
WEB H4X0R 101
KONFIGURASI PLATFORM
DARI NOOBS SAMPAI JADI MASTA!
HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

PENAFIAN

Saya (Hussein bin Mohamed / gh1mau) tidak bertanggungjawap dengan sebarang penyalahgunaan maklumat dari tutorial ini.

Segala teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini adalah bertujuan untuk pembelajaran sahaja.

Tindakan menguji cuba menggunakan teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini terhadap asset / sistem / komputer bukan milik anda atau tanpa mendapat kebenaran bertulis adalah salah di sisi undang-undang.

Gunakan maklumat dan teknik yang dipaparkan untuk meningkatkan kemahiran anda sama ada untuk tujuan akademik atau kemajuan kerjaya.

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

OBJEKTIF MODUL

1	Menyediakan platform bagi tujuan Web Application Penetration Testing.
2	Melaksanakan konfigurasi asas terhadap platform berkenaan untuk memastikan proses Web Application Penetration Testing berjalan dengan lancar.
3	Mempelajari command dan teknik yang berkaitan untuk tujuan pengoperasian platform berkenaan.

SILIBUS MODUL

1	Pengenalan Windows Subsystem for Linux (wsl) 1. Apa itu wsl dan wsl2? 2. Perbezaan wsl dengan wsl2 3. Perbezaan penggunaan wsl dengan Virtual Machine biasa 4. Keperluan asas wsl2
2	Pemasangan / konfigurasi Platform bagi tujuan Web Application Penetration Testing 1. Pemasangan dan Konfigurasi Windows Terminal 2. Pemasangan dan Konfigurasi wsl2 di dalam Windows 10 3. Pemasangan dan konfigurasi kali-linux di dalam wsl2
3	Command asas berkaitan kali-linux wsl2 1. Apa itu Win-KeX? 2. Command asas wsl 3. Menyalin dan mengakses fail dari host ke wsl (vice versa)

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Apa itu wsl dan wsl2?	
1	Windows Subsystem for Linux (WSL) ialah features baharu pada Windows 10, yang membolehkan pengguna menjalankan perintah Linux secara natif dalam sistem operasi Windows, bersekali desktop Windows seperti melancarkan aplikasi biasa, tanpa perlu menggunakan Virtual Machine biasa ataupun dual-boot.
2	WSL direka oleh Microsoft dengan kerjasama Canonical, pencipta Ubuntu. Bersama-sama, mereka membuat kernel compatability layer berdasarkan Ubuntu. Lapisan keserasian ini membolehkan program Linux dijalankan dalam versi Windows 10 shell Bash. Ini bermakna kita boleh menjalankan tools dan utilities linux di dalam Windows 10 melalui fungsi wsl ini.
3	WSL2 pula ialah versi baharu yang membolehkan binary ELF64 Linux dijalankan pada windows. Tujuan utamanya adalah untuk meningkatkan prestasi sistem fail, serta menambah compatability system
4	Arkitektur tersebut direka bentuk semula dalam WSL2, untuk menambah performance file system dan menambah full system call compatibility(The system call is the fundamental interface between an application and the Linux kernel)

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Perbezaan wsl dengan wsl2

Comparing features

Feature	WSL 1	WSL 2
Integration between Windows and Linux	✅	✅
Fast boot times	✅	✅
Small resource foot print compared to traditional Virtual Machines	✅	✅
Runs with current versions of VMware and VirtualBox	✅	✅
Managed VM	❌	✅
Full Linux Kernel	❌	✅
Full system call compatibility	❌	✅
Performance across OS file systems	✅	❌

As you can tell from the comparison table above, the WSL 2 architecture outperforms WSL 1 in several ways, with the exception of performance across OS file systems.

Rujukan:

https://docs.microsoft.com/en-us/windows/wsl/compare-versions

https://thecodeblogger.com/2020/08/22/understanding-differences-between-wsl-1-and-wsl-2/

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Perbezaan penggunaan wsl dengan Virtual Machine biasa	
1	WSL2 menjalankan kernel Linux dan OS di dalam OS windows untuk menterjemahkan Linux system call ke NT calls. Ini membolehkan anda untuk menjalankan distro Linux sebagai desktop. Ini meningkatkan prestasi sistem dan memberikan prestasi native.
2	Virtual Machine menggunakan virtual extensions yang dikendalikan oleh hypervisor yang merupakan manager yang menggunakan separate privileged memory untuk membolehkan kernel Linux berkomunikasi dengan perkakasan anda. Prestasi VM didasarkan pada jenis perkakasan yang digunakan dan ia menambah banyak ciri seperti snapshots, portable virtual hard disks, dan virtual networking.

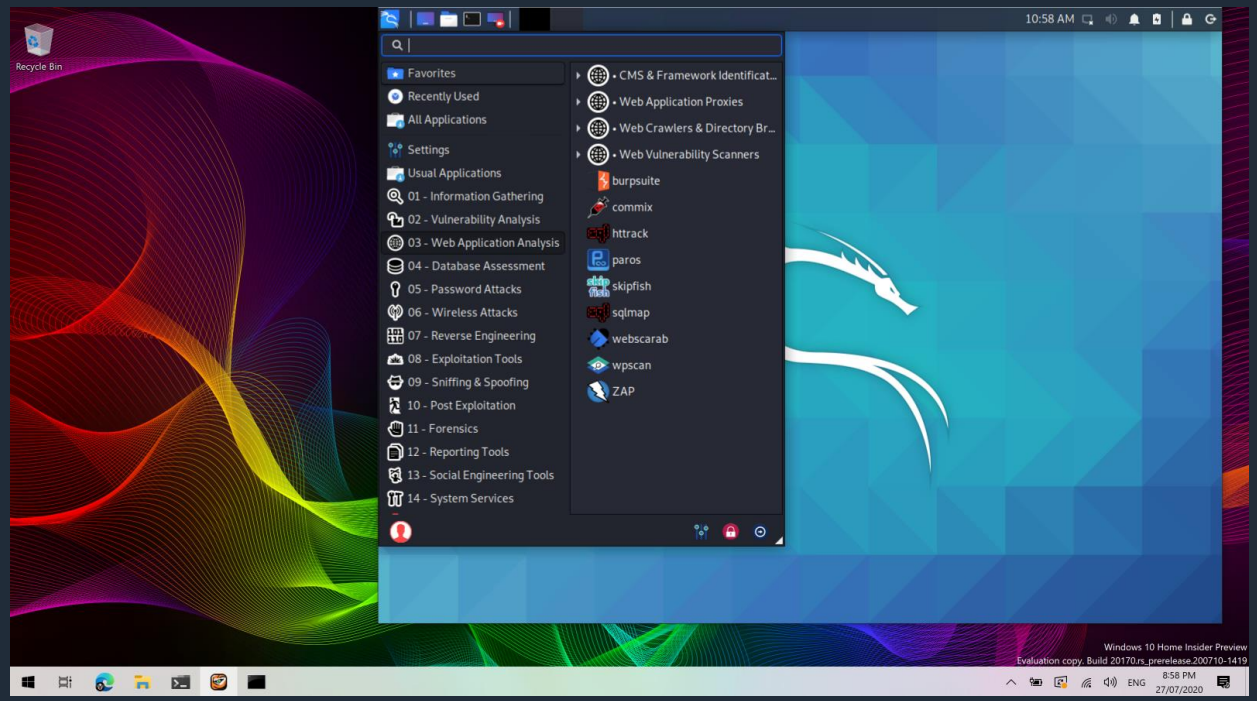
HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Keperluan asas wsl2	
1	For x64 systems: Version 1903 or higher, with Build 18362 or higher.
2	For ARM64 systems: Version 2004 or higher, with Build 19041 or higher.
3	Builds lower than 18362 do not support WSL 2. Use the Windows Update Assistant to update your version of Windows.
4	Gunakan command winver untuk mengetahui Versi Windows 10 anda.

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

APA ITU WIN-KEX?

Win-KeX	
1	Win-KeX dalam Window Mode yang menjalankan sesi desktop Kali Linux di tetingkap yang berasingan(separate windows)
2	Win-KeX menggunakan TigerVNC untuk komponen client dan pelayannya.
3	Rujukan: https://www.kali.org/docs/wsl/win-kex-win/



HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM


WEB H4X0R 101
TARGET SETUP
DARI NOOBS SAMPAI JADI MASTA!
HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

PENAFIAN

Saya (Hussein bin Mohamed / gh1mau) tidak bertanggungjawap dengan sebarang penyalahgunaan maklumat dari tutorial ini.

Segala teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini adalah bertujuan untuk pembelajaran sahaja.

Tindakan menguji cuba menggunakan teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini terhadap asset / sistem / komputer bukan milik anda atau tanpa mendapat kebenaran bertulis adalah salah di sisi undang-undang.

Gunakan maklumat dan teknik yang dipaparkan untuk meningkatkan kemahiran anda sama ada untuk tujuan akademik atau kemajuan kerjaya.

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

OBJEKTIF MODUL

1	Menyediakan target ujian bagi tujuan pelaksanaan Web Application Penetration Testing.
2	Memahami perihal networking dan connectivity target.
3	Membuat ujian ringkas bagi memastikan target berfungsi untuk tujuan Web Application Penetration Testing.

SILIBUS MODUL

1	metasploitable2 sebagai target ujian 1. Pengenalan metasploitable2 2. Pemasangan metasploitable2 ke dalam Virtual Machine (virtualbox) 3. Konfigurasi asas
2	Ujian connectivity antara host(platform pen-test) dengan target 1. ping test 2. Web application access test 3. Simple port scan test
3	Vulnerability Assessment Fasa 1 (Port Scanning) 1. Port Scanning 2. Port Scan target menggunakan nmap terhadap target 3. Pengenalan dan penggunaan nmap vulnscan 4. Pengenalan dan penggunaan masscan 5. Pengenalan dan pengunaan nmap dashboard

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

PENGENALAN METASPLOITABLE2

Apa itu metasploitable2 ?	
1	metasploitable2 adalah sebuah vulnerable ubuntu linux machine yang dapat digunakan untuk melakukan latihan keselamatan, menguji tools, dan mempraktikkan teknik pengujian penembusan(Penetration Testing)
2	VM ini mempunyai beberapa kelemahan yang disengajakan untuk tujuan pembelajaran dan pengujian. Senarai kelemahan yang dimaksudkan boleh dirujuk di: https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

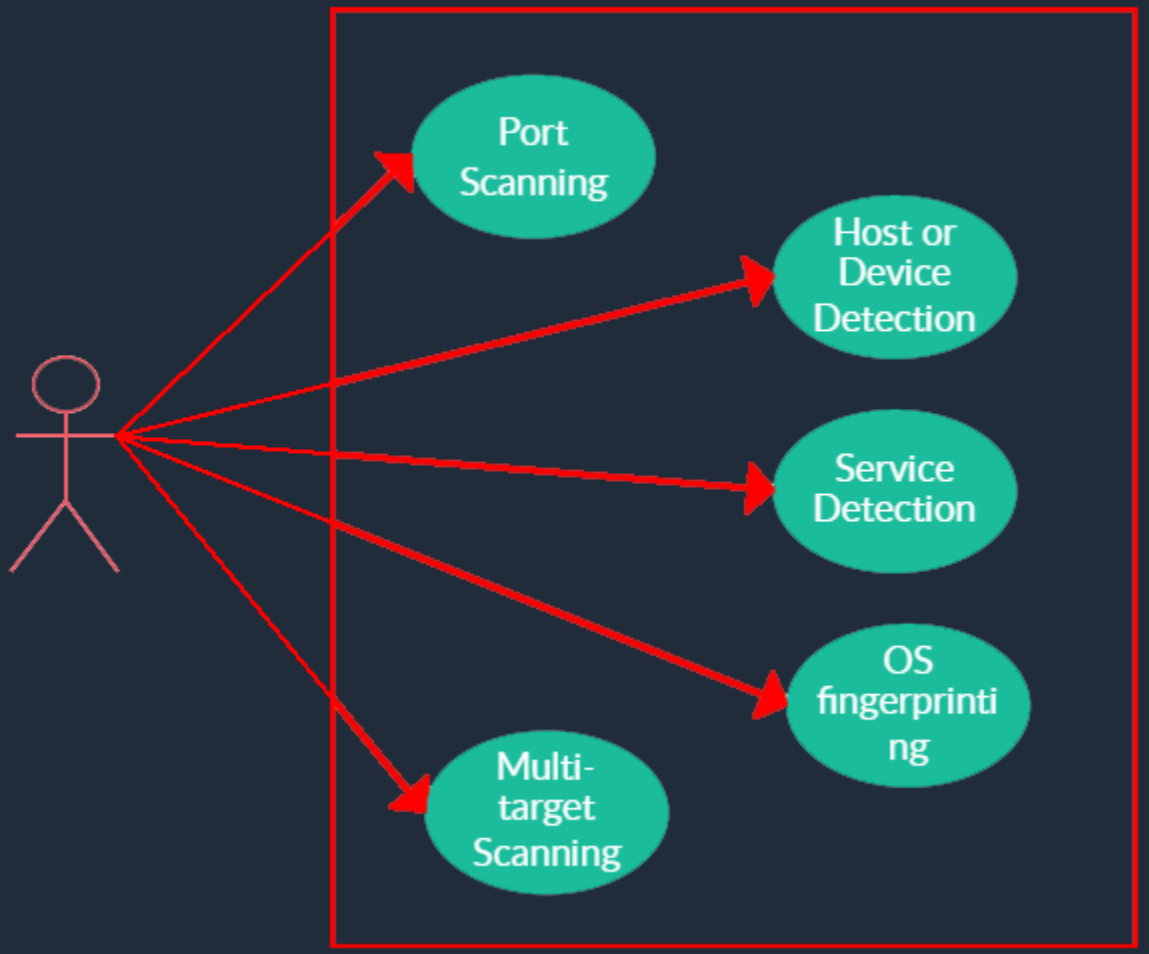
PENGENALAN PORT SCANNING

Apa itu Port Scanning ?	
1	Port Scanning adalah aktiviti yang dilakukan untuk memeriksa status port TCP dan UDP pada sebuah ip / mesin. Banyak aplikasi yang menawarkan fungsi untuk melakukan pemeriksaan port pada sebuah mesin, seperti netcat, nmap, dan sebagainya
2	Tujuan dari aktiviti Port Scanning ini adalah mengenalpasti kemungkinan-kemungkinan kelemahan dari suatu sistem yang terpasang pada suatu komputer atau perlengkapan dan peralatannya melalui port yang terbuka.
3	Pada dasarnya, port scanning ialah untuk mengenalpasti port-port yang terbuka, dan mengenali OS target.

PENGENALAN NMAP

Apa itu nmap?	
1	Nmap (Network Mapper) adalah sebuah aplikasi atau tool yang berfungsi untuk melakukan port scanning. Nmap dibuat oleh Gordon Lyon, atau lebih dikenal dengan nama Fyodor Vaskovich. Aplikasi ini digunakan untuk mengaudit jaringan yang ada. Dengan menggunakan tool ini, kita dapat melihat host yang aktif, port yang terbuka, Sistem Operasi yang digunakan, dan feature-feature scanning yang lain.
2	Rujukan : https://nmap.org/

Apa itu nmap?


Port Scanning
Host or Device Detection
Service Detection
OS fingerprinting
Multi-target Scanning

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

Hussein bin Mohamed aka ch1mau | ch1mau.rulez@gmail.com

PENAFIAN

Saya (Hussein bin Mohamed / gh1mau) tidak bertanggungjawap dengan sebarang penyalahgunaan maklumat dari tutorial ini.

Segala teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini adalah bertujuan untuk pembelajaran sahaja.

Tindakan menguji cuba menggunakan teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini terhadap asset / sistem / komputer bukan milik anda atau tanpa mendapat kebenaran bertulis adalah salah di sisi undang-undang.

Gunakan maklumat dan teknik yang dipaparkan untuk meningkatkan kemahiran anda sama ada untuk tujuan akademik atau kemajuan kerjaya.

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

OBJEKTIF MODUL

1	Memahami proses awalan dalam Web Application Penetration Testing
2	Melaksanakan pengujian secara berstruktur
3	Memahami aspek teknikal Web Application Attack terhadap sesuatu kelemahan yang khusus
4	Membuat analisa asas webserver logfile untuk mengenal pasti sesuatu serangan terhadap Aplikasi Web

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

SILIBUS MODUL

1	Web Application Mapping untuk Ujian Penembusan Aplikasi Web 1. Apa itu Web Application Mapping? 2. Panduan Asas Web Application Mapping
2	Analisa teknikal isu twiki secara asas 1. Isu kelemahan twiki 2. Kaedah exploitation pada twiki
3	HTTP Status Code 101 1. HTTP Status Code asas bagi tujuan analisa logfile secara asas

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

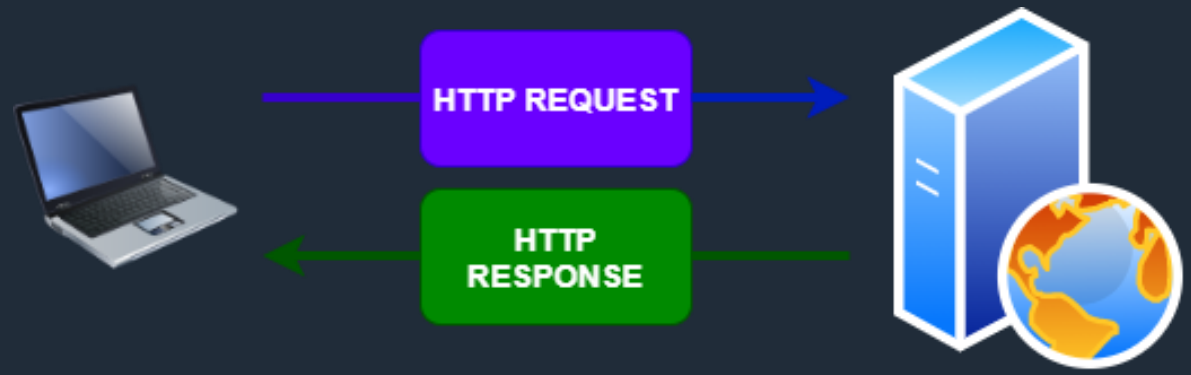
WEB APPLICATION MAPPING

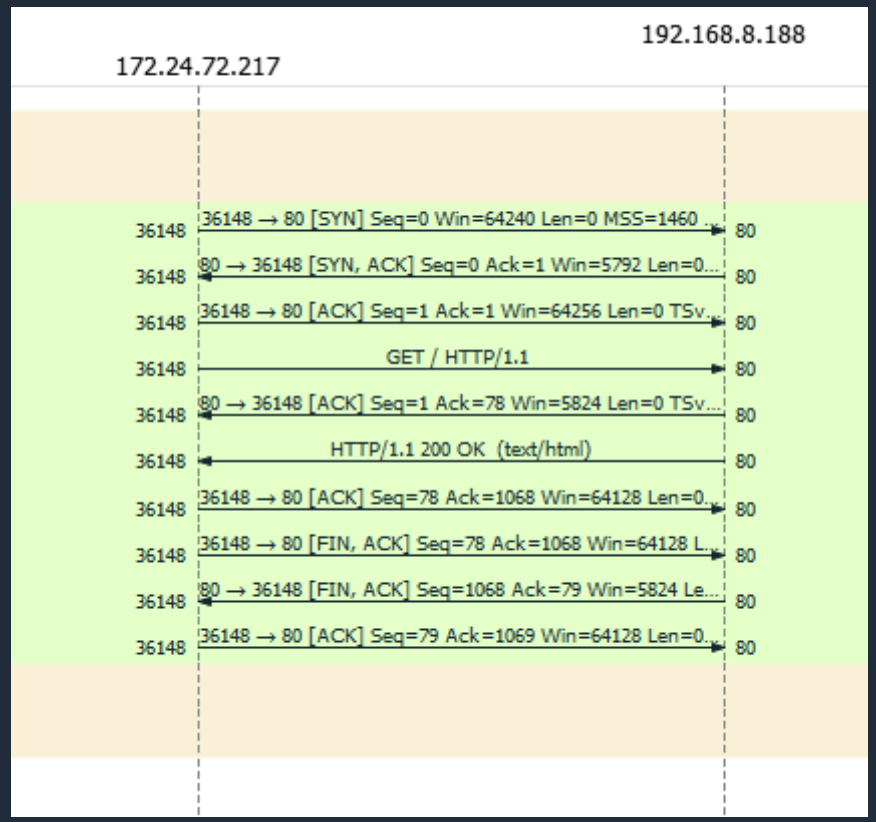
Panduan Asas Web Application Mapping?	
1	Semak imbas aplikasi secara manual (play around pada aplikasi web berkenaan)
2	Spider / crawl the Web Application
3	Directory Bruteforcing
4	Jalankan simple scanner (nikto)
5	Buat potential threat mapping (mind map tools, threat modelling tools)
6	Kenalpasti parameter kompleks, hidden parameter dan seumpamanya

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

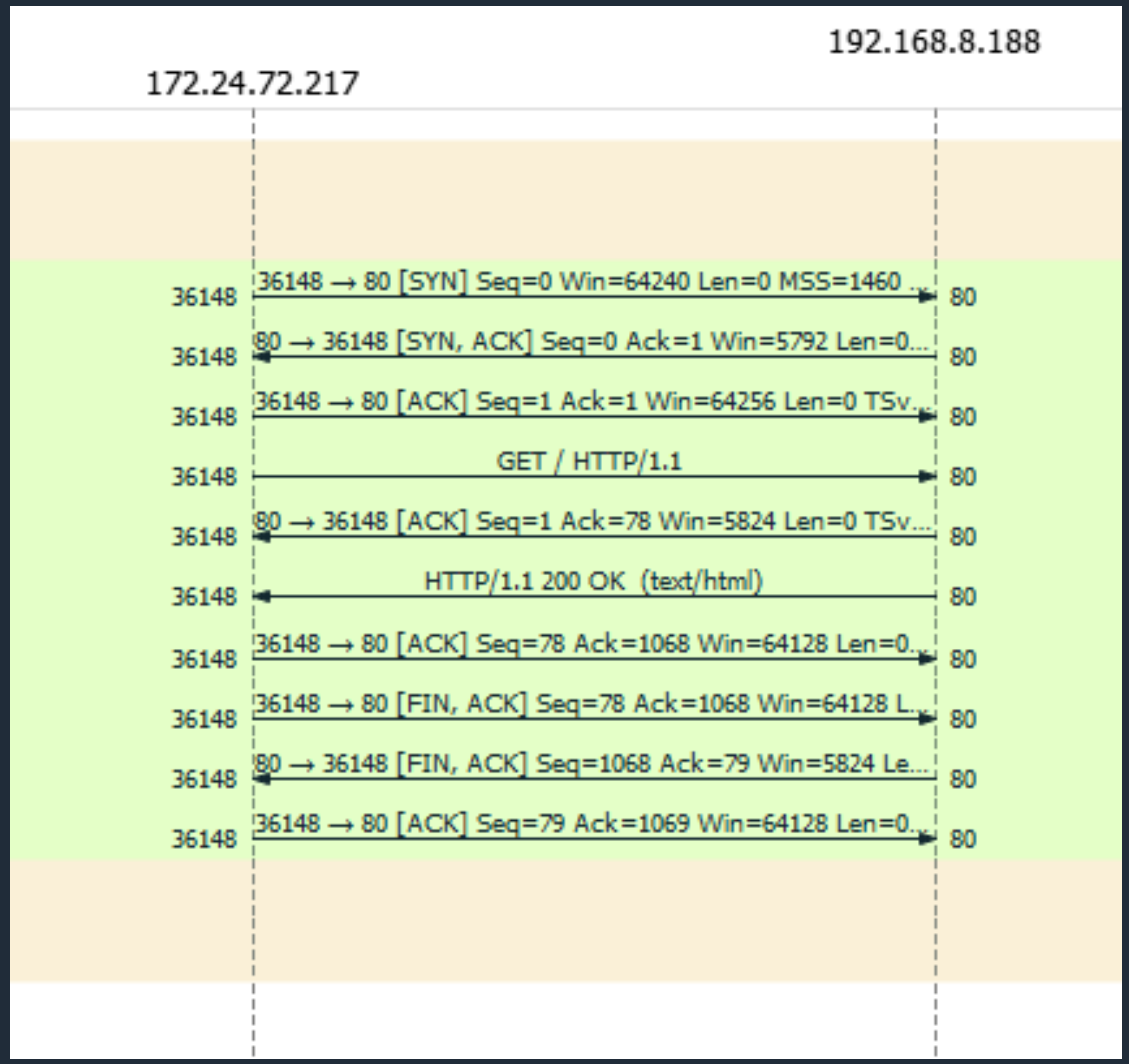
Apa itu Web Application Mapping?	
1	Langkah pertama dalam proses Web Application Penetration Testing adalah mengumpulkan dan memeriksa beberapa maklumat penting pada aplikasi web dan pelayan berkenaan untuk mendapatkan pemahaman yang lebih baik terhadap apa yang anda akan attack. Proses ini dinamakan **enumeration** atau **mapping**.
2	Mapping dimulakan dengan mengenalpasti content dan fungsi aplikasi untuk memahami apa yang dilakukan oleh aplikasi dan bagaimana tindakannya. Sebilangan besar fungsi ini mudah dikenal pasti, tetapi sebahagian daripadanya mungkin tersembunyi, adakalanya **intuisi** dan **nasib** memainkan peranan dalam perkara ini.
3	Intuisi ini dapat dipupuk berdasarkan latihan dan pengalaman secara berterusan.

Protokol HTTP	
1	HTTP adalah application protokol yang paling banyak digunakan di Internet. HTTP adalah client-server protokol yang digunakan dalam laman web dan aplikasi web untuk memindahkan data dan sebagainya.
2	Dalam HTTP, client biasanya menggunakan web browser dan connect ke web server seperti Apache, nginx dan lain-lain





HTTP PROTOCOL



HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

PENAFIAN

Saya (Hussein bin Mohamed / gh1mau) tidak bertanggungjawap dengan sebarang penyalahgunaan maklumat dari tutorial ini.

Segala teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini adalah bertujuan untuk pembelajaran sahaja.

Tindakan menguji cuba menggunakan teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini terhadap asset / sistem / komputer bukan milik anda atau tanpa mendapat kebenaran bertulis adalah salah di sisi undang-undang.

Gunakan maklumat dan teknik yang dipaparkan untuk meningkatkan kemahiran anda sama ada untuk tujuan akademik atau kemajuan kerjaya.

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

OBJEKTIF MODUL

1	Memahami OWASP TOP 10 Vulnerabilites
2	Mengenalpasti entry point berkaitan untuk membuat Web Application Penetration Testing
3	Menguji cuba kelemahan yang berkaitan menggunakan teknik manual dan automated mengikut keperluan

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

SILIBUS MODUL

1	OWASP TOP 10 Vulnerabilities 1. Apa itu OWASP TOP 10? 2. Bagaimana OWASP TOP 10 ditentukan? 3. Perbandingan versi OWASP TOP 10?
2	Senarai OWASP TOP 10 2021 (Draf) 1. Injection 2. Broken Authentication 3. Sensitive Data Exposure 4. XML External Entities 5. Broken Access Control 6. Security Misconfigurations 7. Cross Site Scripting (XSS) 8. Insecure Deserialization 9. Using Components With Known Vulnerabilities 10. Insufficient Logging and Monitoring
3	Web Application Penettration Testing 1. Mengenalpasti common entry point pada Web Application untuk membuat Web App Pentest 2. Membuat ujian secara manual dan automated mengikut keperluan 3. Memahami isu kelemahan dan mitigasi yang berkaitan

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Apa itu OWASP TOP 10?	
1	OWASP TOP 10 adalah sebuah laporan yang dikemaskini dari semasa ke semasa mengikut keperluan. OWASP TOP 10 **menggariskan isu dan masalah keselamatan aplikasi web** (Web Application Security) dengan **memfokuskan pada 10 risiko yang paling kritikal** yang telah dikenalpasti.
2	Laporan ini disusun oleh pasukan pakar keselamatan dari seluruh dunia.
3	OWASP merujuk kepada Top 10 sebagai **'dokumen kesedaran' / 'awareness document'** dan mereka mengesyorkan agar semua syarikat **memasukkan laporan tersebut ke dalam proses mereka** untuk meminimumkan dan / atau mengurangkan risiko keselamatan.
4	OWASP TOP 10 adalah **dokumen kesedaran standard** untuk pembangun dan keselamatan aplikasi web.

How It Works

1. Initial Planning/Data Call

Core team gets together and plans a rough schedule, a data call is released.

2. Industry Survey

We determine content in the survey and release for industry participation.

3. Data Analysis

After the data is collected, it is normalized and analyzed.

4. Draft Top Ten

Once we determine the eight risks from the data and the two from the survey, we draft a new list. The Draft is publicly released for review. All issues raised and decisions made are recorded in GitHub issues.

5. Release

Once we have reached a consensus and the core team agrees, we release the new OWASP Top Ten.

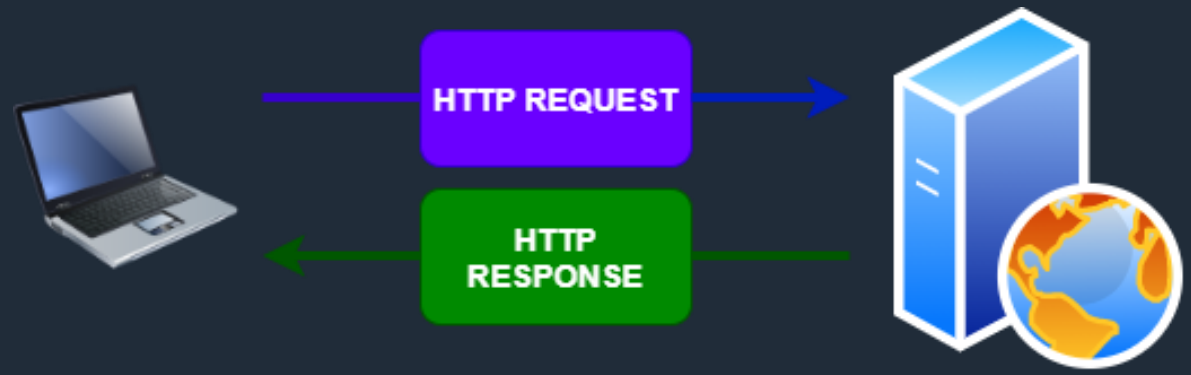
Rujukan

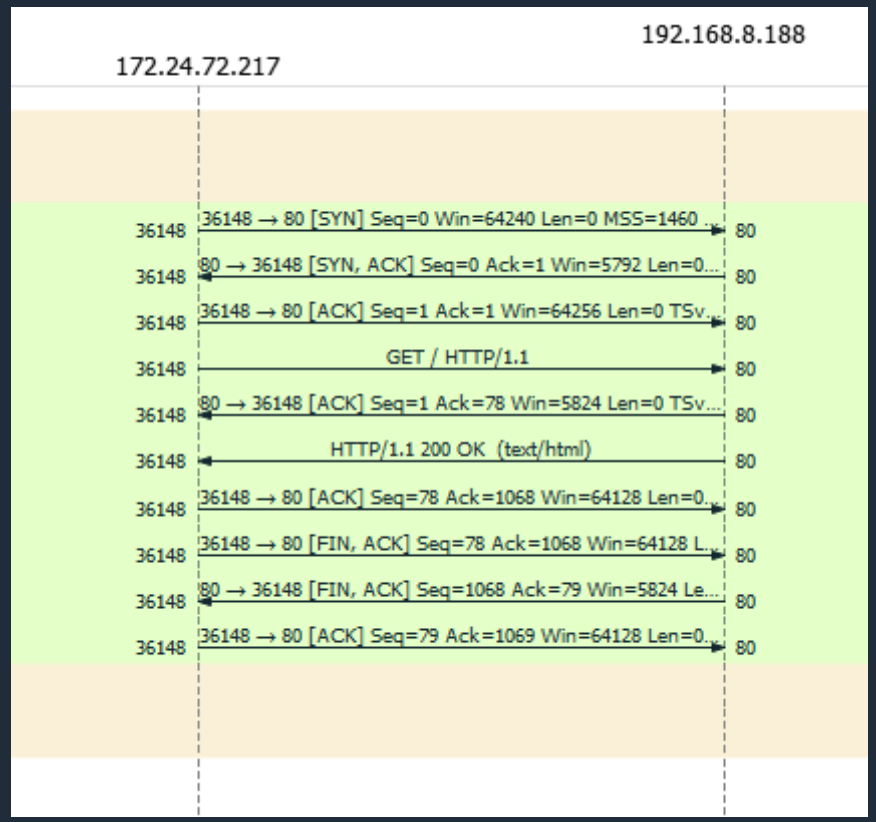
- https://www.owasptopten.org/
- https://owasp.org/www-project-top-ten/
- https://github.com/OWASP/Top10

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Apa itu Web Application Mapping?	
1	Langkah pertama dalam proses Web Application Penetration Testing adalah mengumpulkan dan memeriksa beberapa maklumat penting pada aplikasi web dan pelayan berkenaan untuk mendapatkan pemahaman yang lebih baik terhadap apa yang anda akan attack. Proses ini dinamakan **enumeration** atau **mapping**.
2	Mapping dimulakan dengan mengenalpasti content dan fungsi aplikasi untuk memahami apa yang dilakukan oleh aplikasi dan bagaimana tindakannya. Sebilangan besar fungsi ini mudah dikenal pasti, tetapi sebahagian daripadanya mungkin tersembunyi, adakalanya **intuisi** dan **nasib** memainkan peranan dalam perkara ini.
3	Intuisi ini dapat dipupuk berdasarkan latihan dan pengalaman secara berterusan.

Protokol HTTP	
1	HTTP adalah application protokol yang paling banyak digunakan di Internet. HTTP adalah client-server protokol yang digunakan dalam laman web dan aplikasi web untuk memindahkan data dan sebagainya.
2	Dalam HTTP, client biasanya menggunakan web browser dan connect ke web server seperti Apache, nginx dan lain-lain





```
GET / HTTP/1.1
Host: 192.168.8.189
User-Agent: curl/7.74.0
Accept: */*

HTTP/1.1 200 OK
Date: Sat, 31 Jul 2021 11:26:00 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Content-Type: text/html
```

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

PENAFIAN

Saya (Hussein bin Mohamed / gh1mau) tidak bertanggungjawap dengan sebarang penyalahgunaan maklumat dari tutorial ini.

Segala teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini adalah bertujuan untuk pembelajaran sahaja.

Tindakan menguji cuba menggunakan teknik, prosedur, tools dan bahan yang dipaparkan dalam tutorial ini terhadap asset / sistem / komputer bukan milik anda atau tanpa mendapat kebenaran bertulis adalah salah di sisi undang-undang.

Gunakan maklumat dan teknik yang dipaparkan untuk meningkatkan kemahiran anda sama ada untuk tujuan akademik atau kemajuan kerjaya.

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

Apa itu Command Injection?	
1	Code / Aplikasi yang menjalankan system command untuk tujuan tertentu, di mana code berkenaan tidak dibuat sebarang **input sanitization**.
2	Attacker mengambil peluang ini untuk menambah / mengabung command (malicious) lain untuk tujuan menapau target.

Contoh Code Yang Vulnerable:

ping.php

```
<?php
     $ping = "ping -c 1 ".$_REQUEST['ip'];
     system($ping);
?>
```

Contoh Payload Serangan:

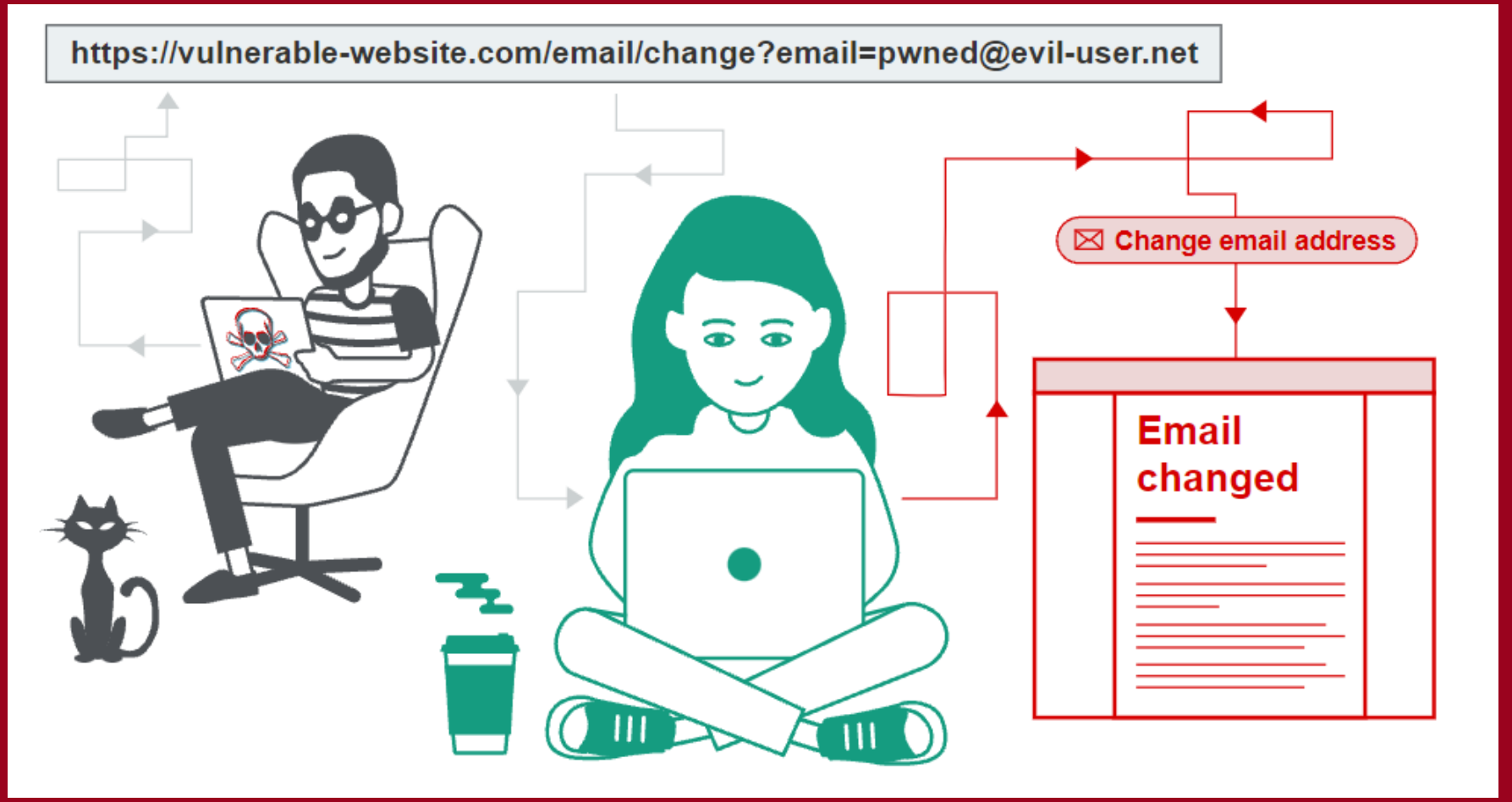
```
ping.php?ip=8.8.8.8

ping.php?ip=8.8.8.8; cat /etc/passwd
```

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Apa itu CSRF/XSRF?	
1	Exploit “trust” antara browser dan aplikasi yang mempunyai kelemahan CSRF dengan keadaan user aplikasi berkenaan sedang logged in (authenticated)
2	Tindakan / actions tertentu dijalankan "bagi pihak" user berkenaan tanpa pengetahuan / kehendak user tersebut.

Apa impak CSRF/XSRF?	
1	Attack yang berjaya akan mengakibatkan user melaksanakan sesuatu action / perkara tanpa disedari, seperti menukar kata laluan, alamat email dan operasi yang lain pada aplikasi web berkenaaan.
2	Sekiranya CSRF dilaksanakan pada user yang mempunyai privillege yang tinggi seperti pentadbir sistem, maka impak attack adalah lebih besar.

Apa itu CSRF/XSRF? (sumber: https://portswigger.net/web-security/csrf)



Common CSRF Attack Vector / Payload Delivery / Trigger	
1	img src (adjust pada width dan style)
2	iframe src (hidden iframe)
3	script src (XMLHTTPRequest untuk multi step CSRF)

Mitigasi umum CSRF	
1	Secure Tokens bagi setiap Request / Session

Apa itu File Inclusion?	
1	Remote File Inclusion (RFI) dan Local File Inclusion (LFI) adalah kelemahan yang biasanya dijumpai dalam poorly-written web applications. Kerentanan ini terjadi apabila aplikasi web memungkinkan pengguna untuk memasukkan input ke dalam fail atau memuat naik fail ke pelayan tanpa sebarang kawalan yang betul.
2	Kerentanan LFI membolehkan attacker membaca dan berkemungkinan melaksanakan fail pada target mangsa. Ini boleh menjadi sangat berbahaya kerana jika pelayan web salah dikonfigurasi dan dijalankan dengan privileges yang tinggi, attacker mungkin mendapat akses ke maklumat sensitif. Sekiranya attacker dapat meletakkan code backdoor pada web server, command execution dapat dilakukan.
3	Kerentanan RFI pula dilakukan dengan mengakses / menjalankan code shell yang dihost pada attacker machine.

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

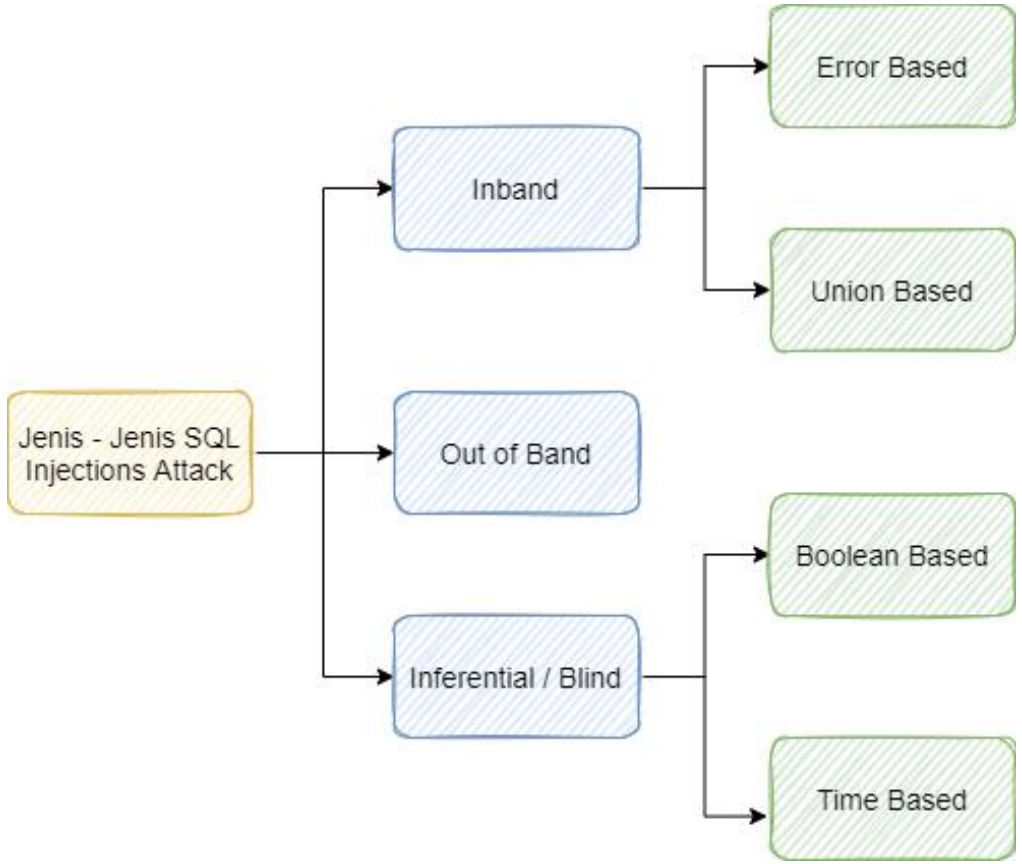
Apa itu File Upload Attack?	
1	Attacker menyalahgunakan / memanipulasi / exploit fungsi fungsi upload untuk memuat naik malicious script.
2	Script berkenaan akan dijalankan untuk tujuan malicious selanjutnya seperti menjalankan sistem command, menjadi pivot point dan lain-lain lagi. Kebiasaannya attacker akan menggunakan webshell bagi tujuan ini.
3	Kerentanan RFI pula dilakukan dengan mengakses / menjalankan code shell yang dihost pada attacker machine.

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Apa itu SQL Injection Attack?

Aplikasi "bercakap" dengan Pangkalan Data menggunakan SQL

Attacker akan inject malicious sql queries pada aplikasi (ruangan input) yang tidak dibuat filtering untuk tujuan SQL Injection Attack



In-Band Injections	
1	In-Band SQL Injection adalah jenis SQLi attack yang paling mudah dikenalpasti dan dieksploit.
2	In-Band bermaksud kaedah/metode connection/communication yang sama yang digunakan untuk mengeksploit kerentanan sqli dan menerima hasil dari medium yang sama.
3	Sebagai contoh, attacker membuat In-Band SQLi attack pada satu aplikasi web, dan kemudiannya dapat mengekstrak data dari pangkalan data melalui aplikasi web yang sama.

Error-Based SQL Injection	
1	Jenis SQL Injection ini adalah yang paling berguna untuk mendapatkan informasi tentang struktur database dengan mudah karena error dari database terus dipaparkan pada browser.

Union-Based SQL Injection	
1	Jenis SQL Injection ini menggunakan operator SQL UNION bersama dengan pernyataan SELECT untuk mendapatkan hasil tambahan ke page. Metode ini adalah cara paling biasa untuk mengekstrak data dalam jumlah besar melalui kerentanan SQL Injection.

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Contoh Payloads In-Band Injection

```
1 UNION SELECT 1
1 UNION SELECT 1,2
1 UNION SELECT 1,2,3

0 UNION SELECT 1,2,3
0 UNION SELECT 1,2,database()

0 UNION SELECT 1,2,group_concat(table_name) FROM information_schema.tables
WHERE table_schema = 'rahsia'

0 UNION SELECT 1,2,group_concat(column_name) FROM
information_schema.columns WHERE table_name = 'pengguna'

0 UNION SELECT 1,2,group_concat(katanama,':',katalaluan SEPARATOR '<br>')
FROM pengguna
```

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Inferential / Blind SQL Injection	
1	Tidak seperti In-Band Injection, di mana kita dapat melihat hasil serangan secara langsung di browser, Blind SQLi adalah ketika kita hanya mendapat sedikit atau tidak ada feedback/response untuk memastikan apakah Injection yang kita lakukan berhasil atau tidak, ini karena error message telah ditutup, tetapi masih ada kerentanan SQLi pada input aplikasi tersebut.

Boolean Based	
1	Boolean based SQL Injection merujuk pada response yang diterima dari SQLi attack berupa benar/salah, ya/tidak, on/off, 1/0 atau apa-apa response yang mempunyai hanya dua outcomes.
2	Outcome/response itu yang menunjukkan sama ada SQLi attack itu berjaya atau tidak.

Time Based	
1	Time-Based blind SQL Injection sangat mirip dengan Boolean Based Injection, payload yang sama dihantar tetapi tiada indikator visual sama ada attack itu berjaya atau tidak.
2	Untuk itu, attacker akan menambah time pada attack query, teknik time delay ini (dalam mysql kita boleh gunakan function SLEEP(n)) akan digunakan bersama UNION statement. Sekiranya ada kerentanan SQLi, function SLEEP berkenaan akan dijalankan, dan attacker boleh memanipulasi keadaan ini untuk mengekstract data atau lain-lain perkara.

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Contoh Payloads Boolean Based

```
admin123' UNION SELECT 1,2,3;--
admin123' UNION SELECT 1,2,3 where database() like '%';--
admin123' UNION SELECT 1,2,3 where database() like 'r%';--

admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE
table_schema = 'rahsia' and table_name like 'p%';--

admin123' UNION SELECT 1,2,3 FROM information_schema.tables WHERE
table_schema = 'rahsia' and table_name='pengguna';--

admin123' UNION SELECT 1,2,3 FROM information_schema.COLUMNS WHERE
TABLE_SCHEMA='rahsia' and TABLE_NAME='pengguna' and COLUMN_NAME like
'k%';--

admin123' UNION SELECT 1,2,3 from pengguna where username like 'g%';--

admin123' UNION SELECT 1,2,3 from pengguna where username='gh1mau' and
password like 'p%';--
```


HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM

Contoh Payloads Time Based

```
admin123' UNION SELECT SLEEP(5);--

admin123' UNION SELECT SLEEP(5),2;--

admin123' UNION SELECT SLEEP(5),2 where database() like 'r%';--
```


HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Out Of Band Injection	
1	Out-of-Band SQL Injection adalah tidak common kerana ianya bergantung pada features tertentu yang di enable pada Server Pangkalan Data atau berdasarkan pada business logic error pada aplikasi berkenaan. Ini membolehkan attacker membuat external network call sebagai result dari query SQL yang di inject.
2	Serangan Out-Of-Band diklasifikasikan dengan memiliki dua communication channels yang berbeza, satu untuk membuat serangan dan yang satu lagi untuk mengumpulkan hasil. Contohnya, channel serangan mengkin berupa web request, dan channel pengumpulan data mungin dengan memantau request HTTP/DNS yang dibuat ke service yang dikawal oleh attacker

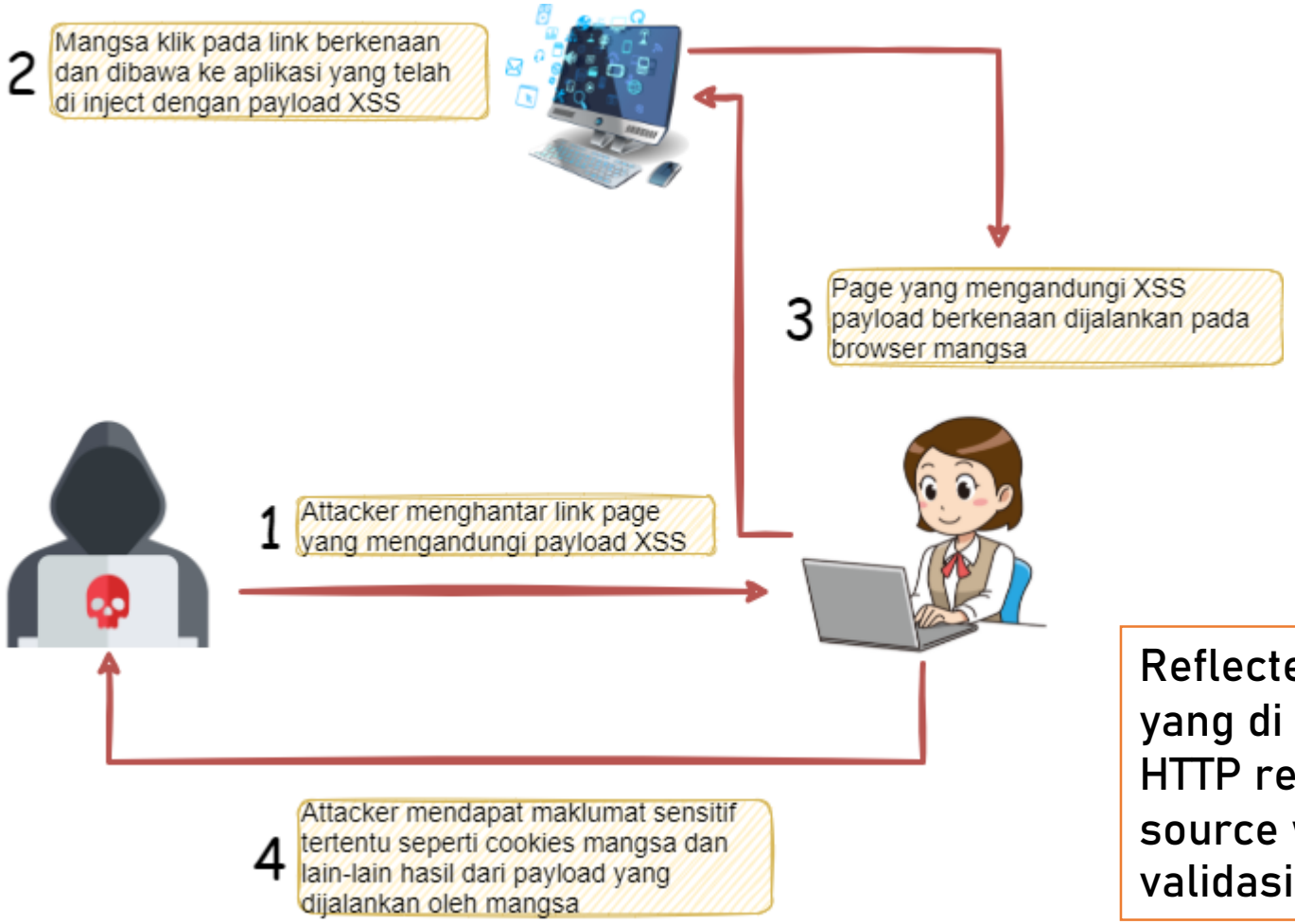
HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Out Of Band Injection

Langkah Pengukuhan	
1	Prepared Statements (Dengan Parameterized Queries)
2	Input Validation
3	Escaping User Input

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Reflected XSS



Reflected XSS terjadi ketika data yang di submit oleh user melalui HTTP request dipaparkan pada source webpage tanpa sebarang validasi.

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Impak

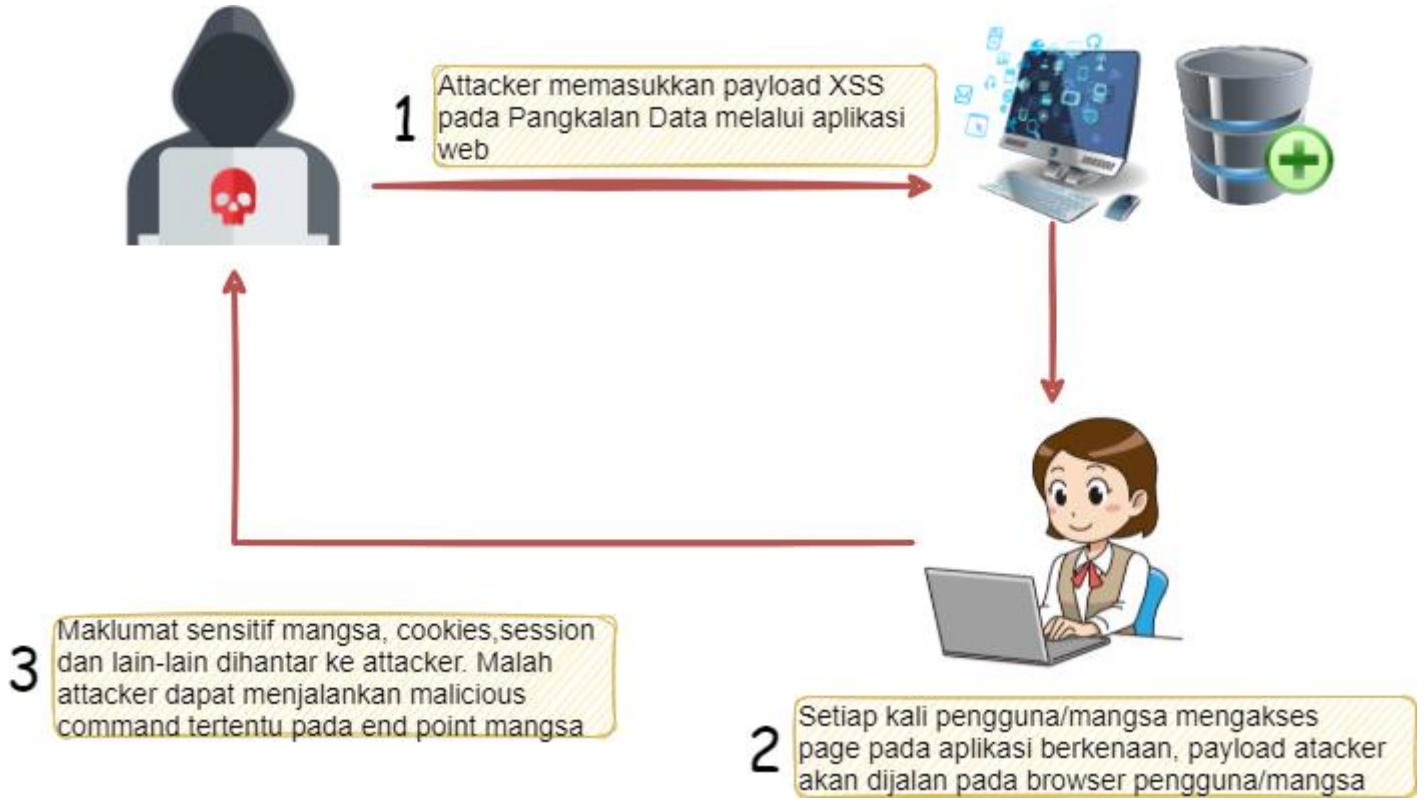
Attacker boleh menghantar link atau embed payload javascript pada mangsa dan kemudian mangsa menjalankan code tersebut pada browser mangsa, ini membolehkan attacker mendapatkan maklumat sensitif mangsa, cookies, session dan lain-lain

Bagaimana menguji kerentanan Reflected XSS?

Setiap entry point haruslah diuji:

- Parameter pada URL Query String
- URL File Path
- HTTP Headers

Stored XSS



Payload XSS di simpan dalam aplikasi web (Pangkalan Data) dan payload berkenaan akan dijalankan ketika pengguna mengunjungi / mengkakses halaman berkenaan.

STORED XSS

Impak

Attacker boleh menghantar link atau embed payload javascript pada mangsa dan kemudian mangsa menjalankan code tersebut pada browser mangsa, ini membolehkan attacker mendapatkan maklumat sensitif mangsa, cookies, session dan lain-lain

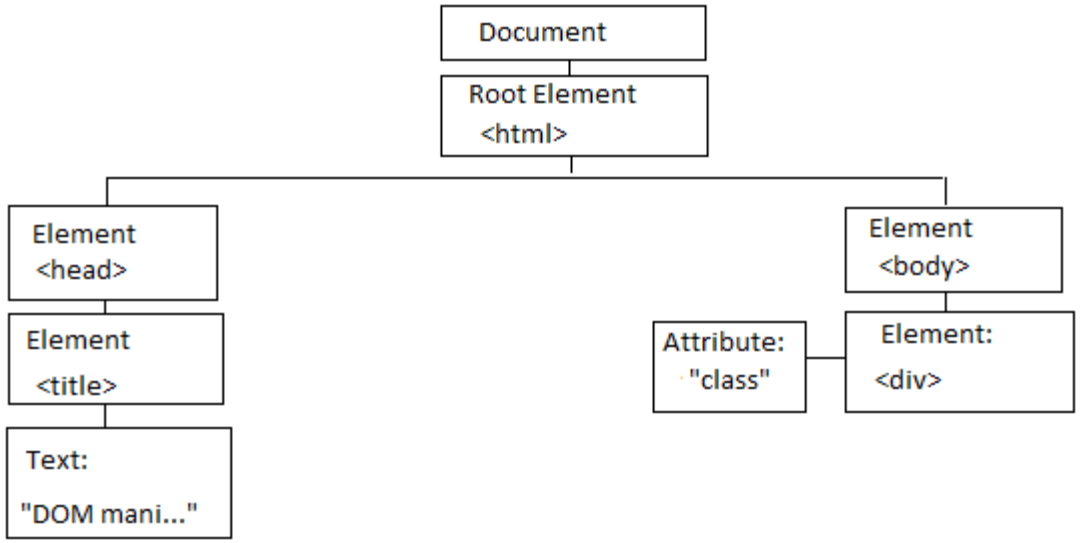
Bagaimana menguji kerentanan Reflected XSS?

Setiap entry point haruslah diuji:

- Ruangan comments / guestbook pada aplikasi
- Ruangan user profile
- HTTP Headers

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Apa itu DOM?

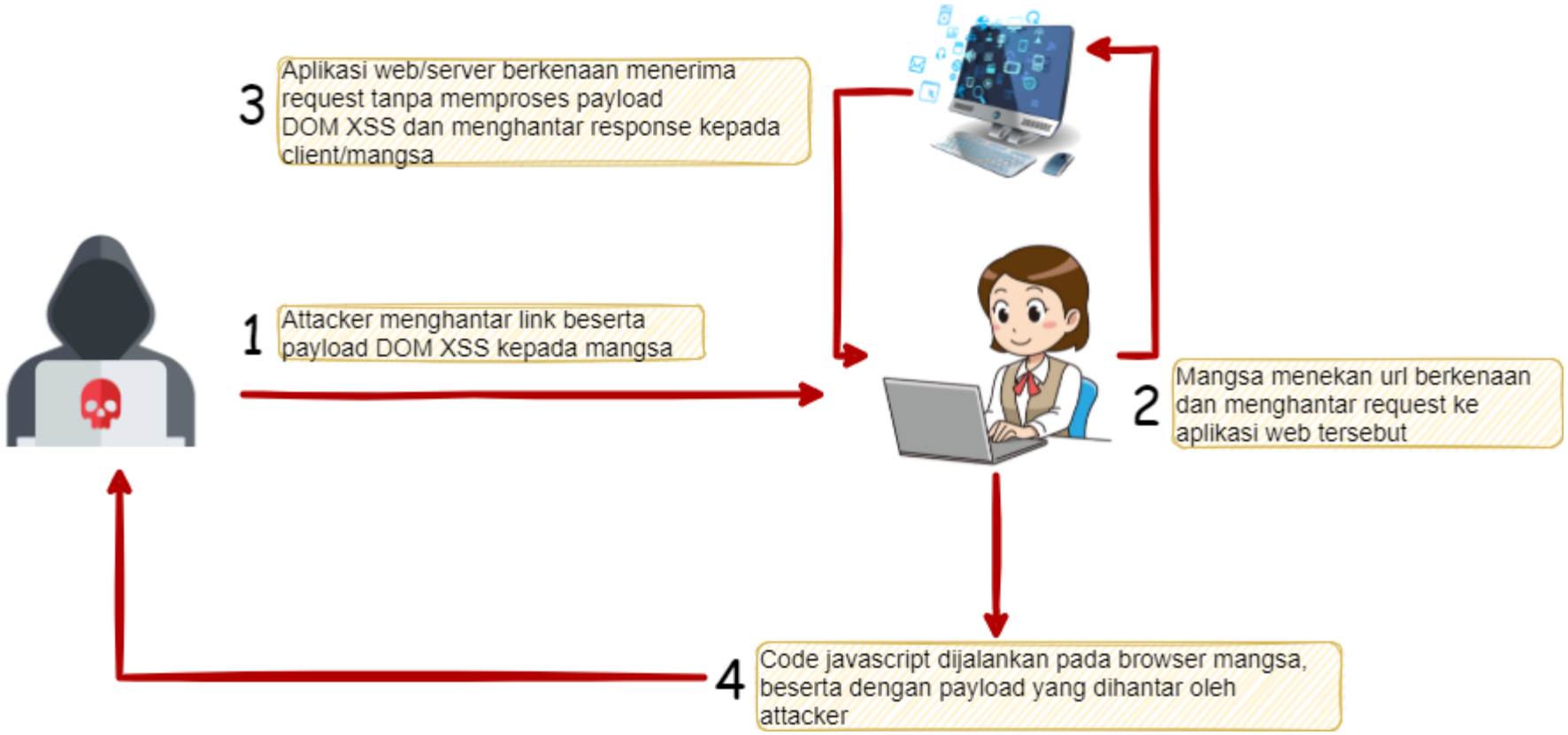


Ketika web page di load, browser akan menghasilkan Document Object Model(DOM) pada page berkenaan.

With the object model, JavaScript gets all the power it needs to create dynamic HTML:

- JavaScript can change all the HTML elements in the page
- JavaScript can change all the HTML attributes in the page
- JavaScript can change all the CSS styles in the page
- JavaScript can remove existing HTML elements and attributes
- JavaScript can add new HTML elements and attributes
- JavaScript can react to all existing HTML events in the page
- JavaScript can create new HTML events in the page

DOM Based XSS



DOM Based XSS	
1	DOM Based XSS adalah disebabkan dari aplikasi yang mengandungi client-side Javascript yang memproses data dari untrusted source secara tidak selamat, selalunya dengan menulis data pada potentially dangerous sink dalam DOM
2	Payload dijalankan hasil dari pengubahan (modifying) pada DOM
3	Tiada perubahan pada HTTP Response
4	source: adalah javascript property yang mengandungi data yang mana berpotensi untuk dikawal oleh attacker. Sebagai contoh: location.search yang membaca input dari query string.
5	sink: adalah function atau DOM object yang membenarkan kod javascript atau HTML dijalankan. Sebagai contoh: code execution sink adalah eval(), dan HTML sink adalah document.body.innerHTML

DOM Based XSS	
Source • document.URL • document.referrer • location • location.href • location.search • location.hash • location.pathname	**Sink** • eval • setTimeout • setInterval • document.write • element.innerHTML

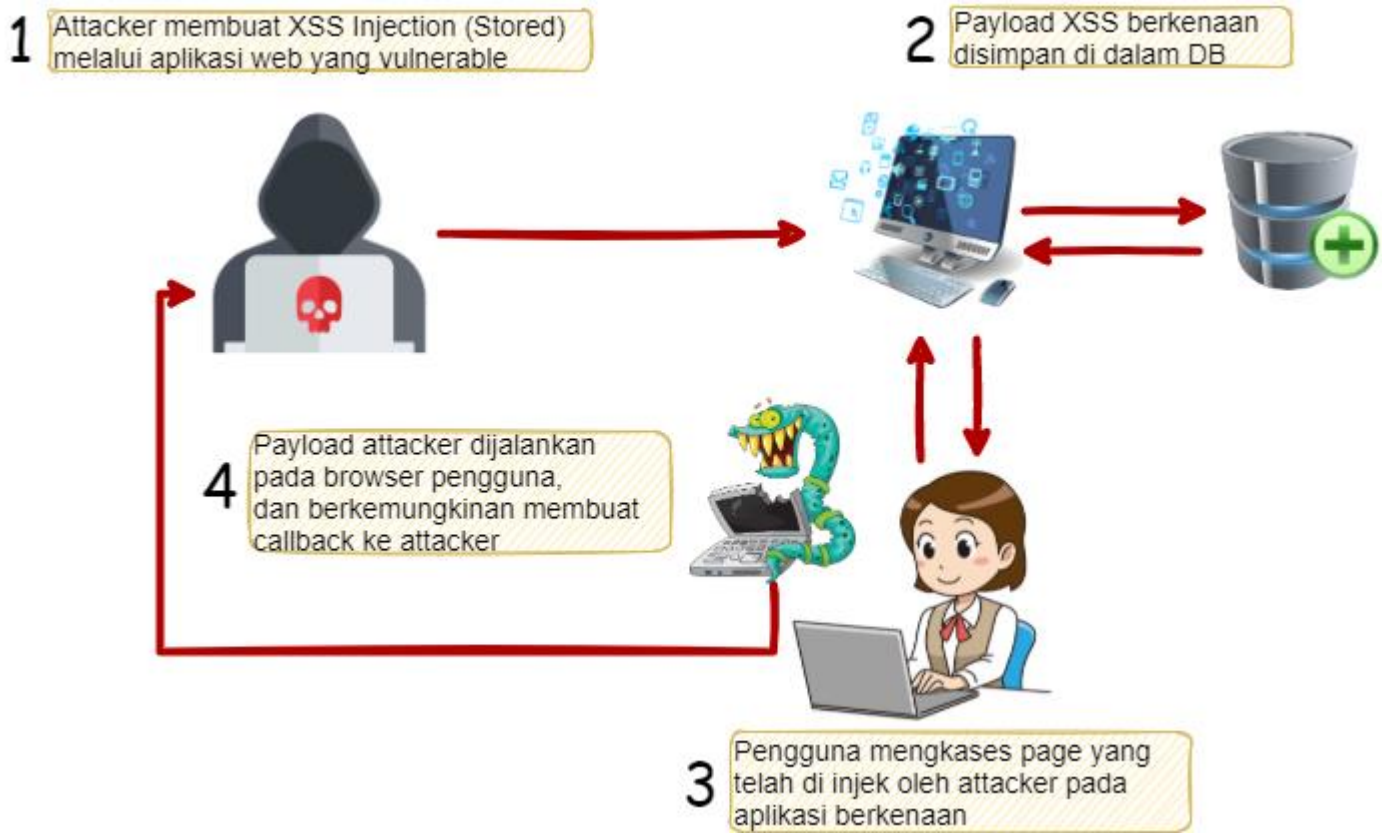
HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

DOM Based XSS : Contoh Vulnerable Code

```
<!DOCTYPE html>
<html>
<body>

<h2>Test DOM Based XSS</h2>

<p id="demo"></p>

<script>
var num = document.URL.split("num=")[1];
document.getElementById("demo").innerHTML = eval(num);
</script>

</body>
</html>
```


HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

Blind XSS



Blind XSS mirip dengan Stored XSS di mana payload attacker disimpan dalam aplikasi web untuk di akses oleh pengguna lain, attacker tidak dapat melihat payload tersebut berjalan, attacker akan menunggu sehingga mangsa mengakses page yang mengandungi payload tersebut.

Blind XSS: Possible Entry Point

- review form
- contact us page
- feedback page
- credit card payment details
- user profile
- user-agent
- comment box
- passwords / login form
- chat applications

HUSSEIN BIN MOHAMED AKA CH1MAU | CH1MAU.RULEZ@GMAIL.COM

HUSSEIN BIN MOHAMED AKA GH1MAU | GH1MAU.RULEZ@GMAIL.COM