



课程内容



- 1 课程概况
- 2 Web安全现状
- 3 什么是Web应用
- 4 脆弱的Web应用
- 5 什么是Web安全

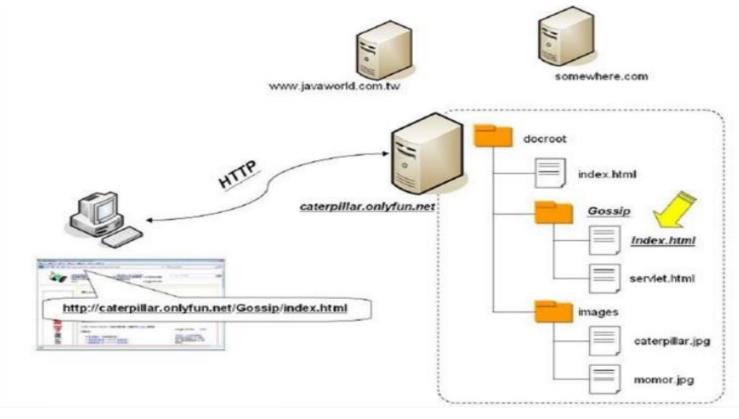






什么是Web应用?

❖通常情况下,我们了解到的Web应用是指提供Web服务的应用系统,其实通俗讲就是一个网站。











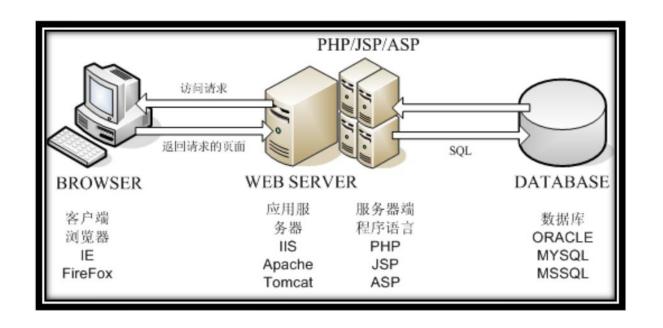
- ❖Web应用对于我们现在的生活已经越来越紧密了,去搜资料、网上购物、看视频、玩游戏、社交等等活动都与Web应用息息相关。





Web应用系统架构

❖实际上一个Web应用并不是我们所理解的那么简单,它是一个由多个要素构成的系统。Web应用程序的设计者、Web应用服务器、动态脚本引擎、数据库是构成Web应用必不可少的要素









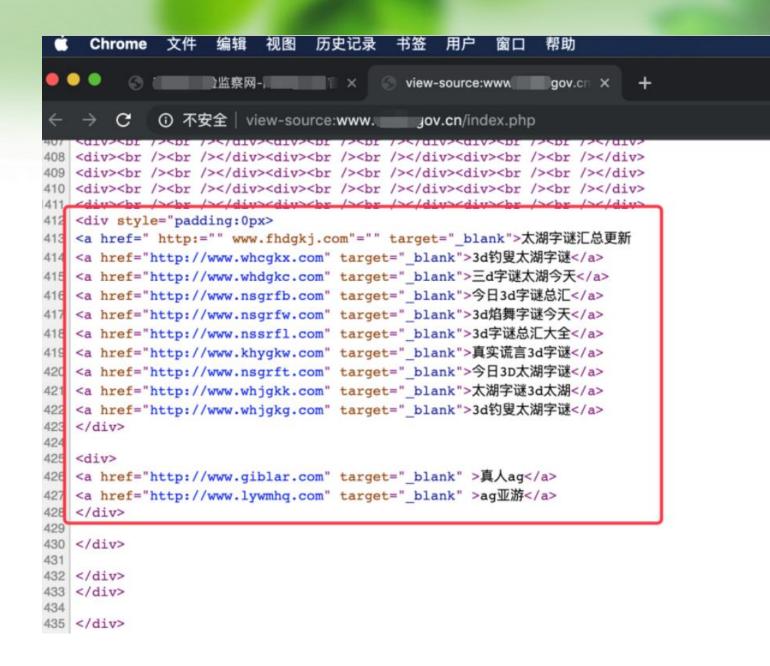
脆弱的Web应用

❖ 有时候我们在访问网站的时候经常会看见各种各样的奇怪的事物,比如博彩、黑页、暗链、反共等等事件出现在各大网站上。















拖库攻击





D H &	a x a a	接(C) 宏(D D	- Pare		ER ER	· 07 50	F7 + 1	- 10-	4	
12306. tat ×		-			Tree res	that the	C1 10	804			
274667266@qq. com	6837605	郑一峰—	-3325221	987050400	11	z6837605	1506	8860664-	2746	67266@gq.	com
zaistar@163.com	tianxia512-	一池善卿-	-35042	619790906	301X-	-chitan	g520	181050133	289	zaistar@l	63. c
weizhongjie55@163.	om wzj277	13-P	. 木2	106021987	1126051	13wz	j871126-	187077	734000-	weizho	ngji
xujsh2004@yahoo.com	n. cn 19830	307—i4	家圣	340103198	3030725	554x	ujsh2012	18225	5513108	xujsh	2004
7939255640gg. com-				319930721	0015	-lijing	nan741-	-1802410	5681	-7939255	640c
chenkan588@163.com	chengkang	陈侃-	36232	619830627	0039-	-chenka	n588	182582880)23	chenkan58	8016
kangjie109@163.com	-159648sl-	康焕卉	4305	031987061	30038-	kangj	ie109-	-13716008	3430	-kangjiel	0901
a21353360163.com	a2135336-	池鹏	33108119	860121001	4cr	p165147-	18888	731462-	-a2135	3360163. c	omi
daqi1003@163.com	liudaqi	刘大奇—	-2301031	985091213	52	daqi1003	1581	0596619-	dagi	10030163.	core
779860552@gg. com-	a26549828	一许子豪	12010	619950119	1514	-xiaoxu	bisheng-	-131321	10868-	779860	5526
122106144@qq. com	-tj119820515		-13082	519940816	1416	-tj1122	106144-	1503163	39524	-1221061	4480
alyce01@163.com	sn6331907-	沈楠	34262319	810914033	5sı	n1101213	7132	41233214	aly	ce010163.	com
chiwuchizu@163.com	-19851103-	杨豪-	-522125	198511033	430	-chiwuch	izu-l	507090019	99cl	hiwuchizu	0163
anjing_thw@yahoo.co	om. cnTHW1	60178	谭宏旺一	4228231	9851116	63376	-anjing	thw1	871776	906 an	jing
441536746@qq. com-	k6r5c4yd-	王雷		880808641						7468qq. co	
momozq@163.com	55627904	K庆——31	01091985	0214201X-				67 			
444587374@qq. com	-7187856	于峰——	70602198	30224041X	— jdr	netyf-	-1390535	4001	1445873	748qq. com	4
444719203@qq. com-	-chen123	陈明——	31223199	110305030	che	enming91	1030-	185706030	041	444719203	Dqq.
396608503@qq. com	-yyc1990	严益春—	-4222011	990011608	14	yanyc861	2137	33453960-	396	608503@qq	. con
253375011@qq. com-	-ilove31219-	刘洋	431002	198211301	517	dragonl	yzq1	345049065	562	533750110	qq. c
nancunzan@163.com	-96163110-	一南存赞-	33038	219890917	1738-	nancun	zan1	829599589	96-n	ancunzan@	163.
mssj03800163.com	-1k77550313-	一规康一	-130982	198610307						103800163	
yujin1984@126.com	65192253	一于谨一	-2206221	984040900	13	yujin198	4.	微信者	す: lei	clania	£16.





2022/6/14



2020年赏金最高的十大漏洞类型

❖ 根据Hacker One发布的十大漏洞列表,跨站点脚本(XSS)仍然是影响力最大的漏洞,因此该漏洞在2020年连续第二年为白帽子黑客获得了最高的回报──2020年为黑客赢得了420万美元的漏洞赏金,比2019年增长了26%

	Weakness Type	Bounties Total Financial Rewards Amount	YOY % Chage
1	XSS	\$4,211,006	26%
2	Improper Access Control - Generic	\$4,013,316	134%
3	Information Disclosure	\$3,520,801	63%
4	Server-Side Request Forgery (SSRF)	\$2,995,755	103%
5	Insecure Direct Object Reference (IDOR)	\$2,264,833	70%
6	Privilege Escalation	\$20.017,592	48%
7	SQL Injection	\$1,437,341	40%
8	Improper Authentication - Generic	\$1,371,863	36%
9	Code Injection	\$982,247	-7%
10	Cross-Site Request Forgery (CSRF)	\$982,247	-7%



https://www.aqniu.com/industry/70970.html

脆弱的原因: 代码不完善

- ❖ 现在Web应用不仅是主要战场之一,它的安全问题也是一直层出不穷,并且到现在仍没有被冲淡。原因有很多:
 - 程序开发人员没有安全意识。开发者不知道哪里的代码存在"Bug", 功能的确是开发完成了,但是开发的代码上出现了漏洞。
 - 有经验的程序员可能会考虑安全问题,但毕竟不是专业的安全人员, 并且并不是每一个人都是"大牛"。
 - 当项目上线之后的服务器环境可能会有变化,本来没有问题的代码可能就变得有问题了。
 - 后台管理的弱口令、一些配置型错误等都会存在安全问题。
- ❖ 并且对于攻击者的技术门槛也并不高,所以对于它的很多攻击手段并没有我们想象中的那么"难"



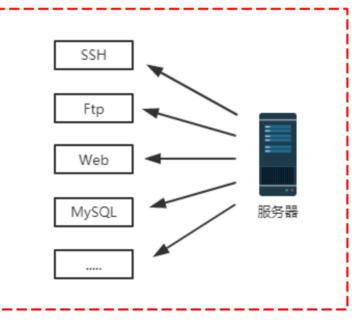




脆弱的原因:端口开放

- ❖对于服务器的入侵方式有很多,比如端口扫描、SSH口令爆破、Ftp爆破、缓冲区溢出攻击等等去直接获取目标的权限。
- ❖由于现在Web应用的飞速发展,现在战场逐渐转移到了Web之上











什么是Web安全?

- ❖Web应用安全是现代计算机安全界中的一个重要组成部分。自 互联网出现以来,关于Web应用的安全问题就一直层出不穷。
- ❖我们常说的Web安全一般是指Web应用中存在着的不安全的隐患,对于这些不安全的隐患,我们常称之为"漏洞"。
- ❖黑客利用网站操作系统和Web服务程序的各类漏洞得到Web服务器的控制权限,轻则篡改网页内容,重则窃取重要内部数据,更为严重的则是在网页中植入恶意代码,使得网站访问者受到侵害。



