上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

被动发现已证实的 Web 漏洞

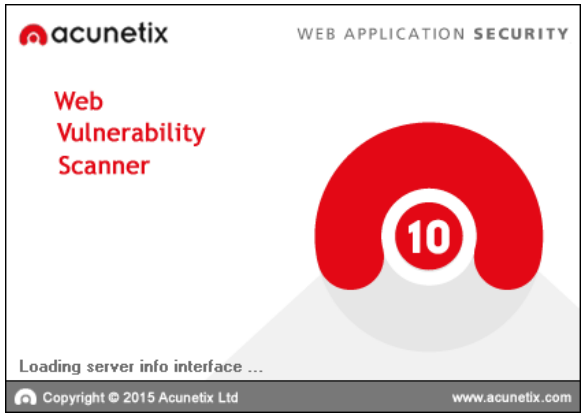
章思宇，姜开达，孙强

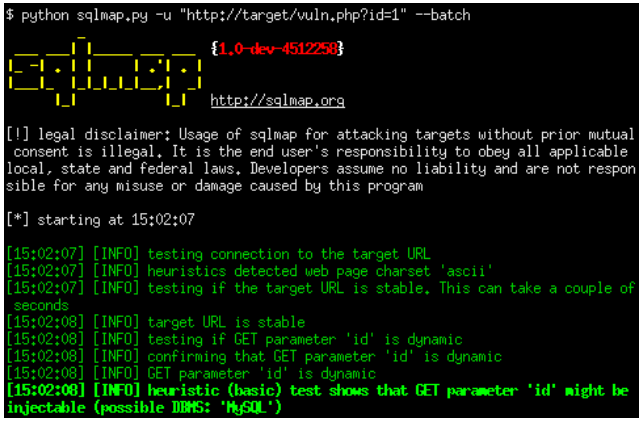
上海交通大学 网络信息中心

2015 年 11 月 25 日

攻击方

- 自动化的扫描、入侵工具
  - 没有专业 Web 和安全知识也能轻松“黑”网站





防御方

- WAF 带来“虚假的安全感”
  - 漏洞未被真正修复
  - WAF 可以被绕过
    - 内部攻击，跳板，VPN，SSL/TLS

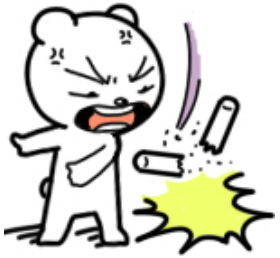
防御方

- 主动安全检测
  - 扫描一个站点平均半小时
    - 部分长达 6 小时以上
  - 爬虫覆盖范围有限

Adam Doupé, et al. “Why Johnny Can‘t Pentest: An Analysis of Black-Box Web Vulnerability Scanners”, DIMVA 2010.

防御方

- 主动安全检测
  - 扫描一个站点平均半小时
    - 部分长达 6 小时以上
  - 爬虫覆盖范围有限
- Web 日志 / WAF 告警分析
  - 任何扫描和入侵企图都会触发告警
    - 无法判断漏洞是否真实存在
  - 扫描器对 所有页面 所有参数 提交攻击代码
    - 对不存在页面也不放过



Adam Doupé, et al. “Why Johnny Can‘t Pentest: An Analysis of Black-Box Web Vulnerability Scanners”, DIMVA 2010.

本文的工作

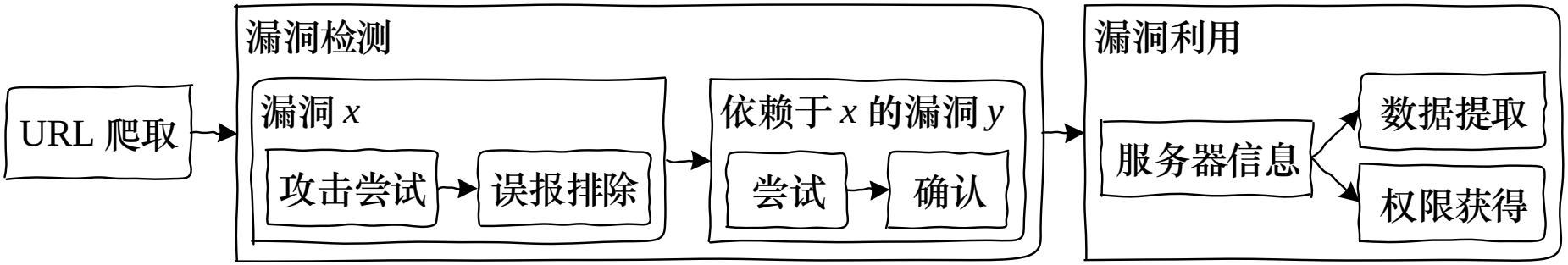
- 目标：

被动发现 已证实 的 Web 漏洞

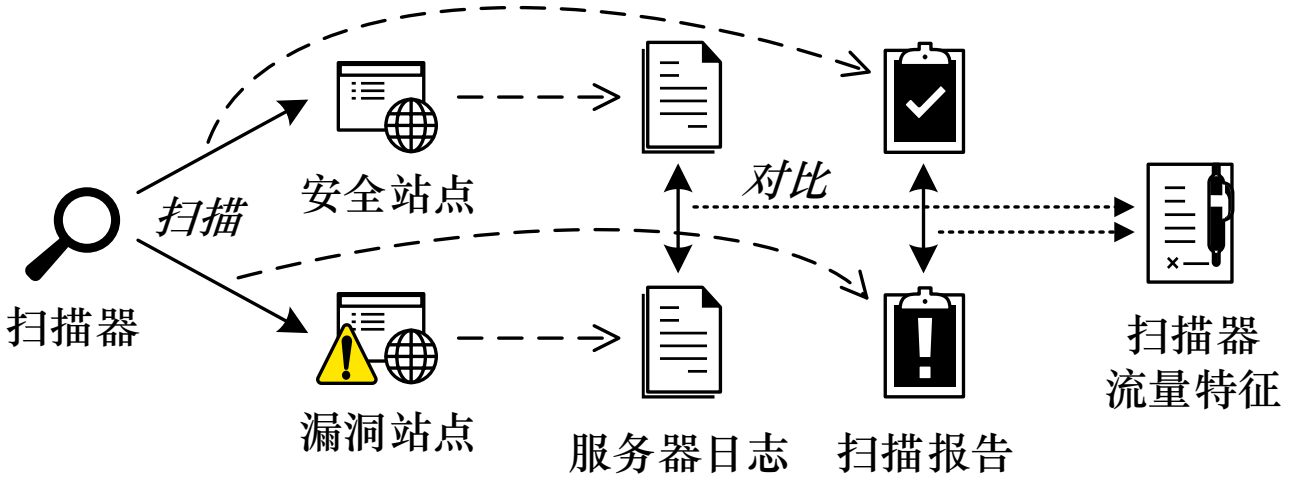
- 基于流量 / 日志分析，不发起主动探测
- 精确定位存在漏洞的页面

本文的方法

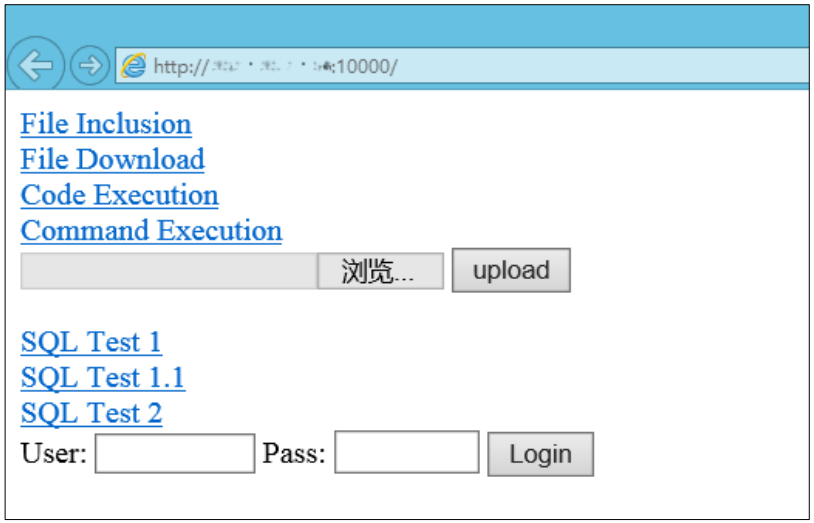
- 分析扫描器的漏洞检测逻辑
  - 先发现漏洞 → 后利用漏洞
  - 漏洞检测分为多个步骤（初步探测 → 验证 / 误报排除）
  - 漏洞之间的依赖关系



提取扫描器特征



- Web Alerts (58)
  - Blind SQL Injection (3)
  - Code execution (2)
  - Cross site scripting (2)
  - Cross site scripting (verified) (4)
  - Directory traversal (4)
  - File inclusion (2)
  - File upload XSS (2)
  - File upload XSS (Java applet) (2)
  - PHP code injection (2)
  - Script source code disclosure (1)
  - Server side request forgery (2)
  - SQL injection (1)
  - Unrestricted file upload (4)
  - Weak password (2)
  - Application error message (1)
  - Cross domain data hijacking (2)
  - Directory listing (1)
  - HTML form without CSRF protection (3)
  - Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28 (1)
  - Password field submitted using GET method (1)
  - User credentials are sent in clear text (1)



案例：通用型扫描器

- SQL 注入
  - `id=1 → id=0+0+0+1 → id=12345+12345+1`
- 基于时间的盲注
  - `if(now()=sysdate(),sleep(6),0)`
    `→ if(now()=sysdate(),sleep(0),0)`
- 文件下载
  - `../../usr/bin/id → /etc/passwd%00.jpg`
- 文件上传
  - `.jpg, .html → .php, .asp, ...`

实际效果：通用型扫描器

- 半年 HTTP 流量日志
  - 2,886 亿条，gzip 压缩后 11.6 TB
- 将需要关注的站点数减少 57.6%
  - 并精确指出存在漏洞的页面

攻击阶段	攻击数	目标站点数
扫描	6,405	3,408
w3af	*573*	*402*
商业扫描器 A	*5,033*	*2,723*
商业扫描器 B	*799*	*527*
漏洞确认	1,744	1,446

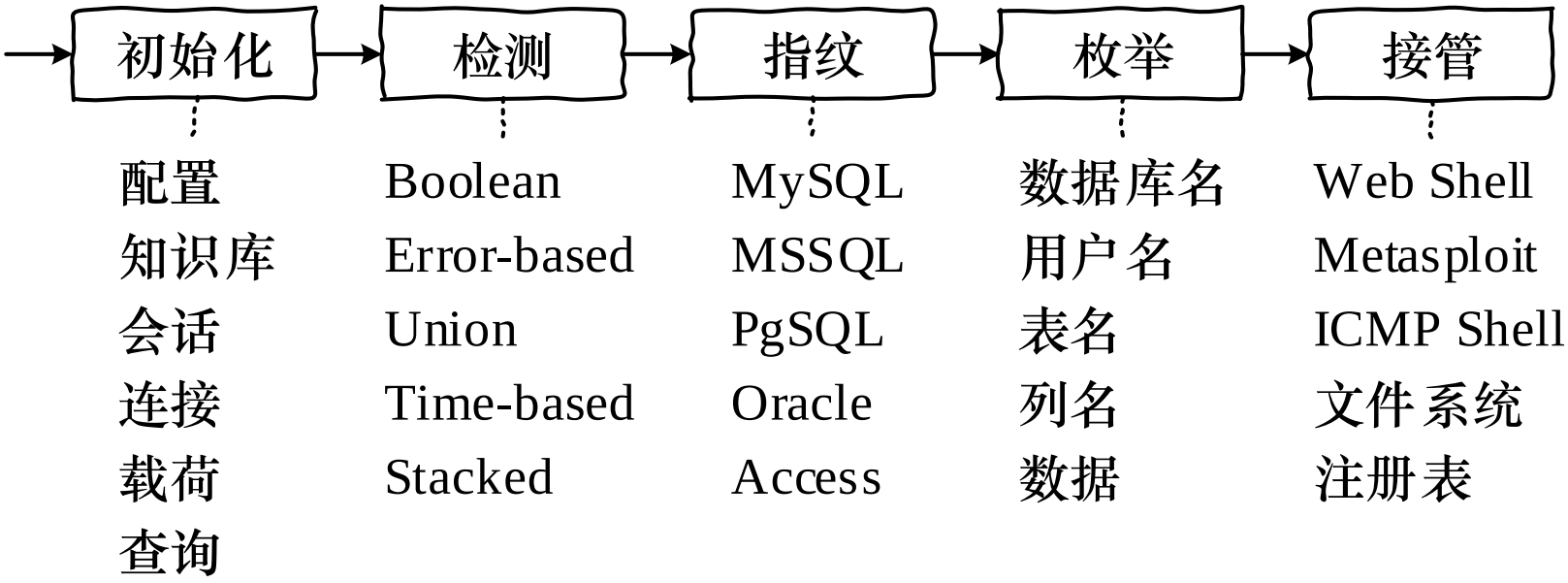
实际效果：通用型扫描器

[To Parent Directory]

2015/6/13	1:40	42	${@print(md5(security test))}
2015/6/13	1:40	164	%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%c0%af%c0%ae%c0%ae%
2015/6/13	1:40	43	'
2015/6/13	1:40	45	';print(md5(security test));$a='
2015/6/13	1:40	30	(select convert(int,CHAR(65)))
2015/6/13	1:40	1	)
2015/6/13	1:40	57	..%5c..%5c..%5c..%5c..%5c..%5c..%5c..%5cwindows%5cwin.ini
2015/6/13	1:40	30	.....windowswin.ini
2015/6/13	1:40	3	1'
2015/6/20	11:08	1	1.asp;.jpg
2015/6/13	1:40	43	1some inex
2014/4/7	14:08	12801	
2015/6/13	1:40	40	;print(md5
2015/6/13	1:40	7	@@av767
2015/6/13	1:40	7	@@UnvKk
2015/6/20	11:10	69	a1.aspx
2015/6/13	9:12	14	.txt
2015/6/13	1:40	156	Test1145.xml
2015/6/13	1:41	337	Test142.phtml
2015/6/13	1:40	44	Test1993.htm
2015/6/13	1:41	547	Test4401.php.ajpg
2015/6/13	1:41	337	Test5593.php3
2015/6/13	1:40	156	Test5934.jpg
2015/6/13	1:40	337	Test5983.php
2015/6/13	1:41	337	Test6798.php.jpg
2015/6/13	1:41	48	Test7168.php
2015/6/13	1:41	337	Test7467.php.123
2015/6/13	1:41	96	Test801.htaccess
2015/6/13	1:41	61	Test8741.asp
2015/6/13	1:40	337	Test9674.jpg
2015/6/13	1:40	418	Applet2593.class
2015/6/13	1:40	221	CDDH3313.jpg
2015/6/13	1:40	6	e''e
2015/6/13	1:40	4	JyI=
2015/6/13	1:40	19	testasp.vulnweb.com

文件上传 & 可执行

案例：Sqlmap



获取用户名	IFNULL%28CAST%28CURRENT_USER%28%29%20AS%20CHAR%29%2C0x20%29
数据库名	IFNULL%28CAST%28DATABASE%28%29%20AS%20CHAR%29%2C0x20%29
枚举表名	IFNULL%28CAST%28table_name%20AS%20CHAR%29%2C0x20%29
枚举列名	IFNULL%28CAST%28column_name%20AS%20CHAR%29%2C0x20%29

实际效果：Sqlmap

- 98% 的 sqlmap 扫描未进入利用阶段
  - 仅 5% 被扫描站点存在较高风险

攻击阶段	攻击数	目标站点数
扫描	108,816	10,578
服务器信息获取	1,343	536
获取用户名	*776*	*371*
获取数据库名	*871*	*326*
数据库枚举	99	60
枚举表名	*77*	*52*
枚举列名	*49*	*30*

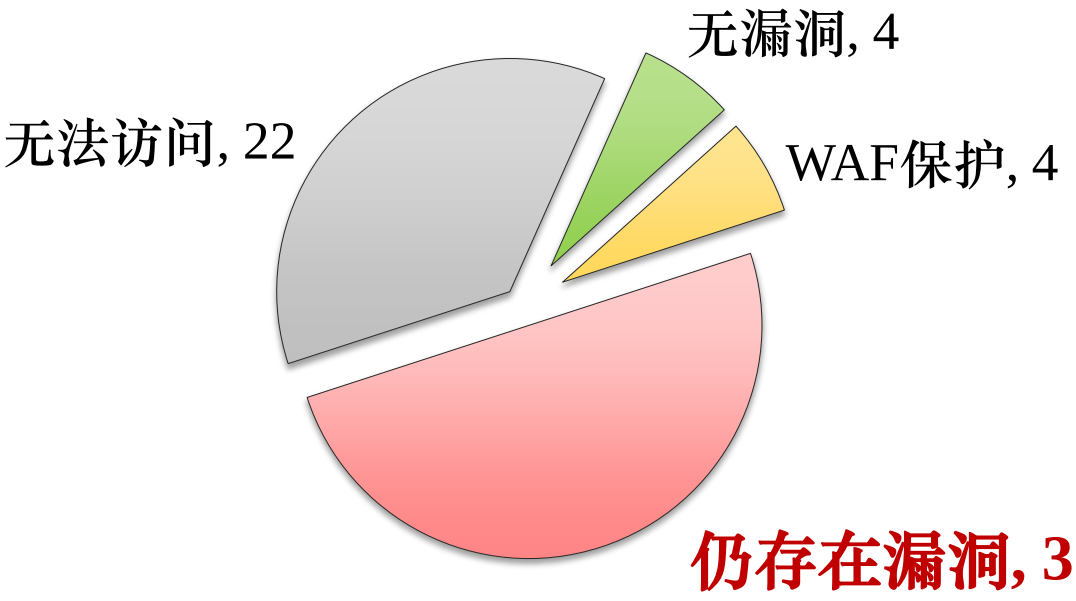
10,578
被扫描

536
潜在漏洞

60
可 “拖库”

实际效果：Sqlmap

- 98% 的 sqlmap 扫描未进入利用阶段
  - 仅 5% 被扫描站点存在较高风险



10,578
被扫描

536
潜在漏洞

60
可 “拖库”

总结

- 被动检测
  - 免去重复全站爬行扫描的开销
- 精确定位漏洞页面
  - 仅报告被自动化扫描器确认存在的漏洞
- 适用于大范围监测和漏洞发现
  - 部署在校园网出口
  - 实时检测、离线分析

谢谢！

章思宇

dfxbb@sjtu.edu.cn

上海交通大学 网络信息中心