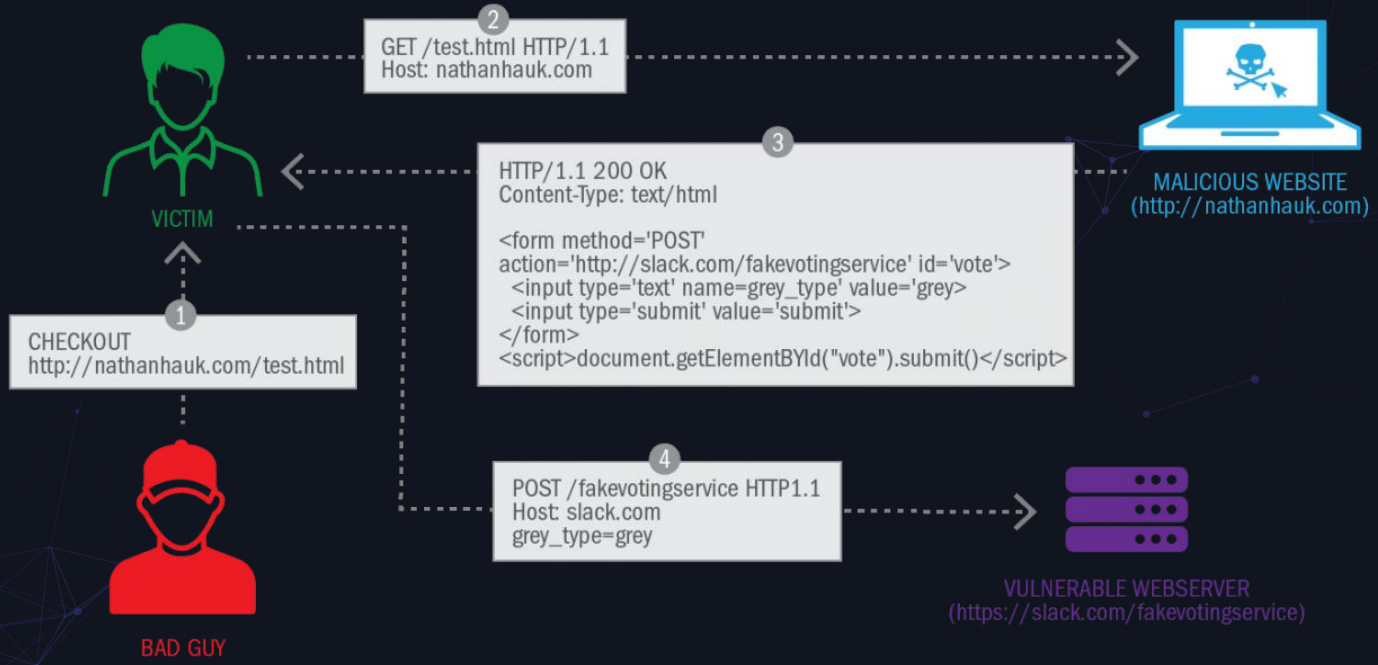
Cross-site request forgery (CSRF)

Cross-Site Request Forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated. With a little help of social engineering, an attacker may trick the users of a web application into executing actions of the attacker's choosing. If the victim is a normal user, a successful CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account, CSRF can compromise the entire web application.

Source: owasp.org

CSRF


2
GET /test.html HTTP/1.1
Host: nathanhauk.com
3
HTTP/1.1 200 OK
Content-Type: text/html
<form method='POST'
action='http://slack.com/fakevotingservice' id='vote'>
<input type='text' name=grey_type' value='grey>
<input type='submit' value='submit'>
</form>
<script>document.getElementBYId("vote").submit()</script>
MALICIOUS WEBSITE
(http://nathanhauk.com)
VICTIM
1
CHECKOUT
http://nathanhauk.com/test.html
BAD GUY
4
POST /fakevotingservice HTTP1.1
Host: slack.com
grey_type=grey
VULNERABLE WEBSERVER
(https://slack.com/fakevotingservice)

CSRF

```
npm install
node server.js

# Open another terminal
node server-malicious.js
```

Don’t mind the code, we will talk about sessions and authentication later.

Now go there: http://localhost:3000

You need to login to sign the petition.

CSRF

Now go there: http://localhost:3001 and complete the form.

What happened?

CSRF

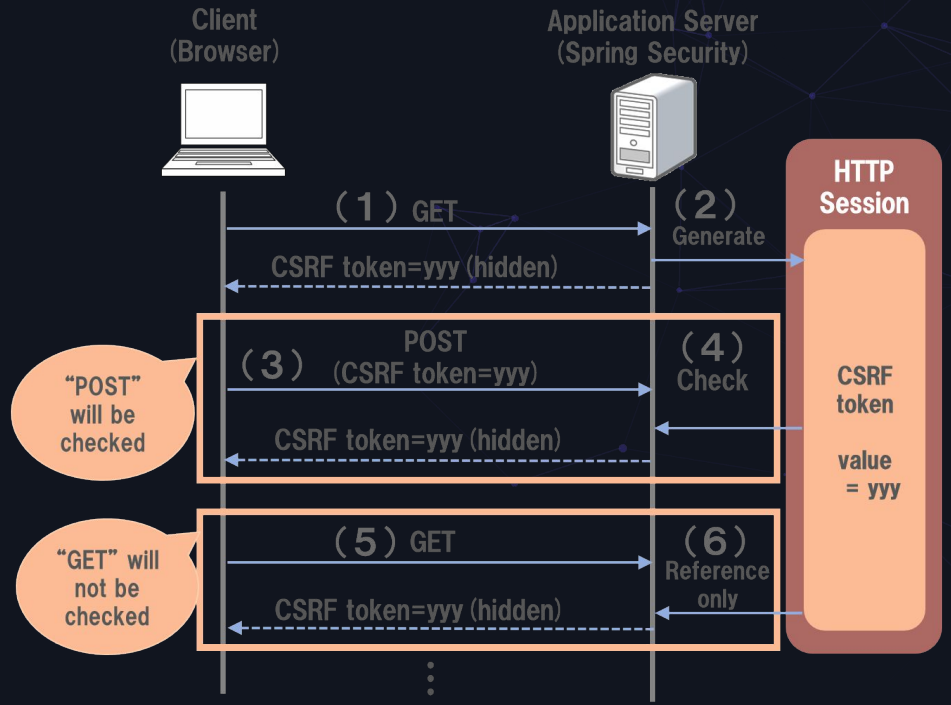
Ok, how could we fix that?

CSRF

We will use token-based mitigation. This defense is one of the most popular and recommended methods to mitigate CSRF.

There is a popular npm package for that:

https://www.npmjs.com/package/csurf



CSRF

Practical work

Only modifying the server.js file, fix the security flaw.

You can install and use the following package to help you:
https://www.npmjs.com/package/csurf

Particularly look at that part of the documentation:

https://www.npmjs.com/package/csurf#simple-express-example