LAPORAN PRAKTIKUM

SESION HIJACKING

DISUSUN OLEH **:**

Nama	: Diki Candra
Nim	: 2022903430010
Kelas	: TRKJ 2B
Jurusan	: Teknologi Informasi dan Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Dosen Pengajar	: Aswandi, S.Kom, M.Kom.

JURUSAN TEKNOLOGI INFORMASI DAN KOMUNIKASI

PRODI TEKNOLOGI REKAYASA KOMPUTER DAN JARINGAN

POLITEKNIK NEGERI LHOKSEUMAWE

TAHUN 2022/2023

LEMBARAN PENGESAHAN

Laporan Yang Berjudul	: Sesion Hijacking
Disusun Oleh	: Diki Candra
NIM	: 2022903430010
Jurusan	: Teknologi Informasi & Komputer
Program Studi	: Teknologi Rekayasa Komputer Jaringan
Mata Kuliah	: Ethical Hacking
Tabel Penilaian	:

Mengetahui,

Dosen Pembimbing,

Aswandi, S.Kom, M.Kom
NIP. 197209242010121001

Penyusun,

Diki Candra
NIM. 2022903430010

Session Hijacking

Latar Belakang Session Hijacking:

Session Hijacking, juga dikenal sebagai session stealing, adalah teknik di mana seorang penyerang mencuri atau mengambil alih sesi otentikasi yang dimiliki oleh pengguna yang sah. Sesi otentikasi ini adalah kumpulan data yang menunjukkan bahwa pengguna telah melewati proses otentikasi dan diidentifikasi oleh sistem sebagai pengguna yang sah. Dalam konteks web, ini seringkali berarti mencuri atau menduplikasi token otentikasi atau ID sesi yang digunakan untuk mengidentifikasi dan mengotentikasi pengguna.

Beberapa latar belakang yang melibatkan Session Hijacking termasuk:

1. **Autentikasi Web:** Sistem web modern menggunakan otentikasi untuk memberikan hak akses yang sesuai kepada pengguna. Ini melibatkan pengguna memberikan kredensial (seperti username dan password) dan menerima token otentikasi yang memungkinkannya mengakses sumber daya tertentu.
2. **ID Sesi:** Setelah proses otentikasi berhasil, pengguna sering diberikan ID sesi atau token otentikasi yang harus disertakan dalam setiap permintaan untuk sumber daya yang dilindungi. Ini memungkinkan server mengidentifikasi pengguna secara unik.
3. **Man-in-the-Middle (MitM) Attacks:** Salah satu metode umum untuk menjalankan Session Hijacking adalah dengan melakukan serangan Man-in-the-Middle (MitM). Penyerang dapat menyusup ke antara klien dan server, memata-matai atau mengubah data yang melewati koneksi.
4. **Cookie Hijacking:** Banyak situs web menggunakan cookie untuk menyimpan ID sesi atau token otentikasi. Jika cookie ini dapat dicuri, penyerang dapat menggunakan mereka untuk melewati otentikasi dan mendapatkan akses ke akun pengguna.
5. **Kelemahan Keamanan:** Banyak Session Hijacking terjadi sebagai akibat dari kelemahan keamanan dalam aplikasi web, protokol otentikasi yang digunakan, atau infrastruktur jaringan.

Konsep Session Hijacking:

1. **Pencurian Token Otentikasi:** Penyerang mencuri token otentikasi atau ID sesi pengguna yang sah. Ini bisa dilakukan dengan mencuri cookie, menyusup koneksi nirkabel, atau mengeksploitasi celah keamanan pada sisi klien atau server.
2. **Replay Attacks:** Dalam beberapa kasus, penyerang dapat merekam dan memutar ulang token otentikasi yang sah untuk mendapatkan akses tanpa melewati proses otentikasi. Ini seringkali terjadi ketika otentikasi tidak menggunakan teknik enkripsi yang kuat.

3. **Sesi Man-in-the-Middle:** Serangan Man-in-the-Middle memungkinkan penyerang memantau dan mengontrol komunikasi antara pengguna dan server. Ini memungkinkan mereka untuk mencuri atau mengubah data sesi.
4. **Cookie Theft:** Mengambil cookie otentikasi dari sistem pengguna merupakan salah satu bentuk umum Session Hijacking. Jika penyerang dapat mendapatkan cookie ini, mereka dapat menggunakannya untuk bersidang sebagai pengguna yang sah.
5. **Penggunaan Proksi:** Penyerang dapat menggunakan proksi atau alat serangan lainnya untuk menyusup ke dalam koneksi antara pengguna dan server. Ini memungkinkan mereka mengawasi dan memanipulasi data sesi.

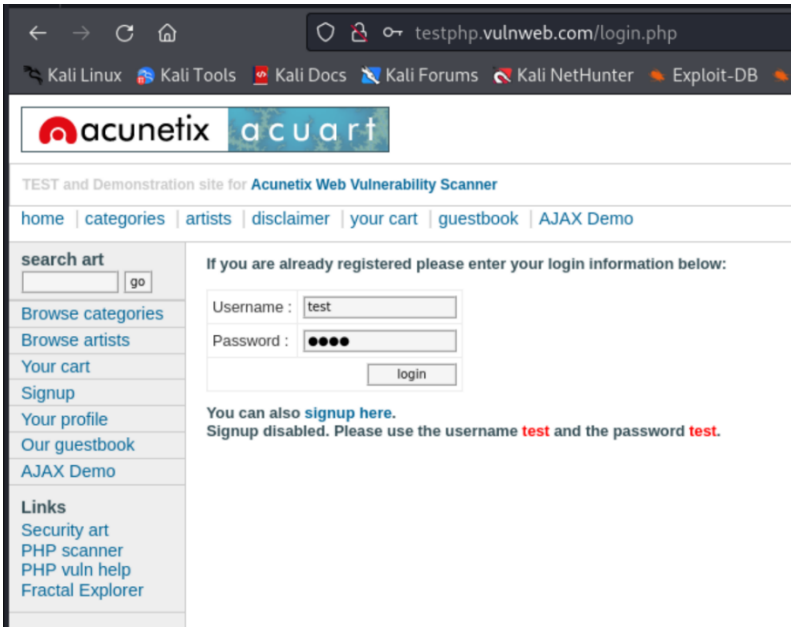
Mitigasi Session Hijacking:

1. **Penggunaan HTTPS:** Menggunakan protokol HTTPS membantu mengamankan data saat transit, mengurangi risiko serangan Man-in-the-Middle.
2. **Token Otentikasi yang Kuat:** Menggunakan teknik otentikasi yang kuat dan token yang dihasilkan secara acak dapat mengurangi risiko pencurian atau penggunaan ulang.
3. **Cookie Security:** Menetapkan kebijakan keamanan cookie yang ketat, seperti penggunaan atribut "Secure" dan "HttpOnly", dapat membantu melindungi cookie dari pencurian.
4. **Pemantauan Aktivitas Sesi:** Memantau aktivitas sesi pengguna dan mendeteksi anomali, seperti perangkat masuk dari lokasi yang tidak biasa atau perubahan perilaku tiba-tiba, dapat membantu mendeteksi Session Hijacking.
5. **Pelatihan Keamanan:** Melibatkan pengguna dalam pelatihan keamanan dapat membantu mereka mengidentifikasi dan menghindari praktik-praktik yang rentan terhadap Session Hijacking.
6. **Pembaruan dan Pemeliharaan Keamanan:** Melakukan pembaruan rutin perangkat lunak dan mengatasi kelemahan keamanan dapat mengurangi risiko serangan Session Hijacking yang memanfaatkan celah keamanan.

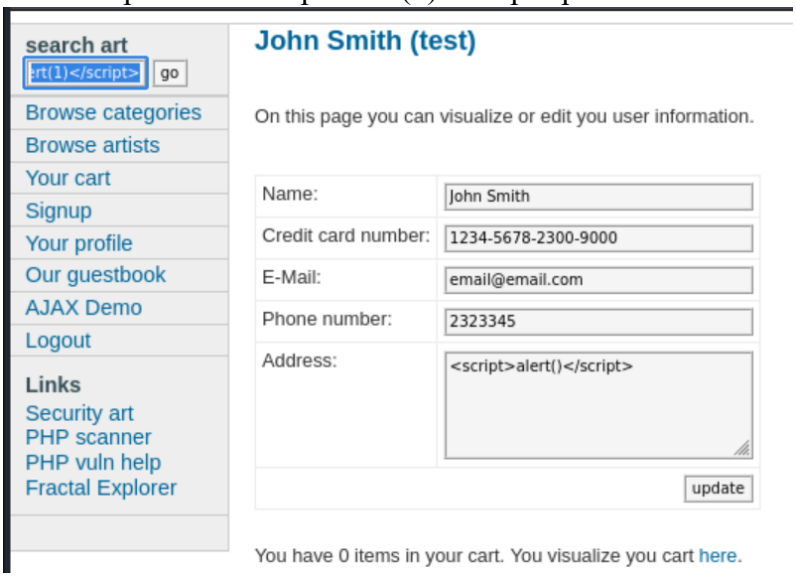
Secara keseluruhan, mitigasi efektif terhadap Session Hijacking melibatkan kombinasi praktik keamanan teknis, pemantauan aktifitas, dan pendidikan keamanan pengguna.

Langkah-langkah melakukan Hijacking

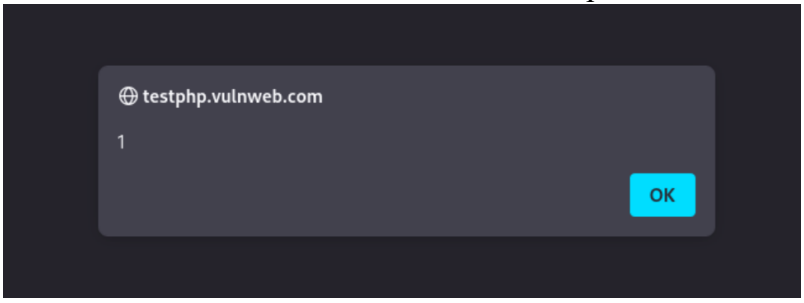
1. Bukan web testphp.vulnweb.com dan login dengan username test dah password test



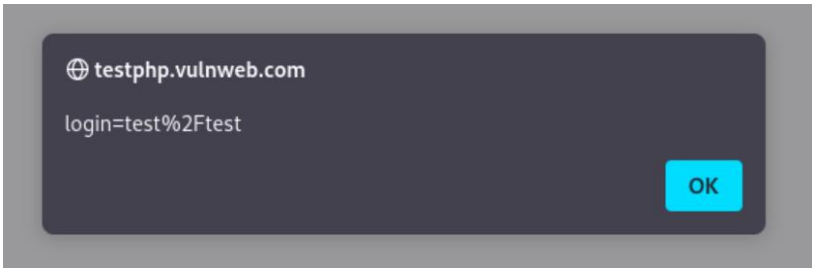
2. Lakukan perintah <script>alert(1)</script> pada kolom search art



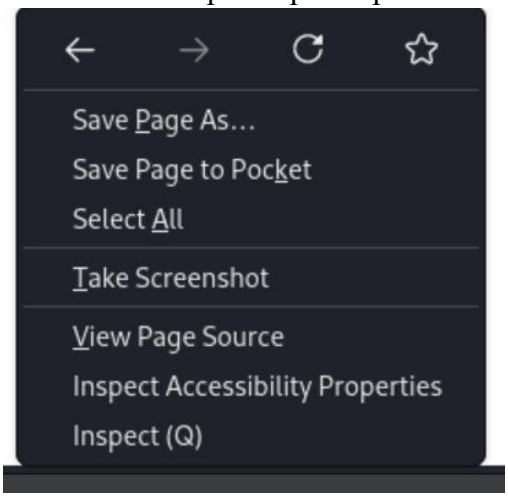
Setelah melakukan enter maka akan keluar seperti berikut ini



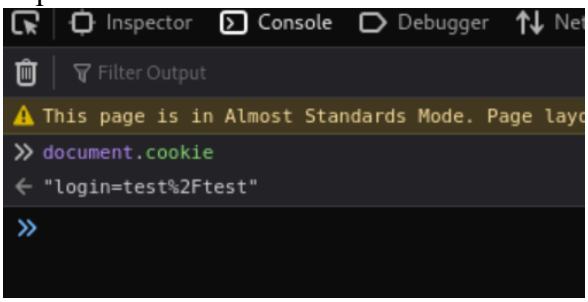
3. Kemudian lakukan perintah <script>alert(document.cookie)</script> pada kolom search art



4. Klik kanan dan pilih opsi inspect untuk mengakses console pada browser

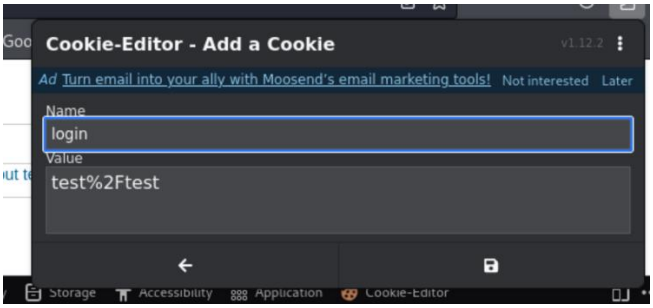


Seperti ini

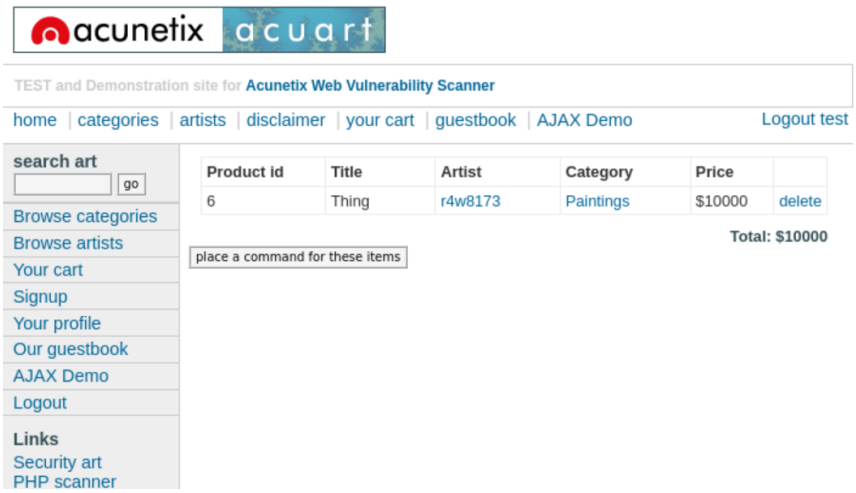


Dan ketik document.cookie

5. Setelah itu install extention cookie editor dan tambahkan seperti ini



6. Lakukan refresh pada halaman web maka akan keluar hasil seperti ini



Kesimpulan dari Langkah-langkah Hijacking:
Langkah-langkah yang disebutkan menunjukkan serangkaian tindakan untuk melakukan hijacking pada situs web testphp.vulnweb.com. Berikut adalah kesimpulan dari setiap langkah:

1. **Masuk ke Situs Web:** Pengguna diminta untuk masuk ke situs web testphp.vulnweb.com menggunakan kredensial dengan username "test" dan password "test". Ini menunjukkan akses ilegal ke akun yang mungkin dimiliki oleh pengguna lain jika informasi masuk dicuri.

2. **Menanamkan Skrip pada Kolom Pencarian:** Dalam langkah ini, serangan dimulai dengan menanamkan skrip JavaScript <script>alert(1)</script> pada kolom pencarian. Tindakan ini dimaksudkan untuk menunjukkan celah keamanan di situs web yang memungkinkan injeksi skrip dan mengeksekusi kode JavaScript pada sisi klien.

3. **Mencuri Informasi Cookie:** Langkah ini melibatkan penggunaan skrip JavaScript <script>alert(document.cookie)</script> pada kolom pencarian untuk mencuri informasi cookie pengguna. Ini menunjukkan adanya celah keamanan yang memungkinkan pencurian informasi sensitif seperti cookie, yang dapat digunakan untuk menduplikasi sesi pengguna.

4. **Menggunakan Console Browser:** Setelah mendapatkan skrip cookie, langkah selanjutnya adalah membuka konsol browser menggunakan fitur "inspect". Di sini, pengguna dapat mengetikkan perintah "document.cookie" untuk mengekstrak dan melihat nilai cookie. Ini merupakan contoh dari teknik pengambilan informasi menggunakan alat bawaan browser.

5. **Menggunakan Ekstensi Cookie Editor:** Pengguna diinstruksikan untuk menginstal ekstensi Cookie Editor pada langkah ini. Ekstensi ini memungkinkan pengguna untuk mengedit dan menambahkan cookie secara manual. Ini adalah langkah tambahan untuk menunjukkan bagaimana penyerang dapat memanipulasi cookie pengguna.

6. **Refresh Halaman Web:** Setelah mengedit cookie dengan ekstensi, pengguna diminta untuk me-refresh halaman web. Hasilnya menunjukkan bahwa manipulasi cookie berhasil dan dapat digunakan untuk mendapatkan akses tanpa otentikasi ulang.
   Kesimpulan Akhir: Langkah-langkah tersebut menciptakan gambaran umum tentang bagaimana serangan hijacking dapat dilakukan melalui injeksi skrip, pencurian cookie, dan manipulasi cookie. Kesimpulannya, situs web tersebut rentan terhadap serangan injeksi skrip dan hijacking sesi, yang mengungkapkan kelemahan keamanan yang perlu segera diatasi oleh pemilik situs. Pada tingkat umum, kesadaran dan pemahaman tentang praktik keamanan web, termasuk penggunaan enkripsi dan perlindungan terhadap injeksi skrip, sangat penting untuk mencegah serangan semacam ini.