



VSR://EDU/SVS

Security of Distributed Software

SS 2020 – 4. Tutorial

Valentin Siegert M.Sc.

Shovra Das M.Sc.

VSR.Informatik.TU-Chemnitz.de

Task 1

What is Cross-Site Scripting (XSS)?

Cross-Site Scripting attacks are a type of injection problem, in which malicious scripts are injected into the otherwise benign and trusted web sites

The Open Web Application Security project

What is achievable with XSS?

- Spy out data (incl. Cookie / Session variables)
- Altering website
- Phishing

Place *guestbook.php* into your PHP delivering server folder from tutorial 3. Script creates simple guestbook app with XML data storage.

- a. Create with XSS a button, which, if pressed, changes color of the page header.
- b. Create with XSS a button, which, if pressed, changes the targets of the anchors (not the labels) to <http://google.de>.
- c. Are actions a and b possible without buttons?

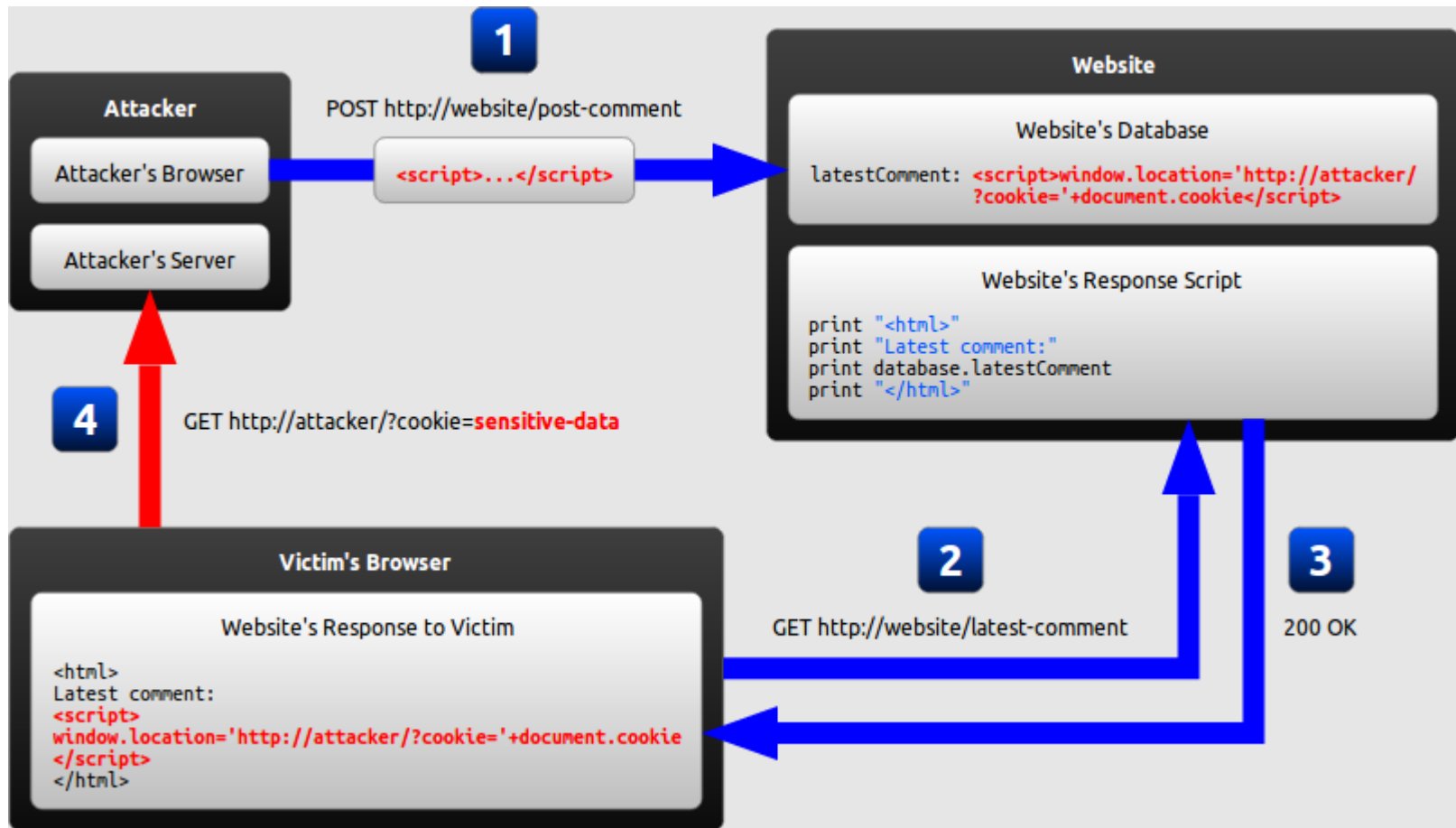
Which defense methods against XSS do you know?

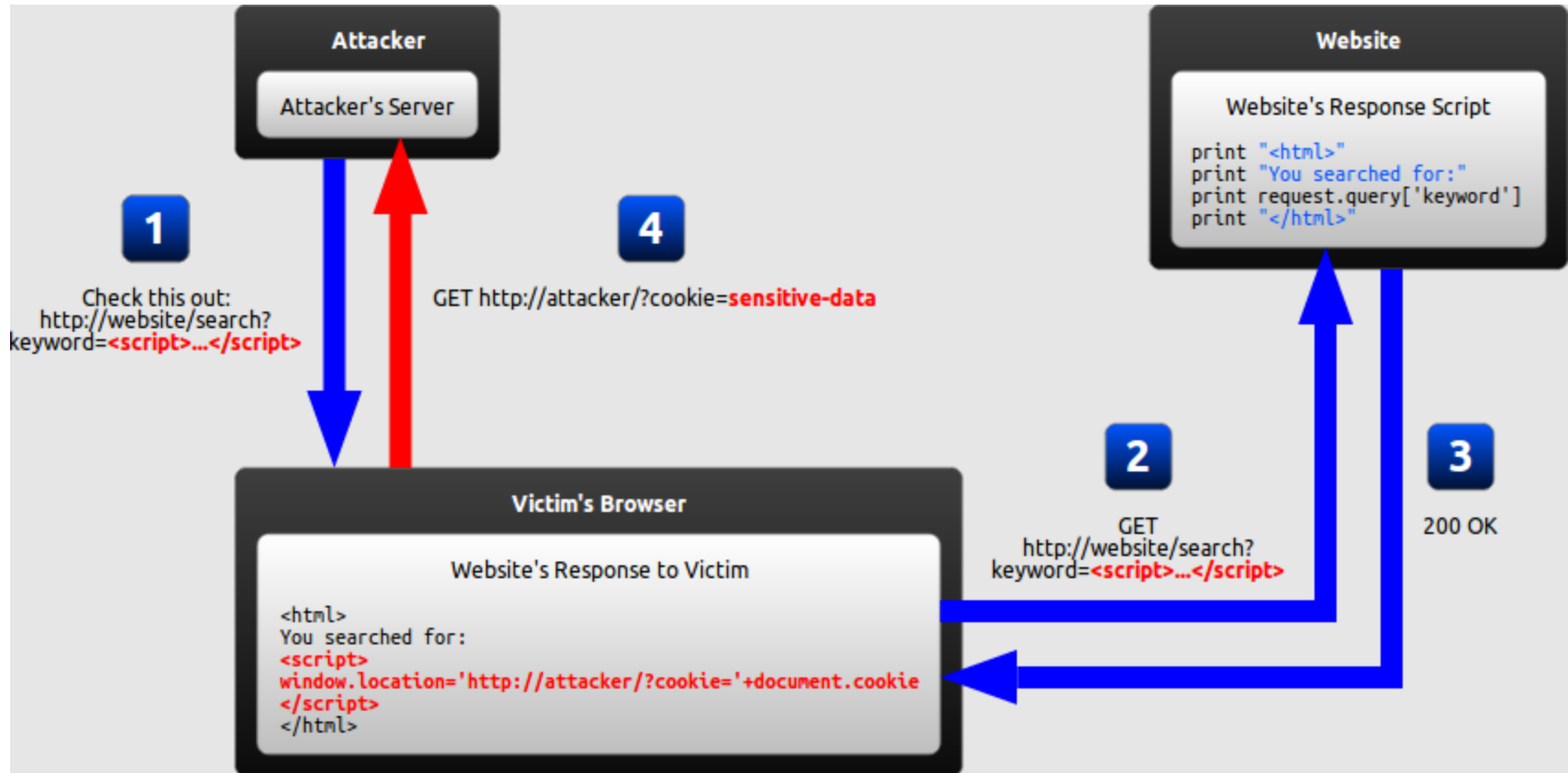
- Validate user inputs
- Encode output
- Use **HttpOnly** flag for cookies
- Deactivate JavaScript in the browser
- Web Application Firewalls

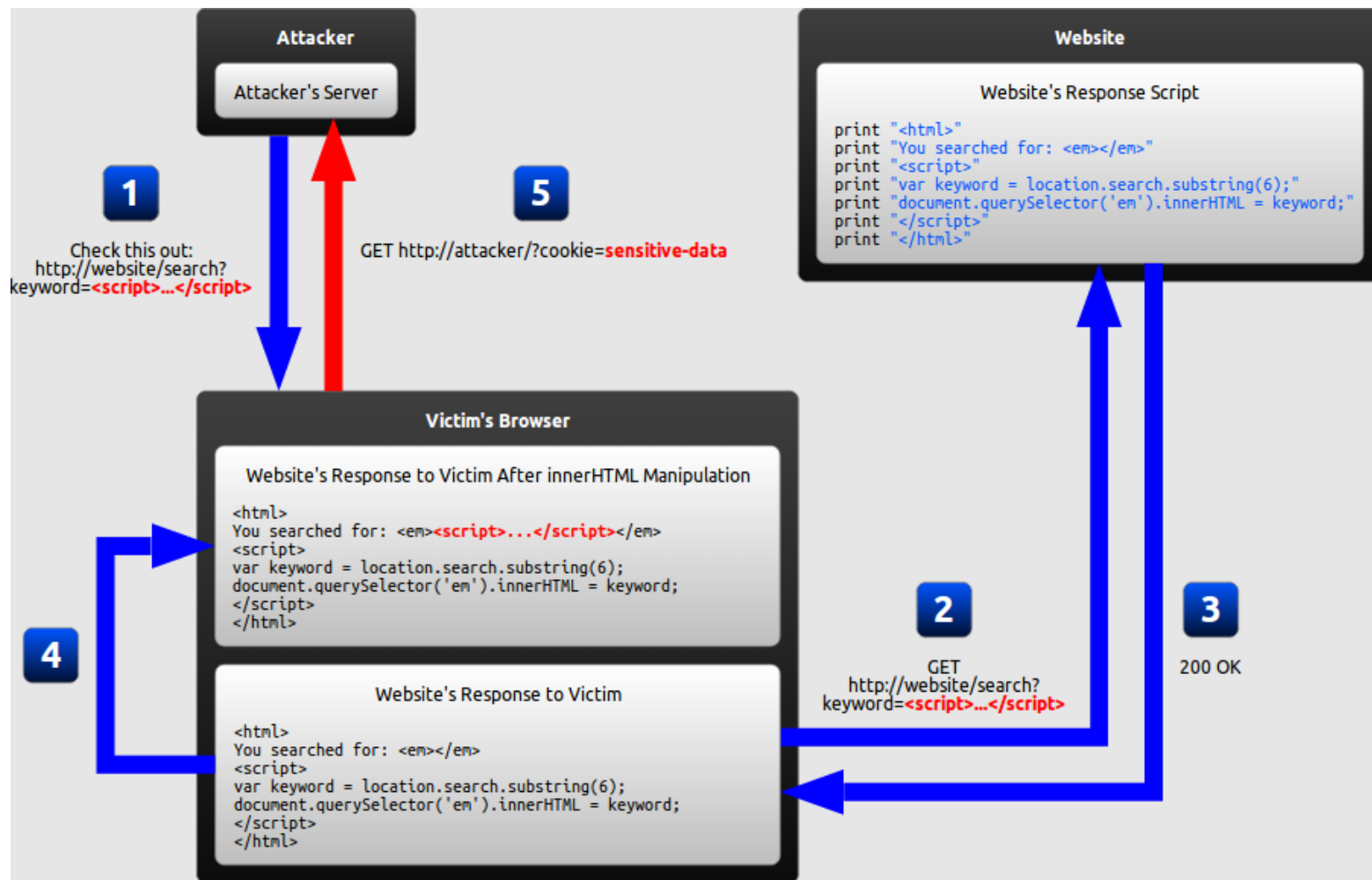
2 Task 2

What is the difference between *stored*, *reflected* and *DOM-based* XSS attacks?

- Stored XSS Attacks
 - Malicious code stored on server side – forums, guestbooks etc.
- Reflected XSS Attacks
 - Malicious code delivered to the client, but not stored on the server side
- DOM-based Attacks
 - Malfunction of normal code behavior via manipulated parameters







The page <http://mytuc.org/jmcp> simulates a search engine, which remembers 5 search queries entered last.

How can an attacker spy on the search history of a user?

<http://mytuc.org/zhkq>

3 Task 3

At <http://mytuc.org/sgdf> one can find a page, which loads two further pages into iframes and below a form to evaluate Javascript.

- a. What can be entered to read the H1-elements of both iframes?
- b. For which frame do your commands work and why (keyword Same-Origin-Policy)?
- c. What is the goal of the security measure behind?

4 Task 4

How a Cross-Site-Request-Forgery (CSRF) attack takes place?

Assumed, a user has logged in into <http://mytuc.org/vwfx>.

How can one log out the user against his will using the guestbook from the task 1?



VSR

Your feedback on today's session:



mytuc.org/tgxs

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.Informatik.TU-Chemnitz.de