

# Web学习路线

## 0x00 前言

这是我依据我浅薄的学习经历来总结的，难免有很多缺漏甚至谬误的地方。一来是因为我个人能力的局限性，二来是Web安全这方面的知识点实在太多太杂，很难完全总结下来。所以，如果你发现有什么问题，请在下面评论或直接发email:[momomomoxiaozi@gmail.com](mailto:momomomoxiaozi@gmail.com)给我，我好修改，谢谢大家。 (orz链接编辑失效了，有点多。。大家自行复制吧)

去年，我与我的团队在我母校创立了一个安全协会与对应的实验室，我们想通过一个这样的学生组织为一些对信息安全知识有充足兴趣的人提供一个较好的学习平台，让大家能够更加容易地跨入信息安全的大门。

之前，我好像过于强调个人自学能力的重要性，而有些忽视对大家的系统培训，只是从一些角度来告诉大家，哪些东西需要去学，安全方面有哪些东西。

现在，我发现这个做法可能不大妥当，安全范围实在太广，让大家自己直接去学，可能大家很难去完全把控好学习的流程，哪些先学，哪些后学。这样，很有可能就大大降低了大家的学习效率。所以，我打算写一篇类似学习路线的博文，希望能给大家一些帮助。

此外，由于我先前学习的主要还是Web方向，所以这篇博文也只是关于Web安全方向的学习流程。后面，我也会尽量请求一些老司机们能花一些时间为大数写一些其他方向的入门学习路线。

## 0x01 基础语言

- 首先，花4天时间大略过一下最基础的语言语法HTML / CSS、JavaScript、PHP、SQL的基本知识（平均一个语言4小时足矣），要做到看到这些代码的时候不会畏惧，能看懂大部分，看到不懂的能通过google或者相关文档查懂。主要参考：<http://www.w3school.com.cn/> <http://www.runoob.com/>
- 现在，你初步了解了一些语言知识，接下来你就需要开始在实践中学习与巩固。

我一直有一个这样的观点，其实我们学习一样东西，最好的学习方式就是实践与理论双螺旋式学习，先学习一部分东西，然后折腾实践，遇到不懂的，再去查，查懂了，再去实践...周而复始，一步步学习。最后，再通过一本相对系统的书，对该知识从头复习一遍。这样，就能基本掌握这部分知识。

这里，我建议你搭建一个个人的博客，初步了解这些语言的应用。在搭建博客的过程中，你需要学习对应的linux操作、Apache+PHP+Mysql环境的配置、域名解析、服务器端口配置等等。如何搭建博客，请自行google搜索。

此外，你也可以编写一些好玩的网页来学习这些知识点。

第2步大约花费你7-14天的时间。

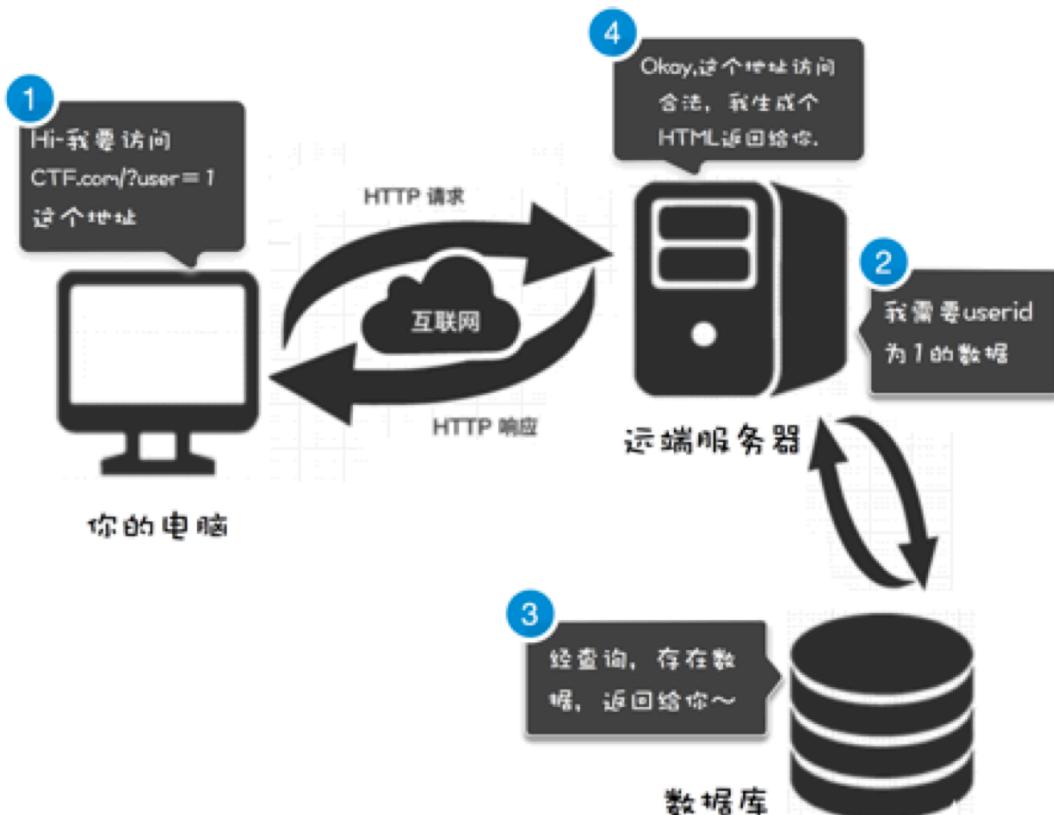
- 如果经过第2步，你掌握了以下几个技能就可以进入下一个阶段了。
  - 大体能看到百分之80以上简单的HTML / CSS、JavaScript、PHP、SQL的代码
  - 基本了解一个index.php是如何解析的。（一个包含了PHP、SQL字符串、JavaScript、

- HTML / CSS代码的文件) 明白为什么前端看不到PHP, 明白为什么后端PHP中可以混杂其他的语言
- 能基本在Linux下配置Apache+PHP+Mysql环境 (请尽量使用最原生的Apache、 Mysql, 不要使用集成工具! 尽量使用命令行, 不要使用Gui)
  - 能基本使用FTP工具、 SSH

4. 后期, 你还需要了解DOM、 BOM、 ajax、 json的知识。

## 0x02 其它基础

1. 了解最基本的C/S物理结构



2. 了解基本的HTTP协议相关知识

- 掌握HTTP请求: GET、 POST、 HEAD, 能基本读懂一个HTTP数据包, 了解GET、 POST、 HEAD的区别
- 能看懂HTTP响应包 404 403 200 500 ...
- 了解Cookie、 session、 token, 知道是什么东西, 作用是什么, 为什么需要这些东西
- 了解Referer、 X-Frame-Options等等的作用

参考:

1. <http://www.ruanyifeng.com/blog/2016/08/http.html>
2. <http://www.cnblogs.com/li0803/archive/2008/11/03/1324746.html>
3. <http://momomoxiaoxi.com/2016/01/26/NetworkAnalysis/>

3. 了解基本的浏览器解析的流程与原理

参考:

1. <http://fex.baidu.com/blog/2014/05/what-happen/>
2. <http://ued.ctrip.com/blog/how-browsers-work-rendering-engine-html-parsing-series-ii.html>
3. <http://www.jianshu.com/p/e305ace24ddf>
4. <http://www.cnblogs.com/yuezk/archive/2013/01/11/2855698.html>

这一部分可能会比较复杂，大家最开始只需要有一种基本的概念即可，后面逐渐弄懂他们。

#### 4. 了解一些编码

1. 基本编码 <http://www.qianxingzhem.com/post-1499.html> 其中宽字节编码重点了解一下<http://www.cnbraid.com/2016/02/28/sql4/>
2. HTML字符实体编码、对应的命名实体、URL编码、JS编码、CSS编码、Base64编码

这三种编码在挖掘XSS漏洞的时候尤为有用！当然，有时候其他的注入攻击的时候也会用到

参考：

1. [http://www.ruanyifeng.com/blog/2010/02/url\\_encoding.html](http://www.ruanyifeng.com/blog/2010/02/url_encoding.html)

2. <https://security.yirendai.com/news/share/26>

3. <http://www.freebuf.com/articles/web/43285.html>

4. <http://bobao.360.cn/learning/detail/292.html> (比较推荐这个)

5.

<http://paper.seebug.org/papers/Archive/drops2/XSS%E4%B8%8E%E5%AD%97%E7%AC%A6%E7%BC%96%E7%A0%81%E7%9A%84%E9%82%A3%E4%BA%9B%E4%BA%8B%E5%84%BF%20---%E7%A7%91%E6%99%AE%E6%96%87.html> (还有这个)

6. 对应的编解码工具：<http://evilcos.me/lab/xssor/>  
<http://evilcos.me/lab/xssee/>

#### 3. 序列化编码问题

Java、PHP、Python序列化问题

1.

<http://www.crazydb.com/archive/Java%E3%80%81PHP%E3%80%81Python%E7%9A%84%E5%8F%8D%E5%BA%8F%E5%88%97%E5%8C%96%E9%97%AE%E9%A2%98>

2. <http://www.hollischuang.com/archives/1140>

3. <http://www.wtoutiao.com/p/1e1gMC1.html>

4. <http://www.milw0rm.cn/Article/web/20161020/607.html>

编码安全问题在前端安全方面一直是一个很重要的方面，请大家务必重视。不过这个方面一开始很难完全掌握，大家一开始只需要有一个较为完整的概念即可，后面迭代深入学习。

#### 5. 稍微了解下同源策略

<http://www.ruanyifeng.com/blog/2016/04/same-origin-policy.html>

知道为何需要同源策略，同源策略有什么好处与坏处，同源策略主要是来应对什么类型的攻击。

在这一块的学习过程中，你肯定会遇到很多很多不懂的地方，也会感觉学习这个东西很难。不过，你要放心，这是最正常的现象。因为我把一些后面的东西都放在了这里。大家可以前后花一周时间，把第二块过下来。每天学习一个知识点，并写一篇博文。然后，再花3-5天的时间，巩固复习这一块。

## 0x02 常见知识普及

该部分主要是一些非常常见的攻击方式，与对应的学习。我尽量把常见的东西写了出来，但是肯定还很不全，请大家谅解。学习这一部分知识的时候，你会发现你很难完全学透，就是学了感觉懂了，遇到真实渗透环境的时候，又啥都不会。要解决这个问题很简单——无他，唯手熟尔。多实践，多写笔记，多总结回顾！

整个部分知识范围很广，大家应该每个知识点花1-2礼拜左右的时间，初步学习。学习完一个后，再换一个知识点学习，加油！

### SQL注入

1. 最基础的注入知识（数字型、字符型、搜索型）注入模式：基于布尔 基于时间 基于报错 联合注入 堆查询注入 各类数据库
2. 宽字节注入
3. 二次注入
4. http头注入
5. 伪静态注入
6. Nosql注入（MongoDB注入）
7. base64变形注入
8. 偏移注入
9. 各种绕waf注入
  - 大小写变种
  - 编码
  - SQL注释
  - 空字节
  - ....

有时候，工具或者单纯手注会比较麻烦，此时你需要用Python或者定制化sqlmap来进行注入：）

参考：

1. <https://github.com/Audi-1/sql-labs> （首要推荐，刷完这些题基本就入门了！Web方向的请务必刷完）
2. [http://websec.ca/kb/sql\\_injection](http://websec.ca/kb/sql_injection) （系统基础知识，很难完全看完，可以当字典）
3. <http://www.cnblogs.com/lcamry/articles/5625276.html> （宽字节）
4. <http://ecma.io/?tag=%E4%BA%8C%E6%AC%A1%E6%B3%A8%E5%85%A5> （二次注入）
5. <http://redtiger.labs.overthewire.org/> （题目）

6. [http://wooyun.tangscan.cn/search?  
keywords=sql%E6%B3%A8%E5%85%A5&content\\_search\\_by=by\\_bugs](http://wooyun.tangscan.cn/search?keywords=sql%E6%B3%A8%E5%85%A5&content_search_by=by_bugs) (乌云的SQL例子，复制点开)

## XSS攻击

1. 基础科普与总结：

<http://www voidcn com/blog/bcbobo21cn/article/p-6066052.html>

[http://iptable.lofter.com/post/1cc1708a\\_6b62e3e](http://iptable.lofter.com/post/1cc1708a_6b62e3e)

2. 比较完整系统的文档（英语，但是非常推荐）[https://www owasp org/index.php/XSS\\_Filter\\_Evasion\\_Cheat\\_Sheet](https://www owasp org/index.php/XSS_Filter_Evasion_Cheat_Sheet)
3. <https://www secpulse com/archives/44299.html?from=timeline&isappinstalled=1> flash XSS
4. 训练平台（废话不多说，开始练吧：）：
  - <http://xsst.sinaapp.com/xss/> 乌云那些年系列
  - <http://xss-quiz.int21h.jp/> 答案：[http://blog knownsec com/ Knownsec\\_RD\\_Checklist/res/xss\\_quiz.txt](http://blog knownsec com/ Knownsec_RD_Checklist/res/xss_quiz.txt)
  - <http://prompt.ml/0> 答案：<https://github com/cure53/XSSChallengeWiki/wiki/prompt.ml>
  - <http://xss-game.appspot.com/>
5. XSS平台：<http://123.57.48.113/xss//index.php?do=login>
6. 乌云XSS实例：[http://wooyun.tangscan.cn/search?  
keywords=XSS&content\\_search\\_by=by\\_bugs&search\\_by\\_html=true](http://wooyun.tangscan.cn/search?keywords=XSS&content_search_by=by_bugs&search_by_html=true)

## 文件上传

简单的上传文件，查看响应

是否只是前端过滤后缀名，文件格式，

抓包绕过

是否存在截断上传漏洞

是否对文件头检测，（图片马等等）

是否对内容进行了检测，尝试绕过方法

是否上传马被查杀，免杀

是否存在各种解析漏洞

http头以两个CRLF(相当于\r\n\r\n)作为结尾，\r\n码没有被过滤时，可以利用\r\n\r\n作为url参数截断http

头，后面跟上注入代码

参考：

1. <http://byd.dropsec.xyz/2016/05/11/%E4%B8%8A%E4%BC%A0%E6%BC%8F%E6%B4%9E%E6%80%BB%E7%BB%93/> (复制点开)
2. <http://lovexiaofeng.cn/2016/07/27/19/>
3. <http://lovexiaofeng.cn/2016/07/27/20/>
4. <http://lovexiaofeng.cn/2016/07/27/21/>
5. <http://thief.one/2016/09/22/%E4%B8%8A%E4%BC%A0%E6%9C%A8%E9%A9%AC%E5%A7%BF%E5%8A%BF%E6%B1%87%E6%80%BB-%E6%AC%A2%E8%BF%8E%E8%A1%A5%E5%85%85/> (复制点开)
6. 乌云例子：[http://wooyun.bystudent.com/search?keywords=%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0&content\\_search\\_by=by\\_bugs](http://wooyun.bystudent.com/search?keywords=%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0&content_search_by=by_bugs) (复制点开)

看完上面的几个博文，基本就了解了什么是上传漏洞，与大多数的手法。不过，暂时没找到专门针对这个漏洞的训练平台，后面找到了再贴上来。

## CSRF

1. <http://seeicb.com/2016/04/19/CSRF%E5%AD%A6%E4%B9%A0/> (复制点开)
2. <http://www.cnblogs.com/hyddd/archive/2009/04/09/1432744.html?login=1>
3. 乌云的例子：[http://wooyun.bystudent.com/search?keywords=CSRF&content\\_search\\_by=by\\_bugs](http://wooyun.bystudent.com/search?keywords=CSRF&content_search_by=by_bugs)

这个漏洞，我没挖过，研究的也不是很深入，这里就抛砖引玉吧。

## 文件包含

1. <http://www.secbox.cn/hacker/9777.html> (一篇比较全的文件包含总结博文)
2. <http://wps2015.org/drops/drops/PHP%E6%96%87%E4%BB%B6%E5%8C%85%E5%90%AB%E6%BC%8F%E6%B4%9E%E6%80%BB%E7%BB%93.html> (复制打开，乌云知识库的一篇)
3. <https://www.secpulse.com/archives/3206.html>
4. 乌云例子：[http://wooyun.bystudent.com/search?keywords=%E6%96%87%E4%BB%B6%E5%8C%85%E5%90%AB&content\\_search\\_by=by\\_bugs](http://wooyun.bystudent.com/search?keywords=%E6%96%87%E4%BB%B6%E5%8C%85%E5%90%AB&content_search_by=by_bugs) (复制打开)

## 命令执行

1. <http://seeicb.com/2016/04/30/%E5%91%BD%E4%BB%A4%E6%89%A7%E8%A1%8C-%E4%BB%A3%E7%A0%81%E6%89%A7%E8%A1%8C%E6%BC%8F%E6%B4%9E%E5%AD%A6%E4%B9%A0/> (复制打开)
2. Struct2 命令执行漏洞
3. [https://www.owasp.org/index.php/Command\\_Injection](https://www.owasp.org/index.php/Command_Injection)
4. 还有一些序列化问题也会导致命令执行

自行搜吧。

# PHP审计

弱类型、intval、strpos、两等于问题、反序列化+destruct、\0截断、iconv截断、parse\_str函数、伪协议、堆栈溢出、缓存读取问题。。

1. 《代码审计：企业级web代码安全架构》 入门可读
2. <http://blog.neargle.com/SecNewsBak/drops/%E4%BB%A3%E7%A0%81%E5%AE%A1%E8%AE%A1%E5%85%A5%E9%97%A8%E6%80%BB%E7%BB%93.html> (复制，一份总结，推荐)
3. <http://xlixi.li.net/?p=488> (小tips)
4. <https://code.google.com/archive/p/pasc2at/wikis/SimplifiedChinese.wiki> (一篇非常值得一看的代码审计提高篇)
5. 例子：<https://github.com/Xyntax/1000php>

PHP审计是一门很深的学问，也非常有趣，不会考验太多的脑洞，很考验基本功。希望大家能沉下心学习。后期，可以尝试用脚本实现一些自动化审计的工作。

## 0x03 一些常用工具学习与使用

1. Burpsuite (必须)
2. Firefox
  - Firebug (必须)
  - Tamper Data
  - Live Http Header
  - Hackbar (必须)
  - Modify Headers
  - Fiddler (推荐)
3. Chrome F12开发者功能分析
4. Sqlmap (必须)
5. NoSQLMap
6. Metasploit
7. chopper

这里推荐一些工具，请大家自行学习：）

了解这些东西，大家大概花一个礼拜就够了，但是用好这些工具至少得实践很久很久。。我感觉自己就不大熟练。

## 0x04 其他

因为Web方面的东西很多，我自己也只是了解了一点点，前面讲的都是非常常见的攻击和知识点。后面会放一些，我觉得可能需要看一看或者了解方面的知识。大家自行学习即可。（如果你完成了前面几步，基本就属于安全入门了）

1. 密码学基础

RSA、AES、MD5、ECC、各类古典密码  
码<http://www.icst.pku.edu.cn/course/Cryptography/%E7%AC%AC1%E7%AB%A0%E7%AC%AC2%E8%AE%B2.pdf> (复制)

## 2. 源码泄漏

- github库中有泄漏
- 网站自带的泄漏，一般常见后缀

```
list1= [" .swp", ".bak", "~", "zip", ".tar.gz", ".rar", ".tar", ".old", ".7z", ".gz", ".txt", ".inc", ".copy", ".src", ".tmp", ".orig", ".dev", ".idea"]  
list2=[".git", ".DS_Store", ".svn", "CVS", "robots.txt"]
```

- 社工相关信息泄漏

## 3. 旁注

渗透的时候需要，CTF还没见过

## 4. 提权

5. 魔法哈希问题
6. 内网渗透
7. 各类CMS漏洞
8. 验证码破解 pytesser
9. 各类开发框架漏洞：Django / Rails / ThinkPHP
10. XSIO 攻击<http://huaidan.org/archives/2154.html#more-2154>
11. LDAP注入
12. XPATH注入
13. XML注入
14. XXE注入<http://blog.csdn.net/u011721501/article/details/43775691>
15. padding oracle attack
16. squid问题
17. 各类缓存导致的问题
18. 反弹shell
19. 中间件解析漏洞
  - IIS
  - Apache
    - Nginx  
<http://thief.one/2016/09/21/%E6%9C%8D%E5%8A%A1%E5%99%A8%E8%A7%A3%E6%9E%90%E6%BC%8F%E6%B4%9E/> (复制打开)

## 20. 乌云

- 公开漏洞、知识库搜索 <http://wooyun.bystudent.com/>
- 知识库 <http://drops.wiki/>

## 23. 威胁情报 <https://x.threatbook.cn/>

24. 脚本编程训练：<https://www.sebug.org/> <http://www.bugscan.net/> (bugscan的扫描器很不错，有时候CTF中都能扫出一些漏洞)

## 25. CTF训练场

- <http://www.wechall.net/challs> (推荐)
- i 春秋最新的百度CTF专场
- <http://hackinglab.cn/>(基础场)
- <https://ringzer0team.com/challenge>

## 0x05 高级技巧

1. 大数据挖掘
2. 云架构安全
3. 威胁情报
4. 协议方面 HTTP2.0 HTTPS
5. CGC研究
6. CDN 缓存 CSP原理
7. APT <https://github.com/kbandla/APTnotes>

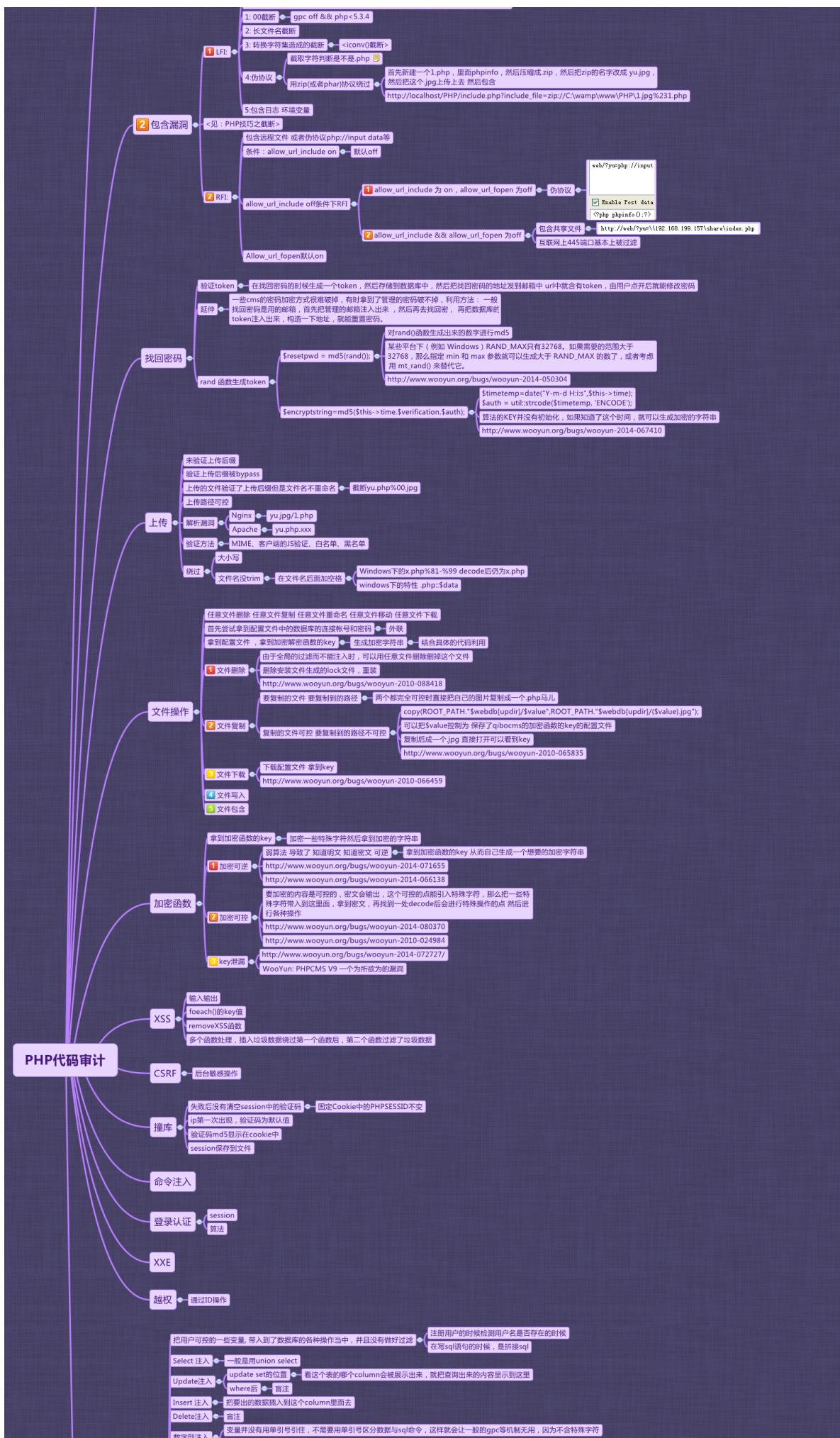
## 0x06 学习建议

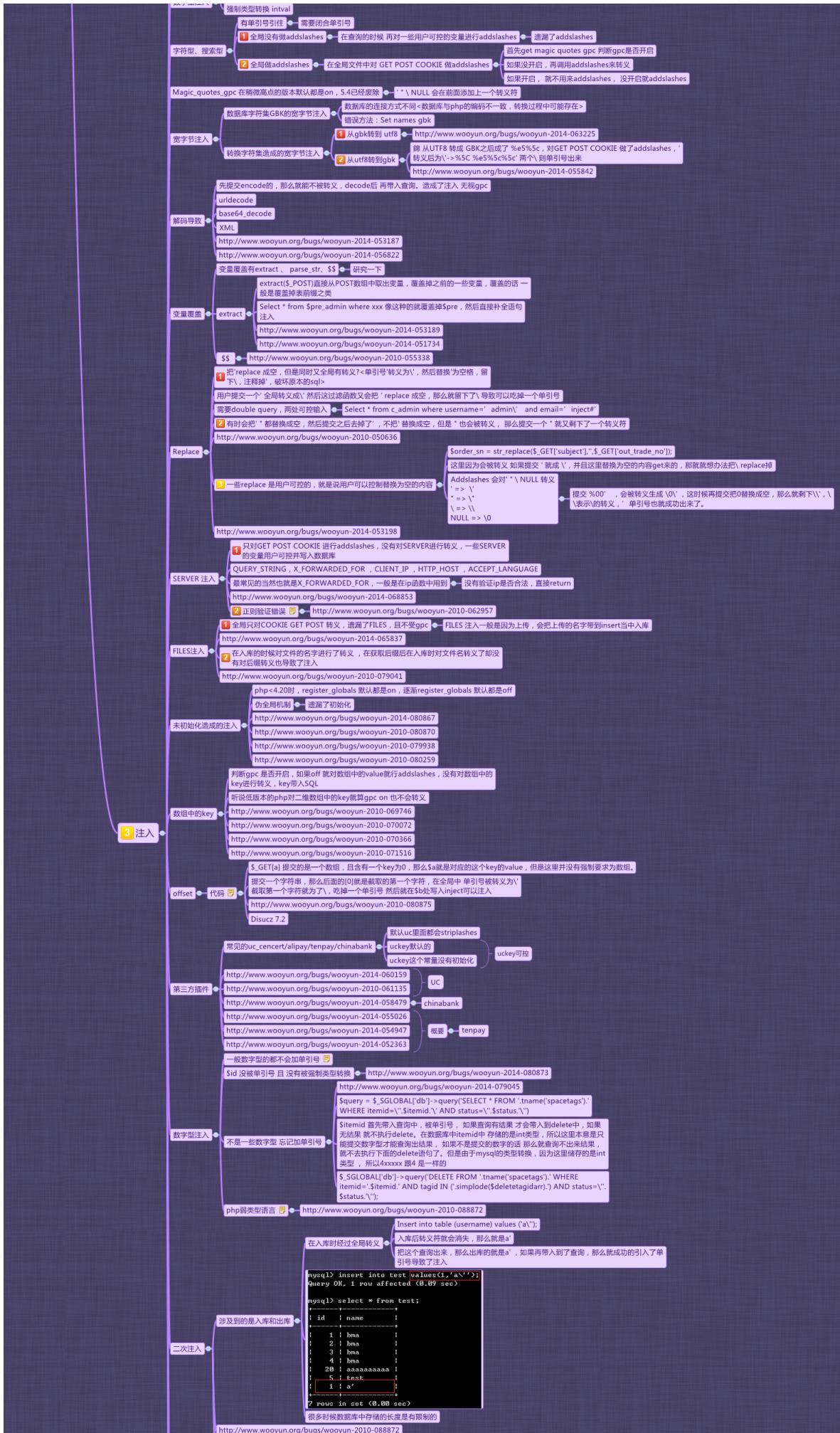
1. 想要了解某个技术，请阅读一些相关文档；想要明白某个技术，请尝试实践这些技术；想要悟透某个技术，请尝试与他人讲解这个技术。
2. 学习一个新的知识点，请务必做学习笔记。如果你有博客，可以尝试写一些技术博文，不需要担心学习笔记太低端，不符合博文的逼格。然后，每个月定期整理学习笔记，回顾学习的东西。
3. 想要快速了解一个领域的前沿情况，请查阅该领域的近几年的优秀论文、看该领域最优秀的人在研究什么（当然最好的方式是找优秀的大牛直接咨询，前提你认识哪些大牛）
4. 专注，我觉得在学习网络安全和任何东西的时候都要分阶段专注学习，切记一下子学太多东西，而都浅尝辄止。
5. 要有依葫芦画瓢的能力，每次看一些0day的分析文章的时候，务必找一些同样版本的代码搭好环境，复现文章的内容。
6. 作为大学生的话，平时可以参与一些安全方面的协会，然后一起打比赛，做项目。不过，切记调控好课程与安全研究的时间，无论怎么不要让自己的课程挂科！切记。如果能力强，十分建议把学习成绩搞好，就算你不打算读研，也很建议你把成绩搞好。

## 0x07 附录：脑图

### 1. PHP代码审计







This screenshot shows a complex interface for analyzing PHP security vulnerabilities. It includes several boxes of text and annotations:

- Top Left:** URLs for various bugs: <http://www.wooyun.org/bugs/wooyun-2014-080877>, <http://www.wooyun.org/bugs/wooyun-2010-068362>, <http://www.wooyun.org/bugs/wooyun-2014-067424>.
- Top Center:** Annotations about `$_POST` being inserted into a query function, leading to a `foreach` loop over keys, which then queries columns. It notes防范方法 (Mitigation) for SQL injection.
- Middle Left:** Annotations for `striplashes` (stripping slashes), mentioning session handling and specific URL: <http://www.2cto.com/Article/201301/182509.html>.
- Middle Center:** Annotations for `cutstr($s,32)` (cutting string to 32 characters), noting it only takes part of the string and does not add characters after the cut.
- Middle Right:** Annotations for `double query` (double query), showing how it can be exploited by injecting a single quote and then another quote.
- Bottom Left:** Annotations for `register_globals` (registering GLOBALS), noting it's disabled by default in REQUEST but enabled in GET/POST.
- Bottom Right:** A link to <http://www.wooyun.org/bugs/wooyun-2010-080723>.
- Bottom Right Corner:** The text "Nop.pw".

## 2. Java



# 致谢

Thanks all !