



Recent Announcements

	<u>Project Sign-up Sheet</u> (https://jhu.instructure.com/courses/49399/discussion_topics/594754) All, Please find the project sign-up sheet below: https://docs.google.com/spreadsheets/d/1zyj9f8xh...	Posted on: Aug 29, 2023, 3:26 PM
	<u>Paper Presentation Sign-up Sheet</u> (https://jhu.instructure.com/courses/49399/discussion_topics/594753) All, As discussed in class, please find the paper presentation sign-up sheet below. https://docs.google.com/spreadsheets/d/1zyj9f8xh...	Posted on: Aug 29, 2023, 3:25 PM

EN.601.640.01.FA23 Web Security

Computer Science EN.601.340/440/640

Web Security

Fall, 2023 (3 credits, E)

Instructor

Professor Yinzhi Cao, yinzhi.cao@jhu.edu (<mailto:yinzhi.cao@jhu.edu>), www.cs.jhu.edu/~yzcao (<http://www.cs.jhu.edu/~yzcao>)

Office: Malone 305, 410-516-6718

Office hours: Thursdays 1:30–2:30 pm and by appointment

Teaching Assistant

Bo Hui

Office: Malone 360

Office hours: Wednesday 8:00–9:00 am

Email: bo.hui@jhu.edu (<mailto:bo.hui@jhu.edu>) (<mailto:mkang31@jhu.edu>)

JianJia Yu

Office: Malone 360

Office Hours: Wednesday 2:00-3:00pm


Email: jyu122@jhu.edu (<mailto:jyu122@jhu.edu>)

(<mailto:yc.yang@jhu.edu>)

Mingqing Kang

Office: Malone 360 (357)

Office Hours: Tuesdays 1:30-2:30 pm (in person) or by appointment only (Zoom)

Zoom: <https://JHUBBlueJays.zoom.us/j/96052151065?pwd=TmJ0Qjg0U3FTUUJ0NS9SQVAzUUt1QT09> 
(<https://JHUBBlueJays.zoom.us/j/96052151065?pwd=TmJ0Qjg0U3FTUUJ0NS9SQVAzUUt1QT09>)

Email: mkang31@jhu.edu (<mailto:mkang31@jhu.edu>)

Kecheng An

Office Hours (Zoom): Tuesday 3:30-4:30 pm

Zoom: <https://JHUBBlueJays.zoom.us/j/6187477726>  (<https://JHUBBlueJays.zoom.us/j/6187477726>)

Email: kan9@jhu.edu (<mailto:kan9@jhu.edu>)

Zhengyu Liu

Office: Malone 360

Office Hours (Zoom): Tuesday 8:00 pm - 10:00 pm

Zoom: <https://JHUBBlueJays.zoom.us/my/jackfromeast.zoom>  (<https://JHUBBlueJays.zoom.us/my/jackfromeast.zoom>)

Email: zliu192@jhu.edu (<mailto:zliu192@jhu.edu>)

Meetings

Tuesday, Thursday, noon–1:15 pm, Gilman 132

Textbook

N/A; See canvas

Online Resources

Please log in to Canvas for all materials related to this course.

Course Information

- This course begins with reviewing basic knowledge of the World Wide Web, and then exploring the central defense concepts behind Web security, such as same-origin policy, cross-origin resource sharing, and browser sandboxing. It will cover the most popular Web vulnerabilities, such as cross-site scripting (XSS) and SQL injection, as well as how to attack and penetrate software with such vulnerabilities. Students will learn how to detect, respond, and recover from security incidents. Newly proposed research techniques will also be discussed.
- **Prerequisites**

Data Structure (600/601.226)

- **Elective or Selective Elective**

Course Goals

Specific Outcomes for this course are that

- Students will have an overall knowledge of Web security threats & vulnerabilities.
- Students will learn techniques & tools for detecting, responding to, and recovering from security incidents.
- [Graduate students] Students will learn how to critique others' papers in this area and present own ideas/views via written technical reports.

Course Topics

- WWW and JavaScript
- Cross-site Scripting (XSS)
- SQL Injection
- Prototype Pollution
- Same-origin Policy (SOP)
- Browser Sandboxing

Course Expectations & Grading

Grades will be based on:

- Graduate students: Homework (30%), Paper Summary (5%), Class Participation (20%), Paper Presentation (15%), and Class Project (30%)
- Undergraduate students: Homework (50%), Class Project (30%), Paper Summaries (10%), and Class Participation (10%)

Important: Homeworks and deliverables are collected at the beginning of class on the due date. If your assignment arrives after this time, it is marked late. Late penalties are 10% for the first 24hrs, 20% for up to 2 days late, 30% for up to 3 days late, 40% for up to 4 days late. No assignment is accepted when it is more than 4 days late.

Paper summaries are due 24 hours before the class. Late penalties are 10% for the first 24hrs, 40% for up to 2 days late. No summary is accepted when it is more than 2 days late.

Presentation slides (for paper and projects) are due 48 hours before the class. Please adhere to the rule. Late penalties are 50% for the first 24hrs.

Paper Summary Format: A paper summary should summarize the paper sufficiently to demonstrate your understanding, should point out the paper's contributions, strengths as well as weaknesses. Think in terms of what makes good research? What qualities make a good paper? What are the potential future impacts of the work? Note that there is no right or wrong answer to these questions. A summary's quality will mainly depend on its thoughtfulness. Restating the abstract/conclusion of the paper will not earn a top grade. In particular, it should cover all of the following aspects:

1. What is the main result of the paper? (One or two sentence summary)

2. What strengths do you see in this paper?
3. What are some key limitations, unproven assumptions, or methodological problems with the work?
4. How could the work be improved?
5. What is its relevance today, or what future work does it suggest?

Paper Presentation: Each presentation will be divided into two teams: presenter and critics. The presenter team (only one student) will present for 15mins, including but not limited to the following facts of the paper:

- What are the compelling motivations for the stated work?
- What are the major contributions over state-of-the-art work in the literature?
- How does the paper achieve their stated goals?

The defense team is welcome to look at and borrow useful contents from the original authors' slide when making their own. The defense team should be well prepared for possible critiques from the offense team.

Each student in the critics team will present for 10mins, including but not limited to:

- What are the limitations in the paper's motivation, e.g., narrow scope?
- What are the technical limitations of the paper? For example, will the technique cause false positives or negatives? If it is a defense paper, can an attacker evade the defense; if it is an attack paper, can the attack be deployed in real-world environment?
- What are the possible improvements or future work of the paper? If you were the authors of the paper, what would you do instead?

Then, both teams will be following up arguments, and then other students will question either team for clarification or add to discussions. The instructor may ask students to comment based on their paper summaries.

Assignments & Readings


They will be posted on the Canvas for this course.





Class Projects



The topics for class projects will be announced in the class.

Tentative Course Schedule

Date	Lectures Topics	Presenter	Reading	Assignment
Tue 8/29	Class overview, motivation and overview of computer security	Dr. Yinzhi Cao		













Thu 8/31	WWW and Web Programming	Dr. Yinzhi Cao		
Tue 9/5	WWW and Web Programming (Cont'd)	Dr. Yinzhi Cao		HW1 Web Programming out
Thu 9/7	WWW Paper Presentation	Defense: Offense:	RuleKeeper: GDPR-Aware Personal Data Compliance for Web Frameworks , IEEE Security and Privacy 2023.	
Tue 9/12	Client-side Web Attacks and Defenses I	Dr. Yinzhi Cao		
Thu 9/14	Client-side Web Attacks and Defenses II	Dr. Yinzhi Cao		
Tue 9/19	Client-side Web Attacks and Defenses Paper Presentation I	Defense: Offense:	The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web , IEEE S&P 2023	HW1 in
Thu 9/21	Client-side Web Attacks and Defenses Paper Presentation II	Defense: Offense:	DiffCSP: Finding Browser Bugs in Content Security Policy Enforcement through Differential Testing  (https://www.ndss-symposium.org/ndss-paper/diffcsp-finding-browser-bugs-in-content-security-policy-enforcement-through-differential-testing/), NDSS 2023	HW2 XSS
Tue 9/26	Server-side Web Attacks and Defenses I	Dr. Yinzhi Cao		
Thu 9/28	Server-side Web Attacks and Defenses II	Dr. Yinzhi Cao		

Tue 10/3	Server-side Web Attacks Paper Presentation I	Defense: Offense:	Silent Spring: Prototype Pollution Leads to Remote Code Execution in Node.js  (https://www.usenix.org/conference/usenixsecurity23/presentation/shcherbakov), USENIX Security 2023.	HW2 in
Thu 10/5	Server-side Web Attacks Paper Presentation II	Defense: Offense:	TeSec: Accurate Server-side Attack Investigation for Web Applications , IEEE Security and Privacy 2023.	HW3 prototype pollution out
Tue 10/10	Browser Security	Dr. Yinzhi Cao		
Thu 10/12	Browser Security Paper Presentation	Defense: Offense:	Isolated and Exhausted: Attacking Operating Systems via Site Isolation in the Browser  (https://www.usenix.org/conference/usenixsecurity23/presentation/gierlings), USENIX Security 2023.	
Tue 10/17	Mid-term Project Presentation			HW3 prototype pollution in
Thu 10/19	Fall Break			
Tue 10/24	SSL and TLS	Dr. Yinzhi Cao		
Thu 10/26	SSL and TLS (Cont'd)	Dr. Yinzhi Cao		
Tue 10/31	SSL and TLS Paper Presentation	Defense: Offense:	Exploring the Unknown DTLS Universe: Analysis of the DTLS Server Ecosystem on the Internet  (https://www.usenix.org/conference/usenixsecurity23/presentation/erinola), USENIX Security 2023.	
Thu 11/2	Social Network Security	Dr. Yinzhi Cao		
Tue 11/7	Social Network Security Paper Presentation	Defense: Offense:	Account Verification on Social Media: User Perceptions and Paid Enrollment  (https://www.usenix.org/conference/usenixsecurity23/presentation/xiao-madelyne), USENIX Security 2023.	HW4 Browser Extension out

Thu 11/9	Online Tracking, WebGL, Privacy and Browser Extension	Dr. Yinzhi Cao		
Tue 11/14	Browser Extension Paper Presentation	Defense: Offense:	Detection of Inconsistencies in Privacy Practices of Browser Extensions , IEEE Security and Privacy 2023.	
Thu 11/16	Password and Authentication	Dr. Yinzhi Cao		HW4 in
Tue 11/21	Holiday			
Thu 11/23	Holiday			
Tue 11/28	Online Tracking Paper Presentation	Defense: Offense:	Defining "Broken": User Experiences and Remediation Tactics When Ad-Blocking or Tracking-Protection Tools Break a Website's User Experience  https://www.usenix.org/conference/usenixsecurity23/presentation/nisenoff-broken), USENIX Security 2023.	
Thu 11/30	Password Paper Presentation	Defense: Offense:	A Large-Scale Measurement of Website Login Policies  https://www.usenix.org/conference/usenixsecurity23/presentation/al-roomi), USENIX Security 2023	
Tue 12/5	Final Project Presentation I			
Thu 12/7	Final Project Presentation II			

Course Summary:

Date	Details	Due
Wed Sep 6, 2023	 9/7 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622908)	due by 11:59am

Date	Details	Due
Mon Sep 18, 2023	 9/19 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622958)	due by 11:59am
Tue Sep 19, 2023	 Assignment 1 (https://jhu.instructure.com/courses/49399/assignments/623167)	due by 11:59am
Wed Sep 20, 2023	 9/21 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622964)	due by 11:59am
Mon Oct 2, 2023	 10/3 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622965)	due by 11:59am
Tue Oct 3, 2023	 Assignment 2: Cross-site Scripting: Attack and Defense (https://jhu.instructure.com/courses/49399/assignments/650988)	due by 11:59am
Wed Oct 4, 2023	 10/5 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622966)	due by 11:59am
Wed Oct 11, 2023	 10/12 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622967)	due by 11:59am
Mon Oct 30, 2023	 10/31 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622969)	due by 11:59am
Mon Nov 6, 2023	 11/7 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622970)	due by 11:59am
Mon Nov 13, 2023	 11/14 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622972)	due by 11:59am
Mon Nov 27, 2023	 11/28 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622973)	due by 11:59am
Wed Nov 29, 2023	 11/30 Paper Summary (https://jhu.instructure.com/courses/49399/assignments/622974)	due by 11:59am