

Web Application Pentesting



Vivek Ramachandran

SWSE, SMFE, SPSE, SISE, SLAE, SGDE Course Instructor

Certifications: <http://www.securitytube-training.com>

Pentester Academy: <http://www.PentesterAcademy.com>

HTTP Statelessness and Cookies

HTTP is Stateless

- Every request is treated independently
- Server does not retain state for clients
- What does this mean?
 - Every request needs to be separately authenticated
 - Every request **MUST** carry auth information

Cookies

- Allows server to store and retrieve data from the client
- Typically stored in a file on the client side
- Text only; No executable code
- Cannot exceed 4K in size
- Allows for retaining state with the Client's help
 - Session Management
 - User Preferences

How does a Cookie look?

Search: yahoo

The following cookies match your search:

Site	Cookie Name
<input type="checkbox"/> analytics.yahoo.com	itsc
<input type="checkbox"/> in.yahoo.com	fpc
<input type="checkbox"/> in.yahoo.com	fpps
<input checked="" type="checkbox"/> in.yahoo.com	fpt
<input type="checkbox"/> in.yahoo.com	fpc_s
<input type="checkbox"/> in.yahoo.com	FPCK2
<input type="checkbox"/> in.yahoo.com	ywadp10002057186656
<input type="checkbox"/> in.yahoo.com	fpc10002057186656
<input type="checkbox"/> yahoo.com	B
<input type="checkbox"/> yahoo.com	fpc
<input type="checkbox"/> yahoo.com	MSC

Name: fpt
Content: d=52SYMBvXedq_2g.V3UFmkOXZ1soz4MCFd2Rfb1ypSWkr0Rm3IFO4sCaAUxvlqzf95TwTWWAlIpJsndLN4j7CRkEyTRsY7getUVy9gm6k5E
Domain: .in.yahoo.com
Path: /
Send For: Any type of connection
Expires: At end of session

How is a Cookie set by the Server?

The screenshot shows a Wireshark interface with a filter set to 'http.set_cookie'. The packet list pane shows four packets, with packet 161 selected. The packet details pane shows the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol section is expanded to show the response body, which includes several Set-Cookie headers.

No.	Time	Source	Destination	Protocol	Length	Info
35	15.472575000	106.10.139.246	192.168.1.:HTTP	HTTP/1.1	1329	Found (text/html)
37	15.472647000	106.10.139.246	192.168.1.:HTTP	HTTP/1.1	1329	[TCP Retransmission] Found (text/html)
161	16.650518000	106.10.139.246	192.168.1.:HTTP	HTTP/1.1	2207	200 OK (text/html)
609	17.647991000	106.10.198.32	192.168.1.:HTTP	HTTP/1.1	71	Found

Frame 161: 2207 bytes on wire (17656 bits), 2207 bytes captured (17656 bits) on interface 0

Ethernet II, Src: Binatone_0a:92:8c (0c:d2:b5:0a:92:8c), Dst: CadmusCo_4c:67:c0 (08:00:27:4c:67:c0)

Internet Protocol Version 4, Src: 106.10.139.246 (106.10.139.246), Dst: 192.168.1.8 (192.168.1.8)

Transmission Control Protocol, Src Port: http (80), Dst Port: 41838 (41838), Seq: 62461, Ack: 394, Len: 2141

[43 Reassembled TCP Segments (64601 bytes): #44(2776), #46(1388), #48(1388), #50(1388), #52(1388), #54(1388), #56(1388), #58(1388), #60(1388), #62(1388)]

Hypertext Transfer Protocol

HTTP/1.1 200 OK\r\n

Date: Tue, 24 Sep 2013 02:45:23 GMT\r\n

P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND

Cache-Control: private\r\n

X-Frame-Options: SAMEORIGIN\r\n

Set-Cookie: IU=deleted; expires=Mon, 24-Sep-2012 02:45:22 GMT; path=/; domain=.yahoo.com\r\n

Set-Cookie: PH=deleted; expires=Mon, 24-Sep-2012 02:45:22 GMT; path=/; domain=.yahoo.com\r\n

Set-Cookie: MSC=t=1379990723X; expires=Wed, 24-Sep-2014 02:45:23 GMT; path=/; domain=.yahoo.com\r\n

[truncated] Set-Cookie: fpc=d=ZUutso2501d422KuX3QRTuLKRWGrXrXdoQG2FCxXENC2EYZvHEM8gNibkXjKi1gK.RZD446fpmPdyVcndjdN8GLFQxVwaFstVmt_ovyTlLzR7lxUGjhIXHgW

[truncated] Set-Cookie: fpc=d=AaQmGle501f9Airb_zUJAuCHtpBfWVAT3.rKEjwDaSxjH_xbG0FAGiaJl7SbH_0NqYzGf2IxsN6YBUAxKNKAON242wljynTkWynwltjzmzI_JU9APhcPWJMhm

Set-Cookie: fpps_page=%7B%22wsid%22%3A%221445690%22%7D; expires=Wed, 24-Sep-2014 02:45:23 GMT; path=/; domain=in.yahoo.com\r\n

[truncated] Set-Cookie: fpt=d=52SYMBvXedq_2g.V3UFmkOXZ1soz4MCFd2Rfb1ypSwkr0Rm3IF04sCaAUxvIqzf95TWTWWAlIpJsndLN4j7CRkEyTRsY7getUVy9gm6k5Bb7m8SwaIgdqJLL

[truncated] Set-Cookie: fpc_s=d=.ext2ky501e_tK53hd9osRtVkm4U8E5sAkkHI.lsJ2.3KvMPTIRZXjBx2yR3TsZ9odb1WTcR9BVgqPV0volR1zyFkSI.R.66HI0o.adkrrktjc1F1XPRTF

Vary: Accept-Encoding\r\n

Content-Type: text/html;charset=utf-8\r\n

Content-Encoding: gzip\r\n

Age: 0\r\n

Transfer-Encoding: chunked\r\n

Connection: keep-alive\r\n

How is a Cookie sent by the Client?

The image shows a Wireshark network traffic capture. The filter is set to 'http.cookie'. The packet list shows several HTTP GET requests. The selected packet (No. 42) is a GET request to 'http://in.yahoo.com/?p=us'. The packet details pane shows the following information:

```
Frame 42: 459 bytes on wire (3672 bits), 459 bytes captured (3672 bits) on interface 0
Ethernet II, Src: CadmusCo_4c:67:c0 (08:00:27:4c:67:c0), Dst: Binatone_0a:92:8c (0c:d2:b5:0a:92:8c)
Internet Protocol Version 4, Src: 192.168.1.8 (192.168.1.8), Dst: 106.10.139.246 (106.10.139.246)
Transmission Control Protocol, Src Port: 41838 (41838), Dst Port: http (80), Seq: 1, Ack: 1, Len: 393
Hypertext Transfer Protocol
  GET /?p=us HTTP/1.1\r\n
  Host: in.yahoo.com\r\n
  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:22.0) Gecko/20100101 Firefox/22.0 Iceweasel/22.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  Cookie: RT=s=1379990721241&u=&r=http%3A//in.yahoo.com/%3Fp%3Dus; B=bgsqtlh941v62&b=3&s=8a\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://in.yahoo.com/?p=us]
```

What Information is allowed in it?

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

[http://msdn.microsoft.com/en-us/library/windows/desktop/aa384321\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384321(v=vs.85).aspx)

Client

```
Cookie: <name>=<value> [;<name>=<value>]...
```


Cookie: Name=Value Pairs

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

- E.g. sessionID=ahj23hkhe32fd23j232ll2323ljk
- Multiple separated by ;
 - E.g. Name=vivek; Age=12; Country=India

Cookie: expires

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

- Session Cookie if “expires” not mentioned
- Format:
 - DAY, DD-MMM-YYYY HH:MM:SS GMT
 - Mon, 22-Nov-2013 22:45:00 GMT
- Max-Age parameter in newer RFC 6265
 - Interval in seconds after receiving the cookie

Cookie: domain

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

- Domain for which it is valid
- E.g.
 - docs.securitytube.net
 - .images.securitytube.net

Cookie: path

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

- Path for which it is valid
- E.g.
 - Sid1=asd; Path=/;
 - Sid2=xyz; Path=/blog;

Cookie: secure

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

- Only sent over HTTPS

Cookie: httponly

Server

```
Set-Cookie: <name>=<value>[; <name>=<value>]...  
[; expires=<date>][; domain=<domain_name>]  
[; path=<some_path>][; secure][; httponly]
```

- Cannot be accessed by Client side scripts directly
- Cannot be scripted using Javascript
- XSS mitigation mechanism

Pentester Academy

PentesterAcademy

a SecurityTube.net initiative



TOPICS

PRICING

WHY SUBSCRIBE

MEMBER ACCESS



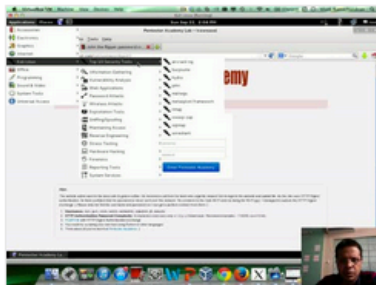
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

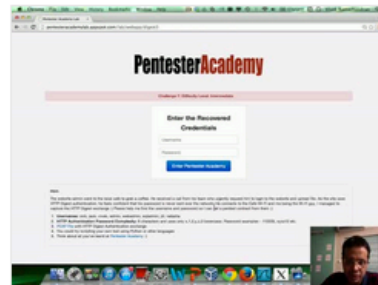
Start Learning Today!

Latest Videos

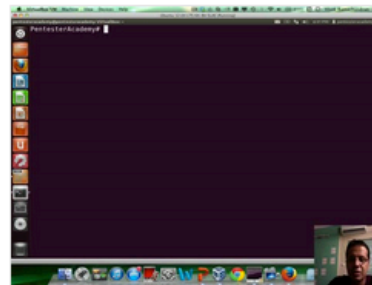
New content added weekly!



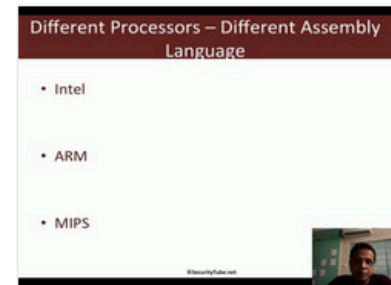
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



Challenge 7: Cracking Digest Authentication in WAP Challenges



Module 1: GDB Test Solution in x86_64 Assembly Language and Shellcoding on Linux



Module 1: CPU Information in x86_64 Assembly Language and Shellcoding on Linux

Twitter and Facebook



Security Tube

@SecurityTube

Comprehensive, Hands-on, Practical and Affordable infosec training. Join students from 73+ Countries:

PentesterAcademy.com Securitytube-Training.com

CyberSpace · securitytube.net

19,964
TWEETS

8,576
FOLLOWING

37,554
FOLLOWERS



Edit profile



SecurityTube

✓ Like

You like this.

You and 36,320 others like SecurityTube.