

短信验证码系列（二）

0X01（四位数验证码爆破）：

原理：在我们收到验证码的时候会有一个时间限制，比如 60s、五分钟内、24 小时内失效，但是往往这些验证码都不会在这个时间内失效，此时我们就可以考虑爆破验证码来获取认证。

（其实此处还有一个漏洞就是如果验证码在规定时间内没有失去效果，也是可以提交的）

常见存在漏洞的功能点：

1、修改密码功能点：修改密码时不需要输入原密码，网站通过验证码决定是否为本用户修改，并且网站的验证码机制没有时间（或者时间在一分钟以外最好，方便爆破）和次数限制，

2、用户注册点：如果可以爆破验证码，此时我们就可以获取任意用户注册漏洞，等级在中 高危 赏金可以达到四位数

3、支付功能点：如果支付时是通过短信验证，而且还是四位数的验证码，也可以尝试爆破

总而言之只要遇见短信验证的地方都可以尝试

爆破验证码最好是爆破四位的，六位的话可能需要更多时间。

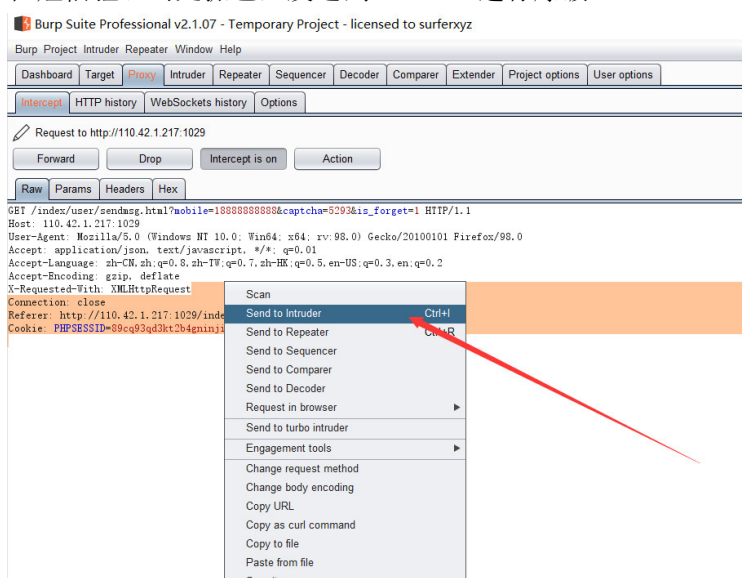
fcmit.cc

0X02（操作）：

1、工具：BURP

2、操作：

在短信验证码处抓包，发送到 intrudre 进行爆破



鼠标左键选择要爆破的位置，然后点击 add 即可

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

1 2 ...

Target Positions Payloads Options

② Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

GET /index/user/sendmsg.html?mobile=18888888888&captcha=5293&is_forget=1 HTTP/1.1
Host: 110.42.1.217:1029
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:98.0) Gecko/20100101 Firefox/98.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: http://110.42.1.217:1029/index/user/forget.html
Cookie: PHPSESSID=89c93qd3kt2b4gninjiu868ic

Start attack

Add \$
Clear \$
Auto \$
Refresh

接下来在第三个模块选择爆破方法：（各种爆破方法去 b 站学习），最后点攻击即可。

Target Positions Payloads Options

② Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 0
Payload type: Simple list Request count: 0

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste
Load ...
Remove
Clear
Add Enter a new item
Add from list ...

② Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add Enabled Rule

Start attack

fcmitt.cc

0X03（案例）：

参与活动

漏洞类型 应用漏洞 >> 设计缺陷/逻辑错误

提交时间 2021-11-15 11:52:32

危害自评 低危

奖励安全币 5

附件 --

描述 在登录框任意输入账号获取验证码：

找回密码

验证码

登录

然后登录抓包 爆破

可以看成成功爆破成功

Wireshark packet capture showing a successful login attempt. The packet list shows a GET request to /login with a status of 200. The packet details show the response body containing a success message.