Welcome to the CoGrammar

XSS (Cross Site Scripting)

The session will start shortly...

Questions? Drop them in the chat. We'll have dedicated moderators answering questions.

Cyber Security Session Housekeeping

- The use of disrespectful language is prohibited in the questions, this is a supportive, learning environment for all - please engage accordingly. **(Fundamental British Values: Mutual Respect and Tolerance)**
- No question is daft or silly - **ask them!**
- There are **Q&A sessions** midway and at the end of the session, should you wish to ask any follow-up questions.
- If you have any questions outside of this lecture, or that are not answered during this lecture, please do submit these for upcoming Academic Sessions. You can submit these questions here: [Questions]()

Cyber Security Session Housekeeping cont.

- For all **non-academic questions**, please submit a query: www.hyperiondev.com/support

- We would love your **feedback** on lectures: [Feedback on Lectures]()

- Find all the lecture **content** in you [Lecture Backpack]() on GitHub.
- If you are hearing impaired, please kindly use your computer's function through Google chrome to enable captions.

Safeguarding & Welfare

We are committed to all our students and staff feeling safe and happy; we want to make sure there is always someone you can turn to if you are worried about anything.

If you are feeling upset or unsafe, are worried about a friend, student or family member, or you feel like something isn't right, speak to our safeguarding team:

Ian Wyles
Designated Safeguarding Lead

Simone Botes

Nurhaan Snyman

Rafiq Manan

Ronald Munodawafa

Tevin Pitts

Scan to report a safeguarding concern

or email the Designated Safeguarding Lead:
Ian Wyles
safeguarding@hyperiondev.com

Stay Safe Series:

Mastering Online Safety One week at a Time

While the digital world can be a wonderful place to make education and learning accessible to all, it is unfortunately also a space where harmful threats like online radicalization, extremist propaganda, phishing scams, online blackmail and hackers can flourish.

As a component of this BootCamp the *Stay Safe Series* will guide you through essential measures in order to protect yourself & your community from online dangers, whether they target your privacy, personal information or even attempt to manipulate your beliefs.

Security Tip

Limit user permissions to the minimum required for their roles. By applying the principle of least privilege, you reduce the risk of unauthorized access or accidental data exposure, even if a breach occurs."

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar

XSS (Cross Site Scripting)

December 2024

Learning Objectives & Outcomes

- Define Cross-Site Scripting (XSS) and identify its common types (Reflected and stored).
- Explain the impact of XSS attacks on web applications and user data.
- Demonstrate how XSS vulnerabilities can be exploited by crafting basic attack payloads.
- Examine a vulnerable web application to identify potential entry points for XSS attacks.
- Propose and implement mitigation strategies to secure a web application against XSS vulnerabilities.

Polls

Please have a look at the poll notification and select an option.

Which of the following best describes your current understanding of how XSS attacks work?

a) I have never heard of XSS attacks.

b) I have a basic idea but cannot explain it.

c) I understand the concept but have never seen or exploited an XSS vulnerability.

d) I can explain and demonstrate how XSS attacks work.

Polls

Please have a look at the poll notification and select an option.

What do you think is the primary reason XSS vulnerabilities occur in web applications?

a) Poor server configuration

b) Lack of input validation and output encoding

c) Weak passwords

d) Using outdated libraries and frameworks

Introduction to Cross-Site Scripting(XSS)

- **Definition:**
  - Cross site scripting (XSS) is a type of security vulnerability where attackers inject malicious scripts into trusted websites. The scripts are then executed in the victim’s browser, allowing attackers to steal sensitive information, hijack user sessions, or perform other malicious activities.

Types of XSS

- **Reflected XSS:**
  - Occurs when malicious scripts are reflected off a web server.
  - Example: Attack payload is embedded in a URL and executed when the victim clicks on it.

Types of XSS

- **Stored XSS:**
  - Malicious scripts are stored on a server and displayed to users later.
  - Example: Injecting malicious <script> tag into a comment section that is displayed to all visitors.

Impact of XSS

- **User session hijacking:** Stealing cookies or session tokens
- **Phishing:** redirecting users to malicious websites
- **Defacement:** Altering website appearance
- **Data theft:** Exfiltrating sensitive user data

Detecting XSS

- **Manual Testing:**
  - Inject common XSS payloads like <script>alert(‘XSS’)</script> in input fields.
- **Automated tools:**
  - Tools like Burp suite, OWASP ZAP, or Acunetix can detect XSS vulnerabilities.

Mitigation strategies

- **Input validation and sanitization:**
  - Validate input data against a whitelist of acceptable characters.
  - Sanitize inputs by escaping special characters.
- **Output Encoding**
  - Encode output using HTML or Javascript-specific encoding
- **Content Security policy (CSP)**
  - Implement CSP to restrict script execution from unauthorized sources.

Mitigation strategies

- **Use prepared statement:**
    - For database queries, use parameterized queries to prevent script injection
- **HTTPOnly and secure Cookies:**
    - Prevent client-side access to cookies using the HttpOnly attribute
- **Disable dangerous features:**
    - Avoid eval() or innerHTML for user-supplied input.

Polls

Please have a look at the poll notification and select an option.

What is a potential consequence of an XSS attack?

a) Defacing a website

b) Stealing user session data

c) Redirecting users to malicious websites

d) All of the above

CoGrammar

Polls

Please have a look at the poll notification and select an option.

Which method is the MOST effective to prevent XSS?"

a) Using HTTP headers

b) Avoiding user input

c) Input validation and output encoding

d) Increasing server memory

CoGrammar

Questions and Answers

CoGrammar

Thank you for attending

SKILLS FOR LIFE
SKILLS BOOTCAMPS

Department for Education

CoGrammar