RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -19

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Cross-site Scripting (XSS)
- “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

Cross-site Scripting (XSS)

❑Cross-site Scripting (XSS) is a client-side code injection attack. The attacker aims to execute malicious scripts in a web browser of the victim by including malicious code in a legitimate web page or web application. The actual attack occurs when the victim visits the web page or web application that executes the malicious code. The web page or web application becomes a vehicle to deliver the malicious script to the user's browser. Vulnerable vehicles that are commonly used for Cross-site Scripting attacks are forums, message boards, and web pages that allow comments.

❑A web page or web application is vulnerable to XSS if it uses unsanitized user input in the output that it generates. This user input must then be parsed by the victim's browser. XSS attacks are possible in VBScript, ActiveX, Flash, and even CSS. However, they are most common in JavaScript, primarily because JavaScript is fundamental to most browsing experiences.

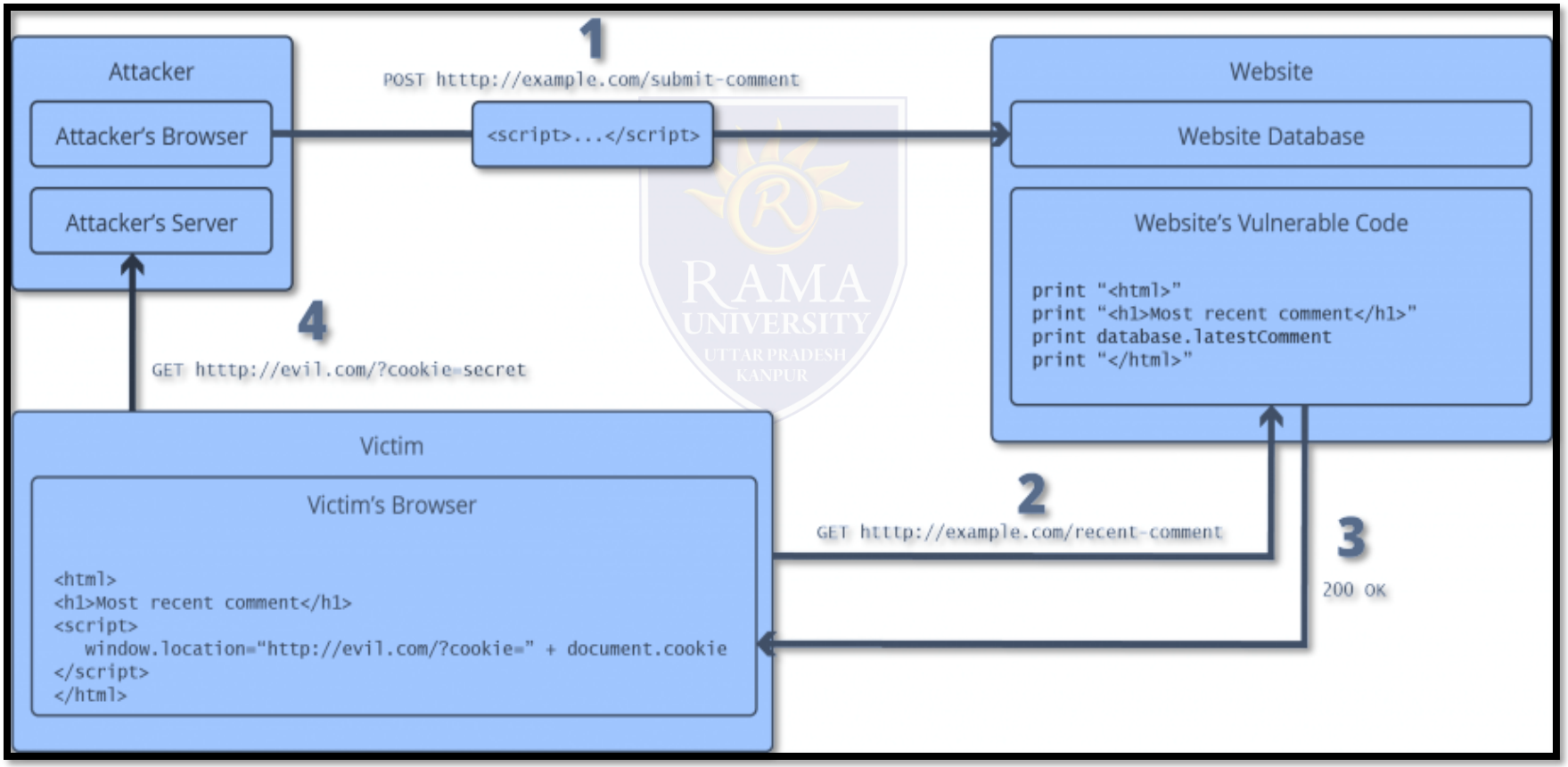
“Isn’t Cross-site Scripting the User’s Problem?”

❑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.



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

1. What is the ethics behind training how to hack a system?
   a) To think like hackers and know how to defend such attacks
   b) To hack a system without the permission
   c) To hack a network that is vulnerable
   d) To corrupt software or service using malware

2. Performing a shoulder surfing in order to check other's password is _____ ethical practice.
   a) a good
   b) not so good
   c) very good social engineering practice
   d) a bad

3. _____ has now evolved to be one of the most popular automated tools for unethical hacking.
   a) Automated apps
   b) Database software
   c) Malware
   d) Worms

4. Leaking your company data to the outside network without prior permission of senior authority is a crime.
   a) True
   b) False

5. _____ is the technique used in business organizations and firms to protect IT assets.
   a) Ethical hacking
   b) Unethical hacking
   c) Fixing bugs
   d) Internal data-breach

REFERENCES

- https://whatis.techtarget.com/definition/input-validation-attack\
- https://www.acunetix.com/websitesecurity/cross-site-scripting/