实 验 报 告 册

|  |  |
| --- | --- |
| 课程名称 | 计算机网络原理 |
| 实验名称 | 实验八：HTTP协议分析 |
| 任课教师 | 阮晓龙 | 学期学年 | 2020-2021学年第1学期 |
| 学生学号 | 2019181 | 年级专业 | 2019级信息管理与信息系统 |
| 实验分组 | [x]  A [ ]  B | 小组编号 | 00 |
| 实验时间 | 2020年12月8日星期二 |
| （10分）实验任务完成情况（本实验任务完成情况，未完成注明原因。） |
| 如实填写您参加本次实验学习的过程，以及实验完成情况。对于未完成的部分或者实验出错的部分，要详细填写具体情况并分析原因。填写内容时删除本提示信息。1、（2分）了解HTTP协议2、（2分）熟悉HTTP状态码含义3、（4分）掌握HTTP报文结构 |
| （10分）实验总结与学习心得（本实验的学习总结，以及对本实验的建议。） |
| 针对本次实验情况进行学习总结，主要从实验效果、内容设计、学习收获、知识掌握等方面开展，如对本次实验的设置和教学组织有好的建议，也可以填写至此。填写内容时删除本提示信息。 |
| （4分）考核点8-1 |
| 请填写HTTP报文数据分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **字段名称** | **字段长度** | **起始位置** | **字段值** | **字段表示的信息** |
| 1 | Request Version |  | 第 位 |  |  |
| 2 | Status code |  | 第 位 |  |  |
| 3 | Response Phrase |  | 第 位 |  |  |
| 4 | Content-Length |  | 第 位 |  |  |
| 5 | Content-Type |  | 第 位 |  |  |
| 6 | Content-Location |  | 第 位 |  |  |
| 7 | Last-Modified |  | 第 位 |  |  |
| 8 | Accept-Ranges |  | 第 位 |  |  |
| 9 | ETag |  | 第 位 |  |  |
| 10 | Server |  | 第 位 |  |  |
| 11 | X-Powered-By |  | 第 位 |  |  |
| 12 | Date |  | 第 位 |  |  |
| 13 | Time Since Request |  | 第 位 |  |  |
| 14 | 抓取数据包的详细内容： |
|  |

 |
| （3分）考核点8-2 |
| 请填写HTTP HEAD请求内容分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | User-Agent |  |  |
| 2 | Host |  |  |

 |
| （3分）考核点8-3 |
| 请填写HTTP HEAD请求内容分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Accept-Rangers |  |  |
| 2 | Cache-Control |  |  |
| 3 | Connection |  |  |
| 4 | Content-Length |  |  |
| 5 | Content-Type |  |  |
| 6 | Date |  |  |
| 7 | P3p |  |  |
| 8 | Pragma |  |  |
| 9 | Server |  |  |
| 10 | Set-Cookie |  |  |
| 11 | Strict-Transport-Security |  |  |
| 12 | Traceid |  |  |
| 13 | X-Ua-Compatible |  |  |

 |
| （3分）考核点8-4 |
| 请填写HTTP HEAD请求报文分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **字段名称** | **字段长度** | **起始位置** | **字段值** | **字段表示的信息** |
| 1 | Request Method |  | 第 位 |  |  |
| 2 | Request URI |  | 第 位 |  |  |
| 3 | Request Version |  | 第 位 |  |  |
| 4 | User-Agent |  | 第 位 |  |  |
| 5 | Connection |  | 第 位 |  |  |
| 6 | Host |  | 第 位 |  |  |
| 7 | 抓取数据包的详细内容： |
|  |

 |
| （3分）考核点8-5 |
| 请填写HTTP HEAD响应报文分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **字段名称** | **字段长度** | **起始位置** | **字段值** | **字段表示的信息** |
| 1 | Request Version |  | 第 位 |  |  |
| 2 | Status code |  | 第 位 |  |  |
| 3 | Response Phrase |  | 第 位 |  |  |
| 4 | Content-Length |  | 第 位 |  |  |
| 5 | Content-Type |  | 第 位 |  |  |
| 6 | Content-Location |  | 第 位 |  |  |
| 7 | Last-Modified |  | 第 位 |  |  |
| 8 | Accept-Ranges |  | 第 位 |  |  |
| 9 | ETag |  | 第 位 |  |  |
| 10 | Server |  | 第 位 |  |  |
| 11 | X-Powered-By |  |  |  |  |
| 12 | Date |  |  |  |  |
| 13 | Time Since Request |  |  |  |  |
| 14 | 抓取数据包的详细内容： |
|  |

 |
| （3分）考核点8-6 |
| 请填写HTTP GET请求内容分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | User-Agent |  |  |
| 2 | Host |  |  |

 |
| （3分）考核点8-7 |
| 请填写HTTP GET响应内容分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Accept-Rangers |  |  |
| 2 | Cache-Control |  |  |
| 3 | Connection |  |  |
| 4 | Content-Length |  |  |
| 5 | Content-Type |  |  |
| 6 | Date |  |  |
| 7 | P3p |  |  |
| 8 | Pragma |  |  |
| 9 | Server |  |  |
| 10 | Set-Cookie |  |  |
| 11 | Strict-Transport-Security |  |  |
| 12 | Traceid |  |  |
| 13 | X-Ua-Compatible |  |  |

 |
| （3分）考核点8-8 |
| 请填写HTTP HEAD响应报文分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **字段名称** | **字段长度** | **起始位置** | **字段值** | **字段表示的信息** |
| 1 | Request Method |  | 第 位 |  |  |
| 2 | Request URI |  | 第 位 |  |  |
| 3 | Request Version |  | 第 位 |  |  |
| 4 | User-Agent |  | 第 位 |  |  |
| 5 | Connection |  | 第 位 |  |  |
| 6 | Host |  | 第 位 |  |  |
| 7 | 抓取数据包的详细内容： |
|  |

 |
| （3分）考核点8-9 |
| 请填写HTTP GET响应报文分析

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **字段名称** | **字段长度** | **起始位置** | **字段值** | **字段表示的信息** |
| 1 | Request Version |  | 第 位 |  |  |
| 2 | Status code |  | 第 位 |  |  |
| 3 | Response Phrase |  | 第 位 |  |  |
| 4 | Content-Length |  | 第 位 |  |  |
| 5 | Content-Type |  | 第 位 |  |  |
| 6 | Content-Location |  | 第 位 |  |  |
| 7 | Last-Modified |  | 第 位 |  |  |
| 8 | Accept-Ranges |  | 第 位 |  |  |
| 9 | ETag |  | 第 位 |  |  |
| 10 | Server |  | 第 位 |  |  |
| 11 | X-Powered-By |  |  |  |  |
| 12 | Date |  |  |  |  |
| 13 | Time Since Request |  |  |  |  |
| 14 | 抓取数据包的详细内容： |
|  |

 |
| （3分）考核点8-10 |
| 请填写HTTPs请求内容分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | User-Agent |  |  |
| 2 | Host |  |  |

 |
| （3分）考核点8-11 |
| 请填写HTTPs响应内容分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Accept-Rangers |  |  |
| 2 | Cache-Control |  |  |
| 3 | Connection |  |  |
| 4 | Content-Length |  |  |
| 5 | Content-Type |  |  |
| 6 | Date |  |  |
| 7 | P3p |  |  |
| 8 | Pragma |  |  |
| 9 | Server |  |  |
| 10 | Set-Cookie |  |  |
| 11 | Strict-Transport-Security |  |  |
| 12 | Traceid |  |  |
| 13 | X-Ua-Compatible |  |  |

 |
| （2分）考核点8-12 |
| 请填写Cilent Hello报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | Handshake Protocol Version |  |  |
| 8 | Random GMT Unix Time |  |  |
| 9 | Random Random Bytes |  |  |
| 10 | Session ID Length |  |  |
| 11 | Cipher Suites Length |  |  |
| 12 | Compression Methods Length |  |  |
| 13 | Extensions Length |  |  |
| 14 | Extension |  |  |
| 15 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-13 |
| 请填写Server Hello报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | Handshake Protocol Version |  |  |
| 8 | Random GMT Unix Time |  |  |
| 9 | Random Random Bytes |  |  |
| 10 | Session ID Length |  |  |
| 11 | Session ID |  |  |
| 12 | Cipher Suite |  |  |
| 13 | Compression Methods |  |  |
| 14 | Extensions Length |  |  |
| 15 | Extension |  |  |
| 16 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-14 |
| 请填写Certificate请求分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | Certificates Length |  |  |
| 8 | Certificate |  |  |
| 9 | signedCertificate |  |  |
| 10 | Certificate version |  |  |
| 11 | Certificate serialNumber |  |  |
| 12 | Certificate signature |  |  |
| 13 | Certificate issuer |  |  |
| 14 | Certificate issuer |  |  |
| 15 | Certificate issuer rdnSequence |  |  |
| 16 | Certificate validity notBefore |  |  |
| 17 | Certificate validity notAfter  |  |  |
| 18 | Certificate subject rdnSequence |  |  |
| 19 | Certificate subjectPublicKeyInfo |  |  |
| 20 | Certificate subjectPublicKeyInfo Padding |  |  |
| 21 | Certificate subjectPublicKeyInfo subjectPublicKey |  |  |
| 22 | Certificate extensions |  |  |
| 23 | Certificate algorithmIdentifier |  |  |
| 24 | Certificate Padding |  |  |
| 25 | Certificate encrypted |  |  |
| 26 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-15 |
| 请填写Server Key Exchange报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | EC Diffie-Hellman Server Params |  |  |
| 8 | Curve Type |  |  |
| 9 | Named Curve |  |  |
| 10 | Pubkey Length |  |  |
| 11 | Pubkey |  |  |
| 12 | Signature Hash Algorithm |  |  |
| 13 | Signature Hash Algorithm Hash |  |  |
| 14 | Signature Hash Algorithm Signature |  |  |
| 15 | Signature Length |  |  |
| 16 | Signature |  |  |
| 17 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-16 |
| 请填写Server Hello Done报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-17 |
| 请填写Server Hello Done报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-18 |
| 请填写Client Key Exchange报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | Handshake Protocol Length |  |  |
| 7 | EC Diffie-Hellman Client Params |  |  |
| 8 | Pubkey Length |  |  |
| 9 | Pubkey |  |  |
| 10 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-19 |
| 请填写Change Cipher Spec（Client）报文分析**表8-18 Change Cipher Spec（Client）报文分析**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Change Cipher Spec |  |  |
| 5 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-20 |
| 请填写Encrypted Handshake Message报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-21 |
| 请填写New Session Ticket报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | Handshake Type |  |  |
| 6 | TLS Session Ticket |  |  |
| 7 | Session Ticket Lifetime Hint |  |  |
| 8 | Session Ticket Length |  |  |
| 9 | Session Ticket |  |  |
| 10 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-22 |
| 请填写Change Cipher Spec报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Change Cipher Spec |  |  |
| 5 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-23 |
| 请填写Encrypted Handshake Message请求报文分析

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Handshake Protocol |  |  |
| 5 | 抓取数据包的详细内容： |
|  |

 |
| （2分）考核点8-24 |
| 请填写Application Data报文分析**表8-23 Application Data报文分析**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **Key** | **Value** | **字段表示的信息** |
| 1 | Content Type |  |  |
| 2 | Version |  |  |
| 3 | Length |  |  |
| 4 | Encrypted Application Data |  |  |
| 5 | 抓取数据包的详细内容： |
|  |

 |
| （5分）实验思考8-1：HTTP请求报文有哪些字段，主要作用是什么？ |
| 从这里开始填写内容，填写时删除本提示信息。 |
| （5分）实验思考8-2：HTTP请求响应有哪些字段，主要作用是什么？ |
| 这里开始填写内容，填写时删除本提示信息。 |
| （5分）实验思考8-3：通过简单流程图对比HTTP与HTTPs通信过程？  |
| 这里开始填写内容，填写时删除本提示信息。 |
| （5分）实验思考8-4：Fiddler Everywhere软件的工作原理是什么？主要应用场景有哪些？ |
| 这里开始填写内容，填写时删除本提示信息。 |