Web安全

《网络安全工程与实践》课程

eki@NISL 2024.12.12

About Me

Eki

- **ID**：Eki（汪琦）
  - NISL 23级博士研究生在读， Redbud 成员
- **研究方向**：协议安全、Web 安全
- **博客**：https://blog.eki.im
- **主页**：http://eki.im

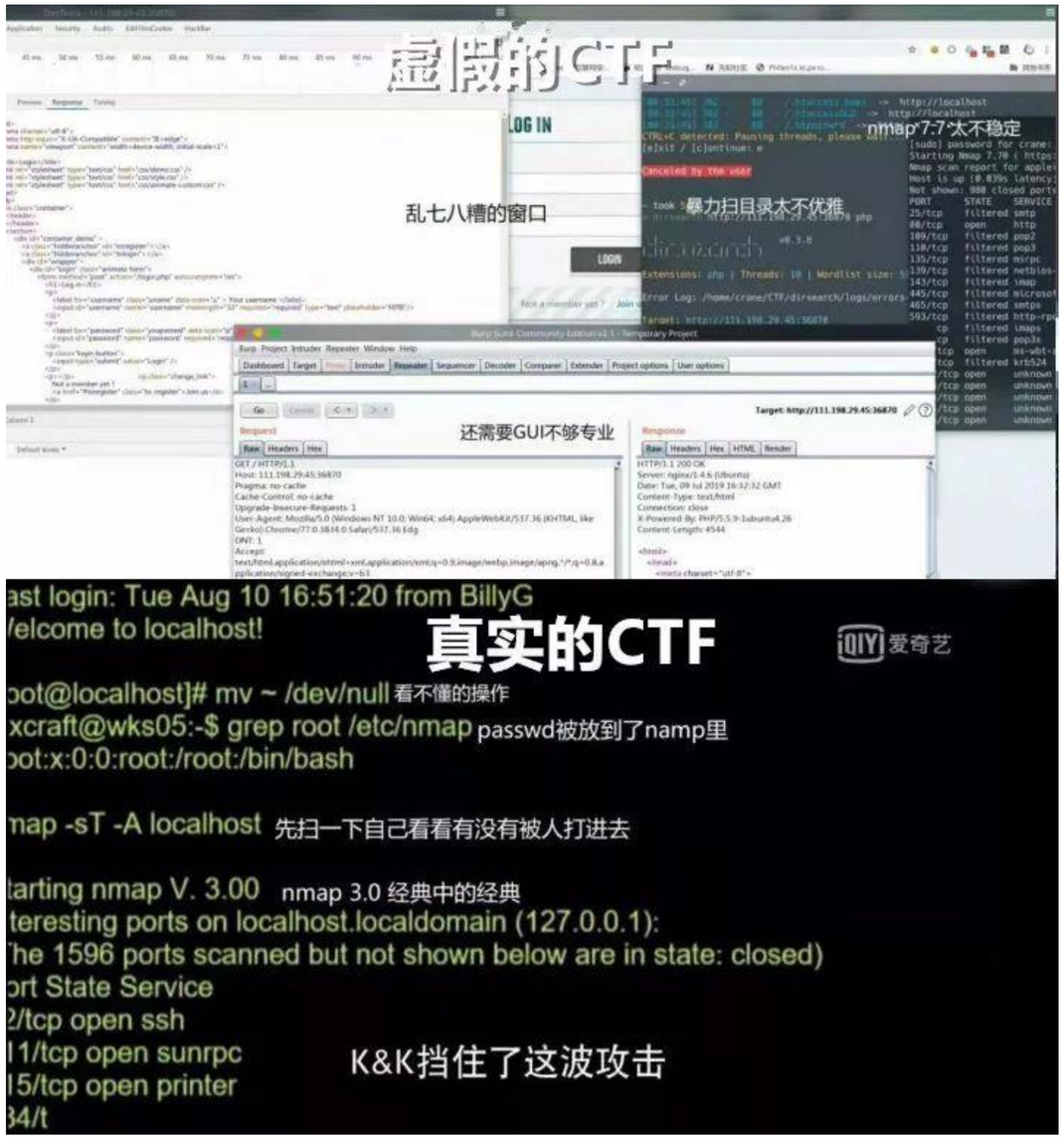
目录

- Web 安全概述
- 常用工具介绍
- OWASP Top 10 漏洞讲解及练习

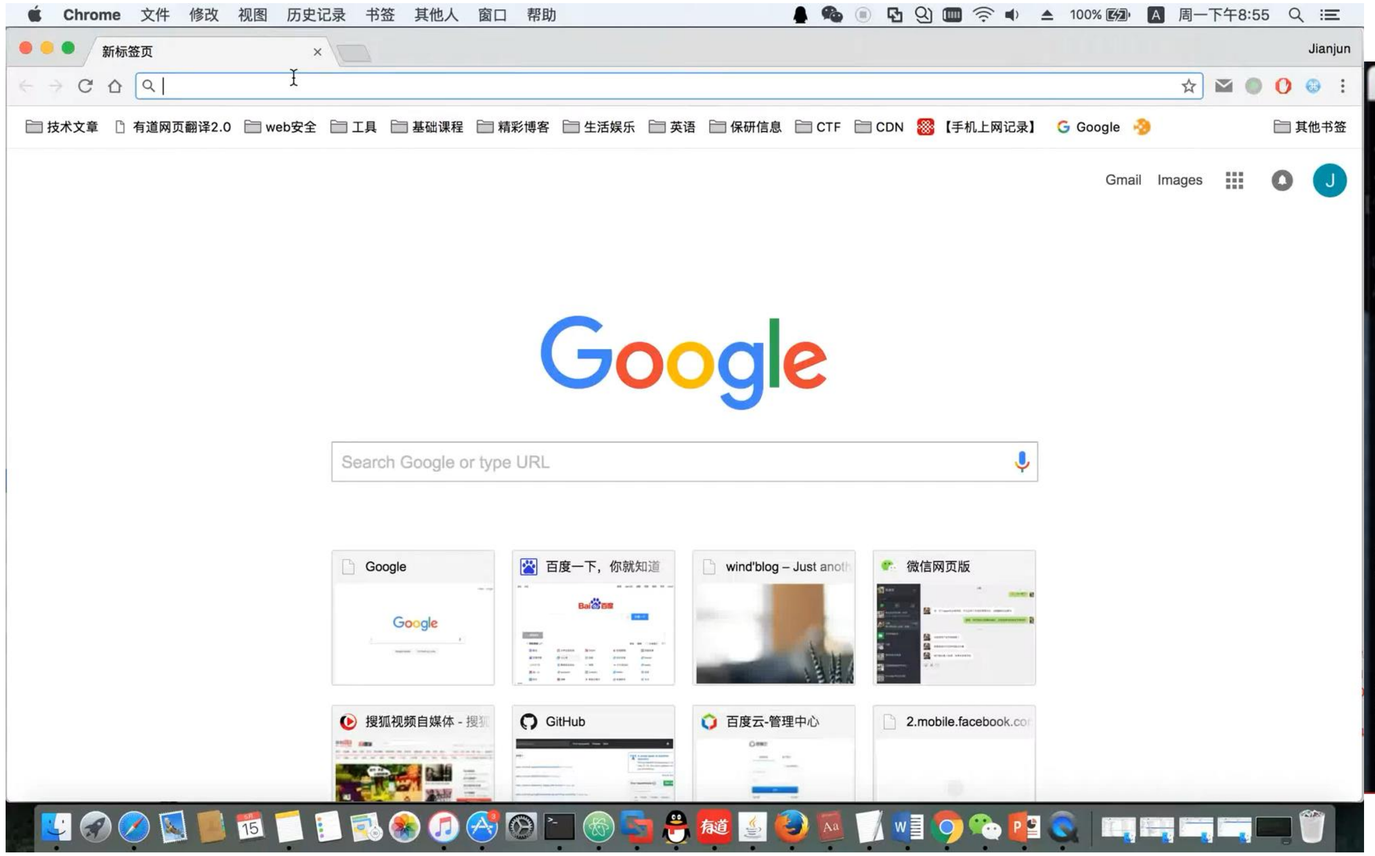
Web 安全概述

Web 安全是什么？

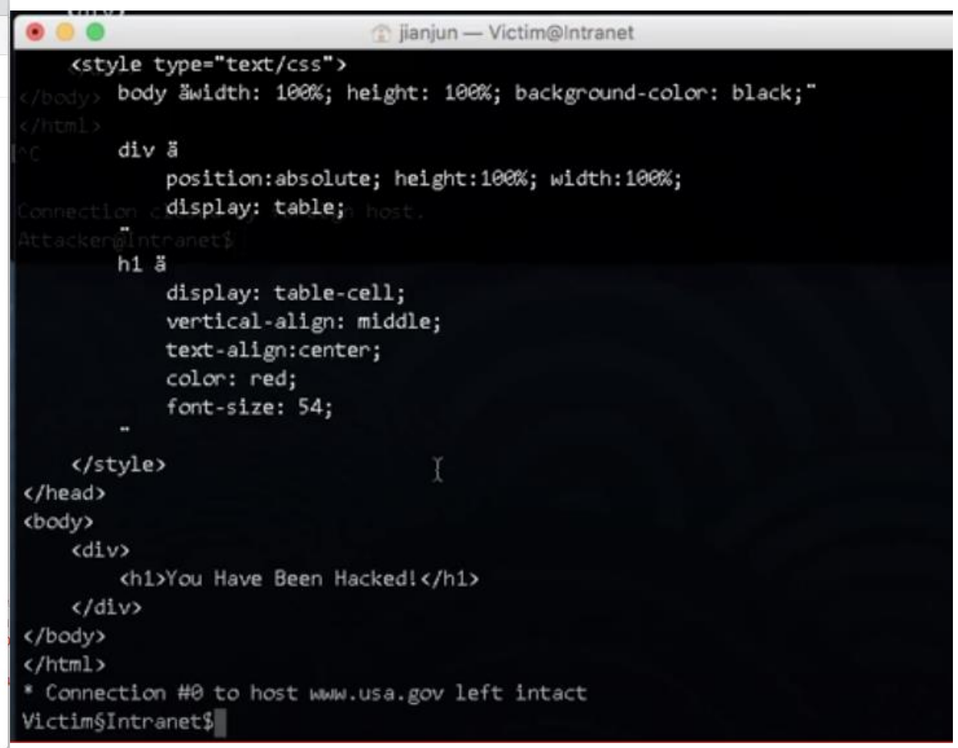
“真实”的WEB安全&“虚假”的WEB安全



真实的WEB安全也可以很“酷”



窃取沃尔玛用户信用卡账户信息



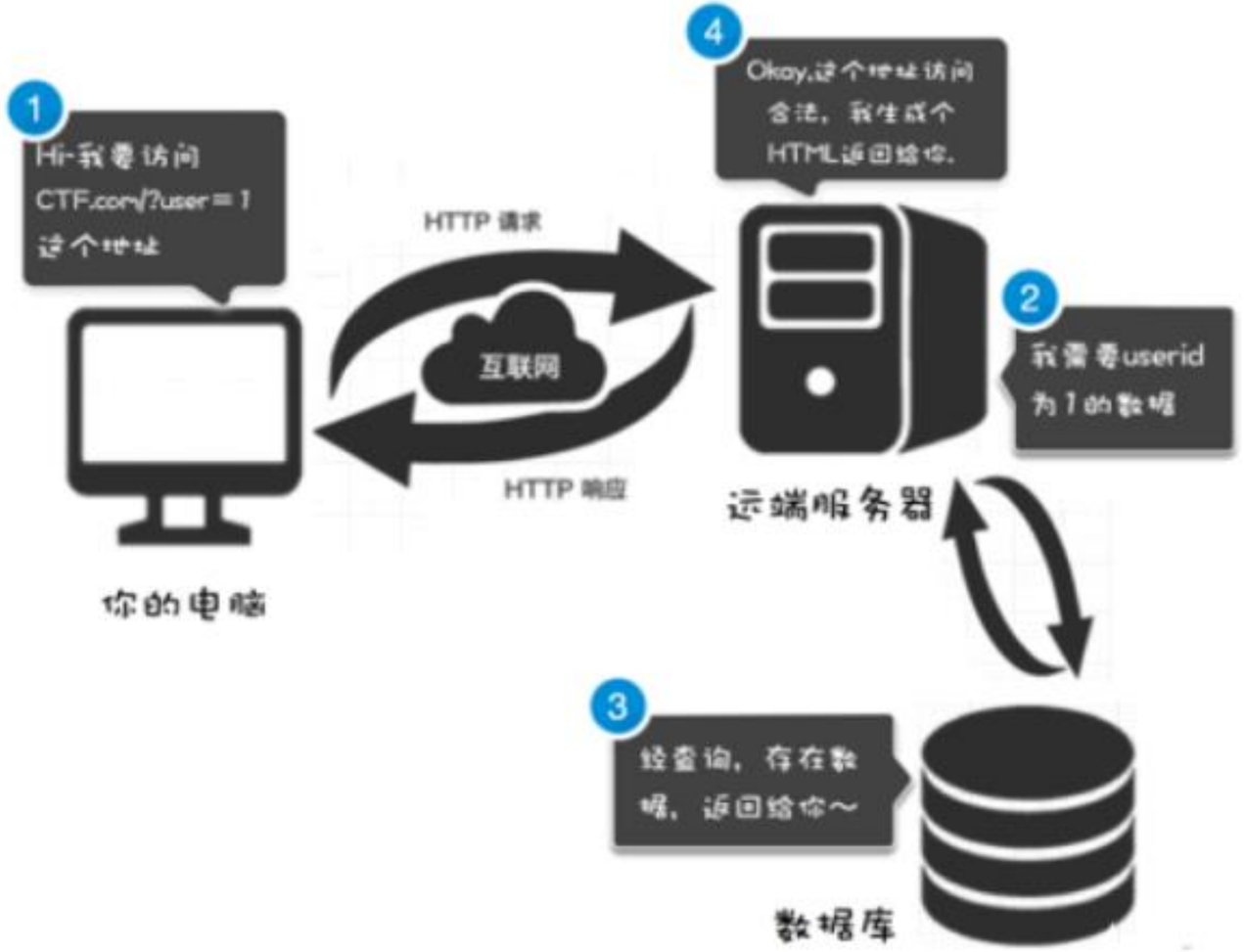
“黑”掉nsa.gov

Web 是什么？

Web 安全概述

Web 基本架构与协议

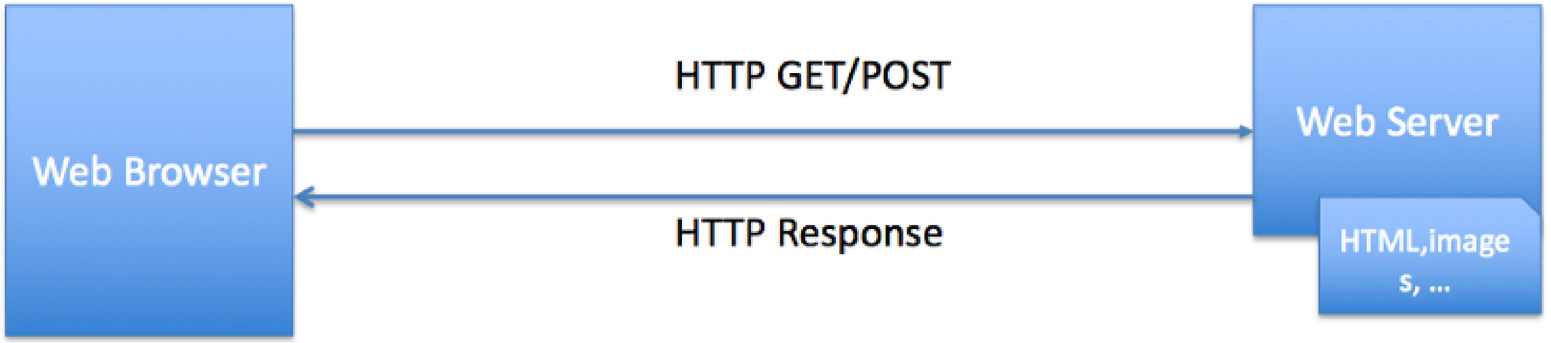
- C/S 架构



Web 安全概述

Web 基本架构与协议

- C/S 架构
- HTTP(S) 协议




```
GET /chs/ HTTP/1.1
Host: netsec.ccert.edu.cn
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; ...
Accept: text/html,a...
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: _ga=xxx; _gid=xxx
Connection: close
```

```
HTTP/1.1 200 OK
Date: xxx
Content-Type: text/html; charset=utf-8
Connection: close
Server: xxx
Content-Length: 20319

<!doctype html><html lang="en" class="no-js"><head>
<meta charset="utf-8"> <!-- begin SEO --><title>
清华大学网络与信息安全实验室 - NISL@THU</title>
...
```

Web 安全概述

Web 基本架构与协议

- C/S 架构
- HTTP(S) 协议
- Web 安全的各个子部分
  - 前端
    - 浏览器 / DOM
    - Electron / WebView
  - 后端
    - Web 应用
    - 数据库
    - 服务器 / 中间件
    - 内网渗透 / 后渗透技术

Web 安全概述

Web 安全的各个子部分

- **Web 前端**（浏览器）
  - 基本语言：Html、CSS、JS 等
  - 前端框架：Vue、React 等
  - Cookie使用、缓存方案
  - 同源策略、跨域问题
- **Web 后端**（应用）
  - 基本语言：PHP、Python、Java、Go、NodeJS 等
  - PHP 框架：Thinkphp、laravel 等
  - Python Web 框架：Flask、Django、Tornado 等
  - Java Web 框架：Spring、Struts 2
  - Session 使用

Web 安全概述

Web 安全的各个子部分

- **数据库**
  - **关系型**：MySQL、MariaDB、SQLite
  - **非关系型**：MongoDB、Redis
  - 不同后端语言连接方式，使用
  - 基本操作：增删改查、权限控制等
- **服务器 / 中间件**
  - NGINX、Apache HTTPd、IIS
  - Tomcat、JBoss
  - 掌握部署、配置等操作
  - 系统特性、重要文件
  - 相关漏洞（绕过、提权、RCE等）

Web 安全概述

Web 安全的各个子部分

- **内网渗透**
  - 操作系统部分
    - Linux & Windows
    - 基本命令使用
    - 系统特性、重要文件
    - 相关漏洞（提权、RCE等）
    - 权限维持 / 权限提升
- 网络部分
  - 环境侦查
  - 网络拓扑识别
  - 端口转发 / 代理 / 内网穿透
  - 横向移动

常用工具介绍

常用工具介绍

Web 安全的攻击阶段

- 四个攻击阶段
  - 信息搜集
  - 漏洞探测和利用
  - 权限维持
  - 内网渗透

常用工具介绍

信息搜集工具

- 在攻击之前，需要了解目标主机的具体情况，才能针对性地发起攻击
- 信息搜集工具
  - dirsearch：目录扫描
  - Nmap、fscan：端口、主机扫描
  - AWVS：综合扫描（目录、漏洞等）

```
~/Security/tools/dirsearch (master*) » ./dirsearch.py -u http://127.0.0.1:8080

  _|. _ _  _  _  _ _|_    v0.4.1
 (_|| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30
Wordlist size: 10877

Error Log: /Users/mukeran/Security/tools/dirsearch/logs/errors-23-04-17_15-13-52
.log

Target: http://127.0.0.1:8080/

Output File: /Users/mukeran/Security/tools/dirsearch/reports/127.0.0.1/_23-04-17
_15-13-52.txt
```

```
~/Security/tools/dirsearch (master*) » nmap 127.0.0.1
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-17 15:14 CST
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000039s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT     STATE SERVICE
53/tcp   open  domain
443/tcp  open  https
3306/tcp open  mysql
5000/tcp open  upnp
7000/tcp open  afs3-fileserver
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

常用工具介绍

漏洞探测和利用工具

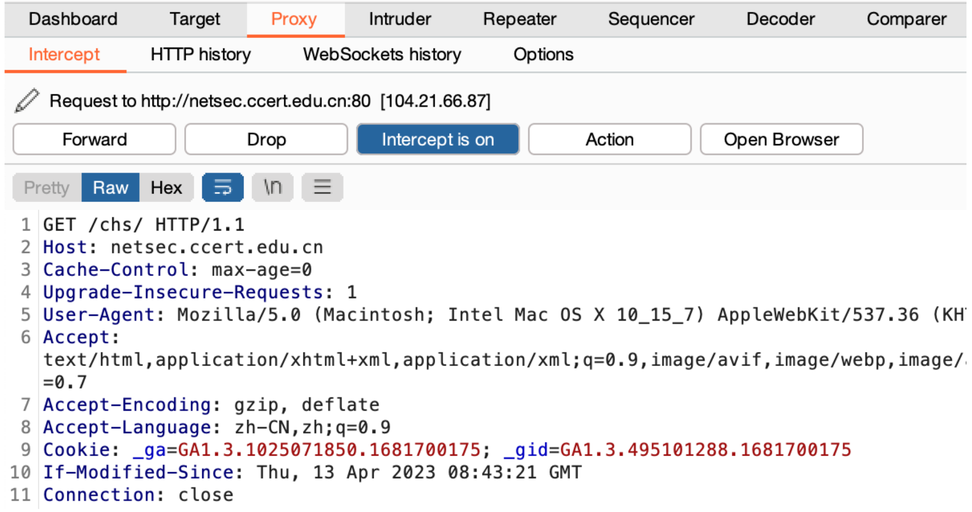
- 获取目标主机信息后，需要探测存在哪些漏洞并加以利用
- 漏洞探测和利用工具
  - **BurpSuite***：抓包、改包、爆破、重放工具（针对新漏洞）
  - **SQLMap**：针对 SQL 注入的漏洞检测、利用工具
  - Metasploit Framework：强大的现有漏洞检测和利用框架

*: Burp Suite Community Edition 2023.3.4 下载镜像：https://cloud.tsinghua.edu.cn/d/3aebbcfc10aa4b4984d7/

常用工具介绍

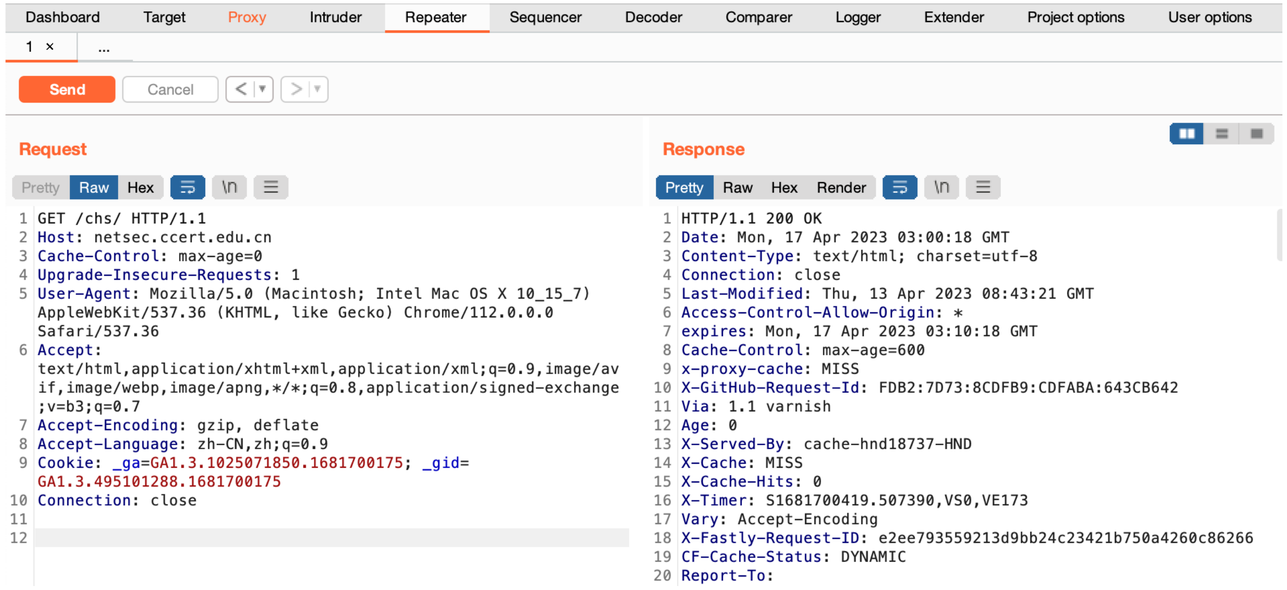
漏洞探测和利用工具

- **BurpSuite**

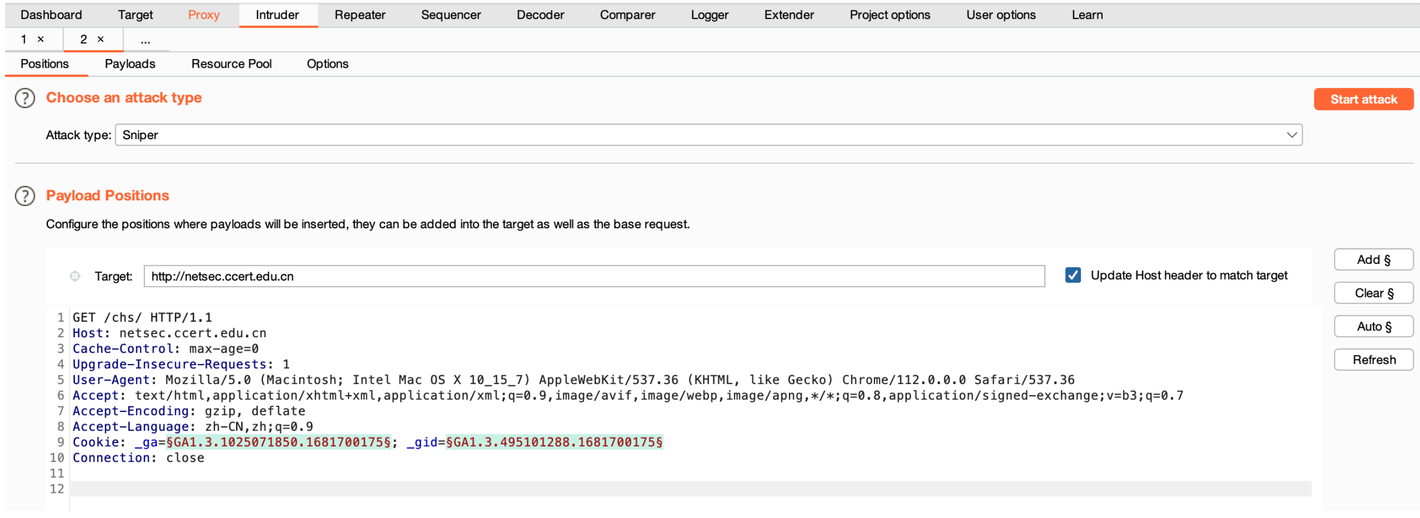


↑ 代理模块（抓包）

↓ 重放模块（改包）



↓ 爆破模块



常用工具介绍

漏洞探测和利用工具

- **SQLMap**

```
~/Security/tools/sqlmap (master*) » ./sqlmap.py -u http://127.0.0.1:8080
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.7.2.22#dev}
|_ -| . ["]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting @ 15:32:59 /2023-04-17/

[15:32:59] [INFO] testing connection to the target URL
[15:33:00] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:33:00] [WARNING] reflective value(s) found and filtering out
[15:33:00] [INFO] testing if the target URL content is stable
```

常用工具介绍

权限维持工具

- 为了漏洞利用后便捷的访问，需要使用权限维持工具，这里以 Webshell 为例
- 信息搜集工具
  - **AntSword**：蚁剑，管理 PHP、ASP 的 Webshell
  - **Behinder**：冰蝎，管理 PHP、ASP、JSP 的 Webshell

常用工具介绍

其他常用工具

- 其他常用工具
  - **curl**：命令行工具，用来发起 HTTP 请求
  - **Proxy SwitchyOmega**：浏览器代理切换工具，便于进行内网渗透

OWASP Top 10 漏洞讲解及练习

OWASP Top 10 漏洞讲解及练习

OWASP

- OWASP（**开放式** Web 应用程序安全项目）关注 Web 应用程序的安全
- OWASP 这个项目最有名的，就是它的“**十大安全**隐患列表”（OWASP Top 10）
  - 这个列表总结了 Web 应用程序最可能、最常见、最危险的十大安全隐患
  - **列表差不多每隔三年更新一次**

OWASP Top 10 漏洞讲解及练习

OWASP Top 10 2021

- A01：权限控制失效
- A02：加密机制失效（导致的信息泄漏或系统被攻破）
- **A03：注入式攻击（包含 XSS）**
- A04：不安全设计
- **A05：安全设定缺陷（包含 XXE）**
- A06：危险或过旧的组件
- A07：认证及验证机制失效
- **A08：软件及资料完整性失效**
- A09：安全记录及监控失效
- A10：服务器端请求伪造

OWASP Top 10 漏洞讲解及练习

A01：权限控制失效

- 缺陷在于未对通过身份验证的用户实施恰当的访问控制
- 例子：
  - 允许查看或编辑他人的帐户（xxx?userid=1）
  - 重放或篡改 JWT 访问控制令牌以提升权限
  - 未经身份验证的用户可以访问用户页面
  - 非管理员权限的用户可以访问管理页面
  - …

OWASP Top 10 漏洞讲解及练习

A02：加密机制失效

- 在 OWASP Top 10 2017 中被称为敏感信息泄漏，其问题根源是加密机制失效
- 包括但不限于：
  - 暴露 API 接口
  - 源码泄漏（GitHub 等）
  - 目录扫描：Git 泄漏、备份文件泄漏、.DS_Store 文件泄漏 …
  - 使用默认加密密钥（**Shiro 反序列化漏洞**）
  - 端口暴露在公网上（Redis 端口、数据库端口等）
  - 明文传输
  - …

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击

- 未经过滤，将不受信任的数据作为命令或查询的一部分发送到解析器直接执行时，会产生注入漏洞
- 注入式攻击在 OWASP Top 10 2017 中排名首位
- 包括：
  - **SQL 注入**
  - **命令注入**
  - 模板注入
  - **XSS 跨站脚本攻击**
  - ...

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— SQL 注入

- SQL 注入漏洞可能是被人知道最多的漏洞，也是目前被利用的最多的漏洞
- **原理**：开发者在编写操作数据库代码时，直接将外部可控的参数**拼接**到SQL语句中，**没有**经过任何过滤或过滤不严谨，导致攻击者可以使恶意语句在数据库引擎中执行
- SQL 注入经常出现在登陆页面、订单处理等**涉及数据库操作**的地方

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— SQL 注入

```php
$user = $_POST['username'];
$pwd = md5($_POST['password']);
$query = "SELECT * FROM admin WHERE username='".$user."'"."and password='".$pwd."'";
mysql_query($query);
```

- 如果令 $user 为「admin' or 1=1#」， SQL 语句将变成这样：

```php
$query = "SELECT * FROM admin WHERE username='admin' or 1=1#' and password='xxxxxxxx'";
```

- 原本的逻辑被修改，使得即使在密码输入错误的情况下仍然可以登录 admin 账户
- **根本原因**：脚本语言无法理解 SQL 语句，两者对查询语句处理不一致导致 SQL 注入，篡改了 SQL 语句原本逻辑

OWASP Top 10 漏洞讲解及练习

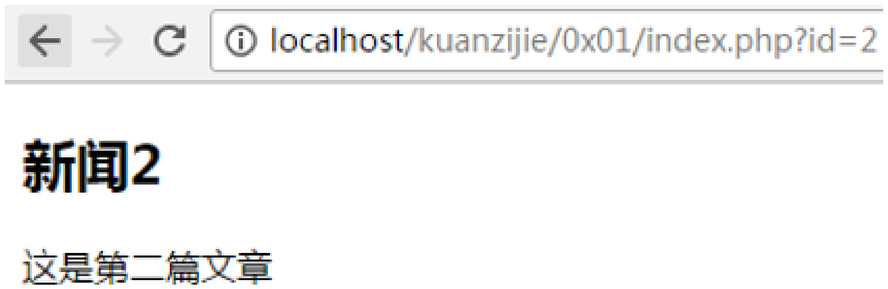
A03：注入式攻击 —— SQL 注入

- **SQL 注入主要类型**
  - **Union 注入**：通过联合操作，直接将数据带出，一般有回显
  - **报错注入**：通过 MySQL 的报错信息，把数据带出来
  - **布尔盲注**：通过页面不一致来把数据盲注出来。
  - **时间盲注**：通过相应时间长短来盲注数据。
- 其他类型：宽字节注入、二次注入等

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

- Union 语句可以填充查询结果，并且额外执行一次查询

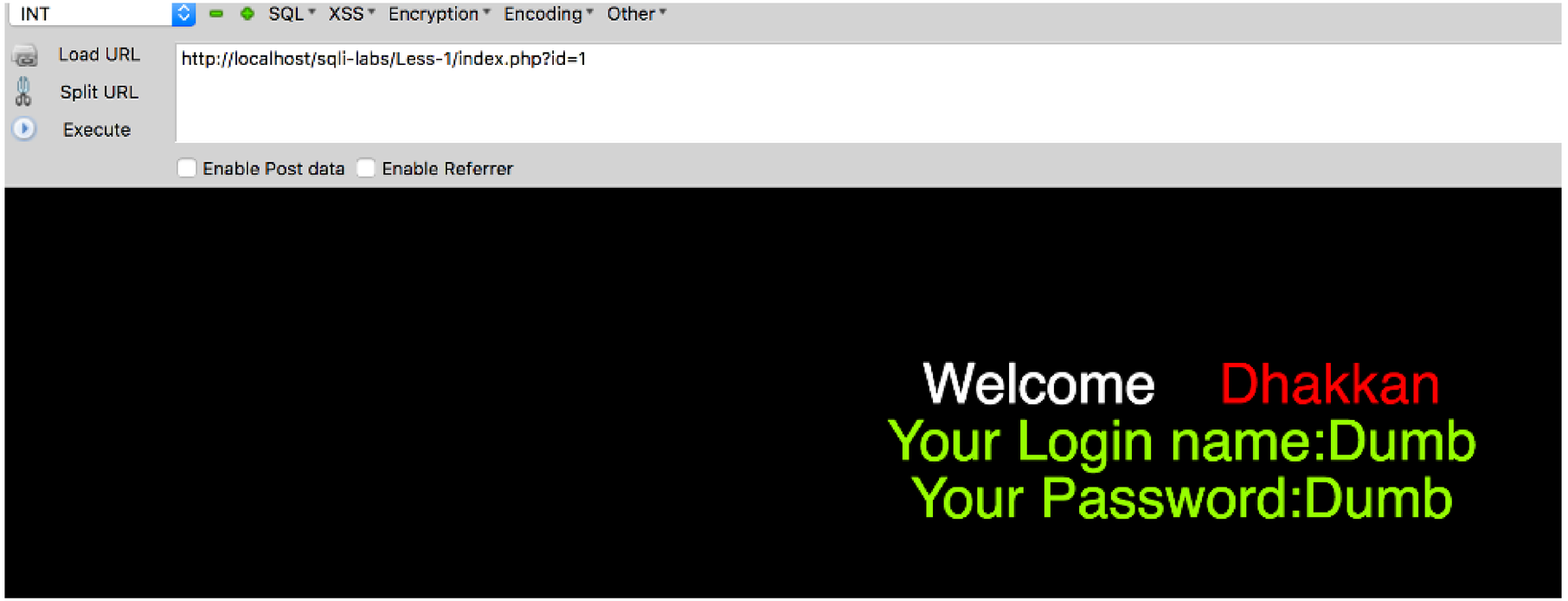



```
mysql> select * from news;
+-----+-------+----------------+
| tid | title | content        |
+-----+-------+----------------+
|   1 | 新闻1 | 这是第一篇文章 |
|   2 | 新闻2 | 这是第二篇文章 |
+-----+-------+----------------+
2 rows in set (0.00 sec)

mysql> select * from news where tid=1;
+-----+-------+----------------+
| tid | title | content        |
+-----+-------+----------------+
|   1 | 新闻1 | 这是第一篇文章 |
+-----+-------+----------------+
1 row in set (0.00 sec)

mysql> select * from news where tid=1 union select 1,2,3;
+-----+-------+----------------+
| tid | title | content        |
+-----+-------+----------------+
|   1 | 新闻1 | 这是第一篇文章 |
|   1 | 2     | 3              |
+-----+-------+----------------+
2 rows in set (0.00 sec)
```

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

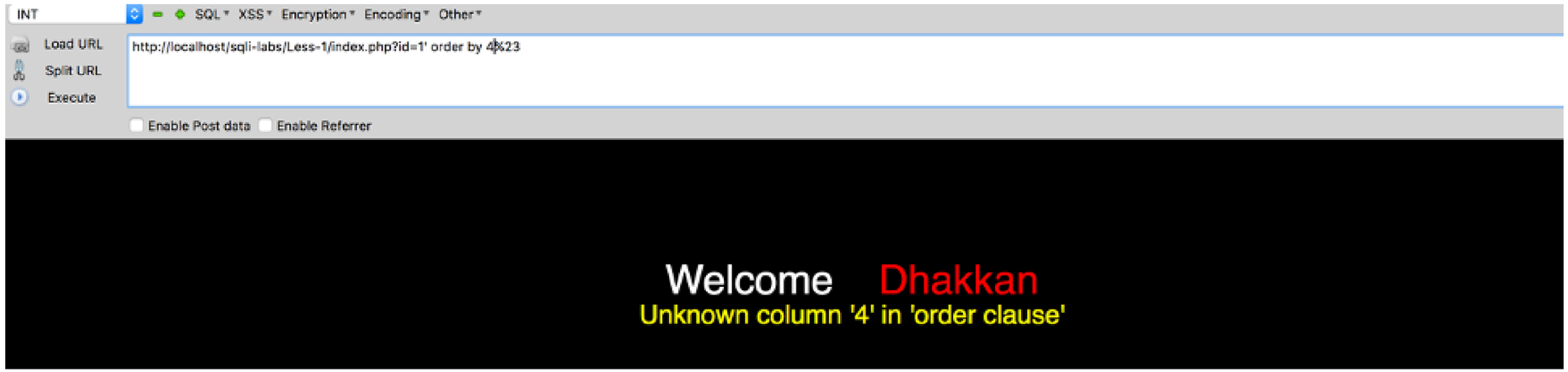
- sqli-labs Less-1 http://c.eki.im:8030/Less-1/index.php
- 正常情况



OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

- order by 判断列数

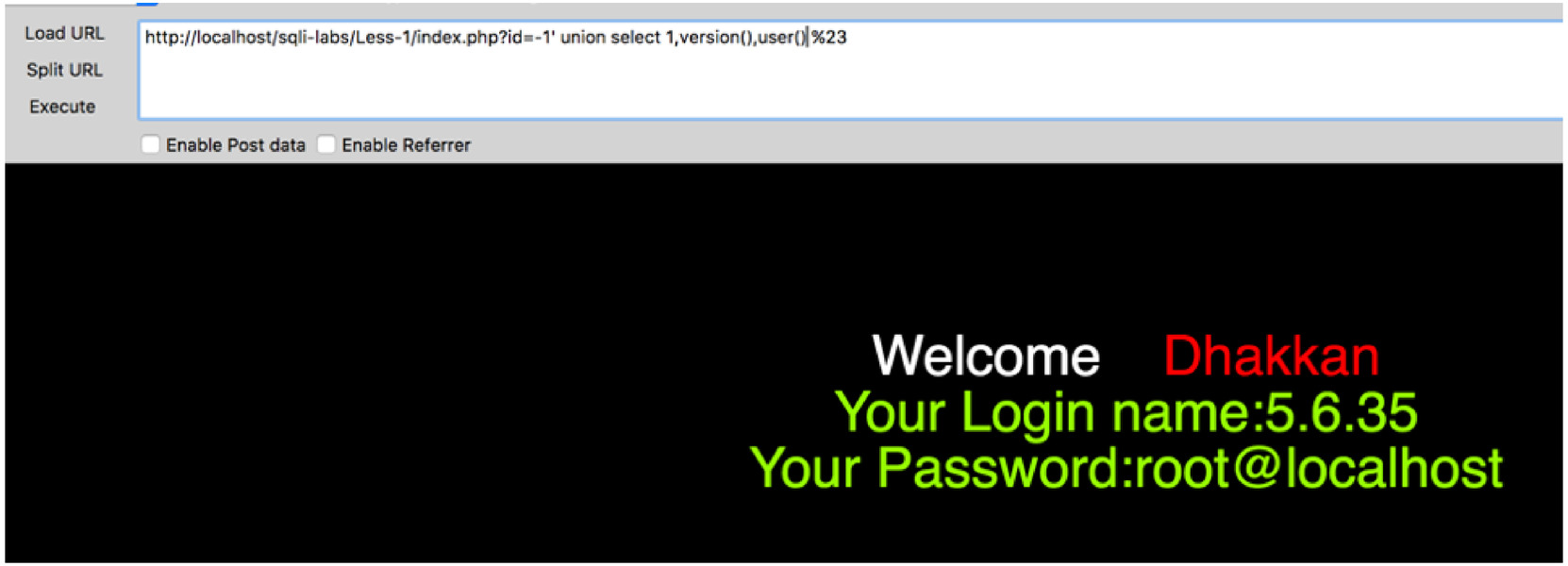


- 说明只有三列。（order by 4 报错）

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

- 注数据



OWASP Top 10 漏洞讲解及练习

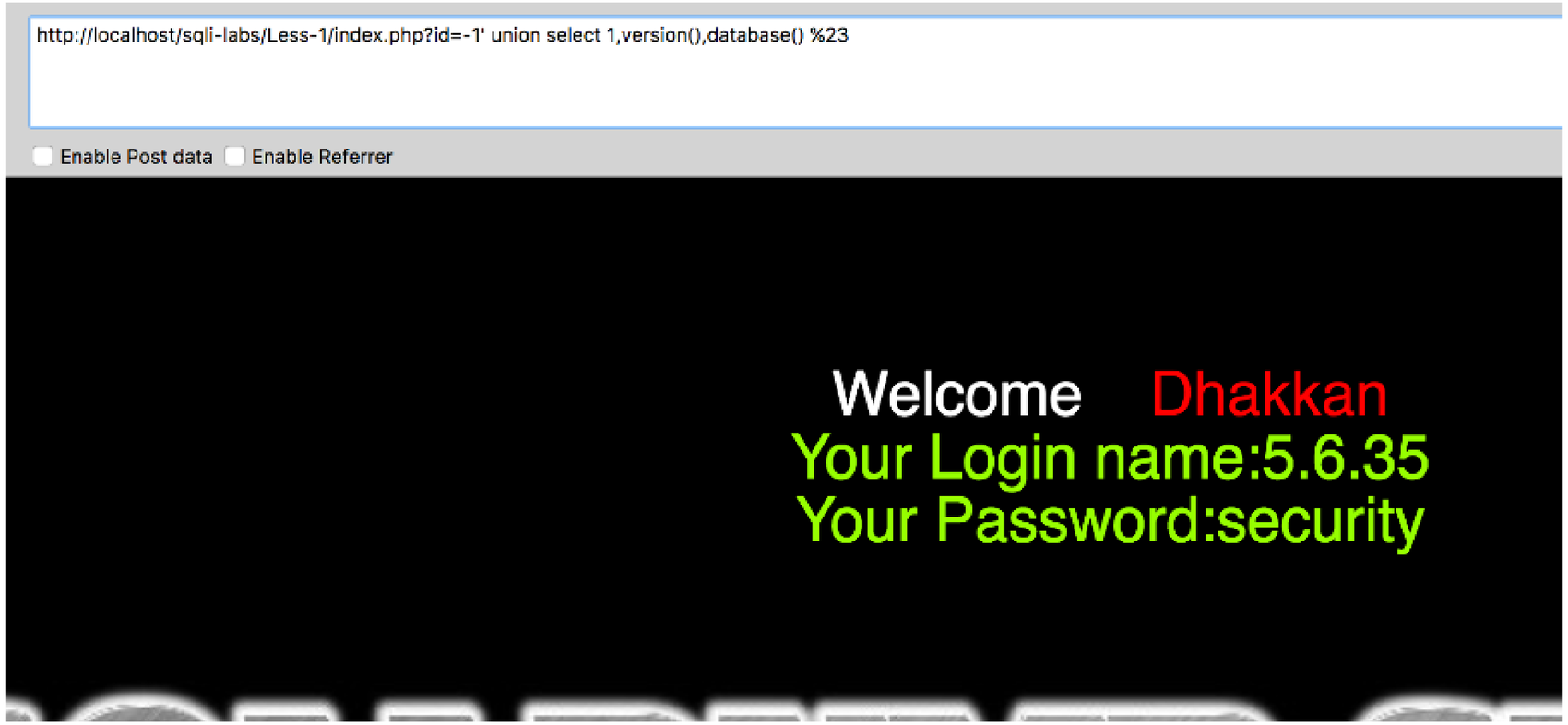
A03：注入式攻击 —— Union 注入

- 一般步骤
  - union select 1,2,database()
  - union select 1,2,table_name from information_schema.tables where table_schema = ‘数据库名字’ limit 0,1 #
  - union select 1,2,column_name from information_schema.columns where table_schema=“xx” and table_name=“xx”limit 0,1 #
  - union select 1,2,列名 from 表名 limit 0,1 #

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

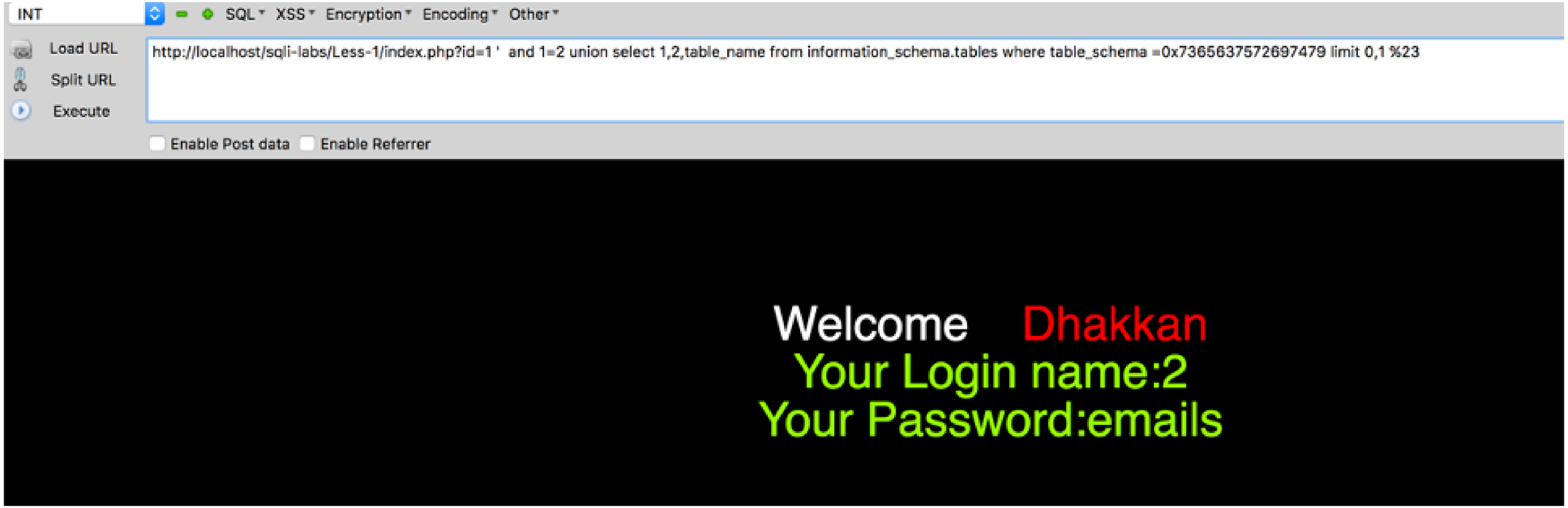
- 获取数据库



OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

- 获取表名



OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

- 练习：http://c.eki.im:8002
- 目标：登陆 admin

```php
$user=trim(str_replace(" ","",$_POST['username']));
$pwd=md5($_POST['password']);
$query="SELECT password FROM admin WHERE username='".$user."'";
$result=$pdo->query($query);
if ($result!=null&&$result->rowCount()!==0)
{
    while($row = $result->fetch())
    {
        if ($row['password']===$pwd)
            echo $flag;
        else
        {
```

OWASP Top 10 漏洞讲解及练习

A03：注入式攻击 —— Union 注入

- 练习：http://c.eki.im:8002

- Payload：
  username=admin'/**/union/**/select/**/'21232f297a57a5a743894a0e4a801fc3'#&password=admin

谢谢大家！