Session hijacking attack

From OWASP

*This is an **Attack**. To view all attacks, please see the Attack Category page.*

Last revision (mm/dd/yy): **08/14/2014**

Description

The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token.

Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

The Session Hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

The session token could be compromised in different ways; the most common are:

- Predictable session token;
- Session Sniffing;
- Client-side attacks (XSS, malicious JavaScript Codes, Trojans, etc);

- Man-in-the-middle attack
- Man-in-the-browser attack

Examples

Example 1

Session Sniffing

In the example, as we can see, first the attacker uses a sniffer to capture a valid token session called “Session ID”, then he uses the valid token session to gain unauthorized access to the Web Server.

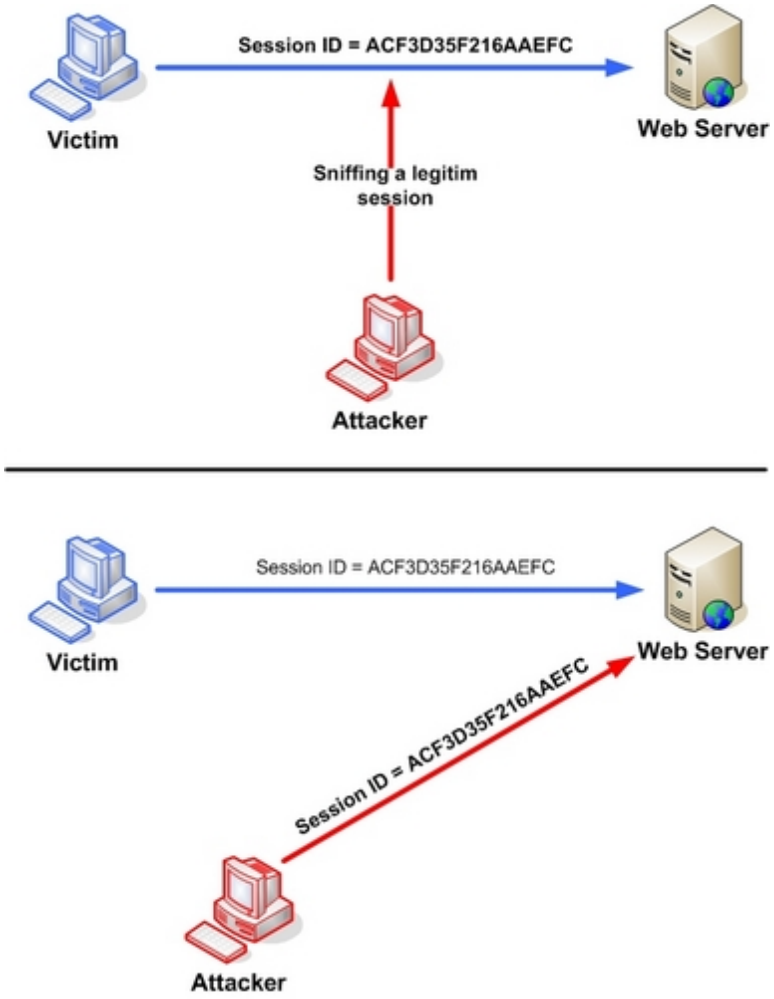

Figure 2. Manipulating the token session executing the session hijacking attack.

Example 2

Cross-site script attack

The attacker can compromise the session token by using malicious code or programs running at the client-side. The example shows how the attacker could use an XSS attack to steal the session token. If an attacker sends a crafted link to the victim with the malicious JavaScript, when the victim clicks on the link, the JavaScript will run and complete the instructions made by the attacker. The example in figure 3 uses an XSS attack to show the cookie value of the current session; using the same technique it's possible to create a specific JavaScript code that will send the cookie to the attacker.

```
<SCRIPT>alert(document.cookie);</SCRIPT>
```

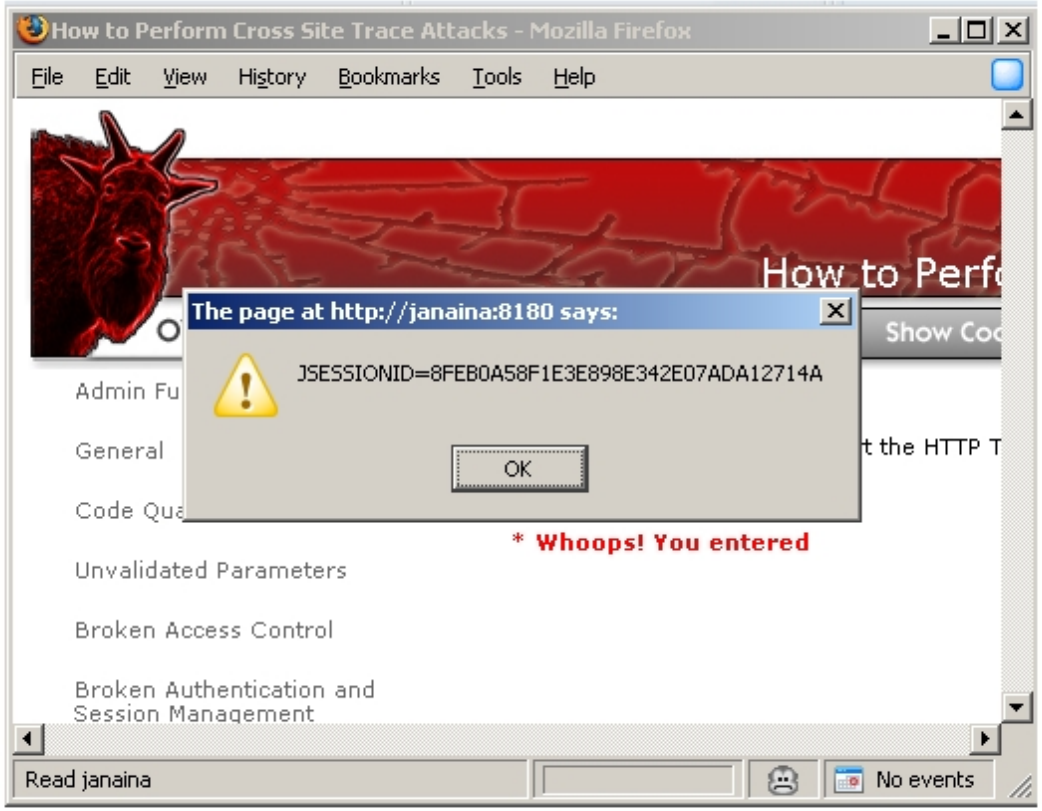

Figure 3. Code injection.

Other Examples The following attacks intercept the information exchange between the client and the server:

- Man-in-the-middle attack
- Man-in-the-browser attack

Related Threat Agents

- Category: Authorization

Related Attacks

- Man-in-the-middle attack
- Man-in-the-browser attack
- Session Prediction

Related Vulnerabilities

- Category:Input Validation Vulnerability

Related Controls

- Category:Session Management

References

- http://www.iss.net/security_center/advice/Exploits/TCP/session_hijacking/default.htm
- http://en.wikipedia.org/wiki/HTTP_cookie

Retrieved from "https://www.owasp.org/index.php?title=Session_hijacking_attack&oldid=180580"
Categories: OWASP ASDR Project | Exploitation of Authentication | Attack

---