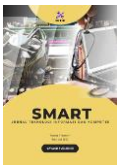


SMART : Jurnal Teknologi Informasi dan Komputer
Available online at https://journal.bengkuluinstitute.com/index.php/smart
Vol. 3 No. 2, July-December 2024, pages: 107-115
ISSN: 2963-6388
https://doi.org/10.58222/smart.v3i1.522

Preventing Session Hijacking Attacks on PHP WEB Applications

Mencegah Serangan Session Hijacking pada WEB PHP

Ismail Puji Saputra [a]

Article history:

Submitted: 4 November 2022
Revised: 17 November 2022
Accepted: 28 November 2022

Keywords:

XSS Attack, Session Hijacking, Secure Session, Authentication

Abstract

Session hijacking attacks pose a serious threat to the security of web applications, potentially leading to the theft of user sessions and unauthorized access to sensitive information. This study aims to develop a method to prevent session hijacking attacks by incorporating two-factor authentication using session and PIN. The system records the user's session and IP address during the login process, then compares both when the user attempts to access critical pages, such as the dashboard. If there is an IP mismatch, the user is prompted to enter a PIN for additional authentication. While this method is effective in preventing session-based attacks, its limitation lies in the potential for Man-in-the-Middle (MITM) attacks, especially when the attacker and the user are on the same network. The results of the testing show that this mechanism can enhance web application security by adding an extra layer of protection against session hijacking attacks.

Abstrak

Serangan session hijacking merupakan ancaman serius bagi keamanan aplikasi web yang dapat menyebabkan pencurian sesi pengguna dan akses tidak sah ke informasi sensitif. Penelitian ini bertujuan untuk mengembangkan metode pencegahan serangan session hijacking dengan menggabungkan autentikasi dua faktor menggunakan sesi dan PIN. Sistem yang dikembangkan mencatat sesi dan alamat IP pengguna selama proses login, kemudian mencocokkan keduanya saat pengguna mencoba mengakses halaman penting seperti dashboard. Jika terjadi ketidaksesuaian IP, pengguna akan diminta untuk memasukkan PIN sebagai langkah autentikasi tambahan. Meskipun metode ini efektif dalam mencegah serangan berbasis sesi, kelemahannya terletak pada potensi serangan Man-in-the-Middle (MITM) yang dapat terjadi jika penyerang dan pengguna berada dalam jaringan yang sama. Hasil pengujian menunjukkan bahwa mekanisme ini dapat meningkatkan keamanan aplikasi web dengan menambah lapisan perlindungan terhadap serangan session hijacking.

[a] Universitas Muhammadiyah Metro

Corresponding author:
Ismail Puji Saputra
Universitas Muhammadiyah Metro
Email address: ismailpujisaputra@gmail.com

1 Pendahuluan

Session hijacking adalah sebuah serangan yang sering terjadi pada system informasi berbasis web, khususnya yang menggunakan bahasa pemrograman Hypertext Processor (PHP). Serangan session hijacking dapat dilakukan dengan berbagai metode, yaitu dengan menggunakan celah keamanan pada website, berupa serangan XSS Attack (Cross Site Scripting), maupun menggunakan serangan berbasis jaringan dengan teknik Man in the Middle (MITM) [1,2].

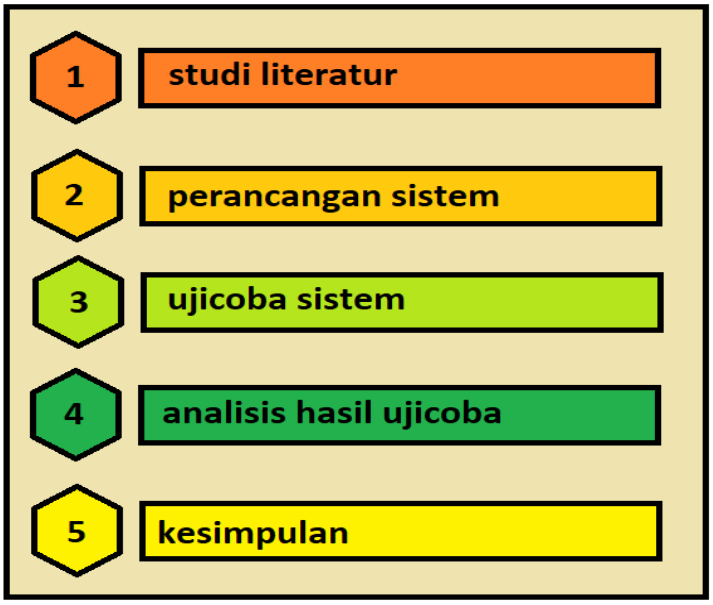
Serangan session hijacking dapat dilakukan dengan berbagai cara, yaitu dengan menyerang melalui network maupun melalui lapisan application, kedua cara serangan tersebut memiliki pendekatan yang berbeda dalam pencegahanya [3,4]. Pencegahan pada bagian application layer dilakukan dengan memberlakukan pembatasan idle time, pengguna akan dipaksa untuk melakukan login ulang jika tidak melakukan apapun (idle) dalam kurun waktu tertentu [5,6]. Sedangkan serangan melalui network misalnya serangan sniffing dapat dilakukan dengan menggunakan protocol yang aman (HTTPS)[7,8], maupun dengan memanfaatkan tunneling [9,10].

Namun beberapa solusi yang ditawarkan dari penelitian sebelumnya dianggap masih kurang aman dan kurang efisien untuk diterapkan pada sebuah website yang memiliki keberagaman pengguna, untuk itu penulis mencoba untuk melakukan modifikasi teknik ATEUI yaitu teknik autentikasi yang menggunakan semua informasi pengguna yang dienkripsi dan melindungi dari serangan sniffing, teknik ini membandingkan perangkat pengguna asli dengan perangkat pengguna illegal, teknik ATEUI menyimpan data perangkat ke server pada saat pengguna login, sehingga apabila terdapat pengguna yang hanya menggunakan sesi dan dengan data perangkat yang berbeda server akan menolak request pengguna tersebut. Kelemahan dari metode ATEUI adalah membutuhkan waktu eksekusi yang tinggi karena proses enkripsi dan dekripsi yang berulang [1].

Penelitian ini akan memanfaatkan PIN (personal identification number) dalam mencegah serangan Session hijacking, ketika pengguna login, sesi dan alamat internet protocol (IP) pengguna akan tersimpan dalam database, ketika terdapat pengguna lain yang menggunakan sesi yang sama dengan alamat IP yang berbeda, maka sistem akan memaksa pengguna tersebut untuk memasukan PIN, dimana PIN tersebut hanya dimiliki oleh pengguna yang sah. Hal ini merupakan proses autentikasi yang tidak hanya memanfaatkan 1 faktor autentikasi, melainkan dengan menggunakan 2 faktor autentikasi.

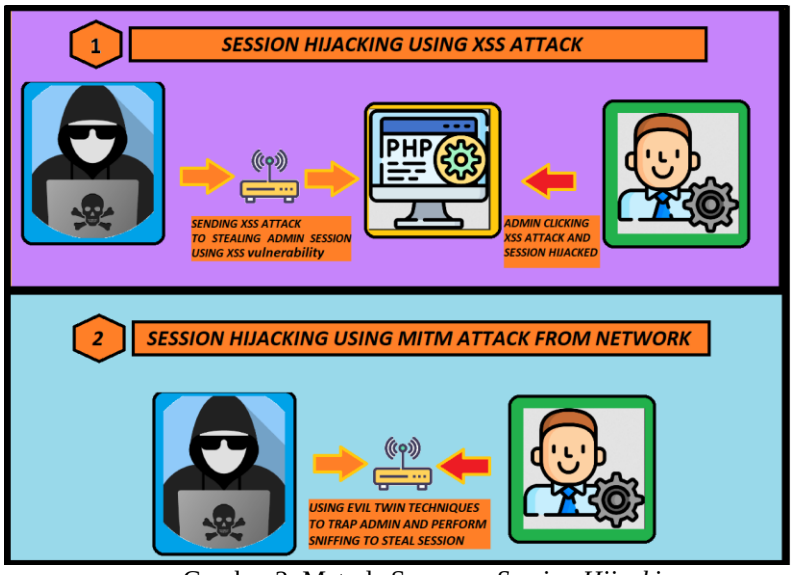
2 Metodologi Penelitian

Penelitian ini bertujuan untuk mengembangkan metode yang dapat mengamankan website dari serangan session hijacking, proses pengamanan dilakukan dalam layer application. Berikut ini gambar 1 yaitu gambar alur penelitian.



Gambar 1. Alur Penelitian

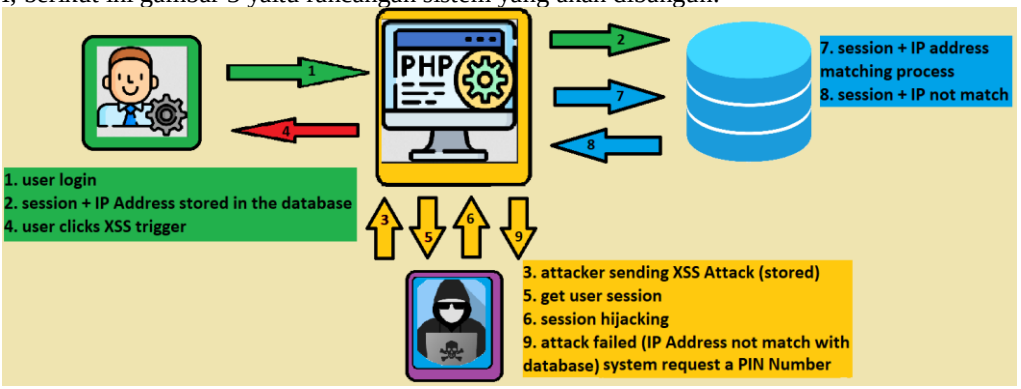
Pada tahap pertama, proses studi litertur dilakukan untuk mengetahui pengertian session hijacking, proses serangan dan berbagai metode dalam mencegah serangan tersebut. Sesuai dengan penelitian [1], session hijacking dapat digambarkan seperti pada gambar 2 dibawah ini.



Gambar 2. Metode Serangan *Session Hijacking*

Pada gambar 2 yang ditunjukan dengan nomor 1 menggambarkan bahwa metode yang paling umum dalam melancarkan serangan session hijacking, didapatkan dengan menggunakan serangan XSS. Serangan XSS, dilakukan pada lapisan application, melalui vulnerability yang telah ditemukan. Sedangkan pada gambar 2 yang ditunjukan dengan nomor 2 adalah serangan yang dilakukan melalui network (jaringan), dengan memanfaatkan serangan Man in the middle dengan teknik evil twin, dimana administrator dijebak untuk masuk ke jaringan palsu yang dibuat oleh penyerang, setelah administrator terjebak dalam jaringan palsu tersebut, penyerang melakukan sniffing untuk menangkap dan membaca trafik dari administrator guna mencuri sesi atau bahkan password administrator. Serangan dengan tipe jaringan ini secara teori tidak akan mampu diatasi dengan metode yang akan diajukan, karena penyerang tetap mampu mendapatkan sesi ataupun data sensitif lainya, selama administrator masih menggunakan jaringan palsu tersebut.

Selanjutnya adalah tahap perancangan sistem, sistem disini adalah sebuah metode atau mekanisme yang dibangun untuk mengamankan sebuah website dari serangan session hijacking dengan melakukan modifikasi teknik ATEUI, berikut ini gambar 3 yaitu rancangan sistem yang akan dibangun.



Gambar 3. Rancangan Mekanisme Pencegahan *Session Hijacking*

Pada gambar 3, dijelaskan proses mekanisme mendeteksi serangan sebagai berikut:

1). Pengguna login dengan menggunakan username dan password.
2). Jika login berhasil, sistem akan mencatat sesi dan alamat IP pengguna.
3). Penyerang melakukan serangan XSS dengan menyisipkan file html ke server; tahap
4). Pengguna mengakses file html sehingga sesinya dicuri.
5). Sesi dikirimkan ke penyerang.
6). Penyerang melakukan serangan session hijacking.
7). Sistem mencocokan sesi dan alamat IP pada database.
8). Sistem menyatakan bahwa sesi dan alamat IP tidak cocok.
9). Sistem meminta penyerang untuk memasukan PIN yang hanya diketahui oleh pengguna.

Setelah perancangan dilakukan, maka selanjutnya adalah mengimplementasikan perancangan sistem dan melakukan pengujian. Implementasi sistem dengan lingkungan yang telah disesuaikan, yaitu sebuah website yang memiliki kerentanan serangan *XSS*, Website dibuat dengan menggunakan bahasa pemrograman PHP dengan menggunakan *database* MySQL. Sistem akan diuji untuk mengetahui apakah sistem mampu mendeteksi dan mencegah serangan. Hasil pengujian akan dianalisis untuk mendapatkan kesimpulan penelitian.

3. Hasil dan Pembahasan

Perancangan Database

Database yang digunakan dalam penelitian ini adalah database MySQL, database diberi nama sessionsecure, dan memiliki tabel user, tabel user memiliki beberapa kolom yang digunakan untuk melakukan simulasi serangan session hijacking. Berikut ini kolom yang ada pada tabel user:

Tabel 1. Tabel user

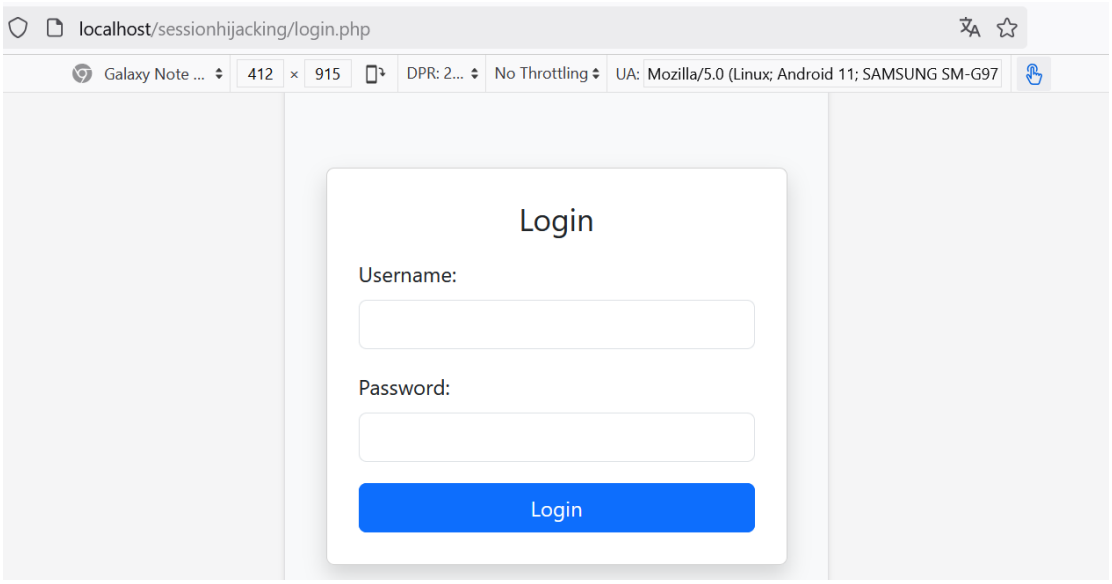
No	Nama Kolom	Type Data
1	IdUserPrimary	Integer (20)
2	UserName	Varchar (30)
3	PassWord	Varchar (50)
4	PIN	Varchar (30)
5	Session	Varchar (50)
6	IPAddress	Varchar (30)

.

Database yang digunakan dalam penelitian ini adalah MySQL dengan nama database sessionsecure. Dalam database ini, terdapat tabel user yang berfungsi sebagai penyimpanan data pengguna. Tabel user memiliki beberapa kolom utama yang digunakan dalam simulasi serangan session hijacking. Kolom IdUserPrimary bertipe data Integer (20) digunakan untuk menyimpan ID pengguna. Kolom UserName bertipe Varchar (30) menyimpan nama pengguna, sedangkan kolom PassWord (50) dan PIN (30), digunakan untuk menyimpan kata sandi dan PIN pengguna. Selain itu, terdapat kolom Session dengan tipe Varchar (50) yang berfungsi menyimpan informasi sesi pengguna, serta kolom IPAddress bertipe Varchar (30) yang merekam alamat IP pengguna. Struktur tabel ini dirancang untuk mendukung penelitian terkait keamanan sesi pengguna dalam sistem berbasis web.

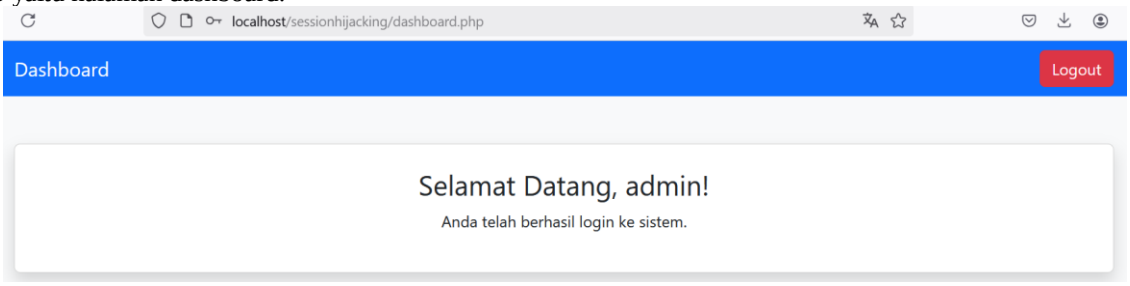
Perancangan Halaman Login, dashboard dan input PIN

Halaman login dirancang untuk membaca username, password, alamat IP dan Session dari user. Data username dan password akan dicocokan dengan data yang telah tersimpan di database, namun untuk data Session dan Data akan disimpan ke dalam database. Berikut ini gambar 4 yaitu gambar halaman login.



Gambar 4. Halaman Login

Setelah login, pengguna akan masuk ke halaman dashboard, data halaman dashboard sendiri merupakan halaman yang membutuhkan data session pengguna, apabila hanya menggunakan session untuk mendapat otoritas kedalam dashboard, maka sistem akan rentan akan serangan session hijacking, oleh sebab itu halaman dashboard dirancang untuk mencocokan session dengan IP Address yang telah tercatat sebelumnya pada saat proses login, dengan demikian hanya user yang melakukan aksi login saja yang dapat mengakses halaman dashboard. berikut ini gambar 5 yaitu halaman dashboard.



Gambar 3. Halaman Dashboard

Pada halaman dashboard sessi dan IP Address akan kembali dicocokan dengan data yang ada pada database, sehingga apabila seseorang masuk ke halaman dashboard dengan IP Address yang berbeda dengan IP Address yang telah tersimpan di database, maka pengguna akan diarahkan ke halaman Input PIN, sehingga proses autentikasi dilakukan Ulang dengan menggunakan PIN yang hanya diketahui oleh pengguna. Apabila pengguna berhasil memasukan PIN dengan benar, maka halaman dashboard akan melakukan update IP Address yang ada di database dengan IP Address baru, namun apabila PIN yang dimasukan salah, maka pengguna akan diarahkan ke halaman login. Berikut ini pseudo code yang menggambarkan proses login, pemeriksaan sessi dan IP Address, dan Iput PIN.

Mulai

Jika sesi pengguna belum ada:

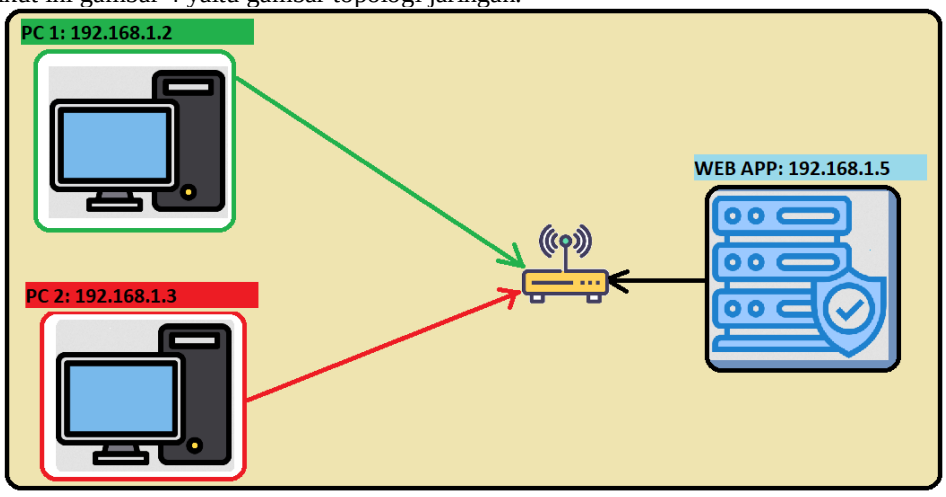
```
        Arahkan ke login
    Ambil data pengguna dari database (IP, sesi, PIN)

Jika IP tidak cocok:
        Tampilkan form PIN
        Jika PIN benar:
            Perbarui IP di database
            Tampilkan "PIN benar, IP diperbarui"
            Arahkan ke dashboard
        Jika PIN salah:
            Arahkan ke halaman login
Selesai
```

Alur yang ditulis menggunakan pseudocode tersebut, dapat dibuat dalam script PHP, script tersebut harus selalu dipanggil pada setiap halaman yang membutuhkan autentikasi, misalnya pada halaman dashboard, pengguna harus melakukan proses autentikasi 1 yaitu dengan username dan password, apabila pengguna tersebut berganti IP Address, maka akan dilakukan proses autentikasi ke 2 yaitu memasukan sebuah PIN, jika PIN yang dimasukan salah, pengguna akan diarahkan ke halaman login.

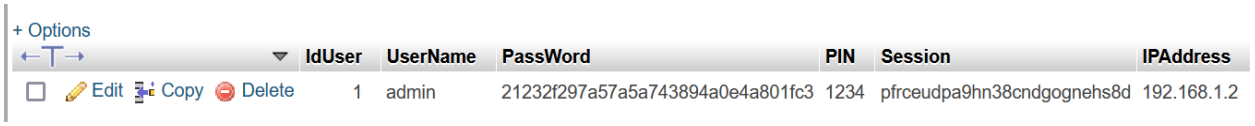
Pengujian Session Hijacking

Simulasi serangan session hijacking dilakukan dengan 2 buah computer, yang terhubung pada satu akses point. Berikut ini gambar 4 yaitu gambar topologi jaringan.



Gambar 4. Topologi Pengujian *Session Hijacking*

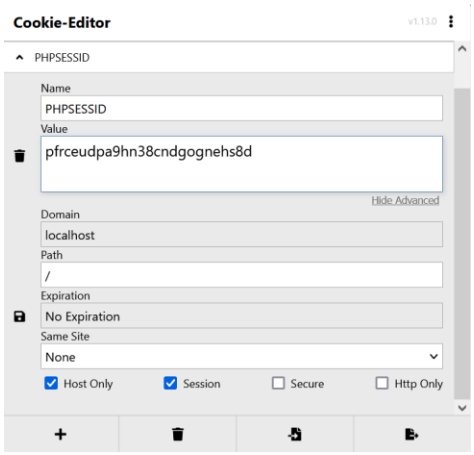
Proses pengujian dilakukan dengan PC 1 berperan sebagai pengguna yang sah dengan alamat IP 192.168.1.2, lalu PC 2 berperan sebagai penyerang dengan alamat IP 192.168.1.3, sedangkan target serangan adalah WEB dengan alamat IP 192.168.1.5. proses diawali dengan PC 1 login ke WEB, maka secara otomatis pengguna pada PC 1 akan diarahkan ke halaman dashboard, bukti keberhasilan pengguna PC 1 login adalah dengan adanya data yang tersimpan pada tabel user. Berikut ini gambar 5 yaitu tampilan pada tabel user.



IdUser	UserName	PassWord	PIN	Session	IPAddress
1	admin	21232f297a57a5a743894a0e4a801fc3	1234	pfrceudpa9hn38cndgognehs8d	192.168.1.2

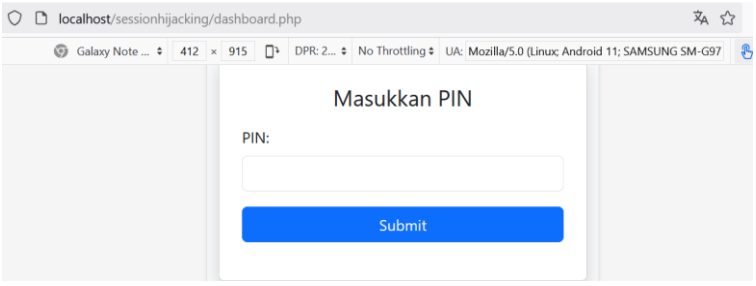
Gambar 5. Tampilan tabel user

Pada gambar 5, terlihat bahwa halaman login menyimpan data sesi (Session) dan alamat IP (IPAddress), dengan demikian pengguna akan diarahkan ke halaman dashboard. Selanjutnya disimulasikan bahwa pengguna yang telah login mengakses halaman yang menicu terjadinya serangan XSS, sehingga sesi dicuri oleh penyerang. Penyerang pada PC 2 memasang sesi tersebut melalui browser dengan memanfaatkan Ekstensi browser Mozilla firefox yaitu Cookie Editor.



Gambar 6. Modifikasi Sesi Dengan Ekstensi Cookie Editor

Pada gambar 6, dijelaskan bahwa penyerangpada PC 2 dengan alamat IP 192.168.1.3 telah memanipulasi sesi browsernya dengan memanfaatkan ekstensi cookie editor, maka apabila dashboard hanya melakukan checking sesi, otomatis penyerang akan berhasil masuk ke dashboard, namun dashboard melakukan proses pencocokan antara Session dan IPAddress, sehingga hanya bermodalkan sesi saja penyerang tidak akan di ijinkan ke halaman dashboard, melainkan penyerang akan diarahkan ke halaman autentikasi PIN. Berikut ini gambar 7 yaitu halaman autentikasi PIN.



Gambar 7. Halaman Autentikasi PIN

Pada gambar 7, penyerang pada PC 2 yang memiliki alamat IP yang berbeda dengan pengguna yang masuk dengan username dan password yang sah, akan diminta untuk memasukan PIN, apabila PIN salah maka pengguna akan diarahkan ke halaman login. Namun jika penyerang juga berhasil mendapatkan PIN pengguna, maka artinya

penyerang akan berhasil mengambil alih sesi dan alamat IP penyerang yaitu 192.168.1.3 akan disimpan ke database, sehingga pengguna yang sah pada PC 1 akan diarahkan ke halaman input PIN.

4 Kesimpulan dan Saran

Kesimpulan

Kesimpulannya, penelitian ini berhasil mengembangkan mekanisme pencegahan serangan session hijacking dengan menggunakan dua faktor autentikasi, yaitu sesi dan PIN. Mekanisme ini efektif untuk mendeteksi perubahan Alamat IP saat sesi aktif dan memaksa pengguna untuk memasukkan PIN jika terdapat ketidaksesuaian. Namun, kelemahan utama dari sistem ini adalah jika web diakses melalui jaringan publik, penyerang dan pengguna yang sah mungkin berada pada jaringan yang sama, sehingga metode ini kurang efektif untuk melawan serangan *Man-in-the-Middle (MITM).*

Saran

Saran untuk penelitian ini adalah memperkuat enkripsi data, terutama untuk sesi dan PIN, guna menghindari serangan yang lebih kompleks seperti Man-in-the-Middle (MITM). Penggunaan protokol HTTPS yang aman juga sangat disarankan untuk melindungi data yang dikirimkan antara pengguna dan server. Selain itu, menambahkan lapisan autentikasi dua faktor seperti OTP atau aplikasi autentikasi dapat lebih meningkatkan keamanan, terutama jika penyerang dan pengguna berada pada jaringan yang sama. Terakhir, penting untuk mengimplementasikan mekanisme pemantauan dan deteksi serangan guna mengidentifikasi pola akses mencurigakan yang dapat menunjukkan adanya upaya serangan..

5 Daftar Pustaka

[1] Hwang, W. S., Shon, J. G., & Park, J. S. (2022). Web session hijacking defense technique using user information. Human-centric Computing and Information Sciences, 12, 16.

[2] Muzammil, M. B., Bilal, M., Ajmal, S., Shongwe, S. C., & Ghadi, Y. Y. (2024). Unveiling Vulnerabilities of Web Attacks Considering Man in the Middle Attack and Session Hijacking. IEEE Access.

[3] Baitha, A. K., & Vinod, S. (2018). Session hijacking and prevention technique. Int. J. Eng. Technol, 7(2.6), 193-198.

[4] Jhanjhi, N. Z., Humayun, M., & Almuayqil, S. N. (2021). Cyber security and privacy issues in industrial internet of things. Computer Systems Science & Engineering, 37(3).

[5] Ogundele, I. O., Akinade, A. O., Alakiri, H. O., Aromolaran, A. A., & Uzoma, B. O. (2020). Detection and prevention of session hijacking in web application management. Int J Adv Res Comput Commun Eng, 9(6), 1-10.

[6] Husin, H. S., & Riduan, F. N. M. (2021). Preventing Data Leakage by Securing Chat Session with Randomized Session ID. Int. J. Commun. Networks Inf. Secur., 13(3).

[7] sri wahyuningsi Manguling, I., & Parenreng, J. M. (2023). Security System Analysis Using the HTTP Protocol Against Packet Sniffing Attacks. Internet of Things and Artificial Intelligence Journal, 3(4), 325-340.

[8] Hasan, M. R., Shuvo, Y. A., & Sakib, J. H. A Review Paper on Session Hijacking Attack.

[9] Shankaramma, N. G. (2023). Methods for Storage Intrusion Mitigation with Data Transport Security Tunnels. Methods, 1(5), 335-341.

[10] Samuel, B., & Somasundaran, V. T. Prevention of Man-in-the-Middle Attacks using Blockchain VPN.