

## Forum:[Hack Forums](#)

Thread: [What should I learn to become a good website penetration tester?](#)

**UKpower** - June 12, 2017, 4:59 am

I have absolutely No programming knowledge or what so ever ?

I've seen few videos on youtube and security penetration testing courses which doesn't explain anything in detail. What should I learn to become a professional sqli tester (work in a company with such knowledge) Should I learn php and mysql? can you suggest me books, tutorials? The whole idea is to get a job in similar field.

**pop.pop.ret** - June 12, 2017, 5:00 am

PHP and SQL are definitely two great starting points. You pretty much answered your own question.

Don't bother focusing on learning SQL injection, instead just learn PHP and various DBMS languages then you should naturally begin to understand how SQLi works

**UKpower** - June 12, 2017, 5:08 am

(Jun 12, 2017 05:00 AM)pop.pop.ret Wrote: [\[CITE\]](#) PHP and SQL are definitely two great starting points. You pretty much answered your own question.

Don't bother focusing on learning SQL injection, instead just learn PHP and various DBMS languages then you should naturally begin to understand how SQLi works  
can u suggest me few books?

should I learn PHP to understand DBMS better?

**Meterpreter** - June 12, 2017, 5:12 am

SQLi tester? Never heard of it.

Website penetration testing and architectural penetration tester.

External penetration testing, internal penetration testing, or both?

You can penetration test someones website and leave it there. Or you can go further to exploit their server and gain access to their internal network.

Really depends what you want to offer. Website penetration alone you should just start off with SQLi, CSS, Metasploit for webserver testing.

But I'd strongly suggest looking at some more enjoyable angles of PT, like targeting whole networks rather than just websites.

**pop.pop.ret** - June 12, 2017, 5:17 am

(Jun 12, 2017 05:08 AM)UKpower Wrote: [\[CITE\]](#) can u suggest me few books?

should I learn PHP to understand DBMS better?

Yeah, look into the mysqli\_\* functions and PDO prepared statements within PHP - then learn various flavours of SQL e.g. MySQL, Postgre, etc. I cannot stress how important it is to actually learn PHP and SQL before learning SQL Injection. You'd use PHP to deal w/ DBMS interactivity in the sense that you'd handle the user inputs and then query the database with those inputs via PHP. SQL injection vulns are very often as a result of badly written PHP code.

As for books, I'm not sure off of the top of my head... but OWASP is a good resource and the site I'm about to launch will go into a LOT of detail regarding SQLi - I'll link you once its ready.

**Meterpreter** - June 12, 2017, 5:20 am

I wrote a massive comment but it decided not to post.

Determine: Do I just want to do website penetration testing?

What do I already know?

Personally, I think you should look into website penetration as a part of architecture penetration testing: That is penetration testing (PTing) web servers.

Do you really want to only offer website penetration testing? You're limiting yourself to external website penetration tests. Why not look at internal and external penetration testing of architecture, and learning how to pivot to gain access to entire networks as well as PTing websites?

If you're certain on solely website PT then there's nothing else I can really say. Look at SQLi and XSS. Keep up to date with firmware vulnerabilities in common website bases such as Wordpress and BB. And if you're still not sure about only doing websites, try learning some basic Metasploit knowledge and target web servers.

(Jun 12, 2017 05:17 AM)pop.pop.ret Wrote: [\[CITE\]](#) Yeah, look into the mysqli\_\* functions and PDO prepared statements within PHP - then learn various flavours of SQL e.g. MySQL, Postgre, etc. I cannot stress how important it is to actually learn PHP and SQL before learning SQL Injection. You'd use PHP to deal w/ DBMS interactivity in the sense that you'd handle the user inputs and then query the database with those inputs via PHP. SQL injection vulns are very often as a result of badly written PHP code.

As for books, I'm not sure off of the top of my head... but OWASP is a good resource and the site I'm about to launch will go into a LOT of detail regarding SQLi - I'll link you once its ready.

My learning curve was reversed. I learnt SQLi at a very young age and when I went into my IT degree later on I understood SQL fluently. :')

But agreed, much easier just to learn SQL then SQLi.

**pop.pop.ret** - June 12, 2017, 5:22 am

(Jun 12, 2017 05:20 AM)Meterpreter Wrote: [\[CITE\]](#) Look at SQLi and CSS.

What does CSS have to do with any of this? Am I missing something? The only practical application of CSS within web-based pentesting that I can even think of is RPO aka Relative Path Overwrite

Meterpreter Wrote: My learning curve was reversed. I learnt SQLi at a very young age and when I went into my IT degree later on I understood SQL fluently. :')

But agreed, much easier just to learn SQL then SQLi.

I did this also but I think my understanding of SQLi got WAY deeper after I learned SQL as a DBMS lang :)

**Meterpreter** - June 12, 2017, 5:26 am

(Jun 12, 2017 05:22 AM)pop.pop.ret Wrote: [\[CITE\]](#) What does CSS have to do with any of this? Am I

missing something? The only practical application of CSS within web-based pentesting that I can even think of is RPO aka Relative Path Overwrite

I did this also but I think my understanding of SQLi got WAY deeper after I learned SQL as a DMBS lang :)

Cross Site Scripting was just a suggestion as I have never heard of a SQLi tester. Merely website penetration tester, but even the ones I know who focused on purely website pentesting have migrated to architecture and websites.

It's a really silly thing really, as you may mark a website as safe, however the actual webserver is vulnerable.

**Giratina** - June 12, 2017, 5:27 am

(Jun 12, 2017 05:12 AM)Meterpreter Wrote: [\[CITE\]](#) Really depends what you want to offer. Website penetration alone you should just start off with SQLi, CSS, Metasploit for webserver testing.

But I'd strongly suggest looking at some more enjoyable angles of PT, like targeting whole networks rather than just websites.

Couldn't agree with your post more.

As someone with a lot of experience in IT security (through interest in my spare time), I find it difficult to find projects to utilize my skills. How do you go about this?

Obviously it's not difficult to put my abilities to work, but I'd rather not be sued by anyone.

**pop.pop.ret** - June 12, 2017, 5:29 am

(Jun 12, 2017 05:26 AM)Meterpreter Wrote: [\[CITE\]](#) Cross Site Scripting was just a suggestion as I have never heard of a SQLi tester. Merely website penetration tester, but even the ones I know who focused on purely website pentesting have migrated to architecture and websites.

It's a really silly thing really, as you may mark a website as safe, however the actual webserver is vulnerable.

Ohh, XSS - gotcha. I thought you were referring to CSS aka Cascading Sytle Sheets e.g. for adding style to a webpage

(Jun 12, 2017 05:27 AM)Giratina Wrote: [\[CITE\]](#) Couldn't agree with your post more.

As someone with a lot of experience in IT security (through interest in my spare time), I find it difficult to find projects to utilize my skills. How do you go about this?

Obviously it's not difficult to put my abilities to work, but I'd rather not be sued by anyone.

Do you do many bug bounties? I find them to a challenging yet profitable way to improve my skills

**UKpower** - June 12, 2017, 5:30 am

(Jun 12, 2017 05:12 AM)Meterpreter Wrote: [\[CITE\]](#) SQLi tester? Never heard of it.

Website penetration testing and architectural penetration tester.

External penetration testing, internal penetration testing, or both?

You can penetration test someones website and leave it there. Or you can go further to exploit their server and gain access to their internal network.

Really depends what you want to offer. Website penetration alone you should just start off with

SQLi, CSS, Metasploit for webserver testing.

But I'd strongly suggest looking at some more enjoyable angles of PT, like targeting whole networks rather than just websites.

What should I learn to understand your question?

Dude seriously.. never knew there are two kinds of testings... Please give me more suggestions..

pop.pop.ret - June 12, 2017, 5:32 am

(Jun 12, 2017 05:30 AM)UKpower Wrote: [\[CITE\]](#) What should I learn to understand your question?

Dude seriously.. never knew there are two kinds of testings... Please give me more suggestions..

Here's some web-based attacks that you can learn instead of focusing only on SQLi:

Quote:Abuse of Callback Functionality

Access Control Bypass

Arbitrary/Unrestricted File Upload

Content Forgery

Covert Redirect

Cross Site Scripting (XSS)

Cross Site Framing

Cross Site History Manipulation (XSHM)

Cross Site Flashing (XSF)

Cross Site Tracing (XST)

Cross Site Request Forgery (CSRF)

Cross Site Timing Attack

Cross Site Port Attack (XSPA)

CRLF Injection

CSV Excel Macro Injection (CEMI)

Directory Traversal

Execution After Redirect (EAR)

Full Path Disclosure (FPD)

HTTP Request Smuggling/Response Splitting

Information Disclosure

Insecure Direct Object Reference (IDOR)

Local File Inclusion (LFI)

LDAP Injection

Mass Assignment

NoSQL Injection

Object Injection

Open Redirect

Race Conditions

Reflected File Download (RFD)

Relative Path Overwrite (RPO)

Remote Command Execution (RCE)

Remote XSL Inclusion

Remote File Inclusion (RFI)

Resource Exhaustion

Resource Injection

Session Fixation

Session Prediction

Session Puzzling

Special Element Injection

SSI Injection

Server-Sided Request Forgery (SSRF)

XML External Entity Injection (XXE)  
XPath Injection  
Web Cache Deception

Although before looking into any of this its best to learn a web language such as PHP, learn a DBMS language, understand OSI model and sockets and how HTTP works as a protocol etc... try getting all of the fundamentals down before moving into a more specific area of exploitation.

**UKpower** - June 12, 2017, 5:35 am

(Jun 12, 2017 05:20 AM)Meterpreter Wrote: [\[CITE\]](#) I wrote a massive comment but it decided not to post.

Determine:Do I just want to do website penetration testing?

What do I already know?

Personally, I think you should look into website penetration as a part of architecture penetration testing: That is penetration testing (PTing) web servers.

Do you really want to only offer website penetration testing? You're limiting yourself to external website penetration tests. Why not look at internal and external penetration testing of architecture, and learning how to pivot to gain access to entire networks as well as PTing websites?

If you're certain on solely website PT then there's nothing else I can really say. Look at SQLi and XSS. Keep up to date with firmware vulnerabilities in common website bases such as Wordpress and BB. And if you're still not sure about only doing websites, try learning some basic Metasploit knowledge and target web servers.

My learning curve was reversed. I learnt SQLi at a very young age and when I went into my IT degree later on I understood SQL fluently. :')

But agreed, much easier just to learn SQL then SQLi.

OMG! your 18 and ur already knew so many things ! you gotta be a child prodigy. I've wasted all my life learning nothing. Can you do me one favor? I know this sounds crazy but what you do can save a human beings life.

Can you tell me the things i should learn to get a good job as an good web penetration tester (internal,external, all kind of things (honestly i have no clue what u were saying))

- 1) do this
- 2) then do that
- 3) then u do this thing..

can u please tell me in this manner so i could make a note (probably make schedules, if possible attend some tuition,coaching..etc)

**pop.pop.ret** - June 12, 2017, 5:37 am

(Jun 12, 2017 05:35 AM)UKpower Wrote: [\[CITE\]](#) OMG! your 18 and ur already knew so many things ! you gotta be a child prodigy. I've wasted all my life learning nothing. Can you do me one favor? I

know this sounds crazy but what you do can save a human beings life.

Can you tell me the things i should learn to get a good job as an good web penetration tester (internal,external, all kind of things (honestly i have no clue what u were saying))

- 1) do this
- 2) then do that
- 3) then u do this thing..

can u please tell me in this manner so i could make a note (probably make schedules, if possible attend some tuition,coaching..etc)

I know im not the guy you're speaking to but honestly just learn the fundamentals first (basic programming, networking, etc) before trying to learn anything relating to exploitation... its way better to just focus on learning how computers work before looking into how to exploit them. Don't dive straight into pentesting, you'll gain a lot more from learning programming properly and understanding the OSI model etc

**Giratina** - June 12, 2017, 5:41 am

(Jun 12, 2017 05:29 AM)pop.pop.ret Wrote: [\[CITE\]](#) Do you do many bug bounties? I find them to a challenging yet profitable way to improve my skills

Thanks man I'll check it out.

(Jun 12, 2017 05:32 AM)pop.pop.ret Wrote: [\[CITE\]](#) Here's some web-based attacks that you can learn instead of focusing only on SQLi:

[...]

Please also note that there is no 'best' method for penetrating a remote system. It all comes down to the machine's configuration and you might have to combine different attack methods in order to gain the leverage you require for the next step.

(Jun 12, 2017 05:35 AM)UKpower Wrote: [\[CITE\]](#) Can you tell me the things i should learn to get a good job as an good web penetration tester (internal,external, all kind of things (honestly i have no clue what u were saying))

- 1) do this
- 2) then do that
- 3) then u do this thing..

can u please tell me in this manner so i could make a note (probably make schedules, if possible attend some tuition,coaching..etc)

Don't be offended, but you come across a little lazy. Imagine I wanted to become a doctor and instead of picking up all the books and information I need I just ask a doctor to break everything down for me so I can understand it more easily.

Hate to break it to you, that's not how it works. Especially in IT, circumstances change daily and having the ability to pick up on new things without external help is part of the profession.

**UKpower** - June 12, 2017, 5:46 am

(Jun 12, 2017 05:37 AM)pop.pop.ret Wrote: [\[CITE\]](#) I know im not the guy you're speaking to but honestly just learn the fundamentals first (basic programming, networking, etc) before trying to learn anything relating to exploitation... its way better to just focus on learning how computers work before looking into how to exploit them. Don't dive straight into pentesting, you'll gain a lot more from learning programming properly and understanding the OSI model etc

yo common brother :) you have helped me a lot..I am just bamboozled. Don't know really where to start. There is a whole lot to learn. I thought of doing MCA (master of computer applicaiton) I looked into the portions/curriculum and it had absolutely nothing to educate myself with real world

scenarios. I am making of note of what you said. planning to learn 1 to 2 hours a day .. Think it will take years to reach your level. If not your level at least I should know what these things are ?

(Jun 12, 2017 05:41 AM)Giratina Wrote: [\[CITE\]](#) Thanks man I'll check it out.

Please also note that there is no 'best' method for penetrating a remote system. It all comes down to the machine's configuration and you might have to combine different attack methods in order to gain the leverage you require for the next step.

Don't be offended, but you come across a little lazy. Imagine I wanted to become a doctor and instead of picking up all the books and information I need I just ask a doctor to break everything down for me so I can understand it more easily.

Hate to break it to you, that's not how it works. Especially in IT, circumstances change daily and having the ability to pick up on new things without external help is part of the profession. you are 100% right. I got shit load of eBooks and honestly don't know where to start. BUT again you are 100% correct. I think it's better to learn everything. It's just that .. there are toooooooooooooo many things to learn..

**Meterpreter** - June 12, 2017, 6:02 am

There's not exactly a single starting point you can come at it at many angles.

I'm 21 but have strayed away from IT and into Psychology.

I started learning SQLi and XSS, predominately SQLi.

If you want a step by step process I can only give you this.

Do you want to do only website PT?

Yes = Study SQLi and XSS mainly. Then look into exploiting web bases such as Wordpress and MyBB.

No = Next point.

Now decide whether you want to attempt to get business opportunities locally and undergo "internal" pentesting. This is done from within the internal network.

If you have businesses which you think you could consult then go for it (you'll need business insurance).

Generally internal architectural exploitation and reconnaissance is the same as external, but is easier to navigate and map IP addresses, as well as pivot to other systems.

There are also some exploits designed ONLY for internal exploitation, and some ONLY for external exploitation.

Either way internal and external will follow the same path of learning. This is generally learning how to use a range of programs and scripts. Easiest way is to use a penetration based computer Linux software, alike Kali Linux which has all the tools you need for beginner hacking.

You will come to find Metasploit as a friend so I suggest putting a lot of effort into learning it (Plenty of youtube tutorials for beginners).

You will need to learn Ruby and Python to understand most exploits and to adjust the code (if necessary).

Look at penetration testing certificates after all this too, it will give you a more professional approach to how to undergo business with clients, as well as teach you some things you may have missed.

You can also consider doing an IT security or computer science degree.

(Jun 12, 2017 05:29 AM)pop.pop.ret Wrote: [\[CITE\]](#) Ohh, XSS - gotcha. I thought you were referring to CSS aka Cascading Sytle Sheets e.g. for adding style to a webpage

Do you do many bug bounties? I find them to a challenging yet profitable way to improve my skills  
Yeh meant to say XSS, am very tired.

**UKpower** - June 12, 2017, 7:53 am

oh boii ! these people are so talented! Thank you very much @ Meterpreter & Giratina and pop.pop.ret

**imadeyouread** - June 13, 2017, 3:48 pm

Cryptography. Everyone should know Cryptography. It increases your skills in learning stuff easier. Practically a brain trainer.