WTH is XSS

What is Cross-site Scripting and How Bad is it Really?

This Guy

Joshua Barone

- Senior Information Security Engineer with Geocent
- Master of Science (Computer Science) from UNO
- Certifications: CISSP, GSEC, GCIH

But Really...

- Code Monkey
- Security Aficionado
- Really Nice Guy

Ten Commandments

1. Thou Shalt Not Use A Computer To Harm Other People.
2. Thou Shalt Not Interfere With Other People's Computer Work.
3. Thou Shalt Not Snoop Around In Other People's Computer Files.
4. Thou Shalt Not Use A Computer To Steal.
5. Thou Shalt Not Use A Computer To Bear False Witness.
6. Thou Shalt Not Copy Or Use Proprietary Software For Which You have Not Paid.
7. Thou Shalt Not Use Other People's Computer Resources Without Authorization Or Proper Compensation.
8. Thou Shalt Not Appropriate Other People's Intellectual Output.
9. Thou Shalt Think About The Social Consequences Of The Program You Are Writing Or The System You Are Designing.
10. Thou Shalt Always Use A Computer In Ways That Insure Consideration And Respect For Your Fellow Humans

Washington Consulting Group and the Computer Ethics Institute

What Is It?

Cross-Site Scripting (XSS) attacks are a type of **injection**, in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates **without validating or encoding it**.

https://www.owasp.org/index.php/Cross-Site_Scripting

Categories of XSS

1. Non-Persistent (Reflected)
2. Persistent (Stored)
3. DOM Based

Non-Persistent XSS

Also known as reflected cross-site script attacks, these attacks take advantage of sites that include request input in the response. These attacks are usually performed by getting a user to click a link with a malicious script included in URL GET parameter.

```
http://example.com/?q=<script>alert(‘xss’);</script>
```

Persistent XSS

Also known as stored cross-site scripting attacks. These attacks leverage the web applications storage medium (database) to store and replay the malicious script to users of the site.

Examples:

- Forums
- Comments
- Message Boards
- Etc...

DOM Based

This version of cross-site scripting takes alters the document object model (DOM) of the site to inject malicious javascript. This differs from other forms of cross-site scripting by not being directly part of the response from the server, rather being entirely handled in the client browser.

```
<SCRIPT>
var pos=document.URL.indexOf("context=")+8; document.write
(document.URL.substring(pos,document.URL.length));
</SCRIPT>
```

Where Can It Hook?

Any place **unvalidated**, or **poorly validated**, user input is rendered on the page.

DEMO TIME

May the Demo Gods Be Merciful

So What?

You made a pop up, so what?

Other than be annoying, what harm can this actually do?

Super Bad!!

- Anything that javascript can do
- Extract Cookies
- Alter Page DOM (rewrite site)
- Hook With js File
- Get List of Visited Sites (sort of)
- Port Scan Internal Network
- Leverage for CSRF attacks

Oh, But It Gets Worse

There are tools to make this even easier

- BeEF Framework
- OWASP Xenotix
- XSS Server
- And Many, Many More...

Filter Evasion

- URL Encoding
- Hex Encoding
- Octal Encoding
- US-ASCII Encoding (¼script¾alert(¢XSS¢)¼/script¾)
- UTF-7 Encoding
- HTML Quote Encapsulation
- And More...

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Q/A

Ask questions, or feel the awkward silence!

Want More?

- Google XSS Game: https://xss-game.appspot.com/

- My XSS Penlab
    - Docker jbarone/xsspenlab
    - Source https://github.com/jbarone/xsspenlab

Thank You

Joshua Barone

email: joshua.barone@gmail.com
twitter: @tygarsai