

Interview with Sumit Siddharth



Sumit „sid“ Siddharth works as a Head of Penetration Testing for 7Safe Limited in the UK. He has over 7 years of experience within the IT security industry. He specializes in the application and database security. Over the years, he has contributed a number of white-papers, articles, advisory, tools and exploits to the industry. He has been a speaker at many security conferences including Black Hat, DEF CON, OWASP Appsec, Troopers, Sec-T etc. He also runs the popular IT security blog: <http://www.notsousecure.com>

Tell us a little bit about your professional experience in the field of Penetration Testing

SS: I have been doing penetration testing for nearly 7 years now. I specialise in Application and Database security. Although, I don't get too much involved with the network security, I still like to read up on things such as latest features within Metasploit, new kernel vulnerabilities etc. I have a very strong inclination towards R&D. My current role as Head Of Penetration testing at 7Safe, allows me time to work with other members of my team and come up with new research in areas such as new attack techniques or improving already known attack vectors.

What drove you to doing extensive research in the area of SQL injection?

SS: I worked with some people who were the masters of the SQL Injection in my last job and was able to pick this area up quite easily. The nature of our job required us to master this and other vulnerabilities, so not learning it was not an option. SQL Injection still remains the top threat for web applications and we see hundreds of websites still being compromised by this vulnerability. I researched into a number of existing tools for this vulnerability and found that each tool has its own problems. Only if you understand the mechanism behind exploiting the vulnerability, you would be able to figure out which tool to use or if you do need a tool at all in the first place. Similarly, identification of this vulnerability could be tricky at times and we worked on a number of

scenarios which were really difficult for automated tools to pick up. These areas were really interesting.

You have done tremendous work in Oracle Vulnerabilities, why Oracle and are you active in finding vulnerabilities in other databases (MySQL, MSSQL)?

SS: When I started researching into SQL Injection, I found that not too many people have looked into exploiting SQL Injection in Oracle from web applications. So, I was always keen on getting an understanding on how to achieve this. I followed the work of a number of Oracle security researchers such as David Litchfield, Alexander Kornbrust, Esteban etc. I looked into the vulnerabilities found by these guys and if these can be exploited over the web. During the process, I started to understand the Oracle database and its security features/problems. I found some new vulnerabilities which Oracle subsequently patched. I also work closely with the Oracle's security team and they have been providing good feedback/support on fixing the flaws. I have not looked too much into MSSQL or MySQL, but that is next on my list.

You offered a training session at OWASP AppSec 2011 titled 'The Art of Exploiting SQL Injection' where you helped trainees identify Second-order code injection attack. Can you tell us about this attack and how it can be mitigated?



PenTest magazine

Join our
Exclusive and Pro club
and get:

PenTest one year subscription
Full page advertisement in
PenTest every month!
Information about your company
send to over 100,000
PenTest readers!

More information at
maciej.kozuszek@software.com.pl

SS: I have been conducting workshops at major OWASP events such as Appsec for last few years. The workshop provides attendees with an in-depth understanding of the vulnerability and they can sharpen their exploitation skills. It also discusses advanced topics such as Second Order Injection. In a second order injection, an attacker's payload is stored in the database and its retrieved and used by a vulnerable SQL call. A typical example is when the application uses the session parameters in the SQL calls without validation. It's quite common practice that developers validate all GET, POST and COOKIE parameters but don't validate the data coming from other source such as databases. A second Order injection leverages this flaw. It just re-emphasises the point that validation is not enough. One should follow best security practices such as using prepared statement which clearly separates data from code.

What process do you follow when you are asked to perform a double-blinded penetration test of a Web Application (for example: B2C E-Commerce Website such as Amazon.com)?

SS: At 7Safe, we get a lot of requests for a black-box penetration test and the clients want to know the risks the application poses. We start by crawling the application and building an understanding of what is the attack surface for the application. We identify publicly known and unknown pages and whether they take any user's input. We assess them for all input validation flaws such as SQL Injection, Cross Site Scripting, CRLF Injection etc. We pay special emphasis on the business logic testing and identify areas where we can bypass business logic. The testing then focuses on other application layer flaws such as error handling, session management, access control validation, web server flaws, insecure HTTP methods, security of data at rest and in transmit, web services assessment, checking for CSRF etc.

While a number of steps in assessing the web application are standard, the business logic assessment can be a bit tricky and requires out-of-box thinking. I guess this is what makes our job interesting and gives us something new to look forward to in every test.

Few professionals run automated vulnerability scans and report the results to the client without carefully reviewing them. What approach do you take when reporting penetration testing results such that it adds value to the organization?

SS: We have put a lot of thought and effort behind this at 7Safe and have come up with a custom reporting engine/application. All our consultants log on to this system and put each security issue within this application. So every host, every port, every vulnerability goes into this and then the reporting engine generates the report. A typical report consists of the following main sections:

- Executive Summary
- Technical Details

The executive summary converts the technical findings into business risks and helps the senior management understand what are the risks the application/system poses.

The Technical Details is where we list all the security flaws which the systems suffer from along with the severity rating and a detailed recommendation on how to fix the flaws. We follow the Microsoft's DREAD rating to give each vulnerability a baseline score so that the organization can better understand how severe a vulnerability is. The technical details section has an appendix which guides the clients on how to recreate the vulnerability. This usually has screenshots/attack payload etc.

Our reporting engine also allows us to do some clever analysis on a client's infrastructure/Application. We also provide an additional document called Management Summary which is mainly aimed at higher management and aims to provide an insight into the organization's security profile.

We are able to provide stats and do analysis to show how a particular client's infrastructure has changed with time and if the security has followed the same pattern or not.

If a client has global infrastructure spread across various countries then we can also do an analysis showing things such as how do the different regions compare, are their common issues across different regions etc.

Most people find this analysis extremely useful in justifying whether the budgets allocated towards security have been rightfully spent or not.

At BlackHat USA 2011, you organized a workshop with Aleksander Gorkowienko titled 'The Art of Exploiting Lesser Known Injection Flaws'. You also released couple of tools which our readers might be interested in. Can you tell us more about these tools?

SS: Our workshop discussed the following injection flaws:

- Hibernate Query Language Injection
- LDAP Injection
- XPATH Injection
- XML Entity Injection

We found that the awareness about these flaws is not good and hence the title. We researched into these areas and also came up with some new attack vectors particularly within the XPATH Injection vulnerability. We released 2 tools during our workshop for exploiting blind LDAP and blind XPATH injection respectively.

Like SQL Injection, an LDAP or a XPATH Injection is when un-validated users input is used within the LDAP or XPATH queries respectively. The end result is that the original query can be manipulated and an attacker could then extract arbitrary information from the LDAP server or the XML file (in case of a XPATH Injection). We showed various examples of these vulnerabilities and talked about the various impact of these vulnerabilities ranging from authentication bypass to extracting arbitrary information from the back-end systems.

The LDAP Injection tool requires you to know a few things about LDAP such as how to write LDAP filter, but the XPATH Injection tool is fully automated.

You can point it to the vulnerable URL and it will download the entire XML file from the vulnerable web/application server. The tools can be downloaded for free from the 7safe website: <http://penetration-testing.7safe.com/tools/>.

What are your responsibilities as the Head of Penetration Testing at 7Safe and what kind of team do you lead?

SS: I head a team of 8 and we conduct penetration testing for our clients. We do all sorts of pentesting such as:

- Web Application Assessment
- Binary Application Assessment
- Mobile Application Assessment (Iphone/Android)
- Internal/External Infrastructure Assessment
- VPN Assessment
- Citrix Breakout Assessment
- Wireless Assessment
- Database Assessment
- Server hardening review
- Firewall Rules Assessment
- Social Engineering

My responsibilities as head of the team are the following:

- Recruiting, managing, mentoring and developing a team of security consultants.
- Ensure that the technical team has good skills sets, adequate knowledge sharing is in place, Industry standards such as CREST, OWASP etc are adhered to at all times.
- Strong input in pre-sales activities.
- Project, Team and People Management.
- Involvement in projects end-to-end from sale through to delivery.
- Strong input into scheduling consultants on various projects.
- Responsible for developing new services within penetration testing.

Penetration Testing is a very niche area, how do you go about providing training to your team members?

SS: We are fortunate that we also have a training department at 7Safe and we therefore run a variety of courses in IT security. These courses are at various levels from introductory through to advanced courses which are aimed for pentesters and security professionals. So, all my team members go on these courses as a part of their career development. I am fortunate that most members of my team (if not all) are self motivated and they spend a lot of time reading up on the Internet and researching new attack vectors. We have a very good culture of knowledge sharing and we have one of the best *hack-labs* in which we can recreate almost any security flaw. It helps us in training the team and also in carrying out R&D activities. Pentesting is one profession in which it's hard to survive unless you really love it. So self motivation is a key and we only hire individuals who do this as a hobby and don't think of it as a 9-5 job.

Have you taken part in any Capture the Flag competitions? If so, can you please tell our readers what the competition and what security professionals can gain from such events?

SS: Yes, I have. I used to participate a lot more a years ago and I still love them. The last one I participated was at AppsecUSA and it was without a doubt the best CTF event I have ever participated in. More details about the CTF can be found here: https://www.owasp.org/index.php/Category:OWASP_CTF_Project.

If any of the readers are attending any OWASP Appsec events in the near future then they should check it out. The event organisers can reach out to steven.van.der.baan@owasp.org and get him to host the CTF at their events.

The CTF was a series of questions and you get marks for each question. Some questions are easy and can be solved in seconds while some can take a good few hours. The questions are in a number of areas of IT security such as application security, password cracking, cryptography etc. You learn so many new things and get to practice exploiting things which you may have only heard of but never come across in real life. So, it gives you confidence in your ability. It also gives you an idea on how good your peers are, where do you stand and what skills you need to work on to get better.

I also find CTFs' very good for team building. We have done a few CTF in which we participate as a team and that helps in getting an appreciation for the skills of other team members.

What is bsqibf?

SS: Bsqibf is a utility for exploiting SQL injection in a web application. There are a number of tools out there for exploiting SQL Injection and some of these are so much better than bsqibf, but, bsqibf has its own unique selling points.

The tool allows extraction of data from Blind SQL Injections. It accepts custom SQL queries as a command line parameter and it works for both integer and string based injections. Databases supported are:

- MS-SQL
- MySQL
- PostgreSQL
- Oracle

Bsqibf is the only tool which supports advanced exploitation of SQL Injection against an Oracle back-end. It has a number of Oracle exploit built-in and in quite a few scenarios which lets you execute OS code against the back-end Oracle database from the web based SQL Injection. It's not a point and click tool. It's a tool for penetration testers who know what they are doing. The following modes of attacks/types are supported in bsqibf:

- Type 0: Blind SQL Injection based on true and false conditions returned by back-end server
- Type 1: Blind SQL Injection based on true and error(e.g syntax error) returned by back-end server.
- Type 2: Blind SQL Injection in *order by* and *group by*.
- Type 3: extracting data with SYS privileges (ORACLE `dbms_export_extension` exploit)
- Type 4: is O.S code execution (ORACLE `dbms_export_extension` exploit)

- Type 5: is reading files (ORACLE `dbms_export_extension` exploit, based on java)
- Type 6: is O.S code execution `DBMS_REPCAT_RPC.VALIDATE_REMOTE_RC` exploit
- Type 7: is O.S code execution `SYS.KUPP$PROC.CREATE_MASTER_PROCESS()`, DBA Privs

The new version will have even more enhancements for exploiting Oracle via SQL Injections in a web application.

Can you name a few commercial and open source tools that you use for exploiting web applications?

SS: We use a variety of commercial tools. To name a few, we use Burp Professional, Netsparker, Tenable Nessus, Nexpose etc. We are always evaluating new commercial products and making sure that we use the best tools out there. We also have a number of in-house written software/scripts. To name a few open source tools, they are nmap, metasploit, ike-scan, nikto, hoppy, sslscan, fierce, sipscan, nbtscan, john-the-ripper etc.

What are some of the soft skills that Penetration testers should pay close attention to?

SS: Soft-skills are extremely important for security consultants/Penetration testers. Often we find that the client's awareness about pentesting or security is not great and they seek our advice on what systems should be tested and what is the level of information they should provide us. Thus it's important that consultants are willing to speak to customers, understand what their requirement is and also guide them on what type of test would be most valuable for them. Soft-skills also come into play when you need to scope the test. The consultants must understand and guide the clients in getting the right scope for the test, what IP addresses/network segments are included, which applications are to be tested; does the application need testing as an authenticated user, what are the different levels of access the application provides etc etc.

Finally, the report writing skills are very important. Not all good consultants write equally good reports. I have seen a few examples where the consultants have done a brilliant job but the report does not justify the quality of test.

The executive summary within the report tests out most consultants and the ability to explain a highly technical issue to a not so tech-savvy CEO takes some skills.

What books would you recommend for Web Application Penetration testing?

SS: I would thoroughly recommend the Web Application's Hackers handbook. It is written by two professionals who know the art of web application pentesting inside out and their book gives a very good understanding for a beginner/intermediate level. I haven't had a chance to look into the 2nd edition of the book, but I have heard good feedback and it seems even better. Other books which I would recommend are:

- Database Hackers Handbook
- Oracle Hacker's Handbook
- SQL Injection: Attack and Defense
- XSS Attacks: Cross Site Scripting Exploits and Defense

In addition to the books, it is also very useful to read the blogs/news feed from various sources on the Internet to keep up-to-date with new vulnerabilities. I would recommend reading the OWASP moderated feed: https://www.owasp.org/index.php/Application_Security_News. It aggregates feeds from a number of blogs.

In addition to this, I would also recommend the readers to look at the material which OWASP has on their website. It really is a treasure trove for the application security. In particular, I would recommend reading the OWASP testing guide: https://www.owasp.org/index.php/Category:OWASP_Testing_Project.

What are some of your hobbies?

SS: I have a six months old daughter (Shriya). So most of my time goes into playing with her, which I look forward to all the time. Other than hacking or reading about hacking, I love cricket. I could watch any cricket game. I remember once I had an argument with my wife because I wanted to watch a match between Kenya Vs UAE and she wanted to change the channel. LOL

ARAO