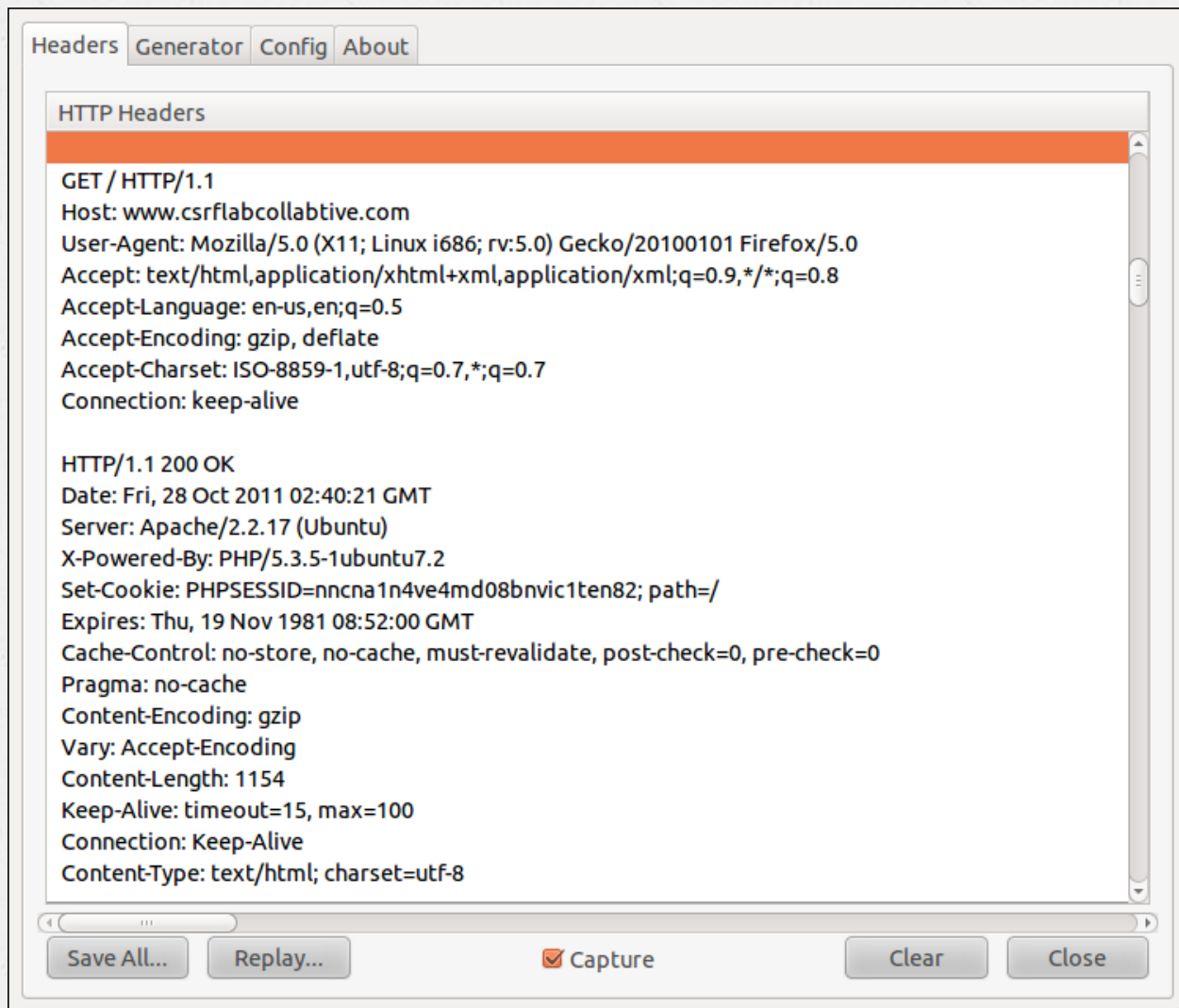




Cross Site Request Forgery Lab

Computer Security

HTTP Headers



PHP Basics

- Variables begin with \$
 - Eg: `$var_name`
- Arrays can be indexed with string values
 - Eg:
 - `$var_name["abc"] = 2;`
 - `$var_name["this is a string"] = 5;`
 - `echo $var_name["abc"];`

PHP Basics

- PHP is compiled to generate an html page
- PHP and HTML can be interchangeably used

Example

```
<html>
```

```
<head><title>This is a title</title></head>
```

```
<body>
```

```
Hello. <?php echo "Good Morning"; ?>
```

```
</body>
```

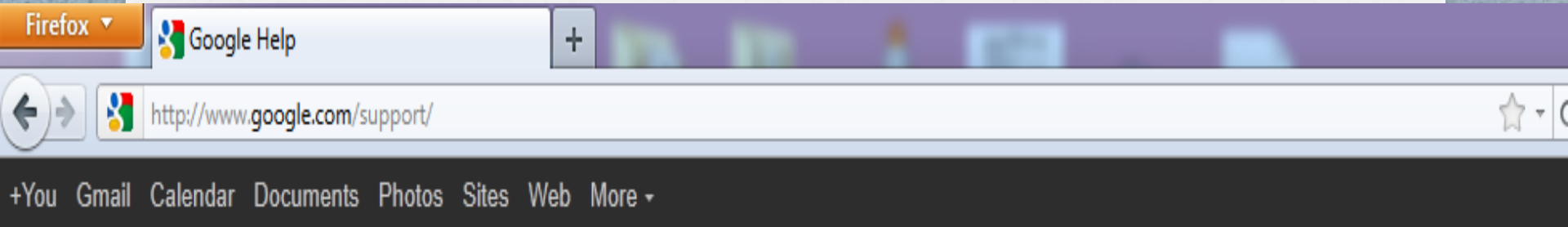
```
</<?php echo "html"; ?>>
```

PHP Variables

- o Three array variables provided to the developer: `$_GET`, `$_POST`, `$_SESSION`
- o Used to get values from GET and POST requests, and also to store or get session data

GET and POST Requests

- GET: Included in the URL of the webpage



Google

abcd




Firefox ▾

Search results - Google Help

+

⬅ ➡

 http://www.google.com/support/bin/search.py?query=abcd&ctx=en%3Asearchbox

☆ ▾ ↻

+You Gmail Calendar Documents Photos Sites Web More ▾

Google

abcd

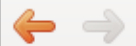


GET and POST Requests

- GET: Included in the URL of the webpage
- POST: Included in the HTTP Request

File Edit View History Bookmarks Tools Help

Gmail - Compose Mail



http://mail.google.com/mail/h/ti5o0qnevnhb/?&v=1



Google



Most Visited

SEED Labs



Google

PhpBB.com



Collabtive



phpMyAdmin



[Gmail](#) [Calendar](#) [Documents](#) [Photos](#) [Sites](#) [Groups](#) [Web](#) [More »](#)

apoorva.iyer@gmail.com | [My account](#) | [Settings](#) | [Help](#) | [Sign out](#)



Search Mail

Search the Web

[Show search options](#)
[Create a filter](#)

Compose Mail

Send

Save Draft

Discard

[Inbox \(1\)](#)

[Starred](#) ★

[Sent Mail](#)

[Drafts \(7\)](#)

[All Mail](#)

[Spam \(306\)](#)

[Trash](#)

[Contacts](#)

Labels

[Invent09](#)

[Bangalore Tr...](#)

[BE Project - ...](#)

[College Stuf...](#)

[Deleted Item...](#)

To:

Cc:

Bcc:

Subject:



Attachments:

/home/seed/Desktop/Screenshot-Live HTTP headers.png

Browse...

Attach More Files

Headers Generator Config About

HTTP Headers

http://mail.google.com/mail/h/bwvi0eyhuza/?&v=b&fv=b&cpt=c&at=AF6bupOjXMJqeXuo8XzA5ef...

POST /mail/h/bwvi0eyhuza/?&v=b&fv=b&cpt=c&at=AF6bupOjXMJqeXuo8XzA5efqVIH9xFPv2g&pv...

Host: mail.google.com

User-Agent: Mozilla/5.0 (X11; Linux i686; rv:5.0) Gecko/20100101 Firefox/5.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip, deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Connection: keep-alive

Referer: http://mail.google.com/mail/h/ti5o0qnevnhb/?&v=b&pv=tl&cs=b

Cookie: S=gmail=ORp7t42lv3qNja6cenXsQ; GX=DQAAAL8AAAA1FoBR29C3zN_vl-SDGcULUg98rEQJ...

Content-Type: multipart/form-data; boundary=—————122479666715502545421953216771

Content-Length: 96900

—————122479666715502545421953216771

Content-Disposition: form-data; name="redir"

20

Save All...

Replay...

☒ Capture

Clear

Close

Resources

PHP:

<http://www.w3schools.com/php/default.asp>

GET/POST:

<http://thinkvitamin.com/code/the-definitive-guide-to-get-vs-post/>

<http://www.w3.org/2001/tag/doc/whenToUseGet.html#checklist>

Basic Idea for Tasks

1. Victim logs into trusted site using username and password
2. Trusted site stores session identifier in a cookie on the victim
3. Victim visits malicious site
4. Malicious site sends request to trusted site via victim's browser
5. Browser automatically attaches cookie to the request from the malicious site
6. Trusted site processes the malicious request forged by the attackers' site

You can use the JS code provided in the lab description