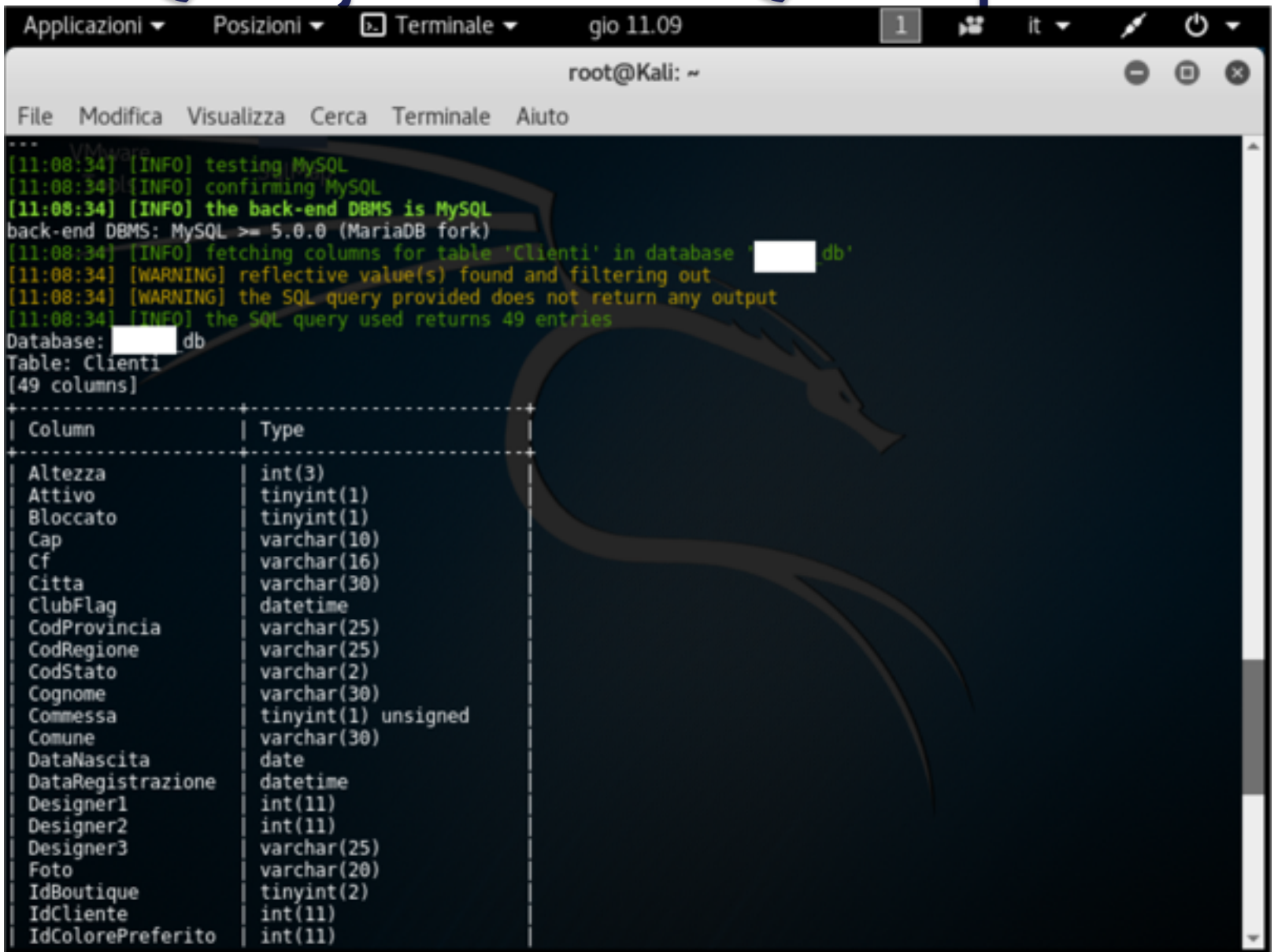


SQL Injection

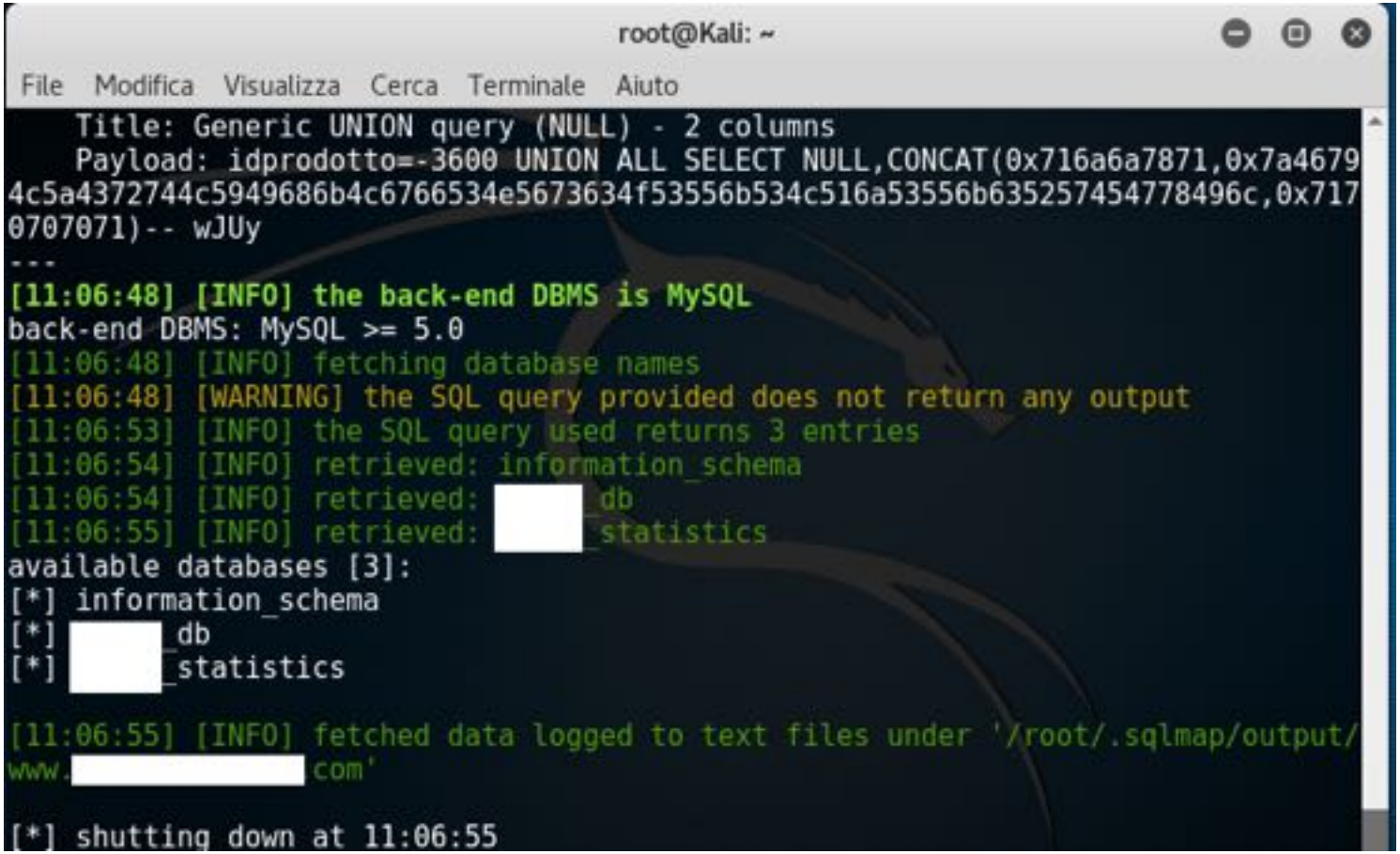
- Union query



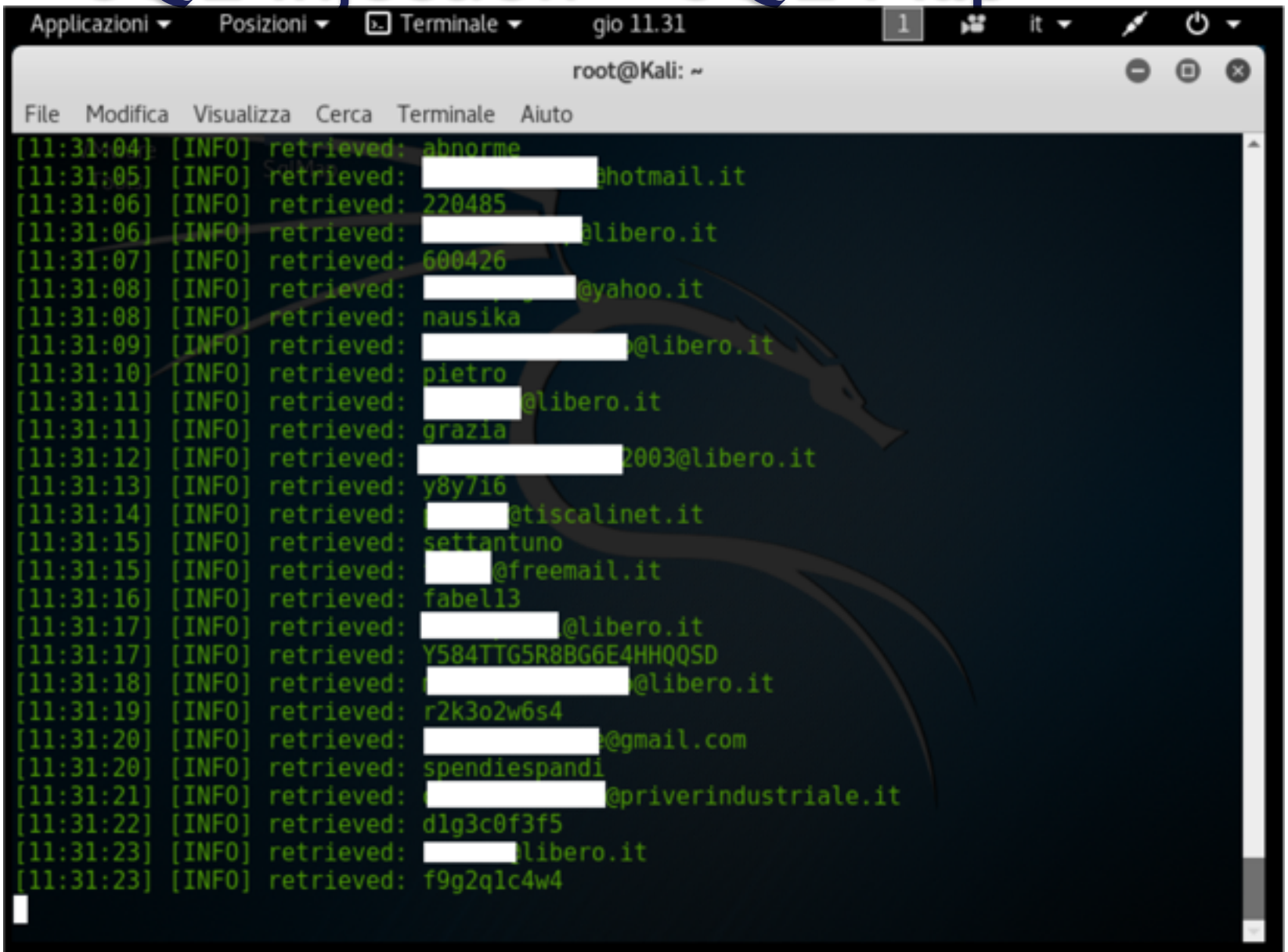
SQL Injection – SQL Map



SQL Injection – SQL Map



SQL Injection – SQL Map



XSS Injection

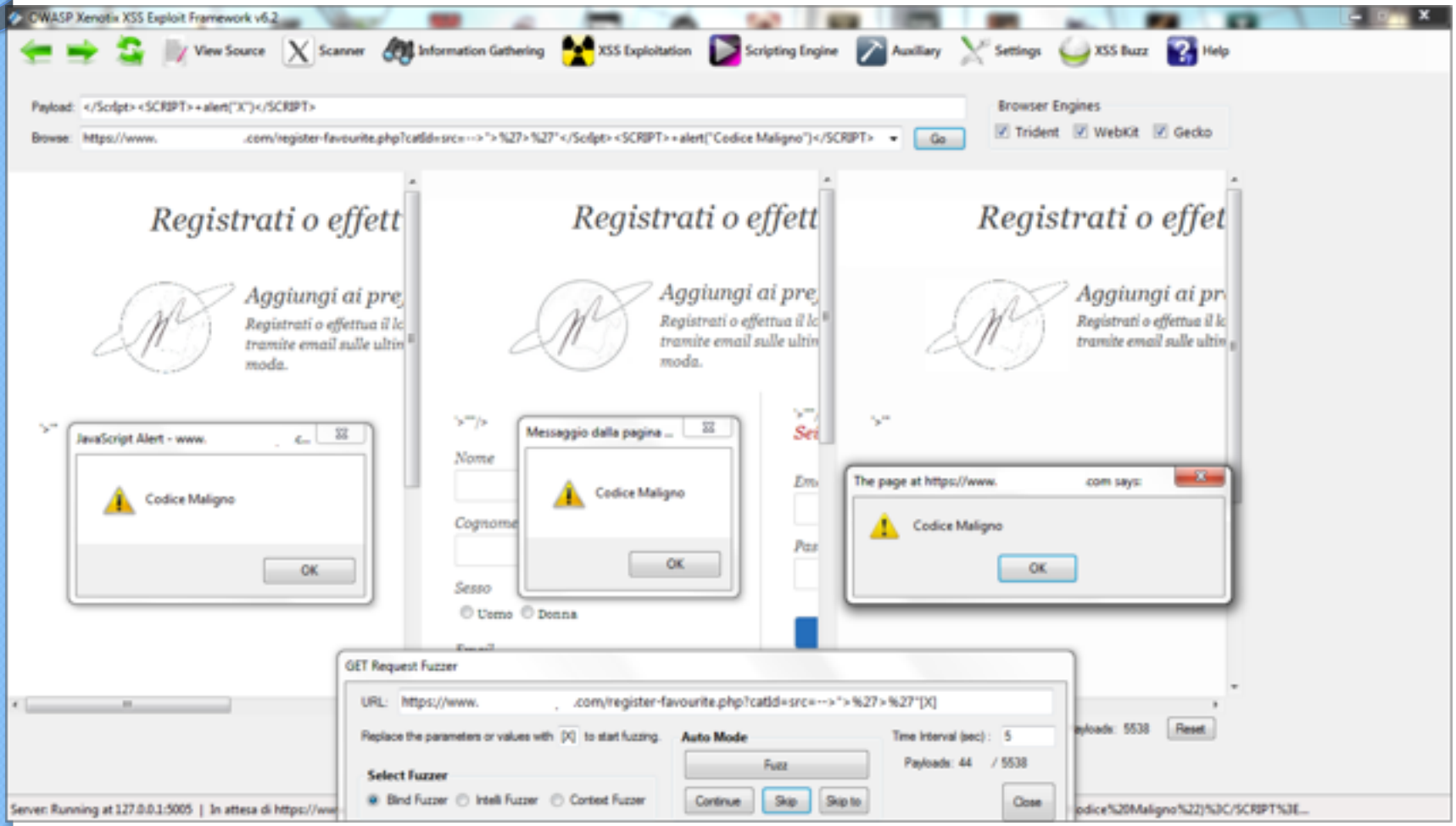
- Definizione

- Diverse tipologie:
  - Persistenti (Stored);
  - Non persistenti (Reflected).

- Soluzioni proposte:
  - Validazione input;
  - X-XSS-Protection:1 ; mode=block

XSS Injection

- Non persistente



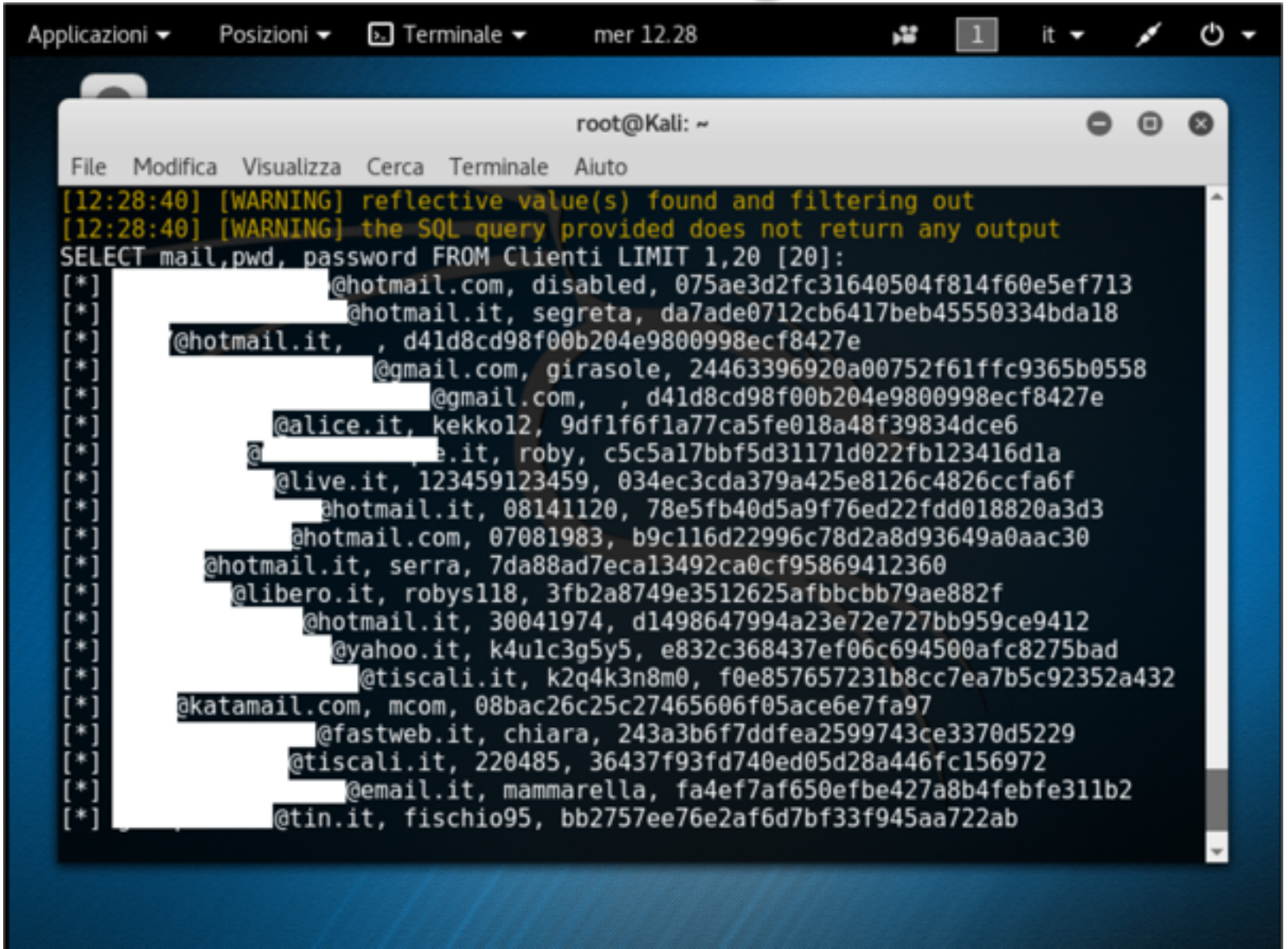
Crittografia delle password (Password Cracking)

- Definizione

- Due diversi approcci:
  - Attacchi a forza bruta;
  - Attacchi a dizionario.

- Soluzione proposta:
  - Algoritmo del sale

Password Cracking

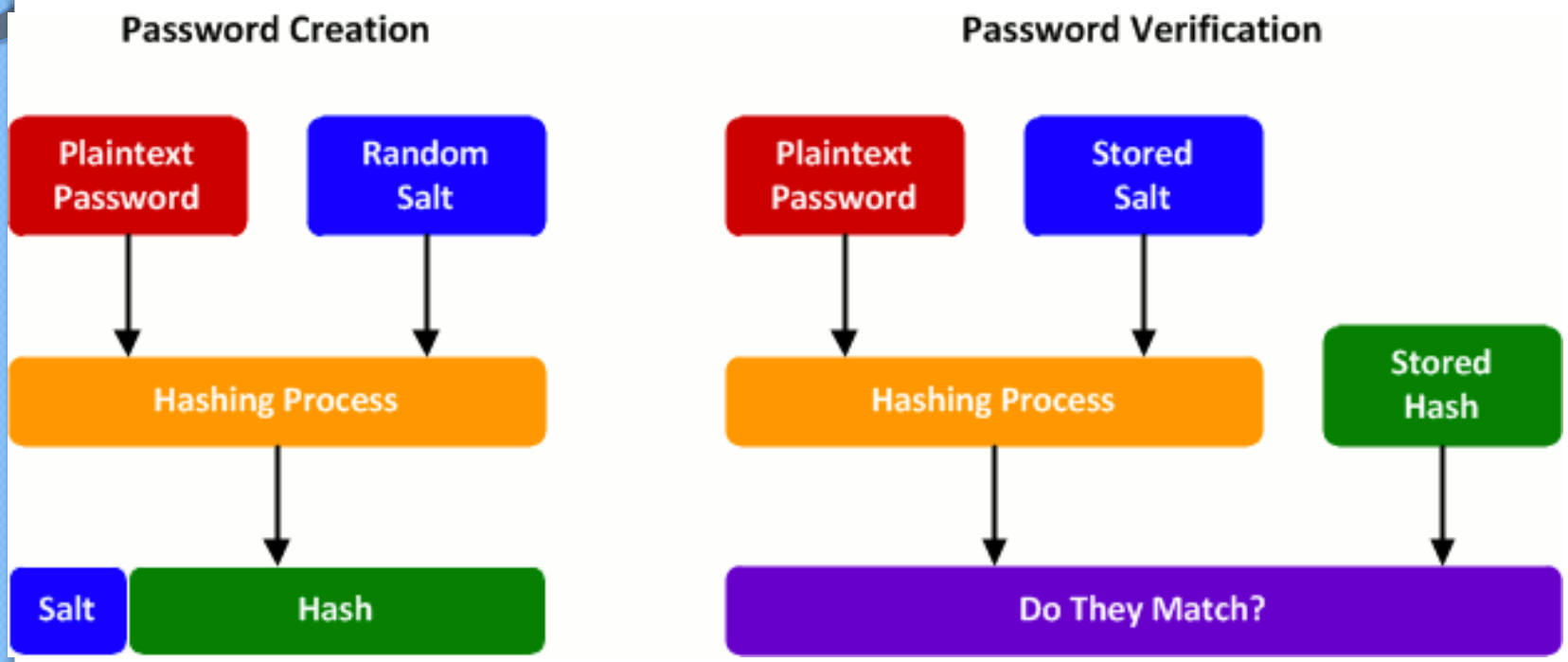


Salt algorithm

- In fase di creazione della password:
  - 1. Generare un sale di una lunghezza arbitraria;
  - 2. Aggiungere il sale alla password fornita dall'utente
  - 3. Applicare un algoritmo di hash (sha256, sha512, bcrypt, scrypt, PBKDF2);
  - 4. Salvare la stringa criptata ottenuta come password dell'utente e il sale in due database diversi.

- Al momento del login:
  - 1. Viene recuperata la stringa oscurata e il sale;
  - 2. Viene aggiunto il sale alla password fornita in input e viene applicato l'algoritmo di hash;
  - 3. Viene confrontata la stringa ottenuta con la stringa presente nel database. Se esse combaciano allora viene consentito l'accesso, se ciò non accade viene fornito un messaggio di errore.

Salt algorithm



Sviluppi futuri

- Risoluzione dei problemi ancora presenti;
- Analisi della sicurezza sull'infrastruttura di rete;
- Implementazione dell'estensione PDO (PHP Data Object) per SQL injection

Grazie per l'attenzione.