YGN ETHICAL HACKER GROUP

Article

WHY SESSION PROTECTION FAILS

By

d0ubl3_h3lix

Tue Jan 29 2008

Web applications usually reply on SESSION cookies to prevent some kinds of flooding data. It can only protect an average bad guy. This is because Session data is submitted to web application as an additional header. The application receives and manipulates that header information as intended by its developer. For example, if a user has submitted the same form information twice, the session information has also been set twice when submitted. The application alerts user not to submit the data twice by interpreting on the session data value.

However, bad guys don't always use browsers for viewing web sites. They can disable the session. They can easily bypass the session protection. When they want to flood the site, they use automated tools to submit millions of packets to your web applications.

The countermeasure is to use capcha image. Use a database to prevent any same information by setting integrity rule like UNIQUE. Or the tricky protection is:

```
Check the Session Data

If The Session Data Is Empty OR Is Not Valid Then

        Deny Form Data Submission
        Log the Attempt

End If
```

I have read a white paper[1] about using session which can cause session exhaustion in highly traffic web sites. I agree with this. In world-widely-popular amusement and entertainment sites, there are millions of users at the same time every day. For those web sites, session protection may cause denial of service to their users due to session collisions.

[1] To be honest, I didn't actually remember the source and name of that white paper.