CSE 484
XSS - Cross Site Scripting Intro

Nicholas Shahan
10/30/2014

XSS Attacks

Cross site scripting attacks enable an attacker to run arbitrary code in a clients web browser.

JavaScript embedded in a web page is executed locally on the client side.

Types of XSS Attacks

Persistent

Attack is saved on the server side and displayed every time the target page is requested.

example: HTML enabled posts on forums

Reflected (non-persistent)

Attack is only present while the victim is viewing the page.

example: Links to a search page with search terms

Searching for Vulnerabilities

Look anywhere you can input text.

Experiment with simple tags.

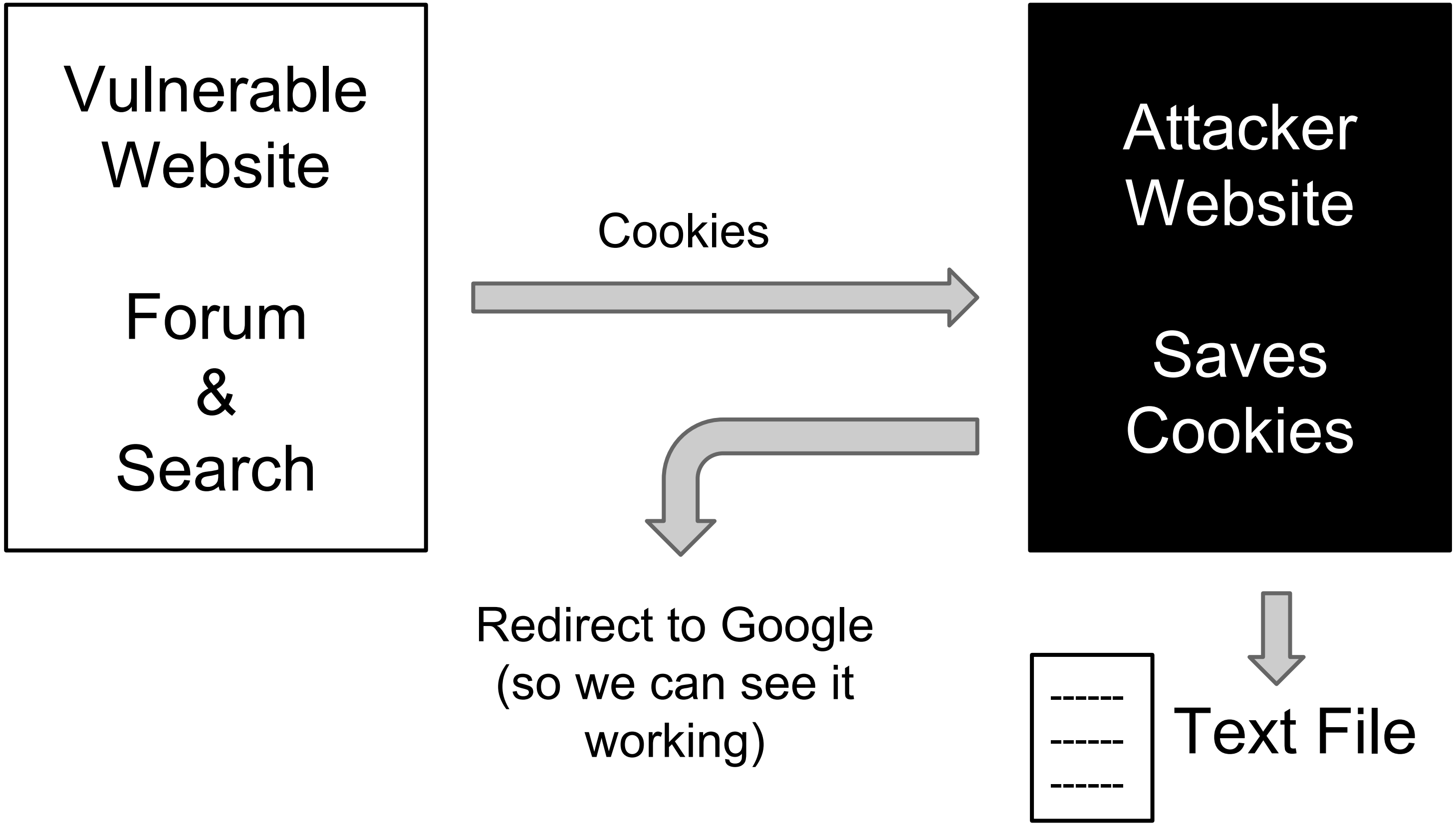
```
<h1>XSS</h1>
```

```
<script>alert("XSS");</script>
```

Move on to More Complicated Structures.

```
<img src="no.image.here" onError="..." />
```

Demo Setup



Vulnerable Website

Forum & Search

Cookies

Attacker Website

Saves Cookies

Redirect to Google (so we can see it working)

Text File

Helpful References

XSS Introduction

http://excess-xss.com/

XSS Information Overload

https://www.owasp.org/index.php/Cross-site_Scripting_%28XSS%29

Encoding Characters

http://www.web2generators.com/html/entities

http://www.w3schools.com/tags/ref_urlencode.asp

Using JSONP to Get Around CORS

http://www.phocean.net/2013/10/13/csrf-with-jsonp.html