CS357 Intro to Information Security

September 22, 2022 Web Audit Project

Web Audit Project

This is a group project. You will work in **teams of four**. You will be choosing your own groups. Each group will submit a single solution (except for *third deliverable* that will be submitted individually).

The work your group submits must be entirely your group's own work. You may consult with other students about the conceptualization of the project and the meaning of the questions, but you may not look at any part of someone else's solution or collaborate with anyone outside your group. You may consult published references, provided that you appropriately cite them (e.g. with program comments), as you would in an academic paper.

All parts of the project are due via gradescope, following the submission checklist below. Your submission MUST include the following information:

1. List of students in your group
2. List of people you discussed the project with (outside your group)
3. List of references used (online material, course nodes, textbooks, wikipedia, etc.)

If any of this information is missing, at least 20% of the points for the assignment will automatically be deducted from your assignment. See also discussion on plagiarism and the collaboration policy on the course syllabus.

This lab will be administrated by Ivan Izhbirdeev.

1 Introduction

In this project you will choose a website and analyze the client-server communication from the website, in order to understand what information is collected and recorded when users surf the selected website. Your *primary tool* will be the developer tools bundled with the Chrome browser or any other browser of your choice.

You will be analyzing and interacting with production systems in this project. Please make sure you read and understand the rules given below before beginning the assignment. **Failure to follow the rules will result in an automatic F in this course**.

The project has three deliverables:

1. Write-up with choice of website, and analysis of the website's responsible disclosure policy. Each group must choose their own website to audit; you cannot audit the same website as another group. **Due: Sep 30, 2022 at 11:59PM.**

2. Video and text report. Each group will submit a video and a report. **Due: Oct 14, 2022 at 11:59PM.**

3. Capstone report. Each group member will submit an individual report. **Due: Oct 21, 2022 at 11:59PM.**

Administration. The technical details of this project (how to use the browser developer tools, questions about cookies, HTML, JavaScript, presentation of the video or final report, etc) will be administrated by Ivan Izhbirdeev. Issues related to disclosing vulnerabilities will be administered by Prof. Goldberg.

2 Websites

You should select a site from the following list of websites that support bug bounty programs:

https://bugcrowd.com/programs

You may only choose a site that has a responsible disclosure policy and/or a bug-bounty program. If you really want to review a web application that is not on the list, please discuss this with Professor Goldberg during her office hours; if you do this, you should be ready with information about the sites' responsible disclosure program.

3 First deliverable: Signup & Responsible disclosure policy

Each group should pick a different website to analyse. Each group should sign up their team and website:

https://docs.google.com/spreadsheets/d/1M71w_zYoeaeIdMCOCy7oJuJSj7xWjfObycj2SLSUpm4
If your website is already selected by another group, please choose a different one.

Your first deliverable will be a short write-up (no more than 2 pages) containing the following information:

1. Your group members.

2. The name and URL of the main page of the website you will analyze.

3. A link to the site's responsible disclosure policy or bug-bounty program.

4. 2 paragraphs describing the process for disclosing a vulnerability that you might have found on that site, according to the site's responsible policy/bug bounty program. Make sure you describe (1) how you would go about disclosing the vulnerability, (2) what the site commits to do once the vulnerability has been disclosed to them (for example, to fix the vulnerability within X days, to not take actions against the person disclosing the vulnerability, to disclose

the vulnerability on their website or blog, etc.). If you feel like the responsible disclosure policy contains any loopholes that can be used against the security researcher, you should also discuss this in your paragraph. If they are particularly worrying, we encourage you to choose a new site to work on for your project. All statements you make should be supported using direct quotes from the site's terms of service, responsible disclosure policy, bug bounty program, etc.

Submissions. You should submit this as `.pdf` file on gradescope.

4 Second deliverable: Website Analysis

Your task is to prepare **(1) a (up to) 5 min video** and **(2) a 3 page report** your website's privacy and security posture.
This is an open ended project, so, **!!!as long as you follow the rules in Section 4.1!!!**, your video can focus on any issues regarding the website. As usual in this class, **we will be looking for in-depth research, rather than superficial information**. So, in additional to just using browser debugger, try reading on CVEs and/or security papers that are related to vulnerabilities that you discovered. Please include any addition content you used in your final video and report.

Make sure your work covers the following points (we will look for these while grading):

1. Deep technical analysis of the website and its infrastructure using browser debugger. This can include:

   (a) cookies; how many, what domains are they from, what purpose they might serve (eg login, tracking, personalization, something else, what security risks they create? what data is stored in the cookies? Who can access these cookies? Are these Secure Cookies? HTTPOnly cookies? Persistent or Session cookies? What could you learn about a user if you had access to their cookies?

   (b) What URLs are fetched when the site loads? Are any of these URLs offsite? Are these URLs protected with HTTPS? What are these URLs used for and what are the privacy risks? Do these URLs contain any sensitive data?

   (c) tracking pixels; do you find any? to what domains? is there discussion of this in the privacy policy?

   (d) are you able to access the site via HTTP? via HTTPS? on what browsers? do you find mixed HTTP/HTTPS content? what are the implications of what you've found on the site's security posture?

   (e) is the site using HSTS? what are the security implications of this finding?

   (f) do you find any CSRF defenses? on what parts of the site? why are these defenses there and how do these defenses work?

   (g) javascript libraries; is the site using any outdated libraries and if so do they have any security vulnerabilities that concern you?

   (h) Are ads shown to the user? Where are these ads loaded from? Who can display these ads? Can the ads contain javascript? What can an advertiser learn about the user?

   (i) What plug-ins are loaded? Java applets? Flash? ActiveX? what are the security implications of this?

2. Review of the site's privacy policy. What information is the site collecting on its users? How are they sharing this information with third parties? Can you determine who some of these third parties are by reading the privacy policy and using the browser debugger? What is the implication of this privacy policy on the site's individual users?

3. Does this site have a GDPR notice? What sort of notice and how does it implicate cookies and tracking on the site?

4. Review any login flows on the site. How does the site authenticate users? Does it use two-factor authentication, and if so, what kind of two-factor authentication? Are there any security risks associated with the type of two-factor authentication that is used? How does the site allow users to recover lost passwords or lost user names? Do you see any security risks associated with these "recovery" flows?

5. Include external sources (e.g. CVEs, research papers) that are relevant to your analysis.

6. General conclusions you can draw about how this site implicates its users' and visitor's privacy and security. This doesn't have to be all negative! If you find something done right that you feel worth mentioning, do it.

4.1 The Rules

IMPORTANT	In the process of your analysis you may discover surprising results and vulnerabilities. Do not discuss them with anyone outside of your group without first consulting with Professor Goldberg. Failure to do this will result in an automatic F.

As this task involves interacting with a private party's computer systems it is very important that you avoid anything outside of what a normal user would do.

THAT MEANS, YOU CAN LOOK BUT YOU CAN'T TOUCH.

The following rules are guidelines for what we consider a "normal user" would do. But, in doing this lab, you should err on the side of caution. Just because the rules do not say not to do something, this does **not** mean that you can do it.[1]

[1] In Airbud a dog is allowed to play basketball because "there is no rule on the books saying that a Dog cant́ play basketball", we will not accept such an argument. The absence of a rule forbidding a particular action does not imply that it is allowed or condone it in anyway.

1. DO: Use the site as a normal user would, follow links, click buttons, interact.
2. DO: Watch and record what actions the site takes, what it saves to your disk, what URLs it requests, what information it asks from the user.
3. DO: Analyze what data the site has about a user and how it saves this data. Is everything stored on the server, or is some of the data recorded locally in cookies? What sorts of vulnerabilities might this create?
4. DO: Read the responsible disclosure policy for your web applications and make sure not to violate it.
5. DO: Read the site's privacy policy and any associated news media on site privacy, and consider how it affects user privacy.
6. DO NOT: Edit URLS.[2],
7. DO NOT: Change cookies, post javascript or strange characters into forms.
8. DO NOT: Do any thing which violates the law, other users' privacy, the user agreement of the web application, or the code of computing ethics and of Boston University.
9. DO NOT: Attempt to attack the server or client in any way, including but not limited to XSS, CSRF and SQL injection.
10. DO NOT: Save the webpage to disk, and then alter it and load it.
11. DO NOT: Post online or discuss your results with anyone outside your group without first consulting with Professor Goldberg.

4.2 Browser development tools.

Your main tool for this project will be the browser's developer tools, we recommend to use Chrome browser tools:

https://developers.google.com/chrome-developer-tools/

or Firefox's browser developer tools:
https://developer.mozilla.org/en-US/docs/Tools

You can access these tools by right clicking on a page and selecting "Inspect Element"; this will open an interface that allows you inspect the requests, cookies, network traffic, etc. **You must not not use the CONSOLE tab as part of your analysis.**

[2] This may seem harmless, but sometimes it is not. We have seen many examples in class where editing URLs can result in successful SQL or XSS attacks. There have also been instances of production systems being crashed by a user deleting a single field from a URL and requesting it. At least one person has been sentenced to more than 3 years in federal prison for generating malicious URLs and accessing them (weev).

4.3 Submission

You should submit the report as `.pdf` file on gradescope. You report should be 3 pages long. We will allow 4 extra pages for an appendix where you can add sources and images. However, the main content of your analysis should appear in the first 3 pages of your report. Your presentation video must be no longer than 5 minutes long, and incorporate all four groupmates in the presentation.

Your report should include a link to your presentation video (which you can host on your BU google drive or as a private video on YouTube). Also, put a link to your presentation video in the assignment's signup sheet, so your classmates can view it as well.

5 Third deliverable: Capstone

Each *individual* group member is responsible for a short (1 page) capstone report. Watch the submission videos of at least four other groups, and think about common themes you observe about web security, tracking and privacy. Your report should concentrate on common trends in web security and privacy that you can identify from your classmates report.

For some inspiration, you can have a look at a tweetstorm from 2019:
https://mobile.twitter.com/goldbe/status/1190380634243506176

You should seek to answer these questions:

- How much of web traffic is encrypted or not? Is end-to-end encryption being used, or can the provider of the site read all your messages etc?
- What are common tracking practices? Who's doing the tracking? How is tracking executed (cookies, pixels, etc)?
- Common themes in privacy policies?
- What surprises you (or does not surprise you) about privacy and security on the web?

Submissions. You should submit this as `.pdf` file on gradescope idividually.