

XSS and More

Sven Vetsch / Disenchant

March 26, 2008

XSS Basics

XSS Basics

Protection

The Meaning of Client Side Security

XSS Related Attacks

Even More Scenarios, Topics and Tricks

Some Information

How to Exploit XSS Vulnerabilities

Technical Explanation

Types of XSS

Why Exploiting XSS is Easy

Why Exploiting XSS is Hard

Information

- ▶ XSS is the most used attack type ever

Information

- ▶ XSS is the most used attack type ever
- ▶ A big Problem is, that many companies which own web applications think, that they're not responsible for their customers machine.

Basic Exploiting

`< script > ... < /script >`

Advanced Exploiting

▶ `< IMG SRC = "jav	ascript : alert('XSS');" >`

Advanced Exploiting

- ▶ `< IMG SRC = "jav	ascript : alert('XSS');" >`
- ▶ `< STYLE > @im\port'\ja\vasc\ript : alert(" XSS")';
< /STYLE >`

Advanced Exploiting

- ▶ `< IMG SRC = "jav	ascript : alert('XSS');" >`
- ▶ `< STYLE > @im\port'\ja\vasc\ript : alert(" XSS");
< /STYLE >`
- ▶ `< XSS STYLE = " xss : expression(alert('XSS'))" >`

Advanced Exploiting

- ▶ `< IMG SRC = "jav	ascript : alert('XSS');" >`
- ▶ `< STYLE > @im\port'\ja\vasc\ript : alert(" XSS");
< /STYLE >`
- ▶ `< XSS STYLE = " xss : expression(alert('XSS'))" >`
- ▶ `< SCRIPT > alert(String.fromCharCode(88,83,83))
< /SCRIPT >`

The Payload

- ▶ Cookie- and Session-Hijacking

The Payload

- ▶ Cookie- and Session-Hijacking
- ▶ Phishing

The Payload

- ▶ Cookie- and Session-Hijacking
- ▶ Phishing
- ▶ Defacements

The Payload

- ▶ Cookie- and Session-Hijacking
- ▶ Phishing
- ▶ Defacements
- ▶ Everything your web browser can do

XSS Basics
Protection
The Meaning of Client Side Security
XSS Related Attacks
Even More Scenarios, Topics and Tricks

Some Information
How to Exploit XSS Vulnerabilities
Technical Explanation
Types of XSS
Why Exploiting XSS is Easy
Why Exploiting XSS is Hard

Why does XSS Work?

Why does XSS Work?

- ▶ Javascript (and also VBScript etc.) is mixed up with (X)HTML

Why does XSS Work?

- ▶ Javascript (and also VBScript etc.) is mixed up with (X)HTML
- ▶ The script code is interpreted by the browser and not by the server

Why does XSS Work?

- ▶ Javascript (and also VBScript etc.) is mixed up with (X)HTML
- ▶ The script code is interpreted by the browser and not by the server
- ▶ Script code can become dynamically added and will still become interpreted

Why does XSS Work?

- ▶ Javascript (and also VBScript etc.) is mixed up with (X)HTML
- ▶ The script code is interpreted by the browser and not by the server
- ▶ Script code can become dinamicaly added and will still become interpreted
- ▶ There are no checks in place, which checks if there was any additional code injected

Reflecting

- ▶ Most of the XSS vulns. out there are *just* reflecting XSS

Reflecting

- ▶ Most of the XSS vulns. out there are *just* reflecting XSS
- ▶ Reflecting XSS means, that you can send your script code to the server and get it right back, so that it will become executed in your browser.

Reflecting

- ▶ Most of the XSS vulns. out there are *just* reflecting XSS
- ▶ Reflecting XSS means, that you can send your script code to the server and get it right back, so that it will become executed in your browser.
- ▶ Example: Search boxes

Persistent

- ▶ The persistent XSS are in most cases much more dangerous than the reflecting ones because they don't need any user interaction from the targeted user (beside of requesting the page where the XSS is stored).

Persistent

- ▶ The persistent XSS are in most cases much more dangerous than the reflecting ones because they don't need any user interaction from the targeted user (beside of requesting the page where the XSS is stored).
- ▶ We call a XSS persistent, if it will become stored on the server or most of the times in the database behind the application.

Persistent

- ▶ The persistent XSS are in most cases much more dangerous than the reflecting ones because they don't need any user interaction from the targeted user (beside of requesting the page where the XSS is stored).
- ▶ We call a XSS persistent, if it will become stored on the server or most of the times in the database behind the application.
- ▶ Examples: Guestbooks, Social Networking Platforms, ...

XSS Basics

Protection

The Meaning of Client Side Security

XSS Related Attacks

Even More Scenarios, Topics and Tricks

Some Information

How to Exploit XSS Vulnerabilities

Technical Explanation

Types of XSS

Why Exploiting XSS is Easy

Why Exploiting XSS is Hard

because...

- ▶ Easy to find

because...

- ▶ Easy to find
- ▶ HTTP or better UFBP (Universal Firewall Bypass Protocol)

because...

- ▶ Easy to find
- ▶ HTTP or better UFBP (Universal Firewall Bypass Protocol)
- ▶ More and more Hardware components have a webinterface

because...

- ▶ Easy to find
- ▶ HTTP or better UFBP (Universal Firewall Bypass Protocol)
- ▶ More and more Hardware components have a webinterface
- ▶ There are uncountable targets out there

because...

- ▶ Easy to find
- ▶ HTTP or better UFBP (Universal Firewall Bypass Protocol)
- ▶ More and more Hardware components have a webinterface
- ▶ There are uncountable targets out there
- ▶ Increasing knowledge in Javascript

because...

To successfully exploiting a XSS vulnerability, it's not enough to just display an alert box. To make your attack successful, you need to understand the logic behind the application and it's business processes. Only with this knowledge, you can write a good payload.

Protection

Not Working Stuff

- ▶ Patching and Anti-Virus

Not Working Stuff

- ▶ Patching and Anti-Virus
- ▶ Corporate Web Surfing Filters

Not Working Stuff

- ▶ Patching and Anti-Virus
- ▶ Corporate Web Surfing Filters
- ▶ Security Socket Layer (SSL)

Not Working Stuff

- ▶ Patching and Anti-Virus
- ▶ Corporate Web Surfing Filters
- ▶ Security Socket Layer (SSL)
- ▶ Two factor authentication

Not Working Stuff

- ▶ Patching and Anti-Virus
- ▶ Corporate Web Surfing Filters
- ▶ Security Socket Layer (SSL)
- ▶ Two factor authentication
- ▶ Stay away from questionable websites

The Only Thing that Works

- ▶ Disable Javascript will work but it's not practiceble with today's web applications aka. Web2.0-Super-Fancy-Ajax-Applications.

Not Working Stuff

Never use Blacklists under any circumstances, you'll never catch all attacks.

Working Stuff

You should always use Whitelisting because your chances to prevent all known and even unknown attacks are much higher. Until now, we don't have any universal remedy against XSS

The Meaning of Client Side Security

LAN vs. WWW

- ▶ Has someone in country XYZ access to your LAN (no, he hasn't hacked into it yet :P)?

LAN vs. WWW

- ▶ Has someone in country XYZ access to your LAN (no, he hasn't hacked into it yet :P)?
- ▶ No he hasn't!

LAN vs. WWW

- ▶ Has someone in country XYZ access to your LAN (no, he hasn't hacked into it yet :P)?
- ▶ No he hasn't!
- ▶ Do you have access to the LAN you're actually in?

LAN vs. WWW

- ▶ Has someone in country XYZ access to your LAN (no, he hasn't hacked into it yet :P)?
- ▶ No he hasn't!
- ▶ Do you have access to the LAN you're actually in?
- ▶ I'm really not going to answer such a dumb question.

LAN vs. WWW

- ▶ Has someone in country XYZ access to your LAN (no, he hasn't hacked into it yet :P)?
- ▶ No he hasn't!
- ▶ Do you have access to the LAN you're actually in?
- ▶ I'm really not going to answer such a dumb question.

This means of course, that normally the guy in country XYZ can't even directly ping our machine. Keep that in mind for the following stuff.

XSS Basics
Protection

The Meaning of Client Side Security

XSS Related Attacks

Even More Scenarios, Topics and Tricks

The Browser is your Weapon

Intranet Hacking

The Browser is your Enemy

Can you Access your Router from the WWW?

Can you Access your Router from the WWW?

- ▶ As we've seen before, you can't do this (unless you changed the configuration) but from the LAN you can do it.

Can you Access your Router from the WWW?

- ▶ As we've seen before, you can't do this (unless you changed the configuration) but from the LAN you can do it.
- ▶ Your browser is on your machine, which's in the LAN

Can you Access your Router from the WWW?

- ▶ As we've seen before, you can't do this (unless you changed the configuration) but from the LAN you can do it.
- ▶ Your browser is on your machine, which's in the LAN
- ▶ Your browser has access to your LAN

Overtaking the LAN

Let's try it out and hacking into a home router.

XSS Basics
Protection

The Meaning of Client Side Security

XSS Related Attacks

Even More Scenarios, Topics and Tricks

The Browser is your Weapon

Intranet Hacking

The Browser is your Enemy

Firefox's Chrome

Firefox's Chrome

- ▶ The chrome is the environment, where Firefox and also it's extensions run in.

Firefox's Chrome

- ▶ The chrome is the environment, where Firefox and also it's extensions run in.
- ▶ When something is started in the chrome, it will gain the privileges of the actual chrome.

Firefox's Chrome

- ▶ The chrome is the environment, where Firefox and also it's extensions run in.
- ▶ When something is started in the chrome, it will gain the privileges of the actual chrome.
- ▶ Through the Mozilla Framework, applications can be written just in Javascript and XML but still have the possibility to access the local filesystem, open sockets and so on.

Writing Malware in Javascript and XML

Firefox Extensions ...

Writing Malware in Javascript and XML

Firefox Extensions ...

- ▶ have full access of the chrome

Writing Malware in Javascript and XML

Firefox Extensions ...

- ▶ have full access of the chrome
- ▶ are easy to write

Writing Malware in Javascript and XML

Firefox Extensions ...

- ▶ have full access of the chrome
- ▶ are easy to write
- ▶ can be made platform independent very easy

Writing Malware in Javascript and XML

Firefox Extensions ...

- ▶ have full access of the chrome
- ▶ are easy to write
- ▶ can be made platform independent very easy
- ▶ nobody will check your code

Writing Malware in Javascript and XML

Firefox Extensions ...

- ▶ have full access of the chrome
- ▶ are easy to write
- ▶ can be made platform independent very easy
- ▶ nobody will check your code
- ▶ easy to install :P

Exploiting Browsers through XSS

Use something like the following exploits as a payload for your XSS:

Exploiting Browsers through XSS

Use something like the following exploits as a payload for your XSS:

- ▶ *MS07-004 VML integer overflow exploit*
- ▶ *Microsoft IE TIF/TIFF Code Execution (MS07-055)*
- ▶ *Mozilla Firefox 2.0.0.7 Denial of Service*
- ▶ ...

Exploiting Browsers through XSS

Use something like the following exploits as a payload for your XSS:

- ▶ *MS07-004 VML integer overflow exploit*
- ▶ *Microsoft IE TIF/TIFF Code Execution (MS07-055)*
- ▶ *Mozilla Firefox 2.0.0.7 Denial of Service*
- ▶ ...

We'll see more on this later in the part about Heap Spraying.

XSS Related Attacks

CSRF

- ▶ CSRF stands for Cross Site Request Forgery

CSRF

- ▶ CSRF stands for Cross Site Request Forgery
- ▶ CSRF is **not** XSS

CSRF

- ▶ CSRF stands for Cross Site Request Forgery
- ▶ CSRF is **not** XSS
- ▶ How does your browser load a whole webpage (incl. images, CSS, ...)?

CSRF

- ▶ CSRF stands for Cross Site Request Forgery
- ▶ CSRF is **not** XSS
- ▶ How does your browser load a whole webpage (incl. images, CSS, ...)?
- ▶ By using additional HTTP GET requests

CSRF

- ▶ CSRF stands for Cross Site Request Forgery
- ▶ CSRF is **not** XSS
- ▶ How does your browser load a whole webpage (incl. images, CSS, ...)?
- ▶ By using additional HTTP GET requests
- ▶ Many actions can be triggered through the HTTP GET method

CSRF

- ▶ CSRF stands for Cross Site Request Forgery
- ▶ CSRF is **not** XSS
- ▶ How does your browser load a whole webpage (incl. images, CSS, ...)?
- ▶ By using additional HTTP GET requests
- ▶ Many actions can be triggered through the HTTP GET method
- ▶ A harmless example of what we can do with CSRF is, to log out a user.

XSA

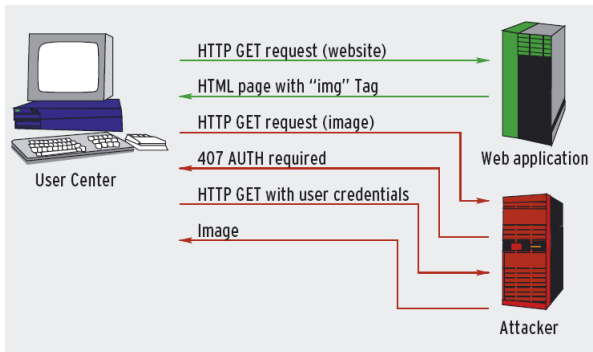


Figure: Shows how XSA works

Even More Scenarios, Topics and Tricks

XSS Worms

Samy

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge
- ▶ Infected MySpace.com

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge
- ▶ Infected MySpace.com
- ▶ After about 24h over 1'000'000 infections/friends

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge
- ▶ Infected MySpace.com
- ▶ After about 24h over 1'000'000 infections/friends
- ▶ MySpace.com had to shut down their servers for cleaning up

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge
- ▶ Infected MySpace.com
- ▶ After about 24h over 1'000'000 infections/friends
- ▶ MySpace.com had to shut down their servers for cleaning up

Yamanner

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge
- ▶ Infected MySpace.com
- ▶ After about 24h over 1'000'000 infections/friends
- ▶ MySpace.com had to shut down their servers for cleaning up

Yamanner

- ▶ Infected Yahoo!-Mail

XSS Worms

Samy

- ▶ Samy had no friends but Javascript knowledge
- ▶ Infected MySpace.com
- ▶ After about 24h over 1'000'000 infections/friends
- ▶ MySpace.com had to shut down their servers for cleaning up

Yamanner

- ▶ Infected Yahoo!-Mail
- ▶ Nobody knows how many mail addresses were stolen for spamming purposes

DDoS Based on XSS

- ▶ Uses a XSS worm

DDoS Based on XSS

- ▶ Uses a XSS worm
- ▶ Depending on the target for the worm, you'll have a huge amount of victims.

DDoS Based on XSS

- ▶ Uses a XSS worm
- ▶ Depending on the target for the worm, you'll have a huge amount of victims.
- ▶ Your payload could be, to send a request to a target webserver

DDoS Based on XSS

- ▶ Uses a XSS worm
- ▶ Depending on the target for the worm, you'll have a huge amount of victims.
- ▶ Your payload could be, to send a request to a target webserver
- ▶ One for-loop in your payload will kill neraly every standard webserver ;)

Self-Contained XSS Attacks

- ▶ Only works in Firefox and Opera

Self-Contained XSS Attacks

- ▶ Only works in Firefox and Opera
- ▶ `data:text/html;base64,PHNjcmlwdD5hbGVydCgiSGkgdGhlcmUgOIAiKTs8L3NjcmlwdD4=`

Self-Contained XSS Attacks

- ▶ Only works in Firefox and Opera
- ▶ `data:text/html;base64,PHNjcmlwdD5hbGVydCgiSGkgdGhlcmUgOIAiKTs8L3NjcmlwdD4=`
- ▶ We can also generate (malicious) binaries this way

Executing Self-Contained XSS Attacks

How to execute it:

- ▶ Put it directly into the URL field of the web browser and press Enter :P

Executing Self-Contained XSS Attacks

How to execute it:

- ▶ Put it directly into the URL field of the web browser and press Enter :P
- ▶ Find a redirecting vulnerability and put it in there.

Executing Self-Contained XSS Attacks

How to execute it:

- ▶ Put it directly into the URL field of the web browser and press Enter :P
- ▶ Find a redirecting vulnerability and put it in there.
- ▶ Redirecting through a XSS vulnerability.

Executing Self-Contained XSS Attacks

How to execute it:

- ▶ Put it directly into the URL field of the web browser and press Enter :P
- ▶ Find a redirecting vulnerability and put it in there.
- ▶ Redirecting through a XSS vulnerability.
- ▶ Sending a Mail with such a Link in it to someone.

SVG

```
< script ><![CDATA[alert(" XSS" );]] >< /script >
```

Webbased Malware

▶ Webbased Keylogger

Webbased Malware

- ▶ Webbased Keylogger
- ▶ Webbased Remote Control aka. XSS Proxy

Webbased Malware

- ▶ Webbased Keylogger
- ▶ Webbased Remote Control aka. XSS Proxy
- ▶ Intranet crawler

Webbased Malware

- ▶ Webbased Keylogger
- ▶ Webbased Remote Control aka. XSS Proxy
- ▶ Intranet crawler
- ▶ Javascript Network Tools

Webbased Malware

- ▶ Webbased Keylogger
- ▶ Webbased Remote Control aka. XSS Proxy
- ▶ Intranet crawler
- ▶ Javascript Network Tools
- ▶ ...

Old Method

- ▶ Find a reflecting XSS, triggered by HTTP GET method

Old Method

- ▶ Find a reflecting XSS, triggered by HTTP GET method
- ▶ Linking to the URL with the XSS

Old Method

- ▶ Find a reflecting XSS, triggered by HTTP GET method
- ▶ Linking to the URL with the XSS
- ▶ Get a Backlink

Old Method

- ▶ Find a reflecting XSS, triggered by HTTP GET method
- ▶ Linking to the URL with the XSS
- ▶ Get a Backlink
- ▶ AFAIK still working except Google

New Method

- ▶ Using the DOM for injecting new Links

New Method

- ▶ Using the DOM for injecting new Links
- ▶ Permanent Links

New Method

- ▶ Using the DOM for injecting new Links
- ▶ Permanent Links
- ▶ Using tinyurl.com

Heap Spraying

If you're interested in it have a look at the following stuff by Alexander Sotirov:

Heap Spraying

If you're interested in it have a look at the following stuff by Alexander Sotirov:

- ▶ *[Heap Feng Shui in JavaScript - Presentation](#)*
- ▶ *[Heap Feng Shui in JavaScript - Paper](#)*

Thanks for your attention :)

Appendix

- ▶ The Open Web Application Security Project (OWASP)
<http://www.owasp.org/>
- ▶ Web Application Security Consortium
<http://www.webappsec.org/>
- ▶ PLANET-WEBSECURITY.org
<http://planet-websecurity.org/>

Jeremiah Grossman
Robert Hansen
Petko D. Petkov