Beijing Forest Studio

北京理工大学信息系统及安全对抗实验中心

Web应用模糊测试技术

硕士研究生　袁晓筱

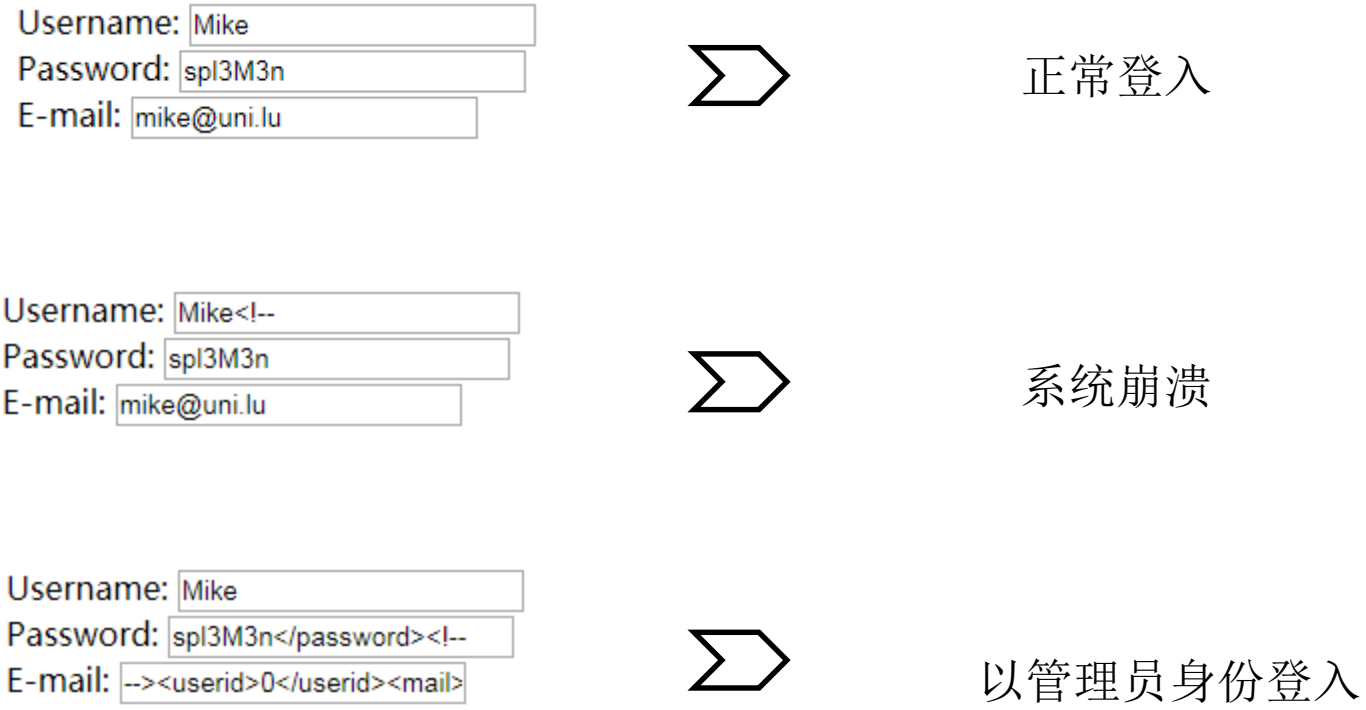
2017年11月5日

目录

基础知识

定义

- 通过一种提供非预期的输入并监视异常结果来发现软件故障的方法。



测试步骤

- 识别目标
  - 分析待测试的目标程序/应用/服务器，确定模糊测试的具体目标范围，定位相关输入输出
- 识别输入
  - 分析测试目标的输入数据，确定目标程序/应用/服务器对输入数据的要求或基本过滤条件
- 生成模糊测试数据
- 执行模糊测试数据
- 监视异常
- 确定可利用性

历史发展

- 纯随机，向目标应用程序抛出随机数据
- 首先分析协议规约，然后产生违背规约或者可能使协议无法正确处理的报文
  - 计算机在内部和外部通信的各个方面都要使用协议，协议构成了数据传输和数据处理的基础结构。
- 可按需自定义功能模块的模糊测试工具框架（平台）
  - 产生长度可变的输入数据
  - 提供一个数值库，库中的数据有较大可能性使应用程序崩溃
  - 一组能产生常见协议和数据格式的函数
- 针对特定程序、文件、漏洞的模糊测试工具
  - 针对环境变量，目的是发现缓冲区溢出漏洞
  - 针对Web浏览器，目的是发现动态HTML脚本的漏洞
  - 针对文件，目的是发现文件格式方面的安全漏洞

分类

- 大类：
  - 基于变异的
    - 对已有数据样本进行变异；
  - 基于生成的
    - 以目标协议或文件格式建模生成；

分类

- 变异或强制性测试；
  - 模糊器从有效的协议或数据格式开始，持续不断的打乱数据包或文件中的每一个字、字节、双字或字符串。
- 协议变异人工测试；
  - 研究者作为模糊器，基于经验输入；
- 随机方法；
  - 大量产生伪随机数据给目标软件；
- 预先生成测试用例；
  - 针对专门的规约，测试所有支持的数据结构和可接受的值范围；
- 自动协议生成测试；
  - 创建描述协议规约如何工作的文法。
  - 模糊器识别数据包或文件中静态和动态的部分，模糊动态部分。

分类

- 本地
  - 命令行
  - 环境变量
  - 文件格式
- 远程
  - 网络协议
  - Web应用
  - Web浏览器
- 内存

Web应用模糊测试方法

Web模糊测试-准备工作

- 建立目标环境
  - 搭建Web服务器和测试客户端
  - 通过客户端发送Web请求，触发Web服务器的漏洞
- 确认输入
  - 输入是发送给Web服务器并被服务器解释的所有信息
  - 测试中需要生成的输入数据是一个发送给Web服务器的完整请求，这个请求可被服务器识别并处理
  - 确认输入后，通过生成不同的Web请求，寻找可能存在的漏洞

Web请求过程

- 发送一个页面请求：

```
1  telnet www.fuzzing.org 80
2  GET / HTTP/1.1
3  Host:www.fuzzing.org
```

  - 启动telnet程序，并提供服务器名和要连接的端口；
  - 将请求方法（GET）告知服务器；发送请求的路径；指明所使用的HTTP协议的版本；
  - 指定主机；
  - 以上是一个最小化请求；

Web请求过程

- 一般的IE浏览器所发送的请求：

```
1  GET / HTTP/1.1
2  Accept: */*
3  Accept-Language: en-us
4  Accept-Encoding: gzip, deflate
5  User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET
   CLR 1.1.4322; .NET CLR 2.0.50727)
6  Host: www.google.com
7  Connection: Keep-alive
8  Cookie: PREF=ID=32a1c6fa8d9e9a7a:FF=4:LD=en:NR=10:TM=1130820854:LM=11354103
   09:S=b9I4GWDAtclpmXBF
```

  - Accept：指定了可以在响应中使用的媒体类型；
  - Accept-Language：指定了可以在响应中使用的自然语言的类型；
  - Accept-Encoding：指定了可接受的编码模式；
  - User-Agent：定义了发出请求的客户端；
  - Host：定义为被请求的Web页提供服务的主机和端口；
  - Connection:指定连接所需要的不同选项；

Web请求模糊测试组成

```
1  [Method] [Request-URI] HTTP/[Major Version].[Minor Version]
2  [HTTP Headers]
3  [Post Data]
```

- 针对以下成分确定模糊测试变量
  - Method
  - Request-URI
  - HTTP Headers
  - Post Data

Method

- 最常用的方法是GET和POST；
- PUT：允许用户向Web服务器上载数据；
- DELETE：允许用户请求从Web服务器中删除一个资源；
- TRACE：允许客户端提交一个请求并返回到发送请求的客户端；
- OPTIONS：允许客户端询问Web服务器以确定服务器所支持的标准和私有的方法；
- HEAD：只返回响应头；
- CONNECT：被保留以供一个代理使用，可以动态转换为一个通道；
- 以上方法在被支持而未被正确实现时，出现相关漏洞；

Request—URI

- URI用于定位被请求的资源（Web页），可以划分为：

```
1  /[path]/[page].[extension]?[name]=[value]&[name]=[value]
```

  - Path
    - 缓冲区溢出攻击；
      - 路径长度超过约65535个字符时，该漏洞被触发；
    - 目录遍历攻击；
      - 发送连续的../字符序列来触发；
  - Page
    - 缓冲区溢出；
      - 发送过长的请求，将面临基于栈的缓冲区溢出；
    - 信息泄露；
      - 不提供授权认证，显示该页内容；

Request-URI

- Extension
  - Web页扩展名指明Web页所采用的技术；
  - 请求使用未知扩展名；
- Name
  - 发送未定义的变量
- Value
  - 发送非期望的数据值或数据类型；
- 分隔符
  - 变为其他格式信息相关字符，如/.=&%等

HTTP Headers和Post Data

- HTTP Headers请求的头信息具有如下格式：

```
[Header name]: [Header value]
```

  - name使用已知的合法值模糊化；
  - value用非预期的值模糊化；
  - ：（分隔符）
  - 堆溢出示例：

```
POST / HTTP/1.1
Content-Length: -900

[覆盖堆的数据]
```

- Post Data数据格式：

```
[Name1]=[Value1]&[Name2]=[Value2]
```

Web应用模糊测试-异常检测

- HTTP状态码
  - 如500服务器错误，401未授权错误；
- Web服务器返回的信息，尤其是错误信息
- 中断连接
- 日志文件
- 调试器

道德经

大成若缺，其用不弊。
大盈若冲，其用不穷。
大直若屈。大巧若拙。
大辩若讷。静胜躁，寒胜热。清静为天下正。

谢谢！