Cross-Site Scripting

The most prevalent web application risk

Helen Gao, CISSP

Q: What damage can XSS cause?

A: Attacker can execute scripts in a victim’s browser to hijack user sessions, deface websites, insert hostile content, redirect users, hijack the user’s browser using malware, etc.

Q: What kind of applications are vulnerable to XSS attacks?

A: Whenever it takes untrusted user data and sends it to a web browser.

- Samy worm attacked MySpace

- *WASC* revealed that 58% of the applications are vulnerable to XSS.

Types of XSS

1. Reflected XSS
2. Stored XSS
3. DOM based XSS

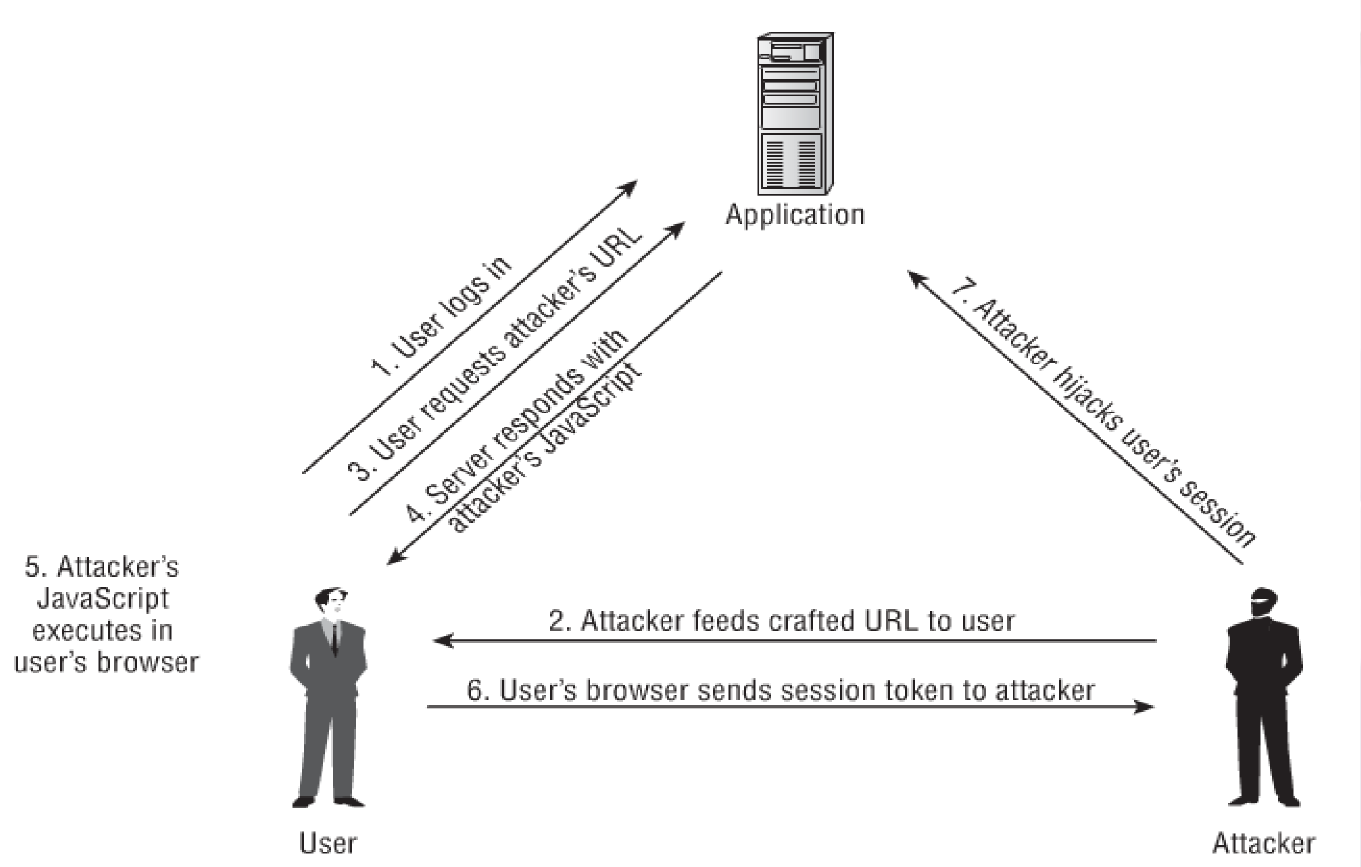
Terminology

- Active content – Malicious data embedded in user input which should always be text
- Malicious data – Attacker embedded JavaScript in user input
- Injected code – same as malicious data
- Payload – same as malicious data
- Script – JavaScript
- User input – User supplied data like recipient email address
- Untrusted data – same as user data

Reflected XSS

Injected code is reflected off the web server

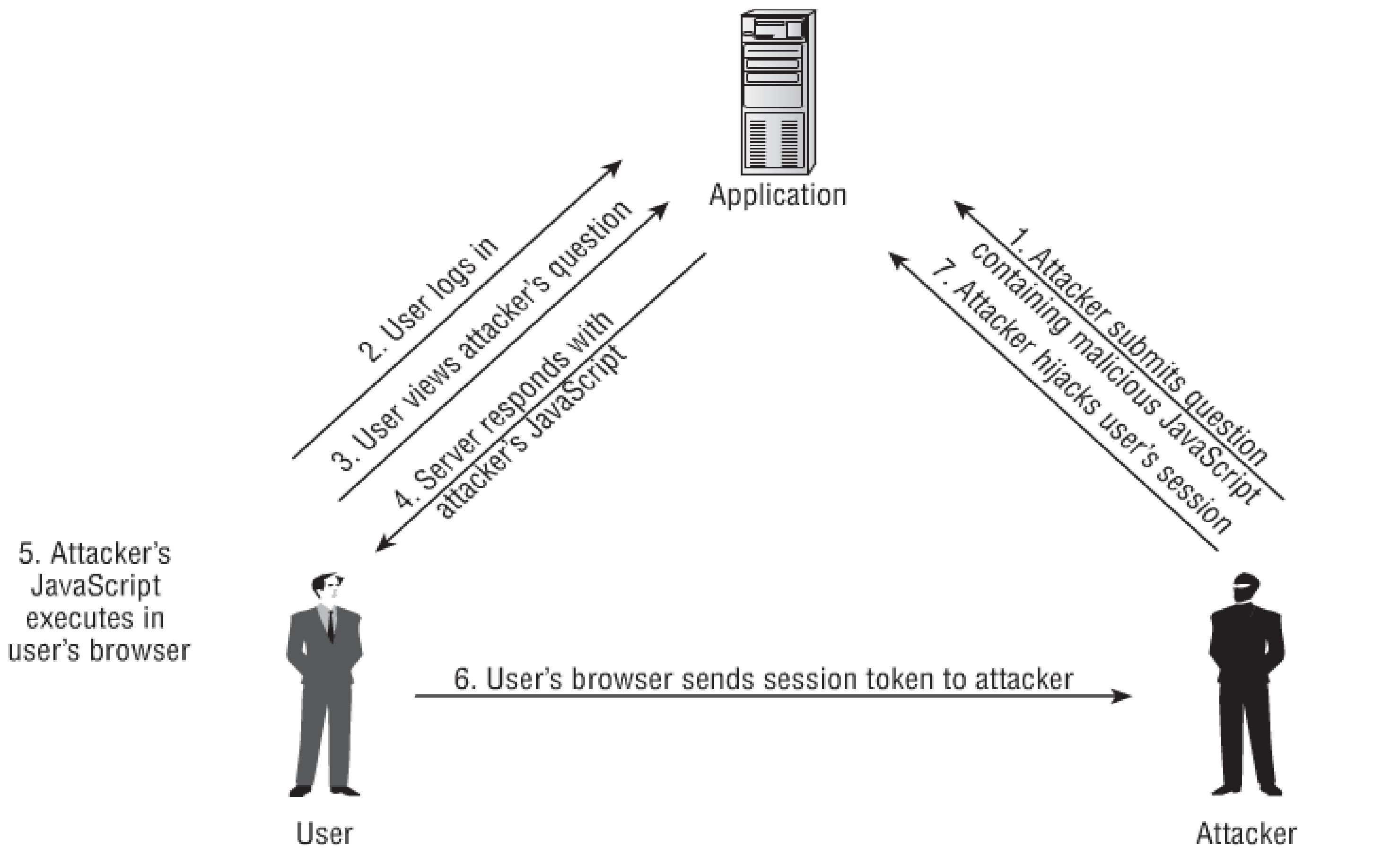
Reflected XSS Attack Sequence


Application
1. User logs in
3. User requests attacker's URL
4. Server responds with attacker's JavaScript
7. Attacker hijacks user's session
5. Attacker's JavaScript executes in user's browser
2. Attacker feeds crafted URL to user
6. User's browser sends session token to attacker
User
Attacker

Stored XSS

Injected code is permanently stored on the target servers

Stored XSS Attack Sequence


Application
1. Attacker submits question containing malicious JavaScript
2. User logs in
3. User views attacker's question
4. Server responds with attacker's JavaScript
5. Attacker's JavaScript executes in user's browser
6. User's browser sends session token to attacker
7. Attacker hijacks user's session
User
Attacker

Review of Reflected and Stored XSS

An example of injected code:
<script><alert(Document.cookies)</script>

How to Prevent Stored and Reflected XSS?

1. Validate input – be very strict

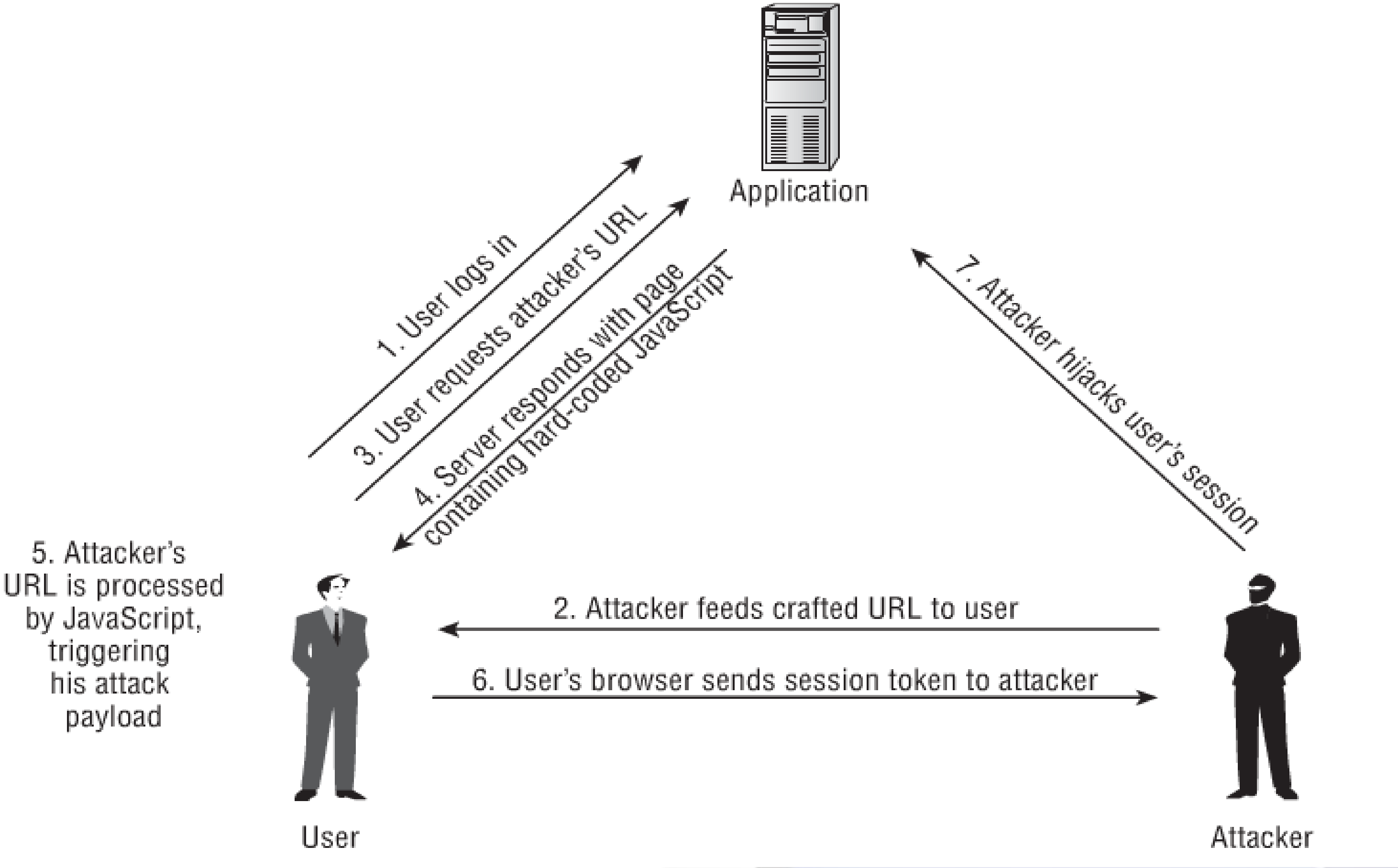
2. Validate output – use untrusted data for display only

3. Eliminate dangerous insertion points

DOM Based XSS

- XSS of the third kind
- It changes the DOM environment instead of the page

DOM Based XSS Attack Sequence


Application
1. User logs in
3. User requests attacker's URL
4. Server responds with page containing hard-coded JavaScript
7. Attacker hijacks user's session
5. Attacker's URL is processed by JavaScript, triggering his attack payload
2. Attacker feeds crafted URL to user
6. User's browser sends session token to attacker
User
Attacker

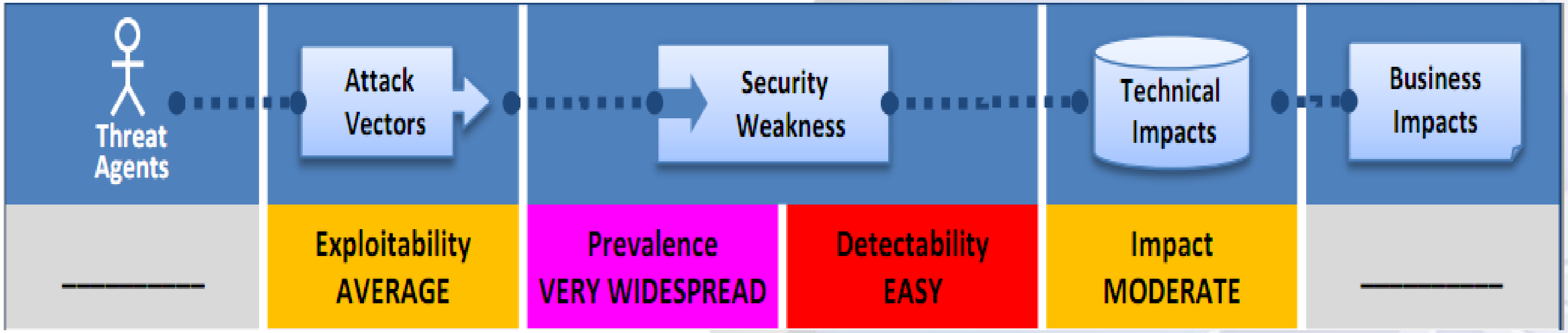
How to Prevent DOM Based XSS?

1. Validate input

2. Avoid using untrusted data in sensitive client side actions

3. Analyze and harden client side JavaScript code

What does OWASP say about XSS?



Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
________	Exploitability AVERAGE	Prevalence VERY WIDESPREAD	Detectability EASY	Impact MODERATE	________

What is the OWASP Top 10?

What is OWASP?

A. Not-for-profit worldwide charitable organization
B. Everyone is free to participate
C. All materials are available under a free and open software license

What do people say about OWASP?

Center for Internet Security (CIS)

Federal Chief Information Officers (CIO) Council

Federal Financial Institutions Examination Council (FFIEC)

Federal Trade Commission (FTC)

Institute of Electrical and Electronics Engineers (IEEE)

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)

National Cyber Security Division

National Institute of Standards and Technology (NIST)

National Security Agency/Central Security Service (NSA)

Payment Card Industry Security Standards Council (PCI SSC)

World Wide Web Consortium (W3C)

What is the OWASP Top 10?

- Top ten most critical web application risks
- An awareness document
- Represents a broad consensus
- Latest version 2010

How do these companies use OWASP Top 10?

Microsoft - As a way to measure the coverage of their SDL and improve security. Also to show how "T10 threats are handled by the security design and test procedures of Microsoft"

NSA - in their developer guidance on web application security

PCI Council - as part of the Payment Card Industry Data Security Standard (PCI DSS). Section 6.5 "*the current OWASP Guide at the time of the assessment should be used. .. Verify that developers are knowledgeable about secure coding techniques.* "

Oracle - for developer awareness

WhiteHat - as a way to explain the coverage of their service

Resources

1. *OWASP Top 10*
2. *OWASP Live CD*

Review Question 1

What is the standard “signature” in an application’s behavior that can be used to identify most instances of XSS vulnerabilities?

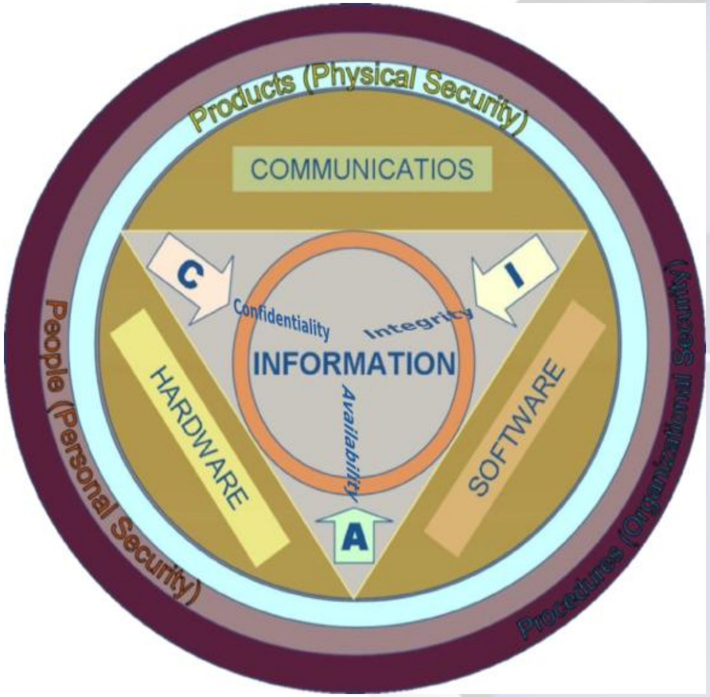
Answer: User-supplied input is returned unmodified within the application’s response to that input.

Review Question 2

Q: You discover a reflected XSS vulnerability. How could it be used to compromise an authenticated session within the application?

A: Arbitrary JavaScript execution within the context of the authenticated user's session.

"The bad guys have to be right only once. The good guys have to be right all the time."


Products (Physical Security)
COMMUNICATIOS
C
I
Confidentiality
Integrity
INFORMATION
Availability
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

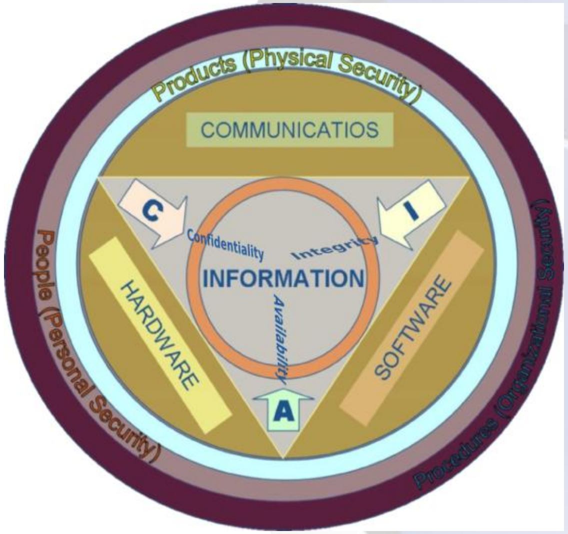
Conclusion

1. XSS is the most prevalent web application security flaw

2. XSS is easy to detect

3. XSS can be defeated

*"The bad guys have to be right only once.
The good guys have to be right all the time."*


Products (Physical Security)
COMMUNICATIOS
C
I
Confidentiality
Integrity
INFORMATION
Availability
A
HARDWARE
SOFTWARE
People (Personal Security)
Procedures (Organizational Security)

Acknowledgement

- *Various sources in OWASP.org*
- *The Web Application Hacker's Handbook: Detecting and Exploiting Security Flaws by Dafydd Stuttard & Marcus Pinto*

Questions?