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

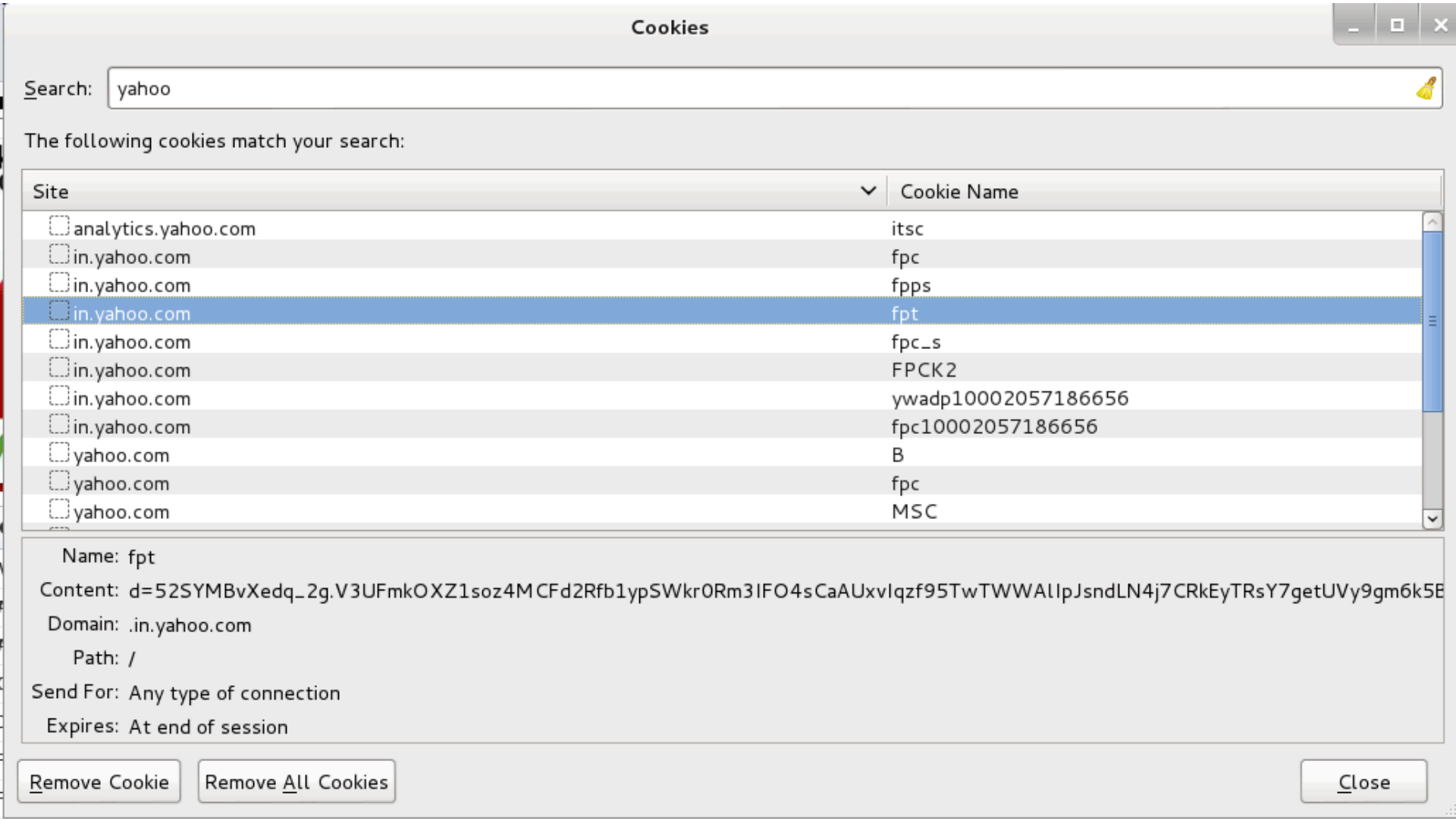
HTTP is Stateless

- 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

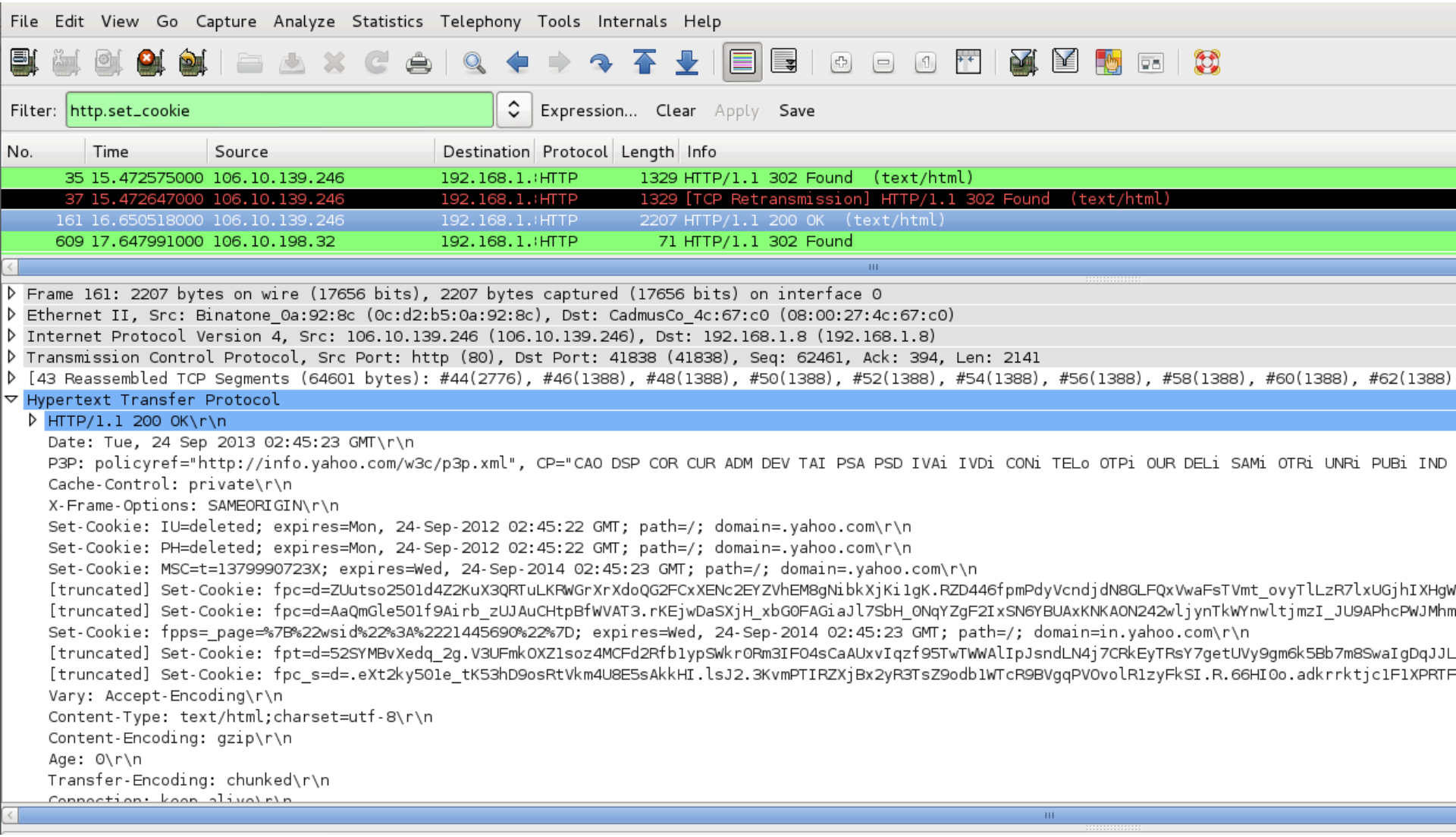
Cookies

- 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

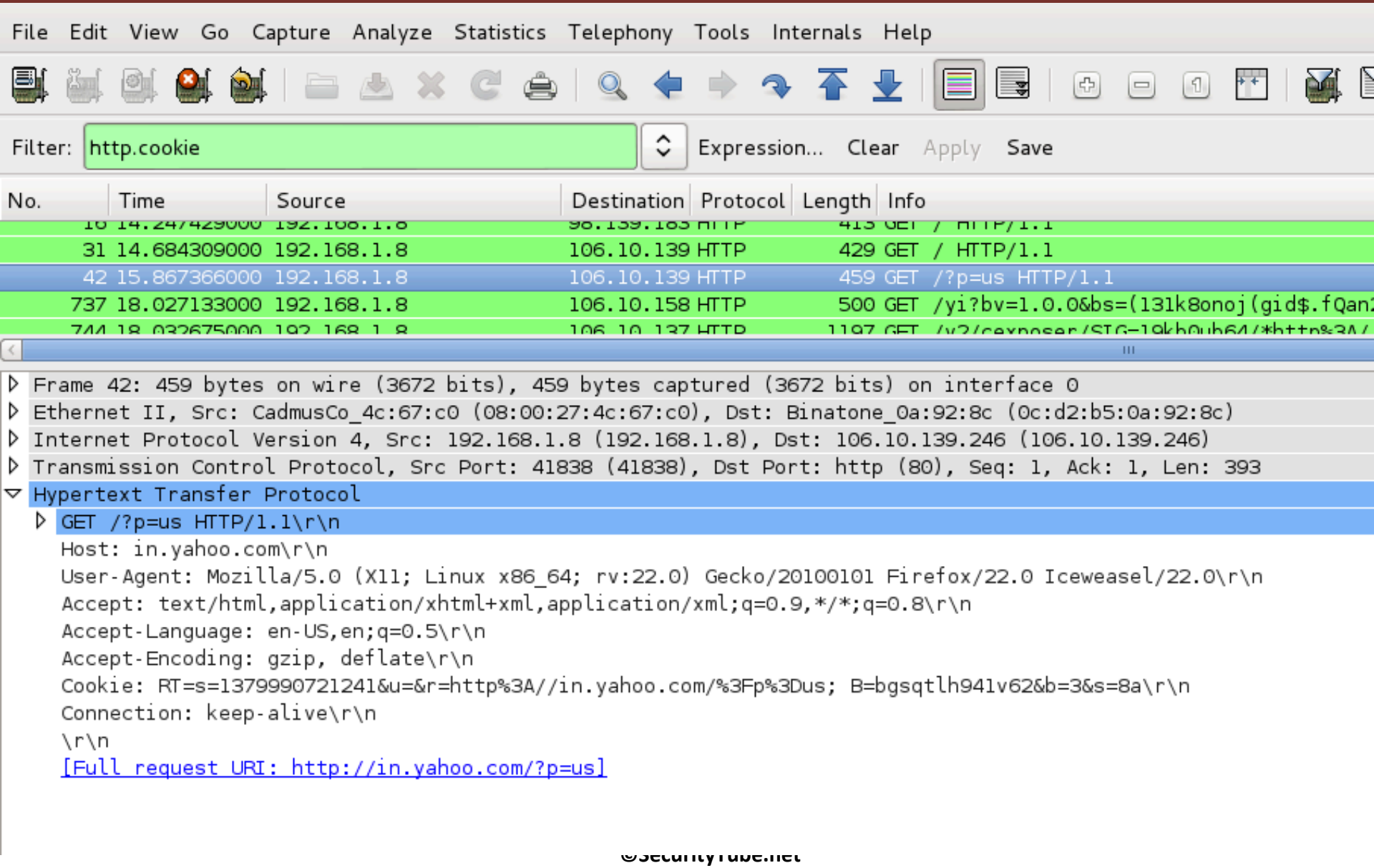
How does a Cookie look?



How is a Cookie set by the Server?



How is a Cookie sent by the Client?



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

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

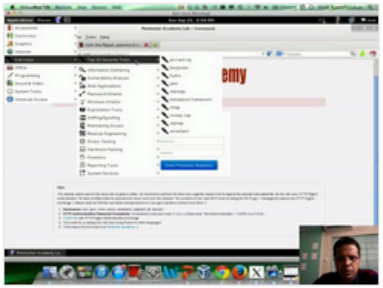
Revolutionizing Infosec Training

Highly Technical, Hands-on, Affordable

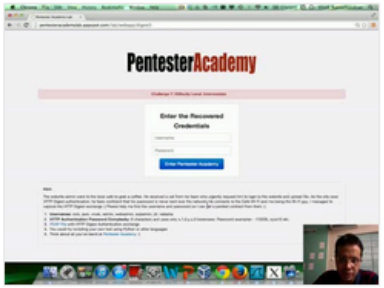
Start Learning Today!

Latest Videos

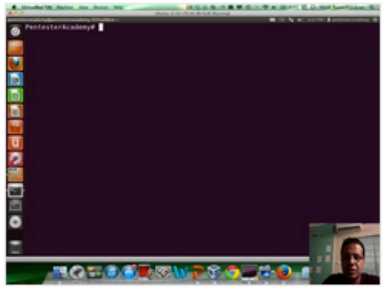
New content added weekly!



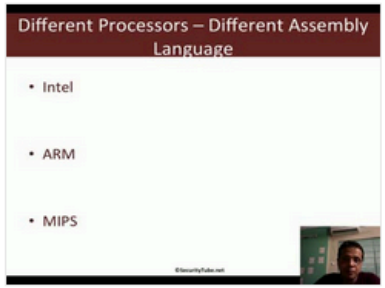
Challenge 7: Cracking Digest Authentication Solution in WAP Challenges



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