CSCI 3403: Project 3

Maura Kieft, Calvin Zikakis, Tiger Yu

Very Basic Linux Exploits (20 points)

Level 0:	bandit0
Level 1:	boJ9jbbUNNfktd7800psq0ltutMc3MY1
Level 2:	CV1DtqXWVFXTvM2F0k09SHz0YwRINYA9
Level 3:	UmHadQclWmgdLOKq3YNgjWxGoRMb5luk
Level 4:	pIwrPrtPN36QITSp3EQaw936yaFoFgAB
Level 5:	koReBOKuIDDepwhWK7jZCORTdopnAYKh
Level 6:	DXjZPULLxYr17uwoIO1bNLQbtFemEgo7
Level 7:	HKBPTKQnIay4Fw76bEy8PVxKEDQRKTzs
Level 8:	cvX2JJa4CFALtqS87jk27qwqGhBM9plV
Level 9:	UsvVyFSfZZWbi6wgC7dAFyFuR6jQQUhR
Level 10:	truKLdjsbJ5g7yyJ2X2R0o3a5HQJFuLk
Level 11:	IFukwKGsFW8MOq3IRFqrxE1hxTNEbUPR
Level 12:	5Te8Y4drgCRfCx8ugdwuEX8KFC6k2EUu
Level 13:	8ZjyCRiBWFYkneahHwxCv3wb2a1ORpYL
Level 14:	4wcYUJFw0k0XLShlDzztnTBHiqxU3b3e
Level 15:	BfMYroe26WYalil77FoDi9qh59eK5xNr
Level 16:	cluFn7wTiGryunymYOu4RcffSxQluehd
Level 17:	xLYVMN9WE5zQ5vHacb0sZEVqbrp7nBTn
Level 18:	kfBf3eYk5BPBRzwjqutbbfE887SVc5Yd
Level 19:	IueksS7Ubh8G3DCwVzrTd8rAVOwq3M5x
Level 20:	GbKksEFF4yrVs6il55v6gwY5aVje5f0j
Level 21:	gE269g2h3mw3pwgrj0Ha9Uoqen1c9DGr
Level 22:	Yk7owGAcWjwMVRwrTesJEwB7WVOiILLI
Level 23:	jc1udXuA1tiHqjIsL8yaapX5XIAI6i0n
Level 24:	UoMYTrfrBFHyQXmg6gzctqAwOmw1IohZ
Level 25:	uNG9058gUE7snukf3bvZ0rxhtnjzSGzG

```
bandit24@bandit: /tmp/mydir12345
File  Edit  View  Search  Terminal  Help
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Wrong! Please enter the correct pincode. Try again.
Correct!
The password of user bandit25 is uNG9O58gUE7snukf3bvZ0rxhtnjzSGzG
```

General Web Exploits (30 points)

Level 0:	natas0
Level 1:	gtVrDuiDfck831PqWsLEZy5gyDz1clto
Level 2:	ZluruAthQk7Q2MqmDeTiUij2ZvWy2mBi
Level 3:	sJIJNW6ucpu6HPZ1ZAchaDtwd7oGrD14
Level 4:	Z9tkRkWmpt9Qr7XrR5jWRkgOU901swEZ
Level 5:	iX6IOfmpN7AYOQGPwtn3fXpbaJVJcHfq
Level 6:	aGoY4q2Dc6MgDq4oL4YtoKtyAg9PeHa1
Level 7:	7z3hEENjQtflzgnT29q7wAvMNfZdh0i9
Level 8:	DBfUBfqQG69KvJvJ1iAbMoIpwSNQ9bWe
Level 8:	W0mMhUcRRnG8dcghE4qvk3JA9lGt8nDl
Level 9:	nOpp1igQAkUzaI1GUUjzn1bFVj7xCNzu
Level 10:	U82q5TCMMQ9xuFoI3dYX61s7OZD9JKoK

PortSwigger Specific Attacks (10 points)
Now go to https://portswigger.net/web-security and register for an account. Go through and complete any 5 of the SQL Injection labs, as well as any 5 XSS attacks and any two CSRF attacks. They are very generous with their solutions, in that it's extremely easy to click on all of them and complete them right away. Resist this urge, and try it for a while before giving in. However, even more importantly, they offer a wealth of good information about each of these attacks, so please read that as you're going about each section to try and gain a deeper understanding. In your report, please make sure you specify which ones you completed. There's no need to provide a solution, since they're all on the respective page. Hint: There are solutions for each of the challenges, but don't look at them immediately! If you do not review the content carefully and struggle through each of the challenges, you will not learn what you need to in order to complete the next challenge. Also, PortSwigger is the company that creates BurpSuite, so of course their solutions will tend to want you to use their product. You should set up a session and install an SSL cert - see links to do this on Piazza. Also, don't forget about URL encodings.

SQL Injection Labs Completed:

- Lab: SQL injection vulnerability in WHERE clause allowing retrieval of hidden data
- Lab: SQL injection UNION attack, retrieving data from other tables
- Lab: SQL injection UNION attack, determining the number of columns returned b the query
- Lab: SQL injection UNION attack, finding a column containing text
- Lab: SQL injection UNION attack, retrieving multiple values in a single column

XSS Attacks Completed:

- Lab: Reflected XSS into HTML context with nothing encoded
- Lab: Reflected XSS into HTML context with all tags blocked except custom ones
- Lab: Reflected XSS with event handlers and href attributes blocked
- Lab: Reflected XSS in canonical link tag
- Lab: Stored XSS into HTML context with nothing encoded

CSRF Attacks Completed:

- Lab: CSRF vulnerability with no defenses: Used Burp Suite Community Edition to fill in an HTML request which we can use as a HTML exploit on the exploit server.
- Lab: CSRF where token validation depends on request method: For this one, changing the csrf value resulted in the request getting denied. Changing the request method to a GET allows us to get in and use an HTML exploit on the exploit server.

A Real Challenge (40 points)

Many companies have hacking challenges where, if you break them, then you get fast-tracked to a job at their company. Now… go get a job! Because of the nature of these challenges, the solutions are not likely to be online. Also, if you work on some company's challenge as a group, do not take that submission and apply for a job with it. That is dishonest, and a violation of our goal of ethical behavior in this class. However, if you all complete the challenge individually, simply note that on your report, and then go claim your job! You are all welcome to each perform this challenge individually. Also note that some of these challenges may be a small step up from what we're used to in this course, which is why they're worth so much credit. However, if you've understood everything, it should be well within reason to complete. So, this challenge is a little different. The challenges are for the company Assured Information Security (AIS), at https://hack.ainfosec.com/. The course staff is in no way affiliated with this company. Go here and complete all 3 Input Validation challenges, as well as the first Exploitation challenge (for 75 points). To receive credit, submit all of the regular explanations for each challenge, as well as your ID for the challenge. It will look something like Your ID: 26ab8eb9-238c-aa8b-8319-c8cb21394a5e. Hint: Because these are used by actual companies to recruit top talent, we can't provide much help in office hours. In fact, if you find you're completely stumped, you should go back to the previous challenges and work through those. However, if you really put your mind to the previous challenges, then this one should be very manageable! Just pay close attention to the descriptions of what they want you to do.

Maura's ID: 5a615dee-d728-4512-9c8f-e3e0f9c50583

Input validation SQL validation: put ' OR 1=1 -- which prints all the usernames and passwords and just copy and paste the password for farnsworth into the password input field

Input validation 75:

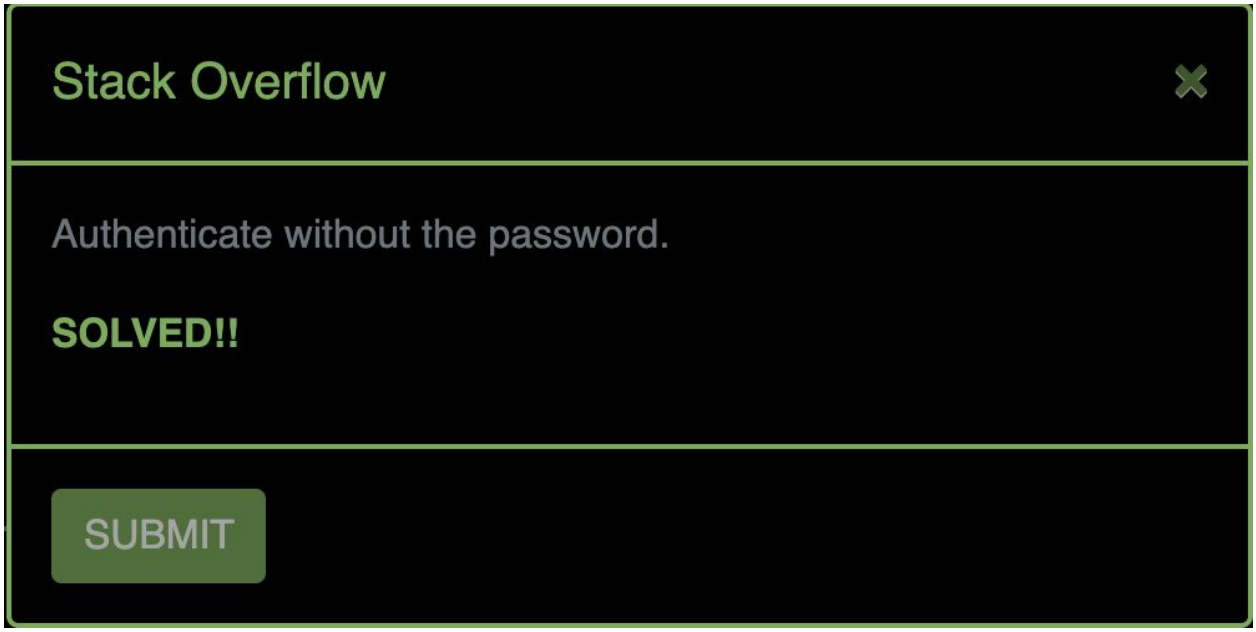
https://hack.ainfosec.com/static/hackerchallenge/img/smile-cookie.png

Calvin's ID: 905eca73-471d-4f4c-855f-de1b74f341b9

Stack Overflow Challenge: My input : "----------2" , authentication value = 50

Basically solved this by finding the amount of characters needed to overflow into the authentication value. Printed the values of each variable then used that to find my authentication

value.

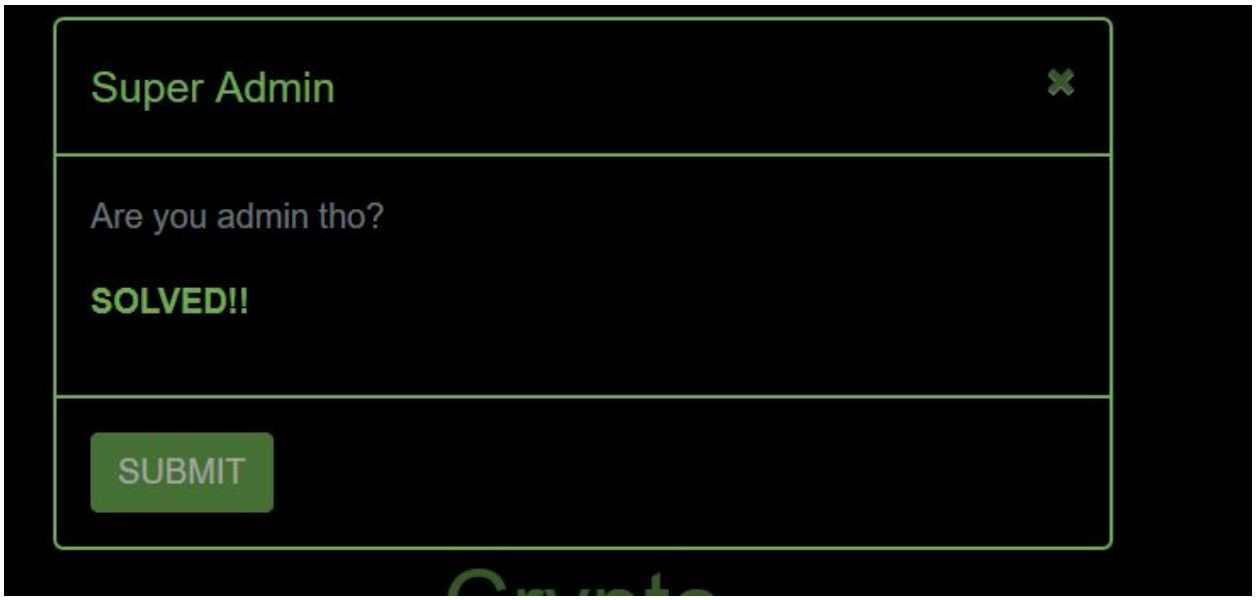



```
Enter the password: ----------2
******** <-- checkpass value  ----------2 <-- password value  50 <-- authentic
ated value  Success!
```

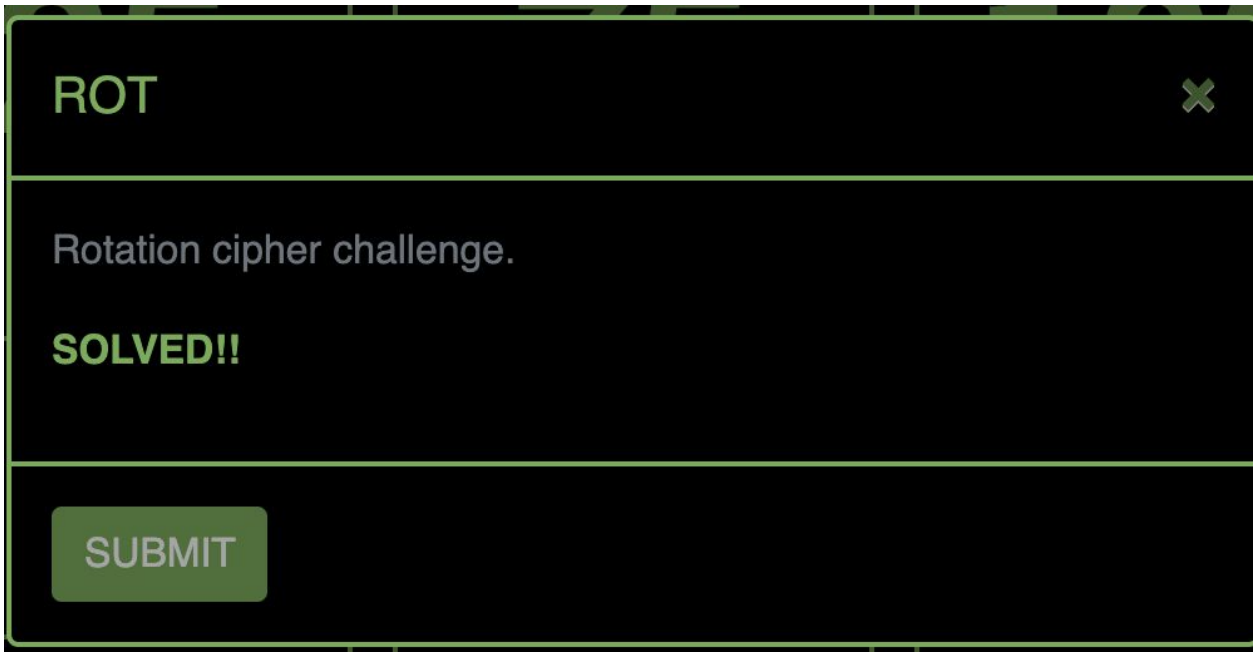
ID:

Extra Credit: Get a Job (40 points) Difficulty: 9 Take the AIS challenge, or some other comparable challenge, and complete it! For full credit, you must show that you completed a challenge by a company sufficiently to get a job. You're already on a good start after the "A Real Challenge" section, so feel free to use your progress there. You will receive 40 points if you complete a challenge to the company's satisfaction. However, on the AIS site, you'll need to complete 670 points to receive all 40 extra credit points, since 300 came from the regular homework. From there it's a linear scale, so you'll receive (x-300)/(670-300)*(40) points. For example, if you earn 450 points, you'll receive (450-300)/(670-300)*(40) = 18.75 extra credit points. Once again, all team members are welcome to complete this individually, then apply for the job. However, if you complete it as a team, then you shouldn't apply for the position using that code. Please don't ruin the experience for the company, your classmates, and future students, as well as your own reputation and credibility. To submit your work for this one for AIS, please use the same ID as the last challenge. If you use a different site, submit their token or whatever they use. You may also need to document

Client-side Protections 10 - change admin cookie to true



Crypto Challenge 15 - It’s a Caesar Cipher. Use a rotating algorithm online



Submission Upload a new document with your answers. At one point in the document it should contain the following: 1. Your team members’ names and emails. 2. A description

of what each team member contributed. One person in the group should turn in a single document to Moodle, but each member should contribute, though naturally, you will contribute to different things. 3. Your descriptions and proofs of challenge completions, as specified in each section.