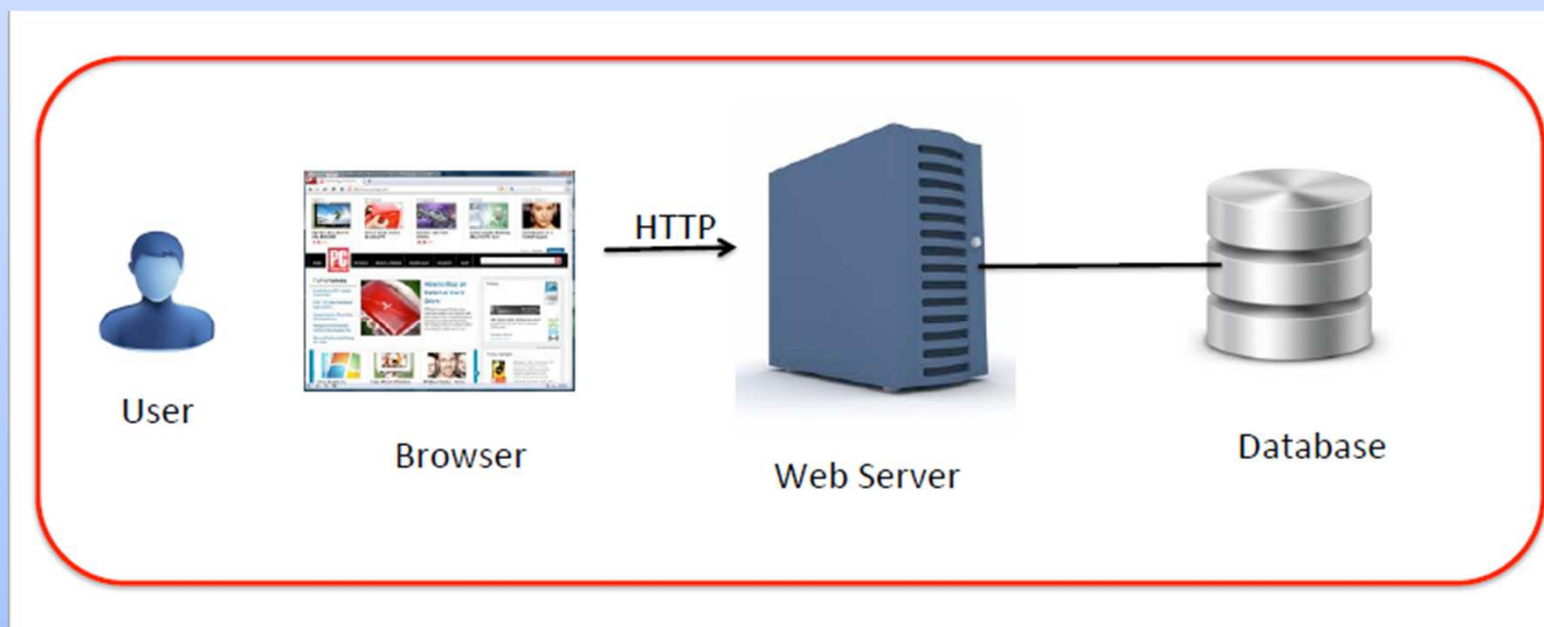


Web Application Pentesting

HTTP(HyperTextTransport Protocol) протокол

- Клиент-Серверная архитектура
- Request-Response модель обслуживания ресурсов
- Идентификация ресурсов по URI\URL
- Версия 1.0/1.1(В версии 1.1 можно использовать множественные подключения)



NetCat,Curl,Browser

```
[~^D*rk_N@de^~] [Mr.Bert0ni|CorpOfHack TeaM] [ ~ ]  
=> curl -Iv www.securitytube.net  
* Rebuilt URL to: www.securitytube.net/  
* Trying 64.233.163.121...  
* Connected to www.securitytube.net (64.233.163.121) port 80 (#0)  
> HEAD / HTTP/1.1  
> Host: www.securitytube.net  
> User-Agent: curl/7.50.1  
> Accept: */*  
>  
< HTTP/1.1 405 Method Not Allowed  
HTTP/1.1 405 Method Not Allowed  
< Allow: GET  
Allow: GET  
< Content-Type: text/html; charset=UTF-8  
Content-Type: text/html; charset=UTF-8  
< X-Cloud-Trace-Context: f7d64f331f06c10b9e0fb3b42108c049;o=1  
X-Cloud-Trace-Context: f7d64f331f06c10b9e0fb3b42108c049;o=1  
< Content-Length: 188  
Content-Length: 188  
< Date: Sun, 18 Dec 2016 17:35:53 GMT  
Date: Sun, 18 Dec 2016 17:35:53 GMT  
< Server: Google Frontend  
Server: Google Frontend  
<  
* Connection #0 to host www.securitytube.net left intact
```

Wireshark Lab

The image shows the Wireshark network traffic capture interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and packet analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list table has columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 8 is selected, showing an HTTP GET request. The bottom pane displays the details of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The raw packet data is shown at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
5	0.011970962	192.168.137.92	64.233.162.121	TCP	74	60504→80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=225181 TSecr=0
6	0.051682194	64.233.162.121	192.168.137.92	TCP	74	80→60504 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=3925
7	0.051730893	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=225191 TSecr=392548298
8	0.051947149	192.168.137.92	64.233.162.121	HTTP	150	GET / HTTP/1.1
9	0.091535849	64.233.162.121	192.168.137.92	TCP	66	80→60504 [ACK] Seq=1 Ack=85 Win=42496 Len=0 TSval=392548338 TSecr=225191
10	0.528438821	64.233.162.121	192.168.137.92	TCP	3854	[TCP segment of a reassembled PDU]
11	0.528524013	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=85 Ack=3789 Win=36864 Len=0 TSval=225310 TSecr=392548774
12	0.528581413	64.233.162.121	192.168.137.92	TCP	4162	[TCP segment of a reassembled PDU]
13	0.528589299	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=85 Ack=7885 Win=45056 Len=0 TSval=225310 TSecr=392548774
14	0.528650882	64.233.162.121	192.168.137.92	TCP	5738	[TCP segment of a reassembled PDU]
15	0.528659988	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=85 Ack=13557 Win=56320 Len=0 TSval=225311 TSecr=392548774
16	0.568052955	64.233.162.121	192.168.137.92	TCP	5738	[TCP segment of a reassembled PDU]
17	0.568089578	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=85 Ack=19229 Win=67712 Len=0 TSval=225320 TSecr=392548814
18	0.568180837	64.233.162.121	192.168.137.92	TCP	11410	[TCP segment of a reassembled PDU]
19	0.568191591	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=85 Ack=30573 Win=90368 Len=0 TSval=225320 TSecr=392548814
20	0.570034774	64.233.162.121	192.168.137.92	HTTP	1633	HTTP/1.1 200 OK (text/html)
21	0.570067497	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=85 Ack=32140 Win=93568 Len=0 TSval=225321 TSecr=392548814
22	0.570325497	192.168.137.92	64.233.162.121	TCP	66	60504→80 [FIN, ACK] Seq=85 Ack=32140 Win=93568 Len=0 TSval=225321 TSecr=3925488
23	0.609713851	64.233.162.121	192.168.137.92	TCP	66	80→60504 [FIN, ACK] Seq=32140 Ack=86 Win=42496 Len=0 TSval=392548855 TSecr=2253
24	0.609754988	192.168.137.92	64.233.162.121	TCP	66	60504→80 [ACK] Seq=86 Ack=32141 Win=93568 Len=0 TSval=225331 TSecr=392548855

Frame 8: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Ethernet II, Src: CadmusCo_de:11:8e (08:00:27:de:11:8e), Dst: 52:f8:da:35:11:6d (52:f8:da:35:11:6d)
Internet Protocol Version 4, Src: 192.168.137.92, Dst: 64.233.162.121
Transmission Control Protocol, Src Port: 60504, Dst Port: 80, Seq: 1, Ack: 1, Len: 84
Hypertext Transfer Protocol
GET / HTTP/1.1\r\n
[Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Host: www.cadmusco.de

0030 00 e5 2d e2 00 00 01 01 08 0a 00 03 6f a7 17 650..e