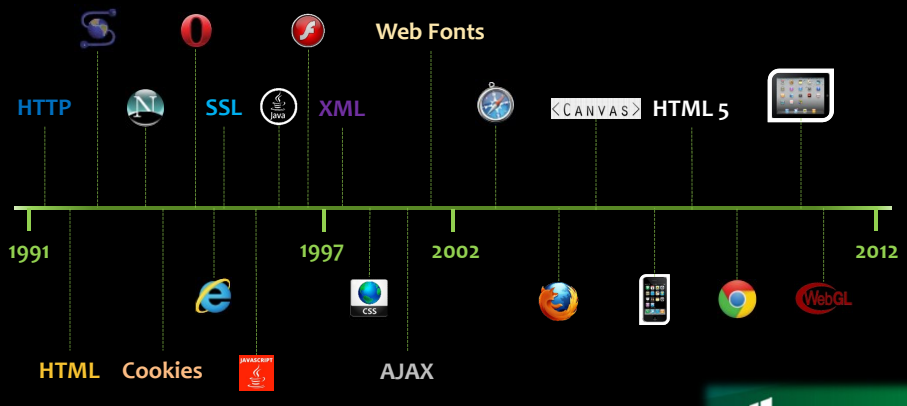
Ethical Web Hacking – Summary Slides

Mostafa Biglari-Abhari

Unitec Institute of Technology
TE WHARE WĀNANGA O WAIRAKA

Evolution of Web Technologies

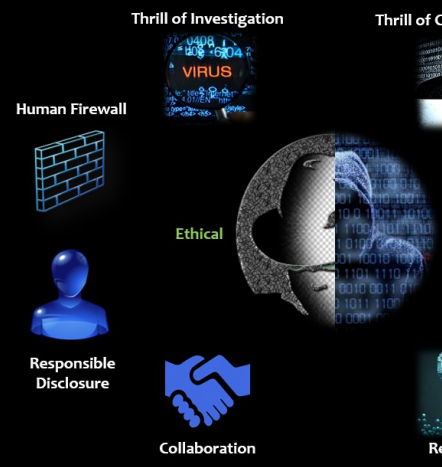


Unitec Institute of Technology
TE WHARE WĀNANGA O WAIRAKA

Key Trends

- Always online, connected devices
- Rapid growth in E-Commerce web sites
- Boom in online advertising
- More complex and interactive web applications

Ethical vs Unethical Hackers



Case Study

Scenario One

Parameter Tampering

Target: Web Application

Scenario Two

Social Engineering

Target: Single User

Scenario Three

Injection Attacks

Target: Web Application

Unitec Institute of Technology
TE WHARE WĀNANGA O WAIRAKA

Introduction to HTTP Request and Response Headers

Send HTTP Request

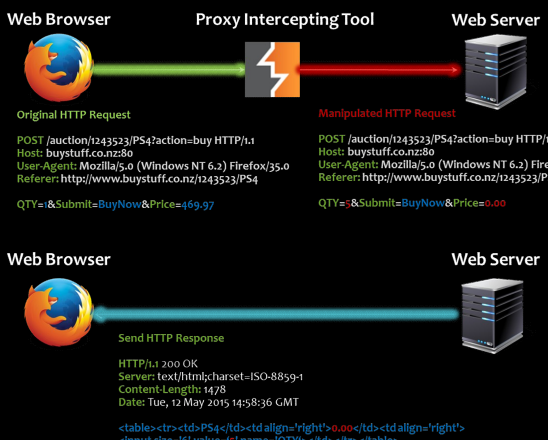
```
POST /auction/1243523/PS4?action=buy HTTP/1.1
Host: buystuff.co.nz:80
User-Agent: Mozilla/5.0 (Windows NT 6.2) Firefox/35.0
Referer: http://www.buystuff.co.nz/1243523/PS4
Content Length: 36

QTY=1&Submit=BuyNow&Price=469.97
```

Send HTTP Response

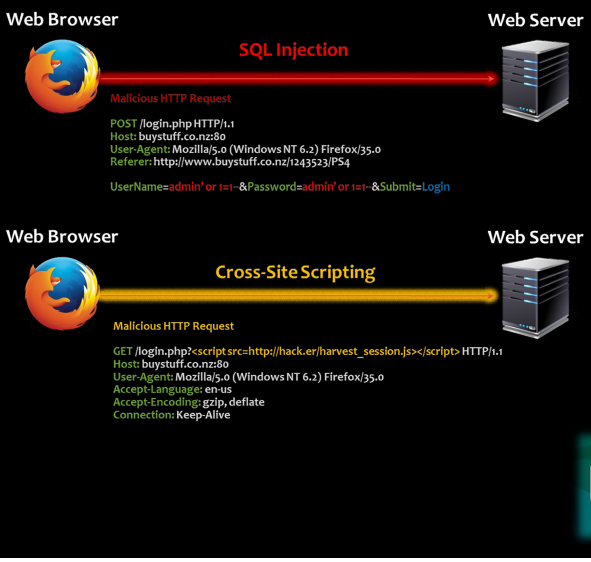
```
HTTP/1.1 200 OK
Server: text/html;charset=ISO-8859-1
Content-Length: 1479
Date: Tue, 12 May 2015 14:58:36 GMT

<tr><td>PS4</td><td align='right'>469.97</td><td align='right'>
<input size='6' value='1' name='QTY'></td></tr></table>
```

Unitec Institute of Technology
TE WHARE WĀNANGA O WAIRAKA

Parameter Tampering with Burp Proxy



SQL Injection and Cross-Site Scripting



Things to ponder…

- Can we really trust the information that our servers receive from various web clients?
- We must always validate incoming requests on our Web Servers to see if they are legitimate before issuing a response
  - E.g. Does the TV that User A wants to buy really cost $0? Our database says $1469.97 so reject the request
- Security by obscurity creates a false sense of security:
  - I don't want standard users the ability to do admin stuff so I will just hide the buttons **– FAIL**
  - The admin password to the database is too hard to remember so I will just hide it in the source code **– BIGGER FAIL**

Useful Links

Ethical Web Hacking

- Burp Suite Tool – portswigger.net/burp/
- WebGoat Framework – webgoat.github.io

Packet Capture Analysis

- **Wireshark Tools –** www.wireshark.org
- **Wireshark Sample Packet Capture Files –** wiki.wireshark.org/SampleCaptures

Log File Analysis – rtcamp.com/tutorials/nginx/log-parsing