12-2017

Teaching Security Defense Through Web-Based Hacking at the Undergraduate Level

Brent Wilson

George Fox University, bwilson@georgefox.edu

TEACHING SECURITY DEFENSE THROUGH WEB-BASED HACKING AT THE UNDERGRADUATE LEVEL

Brent Wilson
George Fox University
Newberg, OR. USA
bwilson@georgefox.edu

ABSTRACT

The attack surface for hackers and attackers is growing every day. Future cybersecurity professionals must have the knowledge and the skills to defend against these cyber attacks. Learning defensive techniques and tools can help defend against today's attacks but what about tomorrow's? As the types of attacks change so must the cybersecurity professional. The only way for the cybersecurity professional to achieve this nimbleness is to understand the structural anatomy of the various attack types. Understanding the threat environment is the key to future success. Security defense through offensive techniques should and can be taught at the undergraduate level. Using the OWASP Mutillidae project [5], students can have a self-contained, sandbox environment for dissecting and discussing cyber attacks.

Keywords: cybersecurity, cybersecurity education, web-based hacking, cyber defense

INTRODUCTION

The importance of information technologies in today's society and our ever-increasing reliance on technological infrastructures creates a local, national, and global dependence on both current and future technologies. There are those who continue to voice concerns over this dependence due to the apparent lack of security throughout information systems. A primary point of focus is the growing reliance on the Internet and the vast client-server technologies worldwide. There are expansive breadths of opportunities, both personal and corporate, made possible by advances in Internet technologies. As a society, we are able to access data as never before and to connect to devices in unprecedented ways.

In addition to the positive aspects provided by the Internet and networking technologies, negative aspects also present themselves in unexpected ways. Criminal activity has been around for a very long time but has been thrust into our homes, schools, and businesses by the pervasiveness of the Internet. Today's criminals have a new platform for their activities, one which can shroud them in virtual anonymity anywhere in the world. People are so awestruck by the scope and prevalence of these endeavors that oftentimes these activities are simply considered reactionary measures. Educational institutions have a responsibility to equip new graduates to fight these nefarious activities at every turn.

The objective of this research was to analyze the impact of incorporating offensive security techniques and methodologies into the curriculum to improve information security education. "Ethical hacking" is a more offensive and proactive method for teaching information security. It provides a controlled environment for the student to carry out various attacks along with an opportunity to debrief and discuss attack mitigations and countermeasures. This methodology may be more successful in preparing cyber security professionals to combat and defend against the unethical hacker's system intrusions. Future cybersecurity professionals will need to be armed with the same knowledge and skill sets being used by attackers. They must understand their threat environment. They must be grounded in the theoretical aspects of computing in order to be successful in the ever-changing landscape of system and network security. Lastly, they must have an ethical grounding which provides a sound moral compass.

MOTIVATION

In 2012, a computer security course was introduced into the undergraduate computer science curriculum as both a computer science and an information systems elective at George Fox University. Over the past five years many students have chosen to enroll. The percentage of graduates having taken the course continues to hover just above 50%. The course was designed as a defensive course based upon theoretical concepts of security. Standard topics included threat environment definitions, security planning, cryptography and cryptographic systems, access control, firewalls, host and data security, and incident and disaster response.

Many of the students who have taken the computer security course also enroll in a client-server technology course. This course requires each student to fully design and implement a LAMP (Linux, Apache HTTP Server, MySQL, and PHP) stack application. Each student's application is tested for basic security vulnerabilities such as SQL and XSS (cross-site scripting) injections. Students who have had the security class fail these vulnerability tests at the same rate as those student who have not had the security class.

The most significant hurdle in moving from a theoretical defensive approach in security education to an offensive one is the development of a secure self-contained environment with known vulnerabilities that can be exploited. Integrating security concepts throughout the curriculum can be achieved quite easily in a theoretical defensive stance. Introductory programming courses can discuss the need for user input sanitization while upper division courses can address topics such as invalid SQL queries, access control, and other theoretical concepts. Transitioning to an offensive stance requires a framework which can be utilized in any course without significant prior knowledge.

ETHICAL CONSIDERATIONS

Ethical hacking has been gaining popularity within security courses at various schools for a number of years now. Curriculum within security courses containing ethical hacking include training in ethics and law in addition to requiring professors to comply with ethical behavior as a role model. There is often concern about teaching such classes. Risks associated with teaching

hacking techniques tend to be addressed by stating that "… students who learn traditionally illegal computing skills in the course of studying computer security will use those skills for the greater good far more often than they will use them illegally or immorally [6]."

For some, this definition may be sufficient, however it must be specified that teaching ethical hacking produces two separate and identified risks. The first is to the community if a student chooses to utilize this newly acquired skill for evil. The second risk is to students in the program who may be enticed into unethical/illegal activity from the training received. Mitigation of these risks is essential to the success of any cyber security program. The first risk must be addressed through the study of information security standards along with local, federal, and international laws. Consequences of violating such laws are easily studied through current case studies. Mitigating the risk of students being enticed to attempt unethical/illegal activities must focus on a combination of standards and laws in addition to the exposure of the gray hat hacker as a non white hat hacker. Gray hats tend to be seen by students as still partially good, yet they have no authorization or legal standing for their activities. Falk [3] makes the point that a gray hat hacker is merely a black hat hacker in a morally ambiguous state. Falk states that "gray hacking is a morally wrong action and as such should be neither condoned by administrators, managers, or other personnel, nor practiced by well-meaning computer professionals." Gray hat hacking is the gateway to black hat hacking.

Teaching hacking techniques in a security course must begin by providing students with a clear and concrete boundary between appropriate and inappropriate behavior. These guidelines/policies need to be established through consultation with your institution's Chief Security Officer and possibly legal review. Students may be required to review and sign a contract of expected behaviors. The goal is to create an environment that protects everyone moving forward [7].

Environment/Tools

Initially, we created a virtual machine using Ubuntu and VirtualBox. The framework used for our ethical hacking exercises is a free, open source, deliberately vulnerable web-application called Mutillidae from OWASP [5]. Mutillidae is a penetration test environment which can be installed in any of the following platforms:

- LAMP (Linux, Apache HTTP Server, MySQL, and PHP, Perl, or Python)
- MAMP (Macintosh, Apache HTTP Server, MySQL, and PHP)
- WAMP (Windows, Apache HTTP Server, MySQL, and PHP)

We chose the LAMP stack on our Ubuntu virtual machine.

Mutillidae currently contains 43 type vulnerabilities and challenges which can be used in many courses. These have been created based upon the OWASP Top Ten 2007, 2010, and 2013 listings [4]. For some of the more important categories such as cross-site scripting, Mutillidae provides multiple vulnerability contexts in HTML, JavaScript, and even JSON injection. Contexts of SQL injections allow for data extraction, uploading of shell scripts, and authentication bypass.

Mutillidae provides the students an open environment for experimentation. The application pages contain 'live' vulnerabilities. Students are not expected to enter specific statements which the platform matches against a list of correct solutions. There are multiple solutions for exploitation and the student is encouraged to experiment. Mutillidae also offers a reset feature which the user can execute to restore the application to its original state.

EXAMPLE EXERCISE

The following is an example of a command injection using Mutillidae. The client interface consists of a dropdown list and a lookup button as seen below (Figure 1). Once a tool has been selected from the interface the client information is sent to the server in an HTTP request. The server then processes the request and returns the information to the client.

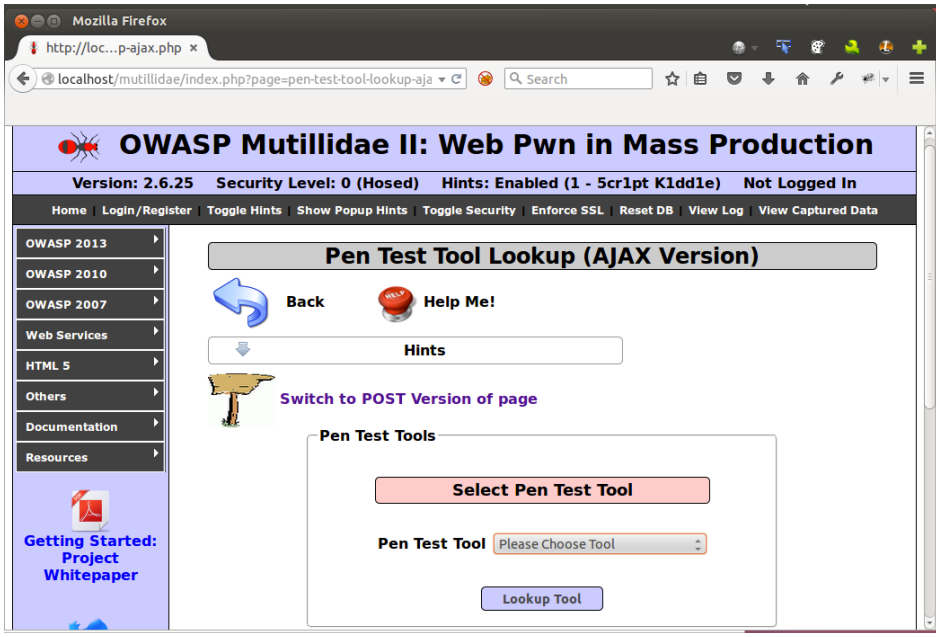

Figure 1. Mutillidae

Upon examining both the HTTP request and response there is a parameter named `ToolID` that is passed in the request that is also directly returned in the response without change. This creates a significant vulnerability since a hacker can inject JavaScript commands for the `ToolID` in the HTTP request and it will be returned in the response and subsequently executed on the client. The following line of code is from the HTTP response after having selected a tool. In this case, the `ToolID` had the value 1.

```
{"query": {"toolIDRequested": "1", "penTestTools": []}}
```

To complete the command injection, code must be developed that replaces the 1 in the line of code. The code must be crafted to be syntactically correct with the current line of code to ensure proper execution on the client machine. The following code could be used as a simple command injection that displays the client's cookie to the screen.

```
"}};alert(document.cookie);//
```

In order for this command to be passed through the server to the client as the JavaScript, it must be sent to the server URL encoded. The encoded statement above would be as follows:

```
%22%7d%7d%29%3b%61%6c%65%72%74%28%64%6f%63%75%6d%65%6e%74%2e%63%6f%6f%
6b%69%65%29%3b%2f%2f
```

The completed command injection when ran can be seen below (Figure 2).

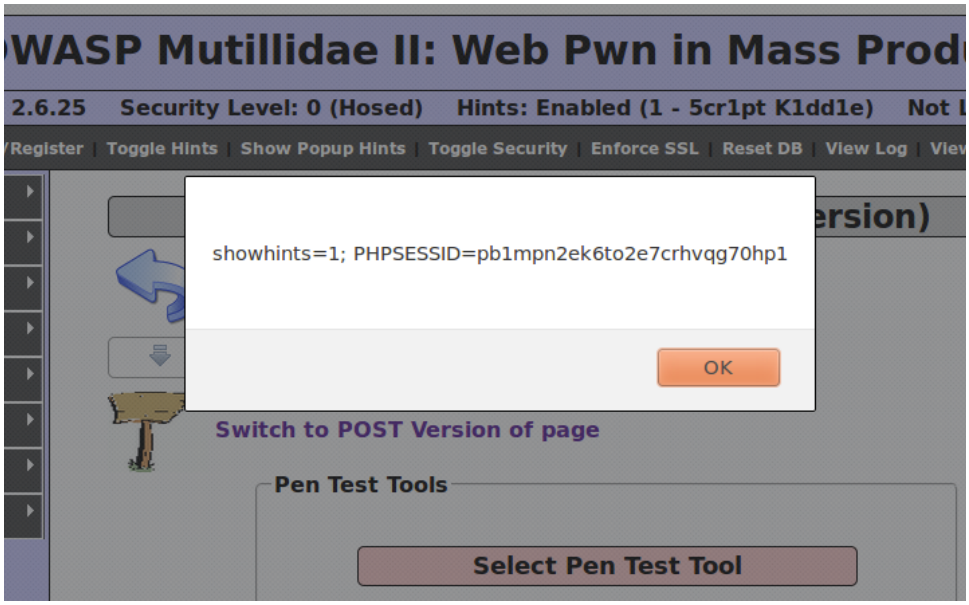

Figure 2. Completed Command Injection

RESULTS

At the conclusion of the spring 2017 semester, an anonymous survey was given to the students enrolled in the courses which implemented the offensive hacking techniques using the virtual machine and the OWASP Mutillidae application. The total sample size was 32. The survey results were as follows:

Q: What was your understanding of security attacks BEFORE you took the security class(es) this spring?	
62.5%	Knew very little, only knew some attacks by name
37.5%	Understood various attacks in concept only
0%	Understood quite a bit including the knowledge to perform an attack

Q: How much did the hands-on hacking exercises increase your knowledge of attacks?	
0%	None
0%	Very little
37.5%	Moderately

37.5%	Quite a bit
25%	Massively

Q: How much did the hands-on hacking exercises increase your knowledge of the defense of attacks?	
0%	None
6.3%	Very little
31.2%	Moderately
43.8%	Quite a bit
18.8%	Massively

Q: Prior to the security class(es) this spring, had you:	
0%	Attempted an actual unethical attack
15.6%	Seriously thought about attempting an unethical attack
84.4%	Neither attempted nor thought about attempting an unethical attack

Q: After the security class(es) this spring, what is the likelihood that you will engage in an unethical hack/attack?	
75.0%	Never
25.0%	Low
0%	Moderate
0%	High
0%	Surething

CONCLUSIONS

College students today are entering into the computer sciences as users of computers and information systems. While this generation has grown up with computer systems, they do not have the depth of understanding as to how they work and more importantly how they can be broken. The survey data shows that students have basic definition knowledge of security attacks but lack a deep understanding of how attacks actually occur. This lack of knowledge will prevent them from being able to fully protect future systems from current and future attacks. The survey also shows that performing offensive exercises greatly improves their knowledge of systems and how they operate. The one aspect of some concern is that a greater percentage of students feel they may engage in an unethical hack/attack after having taken the security courses than had even thought about doing so prior to the security courses. This information will be used to re-evaluate the effectiveness of the security standards and laws knowledge units in these courses.

As a final observation, it was noted anecdotally that attendance had been higher than ever before throughout the entire semester. The instructor reported that students were genuinely more engaged in the material than in past semesters.

REFERENCES

[1] Bai, Y., Wang, X. (2015). Teaching offensive security in a virtual environment. *Journal of*

Computing Sciences in Colleges. 31(1), 140-142.

[2] Dornseif, M., Gartner, F.C., Holz, T., & Mink, M. (2005). *An Offensive Approach to Teaching Information Security: "Aachen Summer School Applied IT Security."* (Technical Report 2005-02). Aachen, Germany: Department of Computer Science, RWTH Aachen University.

[3] Falk, C. (2014). *Gray hat hacking: Morally black and white*. (CERIAS Technical Report, 2004-20). Lafayette, IN: Center for Education and Research in Information Assurance and Security, Purdue University.

[4] OWASP. (2017, May 9). *Electronic References*. Retrieved from https://www.owasp.org/index.php/Main_Page

[5] OWASP Mutillidae II. (2017, May 9). *Electronic References*. Retrieved from https://sourceforge.net/projects/mutillidae/?source=typ_redirect

[6] Pashel, B. A. (2007). Teaching students to hack: ethical implications in teaching students to hack at the university level. *Proceedings of the 2006 Information Security Curriculum Development Conference*, InfoSecCD '06, September 22, 2006 - September 23, 2006, 197–200. Association for Computing Machinery.

[7] Radziwill, N., Romano, J., Shorter, D., & Benton, M. (2015). The Ethics of Hacking: Should It Be Taught?. *Software Quality Professional*. 18(1), 11-15.

[8] Trabelsi, Z., & Ibrahim, W. (2013). A hands-on approach for teaching denial of service attacks: A case study. *Journal of Information Technology Education: Innovations in Practice*. 12, 299-319.