Cross Site Scripting

CYBER SECURITY &
PRIVACY FOUNDATION

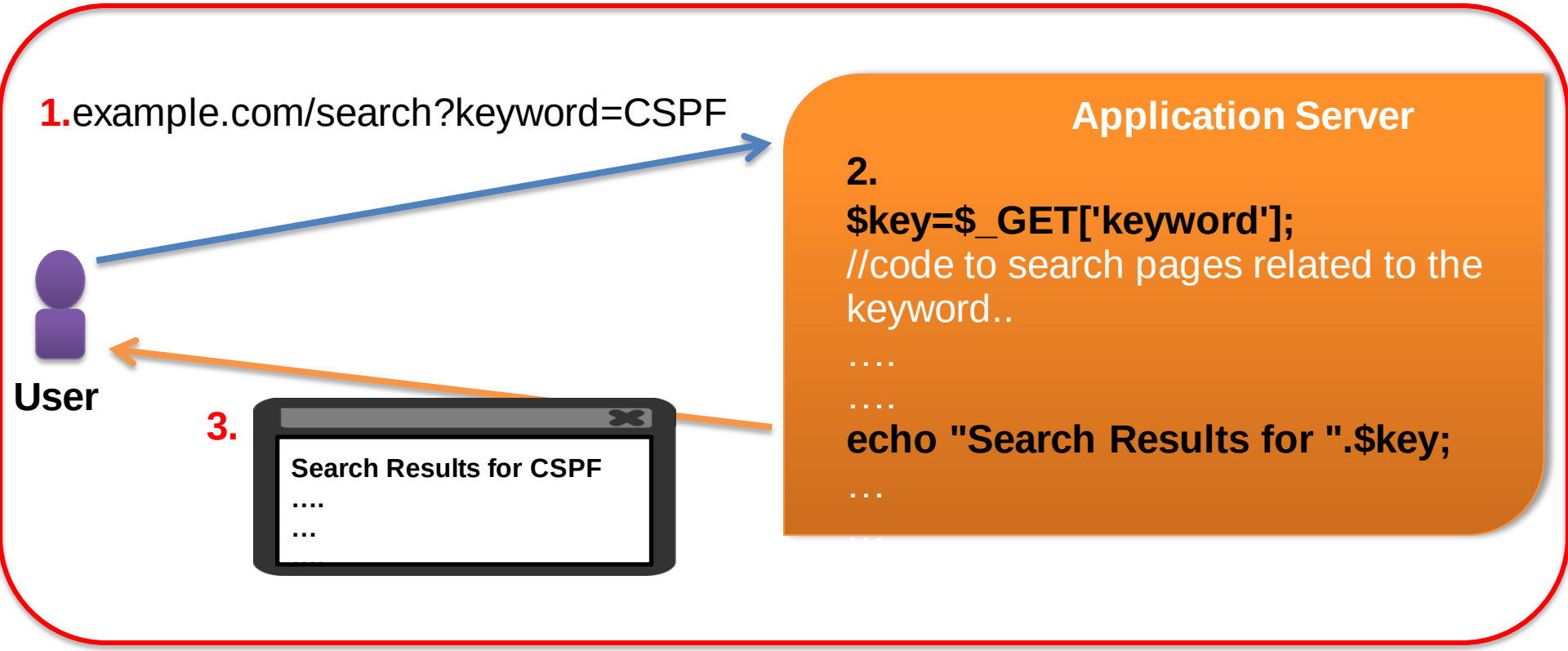
Introduction

Cross Site Scripting (also known as XSS) is one of the most common web application vulnerabilities.

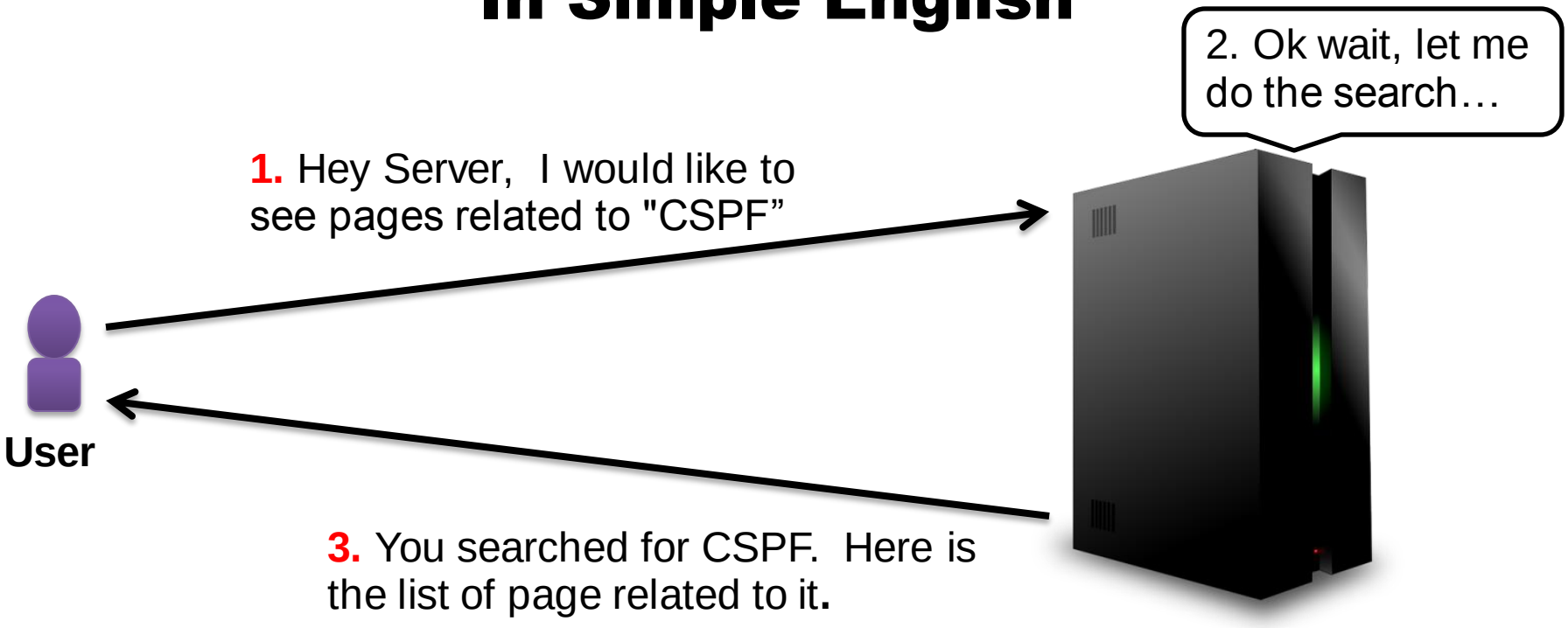
XSS occurs when a web application includes the user-provided data in web pages without sanitizing it.

This vulnerability allows an attacker to inject malicious client-side scripts into web pages displayed to other users.

How a normal Web Application Works?



In Simple English



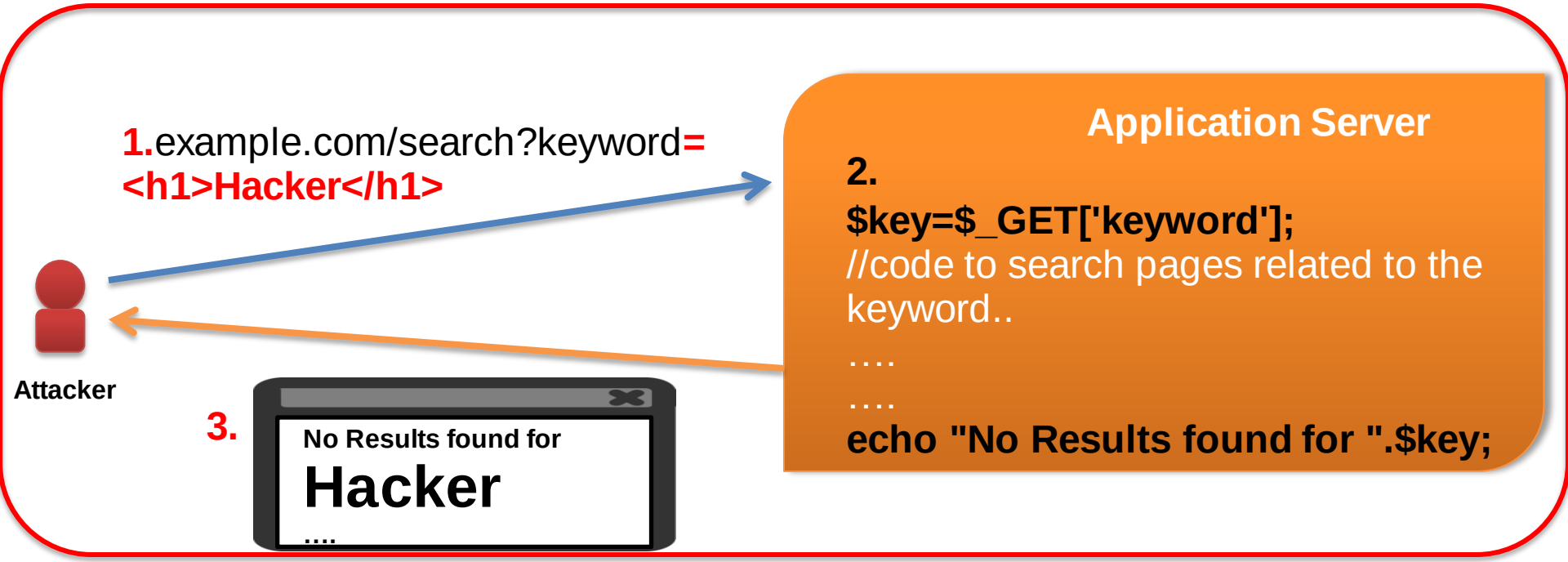
Evil User

- As you can see, the web application takes the User Input and includes into the Web Page displayed to the user without doing any validation.

- So basically, this app trusts users that they won't any insert anything other than a normal word.

- But, an attacker does more than searching a normal string. He will try to inject a client-side code into the keyword field.

Injecting HTML Tag



➢ As a result of including the keyword field in the page without validating it, the “<h1>” is being parsed as HTML tag.

XSS

- **Injecting a Javascript code:**

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

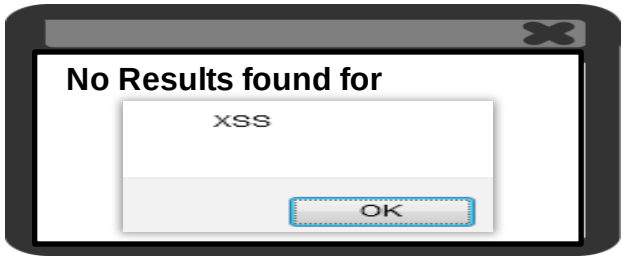
Attacker

Application Server

2.

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

3.



Types of XSS

XSS

Reflected

Stored

DOM

Impact of XSS

An attacker can exploit XSS vulnerabilities to perform following malicious actions:

- Hijacking accounts(Stealing cookies)
- Deface websites
- Redirect users to malicious page
- DDOS attack
- Exploiting browser vulnerabilities to deliver malware
- And more