**Advanced Security 2 - Assignment 1 – 15%**

**Jake Bolger**

**C18395341**

**Part A**

**In this assignment you will be required to research on the skills, certifications and training you will require to be a security expert. List your findings in one or two pages. Hint: start by looking at security job advertisements and reports such as http://goo.gl/c5zikq and** [**http://goo.gl/4s5aAe**](http://goo.gl/4s5aAe)**?**

Skills research

An aptitude for computers is possibly the number one quality of a cyber security expert. Other key skills and qualities include:

* In-depth knowledge of computer operating systems, hardware and software.
* First-class problem-solving skills.
* A strong ability to work well under pressure.
* Solid telecommunications knowledge.
* Rigorous attention to detail.
* persistence and determination.
* Excellent abilities in mathematics.
* Technical Aptitude.
* Knowledge of Security Across Various Platforms. ...
* Communication Skills.
* Fundamental Computer Forensics Skills.
* A Desire to Learn.
* An Understanding of Hacking.

Certifications and Training

1. Certified Information Systems Security Professional (CISSP):

A CISSP designs, implements, manages, and controls the architecture, design, or management of business environments for security.

2. Certified Information Systems Auditor (CISA):

In the IT community, the CISA certification is regarded as the gold standard, and it will make you stand out from the crowd. Obtaining and maintaining CISA certification requires a high level of commitment. It demonstrates your intelligence and ambition, both qualities needed for leadership roles.

3. Certified Information Security Manager (CISM):

Certificate in Information Security Governance. Information Risk Management. Information Security Program Development & Management. Information Security Incident Management.

4. Security+:

# Certification validates the skills required for core security functions and for pursuing a career in IT security.

5. Certified Ethical Hacker (CEH):

To earn the title of Certified Ethical Hacker, you need to demonstrate knowledge of evaluating computer security by looking for weaknesses and vulnerabilities in the target system.

6. GIAC Security Essentials Certification (GSEC):

Through the GIAC Security Essentials certification, practitioners demonstrate a depth of understanding of information security beyond simple concepts and terminology. By holding the GSEC certification, participants demonstrate their ability to perform hands-on security tasks related to IT systems.

7. Systems Security Certified Practitioner (SSCP):

For IT professionals with practical, hands-on security knowledge in operational roles, the Systems Security Certified Practitioner (SSCP) certification is the ideal certification. ... Security Operations and Administration. Access Controls. Risk Identification, Monitoring, and Analysis.

8. CompTIA Advanced Security Practitioner (CASP+):

The CASP+ certification covers security architecture, senior security engineering, governance, risk management, and compliance skills, testing enterprises for cybersecurity readiness, and leading technical teams to implement cybersecurity.

9. GIAC Certified Incident Handler (GCIH)

With a GIAC Incident Handler certification, you can demonstrate your proficiency in detecting, responding, and resolving computer security incidents using a wide range of skills.

10. Offensive Security Certified Professional (OSCP):

It teaches ethical hacking methodologies, as well as how to use the tools included with Kali Linux, which is an ethical hacking certification offered by Offensive Security

**Discuss why there is a shortage of security personnel worldwide.**

Now a days there are a variety of reasons why there is a shortage of security personnel worldwide. These reasons are as follows: lack of corporate security programs, underfunded security resources, lack of good tools and protocols, not enough security patches, not enough email security practices and finally people who don’t follow the policies of their company in security. Other reasons are the lack of interest from younger generations, increased number of attacks and not enough skilled defenders.

**What measures/actions should be taken to address this shortage?**

The measures that should be taken to address this shortage of security personnel are, to hire managed security service providers where your in-house talent is lacking and make sure their expertise matches your compliance requirements.

Provide detailed, enticing descriptions of each role when recruiting.

Teaching students should be done through real life scenarios.

Develop apprenticeships to recruit and prepare future employees. Some states offer tax credits to employers who hire apprentices. Support unique training exercises. IBM has developed mobile cybersecurity ranges help college students and professional practice responding to attacks.

Support mental health and wellness initiatives.

The last on is invest in employee training and certification. 93% of employees would stay at a company longer if it invested in their career.

**Do you think you have enough skills to be a security expert? If no, what are you missing and if yes what are your strengths?**

No, although I have a basic understanding of security, I am no expert. I have previous experience from college including different security techniques and cyphers, encryption, decryption, and penetration testing. I am missing a lot of manual knowledge and physical experience in security. In order to become an expert, I will certainly need to get real life experience in a job or company.

**Part B**

**In this part, you will be required to test and identify security flaws using any two static code analysis tools such as https://goo.gl/VvlkFj. While these tools do not provide 100% guarantee, they can identify most of the security flaws. Use one programs from your labs or assignments you did in third or fourth year. The submission in this part will be a list of identified security flaws in the code.**

The first static code analysis tool that I used is called ‘Guardrails’ which allows me to scan my work for errors and adjust my workflow. This was used to identify security flaws in my code from my games engines assignment I did. I installed this tool on my GitHub account and then scanned for flaws as shown below:

Graphical user interface, text, application

Description automatically generated

The flaws that were found are as follows:

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

The second tool I used was a tool called ‘DeepSource’. Again I linked it with my GitHub account and used my repositories to scan for security flaws.

A screenshot of a computer

Description automatically generated with medium confidence

In the codebase report there were a lot of issues, there were 68 in total. Most of the issues were anti-pattern issues, but there were still two bug risk issues. Below is a screenshot of all the issues listed:

A screenshot of a computer

Description automatically generated with medium confidence

Next I have explained the issues and flaws in more detail.

**Accessor like method has return type `void`:**

A screenshot of a computer

Description automatically generated with medium confidence

**Consider simplifying the boolean comparison expression for concisionCS-R1031:**

A screenshot of a computer

Description automatically generated with medium confidence

**Abrupt application exit CS-W1005:**

**A screenshot of a computer screen

Description automatically generated with medium confidence**

**Use `string.IsNullOrEmpty` or `string.IsNullOrWhiteSpace` to check for empty strings CS-R1014:**

Text

Description automatically generated

**Exception thrown is generic CS-R1015:**

Graphical user interface, text, application

Description automatically generated

**Consider specifying the `CultureInfo` parameter when possible CS-R1018:**

Text

Description automatically generated

**Exception caught is generic:**

Text

Description automatically generated

**Part C**

In this part I will be investigating the use of Basic and Advanced operators. For each operator I will give two examples of where they can be used. The examples will include when the operators are used alone and when they are used together or in combination.

**Basic Operators:**

**Examples of usage for + operator**

This operator is used to include keywords.

Alone: internet + security

Combination: internet + security + application

**Examples of usage for – operator**

This operator is used to exclude keywords.

Alone: application - internet

Combination: application + internet - security

**Examples of usage for ~ operator**

Used to include synonyms and similar words.

Alone: internet **~**security

Combination: internet ~security - google

**Examples of usage for . operator**

Used to include single character wildcards.

Alone: .ternet

Combination: site:cars.blogs.irishindependent.com

**Examples of usage for \* operator**

Used to include single word wildcards.

Alone: internet \* security

Combination: internet – security “hello \* world”

**Examples of usage for “” operator**

Used to include exact matches.

Alone: ”internet security”

Combination: “hello World” AROUND(3) “Jake Bolger”

**Examples of usage for | / OR operator**

Used to include keywords where either one keyword or another is matched.

Alone: internet OR security, internet | security

Combination: internet OR security ~google

**Advanced Operators:**

**Examples of usage for Allintext operator**

Only results containing *all* of the specified words somewhere on the page will be returned.

Alone: allintext:advanced security

Combination: allintext: security site:google.com

**Examples of usage for allintitle operator**

Results containing *all* of the specified words in the title tag will be returned.

Alone: allintitle:advanced security

Combination: allintitle: “operators” “for \*this assignment”

**Examples of usage for allinurl operator**

Results containing *all* of the specified words in the URL will be returned.

Alone: allinurl:advanced security

Combination: allinurl: google secuirty-keywords nikon

**Examples of usage for cache operator**

Used to search and display a version of a web page as it was shown when google crawled it.

Alone: cache:website.com

Combination: cache:website.com OR cache:google.com

**Examples of usage for Define operator**

A dictionary built into Google, basically. This will display the meaning of a word in a card-like result in the SERPs.

Alone: define:especially

Combination: define:especially + sincerely

**Examples of usage for filetype operator**

Used to limit the search to text found in a specific file type.

Alone: mysql filetype:pdf

Combination: mysql filetype:pdf – mysql filetype:txt

**Examples of usage for info operator**

Find information about a specific page.

Alone: info:security.com

Combination: info:security.com / id:security.com

**Examples of usage for intext operator**

Find pages containing a certain word (or words) somewhere in the content.

Alone: intext:security

Combination: intext: “my name is jake vs you”

**Examples of usage for Intitle operator**

Used for searching a string text within the title of a page.

Alone: intitle: index of

Combination: intitle : cars site:thesun.com intitle:earnings

**Examples of usage for inurl operator**

Used to search for a string within a URL.

Alone: inurl:mytext.txt

Combination: site:google.com -inurl:www

**Examples of usage for link operator**

Is used to search for pages that link to the requested URL.

Alone: link:www.website.com

Combination: link:thesun.com -site:irishindependent.com cars

**Examples of usage for related operator**

Find sites related to a given domain.

Alone: related:security.com

Combination: related google.com | related security.com

**Examples of usage for Site operator**

Used to limit the search query to a specific domain or web site.

Alone: site:website.com

Combination: tudublin site:website.com OR site:.gov

**Examples of usage for numrange operator**

Find results from a certain number range.

Alone: numrange:2-8 site:google.com

Combination: numrange:

**Examples of usage for daterange operator**

Find results from a certain date range.

Alone: daterange: 220899-231099

Combination: daterange: 220899-231099 site: security.com

**Next, I will say whether it is possible to achieve the same results without using the operators given above.**

Yes, it is possible you can use googles advanced search which allows you to achieve the same results without using the operators above. Below is a picture and example of the advanced google search:

Graphical user interface

Description automatically generated with medium confidence

**Using the list of operators above I will identify if there are any equivalent operators that can be used in Bing.**

Operators that can be used in Bing and Google:

* Contains:
* Ext:
* Filetype:
* Intitle:
* Related:
* Site:
* \*
* -
* “ ”

Most of the Google operators perform the same task when using Bing so I have not relisted all of them. However, there are some operators that don’t work in Bing:

* Intext
* inurl
* related
* cache
* info
* allinurl
* allintitle
* link:
* ~

**Finally, I will list ten search engines outlining their advantages and disadvantages over Google or Bing.**

1. **Yahoo**

Advantages:

* Mail (1Tb) as opposed to googles 15GB
* Information on almost every subject imaginable.
* Powerful search engines.
* Ability to do research from your home versus research libraries.
* Information at various levels of study. ...
* Message boards where people can discuss ideas on any topic.

Disadvantages:

* There is a lot of wrong information on the internet. Anyone can post anything, and much of it is garbage.
* There are predators that hang out on the internet waiting to get unsuspecting people in dangerous situations.
* Some people are getting addicted to the internet and thus causing problems with their interactions of friends and loved ones.
* Easy to waste a lot of time on the internet. You can start surfing, and then realize far more time has passed than you realized. Internet and television together of added to the more sedentary lifestyles of people which further exacerbates the obesity problem.

1. **AOL**

Advantages:

* The AOL network includes many popular web sites like engadget.com, techchrunch.com and the huffingtonpost.com.
* AOL email makes it easy to keep in touch with friends, family, and business partners. We will get unlimited storage space, and this software suddenly adds personality to emails that can modify fonts, colors, stationery, and signatures.
* AOL is good at controlling spam and helps direct spam emails out of your inbox.
* With AOL, tabs in the browser keep multiple sites open without messing up your screen.
* Your favorite websites and AOL Search are enhanced by Google, and you are automatically protected from phishing sites that are recognized when you browse the Web using the latest AOL software.
* AOL Instant Messenger (AIM) has also been integrated in the latest America Online (AOL) so you can see your friends who are online and instantly chat, share photos, and more.
* AOL XM Radio has collaborated with the largest and most popular music portal in the pop world, and Yahoo has been limited to non-DRM music is very interesting. Good in the field of digital entertainment is undoubtedly suitable.

Disadvantages:

* Speed when opening is not fast enough.
* The display is not good.

1. **One Search**

Advantages:

* No cookie tracking, retargeting, or personal profiling.
* No sharing of personal data with advertisers.
* No storing of user search history.
* Unbiased, unfiltered search results.
* Encrypted search terms.

**Disadvantages:**

* Can return very large number of results, which can be overwhelming.
* Despite being named "OneSearch," it does not search everything the library owns!
  + Several databases that are not searched by OneSearch at all and some databases that are only partially searched.
* OneSearch is a general tool – meaning that it covers all subjects and isn’t very strong in any particular one.
  + The more specific or obscure your research needs, the less helpful OneSearch will be.
  + If you need to focus your search to a particular topic or subject, you may want to move to a subject specific database.

1. **Baidu**

Advantages:

* Has the upper hand in China
* Baidu is [reported](http://www.chinainternetwatch.com/12678/search-engine-market-overview-2014/) to control around 80% of Chinese online search market
* This is the most-used Internet application in China.  And it looks like there continues to be much room for growth.  Consider that Internet consumption among China’s population is still under 35%.
* Baidu has a highly scalable business model, i.e., business owners can easily buy and target ads on the system.  In fact, only a small portion of China’s millions of businesses use paid search marketing.
* With a massive user base, Baidu is looking for ways to offer more services.  To this end, the company has been aggressively investing in research & development.  There also will likely be more acquisitions.

Disadvantages:

* Not an international search engine
* In 2010, Google left the Chinese market.  Despite this, Baidu still must deal with fierce rivals.  Some of the most threatening include Alibaba and Tencent.  These companies have large customer bases and are looking at the lucrative paid search market.  Even **Microsoft**(Nasdaq:[MSFT](https://investorplace.com/stock-quotes/msft-stock-quote/)) is a player in the Chinese market.
* Baidu’s shares trade at a nose-bleed level of 95 times earnings.  The problem is that it’s going to be extremely tough to maintain its hefty growth rates.  In other words, there could be a serious correction in the stock if there is even a small stumble.
* The ads on Baidu are far from cheap.  While this helps to boost revenue, it could make it more difficult to increase its user base.

1. **Wolfram alpha**

Advantages:

* Does calulations. for example if you enter “mortgage 2000” as input it will calculate your loan amount, interest paid etc.
* It answers questions directly rather than pointing to another source.

Disadvantages:

* Capabilities depend on what's in the database; not all questions can be answered.

1. **DuckDuckGo**

Advantages:

* Perfect privacy. No data on your online searches collected or stored. (If you want this privacy to extend further than searches and to all your browser activity, you need to install the complementary Duckduckgo products, which I described below).
* No ads targeting you based on your searches.
* No social engineering techniques are used based on your searches and other interests.
* You can be sure you are getting the same search results as all other users (no targeting or profiling).
* 1-page search results. Infinite scroll: as long as you keep going down, more search results keep loading. It’s a well-known fact that many users don’t make it to the second page of Google search results, but Duckduckgo just presents to you more info on the same page so you never have to click next and lose the initial results from sight.

Disadvantages:

* Has a few nice extra perks and features, but still not as many as Google. Just think of Google Maps, Google Flights, Google Finance, Google Books, etc.
* Less personalization: Duckduckgo doesn’t remember your search history, which is technically an advantage for privacy, but it can also be less convenient sometimes.

1. **Yandex**

Advantages:

* Yandex is the No. 1 search engine in Russia, with a market share of about 64%.  During March, yandex.ru attracted 38.3 million unique visitors.
* Yandex also has a variety of add-on services, like Yandex.News, Yandex.Market, Yandex.Mail and Yandex.Maps. There are also connections to mobile devices, which allow for location-based information.
* Economy.  Russia is one of the world’s top emerging economies.  Since 1998, the growth rate has averaged about 7% per year.  Yet the economy took a big hit from the financial crisis.  However, with a strong resources sector — especially in oil — there has been a recent turnaround.
* The Internet and mobile penetration rates are still relatively small in Russia as well.  So there is much room for growth.
* Talent.  Search engines are incredibly complicated.  Essentially, they must use applied mathematics to process massive amounts of information.  There also needs to be mechanisms to ward off manipulation of the results.
* But Yandex has a top-notch team of engineers, which come from across the world.  The company even has several initiatives like the Yandex School of Data Analysis.

Disadvantages:

* Dependence.  Much of Yandex’s revenue comes from advertising.  So far, it has been a strong growth business.  For example, the company served 180,000 businesses in 2010.  Many are small and medium-size operations.
* However, the advertising sector is highly sensitive to changes in the economy.
* Politics.  Despite many market reforms, Russia still has little respect for property rights.  There have been several high-profile cases where the Kremlin has nationalized assets or renegotiated contracts.
* Just recently, Yandex turned over information on some users to the FSB, which is Russia’s federal security service, to go after dissidents.
* Competition.   There are a variety of players in the search business in Russia.  Perhaps the most important is Google, which has about a 22% market share.
* What’s more, the Russian government is creating its own search engine.

1. **Firefox**

Advantages:

* It has security features that are automatically embedded into it.
* The user experience is virtually the same.
* Firefox offers a number of very helpful extensions to the browsers.
* The interface has minimalistic qualities to it.

Disadvantages:

* There are several compatibility issues.
* It consumes a lot of a computer’s memory.
* It does not automatically resume downloads.
* It struggles with HTML 5 quite a bit.

1. **Opera**

Advantages:

* It offers a relatively small download and memory profile.
* It is fast and responsive.
* It has several integrated protections with proven capabilities.
* There is a large community which provides strong support.

Disadvantages:

* It requires a very strict adherence to coding in order to properly operate.
* Companies that do web development don’t see Opera as a high priority.
* The extensions which are built into Opera are not always easy to find.
* It can offer users too many choices sometimes.

1. **Brave**

* Advantages:
* Better privacy and less tracking
* Built in ad blocking
* Faster and more efficient browsing
* Open-source software
* Disadvantages:
* lack of extensions and add ons
* some features stil in beta
* doesn’t always work well with every site

**Part D**

1. **Injection**

Injection flaws are when an attacker uses unfiltered and often [malicious data to attack databases or directories connected to your web apps](https://owasp.org/www-community/Injection_Flaws). Two common injection attacks often get used. First, SQL injection gets used to attack your databases. Second, LDAP injection gets used to attack directories.

Injection attacks use input fields that interact with directories and databases to execute against vulnerabilities. These include usernames, passwords, and other areas that interact with the target. These fields are often left vulnerable due to the lack of an input filter when the database or directory’s development.

1. **Broken Authentication**

Authentication helps apps identify and validate users. Therefore, broken authentication can allow attackers to access and have the same permissions as the targeted user, creating severe web app vulnerabilities. Issues with authentication can give an attacker unfettered access to your data and wreak havoc on your web application.

Authentication vulnerabilities can include improperly hashed and salted passwords, leaks involving user account data, improperly set timeouts, brute force attacks,  or typical password stuffing like password1 or admin1234.

1. **Sensitive Data Exposure**

Sensitive data gets transported or stored without any encryption or other protection, leaving information vulnerable to various attacks.

There are two ways to attack unprotected data. First, while data is transported from the user to the client, attacks as a man-in-the-middle attack can be used to steal data from packets. Second, stored data, while more complicated, can be exposed through encryption keys get stored with data or weak salt/hash or passwords and credentials.

1. **Broken Access Control**

When server-side authorization is misconfigured, broken, or missing, vulnerabilities will occur that can leave your back-end open to attacks.

These attacks often happen with front-end UIs configured with components to give admins access to data or other vital app elements. In this case, most users can’t see the admin function, but those looking to find vulnerabilities will be able to uncover and exploit this flaw with malicious requests.

1. **Security Misconfiguration**

Often web applications are misconfigured, leaving an array of vulnerabilities for attackers to capitalize. Security misconfigured vulnerabilities can include unpatched flaws, unused pages, unprotected files or directories, outdated software, and running software in debug mode.

All aspects of your web applications can be affected by security misconfigurations. When a misconfiguration is found, it is vital to run a security audit to check for attacks or breaches.

1. **Cross-Site Scripting**

Cross-site scripting uses malicious code injected into benign sites to attack a user’s web browser. An attacker will insert the code through a link and, together with social engineering, will lure the user to clicking the link and executing the code. Attackers using JavaScript for XSS vulnerabilities can access a user’s webcam, location, and other sensitive data and functions.

XSS vulnerabilities are common where input is unsensitized. Additionally, XSS can allow attackers to [steal cookies from users’ browsers](https://pentest-tools.com/blog/xss-attacks-practical-scenarios/)and access browsing history and sensitive information.

1. **Insecure Direct Object References**

When database keys or files get exposed to the user, insecure direct object reference vulnerabilities exist. Because of the exposed internal objects, attackers can use enumeration attacks to access those objects and gain data or access to sensitive databases. Often authentication is either non-existent or broken.

Database objects are often vulnerable through URL parameters exposing serialized data keys an attacker can manipulate to access information. Also, static files can be manipulated and changed by an attacker to access sensitive information or other user’s data.

1. **Cross-Site Request Forgery**

Cross-site request forgeries (CSRF) use social engineering to trick authenticated users into clicking a link, as an example and take control of their sessions. Due to having authenticated sessions, the attacker can perform changes to the state of an app vs. data theft.

Applications without the proper dual authentication or cross-site tokens can be vulnerable to CSRF attacks. Those will little knowledge of social engineering are also at higher risk of their authenticated sessions hijacked.

1. **Using Components with Known Vulnerabilities**

Due diligence needs to get done when considering using a third-party code or component in your web application. Many security issues can come with using unfettered code from sources you aren’t familiar with.

To help find what components may be vulnerable, the [National Vulnerability Database](https://www.nist.gov/) has a comprehensive list of known third-party vulnerabilities to help make the best choice.

Every aspect of your app can be affected by vulnerabilities in third-party code. For example, backdoors can get added to financial services code allowing attackers access to sensitive data.

1. **Insufficient Logging & Monitoring**

Unvalidated redirects and forwards is another input manipulation vulnerability again using parameters like GET requests to execute the attacks.

An example of the vulnerability is an attacker manipulating a URL and redirecting users to a malicious site where information can get stolen using social engineering and links with malicious code or links.

**Cross Site Scripting: demo of how it works.**

**1.**

**Graphical user interface, text, application, email

Description automatically generated**

**2.**

**Graphical user interface, text, application

Description automatically generated**

**3.**

**Graphical user interface, application

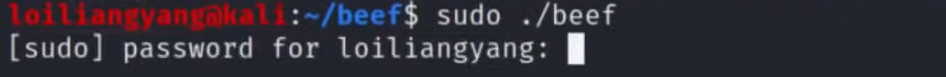
Description automatically generated**

**4.**

**Using browser exploitation framework:**

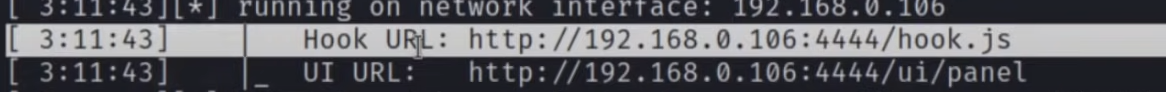
[**https://github.com/beefproject/beef**](https://github.com/beefproject/beef) **download and cd into folder beef.**

**5.**

****

**Loads browser explouts framework**

**6.**

****

**7. copy paste link**

**Graphical user interface, text

Description automatically generated**

**8.**

**Graphical user interface, text, application, email

Description automatically generated**

**9.**

**Graphical user interface, text, application

Description automatically generated**

**10. link 2d interface**

**A screenshot of a computer

Description automatically generated with medium confidence**

**11.**

**Graphical user interface, application, Word

Description automatically generated**

**12.**

**Graphical user interface, application

Description automatically generated**

**13.**

**Fake pretty attack**

**Graphical user interface, application

Description automatically generated**

**14.**

**Graphical user interface, text, application

Description automatically generated**

**Cross Site Request Forgery: demo of how it works.**