```
    Text(
    'Simple Statement or URL',
    style: TextStyle(
      color: Colors.blue[200],
    ),
  ),
],

/
(
ons.star,
lor: Colors.blue[500],

t Text('23'),
```

Webapp Security

@devfest

All The Ways Your Webapp Can Get Hacked

And How to Fix Them

```
 style: TextStyle(
   color: Colors.green[200],
 ),
),
```

Google Developer Student Clubs

devfest

University of Toronto

```
s.star,
r: Colors.green[500],

Text('23'),
```

Admin Stuff

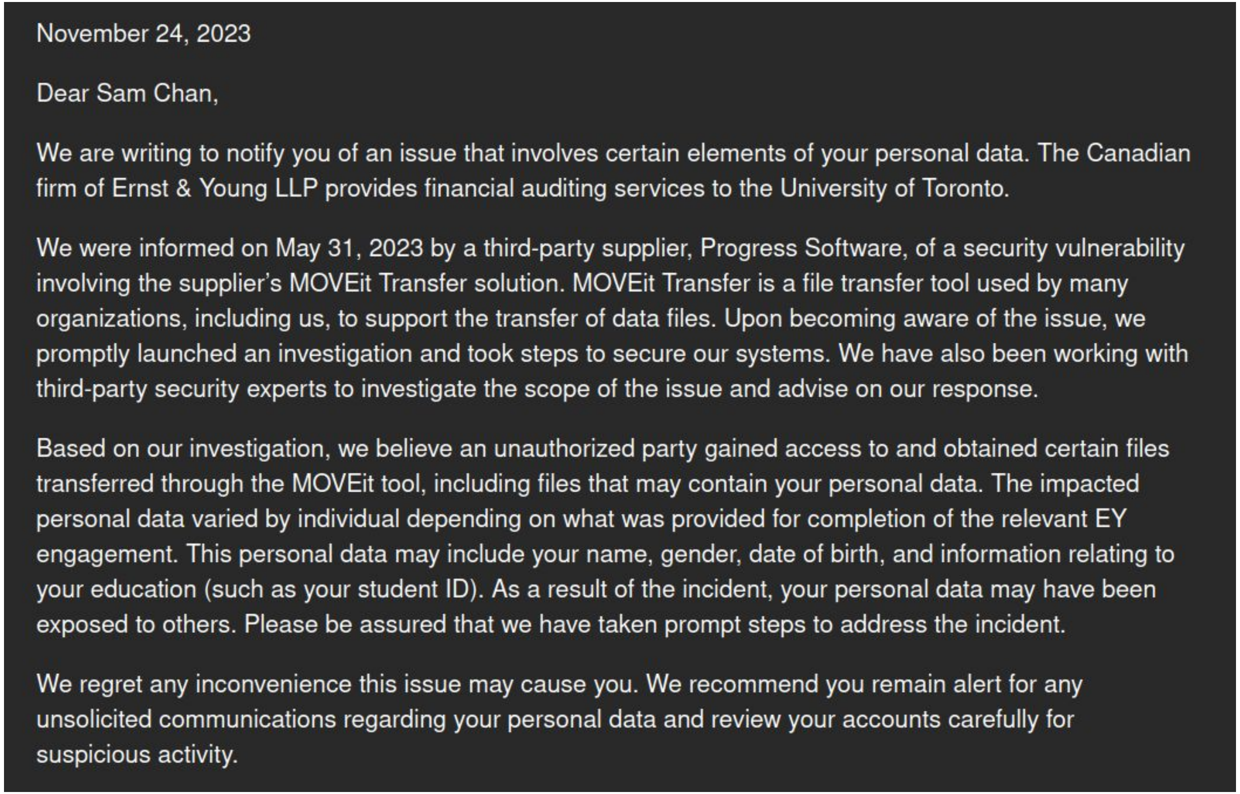
utmgdsc/devfest-web-sec

Today's Agenda

1. Cross-Site Scripting
    a. Reflected XSS
    b. Stored XSS
2. SQL Injection
    a. Unsanitized Inputs
    b. Data Augmentation
    c. Auth Bypass
3. Command Injection
4. Resources

Why is this important?

- Important for future projects
- Important in work
- Responsibility
- Integrity
- Cost (Time and Money)



November 24, 2023

Dear Sam Chan,

We are writing to notify you of an issue that involves certain elements of your personal data. The Canadian firm of Ernst & Young LLP provides financial auditing services to the University of Toronto.

We were informed on May 31, 2023 by a third-party supplier, Progress Software, of a security vulnerability involving the supplier’s MOVEit Transfer solution. MOVEit Transfer is a file transfer tool used by many organizations, including us, to support the transfer of data files. Upon becoming aware of the issue, we promptly launched an investigation and took steps to secure our systems. We have also been working with third-party security experts to investigate the scope of the issue and advise on our response.

Based on our investigation, we believe an unauthorized party gained access to and obtained certain files transferred through the MOVEit tool, including files that may contain your personal data. The impacted personal data varied by individual depending on what was provided for completion of the relevant EY engagement. This personal data may include your name, gender, date of birth, and information relating to your education (such as your student ID). As a result of the incident, your personal data may have been exposed to others. Please be assured that we have taken prompt steps to address the incident.

We regret any inconvenience this issue may cause you. We recommend you remain alert for any unsolicited communications regarding your personal data and review your accounts carefully for suspicious activity.

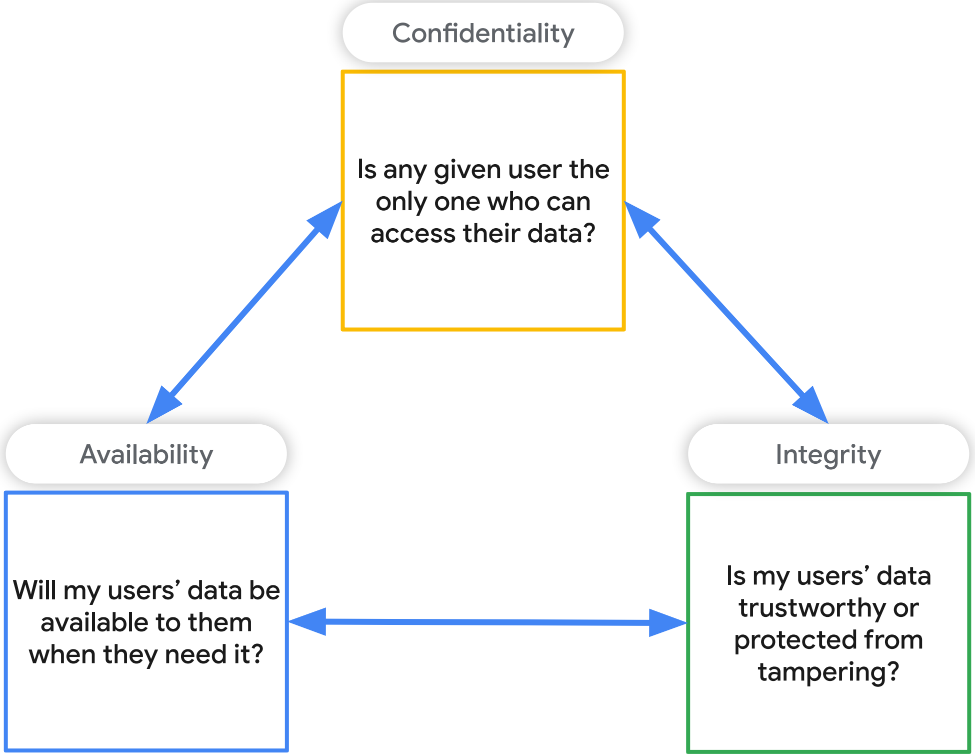
```
  style: TextStyle(
    color: Colors.green[200],
  ),
),
s.star,
r: Colors.green[500],
Text('23'),
```

Google Developer Student Clubs

devfest

University Name

The CIA Triad



Confidentiality

Is any given user the only one who can access their data?

Availability

Will my users’ data be available to them when they need it?

Integrity

Is my users’ data trustworthy or protected from tampering?

```
 style: TextStyle(
   color: Colors.green[200],
 ),
),
```

Google Developer Student Clubs

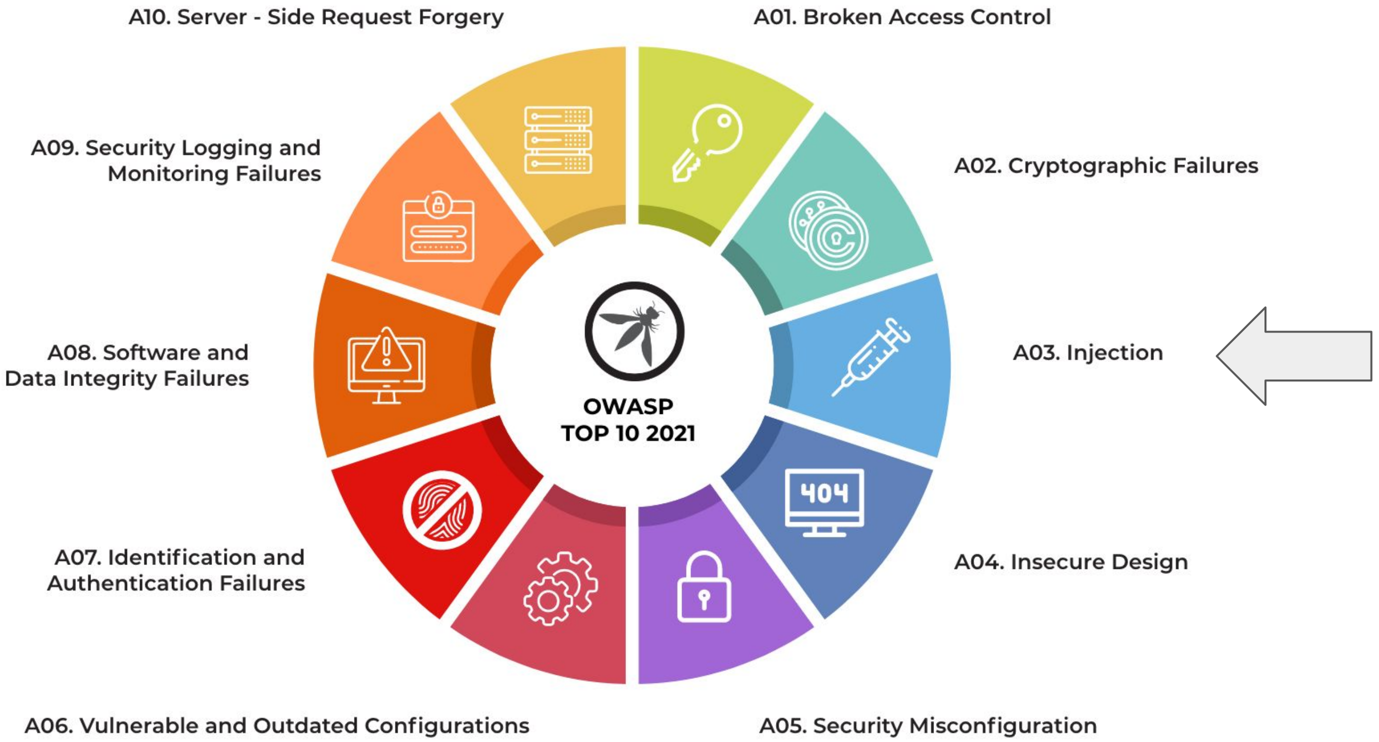
devfest

```
s.star,
r: Colors.green[500],

Text('23'),
```

University of Toronto

The OWASP Top 10



OWASP
TOP 10 2021

A01. Broken Access Control

A02. Cryptographic Failures

A03. Injection

A04. Insecure Design

A05. Security Misconfiguration

A06. Vulnerable and Outdated Configurations

A07. Identification and
Authentication Failures

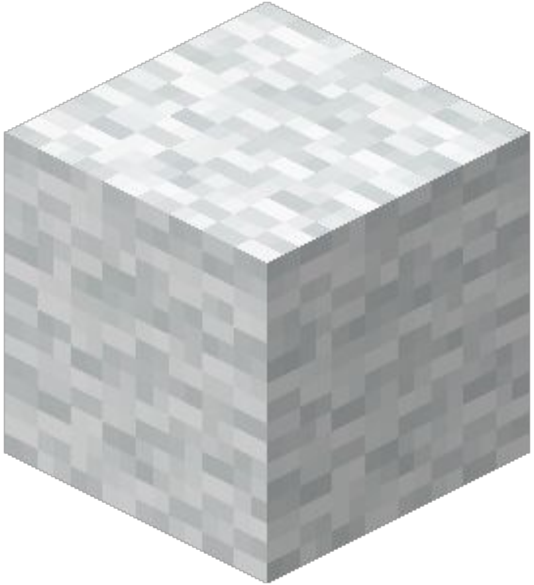
A08. Software and
Data Integrity Failures

A09. Security Logging and
Monitoring Failures

A10. Server - Side Request Forgery

White Box Penetration Testing

- Essentially penetration testing with access to source code
- A more comprehensive penetration test that can identify hidden internal risks



```
  style: TextStyle(
    color: Colors.green[200],
  ),
),
s.star,
r: Colors.green[500],
Text('23'),
```

Google Developer Student Clubs

devfest

University of Toronto

Cross-Site Scripting (XSS)

What is a Cross-Site Scripting Attack?

Inject malicious code into a website that is then served to another user and runs in their browser

Security mechanisms such as Content-Security Policy (CSP) and Same-Origin Policy can mitigate these attacks by restricting where executable scripts may be pulled from.

1. Runs arbitrary code
2. Can steal user's sessions and sensitive data
   a. (PII, PHI, Credentials, etc)
3. Deface websites

Reflected XSS

Triggered by the server reflecting user-provided data back to the browser

The payload is often carried through a get parameter, e.g.

```
?searchTerm=<script>...
```

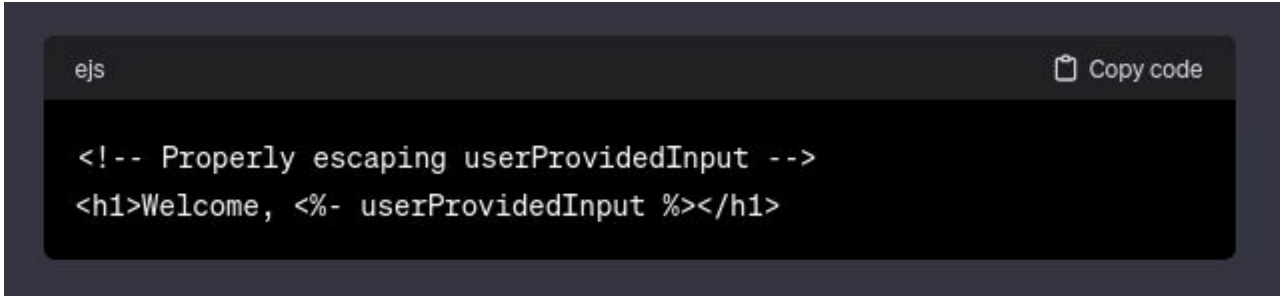
Stored XSS

Involves persistently storing the malicious script on the server

Ex. Javascript added to a ticket, profile, comment, and other pages that are stored on the server-side.

XSS Demo Time

Be Careful With ChatGPT...



```
<!-- Properly escaping userProvidedInput -->
<h1>Welcome, <%- userProvidedInput %></h1>
```

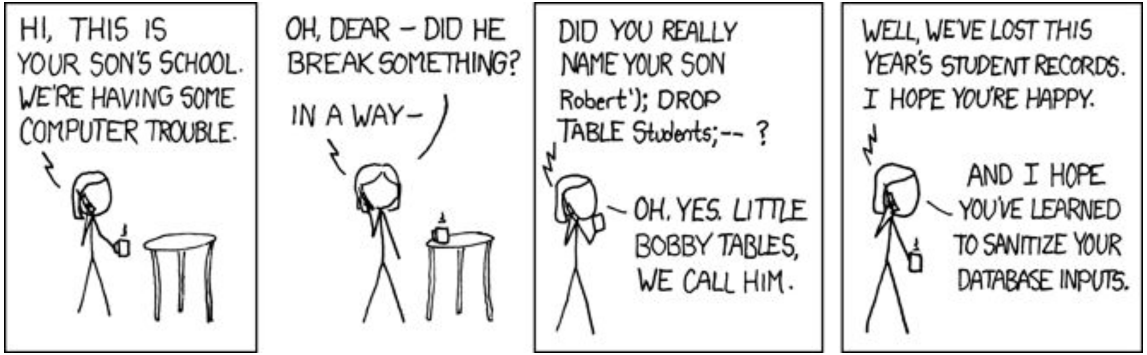
```
  Section Title',
  style: TextStyle(
    color: Colors.green[200],
  ),
),
s.star,
r: Colors.green[500],
Text('23'),
```

Google Developer Student Clubs

devfest

University of Toronto

SQL Injection


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

https://xkcd.com/327/

What is an SQL injection attack?

Exploits a lack of user-input validation/filtering on the backend, leading to modifying the containing SQL query.

1. Attackers can include additional SQL commands
   a. Or replace the original SQL command
2. In-band SQL Injection is the most common
   a. The attacker uses the same channel to send the query and retrieve it (ex. web server)
3. Attackers can retrieve/manipulate data
   a. In very specific configurations be used to execute commands on the remote server

SQLi Demo Time

Google Developer Student Clubs

```
 'Section Title',
 style: TextStyle(
   color: Colors.green[200],
  ),
),
```

Google Developer Student Clubs

devfest

University of Toronto

```
s.star,
r: Colors.green[500],

Text('23'),
```

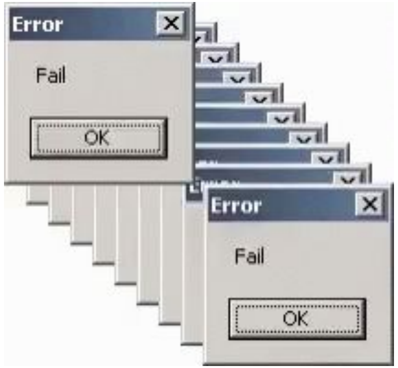
Command Injection

How does OS Command Injection Work?

- Unsanitized/validated user input is used within a shell command.
- An injection just like XSS and SQLi, but within a different albeit severe domain.

- Attacker has the ability to execute arbitrary shell commands.
  1. Allows them to execute PrivEsc
- May lead to total server compromise.
- Severely impacts server integrity.
- Strict preventive measures needed.

Command Injection
Demo Time



```
 style: TextStyle(
   color: Colors.green[200],
 ),
),
s.star,
r: Colors.green[500],
Text('23'),
```

Google Developer Student Clubs

devfest

University of Toronto

Examples in the Wild

Ingress nginx annotation injection causes arbitrary command execution

Blind SQL injection

Stored XSS in plan name field

```
 style: TextStyle(
   color: Colors.green[200],
 ),
),
s.star,
r: Colors.green[500],
Text('23'),
```

Google Developer Student Clubs

devfest

University of Toronto

Resources

Resources

1. Common Vulnerability Scoring System (CVSS)
2. Open Web Application Security Project (OWASP)
    a. OWASP Top Ten
    b. OWASP Security Testing Guide
3. Common Vulnerabilities and Exposures (CVE)
    a. CVE Database by MITRE
4. Interested in Web Security?
    a. Kali Linux (Burp Suite)
    b. HackTheBox Academy (Bug Bounty Hunter Path)
    c. Offensive Security WEB-300